

Cadre de cohérence technique des systèmes d'information et de communication du Ministère des Armées et des Anciens Combattants

CCT 2026-2027 (Version 3.7)

[CCT-MinArm 2026-2027-3.7-17/02/2026]

Rédaction	Contributions : CND, DGA, EMA, SGA Coordination : AGORA Tech]	CND, EMA, SGA
Commentaires Contributions	Experts du ministère	DGA (DIE-IP/MI/S2NA), CND (EMO, SDCS, POENT, PODEV-CDAD, POHEB, SERVPROJ, GOUVSTRAT, CASID, EMA/SNA), EMA(COMCYBER, SNA), SGA (DTPM, MAP, SMSIF-RH), DPID, DSI Domaine
Validation	AGORA Tech	
Validation	Olivier GANIS, sous- directeur de la transformation numérique	CND / GOUVSTRAT / SD GOUV NUM
Validation	GDA Hervé GUILLERAULT, chef du service GOUVSTRAT	CND / GOUVSTRAT
Approbation	GCA Erwan Rollan, Général Commissaire	CND

Évolutions

Edition	Date	Évolution
Version initiale	18 août 2014	Diffusée par courrier n°526/DEF/DGSIC/SDAU/DR du 21/08/14
V2	26 juillet 2016	Diffusée par courrier n°451/DEF/DGSIC/SDAU/DR du 28/07/16
V3	16 juillet 2018	Diffusée par courrier n°316/ARM/DGNUM/DG/DR du 18 juillet 2018
V3.1	Juillet 2019	Diffusée par courrier n°302/ARM/DGNUM/DG/DR du 26 juillet 2019
V3.2	Juillet 2020	Diffusée par courrier n°280/ARM/DGNUM/DG du 28 juillet 2020
V3.3-2021	Octobre 2021	Diffusée par courrier n° 447/ARM/DGNUM/DG/DR du 10 novembre 2021
V3.4-2022	Novembre 2022	Diffusée par courrier n° 505/ARM/DGNUM/SDTN/DR du 29/11/2022
2023-2024 (V3.5)	Novembre 2023	Diffusé par courrier n° 736/ARM/DGNUM/SDTN/DR du 20/12/2023 Actualisée par l'édition 2 publiée en juillet 2024
2024-2025 (V3.6)	Janvier 2025	Diffusé par courrier n° n°141/ARM/DGNUM/SDTN/DR du 05/03/2025 Actualisée par l'édition 2 publiée le 16 juillet 2025
2026-2027 (V3.7)	Mars 2026	Diffusé par courrier

Sommaire

1	Généralités	9
1.1	Objet du document	9
1.2	Périmètre.....	10
1.3	Domaine d'application – Acteurs concernés	10
1.4	Gestion et gouvernance du CCT	11
1.5	Prise en compte dans le cadre des cahiers des charges.....	11
1.6	Organisation du document.....	12
1.6.1	Organisation générale du document	12
1.6.2	Pile logicielle et environnements d'exécution.....	12
1.7	Codification des références du CCT	12
1.7.1	Références documentaires – Typologie de documents.....	12
1.7.2	Règles et recommandations additionnelles	13
1.7.3	Normes et standards	14
1.7.4	Produits et solutions	14
1.8	Critères d'éligibilité des produits et solutions	15
1.8.1	Contraintes à respecter et critères d'appréciation.....	15
1.8.2	Évolutions	15
1.8.3	Le CCT et l'innovation	15
1.9	Conformité au CCT.....	16
1.9.1	Validation des architectures des SI.....	16
1.9.2	Processus de saisine pour validation d'architecture ou dérogation au CCT	16
2	Cadres référentiels généraux.....	16
2.1	Les référentiels internationaux.....	16
2.1.1	OTAN.....	16
2.1.2	Européen	18
2.2	Le cadre interministériel	19
2.2.1	La stratégie du SI de l'État – Doctrine cloud	19
2.2.2	Politique de la donnée - Logiciels Libres – ouverture des codes.....	20
2.2.3	Les référentiels interministériels	21
2.2.4	Communication gouvernementale - Charte Internet de l'État – Charte graphique.....	23
2.2.5	Les outils et l'offre de service au niveau interministériel.....	24
2.3	Le cadre ministériel	25
2.3.1	Politique SIC ambition numérique	26
2.3.2	Architecture générale, politique logicielle.....	26
2.3.3	Socle numérique.....	26
2.3.4	SIC opérationnels – FrOpS.....	26
2.3.5	Sécurité.....	27
2.3.6	Gouvernance	27
2.3.7	Relation client – Offre de service - DIADEME	29
3	Services communs	29
3.1	Services à l'utilisateur	30

3.1.1	Environnement de travail	30
3.1.2	Collaboratif	40
3.1.3	Vie courante	43
3.1.4	Gestion des données	45
3.1.5	Sécurité [SU-SSO, SU-CHI, SU-SIG]	46
3.1.6	Mobilité [SU-AN, SU-ITN]	46
3.1.7	Accès réseaux extérieurs	48
3.1.8	Téléphonie.....	49
3.1.9	Services divers	50
3.2	Socle des applications	51
3.2.1	Généralités.....	51
3.2.2	Hébergement d'applications.....	58
3.2.3	Portail des applications métier	65
3.2.4	Échanges entre applications	66
3.2.5	Données et contenu	74
3.2.6	Informatique « décisionnelle », Big Data, analyse prédictive	88
3.2.7	Cadres particuliers.....	93
3.2.8	Démarche simplifiée (DS) – Dossier numérique de l'agent (DNA).....	97
3.2.9	Intelligence artificielle.....	98
3.2.10	Internet des objets – IOT.....	99
3.3	Services d'infrastructure.....	99
3.3.1	Messagerie / Agenda / Tâches / Listes de diffusion	99
3.3.2	Partage d'information et publication.....	101
3.3.3	Travail de groupe	104
3.3.4	Services d'annuaires [ANN]	106
3.3.5	Utilitaires d'infrastructure	108
3.3.6	Services communs réseau.....	108
3.3.7	Systèmes d'exploitation [OS].....	110
3.4	Services de sécurité.....	110
3.5	Services d'administration et de gestion	110
4	Sécurité.....	110
4.1	Documents de référence	110
4.1.1	Document généraux.....	110
4.1.2	Références pour le non classifié (NP-DR-sensible) et le NR	113
4.1.3	Références pour le niveau Secret	114
4.1.4	Référence pour le SO	114
4.1.5	Références pour le SUE	114
4.1.6	Références pour la protection des informations avec les Nations Unies	114
4.1.7	Accès à la documentation technique	115
4.2	Démarche de sécurité	115
4.2.1	Homologation.....	115
4.2.2	Maintien en condition de sécurité.....	118

4.2.3	Audits	118
4.2.4	Réduction de l'exposition cyber des SI	119
4.3	Cryptographie et gestion des ACSSI.....	119
4.4	Protection contre les signaux compromettants	120
4.5	Sécurisation des COTS.....	120
4.6	Services de sécurité.....	121
4.6.1	Sécurisation des accès	121
4.6.2	Gestion des clés – certificats électroniques [IGC].....	128
4.6.3	Gestion de la preuve	130
4.6.4	Surveillance - Outils LID, détection d'intrusion [SUR] [DEA]	131
4.6.5	Utilitaires de sécurité.....	131
4.6.6	Supports de stockage sécurisés.....	134
4.7	Interconnexions, passerelles et solutions de sécurité iso/multi niveaux	134
4.7.1	Passerelles d'échanges	134
4.7.2	Passerelles transdomaines	134
4.7.3	Autres passerelles.....	136
4.8	Administration de la sécurité.....	136
4.8.1	Gestion des utilisateurs et des droits	136
4.8.2	PCA-PRA	136
4.8.3	Gestion des journaux d'évènements applicatifs ou système.....	137
4.8.4	Maintien en condition de sécurité (MCS) - composant technique.....	138
4.8.5	Sécurisation des flux réseaux	138
4.8.6	Sécurisation des supports de stockage.....	138
4.8.7	Hébergement / Virtualisation	139
4.8.8	Supervision de la sécurité, LID	139
4.8.9	Télémaintenance.....	139
4.8.10	Sauvegardes	140
4.8.11	Gestion de configurations de sécurité	140
4.9	Divers.....	141
5	Infrastructure.....	141
5.1	Matériels, OS, virtualisation et conteneurisation.....	141
5.1.1	Système d'exploitation [OS]	141
5.1.2	Virtualisation.....	144
5.1.3	Conteneurisation.....	147
5.1.4	Poste terminal : fixe / mobile (portable, smartphone, tablette).....	152
5.1.5	Impression et scanners	152
5.1.6	Stockage	152
5.1.7	Téléphonie.....	153
5.2	Réseaux.....	154
5.2.1	Généralités.....	154
5.2.2	Réseaux de transport WAN et routage	156
5.2.3	Services de réseaux de desserte	157

5.2.4	Services des réseaux étendus : filtrage - passerelles [FIL-PAS]	157
5.2.5	ToIP / VoIP	157
5.2.6	Réseaux sans fils	157
5.2.7	Liaison satellitaires.....	158
5.2.8	Équipements : LAN, Routage, Switch, Pare feu, accélérateurs... ..	158
5.2.9	Équipements de chiffrement.....	158
5.2.10	VPN	158
5.2.11	Baies	159
5.2.12	Câblage	159
6	Cadre fonctionnel et technique d'hébergement.....	159
6.1	Plateformes d'hébergement	159
6.1.1	Références générales sur l'hébergement	159
6.1.2	Typologie d'environnements sur les plateformes.....	160
6.1.3	Les niveaux de service d'hébergement.....	161
6.1.4	Processus d'hébergement	161
6.1.5	Hébergement sur Intradef.....	162
6.1.6	Hébergement sur Internet	167
6.1.7	Hébergement mutualisé SIA sur les intranets classifiés	169
6.1.8	Informatique décisionnelle	170
6.2	Opérations – processus.....	170
6.2.1	Gestion des configurations	170
6.2.2	Gestion des demandes	172
6.2.3	Déploiement / Distribution / Orchestration	172
6.2.4	Gestion du stockage	173
6.2.5	Synchronisation / Réplication / Déduplication.....	174
6.2.6	Sauvegarde / restauration	174
6.2.7	Observabilité	174
6.2.8	PCA/PRA – PCI/PRI - Gestion de crise.....	177
6.2.9	Gestion d'exploitation et des capacités	178
6.2.10	Hypervision.....	178
6.2.11	Administration réseaux, performance réseaux et Télécommunications	178
6.2.12	Surveillance et métrologie des salles	178
7	Conception – Développement.....	178
7.1	Règles générales	178
7.2	Analyse, modélisation	179
7.3	Développement.....	180
7.3.1	Outils de développements internes	180
7.3.2	Développement en Java.....	182
7.3.3	Développement en PHP	183
7.3.4	Développement en C# et .NET.....	184
7.3.5	Développement HTML5-Javascript-CSS.....	184
7.3.6	Réalisation d'applications mobiles.....	187

7.3.7	Développement à l'aide d'outils « low-code » ou « no-code »	188
7.3.8	Autres langages	189
7.3.9	Sécurisation du code.....	189
7.3.10	Développement à partir de grands modèle de langage (LLM).....	190
7.4	Test et intégration (pré-intégration, intégration continue)	191
7.4.1	Tests unitaires.....	191
7.4.2	Tests d'intégration des composants.....	191
7.4.3	Intégration continue.....	192
7.4.4	Tests de performance	192
7.5	Qualité logicielle.....	193
7.5.1	Qualité du code	193
7.5.2	Performance - Métrologie	194
7.6	Gestion des anomalies	195
8	Annexes	196
8.1	Changements notables de la présente édition.....	196
8.1.1	Mise à jour et actualisation (hors pile logicielle)	196
8.1.2	Mise à jour et actualisation de la pile logicielle	196
8.2	Glossaire / liens utiles	196
8.3	Piles logicielles du développement sur PICSEL	199
8.4	Règles de nommage	199
8.4.1	Nommage des fichiers.....	199
8.4.2	Annuaire - Identifiant unique - Adresse messagerie.....	199
8.4.3	Nommage DNS	199
8.4.4	Nommage des serveurs.....	200
8.4.5	Nommage composants d'infrastructure de télécommunication.....	200
8.4.6	Nommage VLAN	201
8.4.7	Adressage IP.....	201
8.4.8	Marquage de la sensibilité des informations numériques	201
8.5	Référentiels / Nomenclatures	202
8.5.1	Cartographie des services.....	202
8.5.2	Catalogue des OID	202
8.5.3	Trigrammes de sites géographiques	202
8.5.4	Mots clés d'attribution (MCA).....	202
8.6	Critères d'éligibilité des produits et solutions	203
8.6.1	Objectifs et contraintes.....	203
8.6.2	Critères généraux d'appréciation.....	203
8.6.3	Critères d'éligibilité pour des modules de CMS	205
8.7	Modèles d'architecture.....	205
8.7.1	Introduction aux modèles d'architecture	205
8.7.2	Modélisation des SI avec Archimate.....	208
8.7.3	Modèles d'architectures logiques de référence	211
8.7.4	Catalogue des modèles d'architecture applicatives	215

8.8	Produits / Piles logicielles d'exécution	220
8.8.1	Modules pour CMS Drupal, Joomla ! et Wordpress	220
8.8.2	Pile logicielle : liste des produits.....	220

Table des illustrations

Route API.....	71
SQLite	77
PouchDB	78
Redis.....	78
Cassandra	79
Pgvector.....	79
influxdb	79
S3.....	81
Typologie des environnements sur les plateformes.....	160
Bronze	161
Argent.....	161
Or.....	161
Platine.....	161
A Pattern Language	206
Pattern Oriented Software Architecture	208
Description d'un SI dans Archimate	209
Composant Applicatif.....	209
Composant Interface.....	209
Service Métier	209
Objet.....	209
Framework VueJS	210
Réalisation.....	210
Association.....	210
Lien Service.....	211
Lien dynamique.....	211
Architecture applicative	212
Architecture applicative (modèle logique)	215
Modèle d'architecture PHP	216
Modèle d'architecture Javascript.....	217
Modèle d'architecture applicative Javascript sur le Frontend et Java en Backend	218
Modèle d'architecture applicative de transition permettant d'assurer la modernisation progressive d'un SI « historique » Java	219
Modèle d'architecture « client-léger » permettant un mode déconnecté.....	219

1 GENERALITES

1.1 Objet du document

Le cadre de cohérence technique [CCT] constitue le référentiel ministériel des préconisations et choix techniques relatifs au socle du système d'information du ministère des armées et aux grands composants d'architecture technique.

Il s'inscrit dans le cadre documentaire technique du ministère dont le document d'architecture technique générale des SIC du Ministre des Armées et des Anciens combattants [ATG] est le cadre de référence et complète le référentiel d'architecture technique en décrivant les principaux motifs d'architecture technique mis en œuvre.

Il précise les vues « applicative », « logicielle » et « infrastructure » liées à la démarche d'urbanisation du ministère en déclinaison de la politique ministérielle relative aux SIC.

Conformément à son mandat ¹, l'animation et la réalisation du présent document sont effectuées par l'AGORA Tech qui soumet deux fois par an une nouvelle version à la validation du CECNUM et à la signature du CND.

1.2 Périmètre

De façon globale, le CCT est un référentiel des choix techniques du ministère des armées dans le domaine des SIC. Il concerne essentiellement le domaine technique SIC ayant trait aux intranets du ministère². Le CCT peut le cas échéant être amené à couvrir des segments en couplage même lâche avec les Intranets IP du ministère dès lors que cela présente un intérêt pour l'ensemble de la communauté SIC.

Il décline les chapitres du document [ATG] relatifs aux services communs (services à l'utilisateur, services techniques, socle applicatif), aux services et outils de sécurité, à l'hébergement, l'administration et l'exploitation, à l'infrastructure (réseau, téléphonie, configuration logicielle et matérielle standard), dont il précise les choix techniques. Il couvre également les règles de conception et de développement du ministère. Il a vocation à préciser les préconisations et choix relatifs aux services communs des intranets décrits dans la cartographie des services communs du ministère des armées [CARTO]³.

Le CCT décline le principe de standardisation, combinaison de briques technologiques maîtrisées comme norme et le « sur mesure » comme exception.

La conformité au CCT constitue un des critères d'appréciation dans les revues d'approbation de projets de systèmes d'information relevant des instructions 8 et de l'instruction ministérielle 1618 dans le cadre de la conduite des projets SIC (y compris composants logiciels d'un programme d'armement), et dans l'instruction pour avis conforme prévu à l'article 5 du décret du 28 juin 2018 précité.

1.3 Domaine d'application – Acteurs concernés

Ce référentiel doit être pris en compte par les projets de SIC et référencé dans le cadre des marchés publics ([voir ci après](#)). Tout système d'information ou composant logiciel proposé pour une utilisation tant sur les réseaux du Ministère que sur Internet doit respecter les recommandations du CCT en vigueur au début de sa réalisation et en suivre les évolutions tout au long de son cycle de vie (cette conformité constitue une condition préalable à tout passage en environnement de préproduction ou de production, notamment pour les plateformes C1NP et C1DR). En conséquence, **les évolutions du CCT devront notamment être prises en compte pendant la réalisation des travaux** et dans le cadre de la tierce maintenance d'administration / d'exploitation, a minima pour ce qui concerne les correctifs de sécurité et la gestion de l'obsolescence. Le processus de révision annuelle du CCT tient compte de cette contrainte et s'attache à éviter toute modification brutale toutes les fois que c'est possible.

Le CCT s'adresse à tous les acteurs du numérique du Ministère:

- **Aux directions des systèmes d'information et aux directions d'application**⁴ pour leur présenter les choix et orientations du ministère pour l'accueil, l'hébergement, et l'environnement des systèmes d'information et les aider dans la conduite de leur projet, notamment dans la prise en compte dans les marchés du contexte technique ministériel ; le non-respect du CCT nécessitera pour les directions d'application de justifier leur choix et d'initier des demandes de dérogation ([voir ci après](#)). Par défaut, toute direction d'application doit s'efforcer d'en respecter les parties qui peuvent lui être applicables.

¹ Mandat diffusé par note n°2025/508/ARM/CND/GOUV STRAT/NP du 18 novembre 2025

² Les systèmes d'information hébergés par des sous-traitants doivent respecter les règles de l'intranet auquel ils sont rattachés.

³ cf. [la cartographie des services en annexe](#)

⁴ Par direction d'application, on entend ici l'ensemble des acteurs travaillant au sein ou au profit d'une direction de projet ou de programme (responsable de conduite de projet, responsable fonctionnel, experts techniques ou métier, rédacteurs de marché...).

- **Aux acteurs techniques de la communauté SIC** aux fins de partage, de cohérence et de pilotage de l'évolution des compétences techniques nécessaires au ministère ; le CCT est un outil de partage permettant à des acteurs techniques parfois dispersés de partager une même vision des composants d'architecture et des choix techniques du ministère ; il est également un levier de cohérence du corpus documentaire technique du ministère permettant d'identifier des références redondantes ou en recouvrement, d'identifier des obsolescences ou des lacunes et d'en tirer un plan de travail de mise en cohérence ; le CCT constitue un outil utile dans le cadre d'une démarche visant à assurer l'adéquation entre les compétences techniques existantes ou prévues et les besoins, notamment dans le cadre d'une GPEC⁵ sur les compétences techniques ;
- **Aux acteurs en charge de développements internes** au ministère dont il constitue le cadre de référence.
- **Aux partenaires** étatiques, alliés ou industriels à titre d'outil de communication et de partage, le CCT pour connaître et positionner efficacement les choix du ministère en interministériel notamment dans le cadre des travaux pilotés par la DINUM, comme en interallié et informer les fournisseurs et industriels travaillant au profit des SIC du ministère et d'orienter leurs travaux pour une meilleure prise en compte du contexte ministériel.

Afin de répondre au mieux à ces besoins de communication du CCT vis-à-vis d'entités externes au ministère, la version non protégée (le présent document) permet une diffusion plus large mais doit être encadrée et maîtrisée. Pour faciliter la recherche dans la pile logicielle autorisée, la liste des logiciels autorisés (version NP) est disponible également en format tableur.

1.4 Gestion et gouvernance du CCT

Conformément aux textes en vigueur, la gouvernance des architectures technique et applicative s'appuie sur l'AGORA Tech pour valider les architectures des systèmes d'information du ministère.

Le CCT est un document vivant, mis à jour deux fois par an, prenant en compte les besoins projets qui seront exprimés au travers de leur DSI de rattachement.

1.5 Prise en compte dans le cadre des cahiers des charges

Le présent CCT doit être référencé dans les CCTP⁶. Une formulation possible⁷ est donnée ci-après :

« L'architecture et la pile logicielle du système doivent être conformes au CCT. Tout écart devra faire l'objet d'une justification à faire valider en AGORA Tech. Il est précisé que la saisine de l'AGORA Tech demeure de la responsabilité de la direction de projet qui pour ce faire, s'appuiera autant que de besoin sur son titulaire. Les évolutions du CCT devront être prises en compte pendant la réalisation des travaux et la période de MCO/MCS. » Le CCT doit être ajouté en document applicable dans le marché.

Toute difficulté rencontrée lors de la mise en œuvre du cadre de cohérence technique devra être signalée à l'AGORA Tech.

Afin de s'assurer de la conformité d'une solution au CCT, il est nécessaire de savoir de connaître les dépendances qui la compose. Outre le référencement au CCT, il est important que le CCTP comporte une exigence demandant la liste des composants logiciels utilisés, préférablement sous forme de SBOM (Software Bill of Materials).

Règle	Énoncé	Statut	Portée
CCT_R1_1	Il est RECOMMANDÉ de fournir la liste exhaustive des composants utilisés dans le système d'information, y compris les dépendances des applicatifs développés.	R	Min Arm

⁵ Gestion prévisionnelle des Emplois et Compétences

⁶ Cahier des Charges Techniques Particulières

⁷ Formulation adaptée de clauses analogues du CCT du ministère de l'Intérieur

CCT_R2_1	Il est RECOMMANDÉ que la liste des composants utilisés dans la solution soient transmise dans un des formats standards utilisé pour les Software Bill of Materials (SBOM).	R	Min Arm
----------	---	---	---------

1.6 Organisation du document

1.6.1 Organisation générale du document

La structure du document est cohérente avec le document d'architecture technique générale des SIC du ministère des armées et, pour les chapitres en relevant, avec la cartographie des services des Intranets des armées [CARTO]⁸ :

- Une **partie principale référençant les documents normatifs, guides de paramétrage, règles additionnelles éventuelles** ne se retrouvant pas dans un document référencé, ainsi que les principaux choix logiciels ou interfaces normatives et tout élément ayant vocation à rejoindre le référentiel commun technique du ministère ;
- Un **ensemble d'annexes** complétant ce corpus dont principalement :
 - le catalogue des produits et solutions autorisés dans le ministère, et notamment la pile logicielle soutenue ou exploitée par les structures d'hébergement du ministère (dont CND) selon les environnements ainsi que les piles d'exécution ;
 - le référentiel de l'environnement de développement ;
 - la liste des bibliothèques applicables à certaines technologies.

Les références identifiées dans ce cadre (références documentaires, règles additionnelles, normes/standards et produits/solutions) sont répertoriées dans des cartouches dont les modèles et la codification sont précisés [ci-après](#).

1.6.2 Pile logicielle et environnements d'exécution

Le présent CCT décrit les solutions et produits déployés à différents niveaux au sein du ministère des Armées, avec ou sans le soutien de l'opérateur Défense. La liste exhaustive des produits est jointe au CCT sous l'intitulé « Pile logicielle ». Ce document précise les versions et les statuts de chaque produit, en fonction de son périmètre d'utilisation.

Par ailleurs, il existe des services constitués d'un assemblage de composants intégrés. Il est préférable de privilégier ces services aux briques technologiques sous-jacentes. Parmi ceux-ci, on trouve par exemple la pile d'exécution des structures d'hébergement, la pile de la plateforme décisionnelle, l'environnement de développement interne et des services de socle. Certains de ces environnements techniques sont également détaillés dans le CCT.

1.7 Codification des références du CCT

1.7.1 Références documentaires – Typologie de documents

Document	Date	Origine	Type doc	Portée
①	②	③	④	⑤
⑥ <i>Commentaire: périmètre, recouvrement, évolutions, imprécisions, niveau d'application (difficulté, application non avérée, ...)</i>				

① **Document** : titre + éventuelle référence (timbre)

⁸ La structuration du CCT est aussi compatible avec les NRI/NRA du Cadre Commun d'Urbanisation (CCU) du SI de l'État entretenu par la DINUM (cf. [la cartographie des services en annexe](#)).

- ② **Date** du document : sous la forme : JJ Mois AAAA
- ③ **Origine** : Autorité signataire ou chargée de l'entretien
- ④ **Type de document** : Directive / Note / ITE / Guide / Concept d'emploi / Livrable industriel/Projet
- ⑤ **Portée**{#portee} : peut être de nature différente suivant la référence:
- Organisation : OTAN, UE, France, Interministériel, MinArm, Organisme ;
 - Déploiement : Intradef, Intraced niveau Secret-SF (S-SF), Très Secret (TS), FrOpS, Internet, SIE (segment Intradef embarqué), IST, PICSEL, ... ;
 - Confidentialité: NP, DR, Secret-SF, Secret, Très Secret (TS)... ;
 - Métier : SIAG, SIOC, SI3E, ... ;
- ⑥ **Commentaire** : périmètre, recouvrement, difficulté(s) ou subtilité(s) de mise en œuvre, évolution proposée ou à venir, modalités d'assujettissement ...

1.7.1.1 Typologie de documents

Globalement, les documents de ce référentiel peuvent être classés en 4 grandes catégories :

- Cadre juridique applicable : traités ou accords internationaux, textes européens (règlement/directive), loi, ordonnance, décret, arrêté, circulaire, instruction interministérielle ou ministérielle, référentiels généraux ;
- Cadre général ministériel : politique, stratégie, doctrine ou concept d'emploi, SLR ;
- Cadre technique normatif ou référentiel : STANAG, politique de sécurité, directive, cadre technique, ITE, référentiel ;
- Cadre technique d'accompagnement : guide, note technique, manuel, rapport technique ; documents ou livrables projets...

1.7.2 Règles et recommandations additionnelles

De façon générale les règles recommandées ont vocation à être incluses dans des documents référencés (exemple : les directives) par le CCT. Cependant, lorsque cela présente un intérêt particulier, et si la règle n'est encore présente dans aucun autre document, il est possible de référencer une telle règle directement dans le CCT.

Règle	Énoncé	Statut	Portée
① 1	②	③	④

① **Règle** : CCT_RN (N numéro)

② **Énoncé** de la règle

③ **Statut** : Obligatoire / Recommandé / Déconseillé / Interdit (cf. ci-dessous)

④ **Portée** : cf. [paragraphe précédent](#)

Les niveaux{#niveaux} de recommandation sont conformes à la [RFC 2119] :

- **OBLIGATOIRE** : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;
- **RECOMMANDÉ** : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente;
- **DÉCONSEILLÉ** : ce niveau de préconisation signifie que la règle édictée indique une contre-indication qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé;
- **INTERDIT** : ce niveau de préconisation signifie que la règle édictée indique une interdiction absolue de la directive.

Toute demande de dérogation à ces règles doit être présentée en AGORA Tech pour instruction et recommandations (cf. [ci-après](#)).

1.7.3 Normes et standards

Le CCT n'a pas vocation à recenser l'ensemble des normes et standards du domaine couvert. Cependant, lorsque cela présente un intérêt particulier, il est possible d'inclure dans ce document une norme.

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
①	②	③	④

① **Norme/standard** : nom commun de la norme ou du standard

② **Description** de l'usage et de ses conditions d'utilisation au sein du MinArm

③ **Statut** : Obligatoire / Recommandé / Déconseillé / Interdit (cf. ci-dessus)

④ **Portée** : cf. ci-dessus

1.7.4 Produits et solutions

Ce document référence les solutions ou produits logiciels principaux, ainsi que les orientations principales. Pour plus de détails (version, sous-version...), se référer à l'annexe détaillée de la pile logicielle dont la structure est calquée sur le sommaire du CCT.

Par ailleurs, généralement et sauf contraintes liées à leur mise à disposition sur les réseaux ministériels, les versions indiquées sont les versions minimales autorisées.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
①	②	③	④	⑤	⑥
Commentaire: éventuel pour préciser le cadre d'emploi, l'usage, ...					

① **Solution** : par exemple : grand composant : messagerie,

bureautique, MCS, virtualisation...

② **Produit** : nom du produit ou du service logiciel (ou matériel ou nom de la solution si celle-ci est packagée) / version majeure. L'insertion d'un tel produit dans le CCT est soumis à une présentation préalable, suivi d'un avis, en AGORA Tech. ci-dessous).

③ **Fournisseur** : éditeur / communauté libre ... S'il s'agit d'une solution interne : nom ou organisme point de contact (cf. ci-dessous)

④ **Utilisation / restriction** : conditions éventuelles d'utilisation dans le ministère

⑤ **Statut** : sur deux lettres :

- La première relative au niveau de **recommandation** :
 - **R : Recommandé** (usage général par défaut) ;
 - **E : Émergent** (il est envisagé de recommander la solution à une date à indiquer en commentaire si connue ou produit à l'étude en vue d'une possible recommandation) ;
 - **A : Assujetti** (à un usage particulier ou nécessitant une autorisation ou une justification, détail fourni en commentaire) ;
 - **D : Déconseillé** (obsolescence, abandon par l'éditeur ou autre) ;
 - **I : Interdit** (formellement interdit) ;
 - - : aucune politique sur le produit n'a encore été définie au niveau du ministère ;
 - * : dépend de la version, se référer à l'annexe 8.2.
- La seconde relative à la nature du **soutien** par l'opérateur (optionnelle) :
 - **S : soutenu** : conditions particulières éventuellement préciser en commentaires ;
 - **E : soutien envisagé** à une date à indiquer, si connue, en commentaire ;
 - **O : obsoléscent** bien qu'encore soutenu (retrait futur à anticiper) ;
 - **N : non soutenu** (en cas d'autorisation d'emploi du produit concerné, son soutien devra être assuré par la direction d'application) ;
 - - : le niveau de soutien reste à définir ;
 - * : dépend de la version, se référer à l'annexe 8.2.

Une solution ayant le statut ‘E’, ‘O’, ‘N’, ou ‘-’ ne pourra pas prétendre à une offre infogérance du CND. En conséquence, la direction d’application devra assumer seule l’exploitation technique (l’application des correctifs de sécurité restant obligatoire dans les délais prescrits).

⑥ **Portée** : cf. [plus haut](#)

Les portées SIA S-SF et SIA FrOpS renvoient par défaut au périmètre SIA, il existe encore des bulles historiques Intraced Air, SICF ou FrOpS qui n’utilisent pas forcément le produit ou la solution.

1.8 Critères d’éligibilité des produits et solutions

1.8.1 Contraintes à respecter et critères d’appréciation

Le domaine de l’informatique évolue à un rythme extrêmement rapide. L’introduction d’une nouvelle technologie ou d’un nouveau produit dans le CCT est toujours le fruit d’une équation complexe prenant en compte des besoins et contraintes s’opposant par nature comme l’avantage opérationnel procuré, la maîtrise ou la sécurité du SI, la souveraineté, l’exploitabilité ou encore la rationalisation des choix.

Aussi les demandes d’intégration de nouveaux produits ou solutions dans le CCT comme les demandes de dérogation sont appréciées sur la base d’une grille de critères en termes fonctionnels, de support, de sécurité, de qualité ou encore d’intégration dans le système d’information du ministère.

Les contraintes prises en compte ainsi que les critères d’appréciation sont détaillés en [annexe 8.6](#).

1.8.2 Évolutions

Compte tenu de la nature très évolutive des technologies, le statut associé est susceptible d’évoluer à chaque édition du CCT.

En conséquence, la gouvernance technique (cf. [plus haut](#)) passe en revue régulièrement les technologies recensées et celles qui lui sont soumises par le biais des saisines et demandes de dérogation. Pour ce faire, elle s’appuie sur des expertises identifiées en interne ou en externe (études industrielles, RETEX de nos partenaires, forums, prestations sur mesures, etc).

Toute sollicitation ou contribution spontanée est également bienvenue pour attirer l’attention de la gouvernance technique sur une nouvelle technologie ou une évolution dans un domaine susceptible de faire évoluer une position antérieure.

1.8.3 Le CCT et l’innovation

L’innovation n’a de valeur que dans sa capacité à améliorer durablement le fonctionnement du ministère. Ceci passe avant tout par la mise en œuvre de nouveaux procédés ou l’amélioration des procédés existants en utilisant au besoin les leviers offerts par l’informatique.

Plusieurs outils peuvent répondre à un besoin donné, il convient de choisir celui qui répondra le mieux au besoin dans sa globalité même s’il peut s’avérer être sous optimal pour un aspect spécifique.

Refuser un outil particulier ne signifie donc pas s’opposer à une innovation, mais orienter de manière raisonnée et argumentée vers un autre choix jugé globalement plus efficient.

1.9 Conformité au CCT

1.9.1 Validation des architectures des SI

Afin de préparer et de réduire le risque à l'atterrissage du système d'information sur les infrastructures du ministère, les directions d'application peuvent solliciter les conseils des AGORA (fonctionnelle, tech, cloud et données) dans les processus de gouvernance (cf. [paragraphe Périmètre](#)).

En cas de besoin et sous réserve de la passation de prestations d'assistance, des capacités d'appui, ne se substituant pas aux architectes du projet ou aux DSI domaine, existent pour accompagner le projet dans la consolidation et la vérification de la conformité d'une architecture avant la présentation du projet aux AGORA.

Les conseils des AGORA ne préjuge pas de la validation physique de l'hébergement visé qui est du ressort du plateau d'intégration (validation des matériels physiques, raccordements réseaux, offre de services ou d'hébergement validée, ...).

1.9.2 Processus de saisine pour validation d'architecture ou dérogation au CCT

Les demandes de saisine pour avis AGORA Tech et pour dérogations aux recommandations du CCT doivent être présentées à la gouvernance technique (cf. [paragraphe sur la gouvernance](#) qui instruit ou fait instruire les demandes. Sont concernés notamment :

- la liste de composants logiciels avec leur version ;
- la liste des bibliothèques employées et leurs versions (Java, Javascript, Python, PHP, greffons de CMS, ...) dans les formats demandés ;
- les adhésions à des services tiers (DNS, annuaires, messagerie, PEM, MindefConnect, ...) ;
- les écarts avec les règles prévues par le corpus de directives du ministère ;
- les références des fiches SICLADE SI et Projet .

Toute demande d'étude de projet devra être validée par la DSI de rattachement avant d'être présentée à l'AGORA Tech.

Pour éviter tout report de session, il est rappelé que la direction de projet doit s'assurer de la présence du représentant de la DSI et des compétences nécessaires pour être en mesure de répondre aux questions techniques et d'architecture de l'AGORA Tech (industriels, responsable de réalisation, ...).

2 CADRES REFERENTIELS GENERAUX

2.1 Les référentiels internationaux

2.1.1 OTAN

2.1.1.1 Référentiel NISP

En termes de cadre technique SIC (relevant du périmètre de ce CCT), le référentiel principal d'interopérabilité avec les alliés est le NISP qui fixe les règles d'interopérabilité et les profils d'emploi applicables aux systèmes concourant à la conduite des opérations en réseau NNEC (NATO Network Enabled Capability).

Document	Date	Origine	Type doc	Portée
NATO Interoperability Standard and Profiles (NISP) Edition N Version 2 (STANAG 5524) AdatP-34(N) du 18 août 2023	26 mai 2021	NC3Board	Référentiel	OTAN SIO en interface avec l'OTAN
<i>Commentaire : applicable aux systèmes concourant au NNEC (NATO Network Enabled Capability). Cette version du NISP a été raccourcie et simplifiée Le NISP contient dorénavant 3 volumes :</i> • <i>Volume 1 : introduit les concepts de base, et définit les modalités de gestion du NISP ; il inclut aussi un guide sur le développement de profils d'interopérabilité</i> • <i>Volume 2 : contient les standards et profils d'interopérabilité approuvés et applicables actuellement</i> • <i>Volume 3 : contient les standards et profils d'interopérabilité candidats, applicables aux programmes sous 1 ou 2 ans (dont le profil FMN⁹, répondant à la démarche décrite ci-après).</i> <i>Cette nouvelle version introduit la notion de Base-Standards Profile (BSP) qui renvoie à un profil des meilleures pratiques n'appartenant pas à des profils spécifiques.</i> https://live.nisp.nw3.dk/pdf/NISP-v15.pdf				

2.1.1.2 Démarche FMN (Federated Mission Networking)

La mission de la démarche FMN est de développer et de maintenir une capacité C3¹⁰ interalliée au travers de l'établissement commun d'un référentiel de normes d'interopérabilité et de procédures de mise en œuvre de ce référentiel. Cette capacité s'articule autour de la préparation collaborative par les Affiliés (Nations ou organisations) de forces :

- interconnectées par un réseau de mission constitué suivant des normes et des principes identifiés et expérimentés dans le cadre de l'initiative FMN ;
- dont les capacités d'interopérabilité ont été validées d'un point de vue opérationnel.

Le périmètre technique du FMN couvre ainsi l'interconnexion des réseaux et des moyens de communication, les services communs, les applicatifs C2 (Command & Control) et les fonctions associées : renseignement, appui-feu, ciblage, logistique, médical, ...

Plus globalement, l'initiative multinationale *FMN* s'imposant comme le vecteur principal d'interopérabilité des systèmes d'information et de communication en environnement interalliés, la France a choisi d'y adhérer et de revendiquer le statut **d'affilié de type A (Nation cadre)**. L'OTAN est un affilié de l'initiative FMN via NCS (NATO Command Structure). ACO (Allied Command for Operations) indique que la conformité au référentiel FMN est obligatoire pour les prises de tour NRF.

La démarche FMN s'organise en spirales capacitaires suivant un calendrier¹¹ contraint et ambitieux.

Niveau	Spiral 1	Spiral 2	Spiral 3	Spiral 4	Spiral 5	Spiral 6
Utilisation opérationnelle souhaitée	2017-2018	2019-2021	2022-2024	2025-2027	2028-2029	2030-2031

Entre le jalon "Final Specifications" et le jalon "Preferred operational use", les affiliés doivent réaliser l'acquisition des capacités définies au titre de la spirale, valider les tests techniques FMN de conformité des composants choisis et réussir les tests de mise en œuvre opérationnelle des dites capacités.

L'enjeu pour la France est double, il s'agit :

- de valider sa capacité technique et humaine à respecter les spécifications *FMN* et donc d'établir sa crédibilité à assumer ses ambitions opérationnelles,

⁹ *Federated Mission Networking*, spécifications traitant des composantes procédurales et techniques du système d'information de la coalition

¹⁰ Command, Control and Communications

¹¹ - *Proposed Specifications* – Jalon de spécifications initiales de la spirale- *Final Specifications* – Jalon de validation des spécifications - *Emerging operational use* – Jalon de début de confirmation des nations sur les spécifications de la spirale - *Preferred Operational use* - Phase de mise en œuvre du référentiel de la spirale en contexte interalliés FMN

- d'influencer l'initiative *FMN* afin qu'elle prenne en compte les intérêts nationaux en termes de doctrine, de procédures opérationnelles et de politique industrielle.

Le statut d'affilié de type A impose à la France **certaines engagements** dont la participation active à la gouvernance *FMN* et à l'animation de ses travaux, le respect des spécifications *FMN*¹² élaborées par les affiliés sous pilotage OTAN/ACT et des exigences d'entraînement aux processus en coalition et de mise en œuvre de laboratoires de test à distance des systèmes nationaux.

Afin d'accompagner ce changement de paradigme, une organisation idoine a été mise en place.

Il a donc été décidé de :

- créer une gouvernance de cohérence inter-programmes et intra-ministère vis à vis de cet enjeu *FMN* par le biais de la mise en place d'une revue de cohérence capacitaire *FMN* (en conformité avec l'Instruction Ministérielle 1618) sous la responsabilité de EMA/COCA et DGA/SASD. Cette revue a en charge de définir la feuille de route *FMN*.
- créer une équipe projet FRISE *FMN* (type Manager/OP) qui doit instruire et coordonner la prise en compte de la feuille de route capacitaire au sein des programmes d'armement.

Document	Date	Origine	Type doc	Portée
Déclaration des Autorités Militaires Françaises au secrétariat FMN de leur volonté de devenir affilié du FMN, avec le niveau d'ambition Mission Network Element (Affilié de type A) diffusée par note n°193/REPDEF OTAN/C3/NU du 11 mars 2016	11 mars 2016	RE PDEF OTAN	Note	Min Arm
Mise en place de plateforme FMN diffusé par note D6-19-007236/ARM/EMA/MGA/NCPI/NP du 19/12/2019	19 décembre 2019	EMA	Note	Min Arm
Mandat de la Revue de Cohérence Capacitaire (RCC) diffusé par note sous double timbre : D-20-00377/ARM/EMA/SC/PLANS/COCA/NP DGA01090024720/ARM/DGA/SASD/NP	20 juillet 2020	EMA DGA	Note	Min Arm
Contexte et mandat de l'équipe projet FRISE FMN Présentation des missions et de l'organisation de l'EDPI FRISE FMN diffusé par note sous double timbre : D-20-002452/ARM/EMA/SNA/NP DGA01D20A-8017/ARM/DGA/DO/UM ESIO/NP	29 mai 2020	EMA DGA	Note	Min Arm

2.1.2 Européen

Document	Date	Origine	Type doc	Portée
Règlement e-IDAS – electronic Identification And Signature : Règlement (UE) 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur	23 juillet 2014	Union Européenne	Règlement applicable directement	UE
<i>Commentaire : tout comme le Référentiel Général de Sécurité (RGS) pour la France, e-IDAS a proposé de donner un cadre juridique aux échanges électroniques ayant lieu sur le marché communautaire. e-IDAS propose trois niveaux d'authentification : faible, substantiel, élevé (3 pour le RGS). Ce règlement est applicable depuis le 1er juillet 2016. Le règlement e-IDAS fait actuellement l'objet d'une refonte.</i>				
RGPD : règlement général sur la protection de la donnée : Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données	27 avril 2016	Union Européenne	Règlement applicable directement	UE

¹² *Federated Mission Networking*, spécifications traitant des composantes procédurales et techniques du système d'information de la coalition

Commentaire : le règlement européen RGPD voté en 2016 est applicable depuis le 25 mai 2018. Il vise à renforcer la protection des données à caractère personnel en harmonisant la législation à l'ensemble de l'Union européenne. En pratique, la plupart des déclarations préalables CNIL disparaissent au profit d'une logique de responsabilisation a priori des acteurs et de conformité continue. Les organismes qui traitent des données personnelles doivent veiller au respect des textes tout au long du cycle de vie de la donnée. Les pouvoirs de sanction des CNIL nationales sont renforcés.				
Directive NIS 2 : Directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union	14 décembre 2022	Union Européenne	transposée en droit national	UE
Commentaire : la directive NIS2 (Network and Information Security), entrée en vigueur en octobre 2024, étend les obligations de cybersécurité à de nombreux secteurs (énergie, transports, santé, infrastructures numériques...). Elle établit des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur. Elle s'applique aux opérateurs de services essentiels – Entités du ministère a priori non concernées, mais certains industriels : oui. Elle impose notamment des exigences sur la chaîne de production logicielle: • Évaluation des risques fournisseurs : analyse de la sécurité des prestataires et sous-traitants • Sécurité de la chaîne d'approvisionnement : mesures pour garantir l'intégrité des composants tiers • Gestion des incidents : notification aux autorités sous 24h en cas d'incident significatif Actuellement la déclinaison du NIS 2 au niveau national est en cours par l'ANSSI. https://cyber.gouv.fr/la-directive-nis-2 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555				
RÈGLEMENT (UE) 2018/1807 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne	14 novembre 2018	Union Européenne	Règlement applicable directement	UE
Commentaire : le présent règlement s'applique au traitement de données électroniques autres que les données à caractère personnel dans l'Union qui est: a) fourni en tant que service aux utilisateurs résidant ou disposant d'un établissement dans l'Union, par un fournisseur de services établi ou non dans l'Union; ou b) effectué par une personne physique ou morale résidant ou disposant d'un établissement dans l'Union pour ses propres besoins.				
RÈGLEMENT (UE) 2019/881 Cybersecurity Act , Règlement européen « Cybersecurity Act » relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications.	17 avril 2019	Union Européenne	Règlement applicable directement	UE
Commentaire : le Cyber Resilience Act est un règlement européen adopté en 2024 qui impose des exigences de cybersécurité pour tous les produits comportant des éléments numériques vendus dans l'UE. Il entre en application progressive jusqu'en 2027. Obligations principales : • SBOM obligatoire : tout fabricant doit générer et maintenir un inventaire des composants logiciels, disponible sur demande des autorités de surveillance • Secure by design : les produits doivent être conçus avec la sécurité dès la conception • Mises à jour de sécurité : obligation de fournir des correctifs pendant toute la durée de vie du produit • Signalement des vulnérabilités : notification à l'ENISA sous 24h pour les vulnérabilités activement exploitées https://cyber.gouv.fr/cybersecurity-act				

2.2 Le cadre interministériel

2.2.1 La stratégie du SI de l'État – Doctrine cloud

Document	Date	Origine	Type doc	Portée
Cadre stratégique commun du système d'information de l'État : diffusé par circulaire du Premier ministre du 7 mars 2013	7 mars 2013	PM	Circulaire	Toute admin.

Commentaire: Commentaire : ce cadre est un document d'orientation fixant les objectifs de transformation du système d'information de l'État sous forme de cibles à atteindre et de dispositifs à mettre en œuvre à l'échéance de 5 ans, en partant des principaux enjeux de l'État.				
Décret n° 2023-304 du 22 avril 2023 modifiant le décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique [DINUM] en date du 25 octobre 2019 et publié au JO du 27 octobre 2019	22 avril 2023	PM	Décret	Toute admin.
Commentaire : ce décret définit le système d'information de l'Etat placé sous la responsabilité du Premier ministre ainsi que les attributions de la direction interministérielle du numérique (DINUM). Il introduit l'examen pour avis conforme (article 3) des projets de SI importants (montant prévisionnel global actuellement fixé à 9M€ par arrêté du 5 juin 2020 publié au JO du 26 juillet 2020). Les systèmes opérationnels et de communication et les systèmes d'information scientifiques et techniques n'entrent pas dans le cadre du champ de ce décret, de même que les systèmes comportant des supports ou informations classifiés qui restent sous la responsabilité des ministères concernés.				
Arrêté du 5 juin pour l'application de l'article 3 du décret n°2019-1088 du 25 octobre 2019 (cf. ci-dessus) publié au JO du 26 juillet 2020	5 juin 2020	PM	Arrêté	Toute admin.
Commentaire: Cf. Décret n°2019-1088 ci-dessus.				
Directive DGSIC n°37 relative au traitement d'un dossier éligible à l'article 3 du décret n°2014-879 du 1er août 2014 relatif au système d'information et de communication de l'État modifié par le décret 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique.	8 février 2016	DGSIC	Directive	Min Arm
Commentaire : cette directive qui doit être réactualisée décrit le contenu du dossier qu'il convient de constituer pour l'avis de conformité en DINUM et les modalités de traitement de ce dossier au niveau du MinArm.				
Circulaire n° 6404-SG relative à la doctrine d'utilisation de l'informatique en nuage par l'État	31 mai 2023	PM	Circulaire	Toute admin.
Commentaire : cette circulaire précise la doctrine d'utilisation de l'informatique en nuage par l'État, introduite par la circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État Cf. https://www.numerique.gouv.fr/offre-accompagnement/cloud-administrations/la-doctrine-de-létat/ .				
Doctrine "Cloud au Centre" et offre Office 365 de Microsoft diffusée par note DINUM-DIR-210901 du 15 septembre 2021	15 septembre 2021	DINUM	Note	Toute admin.
Commentaire: cette note clarifie la politique de l'État français "Cloud au Centre" et précise: • interdiction d'Office 365 pour les administrations publiques • souveraineté des données : choisir des prestataires Cloud qui garantissent la protection des données sensibles et qui ne sont pas soumis à des réglementations extracommunautaires, comme le Cloud Act américain • promotion des solutions européennes				

2.2.2 Politique de la donnée - Logiciels Libres – ouverture des codes

Document	Date	Origine	Type doc	Portée
Circulaire n°6264/SG relative à la politique publique de la donnée, des algorithmes et des codes sources	27 avril 2021	PM	Circulaire	Toute admin.
Commentaire : La circulaire met en œuvre une politique publique de la donnée : • constituant une priorité stratégique de l'État dans ses relations avec tous ses partenaires, en particulier les collectivités territoriales, et dont le suivi sera assuré par des RIM régulières (RIM de suivi, RIM transverses, RIM thématiques, dites « Bothorel ») • une orientation marquée sur l'ouverture et la transparence des informations publiques, avec un axe sur le partage des données entre administrations • avec une gouvernance à la main de l'administrateur général des données (AGD) et des administrateurs ministériels (AMD) dont le périmètre de responsabilités est désormais étendu aux algorithmes et aux codes sources (ex : création du Comité Interministériel des AMDAC – CIAD))				

Article L. 311-5 du code des relations entre le public et l'administration modifié par Ordonnance n°2016-1360 du 13 octobre 2016 art 51	13 octobre 2016	PM	Loi	Toute admin.
Commentaire : cet article permet de limiter l'accès aux documents administratifs dont la consultation ou la communication porterait atteinte notamment au secret de la défense nationale ou à la sécurité des systèmes d'information des administrations.				
Politique ministérielle des données approuvée le 05/04/2022 et diffusée par la note n°117/ARM/DGNUM/DG/NP du 5/04/2022	5 Avril 2022	DGNUM	Politique	Min Arm
Commentaire : La politique ministérielle des données définit le cadre pour la valorisation des données du ministère (elle a vocation à être déclinée par les grands subordonnés et les organismes rattachés au ministre), en précisant : • la vision à long terme du ministère sur la valorisation des données ; • 6 principes directeurs (s'appliquant aux organisation comme aux produits en projet et en exploitation/production) : Valeur, Partage, Efficience, Maîtrise en sécurité, Gouvernance et Acculturation ; • 21 ambitions déclinant les principes directeurs (précisant les objectifs à atteindre pour chaque principe) ; • des rôles à instancier par les états-majors, directions et services du ministère (directeur des données, directeur des données délégué, administrateur des données de zone fonctionnelle, architecte de données, référent métier) ; • Des instances de décision et d'animation (Comité des Administrateurs des données de la défense (CADD), Forum ministériel des données (FMD), Commission ministérielle des données (CMD)).				
Orientations pour l'usage des logiciels libres dans l'administration : circulaire du Premier ministre adressée le 19 septembre 2012 à tous les ministères.	19 septembre 2012	PM	Circulaire	Toute admin.
Commentaire : cette circulaire précise les contextes d'usage des logiciels libres favorables au sein de l'administration, décrit l'organisation et les objectifs des instances « logiciel libre » interministérielles (sous l'égide de la DINUM (ex-DINSIC)), incite les ministères à contribuer à cet effort et préconise de considérer désormais le logiciel libre à égalité avec les autres solutions pour répondre aux besoins métiers.				
Conseils à la rédaction de clauses de propriété intellectuelle pour les marchés de développement et de maintenance de logiciels libres	26 février 2014	DINSIC	Guide	Toute admin.
Commentaire : ce guide pratique à destination des administrations a été élaboré sous l'égide de la DINSIC par un groupe de travail regroupant le SAE et diverses administrations de l'état pour faciliter la rédaction des cahiers des charges (notamment les CCAG-TIC) permettant de couvrir des marchés de : • maintenance corrective et adaptative portant sur un logiciel libre ; • maintenance évolutive portant sur un logiciel libre ; • développement de logiciels spécifiques destinés à être mis à disposition de tiers par l'administration sous un régime de licence de logiciel libre. https://www.economie.gouv.fr/apie/actualites/conseils-redaction-clauses-propriete-intellectuelle				
Politique de contribution aux logiciels libres de l'État	15 février 2018	DINSIC	Politique	Toute admin.
Commentaire : cette politique publiée provisoirement sur le site github de la DINSIC (https://www.numerique.gouv.fr/publications/politique-logiciel-libre) a été validée par l'ensemble des DSI des administrations le 15 février 2018. Elle précise : • les règles et principes à respecter pour l'ouverture des codes sources • les bonnes pratiques à respecter par les ministères • la gouvernance des politiques de contribution de l'État. Sont concernés l'ensemble des nouveaux développements de codes sources développés soit en interne soit pour le compte d'une administration dans le cadre du système d'information de l'État tel que défini par le décret du 1er août 2014 n°2014-879 relatif au système d'information et de communication de l'État (cf. 2.2.1)				

2.2.3 Les référentiels interministériels

2.2.3.1 Référentiels généraux (RGI, RGS, RGAA, R2GA, RGESN)

Il s'agit des référentiels touchant à l'interopérabilité, la sécurité, l'accessibilité, l'archivage et l'écoconception.

Document	Date	Origine	Type doc	Portée
Interopérabilité				
Référentiel Général d'Interopérabilité V2 [RGI] approuvé par arrêté du Premier ministre du 20 avril 2016	20 avril 2016	DINSIC	Arrêté	Toute admin.
Commentaire : règles d'interopérabilité (format, protocoles, encodages, ...) rentrant dans le champ d'application de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. La version de référence est publiée sur le site de modernisation de la vie publique https://www.numerique.gouv.fr/offre-accompagnement/referance-interoperabilite-rgi/				
Sécurité				
Référentiel Général de Sécurité V2.0 [RGS] du 13 juin 2014 approuvé par arrêté du Premier ministre du 13 juin 2014	13 juin 2014	PM	Arrêté	Toute admin.
Commentaire : le RGS précise des règles de sécurité s'imposant aux autorités administratives dans la sécurisation de leur SI et notamment sur les dispositifs de sécurité relatifs aux mécanismes cryptographiques et à l'utilisation de certificats électroniques et contremarques de temps. Le RGS propose également des bonnes pratiques en matière de SSI. Le RGS découle de l'application de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Le RGS s'applique également aux échanges entre autorités administratives et usagers, à deux exceptions près : • les autorités administratives doivent accepter les moyens d'identification électronique non conformes au RGS mais répondant aux conditions fixées par l'article 6 du règlement eIDAS ; • les autorités administratives doivent accepter les signatures (respectivement les cachets) électroniques non conformes au RGS mais répondant aux conditions fixées par l'article 27 du règlement eIDAS. L'articulation entre le RGS et l'eIDAS est décrite sur le site de l'ANSSI.				
Accessibilité				
Décret n°2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne	24 juillet 2019	PM	Décret	Toute admin.
Commentaire : le décret détermine les obligations relatives à l'accessibilité des services de communication au public en ligne aux personnes handicapées, comprenant les applications mobiles et le mobilier urbain numérique, à mettre en œuvre selon un référentiel d'accessibilité. Il précise les modalités de mise en œuvre (déclaration d'accessibilité, procédures, sanctions applicables, exemptions)...				
Référentiel Général d'Amélioration de l'Accessibilité 4 [RGAA]	16 février 2021	DINUM	Arrêté	Toute admin.
Commentaire : ce référentiel, anciennement Référentiel Général de l'Accessibilité pour les administrations, découle de l'article 47 de la loi n°2005-102 du 11 février 2005 sur l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées. Cette version est structurée en 2 parties. La première présente les obligations à respecter : elle s'adresse aux juristes, aux gestionnaires et à tous les professionnels du web et de l'accessibilité. La deuxième contient une liste de critères pour vérifier la conformité d'une page web : elle s'adresse aux auditeurs RGAA. Cette version est accessible en ligne via https://accessibilite.numerique.gouv.fr/				
Archivage				
Référentiel Général de Gestion des Archives [R2GA] publié par le comité interministériel aux Archives de France	Octobre 2013	PM	Référentiel	Toute admin.
Commentaire : ce référentiel précise les notions relatives à l'archivage, le périmètre, et les règles précises découlant du livre II du code du patrimoine. Ce référentiel publié sous l'égide du comité interministériel aux archives de France (CIAF) est le fruit d'un travail piloté par le ministère de la culture en étroite collaboration avec les directions des archives des ministères en charge de la Défense et des Affaires étrangères. Voir également corpus lié à l'archivage §3.2.7.4 Archivage				
Ecoconception				
Référentiel général d'écoconception de service numérique [RGESN]	mai 2024	PM	Référentiel	Toute admin.
Commentaire : Le référentiel général d'écoconception de service numérique (RGESN) est un document interministériel édité par la direction interministérielle du numérique (DINUM). Dans une perspective de sobriété numérique, le RGESN présente une grille d'analyse qui s'applique aux SI				

dans leur phase de développement, dès la phase d'idéation. Les objectifs poursuivis à travers cette approche sont de mettre en service, in fine, un SI qui consomme moins de ressources informatiques et énergétiques et des équipements dont l'obsolescence est retardée, qu'il s'agisse des équipements utilisateurs ou des équipements réseau ou serveur.

L'écoconception des services numériques n'est pas uniquement une recherche d'optimisation, d'efficacité ou de performance mais une réflexion plus globale sur l'usage des technologies. Il est important d'intégrer les impacts environnementaux du numérique dans la conception des services numériques en visant directement ou indirectement à allonger la durée des vies des équipements numériques, à réduire la consommation de ressources informatiques et énergétiques des terminaux, des réseaux et des centres de données.

Le RGEN est accessible via <https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/>

2.2.4 Communication gouvernementale - Charte Internet de l'État – Charte graphique

Document	Date	Origine	Type doc	Portée
Internet de l'état : circulaire de la Première Ministre n°6411/SG du 7 juillet 2023	7 juillet 2023	PM	Circulaire	Toute admin.
Commentaire : cette circulaire abroge la circulaire contient notamment : • Une charte de l'internet applicable à tous les sites des administrations centrales et des services déconcentrés de l'état • Les procédures d'agrément auxquelles tout projet Internet et numériques de l'État, en refonte ou en création doit se plier et ce quelle que soit l'extension du nom de domaine concerné (.gouv, .org, .com, .fr...). https://www.systeme-de-design.gouv.fr/static/file/Circulaire_n_6411_SG_sites_Internet_de_l_Etat_et_demarches_numeriques_07_07_2023.pdf				
Note de mise en oeuvre : Mise en œuvre de la circulaire n°6411/SG du 7 juillet 2023 relative à l'amélioration de la lisibilité des sites Internet de l'État et de la qualité des démarches numériques	13 juillet 2023	DINUM	Note	Toute admin.
Commentaire : cette note d'application de la circulaire n°6411/SG en décrit les grands principes d'application et notamment : rôle du SIG, système de Design de l'Etat, extension de domaine réservé .gouv.fr et périmètre d'application. https://www.systeme-de-design.gouv.fr/static/file/Note_SIG_d_application_du_DSFR_et_gouv_fr_13_07_2023.pdf				
Communication gouvernementale : circulaire du Premier ministre n°6120/SG du 14 octobre 2019 relative l'organisation et la coordination de la communication gouvernementale	14 octobre 2019	PM	Circulaire	Toute administration sur internet
Commentaire : cette circulaire renforce le pilotage de la communication gouvernementale par le SIG (Service d'Information du Gouvernement) sur 3 axes : le respect des procédures de demande d'agrément (opération de communication, site internet, réseaux sociaux...), les actions relatives à l'analyse de l'opinion, la planification des actions de communication.				
Charte graphique : circulaire du Premier ministre n°6144/SG du 17 février 2020 relative à la nouvelle stratégie de marque de l'État.	17 février 2020	PM	Circulaire	Toute administration sur internet
Commentaire : cette stratégie se décline en 3 chartes : une charte graphique, une charte des grands principes rédactionnels et une charte des réseaux sociaux. Ces documents sont accessibles sous : https://www.systeme-de-design.gouv.fr/				

2.2.5 Les outils et l'offre de service au niveau interministériel

2.2.5.1 L'offre de services communs

Des travaux engagés depuis plusieurs années sous l'égide de la DINUM, ont donné lieu à des réalisations, des offres de service ou des projets encore en cours parmi lesquels (<https://www.numerique.gouv.fr/services-numeriques/>) :

- le réseau interministériel de l'état (RIE) ;
- la transformation des centres informatiques ;
- le socle interministériel des logiciels libres (SILL, cf. paragraphe suivant) ;
- la démarche [open.data.gouv.fr](https://www.data.gouv.fr/fr/pages/about/opendata/) : relative à l'ouverture des données de l'état (<https://www.data.gouv.fr/fr/pages/about/opendata/>) ;
- la démarche d'API associée permettant d'accéder à ces données via un portail de publication des API (<https://www.data.gouv.fr/dataservices/>) ;
- la démarche FranceConnect dont une des principales réalisations est FranceConnect, permettant l'authentification des particuliers (voir description). Il existe une version FranceConnect+ permettant une authentification forte (<https://www.franceconnect.gouv.fr/franceconnect-plus/>) ; le composant ProConnect permet l'authentification des agents de l'État et des professionnels du privé (<https://www.proconnect.gouv.fr/>). Pour les agents de l'État, ProConnect s'appuie sur les systèmes d'identité des administrations (ex. Passage2, Cerbère). Si aucun fournisseur d'identité n'est disponible, ProConnect crée une identité professionnelle dédiée. Pour les professionnels du privé, ProConnect vérifie l'identité en se basant sur des données fiables, comme le courriel professionnel et le SIRET de l'organisation. Une certification à partir du référentiel national des entreprises est actuellement en développement.
- la solution de messagerie instantanée du secteur public conçue et gérée par l'Administration française, au bénéfice de la fonction publique, pour communiquer facilement en toute sécurité (<https://www.tchap.gouv.fr/>) ;
- le service de *démarches simplifiées* pour effectuer une démarche administrative en ligne (<https://www.demarches-simplifiees.fr/>) ;
- des nouveaux outils collaboratifs pour les agents de l'Etat permettant d'aider au télétravail au sein d'une offre baptisée "LaSuite" (<https://www.numerique.gouv.fr/offre-accompagnement/expertise-suite-num%C3%A9rique/>) : messagerie instantanée, audio et visio conférences, prise de note collaborative, partage de fichiers France Transfert, tableur/base de données, messagerie collaborative pour les petites entités, cf. <https://www.campus.numerique.gouv.fr/la-suite-num%C3%A9rique-de-l%C3%A9tat/> ;
- Resana, plateforme collaborative de stockage, partage et coédition de documents, travail en équipe et en mode projet, y compris en mobilité grâce à une application dédiée (<https://resana.numerique.gouv.fr/public/>) ;
- Webconférence de l'État (Webconf) est un service de Webconférence interministériel jusqu'à 20 personnes (<https://webconf.numerique.gouv.fr/>) ;
- Webinaire de l'État pour les séminaires en ligne, formations, présentations, conférences virtuelles jusqu'à 350 participants (<https://webinaire.numerique.gouv.fr/welcome>) ;
- Audioconférence de l'État (Audioconf) est un service d'audioconférence, accessible depuis n'importe quel téléphone et mis à la disposition de tous les agents de l'État (<https://audioconf.numerique.gouv.fr/>).

2.2.5.2 Le socle de logiciels libres SILL – Marché de support LL

☆☆☆☆☆

La présence d'un logiciel dans ce socle ne présuppose pas de son acceptabilité sur les réseaux du Ministère.

☆☆☆☆☆

Document	Date	Origine	Type doc	Portée
Socle interministériel de logiciels libres (SILL)	mise à jour en continu	DINUM	Référentiel	Toute admin.
<i>Commentaire : ce catalogue constitue un référentiel de logiciels libres préconisés au niveau interministériel et couvrant, dans sa version actuelle, le poste de travail, la gestion de parc, l'exploitation de serveurs, les bases de données, les environnements de virtualisation et les environnements de développement. Chaque logiciel du SILL est suivi par un ministère référent. Le SILL fait l'objet d'une actualisation en continu consultable sur le site web : https://code.gouv.fr/sill/</i>				

2.2.5.3 Les données ouvertes

L'utilisation des données ouvertes exposées sur Internet doit tenir compte des principes suivants :

- Pour les données de référence, le recours à l'utilisation d'une donnée ouverte n'est autorisé que si celle-ci n'est pas déjà exposée au sein du ministère par la zone fonctionnelle en ayant la responsabilité. En effet, la donnée de référence peut déjà être consommable au sein du ministère, soit par reprise de la donnée ouverte ainsi exposée de manière synchronisée à l'ensemble des SI, soit par exposition de la donnée par un abonnement auprès de la source officielle (cet abonnement apportant un enrichissement vis-à-vis de la donnée ouverte);
- Pour les données de production, il est préconisé de s'assurer en amont, qu'un contrat de service puisse être établi avec la source des données, certains jeux de données ne faisant pas l'objet de mises à jour dans le temps.

2.2.5.4 Conception de site Internet

Dans sa mission de « pilote de la transformation digitale de la communication gouvernementale », et dans la lignée de la charte graphique de l'État, le Service d'information du Gouvernement [SIG] met à disposition sous le vocable de « Système de Design » (Design System) un ensemble de composants réutilisables, répondant à des standards et à une gouvernance, pouvant être assemblés pour créer des sites Internet accessibles et ergonomiques.

Le Système de Design de l'État (DSFR) est l'outil destiné à produire les interfaces officielles des sites en .gouv.fr. Il regroupe un ensemble de règles et de composants réutilisables, pour fournir à la population des services numériques simples, accessibles et reconnaissables.

Le système de design est accessible sous <https://www.systeme-de-design.gouv.fr>. Il est impératif que les sites Internet respectent le référentiel d'accessibilité (norme RGAA) à 100%, sous peine d'amendes récurrentes.

2.3 Le cadre ministériel

Les références suivantes ne sont pas uniquement techniques mais sont nécessaires à la compréhension du cadre général global des SIC du ministère, sans pour autant le décrire de façon exhaustive.

2.3.1 Politique SIC ambition numérique

Document	Date	Origine	Type doc	Portée
Ambition numérique du ministère des armées approuvée par le ministre le 30 novembre 2017 et diffusée par note n° 490/ARM/DGSIC/DG/NP du 11 décembre 2017)	30 nov.2017	Ministre	Politique	Min Arm
<i>Commentaire : ce document définit une approche globale et cohérente de la transformation numérique du ministère des armées, en cohérence avec le chantier « Transformation numérique de l'État » de la démarche « Action publique 2022 », lancé par le Premier Ministre le vendredi 13 octobre 2017</i>				

2.3.2 Architecture générale, politique logicielle

Document	Date	Origine	Type doc	Portée
Politique générale sur le logiciel au ministère des Armées diffusée par note n°44/ARM/DGNUM/DG/NP du 11 février 2019	8 février 2019	DGNUM	Politique	Min Arm
<i>Commentaire : cette politique remplace la directive DGSIC n°1 portant sur les logiciels du 17 octobre 2006 Dans le contexte de transformation numérique de l'État et du ministère, elle réactualise sa politique sur le logiciel, autour de 3 principes majeurs (architecture modulaire orientée services, standardisation des échanges, indépendance vis-à-vis de l'infrastructure sous-jacente), et 9 objectifs (dont recours aux standards ouverts, souveraineté, diminution des adhérences, rationalisation des choix, partage et réutilisation, architecture modulaire, principes d'APIsation).</i>				

2.3.3 Socle numérique

Vision du socle numérique ministériel mutualisé 2025-2030 : cf. §2.3.1

Feuille de route du socle numérique ministériel mutualisé : cf. §2.3.6

Le CCT décrit les services du socle disponibles à date ou à court terme.

2.3.4 SIC opérationnels – FrOps

2.3.4.1 Politique et concepts d'emploi

Document	Date	Origine	Type doc	Portée
Note n°508/DEF/EMA/PAC/NP relative à la politique des armées en matière de sensibilité des informations opérationnelles	9 juin 2009	EMA	Note	Armées
Doctrine Interarmées relativeaux SIC en opération : DIA-6_SI-OPS (2020) sous timbre n°138/ARM/CICDE/NP du 16 décembre 2020	16 décembre 2020	CICDE	Doctrine	Min Arm
<i>Commentaire : ce document précise les principes et l'emploi des SIC dans la conduite des opérations. Il présente les grands principes des SIC et définit les différents niveaux de responsabilité dans la conception, la mise en œuvre et la conduite des SIC, enfin il présente l'emploi des SIC en opération.</i>				

2.3.4.2 COTS OTAN / SIC Multinationaux

La liste des SI et COTS OTAN est entretenue et actualisée par EMA/SNA. La liste exhaustive des piles OTAN est toujours tenue à jour par l'agence NCIA. Les détails sont à demander auprès des RSIO.

De même l'EMA/SNA identifie et répertorie tous les besoins et les synoptiques de raccordements pour les SIC multinationaux (OTAN, Européens, bilatéraux ou multilatéraux).

Document	Date	Origine	Type doc	Portée
SI/COTS OTAN – Gouvernance et plan pluriannuel à cinq ans , diffusé par note n°D-21-003071/ARM/EMA/MGA/SNA/NP du 10 juin 2021	10 juin 2021	EMA	Note	Min Arm
<i>Commentaire : cette note liste les principaux produits (SI/COTS) livrés par l'agence NCLIA pour la réalisation des activités opérationnelles en contexte national ou multinational</i>				

2.3.5 Sécurité

Pour une meilleure cohérence du document, l'ensemble des références relatives à la sécurité sont regroupées au chapitre associé (cf. §4.1).

2.3.6 Gouvernance

La réforme du numérique, entamée en décembre 2024 avec l'annonce de la création du commissariat au numérique de défense (CND), introduit une nouvelle gouvernance du numérique au sein du ministère des armées et des anciens combattants.

Document	Date	Origine	Type doc	Portée
Décret 2025-782 du 6 août 2025 portant création du commissariat au numérique de défense	6 août 2025	Ministre	Décret	Min Arm
<i>Commentaire : le décret est disponible sur Légifrance</i>				
Arrêté du 6 août 2025 relatif à l'organisation du commissariat au numérique de défense	6 août 2025	Ministre	Arrêté	Min Arm
<i>Commentaire : l'arrêté est disponible sur Intranum</i>				
Arrêté portant création et organisation d'instances relatives au numérique de défense	14 novembre 2025	Ministre	Arrêté	Min Arm
<i>Commentaire : l'arrêté est disponible sur internet</i>				
Instruction n°8/ARM/CAB/CM3 relative à la gouvernance du numérique	14 novembre 2025	Ministre	Instruction	Min Arm
<i>Commentaire : Cette instruction abroge l'IM 2476.</i>				
Guide relatif aux missions d'une DSI Domaine diffusé par la note n° 443/ARM/DGNUM/DG/NP du 9 novembre 2021	9 novembre 2021	DGNUM	Guide	Min Arm
<i>Commentaire : les principales missions d'une DSI Domaine se structurent autour de quatre «_grands axes_» (Stratégie et pilotage, Architecture et données, Sécurité du numérique et protection des données, Conduite de projets et appui aux SIC en service du portefeuille).</i>				
IM n°1618/ARM/CAB sur les déroulement des opérations d'armement	15 février 2019	Ministre	Instruction	SIOC
<i>commentaire : cette instruction qui abroge l'ancienne instruction 1516 décrit l'ensemble du processus de conduite d'un programme d'armement autour de 3 phases : préparation, réalisation, et utilisation. Cette instruction s'accompagne d'un guide d'application de cette nouvelle instruction.</i>				
Directive portant application de l'instruction ministérielle relative à la gouvernance du numérique de la défense (version 1 novembre 2025), diffusé par note n°2025/633/ARM/CND/GOUV STRAT/SD TIA/NP du 26 novembre 2025	Novembre 2025	CND	Directive	Min Arm
<i>Commentaire : la directive est disponible sur Intranum</i>				
Directive de Gouvernance n°2 relative à la déclaration d'engagements, au plateau d'intégration et à l'urbanisation	S1 2026	CND	Directive	Min Arm

<i>Commentaire : cette directive décrira les interactions relatives à la déclaration d'engagement (DE) et au plateau d'intégration (PI). La DE est un document papier, prochainement numérisé, qui engage l'autorité d'emploi (AE). Elle est transmise avec le dossier de lancement, le calcul du retour sur investissement et d'une architecture prévisionnelle, au CND. Le PI organise la planification des étapes ultérieures du projet ; il est initié sur demande du RCP, avant le lancement des développements</i>				
Note provisoire "appui aux DSI", création de l'offre de services AGORA	18 novembre 2025	CND	Note	Min Arm
<i>Commentaire : la note est disponible sur Intranum</i>				
Transition vers la nouvelle gouvernance numérique n°2025/123/CND/GOUV STRAT/NP	3 décembre 2025	CND	Note	Min Arm
<i>Commentaire : la note est disponible sur Intranum</i>				
Note portant organisation du pilotage du socle numérique n°407060/ARM/DIRISI/SP/DSI SOCLE/NP	13 décembre 2022	DIRISI	Note	Min Arm
<i>Commentaire : ce document est publié sur la communauté de travail de la dsi socle numérique.</i>				

2.3.6.1 Outils de gouvernance

2.3.6.1.1 Gestion du patrimoine applicatif

2.3.6.1.1.1 SICLADE : l'outil de gestion du portefeuille ministériel applicatif

Tout système d'information, tout équipement comportant au moins un logiciel doit obligatoirement être enrôlé dès son initialisation dans l'outil SICLADE DR ou SICLADE Secret (pour les systèmes de niveaux S et TS). Cela permet d'initialiser son processus d'homologation, de recensement, au besoin de rattachement budgétaire et, le cas échéant, de permettre de constituer son dossier d'hébergement par le CND. Cet enrôlement se décompose a minima en une fiche SICLADE, voire une fiche de traitement en cas de manipulation de données à caractère personnel, pour le RGPD. Le registre de traitement du MinARM (article 30 du RGPD) est produit à partir de SICLADE. L'instance SICLADE Secret sera aussi utilisée dans le cadre de l'élaboration de la cartographie ministérielle de Cybersécurité.

Document	Date	Origine	Type doc	Portée
----------	------	---------	----------	--------

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestion de patrimoine	CAST Highlight	Cast Software	Pour l'observation de la qualité applicative du portefeuille des SI du ministère. Destiné à la gouvernance. Son utilisation est recommandée pour les ZF, DSI et segments. Sont analysés les SI métiers (hors COTS, portails) en production afin d'évaluer les forces et faiblesses potentielles du portefeuille.	R / -	Min Arm
Gestion de patrimoine	Diadème	Min Arm	CMDB DIRISI	- / S	Intradef

2.3.6.1.2 Gestion du patrimoine des données

Les administrateurs de données de zone fonctionnelle (ADD-ZF) tiennent à jour la Cartographie des Objets Métier (COM) précisant les données placées sous la responsabilité des zones fonctionnelles ainsi que la Cartographie des Données de Référence et des Référentiels de Données (CD2RD) précisant les données de référence identifiées au ministère et leurs référentiels de données associés.

Cette identification des objets métier et des données de référence, sera complétée de l'identification des données de production au sein des SI, au travers d'un catalogue de données permettant de valoriser l'ensemble des données du ministère par leur recensement auprès de tous les gisements de données, et par l'exposition de ces jeux de données pour consultation par leurs clients potentiels. Cet inventaire centralisé et détaillé des données du ministère permettra de comprendre leur sémantique, leur format, et leur(s) source(s) afin d'identifier rapidement les données pouvant être utilisées dans le cadre de nouveaux cas d'usage exprimés par les métiers.

Ainsi, le ministère se dote du catalogue de données dans le cadre du projet MetadatARM, pour les données de niveau non protégé ou diffusion restreinte. Celui-ci est composé :

- d'un glossaire permettant de recenser les données métier, de les définir en termes de sémantique et de partager cette définition ;
- du catalogue de données proprement dit (aussi appelé dictionnaire des données) permettant de lister et de décrire en termes de métadonnées les données existantes dans les SI ;
- d'une fonction permettant d'analyser le parcours des données et d'identifier leur transformation.

Ce service commun du socle ministériel est mis en service progressivement depuis 2024.

2.3.7 Relation client – Offre de service - DIADEME

Pour les clients du CND, DIADEME est l'accès unique et fédéré au catalogue de services contenant :

- l'ensemble de l'offre de services de l'opérateur ;
- le store, magasin de logiciels librement installables sur Intradef ;
- les articles et la documentation stockée dans les espaces professionnels des bases de connaissances DIADEME ;
- la déclaration des incidents de production comme cyber (en remplacement du formulaire FOURMI) et aux réclamations dans le cas de non résolution ;
- le suivi des demandes dont les formulaires ont été implémentés ;
- le suivi des demandes professionnelles [FEB] dans le cadre du recueil du besoin et du processus de suivi du plan de charge CND.

Pour le CND, DIADEME est l'outil de gestion des services numériques du CND.

3 SERVICES COMMUNS

Les services communs recouvrent l'ensemble des services, hors métier, nécessaires au fonctionnement du système d'information des armées. Les éléments référentiels ci-dessous précisent les composants de ce socle et fixent un cadre mutualisé permettant aux applications de s'y intégrer.

Le socle numérique ministériel mutualisé est un système d'information opérationnel et de communication dont la direction, l'exploitation, la sécurité et le soutien sont assurés par le CND (autorité de domaine). Il rassemble les réseaux d'infrastructure et de desserte, les passerelles, le stockage, le traitement et la sécurisation des données et des applications, les services communs à l'utilisateur et les services d'exploitation.

Intranet Secret-SF / FrOpS

Sur l'intranet Secret-SF, les services déployés issus des programmes d'armement, de l'opération d'ensemble Intraced, et des services déployés par les armées sont pris en compte dans le cadre du programme SIA. Les services communs déployés sont ceux du SIA S-SF.

La démarche est identique pour l'intranet SIA FrOpS : à terme les services communs déployés seront également ceux de SIA S-SF sur l'ensemble du réseau en métropole.

La démarche est identique pour l'intranet SIA TS : à terme les services communs déployés seront identiques à ceux de SIA S-SF.

Composante projetable du SIA

La composante Projetable du SIA articulée autour du Cœur de Configuration (Infrastructure et services de socle) et de briques applicatives (COTS ou développements spécifiques), destinée aux théâtres d'opération et aux bâtiments de la Marine, est actuellement en cours de déploiement sur l'ensemble des niveaux de confidentialité.

Intradef

Une refonte de l'Intradef est en cours, pour le double objectif de forte sécurisation et d'adaptation aux évolutions majeures liées à la transformation numérique au sein du ministère.

Par ailleurs, le CND exerce un rôle renforcé d'administrateur technique de l'Intradef.

Intradef-SIE : sur les bâtiments de la Marine nationale, les services d'usage courant du réseau DR sont prolongés et adaptés aux contraintes apportés par le Segment Intradef Embarqué (SIE), dans la continuité des services de l'« Intramar bateau ». Le SIE version « Baltique » est en service depuis l'été 2021 et la version « Celtique » est en cours de déploiement. Le SIE apporte :

- la disponibilité des services communs à bord y compris en mode déconnecté (autonomie) ;
- l'optimisation des échanges sur les réseaux contraints ;
- la gestion des doubles équipages et des états-majors embarqués (embarquement et débarquement).

L'architecture du SIE comprend :

- les infrastructures embarquées et plateformes d'entraînement (CSC) et de formation (Pôle Ecoles Méditerranée) ;
- une infrastructure nationale à terre, hébergée en datacenter et portant notamment la gestion de configuration centralisée des infrastructures et services embarqués et des plateformes;
- des serveurs de bordure à terre, hébergés en datacenter, assurant le relais des services communs (DNS, LDAP, SMTP, NTP, DECOS, etc.) ;
- des services du socle SIE à terre (portails, etc.), hébergés en datacenter, au bénéfice des équipages des bâtiments « en préparation » (à terre) dont les données sont interchangeables avec les services de l'infrastructure embarquée via un support de stockage dédié.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°87 d'exploitation du STC-IA (V0.2) version 2.0 du 30 juin 2013	30 juin 2013	DIRISI	Directive	Intradef
<i>Commentaire : cette directive décrit l'architecture globale et les principaux services ainsi que les modalités d'exploitation du STC-IA (V0.2) sur l'Intradef. Différents travaux CND (MISHUCO, ...) ont depuis modernisé cette architecture.</i>				

3.1 Services à l'utilisateur

Ce paragraphe renvoie à des services utilisables par les applications mais également visibles directement par les utilisateurs. Ces services font partie du catalogue de services opérés principalement par le CND.

La gouvernance des services du socle du numérique, est décrite en **§2.3.6 Gouvernance**.

3.1.1 Environnement de travail

3.1.1.1 Poste de travail - CCB [SU-PC]

Ce chapitre n'évoque que les postes de travail d'organismes dont le soutien incombe au CND.

Concept d'emploi : le service « Poste de travail » décrit par le concept d'emploi « Environnement de travail » définit une offre matérielle et logicielle répondant aux besoins informatiques standards de l'ensemble des utilisateurs du ministère des armées. Il couvre la définition des différents types de matériel/configuration, les outils logiciels nécessaires à la production/consultation de certains formats

de fichiers et l'ensemble des dispositifs de base permettant à l'agent de travailler quel que soit son environnement (sur site, en mobilité), en accédant à l'ensemble des ressources, et selon les normes ministérielles de sécurité en vigueur, notamment la politique de sécurité des Intranets.

Matériels : l'acquisition, le renouvellement, la configuration ou la réforme du poste de travail sont désormais assurés de façon standardisée au sein du ministère des armées . Ce processus couvre tous les postes bureautiques utilisés en France métropolitaine, quel que soit le niveau de classification , à l'exception des postes dont le soutien n'incombe pas au CND (programmes d'armement, renseignement, hôpitaux...) et qui bénéficient de services restreints par rapport aux postes standardisés.

L'aspect matériel est géré au travers d'une régie « rationalisée » .

Logiciels – CCB : le CND assure la gestion de configuration des postes et des smartphones de tous les Intranets qu'elle infogère. Pour tous les réseaux , le comité de configuration bureautique (CCB) présidé par le CND en valide les évolutions, en conformité avec le CCT. Dans ce contexte, toute création/modification de masters, de logiciels ou d'applications en vue d'un déploiement est instruite par le CCB.

Pour répondre aux contraintes opérationnelles ou aux difficultés techniques, le CCB peut autoriser le déploiement préalable de logiciels en mode manuel (installation par un technicien du CND). En raison des contraintes de charge, ce cas doit demeurer exceptionnel.

☆☆☆☆

La présence d'un logiciel dans un marché cadre ne présuppose pas de son acceptabilité sur les réseaux opérés par le Ministère. Il est hautement recommandé de s'en assurer avant de procéder à son acquisition. À défaut l'installation pourra être refusée au moment de la demande de déploiement.

☆☆☆☆

Outre les masters, le CND réalise les packages logiciels correspondant :

- à des services communs répondant à un besoin générique ;
- à des besoins « métier » nécessaires à des emplois spécifiques ;
- à des pilotes permettant le bon fonctionnement de périphériques.

Préalablement à leur instruction par le CND, les demandes de réalisation de masters et de logiciels font l'objet d'une validation de leur DSI respective.

Logiciels à licences payantes faisant l'objet d'un contrat cadre : l'offre de logiciels à licences payantes repose essentiellement sur des contrats-cadres gérés par le CND ou par la DGA :

- marchés multi-éditeurs : Ouranos, UGAP et PROGIST ;
- marchés-cadres éditeurs.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°8 définissant les règles à appliquer au système de postes terminaux : directive publiée au Bulletin Officiel des Armées	29 juin 2009	DGSIC	Directive	Min Arm
<i>Commentaire : règles d'usage et d'interopérabilité des postes terminaux du ministère des armées. Périmètre : tous les intranets.</i>				
Concept d'emploi « environnement de travail » : note conjointe : n°6691/DEF/EMA/CPI/AUT/NP /n°1261/DEF/SGA/ADJ	6 juillet 2012 10 juillet 2012	SC1	Concept Emploi	Min Arm/NP/DR
<i>Commentaire : concept d'emploi "environnement de travail" : ce document couvre les notions de poste de travail, de son environnement physique (impression, partage de ressources, accès réseaux, matériels en option), de ses ressources logicielles (bureautique, gestion de fichier, messagerie, navigateur, multimédia, ...), de la capacité pour l'utilisateur en fonction de son profil de rechercher et demander des services dans le catalogue de services (NUMERI store) et de l'environnement de sécurité du poste de travail. Il s'applique uniquement au monde NP/DR.</i>				

SLR du service « environnement de travail » : note conjointe : n°1114/DEF/EMA/CPI/AUT/NP /n°201/DEF/SGA/ADJ	26 janvier 2013, 29 janvier 2013	SC1	SLR	Min Arm/ NP/DR
<i>Commentaire : SLR relatif au service de l'«environnement de travail»</i>				
EMO.GUI.003 - Constitution et rôle du Comité de Configuration Bureautique (CCB)	01 février 2026	CND/COMNUMIA/POENT	Guide	Intredef, SIA S-SF, SIA FrOps, SIA TS
<i>Commentaire : ce document précise les modalités de gestion de configuration du poste de travail, notamment le processus d'évolution des socles, ainsi que des demandes logicielles, des mises en production et de déploiement.</i>				

3.1.1.2 Critères d'éligibilité d'un package

L'inéligibilité d'un package du point de vue de la sécurité est déterminée par la mise en évidence d'une des vulnérabilités suivantes (liste non exhaustive) :

- absence de soutien par l'éditeur (notamment au regard du MCS) ; si d'aventure un logiciel packagé ne dispose plus de MCS, alors ce dernier est retiré du déploiement et ne peut plus être demandé en installation même au titre d'un renouvellement du poste (sauf dérogation officielle accordée, pour une durée donnée, par le COMCYBER) ;
- incompatibilité avec le socle technique ou une installation non compatible avec les standards du ministère ;
- initialisation ou fonctionnement nécessitant une connexion Internet (exemple : Internet Sur le Poste de Travail ISPT) ;
- application fonctionnant en mode serveur (se reporter notamment au chapitre **3.1.1.4 Postes de travail autonomes ou en mode déconnecté**) ;
- installation sur la partition C, en dehors du dossier « Program Files » ou « Program Files(x86) » ;
- application qui, par fonctionnement, nécessite ou crée une élévation de privilège ;
- application ou logiciel qui donne à un utilisateur authentifié des droits à la fois en écriture et en exécution sur un même dossier (règle dite W^X ou W xor X, respect de la règle de moindre privilège) ;
- logiciels de virtualisation, de paravirtualisation ou d'émulation ;
- dépendance d'un SI non enregistré dans SICLADE ou ne disposant pas d'une homologation, ou, à défaut, d'une autorisation provisoire d'exploitation (APE) ;
- logiciels de type freeware à usage privé sauf accord explicite de l'éditeur ;
- identification d'un comportement suspect ou malveillant du logiciel ;
- mécanisme interne au logiciel (non désactivable) cherchant à se connecter à un serveur sur Internet ;
- dépendance Java non compatible avec Eclipse Temurin (voir ci-dessous) ;
- installation ne pouvant se faire par les mécanismes du réseau support (package MCM, ex-MECM, ex-SCCM).

3.1.1.3 Recours à la machine virtuelle Java sur le terminal utilisateur

Document	Date	Origine	Type doc	Portée
Orientations ministérielles suite à l'évolution de la politique de la société Oracle relative au composant JAVA (Cf 3.2.2.2.1)	25 juillet 2019	DGNUM	Note	Min Arm

Certains logiciels nécessitent pour fonctionner qu'une machine virtuelle Java (JVM) soit installée sur le poste utilisateur. Ces machines virtuelles sont disponibles sous 2 formes: - JRE¹³ : contient la machine virtuelle Java nécessaire à exécuter les programmes Java sur les serveurs et les postes de travail. - JDK¹⁴ : contient la JRE ainsi que des outils de développement.

Les OpenJDK (Java Development Kit) sont en licences GPL2 (licence GNU). L'OpenJDK constitue l'implémentation de référence officielle et libre de Java SE, tel que défini par le Java Community Process. Il est accepté pour le développement d'application, mais seul un OpenJRE (Java Runtime Environment) peut être déployé sur un environnement de production ou sur un poste client. Pour la gestion des IHM des clients lourds, il est recommandé d'utiliser OpenJFX.

Ces logiciels sont entretenus par la communauté OpenJDK¹⁵ qui fait évoluer le code source de la *Java Platform SE*¹⁶ et apporte les correctifs dont ceux de sécurité. Ce code source est distribué sous licence libre, mais **pas les programmes exécutables (OpenJRE)** obtenus par compilation de ce code source et qui sont nécessaires pour faire fonctionner les programmes Java. De plus, la communauté n'entretient **que la dernière version** de Java, qui change tous les 6 mois ainsi que certaines versions bénéficiant d'un support libre et gratuit de plus longue durée, dites *LTS*¹⁷, toutes les 4 versions (versions 21 et 25 actuellement).

Différents acteurs se chargent ensuite de proposer les versions exécutables obtenues par compilation de ce code source et à déployer sur serveurs et postes de travail pour pouvoir y exécuter les programmes Java. Ces acteurs libres ou commerciaux proposent également des extensions de soutien de durée variable pour différentes versions, dont la plupart nécessitent une souscription et sont soumises à une licence spécifique pas nécessaire libre.

La solution recommandée est la JVM HotSpot incluse dans Eclipse Temurin avec une préférence pour cette dernière selon la version de Java utilisée. Le recours à une autre JVM n'est pas autorisé.

L'installation doit impérativement se faire via les mécanismes du réseau support (package MCM). En particulier, le recours à un déploiement Java Webstart ou équivalent est interdit.

La JVM ne doit pas être incluse dans le package d'un logiciel métier mais indiquée en dépendance (afin de faciliter le MCS de la JVM).

3.1.1.3.1 Interdiction de l'OpenJDK Oracle

Oracle distribue des instantiations binaires d'OpenJDK souvent mise en avant du fait de son positionnement historique vis-à-vis de cette technologie rachetée à Sun en son temps. Outre qu'il y ajoute des composants binaires propriétaires et des modifications spécifiques non standard, cet éditeur leur applique différentes licences selon les versions et leur ancienneté, dont certaines sont extrêmement contraignantes. Il a de plus procédé à des changements fréquents ces dernières années en ce domaine.

Il y a actuellement 4 licences différentes utilisées par Oracle selon les cas : - Oracle TNLA¹⁸ - Oracle NFTA¹⁹ - Oracle OTN²⁰ soumis à l'Oracle Java SE Universal Subscription - GPL2+CE²¹

☆☆☆☆☆

ATTENTION: La Java SE Universal Subscription ajoutée début 2023 se base sur le nombre d'employés de l'organisme, **peu importe qu'ils utilisent ou pas le composant Java concerné**. Oracle demande une souscription pour **tout** les employés, **mais aussi les agents, les sous-traitants et les consultants** qui soutiennent les activités métier internes de l'organisme. Cette souscription

¹³ Java Runtime Environment

¹⁴ Java Development Kit

¹⁵ <https://openjdk.org>

¹⁶ Standard Edition

¹⁷ Long Term Support

¹⁸ [Technology Network License Agreement for JavaSE](#)

¹⁹ [No-Fee Terms and Conditions License](#)

²⁰ [Oracle Technology Network License Agreement for Java SE](#)

²¹ [General Public Licence 2 et Classpath Exception](#)

s'applique aux déploiements des JDK Oracle sur les postes de travail, les serveurs, les conteneurs et les environnements Cloud. De plus, si le nombre de processeurs concernés dépassent 50 000, il faut encore acquérir une licence supplémentaires. Là encore, exécuter un Oracle JDK sur un serveur virtualisé ou dans un conteneur implique de couvrir par licence l'intégralité des processeurs de l'infrastructure de virtualisation (clusters de machines virtuelles ou d'orchestration de conteneurs) Oracle applique des pénalités de régularisation des usages non conformes constatés.

☆☆☆☆☆

Pour éviter la nécessité de devoir souscrire une souscription Oracle Java SE, le moyen recommandé est de **ne pas utiliser l'Oracle JDK**. Les exceptions qui permettraient un usage gratuit de ce Oracle JDK sont:

- exécuter les programmes Java sur l'environnement Cloud Oracle (OCI²²)
- exécuter des applications Java qui incluent une licence embarquée pour Oracle JDK (ASFU²³ à confirmer auprès l'éditeur concerné)
- n'utiliser le Oracle JDK qu'à des fins de développement
- n'utiliser que des versions de l'Oracle JDK 8 antérieures à avril 2019 (jre-8u202 ou inférieure), ce qui exclut d'avoir un MCS et est donc **INTERDIT**
- n'utiliser que des versions de l'Oracle JDK 17 antérieures à octobre 2024 (17.0.11 ou inférieure), ce qui exclut d'avoir un MCS et est donc **INTERDIT**
- utiliser Oracle JDK 21 ou supérieur (avec le risque d'un nouveau changement de posture d'Oracle)

En conséquence, hors usage d'un logiciel apportant une ASFU²⁴ et ayant obtenu une dérogation, une JVM Oracle déjà déployée sur un réseau soutenu par le CND, ainsi que les outils propriétaires associés doivent être désinstallés et les mises à jour automatiques désactivées sur le poste de travail.

Règle	Énoncé	Statut	Portée
CCT_R3_1	Il est INTERDIT d'utiliser un Oracle JDK sur un poste de travail ou un serveur de production du Ministère sauf d'une part, d'obtenir une dérogation, et, d'autre part de disposer d'un ASFU ²⁵ de l'éditeur du progiciel imposant son utilisation ou que le progiciel soit un produit Oracle inclu dans la liste de l'accord OTN de licence pour Java SE.	Min Arm	I

3.1.1.4 Postes de travail autonomes ou en mode déconnecté

Certains cas d'usage peuvent nécessiter de recourir à des postes de travail autonomes (i.e. jamais raccordés à un réseau du ministère) ou déconnectés (i.e. raccordés seulement de manière épisodique à un réseau du ministère).

Les postes de travail autonomes présentent un risque moindre de sécurité (seules les données qu'ils contiennent nécessitent une attention particulière) mais imposent une gestion spécifique coûteuse pour en assurer le maintien en condition opérationnelle ou de sécurité. C'est pourquoi il convient d'en limiter l'usage au strict nécessaire et d'essayer, autant que possible, de ne recourir qu'à des technologies maîtrisées utilisées sur les autres types de postes de travail.

²² Oracle Cloud Infrastructure

²³ 'Application Specific Full Use' ("Usage Complet Spécifique à une Application") : Désigne un type de licence restreinte vendue par un partenaire technologique ou un fournisseur de solutions Oracle pour être utilisée conjointement avec une application spécifique et définie appartenant au partenaire.

²⁴ 'Application Specific Full Use' ("Usage Complet Spécifique à une Application") : Désigne un type de licence restreinte vendue par un partenaire technologique ou un fournisseur de solutions Oracle pour être utilisée conjointement avec une application spécifique et définie appartenant au partenaire.

²⁵ 'Application Specific Full Use' ("Usage Complet Spécifique à une Application") : Désigne un type de licence restreinte vendue par un partenaire technologique ou un fournisseur de solutions Oracle pour être utilisée conjointement avec une application spécifique et définie appartenant au partenaire.

Les postes de travail en mode déconnecté répondent à deux cas d'usage :

- Travail nomade sans possibilité de connexion à un réseau du ministère pendant ce temps ;
- Nécessité impérative (pour des raisons légales ou opérationnelles) de maintenir le fonctionnement en cas de coupure réseau, malgré le risque infime d'occurrence d'un tel incident de nos jours.

L'usage de ces postes doit présenter les garanties de sécurité nécessaires permettant une reconnexion au réseau support. En conséquence :

- Aucun service ne doit y fonctionner en mode serveur pour d'autres postes de travail ou d'autres serveurs. Une demande de dérogation pour un fonctionnement serveur en boucle locale pourra toutefois être soumise à l'AGORA Tech si nécessaire ;
- Les logiciels installés doivent suivre les mêmes règles que celles des autres postes dudit réseau.

Pour ce type de postes, le recours à des technologies faiblement adhérentes dont PWA²⁶ ou un sous-ensemble (stockage local, service worker, ...) est particulièrement recommandé. À défaut, une application en technologie Electron reste préférable à un client lourd classique, malgré le cycle particulièrement rapide de mise à jour de cette solution qui impose un repackaging semestriel. La technologie WebAssembly (WASM) est en cours d'évaluation en vue d'un possible référencement au CCT à terme.

Une attention particulière devra être portée à l'authentification – si elle est nécessaire – afin qu'elle soit opérante avec les conditions de sécurité requises pour les 2 modes de fonctionnement.

3.1.1.5 Socle technique logiciel du poste de travail

Ci-dessous la liste des principaux composants logiciels constituant le socle technique du poste de travail nécessaire au fonctionnement, au maintien en condition de sécurité et de configuration du terminal.

☆☆☆☆ Le Navigateur IE 11 a été décomissionné sur Intradef et sur Internet, et est en cours de décomissionnement sur les réseaux classifiés : les directions d'application doivent faire en sorte que leurs SI ne soient plus adhérents à ce navigateur ni à un navigateur particulier. Navigateurs recommandés : Firefox ESR et EDGE Chromium ☆☆☆☆					
Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Système d'exploitation	Windows	Microsoft		★ / ★	★
Déploiement	Agent Configuration Manager (ex MECM, ex SCCM) Current Branch	Microsoft	Agent MCM de déploiement - cf. 6.2.3	R / S	Intradef
<i>Commentaire : tout autre outil d'installation sur un système d'exploitation Microsoft (tels que ClickOnce, Java Webstart, InstallAnywhere par ex.) ou le recours aux exécutables portables est interdit.</i>					
Environnement exécution	.NET Framework	Microsoft	Framework d'exécution des applications sur OS Windows	★ / ★	Min Arm
Environnement exécution	.NET Core	Microsoft	Framework d'exécution des applications sur OS Windows.	★ / ★	Min Arm

²⁶ Progressive web application : les applications web progressives utilisent des API web modernes ainsi qu'une stratégie d'amélioration progressive pour créer des applications web multiplateformes qui fonctionnent partout et possèdent des fonctionnalités qui donnent aux utilisateurs les mêmes avantages que les applications natives. Cette technologie est de mieux en mieux supportée et intégrée aux navigateurs et notamment EDGE. Par ailleurs, les mobiles sous Android sont compatibles des applications PWA.

Environnement exécution	OpenJDK	Eclipse Adoptium	Machine java virtuelle : suite à changement de politique de Oracle, la version de Java déployée est Eclipse Temurin, déployé hors master en tant <i>que dépendance d'un composant logiciel (cf ci- dessus 3.1.1.3 Recours à la machine virtuelle Java)</i> . Aussi appelé Eclipse Temurin JRE. Assujetti à l'usage sur windows, ou à la fin de vie de la version disponible dans les dépôts de la distribution linux.	★ / ★	Min Arm
<i>Commentaire : tout autre environnement devra faire l'objet d'une demande de dérogation dûment et rigoureusement justifiée. Le recours à l'OpenJDK Oracle ne sera pas accepté.</i>					

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.1.1.6 Offre logicielle du poste de travail [SU-STORE]

Le CND met à disposition des utilisateurs (du domaine DR-CPT) des logiciels déjà packagés en libre-service (Le NUMERI Store).

Par ailleurs, les utilisateurs peuvent demander un logiciel présent dans l'offre de service logiciel à partir du catalogue DIADEME.

Enfin, les utilisateurs peuvent exprimer un besoin dûment motivé et validé par leur tête de chaîne. Ce dernier fera l'objet d'une instruction par le CCB (*cf. §3.1.1.1*).

Pour les logiciels soumis à licence, les packages distribués sur les postes de travail nécessitent la saisie du numéro de licence pour que le logiciel soit installé.

Ci-dessous, la liste des principaux logiciels de bureautique du master ou en accès « libre » :

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Bureautique	Office: incluant Word, Excel, Outlook, PowerPoint, OneNote, Visio Viewer	Microsoft		★ / -	★
Bureautique	Modules Office: Skype for Business	Microsoft		★ / -	Intredef
Bureautique	Libre Office	The Document Foundation	Master : Déploiement sur simple demande pour Windows	★ / -	Intredef
Bureautique	Adobe Reader DC	Adobe	Master. Pour information, Firefox permet nativement de lire des fichiers PDF, de changer l'orientation des pages et de renseigner des formulaires.	R / -	Intredef
Bureautique	7-Zip	Igor Pavlov (logiciel libre)	Master : Compression	★ / -	Intredef
Navigateur	Firefox	Mozilla	Master cf. 4.5 Sécurisation des COTS	★ / -	Intredef S-SF SIA FrOps

Navigateur	EDGE Chromium	Microsoft	Version anaheim basée sur le noyau Chromium	R / -	Intredef
Navigateur	Internet Explorer	Microsoft	Master NB : produit déprécié par l'éditeur. cf. 4.5 Sécurisation des COTS	I / -	Min Arm
<i>Commentaire : le navigateur Microsoft Edge basé sur le noyau Chromium remplace IE. Les directions d'application DOIVENT faire en sorte que leurs SI ne soient plus adhérents à ce navigateur et pour ce faire, peuvent, si nécessaire et de manière transitoire, recourir au mode de compatibilité proposé par EDGE</i>					
Multimedia	VLC	Videolan	Master	R / -	Intredef
Multimedia	Flash player	Adobe	Statut : Interdit / Plus de soutien NB : retiré du socle et du navigateur début 2021	I / -	Min Arm
<i>Commentaire : pour des raisons de sécurité, tous les navigateurs interdisent désormais ce plugin. Le ministère en interdit l'usage. Microsoft a bloqué Flash via la mise à jour de juillet 2021 (KB4577586)</i>					
Sécurité	ACID Cryptofiler	Capgemini Abak Systèmes & MINARM	Master : Chiffrement des données de niveau DR, cf. 4.6.5.3.1 Chiffrement de fichiers [CHI].	R / -	Intredef

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.1.1.7 Messagerie

On distingue deux types de service de messagerie : messagerie officielle et messagerie non officielle. Un même concept d'emploi recouvre ces deux types :

Document	Date	Origine	Type doc	Portée
Concept d'emploi de messagerie électronique : Note conjointe : n°2859/DEF/EMA/CPI/AUT/NP / n°2202/DEF/SGA/ADJ/NP :	21 décembre 2010 15 décembre 2010	SC1	Concept Emploi	Min Arm
<i>Commentaire : concept d'emploi de messagerie électronique officielle et non officielle</i>				
SLR des services "messagerie officielle" et "messagerie non officielle" : note conjointe : n°1619/DEF/EMA/CPI/AUT/NP / n°304/DEF/SGA/ADJ/NP	11 février 2013 15 février 2013	SC1	SLR	Min Arm
<i>Commentaire : SLR relatif au service de messagerie</i>				
Procédure pour le mailing de masse : note conjointe : EMO.PRD.R4.003 version 1.1	01/07/2023	DIRISI	Procédure	Min Arm

3.1.1.7.1 Messagerie non officielle [SU-MEL]

Ce service permet à l'utilisateur de disposer d'une solution de messagerie électronique (personnelle ou de groupe) permettant d'échanger des messages non officiels tels que définis dans le concept de messagerie non officielle.

Ce service inclut des fonctions d'envoi-réception (de message depuis l'interne et l'externe) / archivage automatique / accusé de réception / carnet d'adresse / protection contre le courrier indésirable / envoi à des listes de diffusion.

Cas d'usage :

- Messagerie individuelle ou pour un groupe d'utilisateur, liée ou non à une fonction ;
- Utilisation possible de plusieurs comptes de messagerie ;
- Utilisation tolérée pour des besoins non professionnels dans la limite du respect des règles de sécurité et de non gêne du service professionnel ;
- Comptes techniques de messagerie à destination des systèmes d'information.

Voir partie back office §3.3.1.1 Messagerie non officielle – Agenda

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Messagerie (Client)	Client Outlook	Microsoft	Client de messagerie	★ / -	Intredef S-SF SIA FrOps
Messagerie (Client)	Client Thunderbird	Mozilla	Client de messagerie alternatif. Ce client est également déployé sur les postes CLIP-HESTIA.	A	Intredef
Messagerie (Client)	Outlook Web Access (OWA)	Microsoft	Webmail simulant un client Outlook	R / S	Intredef
Messagerie (Client)	SOG		Assujetti au contexte SIE : Webmail pour le SIE (Baltique/Celtique), connectable avec le client Outlook et offrant des fonctions de partage de calendriers et de carnets d'adresses.	A / -	SIE
Messagerie(serveur)	Partie serveur : cf. 3.3.1 Messagerie / Agenda / Tâches / Listes de diffusion				

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.1.1.7.2 Messagerie officielle [SU-MOF]

Ce service permet à l'utilisateur de disposer d'une solution de messagerie électronique (personnelle ou de groupe) permettant d'échanger des messages officiels tels que définis dans le concept d'emploi de messagerie. (Les messages sont considérés comme officiels, si et seulement s'ils sont émis à partir d'une adresse d'organisme et s'ils respectent un certain formalisme.)

Ce service est assuré de façon principale par NEMO .

La trajectoire des messageries officielles de l'État-Major des Armées en relation avec le nouveau concept de messagerie fait de NeMO (Nouvelle Messagerie Officielle) la messagerie officielle de l'Intredef.

Document	Date	Origine	Type doc	Portée
Nommage des adresses électroniques(cf. §3.3.4.1 Annuaires / référentiels)				
<i>Commentaire : défini par la directive de nommage des annuaires</i>				
Gestion de la liste unique des mots clés d'attribution (MCA) cf. 8.5.4 Mots clés d'attribution (MCA)				
Emploi de la messagerie officielle (NeMO) sur le réseau Intredef de l'EMA diffusé par note I-14-000549/DEF/EMA/ESMG/NP du 7 février 2014	7 février 2014	EMA	Note	Min Arm
<i>Commentaire : cette note décrit l'emploi de NEMO dans le cadre des cellules de management de l'information de l'EMA.</i>				

3.1.1.7.3 Agenda, contacts [SU-AGE]

Ce service recouvre l'accès à la gestion d'un ou plusieurs agendas personnels, depuis tout type de terminal, et ce de façon synchronisée (en cible), la planification d'événement et la réservation éventuelle de toutes ressources associées (salles, moyens techniques...), la gestion des invitations, et toutes les fonctions classiques de configuration et de gestion d'agenda.

Document	Date	Origine	Type doc	Portée
Concept d'emploi agenda : Note conjointe : n°11299/DEF/EMA/CPI/AUT/NP /n°1758/DEF/SGA/ADJ :	22 octobre 201223 octobre 2012	SC1	Concept Emploi	Min Arm
SLR du service "agenda" : note conjointe : n°1117/DEF/EMA/CPI/AUT/NP /n°202/DEF/SGA/ADJ/NP	28 janvier 201329 janvier 2013	SC1	SLR	Min Arm

Les solutions d'agenda, de gestion de contacts et de gestion de tâches personnelles sont intégrées aux solutions logicielles de client de messagerie (*cf. 3.1.1.7 Messagerie*)

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Partage calendriers, contacts, messages	Outlook Web Access (OWA)	Microsoft	Webmail simulant un client Outlook	R	Tout intranet
Partage calendriers, contacts, messages	Outlook	Microsoft	Master	R	Intredef

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.1.1.8 Portail personnalisable [SU-GPE]

Voir partie back office §3.3.2.1 Portail personnalisable [GPE]

3.1.1.9 Accessibilité du poste de travail

Certains logiciels bureautiques d'accessibilité sont autorisés sur les postes du Ministère des Armées.

Pour les personnes malvoyantes : les licences des logiciels autorisés sont disponibles auprès du service SGA/DRH-MD/DNH.

Pour les personnes malentendantes : un marché d'acquisition a été conclu, via l'UGAP, avec la société TADEO.

Packaging des logiciels : Les logiciels identifiés feront l'objet d'une demande de packaging auprès du CCB, et ce de manière régulière, en fonction des renouvellements de versions. Pour les logiciels installés moins fréquemment, il convient de déterminer qui sera responsable de la demande de packaging auprès du CCB : la DSI RH ou le CORSIC de proximité de l'agent.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Accessibilité du poste de travail	Jaws	Freedom Scientific	Logiciel de revue d'écran.	A / -	Min Arm
Accessibilité du poste de travail	Zoomtext	Freedom Scientific	Logiciel d'agrandissement d'écran sans lecture vocale	A / -	Min Arm
Accessibilité du poste de travail	FineReader	ABBYY	Logiciel de reconnaissance de caractère des documents PDF	A / -	Min Arm
Accessibilité du poste de travail	DuxBury Braille Translator	DuxBury Systems	Logiciel d'impression Braille	A / -	Min Arm
Accessibilité du poste de travail	Dragon Professional	Nuance	Logiciel de synthèse vocale (dictée)	A / -	Min Arm
Accessibilité du poste de travail	Fusion Pro	Freedom Scientific	Combinaison : lecture d'écran Jaws et agrandissement d'écran ZommText	A / -	Min Arm

3.1.2 Collaboratif

3.1.2.1 Communication instantanée

3.1.2.1.1 Dialogue en ligne, gestion de présence [SU-PRE], messagerie instantanée [SU-MIN]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "discussion en ligne" : note conjointe : n°11230/DEF/EMA/CPI/AUT/NP / n°1759/DEF/SGA/ADJ	22 octobre 2012 23 octobre 2012	SC1	Concept Emploi	Min Arm
<i>Commentaire : ce concept d'emploi couvre les notions de messagerie instantanée, de gestion de présence et de discussion en ligne</i>				
SLR des services de "discussion en ligne" : note conjointe : n°701/DEF/EMA/CPI/AUT/NP / n°151/DEF/SGA/ADJ/NP	18 janvier 2013 22 janvier 2013	SC1	SLR	Min Arm

3.1.2.1.2 Réunion virtuelle [SU-REV], audioconférence [SU-AUD], visioconférence [SU-VIS], vidéoconférence [SU-VID]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "réunion virtuelle" : note conjointe : n°12477/DEF/EMA/CPI/AUT/NP / n°2033/DEF/SGA/ADJ	26 nov. 2012 30 nov. 2012	SC1	Concept Emploi	Min Arm
SLR des services "audioconférence" et « visioconférence » : note conjointe : n°1116/DEF/EMA/CPI/AUT/NP / n°200/DEF/SGA/ADJ/NP	26 janvier 2013 29 janvier 2013	SC1	SLR	Min Arm
<i>Commentaire : SLR relatif aux services d'audioconférence et visioconférence</i>				
Politique de la messagerie instantanée sécurisée de l'Etat « TCHAP » pour le ministère des armées : diffusée par note n°98/ARM/DGNUM/DG/NP du 21 mars 2019	21 mars 2019	DGNUM	Politique d'emploi	Min Arm
<i>Commentaire : cette politique décrit le cadre d'emploi de la messagerie TCHAP. Cette messagerie est utilisée pour des échanges de confiance des agents du ministère entre eux, avec d'autres agents étatiques ou, sur invitation, avec des partenaires extérieurs, via des téléphones « grand public » non sécurisés, privés ou professionnels de type Android ou Apple.</i>				

3.1.2.1.3 Solutions logicielles client

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Communications instantanées	Lync	Microsoft	Client couplé au serveur	I / -	Min Arm
Communications instantanées	Skype for business	Microsoft		★ / ★	Min Arm
Communications instantanées	JChat	OTAN	Client couplé au serveur TCS. Solution de chat opérationnelle nativement interopérable avec l'OTAN. Sur Intradef, solution de chat opérationnelle uniquement pour les cas d'usage Guyane	A / -	Intrade f S-SF SIA FrOps
Communications instantanées	Audioconf CND	CND	Pour des échanges NP.	R / -	NP
Communications instantanées	Audioconf de l'état	DINUM	Service internet soutenu par la DINUM : https://audioconf.numerique.gouv.fr/	R / -	NP

Communications instantanées	La suite Meet	DINUM	Service internet soutenu par la DINUM : https://visio.numerique.gouv.fr/	R / -	NP
Communications instantanées	Tchap	DINUM	Service internet soutenu par la DINUM	R / -	Interne t
<i>Commentaire : voir politique d'emploi ci-dessus.</i>					
Communications instantanées	OLVID	OLVID	Solution de chat sécurisé	R / -	Interne t
<i>Commentaire : interdit sur intradef, sauf à mettre en œuvre une instance homologuée, sur décision du COMCyber (NeMO n°2024/691 du 18/10/2024)</i>					
Communications instantanées	Webconf de l'Etat	DINUM	Service internet soutenu par la DINUM : https://webconf.numerique.gouv.fr/	R / -	Interne t
<i>Commentaire : fonctionne sur des postes internet à partir d'un navigateur mais pas au travers d'ISPT, en utilisant le service interministériel. https://www.numerique.gouv.fr/outils-agents/webconference-etat/</i>					
Communications instantanées	Webinaire de l'Etat	DINUM	Service internet soutenu par la DINUM : https://webinaire.numerique.gouv.fr/home	R / -	Interne t
<i>Commentaire : fonctionne sur des postes ISPT. https://www.numerique.gouv.fr/outils-agents/webinaire-etat</i>					
Communication instantanée(serveur)	<i>Partie back-office serveur : cf. 3.3.3.1 Messagerie instantanée – Réunion virtuelle – Vidéoconférence - Rédaction collaborative synchrone [MIN-REV-VIH-RCS]</i>				
Communications instantanées	Jabber		Communication OTAN (cf. WEBEX partie serveur)	A / E	SIA FrOps

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.1.2.2 Espace de travail collaboratif [SU-EDT]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "espace de travail collaboratif" : note conjointe : n°11231/DEF/EMA/CPI/AUT/NP / n°1760/DEF/SGA/ADJ	22 octobre 201223 octobre 2012	SC1	Concept Emploi	Min Arm
<i>Commentaire : ce concept d'emploi couvre la gestion d'espaces de travail collaboratif et leur accès ainsi que des outils associés : partage de ressources, workflow de travail, production de documents en commun, gestion de versions, assignation et suivi des tâches, partage d'agenda, outils d'échange ou de partage internes à la communauté (discussion en ligne, wiki, enquêtes, mind mapping, ...)</i>				
SLR du service "espace de travail collaboratif" : note conjointe : n°699/DEF/EMA/CPI/AUT/NP / n°200/DEF/SGA/ADJ/NP	26 janvier 201329 janvier 2013	SC1	SLR	Min Arm

L'accès à un tel service à l'utilisateur doit se faire via le navigateur du poste client.

Solutions : Voir partie back office - serveur §3.3.2.8 **Gestion des communautés d'intérêt [COI]**

3.1.2.3 Wiki [SU-WKI]

L'accès à un tel service à l'utilisateur doit se faire via le navigateur du poste client.

Document	Date	Origine	Type doc	Portée
Concept d'emploi "wiki" : note conjointe : n°6352/DEF/EMA/CPI/AUT/NP / n°960/DEF/SGA/ADJ/NP	3 juin 20135 juin 2013	SC1	Concept Emploi	Min Arm
SLR du service "wiki" : note conjointe : n°1626/DEF/EMA/CPI/AUT/NP / n°1199/DEF/SGA/ADJ	2 juillet 2013, 9 juillet 2013	SC1	SLR	Min Arm

Solutions : Voir partie back office - serveur §3.3.3.2 **Wiki [WKI]**

3.1.2.4 Tableau blanc - Rédaction synchrone

Pour l'instant, les fonctions collaboratives s'arrêtent aux fonctions de tableau blanc et sont essentiellement amenées par le client Skype.

Solutions : Voir partie back office - serveur

§3.3.3.1 Messagerie instantanée – Réunion virtuelle – Vidéoconférence - Rédaction collaborative synchrone [MIN-REV-VIH-RCS]

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Tableau blanc (client)	Lync Live Meeting	Microsoft		I / N	Internet Intradef
Tableau blanc (client)	Lync Live Meeting	Microsoft		D / -	SIA S-SF SIA FrOps
Tableau blanc (client)	Skype for business	Microsoft		★ / ★	Tout intranet
Rédaction synchrone(client)	Navigateur ou Suite bureautique interfacé avec Sharepoint ou Alfresco		Dans le cadre des espaces de travail collaboratif	★ / ★	Tout intranet

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.1.2.5 Forum [SU-FOR]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "forum" : note conjointe : n°3814/DEF/EMA/CPI/AUT/NP / n°555/DEF/SGA/ADJ	26 mars 2013 28 mars 2013	SC1	Concept Emploi	Min Arm
SLR du service "forum" : note conjointe : n°4582/DEF/EMA/CPI/AUT/NP / n°686/DEF/SGA/ADJ/NP	12 avril 201315 avril 2013	SC1	SLR	Min Arm

L'accès à ce service à l'utilisateur se fait via le navigateur du poste client.

Solutions : Voir partie back office - serveur §3.3.3.3 Forum [FOR]

3.1.2.6 Listes de diffusion

Cf. §3.3.1.4 Liste de diffusion [LDF]

3.1.2.7 Réseau social [SU-RSE]

Solutions : Voir partie back office - serveur §3.3.2.9 Réseau social d'entreprise [RSE]

3.1.3 Vie courante

3.1.3.1 Portail intranet [SU PIN]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "portail intranet" : note conjointe : n°529/DEF/EMA/CPI/AUT/NP / n°152/DEF/SGA/ADJ	16 janvier 2013 22 janvier 2013	SC1	Concept Emploi	Min Arm Tout intranet
SLR du service "portail intranet" : note conjointe : n°1349/DEF/EMA/CPI/AUT/NP / n°247/DEF/SGA/ADJ	4 février 2013 16 février 2013	SC1	SLR	Min Arm Tout intranet
Compte rendu du CODIR restreint des Intranets n°24 du 3 avril 2014 diffusé par note conjointe : n°D-14-004992 /DEF/EMA/PSIOC/NP du 19 mai 2014 n°316/DEF/DGSIC/NP du 20 mai 2014	19 mai 2014 20 mai 2014	CODIR Intranets	Note	Min Arm Internet Intradef
<i>Commentaire : le compte rendu porte décision relative au choix des outils pour les portails de communications pour le NP-DR.</i>				

L'accès à ce service à l'utilisateur se fait via le navigateur du poste client.

Solutions : Voir partie back office - serveur §3.3.2.2 Portail d'information [PIN]

3.1.3.2 Annuaire pages blanches, pages jaunes [SU-PJB]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "pages jaunes – pages blanches" : Note conjointe : n°10710/DEF/EMA/CPI/AUT/NP /n°1687/DEF/SGA/ADJ	9 octobre 2012 11 octobre 2012	SC1	Concept Emploi	Min Arm
SLR du service "pages jaunes – pages blanches" : note conjointe : n°591/DEF/EMA/CPI/AUT/NP /n°145/DEF/SGA/ADJ/NP	17 janvier 2013 22 janvier 2013	SC1	SLR	Min Arm

Voir aussi §3.3.4.1 *Annuaire / référentiels* et § 3.3.4.3 *Outils de « provisionning » d'annuaires*

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Annuaire Pages blanches	Solution Annudef	Min Arm	Ce service est réalisé sur développement interne. Échéance prévisionnelle de décommissionnement à l'horizon 2027.	R / S	Intradef
Annuaire Pages blanches	INA (Identité Numérique de l'Agent)	Min Arm	Futur remplaçant de l'Annudef	E / E	Intradef
Annuaire Pages blanches	Annuaire de référence OpenLDAP provisionné via MEIBO	Min Arm	Service packagé IntraCed S-SF et SIA S-SF	R / S	S-SF SIA FrOps

3.1.3.3 Impression – édition multifonction [SU-IMP]

Ces services renvoient essentiellement à des fonctions d'impression, de copies et de numérisation de documents.

Sauf pour répondre à des besoins très spécifiques, ces services sont assurés par des photocopieurs multifonctions réseaux mutualisés entre services et activés via une identification par badge (CIMS par défaut ou une carte subsidiaire si l'utilisateur ne possède pas encore de CIMS) et une authentification par un code numérique. Ces services de proximité doivent être également accessibles en itinérance interne.

L'enrôlement s'opère en fonction du compte Active Directory pour les postes du domaine considéré. S'il n'y a pas de lecteur de badge ou si celui ne fonctionne pas, l'authentification en fonction du compte Active Directory reste toujours possible, si la fonction est disponible. L'authentification sur les photocopieurs multifonctions réseaux mutualisés est obligatoire pour les fonctions copie, impression et numérisation pour permettre l'imputabilité et la traçabilité.

Les photocopieurs multifonctions sont des objets partagés dans l'Active Directory et peuvent être recherchés et installés depuis le poste de travail, en fonction des droits dont dispose l'utilisateur.

L'authentification par badge et code est centralisée par défaut, mais elle peut être locale à un unique photocopieur multifonction pour des besoins spécifiques.

Par défaut, l'acquisition d'imprimantes multifonctions passe par le marché SOLIMP pour les intranets sous responsabilité de l'opérateur CND.

Le SIE met en œuvre le serveur d'impression CUPS sur son domaine local.

Document	Date	Origine	Type doc	Portée
Politique d'impression au ministère des armées - Édition 2 : diffusé par note n°397/ARM/DGNUM/DG/NP	21 juin 2024	DGNUM	Politique	Min Arm
<i>Commentaire :</i>				
Concept d'emploi "point d'édition multifonction" : diffusée par note conjointe : n°5441/DEF/EMA/CPI/AUT/NP / n°827/DEF/SGA/ADJ	13 mai 2013 13 mai 2013	SC1	Concept Emploi	Min Arm NP/DR
<i>Commentaire : concept d'emploi "point d'édition multifonction" : ce document couvre les fonctions d'impression, de copie de documents, de numérisation, de télécopie pour un utilisateur, ainsi que les fonctions de découverte, de paramétrage et de gestion des imprimantes.</i>				
SLR du service "point d'édition multifonction" : note conjointe : n°5955/DEF/EMA/CPI/AUT/NP / n°908/DEF/SGA/ADJ	24 mai 2013 27 mai 2013	SC1	SLR	Min Arm NP/DR
Offre de service SOLIMP DIADEME fiche 1290	2019			Min Arm
<i>Commentaire : le service est assuré via le marché cadre SOLIMP IV. En complément et sur justification, des besoins spécifiques peuvent être couverts .</i>				

3.1.3.4 Moteur de recherche [SU-RMR]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "moteur de recherche" : note conjointe : n°4584/DEF/EMA/CPI/AUT/NP / n°683/DEF/SGA/ADJ	12 avril 2013 15 avril 2013	SC1	Concept Emploi	Min Arm
SLR du service "moteur de recherche" : note conjointe : n°5155/DEF/EMA/CPI/AUT/NP / n°769/DEF/SGA/ADJ	26 avril 2013 29 avril 2013	SC1	SLR	Min Arm

Les moteurs de recherche sont accessibles via le navigateur du poste client. **Voir partie back office §3.3.2.7 Moteur de recherche [RMR]**

3.1.3.5 Enquête et sondage [SU-ENQ]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "enquêtes et sondages" : note conjointe : n°7558/DEF/EMA/CPI/AUT/NP / n°1164/DEF/SGA/ADJ	1er juillet 2013 1er juillet 2013	SC1	Concept Emploi	Min Arm
<i>Commentaire : concept d'emploi "enquêtes et sondages" : ce document couvre les fonctions de création, envoi, réponse, exploitation et analyse de résultats de questionnaires.</i>				
SLR du service "enquêtes et sondages" : note conjointe : n°8487/DEF/EMA/CPI/AUT/NP / n°1295/DEF/SGA/ADJ	12 juillet 2013 13 juillet 2013	SC1	SLR	Min Arm
Rationalisation des logiciels de questionnaires, sondages et enquêtes : note n°294/DEF/DGSIC/SDMA/BGAI du 16 mars 2011	16 mars 2011	DGSIC	Note	Intradef

Ce service à l'utilisateur est accessible via le navigateur du poste client. Voir partie back office §3.3.2.10 **Enquête et sondage [ENQ]**.

3.1.3.6 Réservation de salles [SU-RDS]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "réservation de salles" : note conjointe : n°8889/DEF/EMA/CPI/AUT/NP / n°1270/DEF/SGA/ADJ	18 juillet 2013 18 juillet 2013	SC1	Concept Emploi	Min Arm
SLR du service "réservation de salles" : note conjointe : n°8888/DEF/EMA/CPI/AUT/NP / n°1269/DEF/SGA/ADJ	18 juillet 2013 18 juillet 2013	SC1	SLR	Min Arm

Ce service est adossé au service d'agenda. Sur l'Intradef, sauf à Balard, les salles sont des ressources enregistrées dans l'annuaire technique Active Directory DR-CPT.

Sur Balard, le service fait l'objet d'un service séparé OPALE non intégré au service d'agenda et nécessitant le report manuel de la salle réservée dans le service d'agenda.

3.1.4 Gestion des données

3.1.4.1 Stockage des données [SU-REP]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "stockage de données" : note conjointe : n°4140/DEF/EMA/CPI/AUT/NP / n°640/DEF/SGA/ADJ	2 avril 2013 / 5 avril 2013	SC1	Concept Emploi	Min Arm
<i>Commentaire : concept d'emploi "stockage de données" : ce document couvre : le stockage des données professionnelles d'un utilisateur (support amovible, poste de travail, via l'intranet), le stockage des données professionnelles partagées par des utilisateurs, le stockage des données de personnalisation du poste de travail permettant la mobilité, le stockage des données privées d'un utilisateur.</i>				
SLR du service "stockage de données" : note conjointe : n°4688/DEF/EMA/CPI/AUT/NP / n°713/DEF/SGA/ADJ	18 avril 2013 / 18 avril 2013	SC1	SLR	Min Arm

Partie BackOffice :

Cf. 3.3.2.5 Syndication de contenu [ASY]

Cf. 3.3.2.6 Répertoires partagés [REP]

3.1.4.2 Transfert de données volumineuses [SU-TFV]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "transfert de données volumineuses" : note conjointe : n°444/DEF/EMA/CPI/AUT/NP / n°153/DEF/SGA/ADJ	14 janvier 2013 22 janvier 2013	SC1	Concept Emploi	Min Arm
SLR du service "transfert de données volumineuses" : note conjointe : n°1350/DEF/EMA/CPI/AUT/NP / n°249/DEF/SGA/ADJ	4 février 2013 6 février 2013	SC1	SLR	Min Arm

La solution Defense Drive (Intradef) permet de mettre en œuvre les dispositions principales du concept d'emploi transfert de données volumineuses de niveau non protégé et restreint ainsi que du concept d'emploi "Stockage de données". France Transfert doit également être utilisé pour des échanges de niveau non protégé.

Les solutions serveurs « back office » sont décrites en §3.3.6.5 Transfert fichiers volumineux [TFV]

3.1.5 Sécurité [SU-SSO, SU-CHI, SU-SIG]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "services de sécurité de l'utilisateur" : note conjointe :n°D12-013027/DEF/EMA/CPI/AUT/NP / n°2090/DEF/SGA/ADJ	7 décembre 201210 décembre 2012	SC1	Concept Emploi	Min Arm Intradef S- SF
<i>Commentaire : ce document traite des services de sécurité relatifs à l'utilisateur et couvre les besoins attendus en cible :pour l'authentification : authentification simple en fonction de son besoin, aussi unique que possible (SSO), authentification forte ciblée ;la signature électronique et le cachet serveur : signature répondant au besoin de confiance et de durée de conservation dans le temps, assurant la non-répudiation, garantissant l'intégrité visuelle et sémantique du contenu, assurant des preuves d'envoi et de réception via un service d'horodatage, pouvant faire office de preuve ; ce service doit couvrir tous les besoins d'échanges entre autorités administratives, avec les partenaires et la société civile, les besoins d'échanges impliquant les agents; le chiffrement pour protéger les documents (documents et messages, les échanges, les postes terminaux notamment en situation de mobilité, les données transitant sur un réseau, accéder à des ressources en situation de mobilité).</i>				
SLR des services de "sécurité de l'utilisateur" : note conjointe :n°D13-004806/DEF/EMA/CPI/AUT/NP / n°726/DEF/SGA/ADJ/NP	18 avril 2014 22 avril 2014	SC1	SLR	Min Arm Intradef
Cadre d'emploi de la signature électronique au ministère des Armées – Édition 2 cf. 4.6.3.2 Signature [SGN]	8 juillet 2021	DGNUM	Concept emploi	Min Arm

Pour aller plus loin : Cf. § 4.6 Services de sécurité

3.1.6 Mobilité [SU-AN, SU-ITN]

Deux solutions ministérielles de mobilité (nomadisme) permettant depuis l'extérieur d'accéder à l'Intradef sont actuellement en service au sein du ministère : SMOBI et téléphonie mobile.

SMOBI est la solution proposée par le CND avec :

- un volet « ordiphone » (certains smartphones et tablettes Android de la marque Samsung) basé sur une sécurisation du terminal et de l'accès jusqu'au niveau DR ; une solution complémentaire de gestion de flotte (Mobile Iron en cours de remplacement par Push Manager) est installée sur les terminaux en vue du déploiement d'applications depuis un magasin d'applications dédié du Ministère ;
- un volet poste de travail (sous Microsoft Windows) : il s'agit d'un poste de travail portable standard de l'Intradef équipé d'une sécurisation de l'accès , d'une pile logicielle

complémentaire dédiée (chiffrement du disque dur, détection automatique de l'environnement LAN/mobilité) et éventuellement d'une connexion 4G ;

- l'accès à l'Intraderf se fait via une passerelle dédiée SMOBI. La navigation Internet sur le poste se fait via ISPT (Internet sur le poste de travail) sous réserve, pour le volet poste de travail, de disposer de ce service.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°25 portant sur la mobilité publiée au Bulletin Officiel des Armées modifiant la Directive DGSIC n°12 portant sur la mobilité du 1er juin 2010	29 mars 2012	DGSIC	Directive	Réseaux non classifiés
<i>Commentaire : règles applicables au nomadisme et à la mobilité externe sur les réseaux non classifiés. Cette directive liste notamment les fonctions de sécurité que les solutions de mobilité doivent respecter en priorité.</i>				
Concept d'emploi des services de mobilité : note conjointe n°D11-4204/DEF/EMA/CPI/AUT/NP / n°878/DEF/SGA/ADJ	13 mai 2011 19 mai 2011	SC1	Concept Emploi	Min Arm Intraderf S-SF
<i>Commentaire : ce document traite des services relatifs aux services d'itinérance (mobilité interne) et de nomadisme pour les postes de travail ainsi qu'aux services liés aux Smartphones sur l'Intraderf. Le réseau S-SF n'est concerné que par des services d'itinérance.</i>				
SLR des "services de mobilité" : note conjointe : n°D12-134/DEF/EMA/CPI/AUT/NP / n°79/DEF/SGA/ADJ	06 janvier 2012 16 janvier 2012	SC1	SLR	Min Arm Intraderf
<i>Commentaire : SLR relatifs aux accès en itinérance (BS09) et en nomadisme (BS10)</i>				
Directive DIRISI n° 89 d'exploitation des solutions de mobilité de l'Intraderf version 1.0 du 02/04/2013	2 avril 2013	DIRISI	Directive	Intraderf
<i>Commentaire : cette directive porte sur les solutions techniques de mobilité actuellement en service au sein du ministère, notamment SMOBI.</i>				
Directive DIRISI n° 86 de soutien de la solution de mobilité SMOBI	2 avril 2013	DIRISI	Directive	Intraderf
Directive d'emploi des services de mobilité SMOBI Note n°123/DEF/SGA/ADJ du 31 janvier 2014	31 janvier 2014	SGA	Note	Intraderf
SMOBI – Dérogation à l'étranger diffusé par NEMO UM SNUM 2020/225 du 21 juillet 2020	21 juillet 2020	UM SNUM	Note	Intraderf
<i>Commentaire : ce NEMO porte un avis technique sur les conditions d'utilisation d'un SMOBI à l'étranger</i>				
Plan de management des services de mobilité sécurisée de l'Intraderf (Solution de mobilité de l'Intraderf – SMOBI) diffusé par note n° 501272/DEF/DIRISI/SCI/SI/NP version 1.0 du 1er juin 2014	4 juin 2014	DIRISI	Note	Intraderf
Spécification d'interface SMOBI à l'attention des SI : Cadre d'architecture et contraintes de configuration pour un système d'information accessible sur un terminal SMOBI v1.2	8 décembre 2022	UM SNUM / DIRISI	Note technique	Intraderf
<i>Commentaire : cette note technique s'adresse aux directions d'application ayant vocation à être accédées en mobilité via SMOBI. Elle définit les conditions pour une bonne intégration des applications dans l'écosystème SMOBI.</i>				
Mise en œuvre de la téléphonie mobile au sein des bases de défense. Cf. 5.1.8.1 Téléphonie classique	4 février 2014	EMA	Note	Intraderf

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Mobilité « poste de travail »	SMOBI	CND	Utilisation de la station de travail de l'Intraderf (poste unique) en situation de nomadisme et éventuellement une connexion type réseaux mobiles civils.	R / S	Intraderf
Mobilité « ordiphone »	SMOBI	CND	Utilisation d'un ordiphone du commerce (smartphones et tablettes de marque Samsung fournis par l'administration) .	R / S	Intraderf

3.1.7 Accès réseaux extérieurs

3.1.7.1 Internet sur le poste de travail [SU-WEB]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "internet sur le poste de travail" : diffusé par note conjointe :n°9065/DEF/EMA/CPI/AUT/NP /n°2249/DEF/SGA/ADJ	22 nov. 2011 30 nov. 2011	SC1	Concept Emploi	Min Arm Intraderf
<i>Commentaire : concept d'emploi "internet sur le poste de travail" : ce document couvre les fonctions d'accès depuis le poste de travail à la messagerie et à la navigation sur le réseau internet.</i>				
SLR du service "internet sur le poste de travail" : note conjointe : n°2810/DEF/EMA/CPI/AUT/NP /n°664/DEF/SGA/ADJ	29 mars 2012 4 avril 2012	SC1	SLR	Intraderf
Transmission de données sensibles par Internet : par note n°D-12-002601/DEF/EMA/CPI/SSI/NP /	23 mars 2012	EMA	Note	Intraderf
<i>Commentaire : cette note précise les obligations faites dans l'usage de SISMEI pour la transmission d'informations sensibles : pas de redirection automatique, chiffrement préalable des données sensibles.</i>				

Conformément au concept d'emploi de l'internet sur le poste de travail qui prévoit un poste unique NP/DR relié à l'Intraderf (pour rappel, l'accès aux services de l'internet sur un poste classifié de défense est interdit) et disposant d'accès à l'internet, le catalogue de service du Ministère propose à l'utilisateur le service SISMEI.

SISMEI : service de messagerie (SISMEI) permettant d'émettre/recevoir des messages vers/de l'internet directement depuis la boîte aux lettres hébergée sur l'Intraderf : l'usage de ce service est actuellement limité aux messages non officiels ; les pièces jointes de niveau DR, DR-SF et autre niveau de confidentialité spécifique (personnel, médical, etc.) ne peuvent être émises que si elles ont été préalablement chiffrées par un logiciel adapté à leur niveau de sensibilité (par exemple ACID ou Zed ! pour le niveau DR, Cf. 4.6.5.3.1 Chiffrement de fichiers [CHI]).

Document	Date	Origine	Type doc	Portée
Directive DIRISI d'exploitation de SISMEI V2 : sous timbre n°1100318/DEF/DIRISI/SCOL/B.EMP/Intranets du 26 février 2008	26 février 2008	DIRISI	Directive	Intraderf

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Échanges mail Internet	SISMEI	Min Arm	Passerelle de messagerie sécurisée mise en place par le MinArm entre la messagerie de l'Intraderf et l'Internet	R / S	Intraderf

ISPT – Internet Sur le Poste de Travail : service de navigation sur l'internet depuis le navigateur du poste Intraderf ;

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°232 d'exploitation et de soutien du service Internet sur le poste de travail (ISPT) V8.2	10 décembre 2018	DIRISI	Directive	Intraderf

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Accès Web Internet	ISPT : Internet sur	Min Arm	Passerelle assurant l'accès au service de navigation sur l'Internet depuis le poste de travail de l'Intraderf. Le nombre de postes et	R / S	Intraderf

	le Poste de Travail		d'utilisateurs bénéficiant du service ISPT est limité		
--	---------------------	--	---	--	--

Le service ISPT fonctionne en mode :

- « liste noire » : un site référencé par le CALID dans cette liste noire est interdit d'accès via ISPT ;
- « liste blanche » : un site nécessite d'être autorisé pour être accédé. La demande d'autorisation d'accès à un site non encore connu se fait automatiquement.

Ces deux services (SISMEL et ISPT) mettent en œuvre des politiques de filtrage de flux et de contenus ainsi que de protection contre les codes malveillants. Ces services sont exclusivement à l'usage des utilisateurs finaux et n'ont pas vocation à être consommés via des robots ou des mécanismes d'automatisation. Pour de tels usages, il est recommandé le recours à la route API.

Par ailleurs, pour des besoins particuliers, des boîtes aux lettres fonctionnelles ou nominatives (adresse en @def.gouv.fr) hébergées directement sur l'Internet peuvent être mises à disposition dans le cadre du marché ASTEL-I en remplacement de MIM3.

3.1.7.2 Accès aux réseaux interministériels [SU-RMI] et autres réseaux extérieurs [SU-REX]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "accès réseaux extérieurs" : note conjointe : n°D14-002653/DEF/EMA/CPI/AUT/NP / n°389/DEF/SGA/ADJ	10 mars 2014 12 mars 2014	SC1	Concept Emploi	Min Arm Intradef S-SF
<i>Commentaire : ce document traite des accès aux réseaux extérieurs de même niveau de confidentialité ou de niveau de confidentialité différente via des passerelles et des besoins cibles relatifs à ces passerelles : accès à des applications, échanges de données et besoins de services à l'utilisateur, dans le respect de la réglementation et du droit d'en connaître.</i>				
SLR des services "d'accès aux réseaux extérieurs" : note conjointe : n°D14-003482/DEF/EMA/CPI/AUT/NP / n°687/DEF/SGA/ADJ/NP	27 mars 2014 14 mai 2014	SC1	SLR	Min Arm Intradef

Ces accès sont réalisés au travers de passerelles : cf. **4.7 Interconnexions, passerelles et solutions de sécurité iso/multi niveaux**

3.1.8 Téléphonie

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°7 portant sur la téléphonie sur le protocole internet publiée au Bulletin Officiel des Armées	13 janvier 2009	DGSIC	Directive	Min Arm
<i>Commentaire : Cette directive définit la politique à mettre en œuvre avant le déploiement d'un service de téléphonie sur le protocole internet (ToIP) par les organismes du ministère de la défense. Elle fournit les critères de décision pour l'acquisition, la réalisation et la mise en œuvre d'un service de ToI.</i>				

Voir aussi : §5.1.7

Pour en savoir plus sur Téléphonie et 5 ToIP / VoIP : §5.2.

3.1.9 Services divers

3.1.9.1 E-formation

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
e-formation	ILIAS	www.ilias.de	Learning Management System (LMS) : plateforme d'enseignement à distance/ DR	R / S	Min Arm
e-formation	Suite SCENARI	Université Technologique de Compiègne (UTC) et société KELIS	Logiciel libre. Atelier de production de chaîne éditoriale	R / S	Intradef Internet
e-formation	Moodle	Moodle HQ	Learning Content Management System (LCMS) : Système de création et de gestion de contenu pédagogique pour alimenter un LMS. Logiciel libre sous licence GNU GPL.	★ / ★	Intradef Internet

3.1.9.2 Traduction [SU-TRL]

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Traduction	REVERSO			D / -	SIA S-SF SIA FrOps
Traduction	SYSTRAN Pure Neural Server (SPNS 9) ou SYSTRAN Translate Server (STS 10)	Systran SAS (FR)	- Traduction neuronale disponible pour 55 langues, portail de traduction, web services (API REST) - OS : RHEL/Almalinux pour STS10 (RHEL/Centos 7 ou 8 pour SPNS9) - Intègre nativement un OCR, en option connecteur possible vers un outil de transcription de la parole - Mode SaaS (souverain européen OVH) ou on-premise (CPU ou GPU) - Outil non soumis à des restrictions export ni à des juridictions extra-européennes - Intégré dans ARTEMIS.IA	A / S	Min Arm
Traduction	GenIAI - Traduction	Min Arm	Service en ligne sur Intradef ouvert à tous à partir de grands modèles.	R / S	Intradef

3.1.9.3 Traitement de la parole

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Transcription de la parole	Vocapia (VoxSigma TRANS)	Vocapia Research (FR)	25 langues disponibles dont langues d'intérêt MINARM, outils d'adaptation disponibles, API REST, OS Linux- Mode SaaS ou	A / S	SIA SF

			on-premise- Déployé dans FCR-M (SIA-rems)		
Identification de la langue parlée	Vocapia (VoxSigma LID)	Vocapia Research (FR)	Brique unique intégrant l'identification de plus de 120 langues, variantes et dialectes (dont langues d'intérêt MINARM), API REST, OS Linux, mode SaaS ou on-premise	E / E	Min Arm
Transcription de la parole	GenIAI - Transcription	Min Arm	Service en ligne sur Intradef ouvert à tous à partir de grands modèles.	R / S	Intradef

3.1.9.4 Océrisation

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Océrisation	GénIAI - Océrisation	Min Arm	Service en ligne sur Intradef ouvert à tous pour l'océrisation à partir de grands modèles.	R / S	Intradef

3.1.9.5 Agent conversationnel et synthèse

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Agent conversationnel	GénIAI – Assistant	Min Arm	Service en ligne sur Intradef ouvert à tous à partir de grands modèles.	R / S	Intradef
Agent conversationnel	GénIAI – Synthèse	Min Arm	Service en ligne sur Intradef ouvert à tous à partir de grands modèles.	R / S	Intradef

3.2 Socle des applications

☆☆☆☆☆
Consulter l'AGORA Tech le plus en amont possible pour l'architecture du SI.
☆☆☆☆☆

3.2.1 Généralités

3.2.1.1 Concepts fondamentaux

Les applications réalisées, aussi bien en interne qu'en externe, au profit du Ministère répondent aux critères principaux suivants :

- **Indépendance technologique** : l'application doit pouvoir s'exécuter indépendamment de son environnement (système d'exploitation virtualisé ou non) et du mode d'accès (client léger, client riche, etc.), en évitant autant que faire se peut tout déploiement spécifique sur le poste client ;

Client léger, la règle / client lourd, l'exception

Lors de la validation des architectures, le recours à un client lourd devra être dûment justifié.

Compatibilité des navigateurs

Les projets doivent être compatibles avec tous les navigateurs recommandés, les autres navigateurs étant susceptibles d'être désactivés sans préavis ou d'entraîner des limitations sur le poste utilisateur (accès ISPT, ...). Pour les fonctionnalités conformes à des normes (notamment HTML, ...), il est recommandé d'éviter de prendre ce qu'un éditeur de navigateur aurait pu ajouter en surcouches d'une norme, quelles que soient les justifications légitimes ou

non, au risque qu'en cas de retrait futur de cette fonctionnalité, cela perturbe le fonctionnement des applicatifs qui y auraient eu recours.

- **Rationalisation des techniques utilisées** : limiter le spectre des compétences des architectes, des développeurs mais aussi des exploitants permet de circonscrire les éventuels surcoûts liés à l'acquisition, puis à la maintenance, de compétences trop dispersées ;
- **Interopérabilité native** : anticiper l'interopérabilité, notamment en facilitant l'accès à la couche métier dans un contexte « SOA²⁷ », permet de diminuer les efforts ultérieurs nécessaires à l'intégration de l'application dans le socle ministériel.

En termes d'architecture :

L'architecture générique d'un système d'information doit répondre à de multiples contraintes (sécurité, maintenabilité, mise à l'échelle, exploitabilité ...). Ceci induit *a minima* un découpage en couches (présentation HTML5, CSS3, moteur exposant des services au travers d'API et stockage).

Afin d'éviter un système d'information monolithique difficilement maintenable au fil du temps, il est recommandé de l'organiser en services (granularité à adapter en fonction des besoins et des performances attendues), de s'appuyer sur les services et les données de références existants (API), d'offrir en retour des services/données à valeur ajoutée susceptible d'intéresser d'autres services sous forme d'API (cf. 3.2.1.3.2 *Stratégie API – corpus documentaire API*.)

Le système d'information doit s'appuyer sur des services mutualisés mis en place sur les réseaux supports : service d'authentification, service de temps, service de nommage...

Afin de fluidifier le processus d'hébergement, les directions d'application doivent faire valider leur architecture (architecture applicative, spécifications techniques, intégration sur le/les réseaux supports, déploiement) par les instances de gouvernance technique (cf. 1.4 *Gestion et gouvernance du CCT*) sur dossier ou en présentation au moment de la revue de conception générale.

À tout moment, sur expression de besoin à soumettre à la sous-direction Guichet, Besoins et Services Numériques, les EADS peuvent être accompagnées par les équipes du Département Accompagnement des Systèmes Métiers dont le bureau Architecture Amont, qui intervient pour évaluer les architectures des solutions mises en œuvre, notamment concernant leur conformité au cadre de cohérence technique et les remédiations éventuelles à prévoir mais aussi sur leur efficience par rapport au besoin métier à couvrir ou enfin, pour conseiller les demandeurs sur l'usage de nouveaux composants dans l'écosystème ministériel.

3.2.1.2 Démarche et principes liés aux solutions en nuage (cloud)

Le Ministère a repensé son architecture d'hébergement afin de se doter des outils nécessaires permettant de répondre à son ambition numérique. Se concentrant en premier lieu sur les environnements Intradef et Internet, il a lancé un chantier de « cloudification » qui vise à transformer ses plateformes techniques d'hébergement de sites et applications en une offre de service d'hébergement standardisée et maîtrisée dans la durée.

Cet investissement est réalisé afin de :

- permettre des mises en service rapides et fiables sur les différents environnements grâce aux apports de la simplification des processus, de l'automatisation et de la standardisation (DevSecOps)
- assurer une continuité de service et une résilience accrues apportées in fine par une redondance locale (deux salles d'un même datacenter) et régionale (entre deux datacenter)
- disposer d'une capacité d'enrichissement des services au fur et à mesure grâce à des plateformes évolutives par conception et aptes à offrir les technologies les plus récentes dans ses prochaines versions (orchestration de conteneurs, capacité GPU pour l'IA, Zero Trust, Data Centric Security ...)

²⁷ *Service Oriented Architecture*, architecture orientée services.

- assurer une sécurité et une maîtrise accrues via la mise en œuvre de mécanismes d'observation de bout en bout et d'audit durant tout le cycle de vie des applications
- disposer de plateformes maîtrisées par le Ministère, conformes aux normes et standards modernes et opérables en autonomie

Cette offre de service cloud s'appuie sur 3 plateformes :

- **PICSEL** : première étape du parcours cloud, la plateforme PICSEL apporte des outils de développement et de tests modernes conformes à l'état de l'art. La mise à disposition de services représentatifs des différents environnements facilite les tests. Le contrôle qualité et le mécanisme de livraison automatisé (CI/CD orientée GitOps) fiabilisent et accélèrent la mise à disposition aux utilisateurs ;
- **C1DR** : partie du cloud destinée à la mise en œuvre rapide et automatisée de sites et d'applications au profit du personnel du Ministère. La plateforme C1DR s'intègre pleinement aux services du socle numérique tout en offrant des garanties de sécurité et de résilience adaptées. Chaque application y dispose de son espace dédié et protégé, mais reste capable d'échanger de manière maîtrisée avec les autres applications ou services (notamment celles encore hébergées sur les plates-formes historiques d'Intradef), y compris ceux hébergés sur Internet ;
- **C1NP** : partie du cloud destinée aux sites et applications exposés sur Internet. Bâtie sur le même modèle et les mêmes standards que C1DR et PICSEL et disposant des mêmes services que ces dernières, cette plateforme est dotée de mécanismes de sécurité complémentaires adaptés à cet environnement plus exposé.

La capacité d'hébergement avec orchestration de conteneurs est ouverte sur PICSEL et est opérationnelle sur C1DR. L'AGORA Tech vérifiera la pertinence technique du recours à ce type de technologie pour les systèmes d'information concernés ainsi que l'acceptabilité des composants utilisés (notamment par examen des dockerfiles, charts HELM et du SBOM) jusqu'à ce que le contrôle qualité sur PICSEL assure automatiquement ces vérifications. Les mécanismes de contrôle d'admission bloqueront l'exécution des conteneurs non conformes dans les environnements de production.

Parallèlement, ces offres d'hébergement seront enrichies de façon à fournir des capacités de CPU haute fréquence et GPU aux systèmes d'information (sous le nom « offre GPU », déjà installée au profit d'Artemis.IA sur le C1DR). En vue de garantir la capacité des Datacenter à répondre aux besoins importants induits par ce type de technologie (énergie et refroidissement notamment), le matériel que le CND met en place répond aux spécifications suivantes :

CPU			
Type processeur	Intel Xeon 6338N – 32 coeurs	AMD EPYC 9554 64 coeurs	AMD EPYC 9334 32 coeurs
Fréquence	2,2 Ghz	3.1 Ghz	2.7 Ghz
Extension aux jeux d'instructions	MMX – SSE – SSE2 – SSE3 – SSE 4.2 – AVX – AVX2 – AVX 512 – FMA3 – F16C	MMX – SSE – SSE2 – SSE3 – SSE 4.2 – AVX – AVX2 – AVX 512 – FMA3 – F16C	MMX – SSE – SSE2 – SSE3 – SSE 4.2 – AVX – AVX2 – AVX 512 – FMA3 – F16C
Usages	Courant	À justifier	IA
	Type : base de données, portail applicatif, application web, etc.	Application monothread ou à processus séquentiels ou Artemis.IA DR	Lié au GPU L40S
Infrastructure	C1DR, ISHM	C1DR	C1DR

GPU		
Type GPU	L40S	H100
Capacité Memoire	48 Go	80 Go
Bande passante	864 Gbit/s	2 Tbit/s
FP64	NA	34 Tflops
FP64 Tensore Core	NA	67 Tflops

FP32	91,6 Tflops	67 Tflops
TF32 Tensor Core	366 Tflops ★	989 Tflops ★
FP16 Tensor Core	733 Tflops ★	1979 Tflops ★
FP8 Tensor Core	1466 Tflops ★	3958 Tflops ★
Usages	Intelligence Artificielle	Artemis.IA DR
★ Avec dispersion structurelle. Sans dispersion, les spécifications sont deux fois moins élevées		

Les niveaux de service de ces nouvelles offres sont identiques aux offres

historiques et sont à dessein adossées aux mêmes technologies, ce qui permet à une application conforme au CCT d'être rapidement et facilement migrable.

Plus précisément, pour être éligible C1NP ou C1DR, une application doit :

- disposer d'une pile logicielle à jour et soutenue en MCO/MCS ;
- disposer de scripts de déploiement Ruche conformes (ceux de C1NP sont identiques à ceux d'Intradef);
- s'adosser à l'authentification MinDefConnect de l'environnement support;
- exporter ses données d'observabilité (journaux d'événements applicatifs, métriques et traces applicatives) dans le service d'observabilité, le raccordement étant réalisé automatiquement au déploiement de l'application ;
- instancier a minima l'API REST d'observabilité (l'instrumentation pourra être enrichie via développement mais c'est laissé à l'appréciation du projet de ses besoins en la matière);
- gérer ses secrets et ses certificats via le service de socle Gestion des secrets sur C1NP et C1DR²⁸ ;
- respecter le format des journaux d'événement : le format attendu par le CALID constitue un prérequis à la mise sous supervision de sécurité du SI ;
- effectuer une préintégration incluant le contrôle qualité sur PICSEL.

Les 3 premiers points sont des exigences de conformité préexistantes, non spécifiques au cloud et rappelées systématiquement aux projets concernés par l'AGORA Tech.

L'export des journaux d'événements applicatifs ne nécessite que la configuration d'un agent et le raccordement à la gestion des secrets se limite le plus souvent à une opération technique simple.

L'implémentation de l'API d'observabilité (cf. 6.2.7.4) requiert quant à elle un petit travail de développement complémentaire, pour partie automatisable en utilisant le fichier OpenAPI de description fourni. En retour, la direction d'application ou de projet (ainsi que l'exploitant) bénéficie d'un suivi fiable de l'état effectif de bon fonctionnement de l'application incluant sa capacité à interagir correctement avec les services socles et autres applications avec lesquels elle est en interaction.

Ces exigences constituent le socle minimum requis pour s'assurer que l'application pourra être hébergée avec le bon niveau de sécurité, de maintenabilité, de disponibilité et de résilience sans obérer les capacités d'exploitation de l'opérateur. En conséquence, elles sont désormais requises pour tout nouveau projet et doivent également être prises en compte dans la feuille de route des systèmes d'information existants.

Règle	Énoncé	Statut	Portée
CCT_R4_1	Il est OBLIGATOIRE que tout système d'information déployé sur les environnements C1NP et C1DR : soit déployé et mis à jour via des playbooks et collections ansible conformes à celles définies dans le cadre du projet Ruche, effectue une préintégration sur PICSEL, s'adosse à la seule authentification MinDefConnect de l'environnement, exporte ses données d'observabilité dans le service correspondant de l'environnement, instancie l'API REST d'observabilité du Ministère, gère ses secrets et les certificats X509 qui peuvent l'être via le service Gestion des secrets du socle, respecte le format des journaux d'événement du CALID	O	C1NP Intradef
CCT_R5_1	Il est RECOMMANDÉ que tout système d'information déployé : soit déployé et mis à jour via des playbooks et collections ansible conformes à	R	Min Arm

²⁸ secrets applicatifs et certificats ;

	celles définies dans le cadre du projet Ruche, effectue une préintégration sur PICSEL, instancie l'API REST d'observabilité du Ministère, soit en capacité de gérer ses secrets et les certificats X509 qui peuvent l'être via un service Gestion des secrets du socle.		
CCT_R6_1	Il est OBLIGATOIRE que tout système d'information déployé: s'adosse au service d'authentification du socle disponible dans l'environnement, soit en capacité d'exporter ses journaux d'évènements applicatifs dans le puits de logs de l'environnement, respecte le format des journaux d'évènement du CALID	O	Min Arm

À noter que sur les environnements classifiés, l'infrastructure Ruche n'est pas disponible à date. Le déploiement nécessitera donc que le projet instancie une machine virtuelle hébergeant un moteur ansible pour utiliser ses playbooks et collections.

Mais pour tirer la quintessence des bénéfices du cloud, notamment en cas de recours à un hébergement en conteneurs orchestrés, une application devra être conçue sous forme de services et respecter dans sa conception un certain nombre de principes, notamment les 12 facteurs (<https://12factor.net/fr>) :

- disposer d'une source de code unique. Ce n'est que lors du déploiement que les paramètres spécifiques à l'environnement sont injectés.
- ses dépendances devront être explicitement déclarées, l'application ne devant pas se reposer sur la présence supposée d'une bibliothèque ou exécutable du système d'exploitation. Les dépendances devront être disponibles dans l'instance MEDUSA de l'environnement cible.
- les éléments de configuration devront être communiqués via les variables d'environnement ou récupérés dans un service (données standards ou secrets, ces derniers étant gérés par GDS).
- toutes les ressources externes (bases de données, caches, messagerie, file de messages) seront accédées via des URL ou équivalent, en utilisant des protocoles sécurisés et les authentifications associées.
- l'assemblage sera réalisé sur PICSEL avant la publication, et non lors de l'exécution, avec la capacité de revenir immédiatement à une version précédente en cas de problème.
- l'application sera conçue sous forme de processus sans état et indépendants, les données persistées devant se trouver dans une ressource externe, typiquement une base de données. Le système de fichier local ou la mémoire ne pourront être utilisés que de manière locale, temporaire et ponctuelle, leur persistance n'étant jamais garantie. Aucun mécanisme de session persistante ne sera mis en œuvre. Un processus doit pouvoir s'exécuter sur des machines physiques différentes à tout moment. De plus, ils ne doivent pas s'exécuter comme des démons mais s'appuyer sur le gestionnaire de processus du système. Enfin, les journaux d'évènements doivent être émis sur le flux de sortie standard, gérer proprement les signaux d'arrêt, les redémarrages et la reprise après plantage.
- les services seront exposés uniquement via une URL et un port, sans présupposer de l'existence d'un service d'exposition tiers (type serveur web).
- les services doivent être considérés comme jetables et disposer d'API interrogeables pour indiquer leur bon fonctionnement (heartbeat, ce qu'apporte l'API d'observabilité, cf. 6.2.7.4) et leur capacité à traiter des requêtes (readiness).
- les éventuels processus d'administration doivent se lancer dans des environnements identiques à ceux des autres processus et faire partie des livraisons de l'application.
- les applications devront disposer de tests automatisés permettant d'en vérifier le bon fonctionnement après une installation ou une mise à jour automatisée ainsi que de la capacité de revenir rapidement à la version précédente en cas d'anomalie (application et base de données, notamment).

La conception de ce type d'application implique en outre que les développements se fassent avec les mêmes briques logicielles et ressources que celles de production et qu'elles disposent d'une couverture de tests suffisante et adaptée (unitaires, fonctionnels, métiers, IHM), exécutés dans un environnement d'intégration continue afin de prémunir au maximum des incidents découverts en production.

3.2.1.3 Transformation numérique

3.2.1.3.1 Agilité

Document	Date	Origine	Type doc	Portée
Guide DGSIC n°15 portant sur l'agilité dans le cadre de la transformation numérique diffusé par note n°209/ARM/DGSIC/DG/NP du 4 mai 2018	4 mai 2018	DGSIC	Guide	Min Arm
<i>Commentaire : dans ce cadre de la transformation numérique, le guide ministériel relatif à l'agilité a vocation à aider les usagers, les collaborateurs métier, les acheteurs et les différentes équipes de projet et de programme à mettre en œuvre une démarche agile. Ce guide propose une articulation autour de 5 thèmes :</i> • l'incubation de services numériques • les méthodes agiles • l'agilité et les aspects marchés • l'agilité et la réalisation technique • la sécurité numérique en démarche agile.				

3.2.1.3.2 Stratégie API – corpus documentaire API

Dans le cadre de sa transformation numérique, le Ministère doit pouvoir bénéficier d'un SI plus modulaire, plus ouvert et aux composants facilement réutilisables. L'enjeu des prochaines années est de mettre en œuvre une stratégie d'« API-sation » cohérente et standardisée à l'échelle du ministère des Armées et s'intégrant pleinement à la démarche interministérielle.

Déployée d'abord sur Intradef et Internet, la mise en œuvre de cette orientation s'appuie sur un corpus documentaire en cours de production devant être cohérent de documents existants ou produits par ailleurs.

Le corpus API est constitué :

- d'un document d'orientation générale : la politique générale relative aux API ;
- d'un ou plusieurs documents relatifs au « management des API » et notamment une directive relative à la gouvernance des API ;
- de documents de normalisation et notamment la directive DGSIC 19, le cadre technique de mise en œuvre des API REST et le guide de conception des API (*cf. §3.2.4*) ;
- de documents techniques relatifs aux composants d'architecture mis en place (passerelle API, plateforme d'exposition et de management (PEM) des API REST dite API Gateway, démarche simplifiée...) au fur et à mesure de la disponibilité des services associés ;

Un site de publication des données mises à disposition par l'intermédiaire de la PEM.

Document	Date	Origine	Type doc	Portée
Politique générale sur les API version 1 diffusée par note n°276/ARM/DGNUM/DG/NP du 24 juillet 2020	24 juillet 2020	DGNUM	Politique	
<i>Commentaire :</i>				
Directive DGNUM n°48 relative à la gouvernance des API au sein du ministère des armées diffusée par note n°276/ARM/DGNUM/DG/NP du 24 juillet 2020	24 juillet 2020	DGNUM	Directive	
<i>Commentaire :</i>				

3.2.1.4 Hébergement mutualisé

L'opérateur de défense exploite, via les CNMO-SI, un socle d'exécution permettant la rationalisation et la mutualisation des ressources techniques, tels que locaux techniques, serveurs, licences, socles applicatifs et déchargeant les directions de projet des problématiques d'acquisition de ces moyens. De plus, l'homogénéité de la plate-forme permet une rationalisation et une maîtrise des compétences à détenir par l'hébergeur.

Cet hébergement mutualisé, en environnement NP maîtrisé/DR zone de confiance comme en environnements classifiés est structuré autour de 3 offres de prestation de service (salle blanche, serveur privé virtuel (VPS), infogérance, selon les réseaux) et, pour chacun, 4 niveaux de services (Bronze, Argent, Or, Platine) (**cf. détails §6.1.1 Références générales sur l'hébergement**).

Une opération d'investissement « hébergement » actuellement en cours vise à faire évoluer ces hébergements et apporte une offre de service cloud standardisée :

- sur Intradef (C1 DR) en remplacement des SHSM DR depuis mi 2024 pour les environnements d'intégration, de pré-production et de production ;
- sur Internet (C1 NP) ;

Partie intégrante de cette offre cloud, la plateforme de développement, d'expérimentation et de qualification PICSEL permet aux centres de développement, aux TMA dotées de comptes Intradef et aux directions de projet de s'assurer de la qualité et de l'intégrabilité de leurs applications sur les deux environnements précédents.

Ces hébergements reprennent les technologies utilisées précédemment, les performances et les services actuellement offerts et vont y apporter progressivement une part croissante d'automatisation. Cette dernière qui s'appuie notamment sur le projet Ruche (technologie ansible) a pour premier bénéfice de réduire les délais de mise à disposition des hébergements pour les systèmes d'information sur système d'exploitation durci et le raccordement à différents services d'infrastructure (DNS, NTP, antivirus, sauvegarde, comptes de service, gestion des licences mais aussi supervision, service d'observabilité). Plusieurs outils assurent une plus grande maîtrise et une plus grande sécurité : aux outils précédemment cités et au durcissement des systèmes d'exploitation installés, s'ajoutent les dépôts de logiciels sécurisés via le projet MEDUSA, le suivi de conformité tout au long de la vie du système d'information via le SI Conformité et un gestionnaire des secrets (mot de passe des comptes applicatifs, certificats) via le projet GDS. De plus, chaque application est installée dans un espace cloisonné (technologie NSX-T) la préservant des attaques latérales en cas de compromission d'une autre application hébergée sur la plateforme.

Des capacités complémentaires telles qu'une extension du stockage de masse (réseau DR, NP) ont également été ajoutées (S-SF pour fin 2026 à date). Une première capacité d'hébergement de conteneurs orchestrés ainsi la possibilité de disposer de capacités de calcul supérieures recourant à des processeurs graphiques (GPU) a été mise en œuvre fin 2024 pour héberger Artemis.IA sur le C1DR (104 GPU H100). Cette capacité est d'ores et déjà disponible.

Cf. 3.2.1.2 pour les prérequis s'imposant aux applications afin qu'elles soient éligibles à cette offre de service cloud et puissent en tirer pleinement parti.

La migration des systèmes d'information vers ces hébergements cloud, appelée chantier « migration vers le cloud » ou « move to cloud », nécessite l'investissement des directions d'application et de projet et de leurs DSI Domaine pour la mener à bien dans les temps impartis²⁹.

Ce chantier de migration est soutenu par les dispositifs mis en place tels que le centre de compétence cloud³⁰, l'appui CND, le support PICSEL et le guichet de financement CND.

²⁹ Les plateformes SHSM DR actuelles doivent arriver en fin de vie vers 2028.

³⁰ Précurseur du futur Centre spécialisé Cloud attendu à l'horizon second semestre 2026.

La plateforme de développement et d'expérimentation PICSEL sera systématiquement utilisée pour valider la conformité et la qualité des adaptations réalisées.

3.2.2 Hébergement d'applications

3.2.2.1 Services Web / Serveur de présentation [HSW]

Document	Date	Origine	Type doc	Portée
Recommandations pour la sécurisation des sites Web cf. 4.5 Sécurisation des COTS	22 avril 2013	ANSSI	Note technique	Toute admin.
Recommandations pour la mise en œuvre d'un site Web : maîtriser les standards de sécurité côté navigateur cf. 4.5 Sécurisation des COTS	28 avril 2021	ANSSI	Note technique	Toute admin.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Serveur de présentation	Apache HTTP Server	Apache Foundation		★ / ★	Min Arm
Serveur de présentation	IIS (inclus dans Windows Server)	Microsoft	Si environnement Microsoft retenu	★ / ★	Min Arm
Serveur de présentation	Tomcat	Apache Software Foundation		★ / ★	Min Arm
Serveur de présentation	NGINX	NGINX (racheté par F5 Networks)	Ce serveur est très largement utilisé sur l'internet.	★ / ★	Min Arm
<i>Commentaire : dans la plupart des cas, un httpd Apache correctement configuré répondra au moins aussi bien et apportera plus de richesse fonctionnelle grâce à ses modules. NGINX sera en revanche bien adapté pour servir des ressources statiques sous forte charge.</i>					
Reverse proxy / Répartiteur de charge	HAProxy	HAProxy Technologies	Solution recommandée pour assurer les fonctions de haute disponibilité, de répartition de charge et de proxy HTTP et TCP,	★ / ★	Min Arm
<i>Commentaire : cf. §Equilibrage de charges</i>					

3.2.2.2 Serveurs d'application et environnements d'exécution

Un serveur d'application est un logiciel offrant un contexte d'exécution pour des composants applicatifs. Le terme est apparu dans le domaine des applications web.

Pour l'environnement d'exécution d'un système d'information, tout projet doit s'assurer que les dépendances ou bibliothèques liées font l'objet d'un suivi en sécurité au travers des dépôts ministériels MEDUSA (et DECOS de façon résiduelle transitoire) ou y sont éligibles (**cf. 8.6 Critères d'éligibilité des produits et solutions**) ou alors font l'objet d'une contractualisation d'un suivi de sécurité et de traitement des obsolescences par la direction d'application.

Règle	Énoncé	Statut	Portée
RT_DEV_03_1	L'usage de bibliothèques adhérentes à des outils de développement propriétaires est fortement DECONSEILLE .	D	Min Arm

Ces recommandations sont valables pour un développement réalisé en interne au Ministère comme pour des développements réalisés par des prestataires externes : le maintien en condition de sécurité de ces

bibliothèques ou composants d'exécution embarqués doit être un critère d'homologation, et, pour des réalisations externalisées, doit faire l'objet d'une exigence auprès de l'industriel.

3.2.2.3 Environnement d'exécution Java

3.2.2.3.1 Composant binaire d'exécution Java (JRE / JDK)

En raison de l'évolution de la politique commerciale de la société ORACLE vers un modèle de licence contraignant et payant sur le composant binaire d'exécution des applications Java, dès la version 9, des orientations ministérielles fortes ont été prises sur ce sujet. Ces orientations ont fait l'objet d'une présentation en CECNUM du 9 avril 2019 et d'une note d'orientations ministérielles.

Les systèmes du ministère doivent systématiquement recourir à une instanciation binaire JRE³¹ de l'OpenJDK comme suit :

- Sur un serveur Linux (Redhat, Centos, Debian et AlmaLinux), l'instanciation binaire JRE d'OpenJDK fournie par la distribution ;
- Sur un serveur Windows, l'instanciation binaire JRE d'OpenJDK fournie par Eclipse Temurin.

Pour les cas où un support serait nécessaire :

- Sur un serveur Linux, utiliser une distribution RedHat qui apportera ce support ;
- Sur un serveur Windows, utiliser une instanciation binaire JRE OpenJDK non Oracle apportant ce support (Azul, Microsoft, RedHat ...).

Seules les versions LTS de JRE d'OpenJDK soutenues peuvent être utilisées (actuellement 8, 11, 17 et 21, les nouveaux projets devant systématiquement viser les versions 21 et ultérieures).

Dans les situations où le JRE Oracle ne pourrait pas être remplacé, la direction de projet, après obtention d'une dérogation, devra :

- Selon la situation, demander au fournisseur du système d'information adhérent de mettre en place une feuille de route de migration vers un JRE conforme aux orientations ministérielles ou de faire réaliser la migration de son système d'information pour le rendre conforme ;
- Dans le cas où le JRE serait imposé par une application d'un éditeur elle-même soumise à licence, obtenir de ce dernier une attestation écrite certifiant que le JRE peut être utilisé sans licence complémentaire et dans le cadre d'un environnement virtualisé.
- Financer et faire mettre en œuvre une infrastructure matérielle pour l'hébergement des composants serveurs utilisant le JRE Oracle.
- Financer les licences Oracle correspondant à cette infrastructure, ainsi que leur renouvellement **à condition que cela n'implique pas la souscription d'une licence Oracle Java SE Universal Subscription.**

Document	Date	Origine	Type doc	Portée
Orientations ministérielles suite à l'évolution de la politique de la société Oracle relative au composant JAVA , diffusées par note n°301 /ARM/DGNUM/DG/NP du 25 juillet 2019	25 juillet 2019	DGNUM	Note	Min Arm
<i>Commentaire : cette note définit les modalités d'application des orientations relatives au composant Java suite à l'évolution de la société ORACLE. (cf. supra)</i>				
Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows (cf. §4.5 Sécurisation des COTS)		ANSSI	Note technique	Toute admin.

Composant binaire JAVA

³¹ Le JRE est le composant nécessaire à l'exécution d'applications Java compilées, contrairement au JDK qui y ajoute des outils de développement qui n'ont pas leur place en environnement de production.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Environnement java serveur	Oracle JRE ou Oracle OpenJDK	Oracle	Lorsqu'aucun autre JRE ne peut être utilisé. Le recours à cette solution implique systématiquement un hébergement sur machine physique dédiée dès lors qu'il n'existe pas de licence permettant une utilisation en environnement virtualisé restreinte aux seules ressources utilisées par l'application concernée (donc n'incluant pas la souscription d'une licence Oracle Java SE Universal Subscription)	★ / ★	Min Arm
Environnement java serveur	OpenJDK	Eclipse Adoptium	Toutes les distributions certifiées partagent le même code source et l'intégralité des fonctionnalités nécessaires à la certification Java. Elles se distinguent potentiellement par des compléments et par une offre de service du distributeur. Statut en lien avec l'OS utilisé	★ / ★	Min Arm
<i>Commentaire: sous Linux, utiliser l'instanciation binaire JRE de l'OpenJDK 8, 11, 17 ou 21 fournie par la distribution. Si un support est nécessaire, utiliser la distribution Linux RedHat ; sous Windows, utiliser Eclipse Temurin ou une autre JRE non Oracle si un support est nécessaire.</i>					
Environnement Java serveur	Jakarta Enterprise Edition	Fondation Eclipse	Cf. section suivante sur les serveurs d'application Java et la pile logicielle pour les versions.	★ / ★	Min Arm

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.2.2.3.2 Serveurs d'application Java

Sur Intradef, les serveurs d'application et d'EJB mentionnés ci-dessous sont tous sous statut Assujetti : il est demandé aux directions d'application de se rapprocher de la gouvernance technique (cf. 1.4 Gestion et gouvernance du CCT).

L'architecture recommandée au Ministère privilégie le développement avec les framework Spring, Spring Boot ou Quarkus plutôt que Jakarta EE (cf. infra) tant pour la productivité et la performance qu'ils apportent que pour la qualité de leur documentation.

La technologie Jakarta EE (anciennement Java EE) se décline version complète, avec le profil « Jakarta EE Platform », ou bien en versions allégées avec soit : le profil « Jakarta EE Core Profile » qui offre un runtime réduit par rapport au profil complet, ou bien le profil « Jakarta EE Web Profile » qui est adapté aux sites WEB.

Une initiative complémentaire, mieux adaptée à une architecture micro-services que Jakarta EE, a conduit à spécifier le « MicroProfile » (actuellement en version 6.0) qui intègre le profil « Jakarta EE Core Profile » plus quelques API java, non présentes dans Jakarta EE, mais pertinentes pour des micro-services (par exemple pour gérer la tolérance ou panne, ou interroger l'état de santé d'un micro-service). Du fait de sa complexité et des coûts potentiellement induits en exploitation, une architecture micro-services doit être réservée à des cas d'usages pertinents et il est conseillé de consulter préalablement l'AGORA Tech.

La complexité de l'édition Entreprise de Java a longtemps été causée par la multiplicité des modèles de composants et des conteneurs d'exécution spécifiques à chacun (composants Servlet, JSF, EJB session, EJB Entité, etc...) qui rendait le code peu portable et nécessitait une mécanique d'exécution complexe et donc moins performante et fiable qu'une architecture à base de classes Java standard (nommée POJO). C'est pourquoi les composants EJB ont été fortement décriés et ne sont pas recommandés au Ministère. Conçu pour offrir une alternative, le Framework Spring qui a largement fait ses preuves depuis utilise

un mécanisme dit « d'injection de dépendances » qui a finalement été implémenté dans Jakarta EE, sous le nom de « Contexts and Dependency Injection (CDI) ».

En résumé, l'emploi de Jakarta EE doit être vérifié par l'AGORA Tech afin d'éviter l'emploi d'un serveur d'application supportant cette spécification autant que possible. Il est recommandé une architecture plus simple basée sur un simple serveur de servlet comme Tomcat qui saura répondre au besoin dans la plupart des cas tout en allégeant les charges de développement, de maintien en condition opérationnelle et d'exploitation.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Serveurs d'application	Tomcat	Fondation Apache		★ / ★	Min Arm
<i>Commentaire : Tomcat est suffisant pour supporter Jakarta EE Web Profile. C'est l'option à privilégier pour les nouveaux développements avec Spring et Spring Boot Framework.</i>					
Serveurs d'application et d'EJB	TomEE	Fondation Apache	Serveur d'application pour Jakarta EE	★ / ★	Intradef Internet
Serveurs d'application et d'EJB	Enterprise Application Platform JBOSS EAP	RedHat	Serveur d'application JEE	★ / ★	Intradef Internet
<i>Commentaire : ces deux serveurs ont un statut « Assujetti » car Jakarta EE est globalement assujetti. Cela dit parmi tous les autres serveurs certifiés Jakarta EE (par exemple Glassfish, Payara ou Wildfly), TomEE est la solution à privilégier si un support n'est pas nécessaire (avec une installation sur AlmaLinux par exemple) et JBoss EAP est à privilégier si un support est souhaité (avec l'OS RHEL du même éditeur RedHat). Dans les deux cas, le micro-profil est disponible. Les autres solutions sont déconseillées pour réduire le nombre de solutions à maîtriser en exploitation.</i>					
Serveurs d'application et d'EJB	Glassfish	Eclipse Foundation	Serveur d'application JEE8 en production, centralisé.	I / N	Min Arm
Serveurs d'application et d'EJB	Payara Server	Payara Services Ltd	Serveur d'application JEE	I / N	Min Arm
Serveurs d'application et d'EJB	WildFly	RedHat	Serveur d'application JEE. Attention, seule la dernière version mise à disposition par l'éditeur est tolérée.	★ / ★	Intradef Internet SIA S-SF SIA FrOps
<i>Commentaire : le cycle de vie de cette solution est particulièrement court (une nouvelle version majeure tous les 3 mois), ce qui va imposer a minima au projet une charge de MCO/MCS conséquente afin de la maintenir à jour et dans des versions supportées par leurs communautés ou éditeurs respectifs</i>					
Serveurs d'application	Jetty	Fondation Eclipse	Serveur embarqué pour applications légères à réserver aux travaux de développement.	★ / ★	Internet intradef

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

Les dépendances complémentaires (jar) non présentes dans les dépôts de développement sur MEDUSA sont soumises à demande d'autorisation préalable et devront satisfaire les critères décrits en 8.6.

À noter que les déploiements d'applications Java à destination d'un hébergement en machine virtuelle doivent se faire en production par livraison d'archive war (ou ear pour les cas justifiés) : ce mode de livraison garantit la maîtrise de l'exploitant sur le serveur d'application et lui permet par exemple de procéder si besoin et de façon autonome à l'application d'une mise à jour de sécurité sans devoir attendre la mise à disposition d'une nouvelle version de l'application entière. En conséquence, la réalisation de « fat jar » ou même d'application serveur lancée sous forme de « jar » embarquant un serveur est à réserver aux seuls travaux de développement ou en déploiement en conteneur.

3.2.2.3.3 Environnement d'exécution PHP

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Environnement PHP	PHP	PHP Group		★ / ★	Min Arm
Environnement PHP	PHP-FPM	PHP Group	Pour des sites en PHP devant subir des charges importantes (inclus avec PHP)	R / S	Min Arm
<i>Commentaire : en s'appuyant sur le cadre technique de développement PHP, tout nouveau développement voulant utiliser un Framework PHP doit utiliser une version de PHP récente et maintenue.</i>					

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

Les modules complémentaires non présents dans les dépôts de développement sur MEDUSA sont soumis à demande d'autorisation préalable et devront satisfaire les critères décrits en 8.6.

3.2.2.3.4 Environnement d'exécution .Net

.Net est, à l'instar de Jakarta EE pour le langage Java, la plateforme associée au langage C# de Microsoft.

Dans un environnement Windows, il n'est pas nécessaire de disposer d'un serveur d'application pour héberger un programme, qui s'exécute alors comme un service Windows. Il est néanmoins possible d'utiliser IIS (Internet Information Service). Le recours à cet environnement d'exécution sur un serveur doit toutefois n'être envisagé que lorsque des spécificités ou effets recherchés ne sont pas atteignables à l'aide des environnements Java, JavaScript ou PHP et qu'une capacité de MCS et de MCO est durablement disponible.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
.NET	.NET	Microsoft		★ / ★	Min Arm
.NET	.NET Core	Microsoft		★ / ★	Min Arm

★ / ★ pour les recommandations sur les versions voir le détail en

annexe **8.2.1 Pile logicielle : liste des produits**

3.2.2.3.5 Environnement d'exécution JavaScript

Dans le cadre de développement « backend » le recours à node.js est nécessaire. Il offre une alternative au développement d'un backend Java ou PHP et permet de réaliser un SI entièrement en Javascript. Il est cependant nécessaire que les bibliothèques et dépendances Javascript satisfassent aux critères décrits en 8.6 Critères d'éligibilité des produits et solutions et puissent être maintenues, suivies en configuration de sécurité. De plus, Javascript est une technologie foisonnante offrant souvent, parmi ceux qui sont éligibles, plusieurs frameworks ou bibliothèques différentes pour répondre à un même besoin : afin de garantir la capacité du Ministère à en garantir sa maîtrise et sa capacité à assurer le MCO des SI qui les utilisent, seul un nombre limité d'entre elles pourra être recommandé (cf. 7.3.5 Développement HTML5-Javascript-CSS). Les directions d'application peuvent se rapprocher de la gouvernance technique (cf. 1.4 Gestion et gouvernance du CCT) pour exprimer et faire valider leurs besoins.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Environnement JS	Node.js	OpenJS foundation	Restreint aux versions paires soutenues [LTS]	★ / ★	Min Arm

3.2.2.3.6 Environnement d'exécution Python

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Environnement Python	Python	Python Software Foundation	Auparavant, Python était restreint au domaine de la science des données, à l'emploi d'outils d'administration, aux usages scientifiques (IST) ou	★ / ★	Min Arm

			comme dépendance d'un autre logiciel sur étagère. La disponibilité de MEDUSA permet dorénavant d'utiliser cette technologie dans un cadre plus industrialisé pour réaliser des applications métier.		
Framework Web	Django	Django Software Foundation(License BSD)	Ce framework est recommandé pour réaliser une application WEB avec le langage Python.	★ / ★	Min Arm
Framework API	Flask	Open source(License BSD)	Ce framework est recommandé pour réaliser des API avec le langage Python. Il est facile à apprendre et adapté à des API simples.	★ / ★	Min Arm
Framework API	FastAPI	Open source(License MIT)	Ce framework est recommandé pour réaliser des API avec le langage Python avec un besoin accru de performances.	R / N	Min Arm

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

L'environnement d'exécution Python est déjà requis par un certain nombre d'outils, notamment d'administration (dont Ansible). Son emploi est par ailleurs adéquat dans le domaine de la science des données.

En environnement d'exécution, les bibliothèques et dépendances devront satisfaire les critères décrits en **8.6 Critères d'éligibilité des produits et solutions**.

3.2.2.3.7 Environnement d'exécution R

Le langage et l'environnement d'exécution R sont autorisés pour un emploi dans les domaines des statistiques et de la science des données à condition de disposer d'une ressource de MCO pérenne.

Le recours à des bibliothèques complémentaires non présentes dans les dépôts de développement MEDUSA est soumis à demande d'autorisation préalable ; elles devront satisfaire les critères décrits en 8.6 Critères d'éligibilité des produits et solutions.

3.2.2.3.8 Environnement d'exécution Rust

Rust est un langage de programmation compilé multi-paradigme qui met l'accent sur la performance, la sûreté des types et la concurrence. Il assure la sécurité mémoire, au prix d'une complexité supérieure par rapport à d'autres langages.

Le langage et l'environnement d'exécution Rust sont autorisés pour des applications en `web assembly`, préférentiellement au développement d'un client lourd.

Le recours à des `crates` (nom Rust d'une `library`) complémentaires non présentes actuellement dans les dépôts de développement MEDUSA est soumis à demande d'autorisation préalable ; elles devront satisfaire les critères décrits en 8.6 Critères d'éligibilité des produits et solutions.

3.2.2.3.9 Environnement d'exécution Ruby

Déjà présent dans les distributions Linux en vigueur au ministère, l'environnement d'exécution Ruby est requis par un certain nombre d'outils, notamment d'administration (dont Puppet). Bien que cette technologie ne pose pas de problème technique en soi, son emploi pour des solutions dépassant ce cadre n'était pas envisagé pour un certain nombre de raisons (absence de compétences internes pour assurer un maintien dans la durée, nécessité de disposer de dépôts pour les dépendances `gem` nécessaires alors que celles requises pour d'autres technologies recommandées ne sont pas encore disponibles, pas d'avantage différenciant du langage par rapport à d'autres déjà utilisés et recommandés ...). Les progrès

réalisés sur le socle vont permettre à termes de disposer, avec MEDUSA, d'une solution outillée de dépôts pour des développements réalisés en Ruby sur l'environnement Cloud PICSEL.

Le langage Ruby est interprété par des moteurs comme MRI (Matz's Ruby Interpreter). Depuis la version 2.6, MRI intègre MJIT qui est un compilateur juste à temps, c'est-à-dire qu'il compile dynamiquement certaines parties de code Ruby en code machine pendant l'exécution, ce qui permet d'améliorer les performances. En production, pour développer des API, des micro-services ou des application WEB, il est nécessaire d'utiliser un serveur d'application tel que PUMA.

Pour répondre aux quelques cas d'usage requérant impérativement l'emploi de Ruby sans faire peser de contraintes difficilement gérables sur l'exploitation de ces systèmes en production, il est désormais autorisé d'utiliser cette technologie en l'encapsulant via JRuby dans Java ce qui permet de profiter de la prise en charge de ce dernière par les infrastructures actuelles.

JRuby traduit le code Ruby en bytecode Java. Cela permet de bénéficier de performances accrues par rapport à MRI, mais également d'étendre les possibilités de Ruby en utilisant des librairies Java.

Dans le cas d'une application WEB, un framework tel que RAILS (Ruby on Rails) est également utile pour réduire les coûts et délais de développement et est compatible de JRuby.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Environnement Ruby	Ruby	Ruby Licence		A / N	Min Arm
Framework Web	Ruby on Rails	Licence MIT		★ / ★	Min Arm
Traducteur Ruby en Java	JRuby	Licence GNU	Nécessaire pour traduire en bytecode Java une application Ruby pour la Production	A / N	Min Arm
<i>Commentaire : le langage Ruby et RAILS sont marginaux dans le domaine des SIAG. C'est pourquoi, il n'est pas recommandé ici. Néanmoins, dès lors que la pré-intégration sur PICSEL permet de réaliser un BUILD avec JRuby et une production ensuite dans un environnement d'exécution Java, cette option de développement devient autorisée. Par « assujetti », on entend vérifier si un autre langage que Ruby peut être utilisé pour le SI Cible concerné et si Ruby est confirmé, que JRuby sera effectivement employé. Comme certains GEMs Ruby sont incompatibles avec JRuby, il est de la responsabilité de la DSI Domaine et de l'équipe projet de vérifier que de tels GEM ne seront pas utilisés pendant le développement.</i>					

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.2.2.3.10 Environnement propriétaire

Certains outils propriétaires (Windev, Webdev, FileMaker, ...) proposent en intégré et à titre de "meilleure productivité" des bibliothèques propriétaires ou nécessitent des environnements d'exécution, ou des serveurs d'application propriétaires : ces bibliothèques ou composants ne font pas l'objet d'un suivi en sécurité tout le temps de vie de l'outil, et peuvent donc générer des failles de sécurité sur les systèmes construits à partir de ces bibliothèques ou composants d'environnement d'exécution, et, au-delà faire peser un risque de sécurité systémique sur l'écosystème dans lequel ils sont déployés (Intredef, Internet C1NP ...). Ils entraînent de surcroît une dépendance à leurs éditeurs commerciaux sur les plans financier, technologique et fonctionnel allant à l'encontre de la recherche de souveraineté du Ministère en la matière. Ces outils sont donc désormais interdits et ne sont plus référencés au CCT. Pour tous les projets déjà existants, une montée de versions régulière est exigée jusqu'à la transition rapide vers un nouveau système d'information ou une nouvelle technologie.

Voir aussi §7.3.7 **Développement à l'aide d'outils « low-code » ou « no-code »**

3.2.3 Portail des applications métier

3.2.3.1 Moteur de workflow [WFL]

Cf. 3.2.4.6 Gestion de processus et de règles métiers

3.2.3.2 Process robotisés (RPA)

La RPA (Robotic Process Automation) consiste en l'automatisation de tâches, répliquant l'activité humaine. Elle permet d'effectuer des actions, identifiées comme simples et répétitives, plus rapidement et plus précisément que l'homme. Cette technologie s'articule autour de 3 grandes fonctions :

- le studio, qui permet de designer les robots,
- le robot, qui joue le rôle d'assistant, autonome ou interactif (stand-alone),
- l'« orchestrator », plateforme serveur, qui permet de piloter l'ensemble des robots.

Cette technologie doit être perçue comme **une capacité temporaire** d'automatisation de dispositifs anciens pour en améliorer le fonctionnement en attente de leur refonte basée sur des technologies plus récentes, robustes et maintenables, conformes à la politique ministérielle.

Document	Date	Origine	Type doc	Portée
Cadre des activités de Robotic Process Automation(RPA) du MINARM , diffusé par lettre n°197/ARM/DGNUM/DG/NP du 19 mai 2020	19 mai 2020	DGNUM	Cadre	Min Arm
<i>Commentaire : ce cadre précise les bonnes pratiques à respecter au sein du Ministère des armées dans la mise en place d'un RPA.</i>				
Directive 74 encadrant l'emploi des solutions d'automatisation robotisées des processus au Ministère	14 février 2025	DGNUM	Directive	Min Arm
<i>Commentaire : .</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
RPA (Process robotisés)	UiPath	UiPath	Brique ministérielle	★ / ★	Intradef
<i>Commentaire : cette technologie devant être considérée comme un moyen temporaire d'amélioration du fonctionnement de dispositifs anciens, son usage est assujéti à une demande de dérogation justifiant d'une rejoindte vers un environnement non dérogoaire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n'exonère pas du respect des règles de l'Intradef et, de facto, n'autorise pas son emploi au travers d'ISPT.</i>					

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.2.3.3 Chatbot

Un chatbot, étymologiquement dialogue (chat) automatisé (bot) est un agent conversationnel permettant d'apporter des réponses à des demandes d'un utilisateur de façon automatisée.

On distingue :

- des chatbots simples reposant sur un dialogue basé sur des mots-clés dans un cadre préétabli et des bases de données préexistantes ;

- des chatbots plus complexes qui apprennent et s'améliorent en continu et reposent sur des mécanismes d'apprentissage automatique (machine learning).

Un outil de génération de chatbots a été élaboré avec la fabrique numérique. Il permet de créer facilement, via un playbook ansible, un service de chatbot pour une application basée sur des briques open source dont RASA constitue le cœur.

Pour GenIAI, cf. **3.1.11 Agent conversationnel et synthèse**.

3.2.3.4 Moteur de règles

Pas de référence identifiée à ce jour.

3.2.3.5 Services de gestion des rôles et profils

Pas de référence identifiée à ce jour.

3.2.3.6 Services de gestion des règles d'accès

Pas de référence identifiée à ce jour.

3.2.3.7 Portail des applications mobiles sur Internet – Milistore

Document	Date	Origine	Type doc	Portée
Directive d'emploi MILISTORE version 1 diffusée par la note n°506418/ARM/EMAT/PNI/NP du 06/07/2022	2022	EMAT	Directive	Min Arm
<i>Commentaire : Milistore est la solution de l'Armée de Terre pour accéder depuis un téléphone personnel (BYOD) au catalogue d'applications ou de ressources ministérielles, et au besoin, interministérielles telles que TCHAP. Elle est accessible uniquement aux utilisateurs authentifiés par FranceConnect ou MindefConnect : les utilisateurs accéderont alors à un catalogue filtré selon leur profil, l'accès aux applications de Milistore pourra ainsi être restreint en fonction du rôle, de l'organisation ou de l'emplacement géographique de l'utilisateur. La transposition de MILISTORE au sein du ministère des armées a fait l'objet d'une étude portée par la DGNUM au premier semestre 2020. Il en est ressorti une proposition de refonte de l'architecture technique. Aucune suite n'a pour autant été donnée à ce stade. Cette étude ne remet toutefois pas en cause la feuille de route de MILISTORE de l'Armée de Terre.</i>				

3.2.4 Échanges entre applications

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°19 édition 2 portant sur les échanges inter-applicatifs du ministère de la Défense diffusée par lettre n°72/ARM/DGNUM/DG/NP du 8 mars 2019	8 mars 2019	DGNUM	Directive	Min Arm
<i>Commentaire : sans écarter définitivement les technologies plus anciennes (SOAP...), ne serait-ce qu'au titre du legacy ou de certains besoins spécifiques, la directive préconise des architectures orientées services autour du modèle REST, en déclinaison de la stratégie API de l'état et du ministère et en conformité avec le RGI V2. Cette directive est complétée d'un cadre technique de mise en œuvre API (cf. 3.2.4.4).</i>				
Référentiel général d'interopérabilité [RGI] cf. 2.2.3 Les référentiels interministériels				
<i>Commentaire : règles applicables aux échanges inter-applicatifs du système d'information du ministère des armées.</i>				

3.2.4.1 Généralités

Toute application s'inscrit aujourd'hui dans un contexte plus large que son seul périmètre fonctionnel. Les échanges inter-applicatifs permettent l'économie d'une saisie multiple, dispendieuse en temps et en personnel et source d'erreurs.

La mise en relation des applications s'effectue dans le cadre d'une approche Service Oriented Architecture (SOA). Dans cette approche, les besoins opérationnels sont définis en services et sont satisfaits par des systèmes et des moyens répartis qui s'exécutent et coopèrent dans un environnement réseau.

Cette approche impose une phase préalable d'analyse indépendante de l'implémentation, pour faire émerger une liste de services à partir des besoins opérationnels. Ces services sous-tendent la couche applicative et apportent modularité et une évolutivité accrue à l'application tout en la découplant des autres applications et services avec lesquels elle interagit.

L'économie est alors double, puisque s'ajoute à l'économie des données déjà évoquée une économie d'écriture des fonctions (services) déjà réalisées au travers d'autres SI. Il faut donc inciter à la réutilisation des composants et des services distants en facilitant les échanges de flux inter-applicatifs.

L'approche orientée service impose une grande rigueur de conception aux fournisseurs de services afin de garantir le découplage entre spécification du service et implémentation du service, ceci afin de ne pas compromettre l'évolutivité de l'implémentation. Ceci disqualifie notamment toute API générée automatiquement et calquée sur le schéma de données sous-jacent, ainsi que les outils et frameworks présentant cette approche.

Il en va de même des approches Capture Data Change (CDC) qui visent à propager des modifications apportées au niveau de la base de données vers des systèmes d'information tiers : en effet, un changement en base de données est avant tout la conséquence d'un événement métier qui implique (ou impliquera dans une évolution ultérieure) d'autres actions métier (une notification vers un utilisateur ou un autre service ou application par exemple). La modification en base de données ne pouvant refléter l'événement métier dans sa globalité, **la technologie CDC doit être réservée aux seuls besoins purement techniques** (réplication par exemple).

3.2.4.2 Cas des échanges Intradef avec l'extérieur

Dans le cas de systèmes d'information présents à la fois sur l'internet maîtrisé (C1NP) et Intradef, la sécurité des échanges de données sensibles (données à caractère personnel de personnel militaire, données sur l'état de santé, ...) conduit à promouvoir l'architecture suivante :

- un frontal accessible hors zone de confiance Intradef ne doit afficher que des données éphémères récupérées d'Intradef via des appels REST au travers de la passerelle API ;
- un stockage hors zone de confiance Intradef doit se limiter aux données non sensibles nécessaires à la résilience et à la performance du service ; les autres données sensibles étant stockées sur l'Intradef.

Les échanges de données non protégés entre le frontal hébergé sur C1NP et un système d'information hébergé sur l'Intradef se font de manière synchrone via le protocole d'échanges API REST au travers de la passerelle API v2.1. La passerelle API v2.1 offre deux canaux d'échanges pour faire transiter, soit des données structurées de type json et limitées à 500Ko soit des fichiers (pdf, images, json, csv à ce jour) et limités à 8Mo non compressés.

Il est recommandé, à chaque fois que possible, de privilégier des échanges de petite taille plus fréquents, permettant de bien meilleures performances, une plus grande robustesse des processus et une moindre complexité des traitements à mettre en œuvre.

Les échanges de fichiers non protégés entre le frontal et la partie traitement Intradef se font de manière synchrone au travers de la passerelle API v2.1 pour les fichiers de moins de 8Mo.

Afin de couvrir les cas d'usage légitimes nécessitant des transferts de données supérieurs à 8 Mo, le Ministère étudie actuellement une solution offrant des capacités suffisamment dimensionnées opérées à travers des protocoles adaptés tant en termes d'architecture que de sécurité.

Le décommissionnement d'Acheron, frappé d'obsolescence, interviendra en mars 2026. Aucun nouveau système d'information n'est autorisé à l'utiliser. Les derniers systèmes encore dépendants d'Acheron finalisent leur d'adaptation pour utiliser les passerelles API disponibles. Cette adaptation implique notamment la modification du code applicatif afin de remplacer l'utilisation du protocole WebDav par des appels API REST.

3.2.4.3 Échanges inter-systèmes

Ce chapitre fait référence aux prescriptions en matière d'échanges entre systèmes d'information de différentes administrations, entre domaines de sécurité ou bien encore pour des échanges massifs.

Profils d'interopérabilité recommandés par le Référentiel Général d'Interopérabilité (RGI)

Le RGI a introduit la notion de profils d'interopérabilité : un profil d'interopérabilité est un ensemble limité de standards, un groupe de spécifications à utiliser dans un contexte opérationnel, un usage déterminé. Dans sa version V2, le RGI a identifié 9 profils d'interopérabilité dont notamment 2 profils génériques dans des contextes d'échanges applicatifs :

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
Profil « Fondations État Plateforme »	Il constitue le socle de base en matière d'interopérabilité pour tous les échanges de type entre administrations, et entre les administrations et le citoyen ou l'entreprise. Il concerne plus particulièrement les échanges entre : les usagers, les « fournisseurs de services », les « fournisseurs de données », et la brique mutualisée « FranceConnect » tels que définis dans la stratégie État Plateforme. Le style d'architecture préconisé dans ce cadre est l'architecture REST (cf. description détaillée du profil RGI V2).	R	Toute admin.
Profil « Web Service SOAP »	Ce profil répond aux mêmes types d'échanges que le précédent mais dans le cadre d'une architecture de services SOAP. Sa mise en œuvre est plus complexe, mais peut être nécessaire notamment dans le cadre d'échanges nécessitant une gestion transactionnelle (par exemple : transaction longue). Ce format de Web Service est toutefois en forte perte de vitesse au profit des architectures REST.(cf. description détaillée du profil RGI V2)	A	Min Arm

D'autres profils plus particuliers sont par ailleurs recommandés dans le cadre des échanges du monde de la protection sociale (INTEROPS), de l'archivage ou de la géomatique.

Pour en savoir plus : https://www.numerique.gouv.fr/documents/7/Referentiel_General_Interoperabilite_V2.pdf

Échanges inter-applicatifs entre administrations

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
PRESTO V2	« Protocole d'échanges standards ouverts ». Il pose les bases d'un protocole d'échange de messages informatiques entre applications pour servir les besoins de l'administration électronique. À n'utiliser que pour les cas d'utilisation en cours.	D	Toute administration
<i>Commentaire : PRESTO est un protocole d'échange de fichiers défini par l'administration française pour ses besoins propres. Ce protocole n'est plus entretenu et est classé « fin de vie » par le RGI. Une évolution ouverte vers REST de ce standard permettrait de le repasser à « recommandé ». Seule la version 2.0 peut encore être conservée pour les cas d'utilisation en cours (les versions antérieures font appel à des protocoles de sécurité dépassés)</i>			

Échanges d'informations liées aux processus d'authentification et d'autorisation

Cf. §4.6.1 Sécurisation des accès

Moniteur de transfert

Un moniteur de transfert permet le transport sécurisé de grands volumes d'information entre sites distants.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Moniteur de transfert	CFT	Axway	Assujetti aux cas d'usage ne pouvant être couverts par une brique recommandée (ex : Camel, Talend) pour les échanges en interministériel	A / S	Intradef

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.2.4.4 Architectures SOA - Orchestration et logique métier

L'objectif d'une architecture SOA est d'exposer les fonctionnalités métier mutualisables sous forme de services accessibles à toutes les applications qui peuvent en nécessiter le traitement sous-jacent.

L'architecture SOA offre les moyens de mettre en phase rapidement et régulièrement le système informatique et l'ensemble des règles métiers utilisées, au rythme des évolutions imposées par les travaux d'urbanisation du système d'information (changements techniques et fonctionnels). En conséquence, elle offre un moyen efficace d'aligner le système informatique sur l'expression du besoin fonctionnel en liaison avec les faisabilités et les contraintes techniques.

Le RGI V2 définit un profil d'interopérabilité pour ces architectures (cf. ci-dessus **§3.2.4.2 Échanges inter-systèmes**).

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Enterprise Service Bus	ServiceMix	Apache	Assujetti au seul périmètre des applications s'appuyant sur le framework du SIA (échanges avec Fuse).	I / N	Min Arm
<i>Commentaire : il est recommandé de directement recourir aux versions à jour des bibliothèques historiquement embarquées dans ServiceMix (KARAF, CAMEL, CXF, ...), ce projet ne présentant aucune activité depuis plusieurs années (https://servicemix.apache.org/community/board-reports.html cf. Community Health https://servicemix.apache.org/community/releases-schedule.html)</i>					
Enterprise Service Bus	Open Studio for ESB	Talend	Ce produit n'est plus supporté par une communauté et n'est plus mis à jour. Les projets ayant identifié des alternatives à Open Studio for ESB anciennement fourni par Talend sont invités à se rapprocher de l'AGORA Tech.	I / N	Min Arm
Framework Intégration	Spring	Licence Apache 2.0	Spring Framework. Il met en œuvre les principes et patterns d'intégration d'entreprise, appelés EIP.	★ / -	Min Arm
Framework Intégration	Camel	Licence Apache 2.0	Il ne fait pas partie de Spring Framework mais il est recommandé de s'en servir avec Spring Boot afin de bénéficier de l'infrastructure Spring (Conteneurs IoC, gestion de transactions, sécurité, ...). Il met en œuvre les principes et patterns d'intégration d'entreprise, appelés EIP.	★ / -	Min Arm

Enterprise Service Bus	WSO2 Enterprise Integrator (WSO2 EI) WSO2 Micro Integrator (WSO2 MI)	Licence Apache 2.0	Les solutions d'intégration WSO2 (EI et MI) sont assujetties à des cas complexes d'intégration ou à l'utilisation de connecteurs de médiation non nativement disponibles dans les frameworks Spring et Camel, par exemple des connecteurs ERP. WSO2 Micro Integrator est à privilégier pour une exécution dans des conteneurs. Voir aussi : PEM	★ / N	Intradef
------------------------	---	--------------------	---	-------	----------

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.2.4.5 Architectures API – REST – PEM

3.2.4.5.1 Architecture API REST - PEM

Le cadre de réalisation de l'État Plateforme constitue un modèle d'ouverture des SI à travers les interfaces de type API et du style d'architecture REST. Un profil d'interopérabilité « État plateforme » est d'ailleurs défini dans le RGI V2 (cf. ci-dessus §3.2.4.2 *Échanges inter-systèmes*)

Document	Date	Origine	Type doc	Portée
Cadre technique de mise en œuvre des API au sein du ministère des armées version 1.1 publié le 27 janvier 2025	Janvier 2025	DGNUM	Guide	Min Arm
<i>Commentaire : ce cadre décline et précise la directive DGNUM n°19 sur les échanges inter-applicatifs pour des API de type REST. Il décrit les règles à respecter lors de la conception, la sécurisation et le développement des API et précise les bonnes pratiques à observer dans leur réalisation. .</i>				

Afin de permettre la gestion et la gouvernance des API, le ministère met en place une « plateforme d'exposition et de médiation » (PEM)³². Ce type de composant :

- fournit aux développeurs une plateforme permettant d'enregistrer et documenter les API (côté fournisseur d'API), de consulter la documentation des API, de les tester (côté consommateur d'API), de gérer des droits d'accès à ces API (fonctions de gestion) et d'obtenir des statistiques et indicateurs d'usage (fonctions de pilotage) ;
- est médiateur des échanges entre des applications fournissant des services sous forme d'API et des applications les consommant. Le composant s'assure des autorisations d'accès à l'API, de la conformité des appels d'API en fonction des descriptions et droits d'accès enregistrés. Enfin, il procède au routage de l'API vers le serveur ad hoc et protège le service exposé en assurant la mise en œuvre de politiques de sécurité (quotas d'appels, droits d'accès et d'usage...).

3.2.4.5.2 « Route API »

Le standard d'échanges API RESTful³³ s'impose dans les orientations interministérielles comme moyen de communication entre les systèmes d'information de zones de confiance différentes pour consommer ou exposer des ressources conformément à la politique générale sur les API.

³² Composant dénommé passerelle API ou API Gateway dans la littérature informatique. Mais le terme « passerelle » est réservé au sein du Ministère aux dispositifs permettant des échanges de données entre réseaux de confiance ou de confidentialité différente.

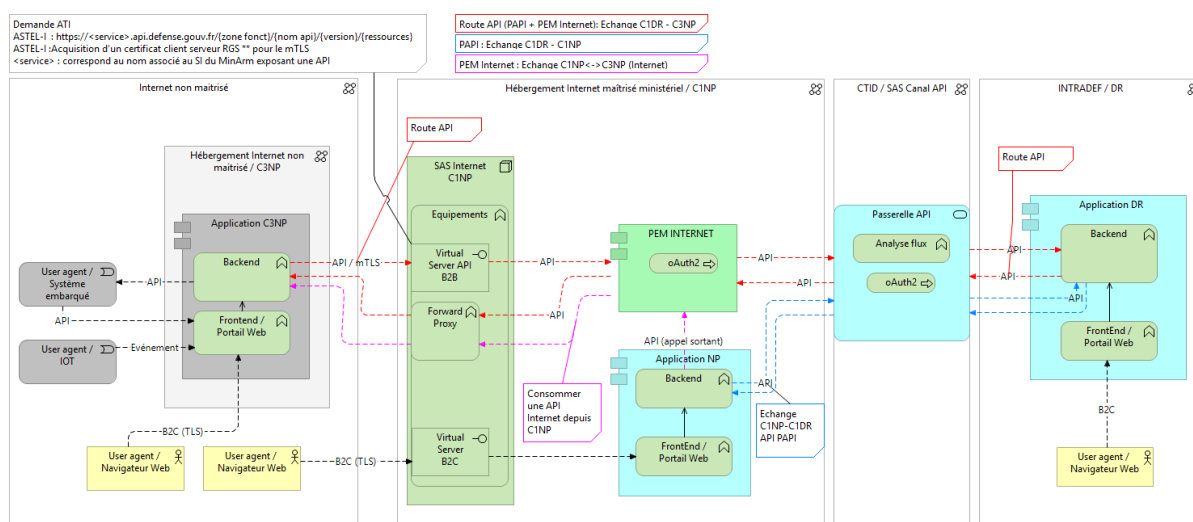
³³ Une API REST est une API qui respecte les principes de conception de REST, ou le style architectural de transfert d'état de représentation. Pour cette raison, les API REST sont parfois appelées API RESTful.

Ces échanges inter-applicatifs entre l'Intradef et l'internet maîtrisé et non maîtrisé adressent les trois zones de confiance suivantes :

- l'Intradef (hébergement historique SHSM DR et C1DR y compris entre elles);
- l'internet maîtrisé (C1NP), c'est-à-dire une zone exposée à l'Internet **mais fortement sécurisée et infogérée par le CND** ;
- l'internet non maîtrisé (public).

Le Ministère instancie cette technologie de PEM pour construire progressivement l'offre de service **Route API** permettant des échanges applicatifs entre systèmes d'information du Ministère et de ses partenaires (B2B³⁴) à l'intérieur de chaque zone et entre chaque zone:

- **une PEM Intradef** pour mettre en relation via API RESTful des SI exclusivement à l'Intradef (donc jusqu'à niveau DR) ;
- **une passerelle API [P.API]** pour mettre en relation via API RESTful des SI Internet maîtrisé avec des SI Intradef. La P.API repose sur les sous-systèmes suivants :
 - une PEM P.API côté Intradef exposant des API NP pour des SI Internet maîtrisé ;
 - une PEM P.API côté internet maîtrisé exposant des API uniquement NP pour des SI Intradef ;
 - des moyens de sécurité entre les deux PEM (SAS API) permettant de sécuriser les échanges via API pour faire transiter des données structurées et des fichiers.
- **une PEM Internet** pour mettre en relation via API RESTful des SI Internet non maîtrisé avec des SI Internet maîtrisé.



Route API

Chacune de ces instances PEM suit des règles communes (standard de description, homologation de l'API, contrat d'usage entre consommateurs et fournisseurs de ressources) du cadre de mise en œuvre des API (cf. paragraphe précédent 3.2.4.4.1), ainsi que certaines spécificités liées à leur positionnement et leur rôle par exemple (une API susceptible de véhiculer des données de type DR ne pourra se trouver exposée que sur la PEM Intradef).

Pour l'internet maîtrisé (C1NP), le cadre d'hébergement très strict et très contraint induit par cet environnement particulièrement exposé impose aux applications des exigences complémentaires en

³⁴ B2B Business to Business désigne une relation d'entreprise qui fournit des biens ou des services à d'autres entreprises.

matière de sécurité, et notamment pour celles dont le rendu est effectué côté client³⁵ (applications SPA³⁶, mobiles ...) :

Dans le cas d'échanges B2C³⁷, le client (qui n'est, par nature, pas maîtrisable par le ministère) ne peut pas faire appel directement aux API exposées par la passerelle API³⁸ : il doit s'adresser à un serveur front web ou un SI rebond (pattern BFF³⁹) sur l'internet maîtrisé qui, seul, est ensuite autorisé à relayer les appels API via une PEM après contrôle, d'éventuels enrichissements et transformation de la base de l'URL⁴⁰. La consommation d'API par ce type de client depuis la PEM Internet n'est pas autorisée pour des raisons de sécurité (la protection du secret pour des appels API n'étant alors pas assurée) ;

- Les échanges API de type B2B entre l'internet maîtrisé et l'internet non maîtrisé doivent se faire exclusivement au travers de la PEM Internet. Des équipements de sécurité complémentaires portés par les services d'infrastructure augmenteront d'autres règles de sécurité ;
- Aucune API exposée par la passerelle API ne peut être consommée directement par un serveur hébergé en dehors de l'internet maîtrisé. Pour consommer une API de la passerelle API depuis l'internet non maîtrisé, la mise en oeuvre d'un serveur hébergé sur C1NP reste obligatoire jusqu'à l'ouverture de la Route API ;
- Par dérogation et dans l'attente de la disponibilité de la PEM Internet, les serveurs hébergés sur l'internet maîtrisé peuvent actuellement consommer directement des API externes (internet public), après configuration des éléments de sécurité (les équipements de sécurité en sortie de plateforme permettant de suivre et de sécuriser les échanges) ;
- Jusqu'à ce que la route API soit disponible, les serveurs hébergés sur Intradef ne peuvent pas consommer directement des API externes (internet public) via la passerelle API mais doivent obligatoirement passer par l'intermédiaire d'un serveur hébergé sur l'internet maîtrisé.

Il est rappelé ici, que dans le cadre des échanges B2C, l'authentification de l'utilisateur doit reposer sur MinDefConnect Internet, exclusivement selon l'« authorization code flow » et que la gestion des droits incombe à l'application (via son serveur hébergé sur C1NP).

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Exposition et médiation d'API [PEM]	PEM Intradef Instance ministérielle mutualisée basée sur le produit WSO2	Min Arm WSO2	pour les échanges inter-applicatifs internes à Intradef via API	R / S	Intradef
Exposition et médiation d'API [PEM]	PEM pour la passerelle API Instances ministérielles mutualisées basée sur le produit WSO2	Min Arm WSO2	Pour les échanges inter-applicatifs de l'Intradef avec la passerelle API Pour les échanges inter-applicatifs de l'internet maîtrisé (C1NP) avec la passerelle API	R / S	Intradef / Internet maîtrisé
Commentaire : le Ministère a mis en place des instances de PEM mutualisées en interne à l'Intradef (PEM Intradef) qui seront complétées S2 2026 par d'autres pour gérer la Route API entre internet et Intradef (composants de la passerelle API Intradef-Internet).					

³⁵ Client Side Render (CSR) par opposition au rendu côté serveur ou Server Side Render (SSR) qui ne s'impose donc pas.

³⁶ Une application monopage ou SPA (« Single-page application » en anglais) est une implémentation d'application web qui ne charge qu'un seul document web, puis met à jour le contenu du corps de ce document via des API JavaScript.

³⁷ B2C Business to Consumer désigne une relation d'entreprise qui fournit des biens ou des services à des particuliers.

³⁸ Les identifiants et mots de passe nécessaires – aucune API n'étant publique – pour consommer une API de la passerelle API (ou d'une PEM), sont uniquement attribués à des serveurs et donc aucunement à des clients.

³⁹ Le pattern Backends For Frontends (BFF) consiste à créer des services « passerelles » adaptés aux besoins spécifiques de chaque client. Ces clients peuvent être des applications frontend ou des interfaces externes.

⁴⁰ Cette transformation, peu contraignante, a pour avantage de ne pas divulguer à l'extérieur l'API telle qu'elle est exposée par la passerelle API en entrée d'Intradef.

Exposition et médiation d'API [PEM]	PEM Internet Instance ministérielle mutualisée basée sur le produit WSO2	Min Arm WSO2	Pour les échanges inter-applicatifs entre Internet maîtrisé (C1NP) et Internet non maîtrisé (internet public)	E / -	Internet maîtrisé / Internet non maîtrisé
Exposition et médiation d'API [PEM]	PEM pour environnement de développement et de validation	Min Arm WSO2		R / S	PICSEL
Enterprise Service Bus	WSO2 API Manager version	WSO2	Si nécessité d'instances dédiées	A / N	Min Arm
<i>Commentaire : lorsque le recours à une PEM dédiée est nécessaire en lieu et place des instances mutualisées ministérielles évoquées ci-dessus, et sous réserve de le justifier en dérogation, l'usage de WSO2 est recommandé, mais son support est à la charge de la direction d'application.</i>					

3.2.4.6 Extraction et transformation (ETL) [TRF]

Un outil d'ETL⁴¹ permet l'extraction, la transformation et le chargement des données depuis des sources, et des cibles diverses par l'intermédiaire de connecteurs : base de données, fichiers, ERP, etc.

Les principaux domaines d'emploi sont l'alimentation ou l'échange entre systèmes opérationnels et l'extraction des données de systèmes opérationnels à l'usage des systèmes dédiés au décisionnel.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
ETL	Talend Open Studio for data integration	QLIK Talend	Abandonné par l'éditeur. Il n'y a donc désormais ni support, ni évolution de prévu.	I / N	Intradef
ETL	Talend Plateform Data integration	Talend	Il est recommandé d'utiliser cette solution si une équipe de 3 développeurs ou plus est dédiée à la création de tâches.	R / S	Intradef
ETL	Talend Plateform Data Management	Talend	Il est recommandé d'utiliser cette solution pour les projets devant implémenter la gestion de qualité des données et si une équipe de 3 développeurs ou plus est dédiée à la création de tâches.	R / S	Intradef
<i>Commentaire : la mise en production des tâches doit se faire par livraison de jar, invoqués par un ordonnanceur type cron et il appartient au projet de se doter dans tous les cas d'une solution de supervision fonctionnelle des échanges.</i>					
ETL	Data Integrator	Oracle	Ce composant n'est pas recommandé.	A / N	Min Arm
ETL	SSIS	Microsoft	Assujetti à l'alimentation d'un infocentre en technologie Microsoft.	A / S	Min Arm
ETL	Logstash	Elastic (Open source)		★ / ★	Min Arm
ETL	Fluentd	CNCF	Assujetti à l'usage de Prometheus	★ / N	Min Arm
ETL	HERMOD	Min Arm	Socle ministériel Basé sur Qlik Talend	E / -	Intradef

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

Pour les solutions liées aux données volumineuses, cf. §3.2.6.5.

⁴¹ Extract, Transform, Load : extraction, transformation, chargement.

3.2.4.7 Gestion de processus et de règles métiers

La gestion des processus (« Business Process Management » ou BPM) consiste à modéliser les processus métier. L'objectif de cette démarche est d'aboutir à une meilleure vue globale de l'ensemble des processus métier et de leurs interactions afin d'être en mesure de les optimiser et, si possible, de les automatiser au maximum à l'aide d'applications métier.

Dans un deuxième temps, permettre de modifier simplement ces processus en fonction des besoins passe par l'établissement de règles métier.

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
BPMN V2	Le Business Process Model and Notation (BPMN) est un modèle de processus métier et une notation graphique standardisée par l'Object Management Group (OMG).	R	Min Arm

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
BPMN	Bonita	BonitaSoft	Déconseillé à cause de son usage Low-Code et rythme de mise à jour élevé, AngularJS spécifique maintenu dans la solution malgré son abandon par la communauté. Attention, interdit sur les C1.	D / -	Min Arm
BPMN	Camunda	Camunda	Assujetti à n'utiliser que lorsque les solutions mentionnées dans le commentaire ci-dessous ne peuvent être mises en oeuvre	A / N	Tout intranet
BPMN	Flowable	Flowable	Assujetti à n'utiliser que lorsque les solutions mentionnées dans le commentaire ci-dessous ne peuvent être mises en oeuvre	A / E	Intradef
<i>Commentaire : pour la majorité des cas développés en Java, le recours à un framework de l'écosystème Spring (WebFlow, StateMachine) peut amplement suffire. Pour les cas plus complexes, l'embarquement d'un framework Camunda peut s'avérer une alternative opportune. Concernant des développements en PHP, il est préconisé le recours à Symfony-Workflow ou Laravel-Workflow.</i>					

Les outils de modélisation BPM, de processus, de workflow et d'architecture sont évoqués au chapitre **7.2.1 Modélisation métier**.

3.2.4.8 Annuaire des applications et services [ANA]

Pas de référence identifiée à ce jour.

3.2.5 Données et contenu

3.2.5.1 Formats de données

Document	Date	Origine	Type doc	Portée
Référentiel Général d'Interopérabilité [RGI]				
<i>Commentaire : (cf. 2.2.3 Les référentiels interministériels). Le RGI, dans sa partie syntaxique effectue les recommandations en matière de formats élémentaires et de formats composites. Il s'applique au ministère.</i>				

L'attention des directions d'application est attirée sur l'encodage des caractères et des formats audio et vidéo.

3.2.5.1.1 Encodage des caractères

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
UTF-8	Norme de codage des caractères sur plusieurs octets. Il est recommandé d'utiliser UTF-8 pour l'encodage des caractères, notamment pour éviter un affichage « exotique » des caractères accentués. L'utilisation de tout autre encodage doit être justifiée par un besoin technique.	R	Min Arm
<i>Commentaire : UTF-8 peut être mis en œuvre sur Windows 10 à partir de la version 1903, là où ce n'est pas possible utiliser par défaut CP65001.</i>			
UTF-16, UTF-32	L'usage de UTF-16 ou UTF-32 est réservé à l'encodage des caractères pour les besoins d'échange démonstrativement plus efficaces en UTF-16 ou UTF-32, ou si l'usage d'UTF-8 est interdit par une disposition normative.	A	
ASCII	Codage historique de caractères sur 7 bits.	D	
ISO-8859-x	Normes de codage de caractères sur 8 bits. Ces normes très répandues sont entrées en obsolescence. L'usage pour les nouveaux systèmes est très fortement déconseillé et nécessite l'obtention d'une dérogation.	D	
Autres encodages	Notamment les jeux de caractères Windows-1252 ou CP1252, CP437, CP850	I	

Voir aussi les règles de nommage des fichiers enfermant des contenus numériques (*cf. chapitre 8.4.1*).

3.2.5.1.2 Formats audio et vidéo

Les données vidéo et audio sont susceptibles d'avoir un impact significatif sur les réseaux du ministère. Par ailleurs, certains formats ne sont pas ou plus pris en charge nativement par les navigateurs. Il convient donc d'utiliser des formats tenant compte de ces contraintes. À noter que Firefox apporte en général une meilleure prise en charge des formats audio et vidéo via HTML5 que Edge. Il peut notamment lire les formats conteneur WAV (des fichiers de type « .wave » ou « .wav ») contenant de l'audio non compressé en MIC (ou PCM) de 8 ou 16 bits par échantillon.

Les formats audio Vorbis, audio Opus, vidéo Theora et vidéo VP8 sont des formats de compression audio/vidéo ouverts, que l'on peut utiliser sans les restrictions des brevets. Ils peuvent être lus dans Firefox s'ils sont intégrés dans des formats conteneurs, tels qu'Ogg (des fichiers de type .ogg, .oga, .ogv, .ogx, .spx ou .opus) et WebM (des fichiers de type .webm).

Firefox prend aussi en charge la lecture des fichiers FLAC (*Free Lossless Audio Codec*, des fichiers de type .flac) et la lecture des fichiers MP3 (des fichiers de type .mp3). Enfin, Firefox prend en charge les vidéos WebM/VP9 sur les systèmes qui ne prennent pas en charge MP4/H.264.

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
WebM	Conteneur vidéo	R	Min Arm
MKV	Conteneur vidéo	R	Min Arm
VP8	Codec vidéo pour le conteneur WebM	R	Min Arm
VP9	Codec vidéo pour le conteneur WebM	R	Min Arm
H264	Codec vidéo pour le conteneur MKV	R	Min Arm
H265	Codec vidéo pour le conteneur MKV	R	Min Arm
<i>Commentaire : la résolution doit être limitée à 720P au maximum, le fullHD ne s'impose pas sur les réseaux MinArm dont les capacités doivent être préservées.</i>			
Vorbis	Codec audio	R	Min Arm
Opus	Codec audio	R	Min Arm

3.2.5.1.3 Outils de conversion de format

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Conversion de format	PANDOC	John MacFarlane	Outil de conversion de documents multi-format utilisable par les applications en tant que de besoin préférentiellement à	R / S	Min Arm

			l'installation niveau serveur de LibreOffice ou MS-Office.		
--	--	--	--	--	--

3.2.5.2 Gestion des accès aux données

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
CSV ⁴²	Format de transfert de données en volume, dit « à plat » ou texte. Recommandé uniquement pour les échanges entre application et utilisateur (cf. RGI v2). Pour tous les autres cas, utiliser XML.	A	Min Arm
XML ⁴³	Format et échange de documents structurés, standard du W3C. C'est un méta langage permettant de définir des langages (format de données) notamment en vue de faciliter l'échange automatisé de contenus complexes entre système informatiques hétérogènes. Il peut cependant être un peu « verbeux » pour des volumétries importantes.	R	Min Arm
XSD	Format de description d'un document XML, standard du W3C. Il est recommandé d'utiliser la syntaxe XSD (XML schema definition) pour décrire le contenu et la structure d'un document XML et en vérifier la validité.	R	Min Arm
XSLT et XPath	Il est recommandé d'utiliser les langages XSLT pour formater et transformer des documents XML et XPath pour localiser une portion d'un document XML et ainsi requêter sur un document.	R	Min Arm
JSON	Usage recommandé pour les protocoles optimisés méga-données (Big Data) et pour les échanges de données en architecture Web.	R	Min Arm
YAML	Usage recommandé pour les fichiers de configuration d'Infrastructure as Code notamment	R	Min Arm

3.2.5.3 Gestionnaire des données [HBD]

Il existe principalement deux grandes familles de moteurs de base de données ayant chacune des limites :

- Les bases de données relationnelles où les données, en général fortement typées et très structurées sont reliées entre elles par une algèbre relationnelle, permettant d'en vérifier rapidement l'intégrité : on leur délègue communément la responsabilité de vérifier le respect des règles métier exprimables sous forme de contraintes et de relations (cas des ERP, ou du reporting pour le décisionnel en mode OLAP). C'est aussi une couche d'abstraction prenant en charge les contraintes du stockage physique de la donnée et de la concurrence des accès. Cependant, elles sont limitées en performance (capacité, temps de réponse) par le respect du modèle d'E. F. Codd et l'implémentation de transactions aux propriétés ACID (Atomicité, Cohérence, Isolation, Durabilité).
- Les moteurs NoSQL qui s'affranchissent d'une partie de ces contraintes. Il y a deux grands cas d'utilisation du NoSQL. Le premier, permet de développer rapidement des applications simples utilisant des données faiblement structurées par essence (et non par manque de conception). Le second, permet de satisfaire des exigences essentiellement techniques, tout particulièrement sur les aspects volumétrie, passage à l'échelle (temps de réponse constant malgré la charge et la volumétrie) et résilience (disponibilité malgré les pannes). Ces moteurs ne sont pas adaptés lorsque des relations existent dans le modèle de données et doivent être exploitées (problèmes de performance voire d'intégrité notamment).

Une grille de choix permet d'orienter le choix sur la solution à employer en fonction du cas d'usage.

⁴² Comma separated values. Valeurs séparées par des virgules (ou des points-virgules lorsque les données contiennent elles-mêmes des virgules).

⁴³ Extensible markup language. Langage de balisage extensible.

	Catégories	Type de base	Cas d'usages	Bases de données
Données structurées	Transactions ACID	Relationnelle	Applications traditionnelles, ERP, Gestion de la relation client	
	Embarqué	Base de données embarquée	Base de données embarquée coté client	 SQLite
	Analytique	OLAP	Analyse de données, informatique décisionnelle	À définir ultérieurement

Données Semi-structurées	Objets imbriqués (XML, JSON)	Documentaire	Gestion de contenus, catalogues, profils utilisateurs	  
	Stockage client NoSQL	Stockage local	Gestion du mode déconnecté, réplication entre client et serveur (CouchDB)	 PouchDB
	Dictionnaire	Clé-Valeur	Applications web à trafic élevé, Applications E-Commerce	 Redis
	Cache	En mémoire	Mise en cache, gestion de sessions	 

	Clé-Valeur en 2D	Colonne Large	Maintenance des équipements, gestion de flottes, optimisation de routes	 Cassandra
	Audit, intégrité	Registre immuable	Systèmes d'enregistrements, supply chain, transactions financières	À définir ultérieurement
	IA, moteur de recherche d'images, de texte, Big Data	Vectorielle	Stockage de vecteurs, moteur de recherche, LLM	 Pgvector
	Séries Temporelles	Séries Temporelles	Applications de l'internet des objets, DevOps, Télémétrie	 influxdb
	Localisation & Entités Géo	Géospatial	Référencement géographique, localisation	 

				 
	Relations Entité	Graphe	Détection de fraudes, réseaux sociaux, moteurs de recommandations	  ArangoDB
Données non structurées	Recherche en texte intégral	Recherche de texte	Recherche texte brut	  

	Objets binaires	Blob	Stockage de données non structurées documents, images et vidéos	 S3
--	-----------------	------	---	--

3.2.5.3.1 Les SGBDR

☆☆☆☆☆

Les choix de SGBDR non recommandés doivent systématiquement faire l'objet d'une demande de dérogation dûment justifiée auprès de la gouvernance technique (§1.9.2 Processus de saisine pour validation d'architecture ou dérogation au CCT)

☆☆☆☆☆

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°5 relative aux systèmes de gestion de bases de données relationnelles publiée au Bulletin Officiel des Armées	7 avril 2008	DGSIC	Directive	Min Arm
<i>Commentaire :</i>				
Note DGSIC relative au choix du SGBDR dans les systèmes d'information diffusée sous timbre n°468/ARM/DGSIC/DG/NP du 24 novembre 2017	24 novembre 2017	DGSIC	Note	Min Arm
<i>Commentaire : cette note soumet tout choix de SGBDR non recommandé dans le CCT à une demande systématique de dérogation auprès de la gouvernance technique (cf. 1.9.2 Processus de saisine pour validation d'architecture ou dérogation au CCT).</i>				

NOTA : Résumé de la politique en matière de SGBDR

- Pour tout nouveau projet ou évolution majeure, et compte-tenu des incertitudes actuelles autour de MariaDB, le choix de la solution PostgreSQL doit être privilégié jusqu'à clarification de la situation ; toute autre alternative de solution doit être soumise pour dérogation à l'AGORA Tech.
- À défaut, SQL Server à dûment justifier si aucune solution opensource recommandée ne peut convenir.
- À défaut, SGBD Oracle, si aucune solution opensource recommandée et si SQL server ne peut être utilisé, à strictement justifier : dans ce cas, sur Intradef, aujourd'hui, ou, à défaut disposer d'une licence spécifique pour environnement virtualisé, ou, à défaut, mettre en place un hébergement sur machine physique dédiée.
- Une solution alternative à la solution de haute disponibilité est en cours de recherche. Les projets ayant identifié une solution possible pourront la partager avec l'AGORA Tech.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
SGBD	PostgreSQL	The PostgreSQL Global Development Group	Solution à privilégier pour les nouveaux développements et les migrations. Elle dispose de beaucoup de fonctionnalités et permet des architectures offrant haute disponibilité et scalabilité.	★ / ★	Min Arm

Commentaire : le recours à un framework ou outil d'exposition REST tel POSTGREST est déconseillé, et nécessite une dérogation dûment justifiée en AGORA Tech. L'exposition d'API de type CRUD n'est pas conforme à la stratégie API du ministère au sens où elle induit un couplage fort entre le schéma de la base de données et l'API générée.

SGBD	MariaDB	MariaDB Foundation	Ce SGBD, « fork » de MySQL depuis 2012, est la solution référencée par le socle interministériel de logiciels libres (SILL). Solution à privilégier par rapport à MySQL à fonctionnalités équivalentes.	★ / ★	Min Arm
SGBD	Galera Cluster	Galeracluster	Solution de clusterisation multi-maître synchrone pour MariaDB	R / S	Min Arm
<i>Commentaire : depuis la version 10.1, MariaDB inclut Galera Cluster</i>					
SGBD	MySQL	Oracle		★ / ★	Min Arm Hors Intrasan
SGBD	MySQL	Oracle		I / -	Intrasan
SGBD	SQL Server	Microsoft	Assujetti : Utilisation à justifier dans le cas ou aucune solution opensource recommandée au CCT ne peut convenir.	★ / ★	Min Arm
<i>Commentaire : MS SQL Server est en assujetti, toutes versions et licences confondues (Express, Standard ou Enterprise)</i>					
SGBD	Oracle Database	Oracle	Assujetti : Utilisation à dûment justifier, si impossibilité de recourir ni à un SGBDR recommandé ni, à défaut, à SQL Server. Standard Edition One	★ / ★	Min Arm
SGBD	SQLite	SQLite	Librairie en langage C qui implémente un moteur de BD relationnelle. Elle est petite, rapide et performante. C'est une solution pertinente en mode « embedded » c'est-à-dire embarquée dans une application sans avoir besoin de l'installation et du management d'un SGBDR. Cette librairie est utilisable sur un nombre très importants d'OS et de langages de programmation. Son usage principal est sur terminaux mobiles (smartphone et tablette). À ne pas utiliser toutefois dans le cadre d'un service cloud, notamment conteneurisé.	A / -	Intredef, Intrasan
SGBD	PostGIS	PostGIS	Surcouche PostgreSQL permettant d'en faire un SGBD spatial ou de cartographie	★ / ★	Min Arm
SGBD	pgAdmin4	PostgreSQL Global Development Group	Assujetti aux usages non couverts par DBeaver	A / -	Intredef

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.2.5.3.2 Les SGBD sous la dénomination NoSQL

Les cas d'utilisation sont volontairement incomplets. Les caractéristiques trop techniques sont exclues. Ne sont présentés que les critères les plus sélectifs qui peuvent être déterminés durant une analyse de besoins.

Les bases de données NOSQL mentionnées ci-dessous sont quasi-toutes sous statut Assujetti : il est demandé aux directions d'application de se rapprocher de la gouvernance technique (cf. 1.4 Gestion et gouvernance du CCT) aux fins de capitalisation sur les usages de ces solutions.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Base de données NOSQL	Elasticsearch	Elastic	Moteur de recherche et d'analyse sans état éventuellement distribué basé sur Apache Lucene. Pour des recherches rapides avec évaluation de pertinence y compris full text. Traditionnellement utilisé avec Logstash pour l'ingestion des données et Kibana pour la visualisation.	★ / ★	Min Arm
<i>Commentaire : (★) : Les produits Elastic offrent de nouveau une licence libre AGPLv3 offrant des garanties compatibles des usages du Ministère. Il existe aussi une version entreprise payante. Compte tenu du cycle de vie, il n'y a pas véritablement de versions LTS mais plutôt deux versions majeures maintenues en parallèle, une stable recommandée et une dite « current » ayant un cycle rapide de mises à jour techniques et fonctionnelles. La seconde remplace la première - qui n'est alors plus maintenue et devient interdite - lorsqu'une nouvelle version majeure est ajoutée.</i>					
Base de données NOSQL	Elasticsearch module machine learning	Elastic		A / S	Intradef
Base de données NOSQL	Opensearch	AWS	Alternative à Elasticsearch/Kibana apportant les fonctionnalités de sécurité (authentification) et alerting	★ / ★	Min Arm
Base de données NOSQL	Prometheus	CNCF	Système open-source de monitoring et d'alerting qui collecte et stocke les métriques sous forme de time-series. Équivalent d'Elasticsearch pour les métriques. Est assujéti à des contextes ne permettant pas l'usage du SI Observabilité, et à l'emploi du mode push-based	★ / ★	Min Arm
<i>Commentaire : La solution à privilégier est la pile Elastic, portée par les C1NP et C1DR et recommandée sur les autres contextes. Sur Intradef la solution legacy de supervision est Shinken. Promoteus accepté hors du cas d'usage Observabilité (réseau isolé, ou réseaux où le service Observabilité n'est pas disponible), ou la pile Elastic n'est pas utilisable, et si le mode push-based est mis en place.</i>					
Base de données NOSQL	Cassandra	Apache ou distribution commerciale DataStax	Base de données orientée colonnes avec un ressenti proche d'un SGBDR. Grands volumes de données et des besoins de bases distribuées hautement disponibles et décentralisées, sous réserve de prendre en compte les impacts réseau	★ / ★	Min Arm
Base de données NOSQL	DocumentDB	Linux Foundation sous licence MIT	Base de données compatible avec MongoDB construite comme extension de Postgresql permettant également d'exécuter des requêtes complexes (recherche <i>full text</i> , géospatiales ou vectorielles par exemple). FerretDB qui permet d'utiliser Postgres plutôt que MongoDB de façon transparente utilise DocumentDB.	R / S	Min Arm
Base de données NOSQL	MongoDB	MongoDB (licence Server Side Public	Indexes et requêtes simples sur un modèle changeant et des données peu structurées (textes plus ou	★ / ★	Min Arm

		Licence non Open Source ou commerciale)	moins longs, données saisies avec peu de contraintes) ; applications de type blog à envisager après étude des fonctionnalités JSON de PostgreSQL		
Base de données NOSQL	Memcached	Danga Interactive	Hautes performances d'écriture et de restitution (accès inférieur à la ms) dans une base clef/chaîne de caractère en mémoire.	★ / ★	Min Arm
Base de données NOSQL	Redis	Redis Labs	Hautes performances d'écriture et de restitution (accès inférieur à la ms) dans une base clef/valeur en mémoire plus riche fonctionnellement et éventuellement persistée.	★ / ★	Min Arm
Base de données NOSQL	Neo4j	Neo4j	Pure base de données graphe. Traitement rapide d'ensemble de nombreuses données fortement en relation les unes avec les autres en grand nombre (ou dont le nombre de relations est variable). Neo4J doit être utilisé en version entreprise, la version communautaire n'ayant pas de gestion de droits. Si cette gestion de droit est nécessaire, utiliser ArangoDB. Attention, interdit sur les C1.	★ / ★	Min Arm
Base de données NOSQL	ArangoDB	ArangoDB	BD multi-modèles (graphes, documents, clés-valeurs) open-source sous licence Apache. Son langage de requêtes AQL déclaratif permet des combinaisons de différents patterns d'accès dans une même requête.	★ / ★	ArangoDB
Base de données NOSQL	SOLR	Fondation Apache	Pour implémenter des moteurs de recherche évolués.	★ / ★	Min Arm
Base de données NOSQL	PouchDB	Fondation Apache(Apache License 2.0)	PouchDB est principalement utilisé pour le stockage de données côté client, ce qui signifie qu'il peut être utilisé pour stocker des données localement dans un navigateur web ou dans un environnement Node.js. PouchDB est conçu pour la réplication bidirectionnelle de données entre la base de données locale et une base de données distante. Cela permet de maintenir les données synchronisées entre différentes instances de l'application, même en cas de déconnexion.	★ / ★	Min Arm
Base de données NOSQL	CouchDB	Fondation Apache(Apache License 2.0)	CouchDB offre une réplication multi-master, ce qui signifie que plusieurs bases de données CouchDB peuvent se synchroniser entre elles de manière bidirectionnelle. Cela permet une	★ / ★	Min Arm

			grande tolérance aux pannes et la distribution des données sur plusieurs serveurs.		
Base de données NOSQL	Clickhouse	Yandex		A / -	IntredefSIA S-SF SIA FrOPS
Base de données orientée vecteurs	PgVector	Base de données NOSQL	Outils de recherche de similarités vectorielles pour PostgreSQL	A / S	Min Arm

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.2.5.3.3 Les SGBD en mémoire

Les bases de données en mémoire (in-memory) visent à accélérer l'accès aux données en les stockant directement en RAM (mémoire temporaire rapide) plutôt que sur les disques durs (mémoire persistante lente).

3.2.5.3.4 Les agents de messages

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Agent de messages	RabbitMQ	Pivotal Software	Logiciel libre sous licence Mozilla Public License permettant l'échange de message. À utiliser pour découpler des systèmes d'information notamment.	★ / ★	Min Arm
Agent de messages	ActiveMQ	Apache Software Foundation	Logiciel libre sous licence Apache 2.0 de serveur de message multi protocoles (AMQP, MQTT, STOMP)	★ / ★	Min Arm
Agent de messages	Redis	Redis Labs	Base clef/valeur en mémoire qui peut aussi être utilisée comme agent de messages.	★ / ★	Min Arm
Agent de messages	Kafka	c	Logiciel libre sous licence Apache 2.0 pour la mise en place de pipeline de messages, la supervision temps réel, l'IoT quand RabbitMQ n'est pas suffisant, qu'il y a un besoin de persistance ou qu'un cluster est nécessaire	★ / ★	Min Arm
Agent de messages	Nats	Agent de messages	Assujetti à un besoin d'agent de messages pour conteneur	A / -	C1DR

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.2.5.4 Gestion des données de référence (MDM) – management de la qualité des données (DQM)

Gestion des données de référence (MDM : master data management)

La gestion des données de référence ou gestion des données maîtres (GDR, plus connue sous le vocable anglais de master data management ou MDM) est une branche des technologies de l'information qui définit un ensemble de concepts et de processus visant à définir, stocker, maintenir, distribuer et imposer une vue complète, fiable et à jour des données de référence au sein d'un système d'information.

Management de la qualité des données (DQM : data quality management)

La mise en qualité des données est un prérequis indispensable à l'optimisation et à l'efficacité des métiers. La maîtrise de la qualité des données est donc un enjeu important au sein des organisations. Il

s'agit de fournir des données correctes, complètes, à jour et cohérentes aux acteurs métier. Une réponse technologique à cette problématique est apportée par la brique de management de la qualité des données.

La mise en œuvre de ces deux concepts au sein du Ministère se concrétise au travers des travaux menés par le CND sur la gouvernance de la qualité des données et la mise en place d'une plateforme technique implémentant les briques MDM, DQM et Service Adresse.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°35 portant sur la gouvernance de la qualité des données du ministère de la Défense , diffusée sous timbre n° 314/DEF/DGSIC/SDS/NP du 11 juin 2015	11/06/2015	DGSIC	Directive	Min Arm
<i>Commentaire : cette directive définit les règles relatives à la gouvernance de la qualité des données des systèmes d'information et de communication (SIC) du ministère des armées. Elle abroge l'ancienne directive DGSIC n°14 portant sur l'administration des données du ministère des armées. Elle est complétée par un guide (ci-dessous).</i>				
Guide DGSIC n°10 portant sur la gouvernance de la qualité des données du ministère de la Défense	11/06/2015	DGSIC	Guide	Min Arm
<i>Commentaire : le présent guide a pour objectif de présenter les principes fondateurs de la gouvernance de la qualité des données, en définissant le périmètre puis en établissant pour chaque démarche relevant de cette gouvernance les objectifs, les concepts, les principes de mise en œuvre et les moyens associés.</i>				

La solution retenue au niveau ministériel est celle mise en œuvre par le projet « Plateforme de gestion des données de référence » (PGDR). Pour mémoire, la gestion des métadonnées est couverte par METADATARM (*cf. 2.3.6.2.2*)

Concernant le MDM, l'offre de service de PGDR concerne les données de référence NP/DR du ministère ; elle est constituée de :

- La réalisation de référentiels de données par le CASID (selon le plan de charge) ou l'industriel (sur financement) ;
- La délégation de capacités de réalisation de référentiels de données à un organisme du ministère (sur ressources humaines et financières de son ressort).

En conformité avec la politique API, les données de référence sont exposées sous forme d'API sur la PEM. Néanmoins des flux complets sont envisageables pour répondre au besoin des SI consommant historiquement les données de référence sous cette forme.

Concernant le DQM, l'offre de service de PGDR se décline en services de qualité des données (diagnostics de la qualité des données, et propositions de correction lorsqu'elles sont automatisables) pour l'ensemble des données des SI NP/DR du Ministère (et pas seulement les données de référence), prenant la forme de :

- La réalisation de services qualité des données par le CASID (selon le plan de charge) ou l'industriel (sur financement) ;
- La délégation de capacités de réalisation de services qualité des données à un organisme du Ministère (sur ressources humaines ou financières de son ressort).

Le DQM est complété d'un service « clef en main » dédié au contrôle et au redressement des adresses postales ou géographiques au périmètre France métropolitaine et DROM COM, certifié SNA (Service Nationale de l'Adresse). Ce service est utilisable selon deux modes :

- un mode batch permettant d'effectuer des mesures de qualité, des traitements de normalisation ainsi que des redressements d'adresses sur des lots de fichiers volumineux (traitement de masse) ;
- un mode API permettant d'intégrer directement au sein d'applications métier une interface de saisie et de contrôle et de redressement en temps réel des adresses.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Composant MDM / DQM	PGDR	Min Arm	Basé sur les logiciels IBM Product Master V12 et IBM InfoSphere Information Server 12 (Information Analyzer et Quality Stage)À vocation ministérielle, l'offre de service	R / E	Intradef

			concerne tout référentiel de données NP/DR quel que soit le domaine métier. Le composant Service Adresse est basé sur les solutions CapencyBatch : CAP RNV PAPI : CAP ADRESSCAP SAISIE (saisie des adresses en « entonnoir »), CAP LINE (saisie des adresses sur un seul champ), CAP VERIF (intégralité d'une adresse quel que soit son mode de saisie)		
--	--	--	---	--	--

3.2.5.5 Gestion électronique de documents [GED]

La gestion électronique des documents (GED, ou EDM pour Electronic Document Management) désigne un procédé informatisé visant à organiser et gérer des informations essentiellement non structurées comme des documents électroniques au sein d'une organisation.

Elle met principalement en œuvre des systèmes d'acquisition (numérisation de masse de documents papiers, par exemple), d'indexation, de classement, de gestion et de stockage, d'accès (navigation et recherche) et de consultation des documents.

L'aspect publication des documents est traité dans le chapitre **3.1.3.1 Portail intranet [SU_PIN]**, et partie back-office **3.3.2.2 Portail d'information [PIN]**.

Le travail collaboratif présidant à leur élaboration est traité en **3.1.2.2 Espace de travail collaboratif [SU-EDT]** et, partie back-office **3.3.2.8 Gestion des communautés d'intérêt [COI]** et **3.3.3 Travail de groupe**.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
GED	Sharepoint	Microsoft		★ / ★	Tout intranet
GED	Alfresco community edition	Hyland		★ / ★	Min Arm
GED	Nextcloud GMBH	Nextcloud	Langues Multilingue - Licence Licence libre (AGPLv3)	★ / ★	Min Arm
GED	Nuxeo	Hyland		★ / ★	Min Arm
GED	Confluence	Atlassian		D / -	Tout intranet
<i>Commentaire : L'éditeur ATlassian abandonne progressivement le support de Confluence on premise jusqu'en 2029. Au delà, les données ne seront plus accessibles qu'en lecture. Cf. le NeMO CND/GOUV STRAT/GOUV NUM n°2025/66 du 27/10/2025.</i>					

3.2.5.6 Masquage / Anonymisation / Pseudonymisation des données

Le masquage des données est une technologie visant à prévenir la manipulation de données à caractère personnel ou dites « sensibles » pour le ministère (exemple : site) en fournissant aux utilisateurs des données fictives mais réalistes au lieu des données réelles. Il s'appuie sur les principes d'anonymisation et de pseudonymisation des données en fonction de l'objectif recherché.

L'anonymisation des données est le processus par lequel les données sont rendues anonymes, et à l'issue duquel elles ne peuvent plus être rattachées à un individu en particulier. Le procédé doit ainsi être irréversible dans le but de rendre impossible la ré-identification.

La pseudonymisation (ou pseudo-anonymisation), en revanche, est un processus technique consistant à remplacer la valeur d'une donnée par une autre valeur. Ce procédé est nécessairement réversible, les deux processus techniques étant utilisés pour des cas d'usage différents.

3.2.6 Informatique « décisionnelle », Big Data, analyse prédictive

3.2.6.1 Introduction et orientations ministérielles

Jusqu'ici l'informatique décisionnelle couvrait traditionnellement l'ensemble de la chaîne décisionnelle depuis l'extraction des données, leur hébergement dans un entrepôt de données, leur transformation, la gestion de leur qualité et la restitution d'analyses statiques.

Le Ministère a ainsi été amené à mettre en place la ferme de stockage Fasttrack servant d'infocentres et la plateforme décisionnelle SAP Business Object BI. Ces plateformes traditionnelles sont opérationnelles depuis plusieurs années et destinées à être remplacées. Actuellement dimensionnées au juste besoin pour les systèmes existants, la ferme Fasttrack ne prendra plus en compte de nouveaux besoins. Les nouveaux outils de « datavisualisation » permettent de naviguer dans des tableaux de bord de façon dynamique. Le Ministère a fait le choix de la technologique QlikSense pour mettre en place une plateforme ministérielle de « datavisualisation » qui à terme remplacera l'ensemble des univers et requêtes SAP BI. Les autres outils de datavisualisation ou de tableaux de bord sont soumis à dérogation.

La partie entrepôts de données et outils de chargements va être remplacée par le projet HERMOD courant 2026.

Les nouveaux outils dits de « big data » permettent de traiter un volume de données beaucoup plus important, d'exploiter leur potentiel par des techniques de « science de la donnée », comme l'analyse prédictive et des algorithmes d'intelligence artificielle.

À noter que POCEAD ne doit plus être utilisé pour de nouveaux projets qui doivent désormais se tourner vers ARTEMIS-IA DR.

Progressivement, un catalogue de solutions s'enrichit d'autres options adaptées en fonction des catégories de besoins.

La feuille de route ministérielle des données porte les stratégies de cohérence en cohérence avec la politique ministérielle des données (Note n°117/ARM/DGNUM/DG/NP du 5 avril 2022).

Document	Date	Origine	Type doc	Portée
Politique ministérielle des données Note n°117/ARM/DGNUM/DG/NP du 5 avril 2022	05/04/2022	DGNUM	Note	Min Arm

3.2.6.2 Datavisualisation, BI Corporate ou BI self-service

L'utilisation des données venant de SI opérationnels se fait avec des outils de restitution allant du simple rapport au tableau de bord composé d'indicateurs complexes.

L'informatique décisionnelle agile permet de créer des tableaux de bords dynamiques. Ces outils permettent de **couvrir le cycle de création d'un tableau de bord de la collecte des données, de leur préparation, de leur nettoyage et de leur visualisation**. Ils se caractérisent en général par une simplicité d'usage, et une interface graphique plus conviviale que celle que l'on retrouve dans l'informatique décisionnelle traditionnelle. Elle permet de s'affranchir d'une phase de restructuration des données.

Pour tout nouveau projet ou toute évolution majeure de projet décisionnel, et conformément à la décision n°4 du CECNUM du 9 juillet 2019, la plateforme ministérielle basée sur l'outil Qlik Sense doit être utilisée.

Dans les autres cas, envisager les outils d'analyse et de visualisation des données mentionnés au §3.2.6.3 *Datavisualisation (ou BI self-service)*.

SAP a annoncé la fin de SAP Business Object en 2027 au profit de sa solution cloud SAP Analytics Cloud. Le support (*mainstream maintenance*) de la version 4.3 s'est achevée fin 2025 (2027 en souscrivant un *priority support*). La version SAP Business Object 2024 recentrée sur les outils les plus utilisés (Web Intelligence, .unx universes et platform BI) prolongera le support jusqu'en fin 2027 et est destinée à faciliter la migration vers la solution Cloud. Cette dernière sera également déclinée en version "on premise" sous le nom SAP BO Enterprise, private cloud edition (PCE) opérée par SAP ce qui la rend impropre à un usage sur les réseaux du Ministère.

En conséquence, la fin de migration des rapports existants vers la solution ministérielle Qlik Sense doit être menée en fonction de cette échéance échue de fin 2025.

Le projet HERMOD (Hub d'Echange et de Recherche pour la Modélisation et l'Organisation des Données), dont la mise en service est prévue pour 2026, vise à mettre en place une infrastructure ministérielle offrant aux métiers du Ministère des capacités de stockage de données structurées en remplacement de la ferme de stockage Fasttrack, ainsi que d'ETL (Extraction, Transformation, Chargement) basé sur Talend.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Décisionnel traditionnel	Plateforme basée sur l'Appliance décisionnelle (matériels et logiciels) Fast track	CND	Plateforme mutualisée Intradef. Implique le recours à SQL Server (Assujetti)	D / O	Intradef
Entrepôt de données	HERMOD	Min Arm	Plateforme mutualisée Intradef de stockage dans les technologies PostgreSQL (recommandé) et SQL Server (assujetti).	E / -	Intradef
Décisionnel traditionnel	Business Objects BI	SAP	Outil de restitution et d'analyse des données (WEBI) <i>Implique le recours à SQL Server (Assujetti)</i> . Attention, interdit sur C1	D / O	Intradef
Décisionnel traditionnel	SQL Server BI SSRS and SSAS.	Microsoft	Outil de restitution et d'analyse des données (WEBI). Attention, interdit sur C1	D / N	Intradef
Décisionnel agile Analyse et de visualisation de données	Plateforme ministérielle QlikSense (Serveur)	Qlik	Service ministériel	R / S	Intradef
	QlikSense	Qlik	Produit logiciel	A / N	Intradef
	KIBANA	Elastic	Assujetti à l'écosystème Elasticsearch et Logstash et à la justification que les outils recommandés de datavisualisation ne satisfont pas.	★ / ★	Min Arm
	GRAFANA	Grafana labs	Pour des besoins non couverts par Kibana, cf. ci-dessus	★ / ★	Intradef
	TABLEAU	Tableau Software	Doit migrer vers la plateforme QlikSense. Attention, interdit sur C1	D / N	Intradef
	POWERBI Server	Microsoft	Doit migrer vers la plateforme QlikSense. Attention, uniquement sur Intradef legacy.	D / N	Intradef
<i>Commentaire : la plateforme ministérielle QlikSense est gérée par le CND.</i>					
Décisionnel traditionnel	Crystal Report	SAP	Permet de créer des rapports de masse avec des graphiques et des tableaux de données. Permet la disposition des	D / N	Intradef

			objets aux pixels près. N'est pas interactif et visualisable via la plateforme SAP ou via un export pdf. Attention, interdit sur C1		
Décisionnel traditionnel	BO LUMIRA	SAP	Permet de développer des tableaux de bord interactifs. Attention, interdit sur C1	D / N	Intradef
Décisionnel traditionnel	Pentaho (version communautaire)	Hitachi Vantara	Solution Open Source en Java. Suite logicielle complète (de la création à la diffusion via une interface web). Attention, interdit sur C1	D / N	Intradef
Décisionnel traditionnel	Jaspersoft BI (version communautaire)	Tibco	Plateforme BI Open Source. Attention, interdit sur C1	D / N	Intradef
Préparation et analyse des données	Data Science Studio	Dataiku	Assujetti à l'usage de la plateforme dataiku de l'Armée de l'Air et de l'Espace dans l'attente de la mise à disposition d'une instance ministérielle.	A / N	Intradef, SIA S-SF, I3E

La plateforme Fasttrack/Business Object BI opérée par le CND reste encore maintenue a minima pour permettre aux projets existants ou intégrés à un écosystème SAP de continuer à pouvoir faire fonctionner les outils d'informatique décisionnelle déjà mis en place en attendant une migration vers HERMOD/Qlik Sense.

Pour la collecte et transformation des données (ETL), se référer au § 3.2.4.6.

3.2.6.3 Données massives ou « Big Data »

Le terme de « Big Data » (parfois appelées « données massives » en français) est au croisement de plusieurs domaines : statistiques, technologies, bases de données et métiers (finances, RH, renseignement, etc.). Le « Big Data » vise à exploiter des données souvent complexes de structures et de sources très diverses, à croissance exponentielle. Ce type de données est difficile à travailler avec des outils classiques de gestion de base de données ou de gestion de l'information.

Les technologies « Big Data » s'appuient essentiellement sur des solutions open source :

- un système de fichiers distribué permettant de stocker des données plus ou moins structurées sur un ensemble de serveurs distribués y compris géographiquement (Hadoop Distributed File System par exemple) ;
- un framework de requêtage sur ces agrégats de données distribuées (les calculs sont effectués au plus près des données puis consolidés en central) : MapReduce et son évolution YARN notamment ;
- des traitements en temps réels réalisés par des moteurs d'indexation temps réel distribués (ElasticSearch, pile ELK, par exemple).

Les approches, architectures et outils diffèrent selon qu'il s'agit de traiter ces données en temps réel ou pas, Dans tous les cas, il est recommandé une approche en deux temps : l'expérimentation (*preuve de concept*) validée par un expert de type *Data Scientist* et l'industrialisation.

3.2.6.3.1 Plateformes exploratoires et d'innovation DATA360, ARTEMIS-IA

Il y a trois plateformes disposant d'une capacité d'exploration de données et de POC (proof of Concept).

La plateforme DATA360 est une plateforme d'expérimentation du Labo BI de la DTPM. Dédiée uniquement à l'innovation, elle est composée des fonctionnalités suivantes :

- collecte des données ;
- stockage indexé des données massives ;
- analyse des données (fouille via un moteur de recherche très puissant) ;
- datavisualisation via la plateforme ministérielle QlikSense ;
- sécurisation (gestion des droits d'accès jusqu'à la donnée) ;
- datascience (mise en œuvre d'algorithme).

Plateforme ARTEMIS.IA : cf. 3.2.6.3.3.

Pour des cas d'usage au stade exploratoire ou d'innovation et la réalisation de POC concernant le « Big Data ou l'analyse prédictive », la gouvernance orientera au Pitch 0 vers l'une des plateformes ayant cette capacité DATA360 ou KDL ARTEMIS.IA sur PICSEL.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Big Data – IA phase exploratoire et POC	POCEAD	Min Arm	En phase exploratoire et d'innovation pour la réalisation de POC et de cas d'usage en production pour des données qui peuvent être réutilisées (open data) avec contractualisation selon les catégories de données utilisées. Basée sur la plateforme SAAGIE : soutenu par le CASID/SAND jusqu'à son retrait de service.	D / S	Intradef
Big Data – IA phase exploratoire et POC	DATA360	Elastic	En phase exploratoire et d'innovation et pour la réalisation de POC. Basé sur Elastic Cloud Enterprise. Pour avoir une vision 360 des données pour l'aide à la décision. Les données peuvent être croisées entre elles et avec d'autres données provenant par exemple de data.gouv.fr via des API : soutenu par SGA/MAP	R / S	Intradef
Big Data – IA phase exploratoire et POC	Bac à sable ARTEMIS IA	Min Arm	Disponible sur environnement de production pour aider au développement, explorer les données, pour entraîner tester et qualifier des algorithmes basés sur de l'IA.	R / S	Min Arm
Big Data – IA phase exploratoire et POC	Kit de Développement ARTEMIS.IA	Min Arm	Kit de développement logiciel ARTEMIS.IA permettant de développer et de packager des applications métier pour intégration sur le socle ARTEMIS.IA. Disponible sur PICSEL ou de manière autonome	R / S	Min Arm

3.2.6.3.2 Plateforme POCEAD – ouverture des données

La Plateforme d'Ouverture, de Centralisation, d'Exposition et d'Analyse des Données (POCEAD) est dédiée à l'ouverture et à la mise à disposition des données du Ministère. Son objectif est d'offrir un ensemble de services permettant d'analyser, de traiter et d'exposer des données aux directions d'application et aux services numériques du ministère. Ce service est en cours de décommissionnement au profit de ARTEMIS-IA et HERMOD.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Big Data – IA Environnement de prod	POCEAD	Min Arm	Vasée sur la plateforme SAAGIE	D / S	Intradef

3.2.6.3.3 Plateforme ARTEMIS.IA

Le programme ARTEMIS.IA (ARchitecture de Traitement et d'Exploitation Massive de l'Information multi-sourceS Intelligence Artificielle) a pour objectifs de fournir une infrastructure unifiée et souveraine d'analyse et de traitement de données massives (Big Data) et d'Intelligence Artificielle (IA) issues de technologies civiles adaptée aux spécificités du MINARM, de mutualiser les développements tout en permettant d'accueillir la variété des cas d'usages des armées, directions et services (ADS) et de capter l'innovation issue du monde civil au profit des Armées.

L'opération ARTEMIS.IA a démarré en 2017 dans le cadre d'un partenariat d'innovation en 3 phases et est en phase d'industrialisation en 2022 avec un premier déploiement sur le réseau Secret-SF SIA. En complément, une instance une offre de service équivalent sur Intradef. Offrant les mêmes composants logiciels que l'instance S-SF, elle s'appuie sur les services d'orchestration de conteneurs et un parc de plus de 100 GPU H100 du C1DR.

L'offre de service est constituée :

- D'un bac à sable permettant :
 - L'élaboration des algorithmes en vue de la mise à disposition de nouveaux modules et applications,
 - L'accès aux données opérationnelles sans nuire à leurs disponibilités pour les applications en cours d'utilisation,
 - La mise à disposition des outils pour explorer les données disponibles, et pour entraîner, tester et qualifier des algorithmes basés sur de l'IA ;
- D'un kit de développement logiciel permettant de doter un tiers d'une suite logicielle autonome, indépendante d'une instance ARTEMIS.IA et de réaliser la conception, l'implémentation et les tests unitaires de modules dans les langages Python, R, Java ;
- D'une plateforme ARTEMIS.IA permettant de réaliser les tests d'intégration des cas d'usage et de les mettre ensuite en production. Cette plateforme est utilisée en mode mutualisé c'est-à-dire qu'elle porte les cas d'usage des directions d'application.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Big Data - IA	ARTEMIS IA	Min Arm		R / S	Min Arm

3.2.6.4 Analyse prédictive et statistique

Alors que les solutions d'analyse et de génération de rapports classiques appartiennent au domaine du constaté et permettent d'analyser la situation à un moment donné, l'analyse prédictive permet au contraire de répondre au pourquoi de la situation en se focalisant sur les variables explicatives.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Analyse prédictive	ARTEMIS IA	Min Arm		A / S	Min Arm
Analyse prédictive	Suite SAS	SAS	Cette plateforme offre une solution simple d'utilisation, couvrant toutes les fonctionnalités depuis l'alimentation en self-service jusqu'au déploiement de l'analytique en temps réel. SAS sont les pionniers dans le domaine des statistiques et de la prédiction.- SAS Analytic Pro server- SAS IML- SAS ETS- SAS Access to ODBC-SAS Access to	D / S	Intradef

			PC Files- SAS Visual Analytics 7.3. Attention, interdit sur C1		
<i>Commentaire : ces solutions sont hébergées sur une plateforme SAS hébergée au CNMO-SI pour des besoins RH (DRH-MD, OSD) et devront migrer dans le cadre de la feuille de route évoquée au §3.2.6.1 Introduction et orientations ministérielles.</i>					
Analyse prédictive	Predictive Analysis	SAP	Cette plateforme offre une solution simple d'utilisation, couvrant toutes les fonctionnalités depuis l'alimentation en self-service jusqu'au déploiement de l'analytique. Attention, interdit sur C1.	D / O	Intradef
Analyse Prédictive	Elastic Search module Machine Learning	Elastic	Cas d'usage spécifique (analyse prédictive sur certaines séries temporelles uniquement)	A / S	

3.2.6.5 Outils logiciels pour données volumineuses

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
IA/ Big Data	NiFi	Apache Software Foundation		★ / ★	Min Arm
IA/ Big Data	Spark	Apache Software Foundation	Cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.	★ / ★	Intradef SIA S-SF SIA FrOPS
IA / Big Data	Conda	Anaconda	Assujetti aux environnements de développement Big Data	A / N	Intradef
IA / Big Data	Flink	Apache Software Foundation		E / N	C1DR
IA/ Big Data	Jupyter			A / N	Intradef
<i>Commentaire : cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.</i>					

3.2.7 Cadres particuliers

3.2.7.1 ERP

Les ERP⁴⁴, ou PGI⁴⁵ en français, sont des logiciels de gestion suffisamment génériques pour convenir à une clientèle élargie. Ils comprennent généralement une base générique et une partie paramétrable.

On parle d'ERP ou de PGI dès lors que le produit considéré couvre au moins deux domaines fonctionnels distincts de l'entreprise (logistique et ressources humaines, par exemple). Cette famille de logiciel peut aller jusqu'à couvrir l'ensemble des besoins de gestion d'une entreprise. Les domaines fonctionnels peuvent être déclinés sous forme de modules optionnels.

Un ERP est efficace lorsqu'il est utilisé pour les processus natifs de la solution. Les personnalisations successives d'un ERP obèrent la possibilité de suivre la feuille de route éditeur et entraîne des coûts de traitement des obsolescences supplémentaires.

⁴⁴ Enterprise Resource Planning.

⁴⁵ Progiciel de gestion intégré.

Un ERP doit pouvoir s'intégrer dans le socle et doit ouvrir ses données aux applications qui le demandent.

SAP : à titre d'information, un accord cadre, porté par le MinArm (pilotage par DRHMD/SRSI/SMSIF-RH) a été notifié en juillet 2022, pour 3 ans et renouvelable 1 an.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
ERP	SAP ECC	SAP	ERP complet utilisé notamment pour les SIRH d'armées (CONCERTO, RHAPSODIE, ORCHESTRA, etc.), la finance (CHORUS) ou la logistique (SINAPSE, ARES, SCALP...). Attention, interdit sur C1	D / N	Intradef
<i>Commentaire : la suite SAP ECC (ERP Central Component) est formellement interdite dans les nouveaux projets mis en production depuis le 1er janvier 2023. À l'heure actuelle le support de cette suite est assuré par la société SAP jusqu'en 2030.</i>					
ERP	SAP HANA/4HANA	SAP	Assujetti à une justification du cadre d'emploi	A / N	Intradef
<i>Commentaire : il est indispensable de pleinement prendre en compte les fortes contraintes imposées par ces ERP, à la fois pour leur hébergement, leur exploitation, leur MCO, leur encapsulation des données que pour leur intégration au sein du SI du Ministère avant d'y recourir.</i>					
ERP	HR Access Suite	HR Access Solutions	Progiciel utilisé pour les RH et la finance, utilisé pour ALLIANCE et SOURCE Solde	A / N	Intradef
<i>Commentaire : il est indispensable de pleinement prendre en compte les fortes contraintes imposées par ces ERP, à la fois pour leur hébergement, leur exploitation, leur MCO, leur encapsulation des données que pour leur intégration au sein du SI du Ministère avant d'y recourir.</i>					

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

Nota : Les produits présentés sont actuellement utilisés au sein du Ministère. Ils ne contraignent pas les évolutions à venir.

⚠ L'obtention d'une dérogation pour mettre un oeuvre un de ces produits n'exempte pas de la nécessité de respecter les normes, standards et directives du Ministère, dont la nécessité de recourir aux briques du socle, pour l'authentification via MinDefConnect ou la consommation et l'exposition des données via API Rest conformes par exemple.

3.2.7.2 Moteur de génération de rapports

Cf. 3.2.6 Informatique « décisionnelle », Big Data, analyse prédictive.

3.2.7.3 Archivage

3.2.7.3.1 Documents de portée générale OTAN

Document	Date	Origine	Type doc	Portée
Politique relative à la gestion des archives courantes et intermédiaires de l'OTAN (C-M(2011)0043)	17 juin 2011	NATO	Politique	Min Arm
Directive sur la gestion des archives courantes et intermédiaires de l'OTAN (C-M(2012)0014)	27 février 2012	NATO	Directive	Min Arm
Stratégie OTAN pour la conservation à long terme des informations numériques (AC/324-D(2012)0003)	8 août 2012	NATO	Stratégie	Min Arm
Directive sur la conservation des informations numériques OTAN pérennes (AC/324-D(2014)0008)	3 juillet 2014	NATO	Directive	Min Arm

3.2.7.3.2 Documents de portée générale nationale

Document	Date	Origine	Type doc	Portée
Code du patrimoine livre II	15 juillet 2008	Ministères	Loi	Toute admin.
Référentiel Général de Gestion des Archives [R2GA] publié par le comité interministériel aux Archives de France cf. 2.2.3.1 Référentiels généraux (RGI, RGS, RGAA, R2GA, RGEN)	octobre 2013	PM	Référentiel	Toute admin.

Le RGI V2 définit par ailleurs un profil d'archivage

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
Profil « Archivage »	Ce profil, entretenu par le Service Interministériel des Archives de France (SIAF), identifie les normes de modélisation conceptuelle et les standards techniques intervenant dans les échanges, liés à la gestion de l'archivage, la consultation ou la conservation de documents.	R	Toute admin.

3.2.7.3.3 Documents de portée générale Ministérielle

Document	Date	Origine	Type doc	Portée
Instruction ministérielle 101 relative à la politique et à l'organisation de générale de l'archivage du ministère de la défense , IM n°101/DEF/SGA/DMPA/DPC du 29 juillet 2011	29 juillet 2011	DMPA	Instruction	Min Arm
Directive DGSIC n°30 portant sur la mise en œuvre de la démarche d'archivage des contenus dans les projets de SI publiée au Bulletin Officiel des Armées	5 déc. 2013	DGSIC	Directive	Min Arm
<i>Commentaire : recommandations sur la prise en compte de l'archivage dans la conduite des projets de SI, notamment pour la conception, les évolutions et le retrait du SI. Point de contact : DMPA / DP Archivage.</i>				
Guide ministériel relatif à l'intégration de la démarche d'archivage dans les projets de systèmes d'information V1.0 approuvé le 30 septembre 2013	30 septembre 2013	DMPA	Guide	Min Arm
Manuel pour élaborer la stratégie d'archivage d'un SI V1.0 approuvé le 30 septembre 2013	30 septembre 2013	DMPA	Manuel	Min Arm
Positionnement des outils collaboratifs dans le cycle de vie du document , sous double-timbre n°394/DEF/DGSIC/SDAU/NP du 8 juillet 2015n°D-15-004558/DEF/EMA/CPI/NP du 8 juillet 2015	8 juillet 2015	DGSIC EMA	Note	Min Arm
<i>Commentaire : cette note issue du comité directeur des Intranets précise pour rappel que les outils de travail collaboratif n'ont pas vocation à être utilisés à des fins d'archivage de documents validés et rappelle les principaux éléments de la démarche d'archivage au sein du ministère des armées.</i>				

3.2.7.3.4 Documents techniques MinArm

Document	Date	Origine	Type doc	Portée
Préconisations pour la pérennisation de l'information : validées en CECSIC du 22 juin 2012	28 juin 2012	DGSIC DMPA	Recommandations	Min Arm
<i>Commentaire : Ce document est un livrable d'un GT archivage piloté par la DGSIC et la DMPA, dont les annexes principales ont été présentées et validées lors du conseil exécutif des SIC (CECSIC) du 28 juin 2012. Le document émet des recommandations concernant :</i> • les métadonnées essentielles pour la maîtrise du cycle de vie de l'information ; • les formats pérennes pour les documents électroniques.				

3.2.7.3.5 Solution ministérielle Archipel

Le projet Archipel a pour objet de mettre en place le système d'archivage du ministère en s'appuyant sur le progiciel Everteam (front office) et la solution d'archivage interministériel Vitam (back office) qui apportent une garantie de sécurité et de disponibilité pour les archives papiers et électroniques, quel qu'en soit le niveau de protection. Le projet est en production pour la partie non protégée et diffusion restreinte et gestion du classifié.

Ses principales caractéristiques sont :

- La prise en compte des besoins utilisateurs métier par l'apport des **fonctionnalités nécessaires au fonctionnement des services publics d'archives** : entrées, recherches, consultation, communication, administration et gestion, structurations arborescentes, référentiels... ;
- La **gestion unitaire de fortes volumétries** de données et l'accès à la pièce par des requêtes riches ;
- La **garantie de la valeur probante** des archives par le respect des normes et standards en vigueur (NF Z 42-013, Z 42- 020, Z 44-022, SEDA...), par la traçabilité des opérations et du cycle de vie des objets et leur journalisation sécurisée ;
- La sécurité et la robustesse : la gestion applicative du stockage permet une **réplication** des données, métadonnées, index et journaux d'évènements sur plusieurs sites et plusieurs offres contrôlées ; l'architecture interne du stockage assure **la capacité de reconstruire** le système à partir d'une seule offre, en une fois ou au fil de l'eau ;
- La possibilité d'une **utilisation mutualisée** grâce à la gestion multi-tenant de Vitam.

Document	Date	Origine	Type doc	Portée
Documentation technique relative à VITAM accessible sur http://www.programmevitam.fr		DINUM	Documentation technique	Interministériel
<i>Commentaire : VITAM est la couche back office de l'archivage développé en interministériel par la DINUM.</i>				
Documentation relative à au télé-service de versement aux archives [TSV]	octobre 2019	DMCA	Documentation technique	Intradef
<i>Commentaire : TSV est un outil de versement au service des archives du Ministère.</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Archivage	ARCHIPEL solution ministérielle	Min Arm		R / S	Intradef

3.2.7.4 Informations géographiques, hydrographiques, océanographiques et météorologiques (GHOM)

3.2.7.4.1 Système d'information géographique

Un système d'information géographique (SIG) est un système d'information permettant de créer, d'organiser et de présenter des données géo référencées, ainsi que de produire des plans et des cartes. Ses usages couvrent les activités géomatiques de traitement, de partage et de diffusion de l'information géographique.

Document	Date	Origine	Type doc	Portée
Directive DGNUM n°9 portant sur les données géographiques, hydrographiques, océanographiques et météorologiques de Défense sous forme numérique diffusée par note n° 649/ARM/DGNUM/SDDCN/NP du 10 novembre 2023	10 novembre 2023	DGNUM	Directive	Min Arm

<i>Commentaire : cette directive précise les règles d'exploitation des données géographiques, hydrographiques, océanographiques et météorologiques de Défense et les formats associés</i>				
Guide DGA S-CAT n°14107 de spécifications fonctionnelles pour la composante géographique des systèmes de la défense 3ème édition entretenue par DT/ST/DGA IP/ASC/ENV	10 octobre 2012	DGA IP	Guide	Min Arm SIO
<i>Commentaire : ce guide traite des données à caractère géographique de l'espace aéroterrestre, hors renseignement et à l'exclusion notamment des données hydrographiques utilisées notamment pour les cartes marines de navigation, des données météo et aéronautiques. Il précise les spécificités fonctionnelles liées aux formats des données choisies. Le guide DGS-SCAT n°14109, même édition, même date, en constitue une version synthétique.</i>				

Le RGI V2 définit un profil géomatique pour l'échange de données géographiques entre administration :

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
Profil « Géomatique »	Ce profil, entretenu par le Conseil National de l'Information Géolocalisée (CNIG), identifie les principaux standards recommandés pour les échanges d'informations géographiques entre les administrations pour localiser notamment des événements, des données, des activités, des objets.	R	Toute admin.

3.2.7.4.2 Moteur cartographique OSM

Le moteur cartographique OSM, en cours de réalisation, offre un service de mise à disposition de fonds de carte, basés sur OpenStreetMap, et un service de visualisation de données géo-référencées, autorisant la recherche d'une ville, d'une adresse et la récupération des coordonnées géographiques associées.

Ces éléments seront accessibles par des API de type REST inscrits dans le catalogue de la PEM Intradef.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Moteur cartographique	Service ministériel basé sur OpenStreetMap	Min Arm		R / S	Intradef
Partage de données géospatial	GeoServer	Open Source	https://geoserver.org/	★ / ★	Min Arm
Framework de gestion de cartes	Leaflet	Open Source		★ / ★	Min Arm

3.2.8 Démarche simplifiée (DS) – Dossier numérique de l'agent (DNA)

3.2.8.1 Démarches simplifiées (DS)

Ce service fonctionnel commun permet de dématérialiser des démarches administratives grâce à un générateur de formulaires et une plateforme d'instruction de dossiers. Il permet de gérer le cycle de vie d'un formulaire, de sa conception jusqu'à son intégration dans les traitements applicatifs, à la main complète des métiers. Cette application est construite sur la solution « demarches-simplifiées.fr » co-développée par la DINUM et le ministère des Armées. Le service offre une API permettant l'intégration réactive (Webhook en GraphQL) avec des systèmes tiers. Sur les instances ministérielles, le service est intégré avec le service DNA pour permettre la simplification administrative et le DNLUF (« Dites-Le Nous Une Foix »), il s'appuie sur les référentiels ministériels pour les données de référence, et fait appel à des notifications par mail pour la gestion des étapes de validation (INA / POCEAD / système de cartographie Open Street Map, API tierces...).

Il existe trois instances :

- **Sur Internet**, la DINUM héberge et maintient le service qui bénéficie de l'interconnexion à de nombreux services de l'État plateforme, notamment France Connect, API Entreprise, API Géo et BAN.
- **Sur Intradef**, le Ministère en a assuré un portage sur Intradef, opérationnel et homologué au printemps 2019.
- **Sur l'Internet Maîtrisé** : le service, d'ores et déjà déployé, permet une continuité Internet / Intradef et s'appuie sur les capacités de fédération d'identités de MindefConnect Internet.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Dématérialisation de procédures	demarches-simplifiées.fr	DINUM	Solution développée et soutenue par la DINUM https://www.demarches-simplifiees.fr/	R / S	Internet
Dématérialisation de procédures	Solution de la DINUM portée sur Internet	Min Arm	Solution maîtrisée par le ministère https://demarches-simplifiees.defense.gouv.fr/	R / S	Internet
Dématérialisation de procédures	Solution de la DINUM portée dans l'environnement Intradef	Min Arm	Soutien par le projet DS au profit du ministère	R / S	Intradef
Commentaire : la documentation du service se trouve sur le portail de la DINUM : https://doc.demarches-simplifiees.fr/					

3.2.8.2 Dossier numérique de l'agent (DNA)

Le DNA est un service en cours de réalisation. Il offrira un espace de stockage et de mise à disposition de documents et justificatifs à des fins de simplification administrative. Le service sera disponible sur l'Internet maîtrisé et l'Intradef fin 2026.

Les documents et justificatifs fournis pourront être mis à disposition des applications après autorisation de l'administré. Les documents et justificatifs sur le DNA sur Internet peuvent être déposés seuls sur Internet, puis être ensuite basculés sur Intradef si besoin est (cas du recrutement ou des pensionnés).

Pour l'administré, le DNA offre un point d'accès unique à ses données tant sur Internet que sur l'Intradef, lui permet de solliciter des rectifications, si nécessaire, et de partager simplement de la donnée avec un tiers.

Pour les directions d'application, le DNA permet, au travers d'une API, de déposer et récupérer un document (notification type A/R à l'administré). Afin d'être en conformité avec le RGPD, la direction d'application doit établir un contrat d'usage accompagné d'un protocole d'échange entre son application et le DNA.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Simplification administrative	DNA Intradef	Min Arm	NP/DR	E / S	Internet Intradef
Commentaire : en cours de déploiement					

3.2.9 Intelligence artificielle

Document	Date	Origine	Type doc	Portée
Dossier relatif aux risques de sécurité et aux bonnes pratiques portant sur l'intelligence artificielle	Avril 2022	CNIL	Dossier	

Guide de recommandations pour la spécification et la qualification de systèmes intégrant de l'intelligence artificielle V2	30 octobre 2020	DGA	Guide	Min Arm
<i>Commentaire : le guide de la DGA présente les principaux enjeux techniques liés à l'intégration d'intelligence artificielle (IA) dans les systèmes opérationnels et propose une méthodologie pour leur mise en œuvre, de la spécification à la qualification des systèmes, mais aussi tout au long de la vie du système déployé. Le dossier de la CNIL présente les différentes attaques possibles sur un système IA, détaille une méthodologie d'analyse de risques et présente les bonnes pratiques pour la sécurisation d'un système IA.</i>				

GénIAI est une plateforme multi-services IA pour faciliter et soutenir l'activité des métiers au quotidien. En évolution, elle offre actuellement plusieurs services dont :

- Agent conversationnel : répond aux questions, aide à la rédaction de contenus textuels et appui à la réflexion et la créativité ;
- Synthétiseur : extrait les idées et informations importantes des documents dans un format synthétique et personnalisable ;
- Traducteur : traduit des messages et des documents.
- Transcription : convertit des contenus audio (fichier ou depuis le micro) en transcription de texte
- Océrisation : effectue une reconnaissance optique de caractères à partir d'images et de documents.

Pour voir la liste complète des services offerts, se référer au catalogue .

GenIAI intradef dispose d'un premier modèle d'agent conversationnel « coloré » Ministère, produit par l'AMIAD, lui permettant de mieux manipuler le vocabulaire propre au Ministère. Ce modèle bénéficiera d'améliorations permanentes pour continuer de s'adapter et de s'enrichir. Des agents spécialisés pourront être proposés pour chaque métier. Des formations à l'utilisation de l'outil sont également proposées.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
IA générative	GenIAI	Min Arm		R / S	Intradef
<i>Commentaire : API disponible sur l'ensemble des services en ligne API embedding en TI 2025 (compatible OpenIA)</i>					

3.2.10 Internet des objets – IOT

Document	Date	Origine	Type doc	Portée
Guide ANSSI de recommandations relatives à la sécurité des systèmes d'objets connectés	27 août 2021	ANSSI	Guide	Toute admin.
<i>Commentaire : ce guide présente des recommandations de sécurité pour un système d'objets connectés. Il peut être utilisé pour concevoir un tel système ou pour en faciliter l'analyse sécuritaire. Ce guide comprend deux parties, l'architecture d'un système connecté et les propriétés de sécurité attendues, puis les recommandations techniques.</i>				

3.3 Services d'infrastructure

3.3.1 Messagerie / Agenda / Tâches / Listes de diffusion

Le service utilisateur associé est décrit en §3.1.1.7 **Messagerie** ainsi que la partie client.

3.3.1.1 Messagerie non officielle – Agenda [MEL-AGE]

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°3 définissant les règles de la messagerie électronique publiée au Bulletin Officiel des Armées.	08 janvier 2008	DGSIC	Directive	Min Arm
<i>Commentaire : mécanismes permettant la mise en œuvre d'une messagerie électronique. Périmètre : tous les intranets. (À noter que dans la RT11, XIMF est à choisir de préférence à XSMTP, que la RT20 relative à Thunderbird n'est plus la solution recommandée par le ministère).</i>				
Directive DIRISI n°53 « Gestion des adresses fonctionnelles et listes de diffusion dans l'Annudef » du 28/08/2013	28 août 2013	DIRISI/SCOE	Directive	Intradef
<i>Commentaire : la directive précise notamment les modalités d'association des adresses fonctionnelles aux adresses personnelles sur l'Intradef, ainsi que les modalités de gestion des listes de diffusion de l'Annudef.</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Messagerie (Serveur)	Exchange	Microsoft		★ / ★	Intradef SIA S-SF SIA FrOpS
<i>Commentaire : les protocoles à utiliser pour l'émission et la réception sont respectivement SMTPs et IMAPs avec authentification.</i>					
Messagerie (Serveur)	Serveur Exchange, Interface Web (OWA) et Webservice (EWS)	Microsoft		R / S	Intradef SIA S-SF SIA FrOpS
<i>Commentaire : ces interfaces permettent l'accès aux fonctions du serveur via un navigateur ou en Webservice</i>					
Messagerie (Interop)	Serveur Postfix	Postfix.org, licence IBM Public Licence	Utilisé pour assurer un relais de messagerie en bordure de système (NEMO). Attention, interdit sur C1 pour cet usage	★ / ★	Intradef S-SF SIA FrOpS
Messagerie (Interop)	Serveur Cyrus IMAP	Carnegie Mellon University, licence BSD	Utilisé en serveur SMTP/IMAP d'appoint, assujéti à un cadre d'emploi ne relevant pas des services communs	★ / ★	Intradef S-SF SIA FrOpS

3.3.1.2 Gestion de tâches [GTA]

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestion de tâches	La gestion de tâche personnelle est intégrée dans les solutions de messagerie. Cf. 3.3.1.1 Messagerie non officielle – Agenda [MEL-AGE]			R / S	Intradef S-SF SIA FrOps

3.3.1.3 Liste de diffusion [LDF]

Document	Date	Origine	Type doc	Portée
Gestion des listes de diffusion dans l'Annudef (cf. 3.1.1.7.1 Messagerie non officielle)				
<i>Commentaire : décrite par la directive DIRISI n°53. Cette directive définit le processus de gestion de liste statiques et dynamiques.</i>				

Gestion des listes de diffusion dans l'Annudef(cf. 3.1.1.7.1 Messagerie non officielle)				
---	--	--	--	--

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Listes diffusion	Produit annuaire défense	Min Arm	Gestion de liste de diffusion gérée suivant la directive DIRISI n°53 (cf. 3.3.1.1 ci-dessus)	R / S	Intradef

3.3.2 Partage d'information et publication

3.3.2.1 Portail personnalisable [GPE]

Le service utilisateur associé est décrit en §3.1.1.9 *Portail personnalisable [SU-GPE]*.

Document	Date	Origine	Type doc	Portée
Portail collaboratif des armées , note diffusée sous timbreD-19-004391/ARM/EMA/ESMG/NP	26 juillet 2019	MGA	Note	Min Arm
<i>Commentaire : cette note fait état d'une décision de l'EMA d'un portail collaboratif unique pour le besoin des armées, dénommé PC@, sur la base de la technologie mise en œuvre sur le portail des opérations existant.</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Portails	Liferay	Liferay	Pour les applications en usage dans le cadre du STC-IA	★ / ★	Min Arm
Portails	Sharepoint	Microsoft		★ / ★	Intradef SIA S-SF SIA FrOPS
Portails	PC@(sur base Sharepoint)	Min Arm	Portail des opérations	R / S	Intradef S-SF SIA FrOps
<i>Commentaire : le déploiement isolé de l'outil Sharepoint Designer, désormais intégré dans les nouvelles versions de Sharepoint (à partir de 2016) n'est plus nécessaire.</i>					

3.3.2.2 Portail d'information [PIN]

Le service utilisateur associé est décrit en §3.1.3.1 *Portail intranet [SU_PIN]*.

Document	Date	Origine	Type doc	Portée
Compte rendu du CODIR restreint des Intranets n°24 du 3 avril 2014 diffusé par note conjointe :n°D-14-004992 /DEF/EMA/PSIOC/NP du 19 mai 2014 n°316/DEF/DGSIC/NP du 20 mai 2014	19 mai 2014 20 mai 2014	CODIR Intranets	Note	Internet Intradef
<i>Commentaire : le compte rendu porte décision relative au choix des outils pour les portails de communication pour le NP-DR.</i>				

Les écosystèmes des systèmes de gestion de contenu (CMS) sont riches et disposent de nombreux modules complémentaires pour étendre leurs fonctionnalités mais non nécessairement qualifiés par l'éditeur. Afin d'en assurer la maintenabilité, il convient, d'une part, d'en limiter le nombre au juste besoin, et, d'autre part, de ne retenir que des modules présentant des critères de confiance tels que définis au §8.6.3 Critères d'éligibilité pour des modules de CMS.

☆☆☆☆

Pour les CMS, la conformité des modules retenus aux critères d'éligibilité doit être vérifiée dans le processus d'homologation ou validée en gouvernance technique (§ 1.9.2 Processus de saisine pour validation d'architecture ou dérogation au CCT)

☆☆☆☆

L'ajout d'un nouveau module est soumis à vérification préalable des critères évoqués ci-dessus.

En conséquence, pour les CMS non infogérés, la conformité des modules aux critères d'éligibilité doit avoir été vérifiée dans le processus d'homologation ou validée en gouvernance technique.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Portails	Drupal	Opensource	Pour une utilisation orientée portail de communication	★ / ★	Internet Intredef
Portails	Joomla!	Joomla!	Pour une utilisation orientée portail de communication	★ / ★	Internet Intredef
<i>Commentaire : Drupal permet la mise en place d'un CMS de type Headless. Ce type de solution vise à découpler le système front-office de présentation des données à l'utilisateur, des données créées et stockées en back-office. Dans cette logique, le back-office expose une API suceptible d'être consommée par différents front-office, permettant ainsi de faciliter la diffusion d'un même contenu sur différents types de canaux et supports.</i>					
Portails	WordPress	Opensource	Pour une utilisation orientée portail de communication	★ / ★	Intredef SIA S-SF SIA FrOPS
<i>Commentaire : le recours à WordPress est assujéti à une demande de dérogation justifiant d'usages non couverts par les produits listés ci-dessus. Le choix des modules déployés doit respecter les critères affichés au chapitre 8.6.2</i>					
Portails	Alfresco Community Edition	Hyland	Pour une utilisation nécessitant des fonctionnalités avancées de travail collaboratif ou d'intégration applicative	★ / ★	Min Arm
Portails	Nuxeo	Hyland		★ / ★	Min Arm
Portails	SharePoint	Microsoft	Pour une utilisation nécessitant des fonctionnalités avancées de travail collaboratif ou d'intégration applicative. NB : embarque nécessairement une base de données SQL Server	★ / ★	Intredef SIA S-SF SIA FrOPS
Mesure d'audience	Matomo	Matomo	Utilisation On Premise, permet de garder la maîtrise des données d'audience	★ / ★	Min Arm

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

Se reporter également à l'annexe **8.6.3 Critères d'éligibilité pour des modules de CMS**

3.3.2.3 Création de sites Web [CSW]

Pas de référence identifiée à ce jour.

3.3.2.4 Gestionnaire de métadonnées [GMD]

Les deux piliers la gestion des métadonnées est:

- Le catalogue des métadonnées ministériel (metadatarm), outil d'« Entreprise Metadata Management » dans la mesure où il ne stocke pas de données mais seulement les métadonnées qu'il « administre » ;
- La gestion des données de référence et de mise en qualité (PGDR).

Ce catalogue des données ministériel doit devenir la référence permettant principalement de (liste non exhaustive des fonctions attendues) :

- Disposer d'une vue exhaustive et concaténée des différents gisements de données, qu'ils soient centralisés ou décentralisés (vues collaboratives) ;
- Réaliser des recherches par mots clés sur ces données pour vérifier leur existence et consulter leurs métadonnées, notamment pour savoir où elles sont stockées, qui en est responsable et leur sensibilité ;
- Découvrir le patrimoine informationnel du ministère par une aide automatique de découverte ;
- Savoir gérer des profils d'utilisateurs différents et leur donner accès à des vues liées à ces profils et droits afférents ;
- Disposer d'un lignage de données afin de visualiser l'ensemble de la vie d'une donnée ;
- Disposer d'un tableau de bord de suivi des métadonnées ;
- Constituer et mettre à disposition en centralisé et décentralisé des glossaires et dictionnaires de données.

Le service de catalogue de données ministériel « MétadatARM » est ouvert depuis le 10 mars 2025.

3.3.2.5 Syndication de contenu [ASY]

Pas de référence identifiée à ce jour.

3.3.2.6 Répertoires partagés [REP]

Ce service est fourni sur l'Intredef ainsi que sur le S-SF et le SIA FrOps (métropole et configuration projetable). Un recours aux répertoires partagés demeure possible dans la mesure où elles autorisent des fonctionnalités avancées de gestion des droits, de recherche et d'affichage n'impliquant pas le recours à des actes techniques d'administration. Compte tenu du coût de maintenance et d'exploitation dans la durée induite par ce type de service, cette solution n'est pas recommandée.

3.3.2.7 Moteur de recherche [RMR]

Le service utilisateur associé est décrit en §3.1.3.4 *Moteur de recherche [SU-RMR]*

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Moteur recherche	Qwant	Qwant	Moteur de recherche préservant les données utilisateurs dont l'usage est encouragé par le gouvernement.	R / -	Internet
Moteur recherche	SYRIARM	AND	Solution ministérielle basée sur Sinequa	R / S	Intredef
<i>Commentaire : l'utilisateur est automatiquement connecté à chaque fois que c'est possible (hors OPEX ou exercice) pour étendre les résultats à des données non publiques selon le droit d'en connaître.</i>					
Moteur recherche	SINEQUA	Sinequa	Toute solution utilisant SINEQUA en dehors de la solution ministérielle est soumise à dérogation.	A / S	Intredef SIA S-SF SIA FrOps

3.3.2.8 Gestion des communautés d'intérêt [COI]

Le service utilisateur associé est décrit en §3.1.2.2 Espace de travail collaboratif [SU-EDT]

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Travail collaboratif	SharePoint Server Enterprise	Microsoft		★ / ★	Tout Intranet
Travail collaboratif	Alfresco Community Edition	Hyland		★ / ★	Min Arm
Travail collaboratif	Nuxeo	Hyland		★ / ★	Min Arm
Travail collaboratif	OSMOSE	DINUM	Proposée par la DINUM, la plateforme Osmose permet aux agents de l'État et de ses établissements publics d'animer en ligne une communauté professionnelle. URL : https://osmose.numerique.gouv.fr	R / S	Internet
Travail collaboratif	RESANA	DINUM	Destinée aux agents de l'État, la plateforme collaborative interministérielle Resana leur offre un espace numérique complet pour faciliter le stockage, le partage et la coédition de documents, mais aussi le travail en équipe et en mode projet, y compris en mobilité grâce à une application dédiée. URL : https://resana.numerique.gouv.fr	R / S	Internet
Travail collaboratif	OnlyOffice	Ascensio System SIA		D / N	Min Arm
<i>Commentaire : Suite au NeMO DPID n°2025/554 du 01/12/2025, l'intégration de ONLYOFFICE dans le système d'information du Ministère est proscrite pour les nouveaux projets. Pour les systèmes qui auraient déjà implémenté ONLYOFFICE, il est impératif de chercher une alternative et de décommissionner ce produit avant fin 2026.</i>					

3.3.2.9 Réseau social d'entreprise [RSE]

Le service utilisateur associé est décrit en §3.1.2.7 Réseau social [SU-RSE]

3.3.2.10 Enquête et sondage [ENQ]

Le service utilisateur associé est décrit en §3.1.3.5 Enquête et sondage [SU-ENQ]

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Enquêtes-Sondages	SHERLOCK	SGA	Solution ministérielle basée sur Limesurvey	R / S	Intredef
Enquêtes-Sondages	Limesurvey	Limesurvey	En cas d'impossibilité d'utiliser la plateforme ministérielle	★ / ★	Internet Intradef
Enquêtes-Sondages	Isidate	DGA	Outil de sondage pour recherche d'une date	R / S	Intradef

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

3.3.3 Travail de groupe

Service utilisateur associé : cf. 3.1.2.1 Communication instantanée ainsi que la partie client.

3.3.3.1 Messagerie instantanée – Réunion virtuelle – Vidéoconférence - Rédaction collaborative synchrone [MIN-REV-VIH-RCS]

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Communications instantanées	Skype for business Server	Microsoft		★ / ★	Intradef SIA S-SF SIA FrOPS
Communications instantanées	Lync (serveur couplé au client Lync)	Microsoft	Solution obsolète (remplacement par Skype)	I / -	Min Arm
Communications instantanées	TCS (solution serveur basé sur openfire, couplé au client JChat)	NCIA	Solution de chat opérationnelle nativement interopérable avec l'OTAN	A / S	Intradef SIA S-SF SIA FrOps
Communications instantanées	Prosody	Equipe Prosody	Assujéti au contexte SIE : Serveur XMPP sous licence libre MIT utilisée dans le cadre du SIE	A / S	SIE
Communications instantanées	Tchap	DINUM	Solution de chat sécurisé interministériel Soutien DINUM	R / -	Internet
Communications instantanées	WEBEX Version entreprise	Cisco	Solution de visio/toip (S-SF / SIA FrOps / Mission Secret...). S'adosse à des équipements de télévisioconférence. (Client Jabber standard).	A / N	SIA S-SF SIA FrOps
Communications instantanées	VVIPER	AND	Solution de visio/toip (S-SF). Déploiement envisagé sur SIA FrOps. Soutien via une TME	E / S	S-SF
Plateforme de collaboration	NextCloud	NextCloud GmbH	L'assujétissement porte sur les plugins NextCloud	★ / ★	Min Arm

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits***

3.3.3.2 Wiki [WKI]

Le service utilisateur associé est décrit au **§3.1.2.3 Wiki [SU-WKI]**. La gouvernance technique ne recommande aucun produit particulier, cependant il est désormais préconisé de recourir aux solutions de wiki compatibles du langage Markdown pour ses possibilités de normalisation et d'interopérabilité. Les solutions mentionnées ci-après demeurent celles principalement déployées au sein du Ministère.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Wiki	Mediawiki		Déployé pour wikidéfense et dans TULEAP, recommandé dans le SILL 2020	★ / ★	Intradef
Wiki	DokuWiki	Communauté DokuWiki	Assujéti au contexte SIE : Déployé dans le cadre du SIE	A / S	SIE
Wiki	xWiki	xWiki SAS		★ / ★	Min Arm

3.3.3.3 Forum [FOR]

Le service utilisateur associé est décrit au §3.1.2.5 **Forum [SU-FOR]** ainsi que la partie client, un forum pouvant être mis en place, de façon intégrée avec les outils collaboratifs.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Forum	PhpBB		Déployé actuellement assez largement (Marine Nationale, Armée de Terre...)	★ / ★	Intradef

3.3.4 Services d'annuaires [ANN]

Les annuaires s'inscrivent dans la démarche menée au niveau ministériel autour de la « gestion des identités numériques et des accès », plus connue sous l'acronyme anglais IAM (pour identity and access management). Cette démarche est portée par le projet d'ensemble « Identités Numériques et Autorisations » [INA] (cf. §4.6.1.1 **Démarche INA : RIN**) présentant une architecture à trois niveaux :

- au niveau ministériel, un référentiel des identités numériques [RIN] contenant les données communes à tous les intranets du ministère relatives aux données d'identités des personnes ; l'Annudef sur l'Intradef fait aujourd'hui fonction de référentiel ministériel ;
- sur chaque intranet, le RIN sert de base à la constitution d'un référentiel d'intranet (RIAxxx) avec l'adjonction de données spécifiques au niveau d'intranet (adresse électronique, certificats, organisation...) ou de données permettant aux applications de gérer les autorisations ;
- enfin ces référentiels d'intranet servent de point d'alimentation et d'adossement des annuaires techniques nécessaires au fonctionnement des services, des applications et du composant MindefConnect de l'intranet concerné.

La constitution de ces annuaires fait l'objet du projet SI INA mené dans le cadre de la démarche INA.

Le webservice Personnes fourni par INA, équivalent du webservice User_info d'Annudef, sera disponible pour l'été 2026 sur C1DR.

3.3.4.1 Annuaires / référentiels

Document	Date	Origine	Type doc	Portée
Directive DGSIC n° 2 portant sur le système d'annuaires du ministère de la Défense (publié au BOA sous la référence BOC n°17 du 19 juillet 2007, texte 1)	9 mars 2007	DGSIC	Directive	Min Arm
<i>Commentaire : directive de portée générale (LDAP, schéma d'annuaire, ...).</i>				
Directive de nommage des annuaires : note n°D-12-005368/DEF/EMA/CPI/SIA/NP du 12 juin 2012	12 juin 2012	EMA	Note	Min Arm
<i>Commentaire : mise en forme des informations d'annuaire et des adresses de messagerie électronique. A plusieurs textes définissent les règles de nommage d'annuaire notamment pour la levée d'homonymie, les notions d'organisme (directive DGSIC, n°2 et n°3, directive de nommage des annuaires EMA, RGI, concept d'emploi pages jaunes/pages blanches...). Un travail de mise en cohérence de ces textes doit être mené pour lever toute ambiguïté et préciser le texte applicable.</i>				
Directive DIRISI/SCOE n° 53 « Gestion des adresses fonctionnelles et listes de diffusion dans l'Annudef » version 2 (cf. 3.1.1.7.1 Messagerie non officielle)	28 aout 2013	DIRISI	Directive	Min Arm
<i>Commentaire : déjà cité dans le chapitre sur les messageries, la directive précise notamment les modalités d'association des adresses fonctionnelles aux adresses personnelles sur l'Intradef</i>				
Schéma d'annuaire des Intranets de la Défense v2.5.1 (n°2025/809/ARM/CND/FAB NUM/POCIP/DR du 17 novembre 2025)	17 nov. 2025	POCIP	Référentiel	Min Arm
Catalogue des OID de la défense v2.6.1 (n°2025/165/CND/GOUV STRAT/DR du 10/12/2025)	17 nov. 2025	POCIP	Référentiel	Min Arm

<i>Commentaire : catalogue des OID spécifiques défense associés.</i>				
ACP133 (D) Common Directory Services and Procedures – Juillet 2009 ACP 133 SUPP-1 (A) Common Directory Services and Procedures Supplement – Juillet 2009	Juillet 2009	OTAN/CCEB	Référentiel	OTAN

Référentiel d'Identités Numériques [RIN]

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Annuaire	RIN : référentiel ministériel des Identités Numériques	Min Arm	À terme, le Ministère disposera d'un seul référentiel d'identités entretenu par le SI INA pour tous les intranets	R / E	Intradef
<i>Commentaire : présentation du service de gestion des identités et accès SI INA cf. 4.6.1.1 Démarche INA : RIN</i>					

Référentiel d'annuaires par intranet

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Annuaire	Annudef	Min Arm	Le rôle du RIN est tenu actuellement par l'annuaire référent de l'intranet sensible (Annudef). À terme l'Annudef sera remplacé par le RIADef, extraction du RIN pour l'Intradef.	R / S	Intradef
Annuaire	RIADef : Référentiel d'Identités et d'Autorisations du ministère	Min Arm	À terme, le ministère disposera d'un référentiel d'identités et des données d'autorisations entretenu par le SI INA sur Intradef	R / E	Intradef
Annuaire	OpenLDAP : annuaire de référence Annubat : interface de consultation	Min Arm	Solution déployée dans le cadre du SIE	R / S	SIE
Annuaire	OpenLDAP : Annuaire de référence MEIBO : gestion de contenu	Min Arm	Solution SIA S-SF pour la métropole. Solution également pour le fédérateur Intraced	R / S	SIA S-SF SIA FrOps
Annuaire	OpenLDAP : Annuaire de référence	Open Source	Solution SIA S-SF pour le théâtre	★ / ★	SIA S-SF SIA FrOps

3.3.4.2 Annuaire techniques de ressources

Document	Date	Origine	Type doc	Portée
Directive technique sur la gestion des comptes dans un annuaire et application à un Active Directory V1.0	28 juin 2012	DGSIC	Directive	Min Arm
<i>Commentaire : directive relative aux règles de sécurité à observer dans la gestion des comptes Active Directory</i>				
Points de contrôle Active Directory du 02 juin 2020 : "CERTFR-2020-DUR-001" https://www.cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/	16/11/2022	CERT	Note technique	Toute admin.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Annuaire technique	Active Directory	Microsoft		★ / ★	Intradef SIA S-SF SIA FrOPS

Annuaire technique	OpenLDAP	OpenLDAP project	.	★ / ★	Min Arm
--------------------	----------	------------------	---	-------	---------

3.3.4.3 Outils de « provisionning » d'annuaires

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Provisionnement Annuaire	MEIBO	ILEX	SIA S-SF métropole	★ / ★	SIA S-SF SIA FrOps
Provisionnement Annuaire	Solution ministérielle INA	Min Arm	Solution ministérielle de gestion des identités numériques basée sur le produit USERCUBE. Cette solution est en cours de réalisation et doit permettre de constituer le RIN et les RIAxxx d'intranets.	R / E	Intredef

3.3.5 Utilitaires d'infrastructure

3.3.5.1 Serveurs d'impression – numérisation [IMP]

Cf. 3.1.3.3 Impression – édition multifonction [SU-IMP]

3.3.5.2 Diffusion audio-video [DAV]

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Streaming Video	Deftube	Min Arm	Solution ministérielle construite autour des produits Ubcast	R / S	Intredef

Commentaire : seule l'instance Deftube est autorisée pour publier sur l'intredef des supports vidéo.

3.3.6 Services communs réseau

3.3.6.1 Nommage DNS⁴⁶[NOM]

Nommage sur l'Internet : le CND exploite pour les besoins ministériels sur Internet deux domaines DNS « defense.gouv.fr ». La gestion des sous-domaines se fait au travers du marché ASTEL-I. À noter que les adresses professionnelles sur Internet sont en « def.gouv.fr » et gérées au travers d'un lot du marché ASTEL-I.

Document	Date	Origine	Type doc	Portée
Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine v1.3	10 novembre 2017	ANSSI	Note technique	Toute admin.

Nommage sur l'Intredef : La mise en place de l'Intredef modernisé a conduit à la création d'un nouveau domaine « intradef.gouv.fr » autorisé par le SIG (Service d'Information du Gouvernement) en 2009. L'ancien domaine « defense.gouv.fr » perdure pour des cadres d'emploi spécifiques .

Document	Date	Origine	Type doc	Portée
Guide EMO.GUI.R4.016 « Nommage DNS » V1.2	01/07/2025	DIRISI	Guide	Tout intranet

⁴⁶ DNS : Domain Name System

<i>Commentaire :</i>				
Directive DIRISI n°101 d'exploitation du DNS (Intredef) v1.0 diffusée par note n°923571/DEF/DIRISI/SCOE/EXP/NP du 12 juillet 2013	12 juillet 2013	DIRISI	Directive	Intredef
<i>Commentaire : cette directive présente l'architecture technique globale du service DNS ainsi que les éléments relatifs à l'exploitation des services du DNS de l'Intredef. Cette directive ne traite que de l'exploitation du DNS dans l'espace de confiance (Intredef modernisé) tant dans le domaine « intradef.gouv.fr » que « defense.gouv.fr ». Elle ne traite pas de l'exploitation des chaînes DNS historiques des organismes, ni des organismes hors de l'espace de confiance.</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
DNS	Windows Server (service DNS)	Microsoft	Dans le cadre de STC-IA, utilisé pour la résolution des adresses de ressources référencées dans Active Directory.	★ / ★	Min Arm
DNS	Bind	Internet Systems Consortium	Pour la résolution des adresses des composants hors STC-IA.	★ / ★	Intredef SIA S-SF SIA FrOPS

3.3.6.2 Synchronisation horaire [SYN]

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°24 portant sur le service de synchronisation horaire au standard IP publiée au Bulletin Officiel des Armées	09 mars 2012	DGSIC	Directive	Min Arm
<i>Commentaire : règles d'usage et de mise en œuvre de la synchronisation horaire des réseaux IP de la défense. Périmètre : tous les intranets.</i>				
Guide Service NTP (Diffusion Restreinte) EMO.MOD.R4.035-v1-01 version 1.0	01/04/2025	DIRISI	Guide	Min Arm

Pour les directions d'application : les applications doivent se synchroniser sur l'architecture de synchronisation horaire ministérielle mise en place par le CND (pour l'Intredef, cf. la directive supra).

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Synchro Horaire	NTP	Meinberg	Client & serveur Meinberg. Sur les configurations projetables.	A / N	Intredef SIA S-SF SIA FrOps
<i>Commentaire : mise en œuvre dans le cadre de STC-IA et sur certains réseaux isolés</i>					
Synchro Horaire	Ntpd/Chronyd	Natif	Sur les OS Linux	R / S	Min Arm

3.3.6.3 Adressage - DHCP [ADR]

Cf. §4.6.1.5

3.3.6.4 Marquage des flux réseaux [MQR]

Cf. 5.2.1.3

3.3.6.5 Transfert fichiers volumineux [TFV]

Le service utilisateur associé est décrit au §3.1.4.2 Transfert de données volumineuses [SU-TFV].

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Transfert de données volumineuses	Defense Drive	Min Arm	Solution CND sur la base du produit OODRIVE	R / -	Tout intranet
Transfert de données volumineuses(serveur)	Skype	Min Arm	Assujetti à l'usage de la messagerie instantanée	★ / ★	Intredef
Transfert données volumineuses	Pydio Cells	Pydio	Solution de partage de fichiers en web.	R / S	Internet
Transfert données volumineuses	France Transfert	Dinum	Echanges Internet-Internet de fichiers NP uniquement entre individus	R / -	Internet

3.3.7 Systèmes d'exploitation [OS]

Cf. §5.1.1 Système d'exploitation [OS]

3.4 Services de sécurité

Cf. §4.6 Services de sécurité

3.5 Services d'administration et de gestion

Cf. §6.2 Opérations – processus

4 SECURITE

4.1 Documents de référence

4.1.1 Document généraux

4.1.1.1 Politiques de sécurité des systèmes d'information

Document	Date	Origine	Type doc	Portée
Circulaire n°6095/SG relative à l'organisation gouvernementale pour la gestion des crises majeures	01/07/2019	PM	Circulaire	Toute admin.
Circulaire n° 6290/SG relative aux actions à engager pour renforcer la cybersécurité de l'État.	15/07/2021	PM	Circulaire	Toute admin.
Décret n°2022-513 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics	08/04/2022	PM	Décret	Toute admin.
Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle no 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics	26/10/2022	PM	Arrêté	Toute admin.
Politique de sécurité des systèmes d'information du ministère de l'État (PSSIE) diffusée par circulaire du premier ministre n°5725/SG du 17 juillet 2014	17 juillet 2014	PM	Circulaire	Toute admin.

Politique de sécurité des systèmes d'information du ministère de la défense [PSSIM] : instruction ministérielle n°7326/DEF/CAB du 25 juin 2018	25 juin 2018	DEF/CAB	IM	Min Arm Tutelles
<i>Commentaire : la PSSIM prend en compte la PSSI de l'État. Ce document fixe les orientations stratégiques de la SSI, et définit les règles techniques et opérationnelles de SSI à respecter en les renvoyant éventuellement à des instructions et directives techniques correspondantes. Elle est complétée d'un volet technique (cf. ci-dessous) dont des mises à jour sont actuellement en préparation. Par ailleurs, la nouvelle politique ministérielle de sécurité numérique (PMSN) est actuellement en cours de rédaction. Elle sera composée de trois volets : stratégique, organisationnel et technique.</i>				
Volet technique de la politique de sécurité des systèmes d'information [PSSIM-T] : instruction ministérielle n°7326-2/DEF/CAB Edition 2 diffusée par note n°2475 du cabinet le 21 juillet 2021	21 juillet 2021	DEF/CAB	IM	Min Arm Tutelles
<i>Commentaire : ce document définit un socle de mesures répondant aux orientations stratégiques de la PSSI ministérielle. Il tient compte notamment de la PSSIÉ, de l'IGI1300 et de II901.</i>				

4.1.1.2 OIV/OSE

4.1.1.2.1 Opérateur d'importance vitale

Document	Date	Origine	Type doc	Portée
Arrêté du 22 mars 2021 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité, relatives au sous-secteur d'activités d'importance vitale « Activités militaires de l'État ».	22/03/2021	PM	arrêté	AME
Arrêté du 8 septembre 2017 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Activités industrielles de l'armement »	08/09/2017	PM	arrêté	ID

4.1.1.2.2 Opérateur de services essentiels

Document	Date	Origine	Type doc	Portée
Décret 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des OSE et des fournisseurs de service numériques	23/05/2018	PM	Décret	Toute admin
Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n°2018-384 du 23 mai 2018	14/09/2018	PM	Arrêté	Toute admin

4.1.1.3 Droits et obligations des usagers et des administrateurs

Document	Date	Origine	Type doc	Portée
Instruction n°2003/DEF/DGSIC portant code de bon usage des systèmes d'information et de communication du ministère de la Défense.	20 novembre 2008	DGSIC	Instruction	Min Arm
Instruction n°2004/DEF/DGSIC relative à la fonction d'administrateur de systèmes d'information et de communication au sein du ministère de la Défense	14 décembre 2009	DGSIC	Instruction	Min Arm

4.1.1.4 Protection du secret

Document	Date	Origine	Type doc	Portée
Instruction générale interministérielle n°1300 portant sur la protection du secret de la défense nationale	09 août 2021	ARM/CAB	Arrêté	Toute admin.
<i>Commentaire : cette nouvelle IGI 1300 remplace l'IGI300 du 13 novembre 2020.</i>				
Instruction ministérielle n°900/ARM/CAB portant sur la protection du secret et des informations diffusion restreinte et sensibles	15 mars 2021	ARM/CAB	Instruction	Min Arm
<i>Commentaire : une nouvelle version est à la publication.</i>				
Note n°508/DEF/EMA/PAC/NP relative à la politique des armées en matière de sensibilité des informations opérationnelles (cf. 2.3 Le cadre ministériel)	9 juin 2009	EMA	Note	Armées

4.1.1.5 Protection des données à caractère personnel (RGPD, CNIL ...)

Différents fichiers informatiques sont soumis au régime juridique de protection des données à caractère personnel. Ces données sont celles qui concernent les personnes physiques et celles qui permettent de l'identifier directement ou indirectement (informations nominatives, images, voix notamment).

Document	Date	Origine	Type doc	Portée
RGPD : règlement général sur la protection de la donnée : Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (cf. 2.1.2 Européen)	27 avril 2016(application à compter du 25 mai 2018)	Union Européenne	Règlement	Union européenne
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	6 janvier 1978	Ministères	Loi	Toute admin.
Dispositions relatives à l'agrément « hébergement des données de santé » : article L. 1111-8 du code de la santé publique; articles R. 1111-8-8 et suivants du code de la santé publique.		MSS	Loi et décret	Toute admin.
Décret n°2019-536 du 29 mai 2019 en application de la loi Informatique et Libertés, Décret n°2007-914 du 15 mai 2007 en application de la loi Informatique et Libertés; Décret n°2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification	29 mai 201915 mai 200719 avril 2019	PM	Décrets	Toute admin.
<i>Commentaire : le 2ème décret liste les traitements automatisés de données à caractère personnel intéressant la sûreté de l'État, la défense ou la sécurité publique. Le 1er explicite l'ensemble du dispositif CNIL et les procédures afférentes en déclinaison du RGPD. Le 3ème décret apporte des précisions concernant les conditions spécifiques de traitement du numéro d'identification au RNIPP (répertoire national d'identification des personnes physiques) ou numéro de sécurité sociale et notamment les catégories de responsables de traitement et les finalités des traitements qui sont autorisés à l'utiliser par principe, les acteurs qui ne sont pas dans cette liste ne peuvent pas l'utiliser.</i>				
Instruction ARM/SGA/DAJ/D2P/DPSP relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense .	31 janvier 2020	Min Arm/DAJ	Instruction	

<i>Commentaire : l'instruction précise la mise en œuvre du RGPD au sein du ministère des armées. Elle ne traite pas l'ensemble des problématiques relatives à la mise en œuvre des textes relatifs à la protection des données personnelles.</i>				
Note n°20236 ARM/CAB relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère des armées	18 juillet 2018	Min Arm/	Note	
Décret n°2018-932 du 29 octobre 2018 modifiant les dispositions du code de la défense relatives à la sécurité des traitements de données à caractère personnel comportant la mention de la qualité de militaire	29 octobre 2018	Min Arm	Décret	Toute admin.
<i>Commentaire : ce texte entré en vigueur le 1er avril 2019, porte modification du code de la défense, et décline des dispositions du RGPD pour les traitements de données à caractère personnel dont la finalité exige, outre les données d'identification, la collecte d'au moins une donnée révélant, à sa seule lecture, la qualité de militaire.</i>				
Arrêté du 7 avril 2011 relatif au respect de l'anonymat de militaires et de personnels civils du ministère de la défense modifiée par l'arrêté du 7 mai 2020 portant actualisation de deux arrêtés relatifs au respect et à la préservation de l'anonymat de militaires et de personnels civils du ministère des armées	7 mai 2020		Arrêté	Min Arm
<i>Commentaire : cet arrêté précise la liste des services ou unités dont les missions exigent le respect de l'anonymat des militaires et civils qui y sont affectés.</i>				
Arrêté du 27 janvier 2023 autorisant la mise en œuvre de traitements automatisés de gestion des traces relatives aux systèmes d'information et de communication du ministère de la défense	27 janvier 2023	Min Arm	Arrêté	Tout intranet
<i>Commentaire : les devoirs de ces personnels sont rappelés dans l'instruction ministérielle n°2004 (cf. 4.1.1.3 Droits et obligations des usagers et des administrateurs).</i>				

4.1.2 Références pour le non classifié (NP-DR-sensible) et le NR

Document	Date	Origine	Type doc	Portée
Instruction interministérielle n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles	11 février 2015	ANSSI	Instruction	Toute admin.
<i>Commentaire : cette instruction ministérielle complète l'IGI 1300 et la PSSIE en instaurant des règles relatives à la protection des systèmes d'information sensibles ou diffusion restreinte. Elle doit être rendue applicable dans les contrats d'externalisation.</i>				
Document AC/35-D/1034 relatif à la protection des informations NATO RESTRICTED : document diffusé le 25 mai 2005.	25 mai 2005	OTAN	Document international	Toute admin.
<i>Commentaire : ce document décrit les éléments de politique de sécurité, les orientations et exigences à appliquer aux informations « NATO RESTRICTED »</i>				

Pour en savoir plus : <https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-secret-de-la-defense-nationale/accords-generaux-de-securite>

4.1.3 Références pour le niveau Secret

Document	Date	Origine	Type doc	Portée
Guide n°972/SCSSI/SI relatif à la protection des supports classifiés de défense.	9 avril 1998	PM	Guide	Toute admin.
<i>Commentaire : ce document traite de la protection, manipulation et destruction des supports d'information tels que disques durs, clé USB, carte à puce,</i>				
Guide technique 972-1 pour la confidentialité des informations enregistrées sur disque dur à recycler ou exporter sous timbre n°972-1/SGDN/DCSSI du 17 juillet 2003	17 juillet 2003	PM	Guide	Toute admin.
<i>Commentaire : ce guide précise le guide 972 dans son chapitre 8 relatif à l'effacement d'un support pour recyclage interne. Il s'applique aux supports magnétiques d'informations classifiées de défense ou d'informations sensibles non classifiées de défense.</i>				

4.1.4 Référence pour le SO

Document	Date	Origine	Type doc	Portée
Document AC35-D1002-REV5 Liste des équivalents nationaux des classifications de sécurité OTAN : document diffusé le 6 octobre 2010	6 octobre 2010	OTAN	Document international	Toute admin.
Accord entre l'Union Européenne et l'Organisation du Traité de l'Atlantique Nord sur la sécurité des informations du 14 mars publié au JOUE du 27 mars 2003	14 mars 2003	UE-OTAN	Accord international	Toute admin.

4.1.5 Références pour le SUE

Document	Date	Origine	Type doc	Portée
Accord relatif à la protection des informations classifiées échangées dans l'intérêt de l'Union européenne publié au journal officiel de l'union européenne du 8 juillet 2011	4 mai 2011	UE	Accord	Toute admin.
<i>Commentaire : aux termes de cet accord, les États membres prennent toutes les mesures appropriées pour que le niveau de protection accordé aux informations classifiées de l'UE soit équivalent à celui qui est accordé par la décision 2011/292/UE du Conseil de l'UE</i>				

4.1.6 Références pour la protection des informations avec les Nations Unies

Il n'existe pas d'accord de sécurité avec les Nations Unies pour la protection des données classifiées. L'échange de données classifiées n'est donc en théorie pas possible.

D'un point de vue pratique, en l'absence d'accord de sécurité, il est difficile de définir des équivalences de classification. Si un traitant doit utiliser ou transmettre des informations sensibles de l'ONU, il lui appartient de déterminer le niveau de protection à accorder aux informations, en fonction de leur nature.

Il pourra également se référer aux instructions relatives à la sensibilité, à la classification et à la gestion des informations de la section des archives de l'ONU, pour la protection des données classifiées de l'ONU.

Document	Date	Origine	Type doc	Portée
Boîte à outils consacrée à la gestion de l'information confidentielle	26 avril 2010	SARM – DM (ONU)	/	Toute admin.

Commentaire : document édité et réalisé par la Section des Archives et du Records Management (arms@un.org) et l'unité de gestion de l'information relative au maintien de la paix (peacekeepingimu@un.org). Remarque : la même version en langue anglaise intitulée Information Sensitivity Toolkit éditée le 24 février 2010 est également disponible.

4.1.7 Accès à la documentation technique

Les réglementations techniques internationales (OTAN, UE) sont soumises à des traités et des accords de sécurité particuliers.

4.2 Démarche de sécurité

Document	Date	Origine	Type doc	Portée
Guide des clauses de sécurité des systèmes d'information types à intégrer dans les marchés publics , diffusé par lettre n°DAE-2019-10-11495 du 13 novembre 2019	Juillet 2019	DAE - ANSSI	Guide	Toute admin.
Guide d'achat de produits de sécurité et de services de confiance conformément à la politique de sécurité des SI du ministère de la défense , diffusé par lettre n° 732/DEF/DGSIC/FSSI/NP du 17 novembre 2014	17 novembre 2014	DGSIC	Guide	Min Arm
<i>Commentaire : la PSSI ministérielle en déclinaison de la PSSI de l'État fait obligation à l'autorité d'homologation de la sécurité d'un système d'information d'identifier les produits et services qui doivent être de confiance. Ce guide explique les modes de mise en application de ces dispositions.</i>				
Guide DGSIC n°14 sur la typologie des attaques informatiques et les contre-mesures possibles , diffusé par lettre n° 113/ARM/DGSIC/DG/NP du 7 mars 2018	7 mars 2018	DGSIC	Guide	Min Arm
<i>Commentaire : ce guide a pour objectif d'aider un responsable de la sécurité des systèmes d'information (RSSI) ou un responsable de conduite de projet (RCP) à mieux comprendre les menaces qui pèsent sur leur SI, en présentant les différentes méthodes d'attaques génériques qui viennent ponctuer l'actualité du numérique et en explicitant les liens avec les menaces types de la méthode d'analyse de risques du ministère.</i>				
Guide ministériel de bonnes pratiques contractuelles dans le domaine du numérique édition 2	Janvier 2023	DGNUM	guide	Min Arm, acheteurs
<i>Commentaire : le guide constitue une aide de référence pour les acteurs de l'achat, tant pour les acheteurs que les conseillers juridiques. Il ne se substituera toutefois pas aux guides de bonnes pratiques adoptés par la voie réglementaire. Il traite notamment de la propriété intellectuelle, la protection des données (à caractère personnel et non personnelles).</i>				

4.2.1 Homologation

4.2.1.1 Généralités

L'autorité nationale de sécurité en matière de systèmes internationaux est le secrétariat général de la défense et de la sécurité nationale (SGDSN). Le SGDSN assure, en application des accords internationaux, la sécurité des informations classifiées confiées à la France (§ 7.2.1.3 de IGI 1300). Les homologations de sécurité des systèmes d'information correspondantes relèvent ainsi de sa responsabilité et sont instruites par l'Agence nationale des systèmes d'information (ANSSI). Toutefois, pour permettre au ministère des armées un fonctionnement amélioré, le SGDSN a délégué au CEMA un pouvoir d'homologation pour certains systèmes traitant des informations. Fondamentalement même si le formalisme et les réglementations à appliquer diffèrent, le principe reste toutefois le même, à savoir qu'une autorité responsable (SAA pour Security Accreditation Authority) atteste formellement que le niveau de sécurité requis pour le système d'information est atteint.

Le SGDSN, en tant qu'ANS⁴⁷, émet les instructions générales interministérielles relatives à la mise en application des dispositions des différents organismes internationaux. En matière de hiérarchie des normes, un traité international a valeur supérieure à la législation nationale.

4.2.1.2 Principes

La démarche d'homologation est une composante de la gestion de la sécurité réalisée tout au long du cycle de vie d'un système d'information. **Tout système doit être homologué.**

L'homologation est une des responsabilités de l'Autorité Qualifiée en SSI (AQSSI). Une AQ peut déléguer le suivi de la démarche ou les décisions d'homologation à une ou plusieurs Autorités d'Homologations (AH). La décision d'homologation de sécurité est l'acte formel par lequel l'AH certifie, après évaluation des risques et analyse des mesures de sécurité mises en œuvre, que la protection des informations du système est assurée au niveau requis. Elle est un préalable à l'autorisation d'exploitation.

4.2.1.3 Homologation nationale

Tout système d'information ne présente pas les mêmes enjeux de sécurité en matière de confidentialité des données, d'intégrité, de disponibilité et de criticité pour les missions du ministère. De plus, de nombreux SI ou applications sont hébergés sur les Intranets du ministère bénéficiant, par héritage, des services de sécurité apportés par ces réseaux.

Dans ces conditions, deux méthodes d'homologation permettent d'alléger le processus d'homologation : la démarche sommaire d'homologation et la démarche d'homologation simplifiée.

Document	Date	Origine	Type doc	Portée
Décision du 04 juillet 2024 n°503844/DEF/CAB/CM3/NP relative à la désignation des autorités qualifiées du ministère des Armées	04 juillet 2024	CABMIN	Note	Armées
Directive DGNUM n°27 portant sur l'homologation des systèmes d'information du ministère des Armées, 3ème édition diffusée par note n°DEP-00337/2022/ARM/DPID/NP du 7 juin 2022	07 juin 2022	DPID	Directive	Min Arm
<i>Commentaire : cette directive définit la politique à mettre en œuvre en matière d'homologation de sécurité pour les systèmes d'information (SI) au sein du ministère des armées. Elle fournit les critères de décision pour mener à terme toute démarche d'homologation, permettant ainsi d'identifier, d'atteindre, puis de maintenir un niveau de risque acceptable, tant du point de vue de la sécurité que des coûts. Elle concerne tous les systèmes d'information du ministère, quel que soit le niveau de sensibilité des informations traitées. La présente édition n°3 permet d'optimiser la documentation attendue et étend les cas d'usage présentés pour faciliter l'appropriation du dispositif d'homologation 2022.</i>				
Guide ministériel n°6 Ed.2 relatif aux données de caractérisation d'un système d'information diffusé par note n°372/DEF/DGSIC/SDSSI du 4 avril 2013	2 avril 2013	DGSIC	Guide	Min Arm
<i>Commentaire : ce guide fixe le cadre sémantique et documente la liste des valeurs permises pour les données chargées de caractériser un système d'information. Ce guide s'adresse principalement aux différentes directions de projet faisant appel à ces différents types de données.</i>				
Guide ministériel n°7 relative à l'intégration de la sécurité des systèmes d'information dans les projets de systèmes d'information, Ed-4. Diffusé par note 355/ARM/DGNUM/SDSN/NP	30 septembre 2022	DGNUM	Guide	Min Arm
<i>Commentaire : ce guide fournit aux RSSI, aux équipes de projet et aux centres d'experts des autorités d'homologation les éléments nécessaires à l'intégration de la sécurité numérique dans la vie des systèmes d'information, du stade d'initialisation, jusqu'au stade d'utilisation, puis de retrait de service. Cette 3ème édition se présente sous forme d'un recueil de fiches évolutives, propose des modèles de livrables et des</i>				

⁴⁷ ANS : Agence Nationale de Sécurité

outils, ainsi que de liens vers des référentiels utiles. Remarque : le présent guide ne concerne pas les opérations d'armement, les systèmes industriels ou les SI relevant de l'OTAN ou de l'UE. Cependant, les responsables de programmes d'armement peuvent s'y référer. La DGA dispose de son propre guide (Guide S-CAT n° 15 002 référencé ci-après)

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Pilotage des risques	Questionnaire d'évaluation initiale (QEI)	Min Arm	version 2.17	R / S	Min Arm
Commentaire : ce questionnaire, actualisé en 2021, constitue la toute première étape d'analyse de risque SSI recommandée par la directive ministérielle relative aux homologations. Par le biais d'une auto-évaluation, il offre un moyen simple de déterminer rapidement si un SI présente des enjeux de sécurité importants ou non. Cette auto-évaluation prend la forme de 15 questions attendant une réponse graduée de 0 à 3. La méthode de calcul proposée, quoique simple, applique les principes de la méthode d'analyse de risque EBIOS. Les 15 questions proposées couvrent globalement tous les aspects d'une analyse de risque EBIOS à savoir : / les besoins de sécurité, les impacts potentiels, l'importance des menaces potentielles et l'importance des vulnérabilités.					
Pilotage des risques	OARDHS	DGNUM	Outil d'analyse de risques pour une démarche d'homologation simplifiée. Outil sous Excel maintenu par la DGNUM Version du 19/03/2024	R / S	Min Arm
Commentaire : cet outil est proposé pour outiller la démarche d'homologation simplifiée. Il n'y a pas d'évolution prévue.					
Pilotage des risques	MAITRISK	Min Arm	Solution ministérielle de conduite des analyses de risques basée sur la suite EGERIE Risk Manager. Cf. Directive générale d'emploi DGNUM n°45 (ci-dessus)(*) soutien par TME	R / S(*)	Min Arm

4.2.1.4 Homologation interalliée

Document	Date	Origine	Type doc	Portée
AC35-D2004 (NSC)/ AC322-0052 (C3B) Rev 3 diffusée conjointement par le Nato Security Committee et le C3Board le 15 novembre 2013	15 nov. 2013	OTAN	Directive	Toute admin.
Commentaire : directive principale sur l'INFOSEC [Nato Unclassified]				
AC/35-D/1021-REV3 - Lignes directrices pour l'homologation de sécurité des systèmes d'information et de communication (SIC) : document diffusé le 31 janvier 2012	31 janvier 2012	OTAN	Guidelines	Tout SIC traitant d'infos. OTAN.
Commentaire : ce document donne les orientations sur les modalités requises et les processus mis en œuvre pour remplir la fonction d'homologation de sécurité des SIC traitant d'informations OTAN classifiées ou non. [Nato Non classifié]				
AC35-D1014-REV3 – Lignes directrices concernant la structure et le contenu de la procédure d'exploitation et de sécurité (SecOPS) des systèmes d'information et de communication : document diffusé le 31 janvier 2012	31 janvier 2012	OTAN	Guidelines	Toute admin.
Commentaire : ce document précise la structure et le contenu attendu d'une SecOPS et les attendus pour les catégories d'agents et de personnes concernés par l'utilisation des SIC (utilisateurs sur réseaux locaux, utilisateurs de moyens portables, utilisation par les visiteurs, autorités d'exploitation ou responsables de la gestion de la sécurité) [Nato Non classifié]				

4.2.1.5 Cas particuliers des systèmes industriels (dont SCADA)

Un système industriel est un système d'information commandant ou contrôlant automatiquement des dispositifs physiques à partir des données collectées par des capteurs. Il existe ainsi une interaction entre le monde virtuel et le monde réel.

Les systèmes industriels se sont rapprochés tardivement mais progressivement des standards du monde numérique et notamment du standard IP. Des systèmes hétérogènes ont ainsi été interconnectés dans un souci majeur de productivité, tout en cherchant à préserver la sûreté de fonctionnement mais sans attention pour la sécurité des systèmes d'information.

Davantage exposés, ces systèmes constituent désormais une cible privilégiée pour des cyber-attaquants car leurs actions peuvent avoir un impact direct sur nos intérêts vitaux (électricité, nucléaire, sanitaire, transport, ...) voire porter atteinte à l'intégrité des personnes.

Document	Date	Origine	Type doc	Portée
Directive n°39 relative à la sécurité des systèmes industriels (DIR S.INDUS)	9 juin 2023	DPID	Directive	Min Arm
<i>Commentaire : cette directive s'adresse principalement à tous les acteurs participant à la conception, la réalisation, l'exploitation des systèmes industriels, en particulier les personnes en charge des projets, les responsables d'opérations d'infrastructure mais également aux acteurs participant à leur maintien en condition de sécurité. Ces acteurs peuvent être du domaine cybersécurité ou de tous les domaines concourant à la vie des systèmes industriels.</i>				
Guide ANSSI relatif à la doctrine de détection pour les systèmes industriels	3 décembre 2020	ANSSI	Guide	Toute admin.
<i>Commentaire : ce guide présente :</i> • les grands principes de la supervision de la sécurité d'un système numérique ; • les particularités des systèmes industriels ; • la définition des périmètres de détection ; • les principes généraux de détection ; la définition des points de détection.				

4.2.2 Maintien en condition de sécurité

Le maintien en condition de sécurité (MCS) a pour objectif d'établir les procédures permettant de traiter les vulnérabilités ou incidents de SSI.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°143 portant sur le maintien en condition de sécurité (MCS) des postes de travail de l'Intradef (cf. 3.1.1.1 Poste de travail - CCB [SU-PC])		DIRISI	Directive	Armées

4.2.3 Audits

Document	Date	Origine	Type doc	Portée
Référentiel d'exigences applicable aux prestataires d'audit de la sécurité des systèmes d'information V2.1 [PASSI] (cf. 2.2.3 Les référentiels interministériels).	6 octobre 2015	ANSSI	Référentiel	Toute admin.
<i>Commentaire : le référentiel PASSI est constitutif du référentiel général de sécurité (RGSv2), cosigné de l'ANSSI et du SGMAP. Il est devenu applicable à la diffusion de celui-ci (1er juillet 2014). Les autorités administratives doivent recourir, notamment dans leurs appels d'offres à des prestataires d'audit conformes aux exigences de ce référentiel.</i>				

4.2.4 Réduction de l'exposition cyber des SI

Plusieurs axes d'effort sont envisageables par les DA/DP pour réduire l'exposition cyber des SI, et par voie de conséquence celle de l'environnement d'hébergement mutualisé :

- Veille des alertes de sécurité : cette étape nécessite un suivi des gestions de configuration des SI. Le SI Conformité, dans les environnements dans lesquels il est disponible (SHSM DR, à venir sur C1DR), répond actuellement à ce besoin en fournissant la liste des logiciels installés sur les serveurs, l'état des ressources systèmes consommées, les vulnérabilités actives, ainsi que les non conformités aux référentiels de sécurisation (et du présent cadre de cohérence technique). Cet outil est accessible à tous les acteurs (RSSI, RCP, ...) autorisés par leur DSI de rattachement
- Migration des SI vers le C1DR qui permet de bénéficier des fonctionnalités de sécurité, notamment apportées par la micro segmentation entre les SI hébergés, assurant ainsi une protection renforcée des risques de latéralisation d'attaque cyber, ou tout au moins d'effets de bord d'éventuels dysfonctionnements d'un SI sur les autres . Le portage des SI vers cette nouvelle infrastructure, nécessite une opération de transformation (MoveToCloud) des SI par les DA/DP. Ses avantages sont multiples et sont décrits sur le portail hébergement du CND .
- Recourir à chaque fois que possible à des frameworks recommandés plutôt qu'à des développements spécifiques, afin de bénéficier des mécanismes de sécurisation éprouvés qu'ils apportent (validation des entrées utilisateurs dans les formulaires par exemple).

4.3 Cryptographie et gestion des ACSSI

Cryptographie :

Document	Date	Origine	Type doc	Portée
RGS_B_1 Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. V2.03 (cf. 2.2.3 Les référentiels interministériels)	21 février 2014	ANSSI	Directive	Toute admin.
<i>Commentaire : document constitutif du RGS V2. Les règles et recommandations contenues s'adressent à un lecteur familier des concepts cryptographiques. Les concepts de base ne sont donc pas systématiquement rappelés.</i>				
RGS_B_2 Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. V2 (cf. 2.2.3 Les référentiels interministériels)	8 juin 2012	ANSSI	Directive	Toute admin.
<i>Commentaire : document constitutif du RGS V2. L'objectif de ce document est de présenter le cycle de vie d'une clé cryptographique et les différentes architectures de gestion de clés possibles. Ce document complète le document RGS_B_1 ci-dessus</i>				
RGS_B_2 Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. V2 (cf. 2.2.3 Les référentiels interministériels)	8 juin 2012	ANSSI	Directive	Toute admin.

Gestion des ACSSI – ACSSI non classifiés :

Document	Date	Origine	Type doc	Portée
Instruction interministérielle n°910 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI) sous timbre n°910/SGDSN/ANSSI du 22 octobre 2013	22 octobre 2013	ANSSI	Instruction	Toute admin.
<i>Commentaire : la directive 34 décline cette instruction sur le périmètre MINARM.</i>				

4.4 Protection contre les signaux compromettants

Document	Date	Origine	Type doc	Portée
Instruction interministérielle n°300/SGDSN/ANSSI du 23 juin 2014 relative à la protection contre les signaux compromettants	23 juin 2014	SGDSN	Instruction	Toute admin.
Répertoire n°490 des matériels évalués au plan de la protection contre l'émission SPC	20 juin 2016	ANSSI	Répertoire	Toute admin.
<i>Commentaire : ce document répertorie l'ensemble des matériels ou systèmes satisfaisant aux exigences de la norme SDIP-27 niveau A (TEMPEST), B ou C (raisonnement et conduction), ou zone 1 ou 2 en rayonnement au sens du zonage TEMPEST.</i>				

4.5 Sécurisation des COTS

Document	Date	Origine	Type doc	Portée
Procédure « Certification de sécurité de premier niveau des produits des technologies de l'information » (CSPN) diffusée sous timbre n°86/ANSSI/SDE/PSS/CCN du 13 janvier 2020	13/01/2020	ANSSI	Directive	Min Arm
Processus de qualification d'un produit v1.0	12/01/2017	ANSSI	Directive	Toute admin.
Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection v3.3	13/01/2020	ANSSI	Directive	Toute admin.
<i>Commentaire : les présentes procédures décrivent l'ensemble du processus de certification et de qualification de sécurité d'un produit, depuis la demande officielle par un commanditaire jusqu'à l'attribution d'un certificat pour le produit évalué, ainsi que le rôle de chacun des acteurs.</i>				

La sécurisation des systèmes d'information nécessite une bonne maîtrise de la configuration des composants logiciels qui les constituent. La mise en service d'un composant logiciel basé sur les options de configuration par défaut est déconseillée. Le déploiement de composants logiciels qui n'auraient pas fait, au préalable, l'objet de la réalisation d'un guide de configuration est à analyser comme une vulnérabilité potentielle dans le cadre de la démarche d'homologation.

Guides et notes techniques (ANSSI, DGA, etc.) :

Document	Date	Origine	Type doc	Portée
Guides et notes techniques ANSSI liés à des bonnes pratiques ou des solutions technologiques https://cyber.gouv.fr/publications		ANSSI	Guides	Toute admin.
<i>Commentaire : ces guides de bonnes pratiques, notes techniques ou méthodologiques sont en général liés à des thématiques. A titre d'exemple pour les 3 dernières années :</i> • <i>Recommandations de sécurité relatives aux déploiements de conteneur Docker (décembre 2019) ;</i> • <i>Profil de fonctionnalités et de sécurité – SAS et stations blanches (août 2020) ;</i> • <i>Guide des mécanismes cryptographiques (janvier 2020) ;</i> • <i>Guide de sélection d'algorithmes cryptographiques (mars 2021) ;</i> • <i>Recommandations pour la mise en oeuvre d'un site web : maîtriser les standards de sécurité côté navigateur (avril 2021) ;</i> • <i>Recommandations relatives à la sécurité des (systèmes d') objets connectés (août 2021) ;</i> • <i>Recommandations relatives à l'authentification multifacteur et aux mots de passe (octobre 2021) ;</i> • <i>Recommandations de sécurité pour l'architecture d'un système de journalisation (janvier 2022) ;</i> • <i>Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory (janvier 2022).</i> <i>Certains guides adressent des produits plus ciblés : commutateurs industriels Hirschmann et Siemens Scalance (février 2022), pare-feu Stormshield (avril 2021)...</i>				

4.6 Services de sécurité

4.6.1 Sécurisation des accès

4.6.1.1 Démarche INA : RIN – RIA-Def - MindefConnect

L'authentification a pour but de vérifier l'identité dont une personne se réclame. L'authentification est généralement précédée ou combinée avec une identification qui permet à cette personne de se faire reconnaître du système par un élément - l'identifiant - dont on l'a précédemment dotée.

Le référentiel d'identités du ministère est actuellement porté par Annudef sur Intradef mais se limite aux seules personnes ayant un accès à ce réseau. Il offre des services de pages blanches et de pages jaunes (il dispose également d'un webservice SOAP d'authentification désormais obsolète, non pérenne et par conséquent déconseillé : les projets y ayant recours doivent planifier rapidement les travaux nécessaires pour basculer sur une authentification MindefConnect Intradef) et de webservices SOAP d'accès aux informations sur ces personnes dans le respect du besoin d'en connaître.

Le projet d'ensemble INA vise à dégager une vision homogène et construite de la problématique de gestion des identités et des accès (IAM/IAG pour Identity and Access Management/Governance) pour le ministère des armées. INA vise à :

- rationaliser et sécuriser la gestion des identités numériques, dans le respect du RGPD, par la construction d'un Référentiel d'identités numériques (**RIN**) commun étendu aux agents civils, gendarmes, réservistes, candidats, pensionnés, ayant-droits, partenaires, militaires étrangers n'ayant pas vocation à disposer d'un compte Intradef ;
- simplifier l'administration des comptes utilisateurs en réduisant la charge administrative ;
- automatiser et centraliser la gestion de ces données afin d'en garantir l'exactitude et de minimiser les délais de mise à jour ;
- pour chaque intranet, simplifier la gestion des accès par l'installation d'un dispositif de fédération des moyens d'authentification (**MinDefConnect**) et d'un Single Sign On (SSO) ;
- pour chaque intranet, disposer d'un Référentiel des Identités et Accès de l'intranet considéré, à terme Référentiel des Identités et Autorisations (RIA-xxx) permettant de gérer et maîtriser les droits d'accès des utilisateurs aux applications, sous la forme de macro droits⁴⁸ selon le cycle de vie de l'identité numérique (entrée, parcours, sortie) : **RIA-Net** pour l'internet, **RIA-Def** pour l'Intradef, **RIA-Ced** pour le Secret-SF, **RIA-FrOpS** pour le SIA FrOps.

Référentiel d'identités numériques (RIN) : Base fédérée d'identités, le RIN contient un référentiel des liens entre les identités d'une personne. Cette base de données commune contient l'ensemble des attributs de type RH et organisationnel (au sens SI-ORG) pour tout le personnel du ministère. Le RIN contient également les identités provenant des chaînes de confiance (pour les extérieurs, les identités protégées, les ayants droits...). Enfin, ces données sont complétées avec les informations d'emploi locales renseignées par le réseau de proximité Employeur. Ce RIN dont le rôle est assuré aujourd'hui en partie par l'annuaire référent de l'intranet sensible (Annudef), est en cours de consolidation et de fiabilisation. Il sera constitué :

- des données d'identité dites « pivot » du type nom de naissance, prénom(s), sexe, date, ville et pays de naissance ;
- de données d'identité complétées par les SIRH pour les agents du ministère des armées et renseignées via une interface dédiée pour les personnes extérieures et employées au ministère des armées ;

⁴⁸ Les macro-droits seront calculés sur la base des modalités d'accès et de profils métier dits « Profils Filière Métier Applicatif » (PFMA). Les droits fins (micro droits) et la gestion des profils des utilisateurs restent de la responsabilité des applications

- des attributs techniques permettant l'identification des personnes au sein du système d'information : nom de connexion unique, numéro d'employé...

Référentiel d'identités et d'autorisations de l'Intredef (RIA-Def) : Alimenté par le RIN et complété de données propres à l'Intredef, le RIA-Def doit permettre de gérer les données d'autorisations associées à ces identités dans le contexte de l'Intredef. Il provisionnera les annuaires techniques, et fournira à terme les identités et autorisations d'accès de haut niveau (macro droits) aux SI Clients par l'intermédiaire du composant MindefConnect Intredef.

MindefConnect Intredef : Service centralisé d'authentification des utilisateurs et de contrôle d'accès aux ressources. Il permet aux SI Clients de :

- déléguer l'authentification de leurs utilisateurs ;
- déléguer les contrôles d'accès de leurs utilisateurs (il ne gère pas les droits applicatifs) ;
- disposer du support de différents mécanismes d'authentification et des protocoles OpenId Connect et, à défaut, SAMLv2, lorsque le premier n'est pas supporté.

Il permet aux utilisateurs de bénéficier d'une authentification unique (SSO).

Document	Date	Origine	Type doc	Portée
Instruction ministérielle n°3 relative à l'identité numérique et aux autorisations diffusée par note n°154/ARM/DGNUM/DG/NP	18 mars 2024	DGNUM	IM	Min Arm
<i>Commentaire : cette instruction précise les concepts et définitions liés à l'identité numérique, ainsi que les principes retenus. L'organisation, les acteurs en jeu et leurs rôles dans la gestion des identités numériques au sein du ministère seront définis dans un document de politique ministérielle et une directive de gouvernance.</i>				
Politique ministérielle relative à l'identité numérique et aux autorisations diffusée par note n°154/ARM/DGNUM/DG/NP	18 mars 2024	DGNUM	Politique	Min Arm

4.6.1.2 Identification / Authentification des personnes [CAU]

Pour mémoire, la PSSI-A fixe un certain nombre de règles concernant l'identification et l'authentification des personnes, et notamment :

- l'accès à un système ou un réseau du ministère ne doit être possible qu'après un processus d'identification/authentification ;
- chaque utilisateur doit disposer d'un identifiant unique ;
- pour les SI jusqu'au niveau DR inclus, des comptes fonctionnels peuvent être autorisés par le chef d'organisme dans le cas des centres opérationnels (CO) et des postes de permanence, si des mesures organisationnelles garantissent la traçabilité des usagers :
 - une note de service décrivant ces mesures est signée par le chef du CO ou d'organisme. Les mesures peuvent aussi être intégrées dans la note d'organisation SSI de l'organisme ;
 - une main courante conserve les noms des personnes utilisant ces comptes fonctionnels ;
 - ces comptes fonctionnels sont «attachés» à la machine désignée dans la note de service. Cette règle n'est pas imposée dans le cas d'une authentification forte.

4.6.1.2.1 Authentification sur Internet

Sur Internet, le ministère a développé une capacité d'identification et d'authentification sur internet. Cette capacité qui est construite sur les composants MinDefConnect Internet et Fournisseur d'identité Intredef est obligatoire sur C1NP et offre :

- un mécanisme de réconciliation de l'identité Internet avec l'identité Intredef (impliquant le système d'information utilisant le service incluant un composant sur Intredef, la passerelle API, le fournisseur d'identité Intredef et Annudef) ;

- la possibilité d'utiliser une authentification à double facteur en ajoutant un mot de passe à usage unique (one time password ou OTP) sans connexion à un service ;
- la possibilité d'utiliser France Connect.

En application des critères du CCT, l'emploi des clients FreeOTP (ne bénéficiant pas de mises à jour suffisantes) et de Google Authenticator (solution GAFAM) est déconseillé. Les alternatives suivantes sont préconisées, pour les appareils disposant d'un système d'exploitation Android : Aegis Authenticator, FreeOTP+ (version dérivée de FreeOTP).

Ces deux solutions disposent par ailleurs de fonctionnalités d'export et d'import des données et autorise un fonctionnement en mode déconnecté (hors connexion réseau).

Les alternatives suivantes sont préconisées pour les appareils disposant d'un système d'exploitation iOS : Tofu Authenticator, Authenticator.

MinDefConnect Internet n'est pas destiné à gérer les droits fins des applications pour lesquelles il assure l'identification et l'authentification.

Les protocoles supportés sont OpenIdConnect (mode *confidential* seulement) à privilégier et, à défaut, SAMLV2, lorsque le premier n'est pas supporté.

Document	Date	Origine	Type doc	Portée
Spécification d'interface générique MindefConnect Internet / Si clients V1.0.7	19 juillet 2022	AND	Guide	Min Arm

En interministériel, a été lancée la démarche France Connect, premier composant de la stratégie « État Plateforme », dispositif permettant de garantir l'identité d'un usager en s'appuyant sur des comptes existants pour lesquels son identité a déjà été vérifiée.

Cette démarche s'est scindée en plusieurs volets :

- « France Connect » pour les usagers d'internet : le système, en service depuis janvier 2016 et opéré par la DINUM, a vocation à être reconnu à terme par l'ensemble des services publics numériques sur Internet, dont il propose de fédérer les comptes ; MinDefConnect Internet permet aux systèmes d'information hébergés sur CINP de recourir à ce service ;
- « ProConnect » pour les agents de l'Etat sur le réseau interministériel RIE et mis à disposition sur Internet. Le projet vise à déterminer les moyens d'identification et d'authentification des agents du service public, agents des ministères et des collectivités territoriales dans le cadre de l'usage d'applications entre les collectivités et les S.I. de l'État. Il permet aussi d'identifier les professionnels du privé, en remplacement de « MonComptePro ».

4.6.1.2.2 Authentification sur Intradef

Sur l'Intradef, l'authentification sur le poste de travail repose en standard sur un mécanisme technique « login / mot de passe » relié au jeton d'authentification Kerberos sur Active Directory.

MinDefConnect sur Intradef est désormais le mode d'authentification imposé aux systèmes d'information. Il pourra également permettre d'utiliser le dispositif France Connect. Il permettra la mise en œuvre de fédérations d'identité avec d'autres ministères au travers du Réseau Ministériel d'Etat RIE.

MinDefConnect Intradef offre aux applications la gestion des accès et des éléments génériques permettant aux applications de gérer des droits mais n'est pas destiné à gérer les droits eux-mêmes des applications pour lesquelles il assure l'identification et l'authentification.

Les protocoles supportés sont OpenIdConnect à privilégier et, à défaut, SAMLV2, lorsque le premier n'est pas supporté.

Pour les applications le nécessitant, une authentification forte est mise en place au moyen de la carte à puce CIMS⁴⁹ contenant un certificat électronique d'authentification issu de l'IGC CIMS. En revanche,

⁴⁹ Carte d'Identité Multi-Services

l'adossement au web service d'authentification de l'Annufef ou à l'authentification directe sur l'Active Directory sont des modes d'authentification fortement déconseillés.

Document	Date	Origine	Type doc	Portée
Modalités d'authentification pour l'accès aux applications par note conjointe DGSIC-EMAn°447/DEF/DGSIC/SDAU/NP du 22 juillet 2016 n°D-16-008130/DEF/EMA/CPI/NP du 26 août 2016 [abrogée]	26 août 2016	DGSIC - EMA	Note	Min Arm
Spécifications d'interface générique MindefConnect IntraDef v2.6	29/01/2021	UMSnum	Rapport	Min Arm

Pour rappel, la spécification d'interface relative à MindefConnect Intradef mentionne la règle suivante :

Règle	Énoncé	Statut	Portée
CCT_R7_1	Il est OBLIGATOIRE que les applications utilisant le composant MinDefConnect Intradef/Internet traitent l'authentification côté serveur en implémentant l' « authorization code flow » à l'exclusion de tout autre « flow ».	O	Intradef Internet

4.6.1.2.3 Authentification sur intranets classifiés

Sur les intranets classifiés de défense, l'accès est protégé par « carte à puce et code PIN » généralement au niveau du poste, sinon au niveau du portail ; il équivaut donc à une authentification forte. La carte est aujourd'hui fournie par le projet IGCg NG.

4.6.1.2.4 Authentification mutualisée et SSO

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
RFC 4120	The Kerberos Network Authentication Service : standard décrivant le mécanisme d'authentification via le protocole Kerberos	R	Min Arm
SAML v2	Security assertion markup language (SAML) est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. Basé sur le langage XML, SAML a été développé par le consortium OASIS. SAML propose l'authentification unique (en anglais single sign-on ou SSO) sur le web permettant à un utilisateur de naviguer sur plusieurs sites différents en ne s'authentifiant qu'une seule fois, sans pour autant que ces sites aient accès à des informations trop confidentielles.	A	Toute admin.
OpenIDConnect 2.0	OpenID Connect est une couche d'identification basée sur le protocole OAuth 2.0, qui autorise les clients à vérifier l'identité d'un utilisateur final en se basant sur l'authentification fournie par un serveur d'autorisation, suivant le processus d'obtention d'une simple information du profil de l'utilisateur final. Ce processus est basé sur un dispositif interopérable de type REST.	R	Toute admin.
<i>Commentaire : OpenID Connect v2 et SAML v2 sont tous deux recommandés par le RGI. OpenID Connect v2 est par ailleurs le protocole retenu par la démarche FranceConnect et celui privilégié par le Ministère des Armées. Pour le ministère, ces protocoles sont adaptés à des applications partagées en interministériel aux fins de fédération d'identité : chaque organisme gère ses propres identités (fournisseur d'identité), l'accès à l'application se fait au travers d'une fédération d'identité, sphère de confiance reposant sur l'un de ces protocoles.</i>			

Document	Date	Origine	Type doc	Portée
Modalités d'authentification pour l'accès aux applications cf. §4.6.1.2.2 Authentification sur Intradef			Note	Min Arm

Spécification d'interface générique MindefConnect Intradef / Si clients V2.7	21 juin 2021	UM SNUM	Guide	Intradef
Spécification d'interface générique MindefConnect Internet / Si clients V1.0.7	19 juillet 2022	AND	Guide	

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
SSO	MindefConnect Intradef v2 (reposant sur RedHat SSO)	Min Arm	Solution d'authentification sur Intradef. Cette solution de fédération d'identité prend en charge les protocoles OpenID Connect (en priorité) et SAML V2 (par défaut).	R / S	Intradef
SSO	KEYCLOAK	REDHAT	Solution open source de fédération d'identité. Lorsque des besoins spécifiques non rendus par les solutions ministérielles nécessitent une instanciation particulière. (Exemple : Axone...). Ce besoin particulier doit être justifié.	★ / ★	Intradef Internet
<i>Commentaire : vu la rapidité des évolutions sur ce logiciel et la durée de vie très courte des versions (3 mois), il peut être intéressant d'utiliser la version soumise à licence REDHAT SSO ou disposer d'un maintien en condition de sécurité adapté à ce rythme très rapide de mises à jour. Une tendance de certains intégrateurs à recourir à cette solution est constatée, plus par facilité que par besoin technique. Par conséquent, en dehors d'une logique de mutualisation de la gestion des rôles et droits d'un écosystème logiciel donné, l'intégration des ces mécanismes au sein même des projets est préconisée (via potentiellement certaines bibliothèques proposées par les frameworks de développement tels que Spring Security).</i>					
SSO	Red Hat Build for Keycloak	REDHAT	Solution packagée faisant l'objet d'une offre de service de Red Hat sur la base de Keycloak	A / N	Intradef
Authentification mutualisée	WebService Annudef	DIRISI	Ce mode est interdit pour tout nouveau projet et soumis à dérogation pour tout système historique.	I / S	Intradef
<i>Commentaire : ce mode d'authentification obligeant les utilisateurs à disposer d'un second jeu d'identifiant et de mot de passe, moins intégré et communiqué au système d'information l'utilisant ne doit désormais plus être utilisé. Il est de plus obsolète et non pérenne. L'usage des autres WebServices reste possible pour accéder à des données utilisateurs contenues dans l'Annudef (la direction d'application doit alors en demander l'autorisation sur DIADEME), l'interrogation directe de l'annuaire LDAP n'étant pas autorisée. A noter toutefois que ces webservices ont vocation à être remplacés par des API Rest à interroger depuis la PEM Intradef. Enfin, il convient de signaler qu'au moment de l'authentification, MindefConnect Intradef renvoie systématiquement un certain nombre d'informations pivot relative à l'utilisateur identifié. A l'horizon été 2026, INA fournira le webservice Personnes qui reprendra a minima le périmètre d'informations du webservice User infos de l'Annudef.</i>					
SSO	Windows Server reposant sur le protocole Kerberos	Microsoft	Si MindefConnect Intradef ne peut pas être utilisé. Cela devra être justifié.	R / S	Intradef
<i>Commentaire : pour les smartphones SMOBI (sous OS Android), Kerberos n'est pas encore pris en charge. Les serveurs doivent alors ajouter un mécanisme complémentaire, se déclenchant en cas d'échec de l'authentification automatique et demandant à l'utilisateur de saisir son identifiant et son mot de passe de session.</i>					
SSO	Windows Server reposant sur le protocole Kerberos	Microsoft		R / S	S-SF SIA FrOps
<i>Commentaire : pour le théâtre, il s'agit de Kerberos sur Windows Server 2012/2016.</i>					

SSO	SIGN&GO	ILEX	Dans SIA S-SF métropole	D / S	S-SF SIA FrOps
<i>Commentaire : assujetti aux cas d'utilisation en cours.</i>					
SSO	MindefConnect Internet v2 (reposant sur RedhatSSO de Redhat)	Min Arm	Solution d'authentification sur Internet. Cette solution de fédération d'identité prend en charge OpenID Connect, l'OTP, FranceConnect Particuliers ainsi qu'une réconciliation d'identité avec Intradef pour les ressortissants du MinArm.	R / S	Internet
<i>Commentaire : l'utilisation de cette brique s'impose désormais aux systèmes d'information hébergés sur CINP. Ces derniers doivent, pour des raisons de sécurité et conformément à l'homologation de MinDefConnect Internet, impérativement implémenter l'autorization code flow à l'exclusion de tout autre « flow », y compris lorsque le client est une application web SPA ou une application mobile.</i>					
SSO	FranceConnect Particulier	DINUM	Dispositif préconisé par l'État (État plateforme) pour garantir l'identité d'un usager en s'appuyant sur des comptes existants pour lesquels son identité a déjà été vérifiée.	R / -	Internet
<i>Commentaire : certaines démarches administratives en ligne requièrent davantage qu'une authentification simple, reposant sur un identifiant et un mot de passe. La DINUM étudie donc la piste d'un « second facteur » à utiliser par les fournisseurs de services. Autrement dit un système supplémentaire de vérification reposant sur ce que possède l'utilisateur, ce qu'il sait ou ce qu'il est. Cette authentification renforcée est nécessaire dans un cas d'usage sensible tel que la modification d'un RIB préenregistré. L'ensemble de la documentation technique concernant FranceConnect est accessible sur le site dédié : https://partenaires.franceconnect.gouv.fr/</i>					

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

4.6.1.3 Habilitation et gestion des profils

Actuellement la sécurisation de la gestion des profils de comptes utilisateurs et des accès des utilisateurs aux services de l'Intradef se fait au travers de stratégies de groupes ou GPO (Group Policy Object) déployées dans l'annuaire Active Directory DR-CPT.

Règle	Énoncé	Statut	Portée
CCT_R8_1	Il est OBLIGATOIRE que les applications assurent la gestion des droits fins à leur niveau.	O	Min Arm

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestion des profils	Gestion des GPO sur Active Directory (GPMC : Group Policy Management Console ou AGPM : Advanced Group Policy Management)	Microsoft	AGPM est lié au pack MDOP (Microsoft Desktop Optimization Pack) et n'est pas disponible depuis les sites VisualStudio ou MAC (ex VLSC) il doit faire l'objet d'une FEB.	R / S	Min Arm

4.6.1.4 Supports matériels – Cartes à puces

Document	Date	Origine	Type doc	Portée
e-IDAS – electronic Identification And Signature : règlement européen (cf. §2.1.2 Européen)	23 juillet 2014	Union Européenne	Règlement	UE
RGS B3 – Mécanismes d’authentification version 1.0 : annexe du référentiel général de sécurité (RGS) cf. 2.2.3 Les référentiels interministériels	13 janvier 2010	ANSSI	RGS	Toute admin.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Carte à puce	CIMS	Min Arm	La carte CIMS est la carte d’identité professionnelle et militaire pour les agents du ministère. Les données apposées sur et contenues dans la puce de la carte proviennent des SI RH et de l’Annudef.	R / S	Intradef
<i>Commentaire : la carte est équipée d’une puce qui offre plusieurs interfaces :</i> • Une interface sans contact (Mifare DESFire) utilisée notamment pour du contrôle d’accès, la restauration et l’utilisation de l’impression sécurisée ; • Une interface avec contact : des certificats électroniques (un d’authentification, un de signature et un de chiffrement) délivrés par l’IGC CIMS ; Les certificats électroniques CIMS sont utilisés par exemple pour : • l’authentification forte auprès d’applications le nécessitant sur l’Intradef (CHORUS, SI CIMS, Source Solde, MindefConnect ...) ; • la signature électronique (SI CIMS, ...) Plusieurs générations de puce sont en circulation. Un logiciel tiers (middleware) est nécessaire pour utiliser les certificats électroniques.					

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestion des clefs	TrustWay Proteccio	ATOS	TrustWay Proteccio est le HSM à usage général. De conception et de fabrication européenne, il s’inscrit comme le successeur des HSM TrustWay Crypto PCI et TrustWay box. Produit certifié Critères Communs EAL4+. Produit qualifié niveau Renforcé par l’ANSSI en mars 2020	R / S	Min Arm

4.6.1.5 Authentification Machines [CAR]

Avant l’ouverture d’une session, les machines peuvent s’identifier via le protocole 802.1.x.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°88 « Implémentation du 802.1x sur les réseaux de dessert » : version V1.0 du 27 mars 2013	27 mars 2013	DIRISI	Directive	Intradef SIA S-SF SIA FrOps
<i>Commentaire : cette directive décrit l’architecture et la mise en œuvre de l’infrastructure 802.1x d’authentification des équipements d’extrémité (ordinateurs, portables, téléphones, imprimantes, etc...) déployée au sein du Ministère des armées. Cette architecture permet de répondre partiellement au besoin d’itinérance et de sécurisation des services communs du STC-IA, ainsi qu’au dialogue entre l’infrastructure mise en œuvre par le CND et celles mises en œuvre dans le cadre de partenariats public privé (Balard, RDIP...).</i>				
Recommandations de l’ANSSI relatives au déploiement du protocole 802.1X pour le contrôle d’accès à des réseaux locaux	07 août 2018	ANSSI	Guide	Toute administration
<i>Commentaire : ce document détaille le fonctionnement d’un réseau à accès contrôlé, qu’il soit filaire ou sans fil et présente les recommandations de la technologie reposant sur le protocole 802.1X, ainsi que</i>				

l'architecture et les composants principaux d'un tel réseau. Il détaille les fonctions de sécurité et les bonnes pratiques à appliquer pour augmenter le niveau d'un tel réseau.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
802.1x	Architecture basée sur l'infrastructure Microsoft :- service Radius NPS- AD- PKI Microsoft ou IGCg (NG)	DIRISI	Cette infrastructure est basée sur l'infrastructure Microsoft avec : • l'architecture de certification sous PKI Windows ; • les groupes de sécurité dédiés à l'architecture 802.1x sous Active Directory ; • les services Radius déployés en configurant des serveurs NPS (Network Policy Server) sous Windows.	R / S	Min Arm

4.6.1.6 Authentification Services [CAR]

Dans le cadre des chantiers de transformation et de sécurisation des socles non classifiés, le gestionnaire de secrets est accessible sur le C1NP et C1DR.

Ce gestionnaire de secrets offre deux catégories de fonctionnalités :

- Une infrastructure de gestion de clefs automatisée avec :
 - Un service de création et de renouvellement de certificats finaux X509 HTTPS. Le gestionnaire de secrets se positionne en tant qu'Autorité de Certification Délégée d'une ACR issue d'IGC-G-NG ;
 - Un service de production de certificats de type client SSH (authentification d'un client SSH par certificat).
- Des fonctionnalités de stockage de secrets (mots de passe de comptes de service, jetons...) avec :
 - Un service de stockage de secrets avec gestion de versions ;
 - Un service de création et de renouvellement automatique de mots de passe de bases de données.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestionnaire de secrets	Service GDS	Min Arm	gestion et mise à disposition d'éléments secrets via API REST et la fourniture de certificats serveur	R / S	C1NP, C1DR

4.6.1.7 Relais (messagerie, services web, services utilisateurs)

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Relais messagerie	Postfix	Postfix.org	Dans le cadre de SIA et SIE	R / S	SIA S-SF SIA FrOps SIE
Relais Web	Apache HTTP Server	Apache Foundation	Dans le cadre de SIA	R / S	SIA S-SF SIA FrOps

4.6.2 Gestion des clés – certificats électroniques [IGC]

RGS

Le référentiel général de sécurité (RGS) définit un ensemble de règles de sécurité (authentification, horodatage, confidentialité, signature électronique...) qui s'imposent aux administrations et aux collectivités territoriales pour sécuriser leurs systèmes d'information. Certaines annexes du RGS concernent les IGC.

L'arrêté du 13 juin 2014 porte approbation du RGS et précise les modalités de mise en œuvre de la procédure de validation des certificats électroniques. Cet arrêté rend applicable la deuxième version du RGS au 1er juillet 2014.

Document	Date	Origine	Type doc	Portée
e-IDAS – electronic Identification And Signature : règlement européen. Cf. §2.1.2 EuropéenCe texte fait actuellement l'objet d'une refonte.	23 juillet 2014	Union Européenne	Règlement	UE
• RGS A1 – Fonctions de sécurité basées sur l'emploi de certificats électroniques version 3.0 • RGS A2 – Politique de certification type « certificats électroniques de personne » version 3.0 • RGS A3 – Politique de certification type « services applicatifs », version 3.0 • RGS A4 – Profils de certificats, CRL, OCSP et algorithmes cryptographiques, version 3.0 • RGS A5 – Politique de certification type « services applicatifs », version 3.0 Cf. 2.2.3 Les référentiels interministériels (Annexes du RGS)	27 février 2014	ANSSI	RGS	Toute admin.

MINARM

Document	Date	Origine	Type doc	Portée
Politique ministérielle des IGC au MINARM diffusée par la note n°194/ARM/DGNUM/SDSN/NP	18 mai 2022	DGNUM	politique	Min Arm
<i>Commentaire : ce document définit les grands principes d'utilisation des IGC au sein du ministère des armées.</i>				
Directive DGSIC n°21 édition 4 portant sur les certificats électroniques employés au sein du ministère des armées diffusée par la note n°194/ARM/DGNUM/SDSN/NP du 18/05/2022	18 mai 2022	DGNUM	Directive	Min Arm
<i>Commentaire : cette directive décrit les besoins du ministère en services de confiance, ainsi que les modalités de délivrance et le concept d'emploi des certificats électroniques. Règles pour tout niveau de confidentialité découlant du RGS (hors algorithmes gouvernementaux).</i>				
Cadre de gouvernance des infrastructures de gestion de clés diffusée par note n° 194/ARM/DGNUM/SDSN/NP du 18/05/2022	18 mai 2022	DGNUM		Min Arm

L'IGCg-NG est le système, de référence, à utiliser par l'ensemble des projets.

Sur l'Intradef, l'IGCg NG est employée pour les certificats machines. Les certificats personnes sont fournis par l'IGC CIMS, apportée dans le cadre de la délivrance de la carte CIMS (Carte d'identité Multi-Services).

Sur l'internet et pour les échanges interministériels :

- les certificats machines exposés vers l'Internet public peuvent être obtenus via le lot 3 du marché ASTEL-I géré par le CND ;
- les certificats machines utilisés en interne sur la plateforme d'hébergement C1NP seront délivrés par le service socle gestion des secrets disposant d'une autorité de certification déléguée ;
- les certificats de personne (conformes aux RGS***) sont fournis par l'IGC dite IGC CIMS, apportée dans le cadre de la délivrance de la carte CIMS (Carte d'identité Multi-Services).

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
IGC	Certificats machine Internet	Marché CND ASTEL-I	Certificats machines pour Internet à acquérir via le marché ASTEL-I mis en service par le CND.	R / S	Internet
<i>Commentaire : attention, la durée des certificats est imposée. (de 90 jours à 3 ans).</i>					
IGC	IGC CIMS	ANTS	IGC opérée par l'ANTS ⁵⁰ dans le cadre du déploiement de la carte CIMS ⁵¹ sur l'Intredef. Les certificats sont portés par la carte à puce. Ces certificats peuvent être utilisés pour des échanges avec d'autres administrations sur Internet ou le RIE. (★) Soutien assuré l'opérateur Imprimerie Nationale	R / S (★)	Intredef Internet RIE
IGC	IGCg	Min Arm	IGC remplacée par IGCg NG et ne doit plus être utilisée par les projets (dérogation déléguée au COMCYBER).	I / S	Intredef SIA S-SF SIA FrOps
IGC	IGCg NG	Min Arm	Unique service de gestion de certificats du MinArm. IGC opérée par le CND permet de délivrer des certificats logiciels et sur les réseaux classifiés, des certificats sur cartes à puce.	R / S	Intredef SIA S-SF SIA FrOps

4.6.3 Gestion de la preuve

4.6.3.1 Horodatage [HOR]

Pas de référence identifiée à ce jour.

4.6.3.2 Signature [SGN]

Document	Date	Origine	Type doc	Portée
Cadre d'emploi de la signature électronique au ministère des Armées – Ed 2 diffusée par note n° 313/ARM/DGNUM/SDSN/NP du 8 juillet 2021	8 juillet 2021	DGNUM	Concept Emploi	Min Arm
<i>Commentaire : ce document précise les aspects techniques, juridiques et organisationnels à prendre en compte pour intégrer le processus de signature électronique dans un projet. Il détaille les offres de signature électronique susceptibles d'adresser les besoins du ministère.</i>				

Niveaux de signature	Définition technique	Solution
Signature simple	Les systèmes respectant, a minima, les trois conditions d'identification, d'intégrité et de consentement. Généralement, on s'appuie sur les certificats de l'IGC g/NG	Aucune
Signature avancée	Les systèmes répondant aux principes de la signature simple avec l'utilisation de certificats électroniques issues d'une IGC de confiance (mais non qualifiée au sens du règlement eIDAS), exemple CIMS	SOSIE
Signature qualifiée	Utilisation d'un certificat électronique qualifié délivré par un Prestataire de Service de Certification Electronique (PSCE)	ChamberSign : solution disponible au catalogue OURANOS

⁵⁰ Agence National des Titres Sécurisés

⁵¹ Carte d'Identité Multi-Services

	qualifié, mise en place d'une organisation audité et certifiée par l'ANSSI.	
--	---	--

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Signature	Eiducio+ (pilote Idope 6.22.2.10)	ChamberSign	Solution de signature qualifiée sur l'Intredef	R / S	Intredef
Commentaire : le pilote nécessaire au fonctionnement du support cryptographique USB sur lequel est livré le certificat est disponible dans DIADEME					

4.6.4 Surveillance - Outils LID, détection d'intrusion [SUR] [DEA]

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°10 sur la prévention contre les codes malveillants. Cf. 4.6.5.1 Antivirus – codes malveillants [ANV] [SSV]	05 novembre 2009	DGSIC	Directive	Min Arm
Commentaire : cette directive définit les règles du ministère des armées en matière de prévention contre les codes malveillants (PCM). Ce processus est prolongé par des processus opérationnels, dans le cadre plus général de la lutte informatique défense (LID), qui ne sont pas traités dans cette directive				

4.6.4.1 Autres solutions

4.6.5 Utilitaires de sécurité

4.6.5.1 Antivirus – codes malveillants [ANV] [SSV]

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°10 sur la prévention contre les codes malveillants	5 nov. 2009	DGSIC	Directive	Min Arm
Commentaire : cette directive définit les règles du ministère des armées en matière de prévention contre les codes malveillants (PCM). Elle en précise les principes, les objectifs et les moyens généraux pour y parvenir. La lutte contre les codes malveillants repose sur deux types de processus différents. La PCM est le processus amont de cette lutte, et fait l'objet de cette directive. L'effet majeur recherché de la PCM du ministère est de minimiser les impacts des codes malveillants, dans le cadre d'une analyse de risques globale des systèmes d'information. Ce processus est prolongé par des processus opérationnels, dans le cadre plus général de la lutte informatique défense (LID), qui ne sont pas traités dans cette directive.				
Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows cf.4.5 Sécurisation des COTS	13 janvier 2017	ANSSI	Note	Toute admin.
Commentaire : https://cyber.gouv.fr/publications/mettre-en-oeuvre-une-politique-de-restrictions-logicielles-sous-windows				

4.6.5.2 Contrôles d'intégrité [CIN]

Pour s'assurer de l'intégrité d'un fichier ou d'une livraison, il est possible de recourir aux utilitaires Microsoft CertUtil ou Get-FileHash présents en standard sur les postes et serveurs. A l'identique, les utilitaires MD5sum et SHA1sum peuvent être utilisés sur les environnements de type Linux. Cependant pour des raisons de sécurité, l'utilitaire sha256sum sera préféré.

4.6.5.3 Chiffrement

4.6.5.3.1 Chiffrement de fichiers [CHI]

ACID⁵² Cryptofiler : L'opération de chiffrement des données sensibles doit être effectuée dans un environnement de confiance soit validé pour traiter des informations du niveau visé. C'est la raison pour laquelle le logiciel ACID Cryptofiler n'est pas installé sur des postes Internet en libre-service.

Certains produits agréés, ou certains systèmes ayant reçu une homologation, peuvent disposer d'un chiffrement ACID alors qu'ils disposent d'un accès à internet filtré (ISPT). Les mesures de protection face à la menace liée à Internet sont alors jugées suffisantes.

Document	Date	Origine	Type doc	Portée
Recommandations pour une utilisation sécurisée de Zed! diffusée par note n°ANSSI-PG-068 du 14/11/2019 (v1.1)	14 novembre 2019	ANSSI	Note technique	Toute admin.
Décision de qualification d'un produit : Zed! version Q2023.X avec X>2, n°1 398/ANSSI/SDE/NP du 23/06/2025.	23/06/2025	ANSSI	Décision	Toute admin.
Commentaire : La décision précise les limites de l'agrément, https://cyber.gouv.fr/sites/default/files/decisions-qualifications/2025_1398_np.pdf				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Chiffrement	ACID Cryptofiler	Capgemini-Abak Systèmes	Permet le chiffrement au niveau DR. Plugin pour Outlook 2016 disponible dans le Store DIRISI DR-CPT.	R / S	Min Arm
Commentaire : le logiciel ACID Cryptofiler est une solution développée par le ministère des Armées, pour la protection de fichiers sensibles non-classifiés, jusqu'au niveau Diffusion Restreinte (y compris avec une mention spéciale comme Spécial France), Restreint UE, ou Restreint OTAN. Il est largement déployé auprès des personnels du ministère des Armées, dont il est l'outil de chiffrement de fichiers sensibles de référence. Les conditions d'accès à ce logiciel sont néanmoins strictes : un industriel doit justifier d'un contrat d'armement, ou d'un système d'information homologué au niveau Diffusion Restreinte a minima, pour pouvoir bénéficier de ce logiciel, et recevoir des clés pour certains de ses personnels, générées par le ministère des Armées. L'emploi d'Acid doit être recommandé en interne du ministère, et dans les échanges entre le ministère et les industriels de l'armement.					
Chiffrement	ACID Eleonore	Min Arm - DGA	Permet le chiffrement au niveau Secret.	D / S	Min Arm
Commentaire : cette solution est désormais déconseillée (liste C ANSSI)					
Chiffrement	Zed! (à ne pas confondre avec « Zed! Free » qui est interdit)	Prim'X	Assujetti aux échanges à l'interministériel jusqu'au niveau DR-SF, à l'exception des échanges avec l'UE au niveau RUE où il est autorisé ainsi qu'avec les industriels qui ne disposent pas d'ACID	A / S	Toute administration
Commentaire : Le logiciel Zed! est une solution commerciale développée par la société française Prim'X en différentes versions. Sa version complète a été agréée le 23 juin 2025 par l'ANSSI pour la protection d'informations marquées Diffusion Restreinte, ou classifiées Restreint UE dans un contexte national uniquement, ou classifiées Restreint OTAN. Le logiciel Zed! peut aussi être utilisé pour protéger des informations de sensibilité plus faible que le niveau "Diffusion Restreinte", vers des correspondants ne disposant pas d'un système d'information support homologué à ce niveau. Le logiciel Zed! ne doit pas être utilisé pour les cas d'emploi couverts par ACID Cryptofiler. Zed! est accessible sur le NUMERI Store.					

⁵² Automate de Chiffrement des Informations de Défense

4.6.5.3.2 Effacement sécurisé

Document	Date	Origine	Type doc	Portée
Guide technique 972-1 pour la confidentialité des informations enregistrées sur disque dur à recycler ou exporter (cf. 4.1.3 Références pour le niveau Secret)	17 juillet 2003	SGDN		Toute admin.
<i>Commentaire : ce guide précise le guide 972 dans son chapitre 8 relatif à l'effacement d'un support pour recyclage interne. Il a valeur de circulaire.</i>				
Directive DIRISI n°117 relative au traitement des supports ayant contenu des informations sensibles ou classifiées sous timbre n°400757/DEF/DIRISI/SDSSI/NP du 13 février 2014	13 février 2014	DIRISI	Directive	DIRISI
Directive DIRISI n°119 relative à l'obfuscation sécurisée des données sous timbre /DEF/DIRISI/SDSSI/NP du 17 février 2014	17 février 2014	DIRISI	Directive	DIRISI

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Effacement de fichiers sécurisé	Fonction d'effacement sécurisé d'ACID	Capgemini-Abak Systèmes	Permet d'effacer des fichiers ou répertoires sur un poste sur lequel Acid est installé. Il ne permet pas de blanchir un disque entier. ACID ne permet pas de déclassifier le support effacé.	R / S	Min Arm

Bien que des solutions d'effacement sécurisé soient recommandées dans le CCT, il est préférable d'appliquer des solutions de chiffrement de disque ou de fichier . Par ailleurs, il est rappelé que l'effacement de données par réécriture demeure une technologie peu fiable et est réservée à des cas d'emploi particulier.

4.6.5.4 Pare-feux

Règle	Énoncé	Statut	Portée
CCT_R9_1	Par défaut, il est OBLIGATOIRE de laisser actif le pare-feu logiciel intégré aux OS et de le configurer.	O	Min Arm

Les machines virtuelles provisionnées par les Clouds C1NP et C1DR sont livrées avec ce pare-feu activé et préconfiguré. Les flux Https, SMTP, DNS et ssh sont autorisés par défaut. Les éventuels flux complémentaires spécifiques qui pourraient s'avérer nécessaires doivent être spécifiquement ouverts par la collection d'installation Ruche.

Document	Date	Origine	Type doc	Portée
Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu cf. 4.5 Sécurisation des COTS	30 mars 2013	ANSSI	Note technique	Toute admin.
Recommandations de sécurisation d'un pare-feu Stormshield Network Security cf. 4.5 Sécurisation des COTS	02 avril 2021	ANSSI	Guide	Toute admin.
Guide PA-044 « Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à internet »	22 janvier 2018	ANSSI	Guide	Toute admin.

Concernant les OS Windows, il est interdit de désactiver le service associé, et ce, même en cas de recours à un pare-feu tiers. En effet, le service « pare-feu » ne gère pas que le pare-feu mais gère également tout l'aspect « hardening de service » de Windows. Aussi, dans le cas où l'on ne souhaite pas utiliser le pare-feu de Windows au profit d'un pare-feu tiers, il faut désactiver le pare-feu en tant que composant pour les différents profils (privé-public et domaine) mais ne pas désactiver le service.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Pare-feu	PALO ALTO	PALO ALTO		R / S	Intredef Internet S-SF SIA FrOps
Pare-feu applicatif Web (WAF)	UBIKA WAF	UBIKA	Sur C1NP	R / S	Internet

4.6.6 Supports de stockage sécurisés

4.7 Interconnexions, passerelles et solutions de sécurité iso/multi niveaux

4.7.1 Passerelles d'échanges

Document	Date	Origine	Type doc	Portée
Concept d'emploi « accès réseaux extérieurs ». SLR des services “d'accès aux réseaux extérieurs”. Cf. 3.1.7.2 Accès aux réseaux interministériels [SU-RMI] et autres réseaux extérieurs [SU-REX]		SC1	ConceptEmploiSLR	Min ArmTout réseau
Guide « Recommandations pour les architectures des systèmes d'information sensibles ou diffusion restreinte » réf. PG-075	28 déc. 2020	ANSSI	Guide	Toute admin. NP-DR
Guide « Recommandations relatives à l'interconnexion d'un système d'information à Internet » V3.0 du 19 juin décembre 2020	19 juin 2020	ANSSI	Guide	Toute admin. NP-DR
<i>Commentaire : ce document adresse des interconnexions entre un réseau privé hébergeant des informations sensibles non classifiées de défense et un réseau ouvert type Internet. Ce document n'édicte pas de règle impérative, mais décrit un ensemble de concepts ou de recommandations à adapter en fonction des contraintes et enjeux du contexte.</i>				
Recommandations relatives à l'interconnexion d'un système d'information à Internet : guide ANSSI-PA-066 du 19 juin 2020	19/06/2020	ANSSI	Guide	Toute admin.
Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu. Cf. 4.5 Sécurisation des COTS	30 mars 2013	ANSSI	Note technique	Toute admin.
Recommandations de sécurité concernant l'analyse des flux HTTPS. Cf. 4.5 Sécurisation des COTS	9 octobre 2014	ANSSI	Note technique	Toute admin.
Directive DGSIC n°13 sur la sécurité des accès aux services de l'Internet et de l'hébergement des services Internet du ministère. Cf. 6.1.3.2 Hébergement Internet	30 juin 2010	DGSIC	Directive	Min Arm
<i>Commentaire : règles applicables aux accès au réseau et aux services de l'Internet ainsi qu'en matière d'hébergement de services internet.</i>				

4.7.2 Passerelles transdomaines

Passerelles ministérielles génériques

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Passerelle	PES	DIRISI	Plateforme d'échange sécurisée Internet/Intredef composée de : • SISMEL, • ACHERON (obsoléscent), • Passerelle API v2.1 décrits ci-dessous.	R / S	Intredef Internet
Passerelle	ACHERON	DIRISI	Passerelle d'échange de fichiers asynchrone (entre 2 et 15 mn) entre SI Intredef/Internet utilisant le protocole WebDav et les mécanismes de filtrage ISPT. Soumise à des restrictions de volumétrie, de formats et restreinte aux fichiers NP non chiffrés.	D / S	Intredef/Internet
<i>Commentaire : cette passerelle en voie d'obsolescence dont l'arrêt définitif interviendra en mars 2026 et qui ne doit plus être utilisée pour les nouveaux projets (lui préférer la passerelle API v2.1 pour les échanges de fichiers de taille inférieure à 8Mo.). Ceci implique d'utiliser des API Rest plutôt que le protocole WebDav. Le recours à des échanges asynchrones de gros blocs de données dans le cadre d'échanges inter-applicatifs ne constitue pas une bonne pratique d'architecture : échanger des données unitaires en mode synchrone présente de meilleures qualités de fiabilité et de résilience, raison pour laquelle le recours à la PAPI v2.1 doit systématiquement être recherché.</i>					
Passerelle	PASSERELLE API v2.1	DIRISI	Passerelle API RESTful entre des SI Intredef et Internet offrant des fonctions de gestion des API, des droits associés, de publication, de documentation et de sécurité. Limitée aux seuls systèmes d'information hébergés sur des plateformes opérées par le CND (Intredef et C1NP). Cette nouvelle version de la passerelle API RESTful inclut la capacité d'échange des fichiers de manière synchrone avec des fichiers limités en taille à 8 Mo non compressés.	R / S	Intredef C1NP
Passerelle	PASSERELLE API v2.2	DIRISI	Fonctions de la passerelle API V2.1 avec, en plus, la capacité d'échange des fichiers tel qu'envisagé initialement pour une version synchrone de la passerelle ACHERON.	E / -	Intredef
Passerelle	ISPT	DIRISI	Passerelle Web permettant d'accéder à la navigation Web Internet depuis les postes Intredef. Système homologué jusqu'au 13 juin 2024(cf. 3.1.7.1 Internet sur le poste de travail)	R / S	Min Arm Intredef
Passerelle	DMZ IRD	DGA	Interconnexion des Réseaux de Défense : permet l'interconnexion des sociétés avec la DGA. Permet également le raccordement avec des collectivités territoriales.(*) soutien assuré par la DGA	R / S (*)	DGA

Document	Date	Origine	Type doc	Portée
Passerelle API : spécification d'interface générique de la passerelle API avec les SI clients V1.2	16 Septembre 2022	SAND	Spéc. Technique	Min Arm
<i>Commentaire : ce document fournit aux directions de projets, maîtrises d'ouvrage et maîtrises d'œuvre toutes les informations fonctionnelles et techniques nécessaires à l'utilisation du service « passerelle API » mis en œuvre par le CND entre les segments Intradef & Internet maîtrisé (C1NP). Le développement des API doit suivre le cadre technique de mise en œuvre des API du ministère [cf. 3.2.4.4]</i>				

Passerelles et moyens d'accès spécifiques

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Passerelle	SMOBI	DIRISI	Solution de MOBilité de l'Intradef Service permettant un accès sécurisé à l'Intradef en mobilité	R / S	Min Arm

4.7.3 Autres passerelles

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Passerelle	ADER	DIRISI	Permet l'accès des administrations au réseau ADER (Administration En RESeau). Le support utilisé est le RIE (Réseau Internet d'État)	R / S	Intradef Toute admin.
Passerelle	Espace Partenaires (voir IRD)	DIRISI - DGA	L'espace partenaires offre un espace de confiance permettant un échange entre le ministère des armées et ses partenaires. Il repose sur l'utilisation du réseau ENX, d'une politique de sécurité définie et maîtrisée par le ministère. Point de contact : direction du projet Espace Partenaire (DGA)	R / S	Intradef Partenaires

4.8 Administration de la sécurité

4.8.1 Gestion des utilisateurs et des droits

Cf. aussi §4.6.1.3 Habilitation et gestion des profils

Document	Date	Origine	Type doc	Portée
Directive technique sur la gestion des comptes dans un annuaire et application à un Active Directory. Cf. 3.3.4.2 Annuaire techniques de ressources	04 avril 2013	DGSIC	Directive	Min Arm
<i>Commentaire : ce document définit les règles de sécurité du ministère des armées pour la gestion des comptes dans un Active Directory.</i>				

4.8.2 PCA-PRA

Document	Date	Origine	Type doc	Portée
Guide DGSIC n°4 portant sur la rédaction des plans de continuité d'activité (PCA) et plan de reprise d'activité (PRA) diffusé par note n°771 /DEF/DGSIC du 26 juillet 2010	23 juillet 2010	DGSIC	Guide	Min Arm
<i>Commentaire : aide à la réflexion pour la rédaction de PCA-PRA au sein du ministère peu adapté à des entités éphémères (comme les structures liées aux OPEX).</i>				

Guide pour réaliser un plan de continuité d'activité	12 juin 2013	SGDSN	Guide	Etat
<i>Commentaire : ce guide élaboré par le SGDSN présente une démarche méthodologique permettant l'élaboration concrète d'un PCA. Il est destiné aux organismes relevant de l'État, aux collectivités territoriales ainsi qu'aux entreprises.</i>				
Guide DGSIC n°5 « dispositions pratiques et techniques de continuité informatique » diffusée par note n°1323/DEF/DGSIC/SDSSI du 10 décembre 2010	10 déc. 2010	DGSIC	Guide	Min Arm
<i>Commentaire : éléments d'aide issus de retours d'expérience pour la mise en place de PCA/PRA et plus particulièrement de PCI/PRI.</i>				
Directive DGSIC n°17 portant sur l'identification et le suivi des systèmes critiques (DIR-ISSC) diffusée par note n°805/DEF/DGSIC/ du 7 juillet 2011	6 juillet 2011	DGSIC	Directive	Min Arm
<i>Commentaire : cette directive définit la méthode à mettre en œuvre par des organismes du ministère des armées en matière de systèmes critiques, les critères d'identification et de caractérisation de ces systèmes, et les dispositions de suivi de leur état de préparation. Le premier objectif est de cartographier les systèmes critiques du ministère, de les caractériser et de maintenir à jour la cartographie ainsi réalisée. Un système d'information est dit critique dès lors qu'il remplit ou supporte une ou plusieurs mission(s) essentielle(s) du ministère. Il s'agit ensuite d'établir des plans d'action et calendriers de progrès vers les objectifs de sécurité retenus et de suivre leur application. Cette démarche d'amélioration continue et itérative implique de réviser régulièrement les résultats.</i>				

4.8.3 Gestion des journaux d'événements applicatifs ou système

La gestion des journaux d'événements applicatifs ou système ou « logs » (précédemment désignés en tant que « traces », terme non approprié qui renvoie à un autre aspect de l'observabilité, cf. 6.2.7) issus des équipements des réseaux informatiques du ministère (serveurs, postes de travail, pare-feux, sondes, ...) et portant sur des données multiples (données à caractère personnel, données de trafic, de localisation, de systèmes d'information...) est couverte par plusieurs textes de portée globale engageant le ministère, notamment au regard des données à caractère personnel.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°29 portant sur les traces et leur gestion au sein du ministère de la Défense diffusée par note n°1065/DEF/DGSIC/SDSSI/NP du 12 novembre 2013	12 nov.2013	DGSIC	Directive	Min Arm
<i>Commentaire : la directive n°29 a pour objet la définition des principes, des buts et des objectifs ainsi que des moyens généraux pour parvenir à une gestion des traces efficiente au ministère des armées. Elle stipule notamment que la mise en œuvre des traces répondant au juste besoin est obligatoire et que le format doit être celui de la RFC 5424 (syslog).</i>				
Arrêté du 27 janvier 2023 autorisant la mise en œuvre de traitements automatisés de gestion des traces relatives aux systèmes d'information et de communication du ministère de la défense https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047089467	27 janvier 2023	Min Arm	Arrêté	Min Arm
Directive DIRISI n°270 relative à la mise sous supervision de sécurité	1 décembre 2018	DIRISI	Directive	Armées
<i>Commentaire : cette directive décline la directive Cyber sur la cyber surveillance (cf. §4.1.1.6 Cyberdéfense et Lutte Informatique Défensive (LID)). Elle présente le dispositif mis en place par le CND pour assurer la mise en supervision de sécurité des SI dans le cadre de l'amélioration de leur « défendabilité ». Elle s'adresse aux acteurs SIC et SSI (RCP, DP, RSSI, architectes SSI, SOC...) et présente notamment le contexte organisationnel et un référentiel d'exigences permettant une mise sous supervision de sécurité de leur système d'information.</i>				

4.8.4 Maintien en condition de sécurité (MCS) - composant technique

Voir également : cf. 4.2.2

DECOS-S : Sur l'Intradef, le service DECOS-S⁵³ opéré par le CND permet le déploiement des correctifs de sécurité de systèmes soutenus sur l'Intradef : le périmètre couvert concerne les systèmes et produits Microsoft, les produits Adobe et les distributions LINUX soutenues par le CND (incluant les produits RedHat) au travers des mécanismes techniques idoines et adaptés (WSUS pour les serveurs Windows, dépôts LINUX, suite RedHat Satellite pour les serveurs RHEL rattachés, bases de signatures antivirales, ...).

A partir de 2024, DECOS-S est progressivement remplacé par MEDUSA, dépôt généralisé d'artefacts binaires en cours de réalisation par l'AND (cf. §6.2.1.3 *Dépôt d'artefacts*)

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°111 d'emploi DECOS-S diffusée par note n°400954/DEF/DIRISI/DIR	25 février 2014	DIRISI	Directive	Armées
<i>Commentaire : cette directive d'emploi décrit le périmètre et l'organisation relative au projet DECOS-S et liste les produits et systèmes couverts.</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Correctifs de sécurité	Projet DECOS-S	DIRISI	Ce système opéré par le CND permet le déploiement de correctifs de sécurité pour :- les systèmes et produits Microsoft- les systèmes Centos 7, AlmaLinux 8+ et RedHat 8+ (ainsi que Debian et Ubuntu)- les produits d'Adobe- des middlewares et bibliothèques logicielles non présents dans les dépôts précédents	R / S	Intradef
<i>Commentaire : les systèmes d'exploitation Debian (assujetti principalement à un usage SIE en voie d'extinction et Ubuntu non autorisé) ne sont mentionnés que par complétude de description d'usages historiques en cours de suppression. Cela signifie que leur présence dans le dépôt DECOS-S ne vaut pas recommandation d'utilisation. Le support des systèmes d'exploitation Centos a été arrêté par RedHat en juin 2024. Le CND a toutefois souscrit une prolongation de support LibertyLinux de 3 ans de Centos 7.9 et d'un an de Centos 6.10 afin de permettre aux systèmes d'information de satisfaire à l'ensemble des prérequis C1DR sans passer par une étape intermédiaire de montée en version de système d'exploitation. Cette prolongation ne sera pas reconduite.</i>					

4.8.5 Sécurisation des flux réseaux

Document	Date	Origine	Type doc	Portée
Recommandations de sécurité relatives à IP Sec pour la protection des flux réseau. Cf. 4.5 Sécurisation des COTS	3 août 2015	ANSSI	Note technique	Toute admin.
Recommandations de sécurité relatives à TLS, édition 1.2	26 mars 2020	ANSSI	Note technique	Toute admin.
<i>Commentaire : se reporter à l'annexe 8.2 pour connaître la dernière version recommandée pour TLS</i>				

4.8.6 Sécurisation des supports de stockage

Supports classifiés de défense

⁵³ DECOS-S : Déploiement des COrrectifs de Sécurité sur l'intranet Sensible

Document	Date	Origine	Type doc	Portée
Guide n°972/SCSSI/SI relatif à la protection des supports classifiés de défense. Cf. 4.1.3 Références pour le niveau Secret	9 avril 1998	PM	Circulaire	Toute admin.
Guide technique 972-1 pour la confidentialité des informations enregistrées sur disque dur à recycler ou exporter. Cf. 4.1.3 Références pour le niveau Secret	17 juillet 2003	PM	Circulaire	Toute admin.
<i>Commentaire : ce document traite de la protection, manipulation et destruction des supports d'information tels que disques durs, clé USB, carte à puce, etc.</i>				

Supports amovibles sur l'Intradef

Document	Date	Origine	Type doc	Portée
Concept d'emploi des stations blanches NG sur l'Intradef sous timbre n°403275 /DEF/DIRISI/SDSSI du 18 juin 2013 diffusé par note n°403277/DEF/DIRISI/DIR du 18 juin 2013	18 juin 2013	DIRISI	Concept d'emploi	Intradef

4.8.7 Hébergement / Virtualisation

Document	Date	Origine	Type doc	Portée
Directive DGSIC n° 32 portant sur la sécurité de l'hébergement des SI au sein du ministère diffusée par note n°170/DEF/DGSIC/SDSSI/NP du 11 mars 2014	11/03/2014	DGSIC	Directive	Min Arm
<i>Commentaire : cette directive définit les exigences de sécurité que doivent respecter les opérateurs du ministère en matière d'hébergement. Les règles se décomposent en deux grandes parties : celles applicables à l'opérateur et à son système d'information, celles applicables aux systèmes informatiques hébergés, classées en fonction du niveau d'hébergement. Lorsque le système informatique ou l'application est hébergé à l'extérieur du ministère, les directions de projet peuvent s'inspirer des règles qui y sont contenues afin de rédiger le contrat avec l'opérateur. Elle n'a pas pour but d'imposer des architectures aux opérateurs au sein des datacenters, ni de traiter des réseaux de transit.</i>				

Cf. aussi §5.1.2 *Virtualisation*

4.8.8 Supervision de la sécurité, LID

4.8.9 Télémaintenance

La disponibilité de fonctionnalités de plus en plus riches au niveau du poste de travail, combinée à la diminution des ressources humaines techniques, entraînent un recours généralisé à des opérations d'assistance ou de maintenance à distance.

Constatant que la sécurité n'est pas toujours bien appréhendée pour réaliser ce type d'interventions et que les solutions utilisées amènent des vulnérabilités et octroient aux intervenants des droits importants, l'ANSSI a publié un certain nombre de notes techniques permettant de mieux sécuriser le recours à la téléassistance.

Document	Date	Origine	Type doc	Portée
Recommandations de sécurité relatives à la téléassistance (MS-RDP et VNC). Cf. 4.5 Sécurisation des COTS	13 janvier 2017	ANSSI	Guide technique	Toute admin.
Recommandations de sécurité relatives à IP Sec pour la protection des flux réseau V1.1 Cf. 4.5 Sécurisation des COTS	3 août 2015	ANSSI	Note technique	Toute admin.
Recommandations pour un usage sécurisé d'(Open)SSH V1.3 (cf. 4.5 Sécurisation des COTS)	17 août 2015	ANSSI	Note technique	Toute admin.

4.8.10 Sauvegardes

Cf. §6.2.6 *Sauvegarde / restauration*

4.8.11 Gestion de configurations de sécurité

Le format **SCAP** (Security Content Automation Protocol) est le protocole préconisé par le ministère pour mettre en œuvre des outils de gestion et de contrôle des configurations de sécurité.

C'est une **synthèse interopérable de spécifications ouvertes énumérant** les noms des produits utilisés, **les défauts des logiciels et les problèmes de configuration**. Dans certains cas, il permet, grâce notamment à des mécanismes de classement, d'évaluer l'impact de la découverte des problèmes de sécurité.

SCAP offre un moyen :

- d'évaluer la sécurité des failles et les erreurs de configuration des logiciels dans l'entreprise de manière transparente, interopérable, reproductible et automatisable ;
- d'évaluer à chaque instant la posture de sécurité du système d'information ;
- de gagner du temps en orientant le travail des équipes d'administration ou d'audits sur des aspects plus importants de la sécurité.

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
SCAP	Security Content Automation Protocol. Ensemble de spécifications entretenues par le NIST ⁵⁴ et accessibles sur le site http://scap.nist.gov . Le ministère retient essentiellement les spécifications suivantes : • CVE (pour Common Vulnerability Enumeration), permet d'associer un numéro unique à chaque nouvelle vulnérabilité (indépendamment de la référence donnée par l'éditeur). Cette norme est aujourd'hui incontournable dans le domaine de gestion de vulnérabilités ; • CCE (pour Common Configuration Enumeration), fournit un identifiant standard et un dictionnaire des problèmes de configuration liés à la sécurité ; • CPE (pour Common Platform Enumeration), fournit un système de nommage permettant de désigner de façon non ambiguë des composants informatiques tels que machine, système d'exploitation ou paquetage logiciel ; • XCCDF (pour eXtensible Checklist Configuration Description Format), fournit un standard XML pour la spécification des listes de tests et la publication des résultats des tests ; • OVAL (pour Open Vulnerability Assessment Language), fournit un standard XML pour les procédures de test des défauts liés à la sécurité des logiciels, des problèmes de configuration et des correctifs ; • CVSS (pour Common Vulnerability Scoring System), fournit un système de notation compris entre 0 et 10 pour évaluer la dangerosité d'une vulnérabilité.	R	Min Arm

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestion de conformité	OpenSCAP	Opensource	Chaines CI/CD mises en place par l'AND	E / N	Intradef

« **Conformité serveurs et postes de travail** » : Le système de gestion de la Conformité serveurs et postes de travail a pour objectif de pouvoir réaliser un contrôle automatique et périodique de la conformité (conformité aux référentiels de sécurité et à l'annexe 8 du CCT) des serveurs et des postes

⁵⁴ NIST : National Institute of Standards and Technology

de travail. Il utilise le standard SCAP. Il propose de plus un affichage des vulnérabilités associées à la pile logicielle détectée.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestion de conformité	Conformité Serveurs et postes de travail	Min Arm	Solution ministérielle en cours de déploiement sur les serveurs et totalement déployée sur les postes de travail .	R / S	Intradef

4.9 Divers

La sécurité est transverse à tous les segments couverts par le CCT. Des préconisations relatives à la sécurité se retrouvent notamment dans les chapitres listés ci-après :

3.1.1.5 Socle technique logiciel du poste de travail

3.1.5 Sécurité [SU-SSO, SU-CHI, SU-SIG]

3.1.6 Mobilité [SU-AN, SU-ITN]

5.1.1 Système d'exploitation [OS]

5.1.2 Virtualisation

5.1.8.1 Téléphonie classique

5.1.8.2 Téléphonie chiffrée

5.2.5 ToIP / VoIP

5.2.6 Réseaux sans fils

6.1.1 Références générales sur l'hébergement

7.4 Conception et codage

5 INFRASTRUCTURE

5.1 Matériels, OS, virtualisation et conteneurisation

Ce paragraphe décrit les matériels, OS et composants.

5.1.1 Système d'exploitation [OS]

5.1.1.1 Système d'exploitation client

Document	Date	Origine	Type doc	Portée
Configuration sécurisée de Windows 10 V3.1 : (cf. 4.5 Sécurisation des COTS)	18 mars 2022	DGA MI	Guide technique	Min Arm
<i>Commentaire : Windows 10 a atteint sa fin de vie et son remplacement s'achève sur Intradef. Cette référence est toutefois conservée pour les usages résiduels dans l'attente d'une référence équivalente pour Windows 11.</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
OS Client	Windows Mobile	Microsoft	Ces OS ne sont plus maintenus et ne doivent en aucun cas être utilisés (y compris les versions 6.5 et 10)	I / N	Min Arm

OS Client	Windows	Microsoft		★ / ★	SIA S-SF SIA FrOps
OS Client	Android version	Google		★ / ★	★
OS Client	Autres OS		Tablettes et autres, soumis à stricte dérogation suivant cas d'usage.	D / N	

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

5.1.1.2 Système d'exploitation serveur

Document	Date	Origine	Type doc	Portée
CIS Benchmark		CIS	Guide technique	Min Arm
<i>Commentaire: les guides du CIS⁵⁵ sont accessibles à cette URL: ils couvrent de nombreux systèmes d'exploitation récents et plus anciens pour serveurs et postes de travail et notamment ceux utilisés au sein du Ministère</i>				

- **CENTOS** : Suite au changement de stratégie annoncé en décembre 2020 par REDHAT/IBM, le soutien de CentOS 8 s'est arrêté en novembre 2022, et celui de CentoS 7.9 en juin 2024. Toutefois, la société Suse prolonge le support de ce dernier via son offre Suse Liberty Linux, support qui a été souscrit pour 3 ans non renouvelable par le CND en 2024 afin notamment de permettre aux directions de projet et d'application de procéder aux ajustements nécessaires à la migration vers le C1DR dans les conditions de MCO et de MCS requises. Seule la version 7.9 est concernée. Les versions mineures antérieures (de 7.1 à 7.8) ne doivent plus être utilisées. Tout système d'information qui utiliserait de telles versions doit impérativement procéder à la montée de version dès à présent. A noter la possibilité de bénéficier sur demande au CND d'un support de même type et pendant 1 an seulement pour la version 6.10. Les demandeurs devront s'identifier auprès de la DSI Socle.
- **ALMA LINUX** : Suite à l'instruction du sujet et sa validation en CECNUM de juin 2022, Alma Linux est devenue la distribution Linux communautaire de substitution à CentOS sur les Intranets ministériels (disponible sur C1DR et PICSEL, à venir sur C1NP). Ceci a été confirmé depuis, après vérification de la capacité d'AlmaLinux à poursuivre ses activités dans la durée suite à la limitation d'accès aux sources des paquets par RedHat à ses seuls clients sous licence. AlmaLinux, qui conserve son principe de compatibilité binaire avec RedHat Enterprise Linux, mais ne recherche plus le principe d'identité parfaite en matière de correctifs, ce qui lui permet de les appliquer sans attendre que RedHat le fasse (RedHat n'appliquant d'ailleurs pas systématiquement tous les correctifs). Le Ministère fournit des versions durcies des versions 8 et 9 d'AlmaLinux (version 9.6 à date, disponible sur C1DR et PICSEL). La version mineure 8.10 désormais disponible est une version stabilisée utilisable jusqu'au 31 mai 2029 : c'est la version à privilégier. La version 9 est encore en évolution, nécessitant quant à elle une montée de version mineure environ tous les 6 mois attendu que seule la dernière version mineure est soutenue. La version stabilisée 9.10 est attendue au premier trimestre 2027.
- **REDHAT ENTERPRISE LINUX** : L'option RedHat reste disponible et recommandée pour les SI pour lesquels le support de l'application hébergée ou les conditions d'infogérance l'imposent. La version 8.10 est disponible sur PICSEL, C1DR et C1NP. Le cycle de vie et les contraintes de la version 9 sont identiques à celles d'AlmaLinux. Les versions durcies fournies par le Ministère sont également disponibles (version 9.6 disponible à date sur PICSEL et C1DR, à venir sur C1NP). RedHat permet, moyennant souscription à la charge du projet concerné, peut assurer un support étendu pour des versions mineures paires. Sur les hébergements C1NP et C1DR, le CND a acquis des licences globales pour les versions à jour : les projets légitimes à les utiliser n'ont donc pas à les souscrire.

⁵⁵ Center for Internet Security

- **WINDOWS SERVER** : Ce système d'exploitation n'est utilisable que pour les systèmes d'information ne pouvant techniquement pas être opérés sur une distribution Linux, compte-tenu des investissements en matière de maîtrise des dépôts binaires (MEDUSA), d'automatisation (RUCHE) et de standardisation menés par le Ministère pour ses hébergements de systèmes d'information. Ceci inclut le cadre d'un hébergement VPS ou salle blanche. La migration vers Linux sera systématiquement demandée lors de toute évolution majeure ou migration vers le C1DR d'un système d'information éligible. Le personnel en charge de l'administration devra être formé en conséquence. Les versions durcies 2016, 2019 et 2022 (variante `en_US GUI`) sont respectivement disponibles sur PICSEL et C1DR. La mise à disposition sur C1NP est prévue mais n'est pas encore planifiée.

Le Ministère s'est doté d'une capacité à fournir et à tenir à jour rapidement des templates d'OS durcis et testés à destination des machines virtuelles VMWare Broadcom version 7 et 8. Ces templates sont ceux mis en œuvre dans les machines virtuelles fournies par le CND. Ils sont fournis avec une fiche de version précisant les paramètres appliqués.

5.1.1.3 Stratégie en matière de versions des systèmes d'exploitation

Afin de pouvoir maîtriser ses hébergements, le Ministère se limite en principe volontairement à maintenir au plus 2 versions majeures de systèmes d'information simultanément (par exemple Windows Server 2019 et 2022, Windows 2016 atteignant sa fin de vie, Redhat Enterprise Linux ou AlmaLinux 8 et 9) ; Windows Server 2025 pourra toutefois être autorisé après obtention de dérogation pour des services d'infrastructure et hors des structures d'hébergement de systèmes d'information opérées par le CND.

Redhat Enterprise Linux et AlmaLinux possèdent des cycles de version majeures et mineures identiques, le second se conformant au rythme du premier :

- Chaque version majeure dispose d'un support complet pendant 5 ans suivi d'une période de maintenance de 5 ans supplémentaires, RedHat apportant une possibilité d'une extension de support de 3 ans supplémentaires sur souscription, option non retenue par le Ministère⁵⁶.
- Chaque version mineure (numéroté de 8.0 à 8.9, 9.0 à 9.9 ou 10.0 à 10.9) est maintenue 6 mois (RedHat propose une extension de support 18 mois supplémentaires pour les versions x.1, x.2, x.4, x.6 et x.8 sur souscription de l'Extended Update Support, option non retenue par le Ministère). Ceci couvre une période de 4 ans et demi, la version 8.10 ou 9.10 ajoutant les 6 mois manquant pour atteindre les 5 ans de support complet indiqués précédemment.
- La dernière version mineure (8.10, 9.10 ou 10.10) dispose donc de 6 mois de support complet puis de 5 ans de maintenance complémentaires.

En conséquence, un système d'information utilisant une version 9 inférieure à la version 9.10 devra suivre le cycle des mises à jour tous les 6 mois jusqu'à atteindre la version 9.10. Attendu que les dépôts de la version mineure n-1 restent disponibles jusqu'à ce que la version n+1 devienne disponible, cette montée de version mineure devra s'achever au plus tard à ce moment (un système d'information en version 9.6 doit migrer au plus tard quand la version 9.8 est disponible, idéalement lorsque la version 9.7 est mise à disposition).

Une fois la version 8.10 utilisée, le système d'information peut adopter deux stratégies différentes :

- rester en version 8.10 (en effectuant les mises à jour régulièrement) jusqu'à ce que la version 9.10 soit disponible (environ 2 ans ½ après) : le projet dispose alors de 2 ans ½ pour effectuer cette montée de version majeure ;
- poursuivre le cycle des versions mineures 9.x tel que décrit plus haut.

A noter que la seconde stratégie implique des opérations plus fréquentes de mises à jour mais beaucoup plus faciles à mener, le changement d'une version mineure à l'autre ne présentant qu'un risque faible de dysfonctionnement.

⁵⁶ <https://access.redhat.com/support/policy/updates/errata>

De plus, l'obligation de MCS souscrite dans le cadre de l'homologation du système d'information impose de toute façon des mises à jour très régulières, et qui vont faciliter les services et les automatismes mis en place dans le cadre de la cloudification des hébergements du Ministère.

La première stratégie, qui impose également ces mises à jour régulières, conduira à des travaux beaucoup plus conséquents, et d'autant plus difficiles qu'ils sont espacés dans le temps (maintien de la connaissance, campagne de tests de non régression d'envergure ...)

Dans tous les cas, **il est impératif que les projets prévoient des tests fonctionnels de non régression** : ces travaux indispensables dans un contexte de cloudification et d'automatisation des déploiements s'avèrera en outre un investissement extrêmement rentable pour mener les indispensables campagnes de tests, lors du déploiement initial puis à chaque mise à jour mineure ou majeure, qu'il s'agisse de MCO, MCS ou d'évolution.

Pour appuyer cette démarche et renforcer sa maîtrise en la matière, le Ministère met en œuvre une usine d'images de systèmes d'exploitation durcis afin de pouvoir les générer, les tester et les mettre régulièrement et rapidement à disposition sur PICSEL, C1DR et C1NP.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
OS Server	Windows Server	Microsoft		★ / ★	★
OS Serveur	Redhat Enterprise Linux RHEL	Redhat		★ / ★	★
OS Serveur	Debian	Debian		★ / ★	★
OS Serveur	CentOS	Redhat		★ / ★	★
OS Serveur	AlmaLinux	Alma		★ / ★	★
OS Serveur	Autres distributions LINUX		Soumis à stricte dérogation après démonstration d'impossibilité d'utiliser une distribution Linux recommandée et mise en œuvre d'un durcissement équivalent. Les travaux d'automatisation de déploiement seront également à la charge du projet.	D / N	

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

5.1.1.4 Autres (équipement réseau)

Pas de référence identifiée à ce jour.

5.1.2 Virtualisation

Face aux évolutions de la technologie dans le domaine de la virtualisation et de la conteneurisation, de l'émergence de nouveaux acteurs et des changements profonds impulsés à partir de 2023 par Broadcom, nouvel acquéreur des produits américains VMWare massivement utilisés au sein du Ministère (suppression des licences perpétuelles, réduction des gammes pour contraindre à l'acquisition de l'intégralité des produits, changement des modes de calcul des prix sur des dimensionnements matériels plus élevés), il s'est avéré nécessaire d'étudier rapidement les solutions alternatives susceptibles de répondre aux besoins du Ministère.

Ces premières études ont été menées en tenant compte de multiples contraintes dont la couverture fonctionnelle (en regard des fonctions réellement utilisées actuellement), la maturité, l'exploitabilité et la maîtrise à l'échelle par le personnel du Ministère, la capacité à disposer d'un support éditeur ou

industriel adapté, la soutenabilité financière, les évolutions prévisibles du domaine dont l'interopérabilité avec les technologies Cloud, l'infrastructure as code, la conteneurisation et les retours d'expérience des entités qui en mettent déjà en œuvre au Ministère et à l'extérieur. La capacité à opérer simultanément et de façon très similaire des machines virtuelles (dont la part va progressivement décroître mais perdurer dans les prochaines années) et des conteneurs orchestrés est un critère de première importance, tout comme la mise en place d'une solution ne reproduisant pas les faiblesses de celle qu'elle doit progressivement remplacer.

Harvester est une solution opensource européenne pour une gestion mutualisée de la virtualisation (via kubevirt) et de la conteneurisation et qui se voit doté désormais de capacités de micro segmentation (kube-ovn). Cette solution doit être systématiquement étudiée, quel que soit le cas d'usage. Il s'agit d'une solution envisagée pour les C1. Elle a été testée avec succès via une preuve de concept.

Proxmox est une solution open source simple, utilisant l'hyperviseur KVM. Elle est adaptée pour le déploiement d'un faible nombre de machines virtuelles (de l'ordre de la dizaine). En revanche, elle n'est pas pleinement outillée pour gérer un nombre important de VMs, ou pour répondre à des exigences élevées de disponibilité. Les possibilités restreintes de support et la difficulté de sécurisation s'ajoutent à ces inconvénients. Elle est également dépourvue de fonctionnalités de micro-segmentation. L'usage de conteneurs LXC, attendu que cette technologie diffère de celle retenue par le Ministère - images OCI - est de ce fait interdit au Ministère dans un objectif de rationalisation et de standardisation nécessaire à une maîtrise globale. Promox permettant toutefois d'exécuter des technologies de conteneurs conformes, ceci ne constitue pas un point bloquant.

Nutanix est une solution d'hyperconvergence basée sur des solutions propriétaires. Elle embarque l'hyperviseur AVH (Acropolis HyperVisor), dérivée de KVM. Elle apporte des fonctionnalités similaires à VMWare (calcul, stockage, gestion réseau, gestion centralisées, scalabilité horizontale, réplication et haute disponibilité, conteneurisation...). Elle pourrait être adaptée pour des besoins de type datacenter (de l'ordre de la centaine voir des milliers de VM), mais cet emploi n'aurait pas de sens car il impliquerait des investissements conséquents pour retrouver une situation analogue à la situation actuelle avec simplement un éditeur américain différent. Le Ministère estime, après étude, que le modèle hyperconvergé n'est pas adapté pour les hébergements dans ses datacenters, du fait notamment de la gestion dédiée des réseaux des datacenter au sein de l'IPFabric - GARD - et des taux de duplication que permettent le regroupement du stockage en baie grâce à l'homogénéité des systèmes d'exploitation utilisés.

Openshift utilise également l'hyperviseur KVM. Elle offre des fonctionnalités similaires à celles de VMWare mais en se basant sur des technologies recommandées (kubernetes et kubevirt) incitant toutefois à recourir à des outils spécifiques non standards, via la documentation notamment - cette dernière restant cependant de bonne qualité. Bien que cette solution pourrait donc être adaptée pour des besoins de type datacenter (de l'ordre de la centaine voir des milliers de VM), elle n'apporte pas de différenciant significatif avec la solution mentionnée précédemment. S'y ajoutent une certaine dépendance à l'éditeur IBM et une relative complexité de mise en œuvre, notamment dans sa déclinaison sans support nécessitant des mises à jour fréquentes qui amènent à ne pas la recommander.

L'usage des briques VMWare (l'hyperviseur ESXi, NSX, vSAN...), encore largement utilisé dans le ministère, notamment dans les datacenters CND, reste autorisé. Son utilisation pour de nouveaux projets s'inscrivant dans la durée (2 à 3 ans) est en revanche déconseillée. Dans tous les cas, il est recommandé de rejoindre les offres d'hébergement ministérielles à chaque fois que possible. Dans le cas contraire, il conviendra d'éviter de recourir aux fonctionnalités spécifiques pour éviter un enfermement qui rendrait la migration ultérieure vers une nouvelle solution plus difficile voire impossible, surtout sous pression d'augmentations tarifaires significatives qui ne sont pas à exclure. L'usage de déploiement en infrastructure as code (Terraform notamment), constitue un moyen de rester relativement agnostique de la solution de virtualisation utilisée et facilitera donc ces migrations.

Hyper-V, utilisé en particulier pour les briques du tier 0 et l'hébergement en OME, dispose d'un ensemble de fonctionnalités plus limité et d'une ressource de compétences beaucoup plus comptée au sein du Ministère, raison pour laquelle elle n'est pas non plus recommandée hors de déploiements historiques ou ponctuels de petite envergure.

Document	Date	Origine	Type doc	Portée
Guide EMO.GUI.R4.005 Format des VLAN v1.0 cf. 8.4.6 Nommage VLAN	01 mars 2022	DIRISI	Guide	Min Arm
<i>Commentaire : ce guide a pour objet de définir et de permettre de contrôler l'utilisation des VLAN, mis en œuvre pour les réseaux de desserte des sites du Ministère et de définir de manière normée la définition : • du périmètre d'utilisation des VLAN ;</i> • du standard de nommage des VLAN ; • des principes d'attribution des ID VLAN ; • des principes de mise en relation de l'adressage réseau entre le 3ème octet d'adressage avec l'utilisation des VLAN ; • du processus des demandes de création de VLAN				
Sécurisation d'une infrastructure VMware version 1.0	02 avril 2024	ANSSI	Note	Toute admin.
<i>Commentaire : https://messervices.cyber.gouv.fr/documents-guides/anssi-fondamentaux-securisation_infrastructure_vmware_v1-0.pdf</i>				
Recommandations de sécurité pour les architectures basées sur VMware vSphere ESXi cf. 4.5 Sécurisation des COTS	25 mai 2016	ANSSI	Note	Toute admin.
<i>Commentaire : https://messervices.cyber.gouv.fr/documents-guides/np_vmwareesx_notetech_v1.pdf</i>				
Problématiques de sécurité associées à la virtualisation des systèmes d'information version 1.1 , cf. 4.5 Sécurisation des COTS	26 septembre 2013	ANSSI	Note technique	Toute admin.
<i>Commentaire : https://messervices.cyber.gouv.fr/documents-guides/NP_Virtualisation_NoteTech_v1-1.pdf</i>				
Recommandations pour la sécurisation des commutateurs Ethernet et l'utilisation des VLAN cf. 4.5 Sécurisation des COTS	22 février 2010	DGA MI	Guide technique	Min Arm

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Hypervision / Virtualisation	Virtualization	SUSE	Anciennement Harvester. Rancher + kubernetes + Kubevirt. Assujetti à l'absence d'offre d'hébergement dans le contexte visé. Cela implique de monter son propre hébergement en salle blanche.	R / E	Tout intranet
Hypervision / Virtualisation	Proxmox VE	Proxmox	Assujetti à un besoin de gérer un faible nombre de VMs (de l'ordre de la dizaine). L'usage de conteneurs LXC est interdit. Assujetti à l'absence d'offre d'hébergement dans le contexte visé. Cela implique de monter son propre hébergement en salle blanche.	A / N	Tout intranet
Hypervision / Virtualisation	AHV	Nutanix	Appliance ; adapté pour un grand nombre de VMs (100+) ; assujetti à l'absence d'offre d'hébergement dans le contexte visé. Cela implique de monter son propre hébergement en salle blanche.	A / N	Tout intranet
Hypervision / Virtualisation	Openshift	RedHat	Adapté pour un grand nombre de VMs (100+) ; assujetti à l'absence d'offre d'hébergement dans le contexte visé. Cela implique de monter son propre hébergement en salle blanche.	A / N	Tout intranet
Hypervision / Virtualisation	ESXi	Broadcom	Ex VMWARE. Assujetti à l'absence d'offre d'hébergement dans le contexte visé. Cela implique de	A/S	Tout intranet hors intrasan

			monter son propre hébergement en salle blanche.		
Hypervision / Virtualisation	ESXi	Broadcom	Ex VMWARE. Il est recommandé d'utiliser l'ESXi mis à disposition par le SSA.	R/-	Intrasan
Hypervision / Virtualisation	Hyper-V	Microsoft	Assujetti à l'absence d'offre d'hébergement dans le contexte visé ou à des configuration projetables (théâtre et bâtiments tous intranets et sites de proximité STC-IA V02). Cela implique de monter son propre hébergement en salle blanche.	A/S	IntradeF, SIA S-SF, SIA FrOpS

★ / ★ pour les recommandations sur les versions voir le détail en annexe **8.2.1 Pile logicielle : liste des produits**

Pas de référence identifiée à ce jour pour les sujets suivants :

- Virtualisation applications
- Virtualisation poste de travail
- Virtualisation stockage, sauvegarde
- Virtualisation réseau

5.1.3 Conteneurisation

Document	Date	Origine	Type doc	Portée
Cadre technique de mise en œuvre des conteneurs au sein du Ministère des Armées et des Anciens Combattants version 1	S1 2026	CND	Cadre technique	Min Arm
<i>Commentaires : Ce document en cours de validation décrit les règles et bonnes pratiques applicables par les différents acteurs pour mettre en œuvre les technologies d'orchestration de conteneurs au sein du Ministère afin d'assurer un bon fonctionnement de l'écosystème dans le respect des enjeux de maîtrise dans la durée. Il a été élaboré en cohérence avec la recommandation ADatP-5673 également en cours de finalisation.</i>				
NATO STANDARD ADatP-5673 Deployment of applications and services in trusted containers Edition 1, version 1	mars 2026	OTAN	Recommandation OTAN	Environnement OTAN
<i>Commentaires : l'objet de ce document est de standardiser la façon dont les conteneurs sont créés, partagés et utilisés dans un scénario de fédération afin de bénéficier des solutions de conteneurisation et des technologies "cloud native" à des fins d'interopérabilité, de sécurité, de passage à l'échelle, de disponibilité et de survabilité, entre autres avantages. En complément, ceci rendra possible l'hébergement de solutions à l'état de l'art de l'industrie qui ne peuvent pas fonctionner avec les anciennes technologies ni avec la façon avec laquelle les applications sont actuellement déployées.</i>				

Les avantages généralement reconnus de la technologie des conteneurs sont :

- rapidité de démarrage : un conteneur démarre en quelques secondes voire moins, là où une machine mettra généralement plusieurs minutes, ce qui induit une capacité d'adapter en temps réel la capacité face à un pic de charge.
- légèreté et optimisation de la consommation des ressources : parce que les conteneurs utilisent le système d'exploitation de leur hôte, contrairement aux machines virtuelles qui ont chacune le leur, ils possèdent une **empreinte réduite** (RAM et CPU).

- immutabilité⁵⁷ : par principe, le conteneur est un composant généralement sans état : Les modifications sont réalisées par génération d'un nouveau conteneur qui vient remplacer l'ancien, simplifiant drastiquement les actes d'exploitation.
- facilité de déploiement : un conteneur prédéfini est auto-suffisant et isolé de son hôte et peut donc être directement déployé en production sur celui-ci en s'affranchissant de tout problème de dépendance logicielle.

Les qualités évoquées ci-dessus font de la technologie de la conteneurisation un outil tout à fait adapté pour répondre à certains besoins engendrés par la transformation numérique qui anime actuellement le ministère.

Il convient néanmoins de rappeler que l'emploi de ces solutions n'est pas sans incidence sur les pratiques en vigueur au sein du Ministère tant en termes d'hébergement, de pratiques d'exploitation et de maintien en condition de sécurité.

Au niveau de l'exploitation de ces solutions, la remise en cause de certains paradigmes et approches en la matière nécessite un accompagnement et une évolution des mentalités et pratiques en matière de développement, de tests, d'administration, de gestion et d'exploitation de ces structures et des applications qui en dépendent. De même, il s'agit pour le ministère d'accompagner la montée en compétences du personnel qui est associé à cette évolution. Enfin, ces nouveaux modes de travail doivent s'intégrer avec ceux des systèmes classiques (nombre de systèmes d'information ne tireraient aucun bénéfice à adopter une architecture conteneurisée) et avec la démarche DevSecOps que le Ministère met progressivement en place dans le cadre notamment de l'opération de cloudification de ses hébergements.

Concernant la sécurité de l'information, les conteneurs présentent, par défaut, une étanchéité moindre qu'une VM : des règles de conception (*rootless*), de durcissement et des frameworks de sécurité devront être choisis pour assurer le niveau de sécurité requis. L'approche « boîte noire » des conteneurs pose la problématique de la gestion des images, de leur source, de leur sécurité, de leur maintien en condition opérationnelle et de sécurité et de leur gestion. Le modèle à l'échelle est en train d'être construit afin d'offrir les garanties nécessaires au déploiement d'images externes sur les intranets ministériels (fourniture du dockerfile ou équivalent, vérification des règles de construction et des dépendances, contrôle de la composition via des outils d'analyse introspectifs ou via fourniture du SBOM⁵⁸, ...).

Techniquement, l'éclatement du système d'information dans de multiples conteneurs et l'absence de visibilité directe sur leur composition et leur fonctionnement intra et inter conteneurs va entraîner une complexification significative de la tâche des exploitants qu'il faudra au préalable contrebalancer par le recours à des outils d'orchestration et de supervision adéquats.

Le paragraphe **3.2.1.2 Démarche et principes** rappelle les grands principes d'architecture logicielle à mettre en œuvre afin de concevoir une application éligible à ce type d'hébergement.

Le Ministère fournit cette capacité : disponible sur PICSEL à des fins de développement et d'expérimentations et sur le C1DR pour les SI en production.

Les systèmes d'information hébergés en orchestration de conteneurs sont soumis aux mêmes exigences de gouvernance que ceux hébergés en machines virtuelles.

Règle	Énoncé	Statut	Portée
CCT_R10_1	Il est OBLIGATOIRE que les solutions retenues en matière de conteneurisation ou d'outillage de la conteneurisation respectent les standards OCI.	O	Intradef, C1NP

⁵⁷ Infrastructure immuable (immutable infrastructure) : Les images de machines virtuelles ou de conteneurs sont générés à partir de rôles ansible et d'un dépôt de composants logiciels maîtrisé ; une fois testées, ces images servent à instancier le système d'information en production. Toute modification de ces instances nécessite de régénérer de nouvelles images et de les instancier en production pour remplacer les anciennes. Aucune modification directe des instances en production n'est permise.

⁵⁸ Software Bill of Material : liste de l'exhaustivité des composants logiciels utilisés et livrés, toutes dépendances comprises, dans un format normalisé comprenant également les versions précises associées.

CCT_R11_1	Il est RECOMMANDÉ que les solutions retenues en matière de conteneurisation ou d'outillage de la conteneurisation respectent les standards OCI.	R	Tout intranet hors Intradef, hors Intrasan
-----------	--	---	--

A titre d'exemple, les runtimes `containerd`, `cri-o` ou `runc` seront envisageables, tandis que `lxc/lxd` sera refusé dans le premier cas et déconseillé dans le second.

Le fait que `podman` ou `docker` utilisent ou puissent utiliser l'un des runtime OCI ne les rend pas pour autant recommandés pour un déploiement en production où les contraintes d'exploitabilité et de maîtrise globale nécessitent des solutions dotées des fonctions nécessaires. Hors environnements de test ou de développement, il conviendra d'utiliser une distribution Kubernetes.

Les travaux menés cette année ont conduit le Ministère à sélectionner les technologies suivantes, dans le respect des standards OCI.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Hébergement en orchestration de conteneurs	CaaS C1DR	Min Arm	Service d'orchestration de conteneurs sur base de Kubernetes (distribution RKE2)	R / S	Intradef
<i>Commentaire : Un service équivalent est mis en place à des fins de développement et d'expérimentations sur la plateforme PICSEL. Tout système d'information conteneurisé sur Intradef doit être déployé via cette offre.</i>					
Hébergement en orchestration de conteneurs	CaaS C1NP	Min Arm	Service prévu mais non planifié à date	E / E	C1NP
<i>Commentaire : un service identique à celui mis en place sur la plateforme C1DR sera mis en œuvre ensuite sur la plateforme C1NP. Dans l'attente, cette plateforme ne permettra pas de recourir à la technologie des conteneurs.</i>					
Hébergement en orchestration de conteneurs	CaaS IST-C 3E	Min Arm	Service d'orchestration de conteneurs sur base de Kubernetes (distribution RKE2)	R / S	I3E – IST
<i>Commentaire : l'hébergement en conteneur est mis en œuvre au sein des SI d'hébergement et métier de l'intranet IST secret du site de Bruz ainsi que pour le domaine 3E. Les applications/SI candidats sont soumis aux règles d'hébergement émises par l'intranet d'accueil. Les travaux de l'intranet IST-C seront reconduits sur les SI nationaux RI3E DR et S. Le S2NA a une capacité à déployer et utiliser des solutions d'orchestration de conteneurs sur la base Kubernetes.</i>					
Orchestracteur	Kubernetes	CNCF	Orchestracteur de conteneurs de référence, développé initialement par Google et retenu pour les offres de conteneurisation cloud C1 du Ministère.	A / N	Min Arm
<i>Commentaire : une nouvelle version de Kubernetes est publiée tous les 4 mois et est soutenue pour environ 1 an. Les directions de projet doivent donc organiser en conséquence pour soutenir ce rythme de mise à jour. La complexité des écosystèmes nécessaires pour faire fonctionner l'ensemble des briques nécessaire à l'orchestration de conteneurs plaide pour le recours à une distribution.</i>					
Distribution	RKE2	CNCF/SUSE	Ou « RKE Government » : ensemble de composants assemblés en vue de répondre aux besoins induits par l'orchestration de conteneurs. Distribution retenue pour les offres de conteneurisation cloud C1 du Ministère.	A / N	Min Arm
<i>Commentaire : RKE2 a été retenue pour son adéquation à l'environnement de déploiement hors connexion Internet (dite « air gap ») et le niveau de sécurisation nativement intégré dont l'application du durcissement CIS (v1.7 ou v1.8) et la conformité FIPS 140-2 avec un minimum d'intervention des exploitants. Chaque version est maintenue environ 1 an, la fin de vie survenant environ 2 mois après. Les projets doivent s'organiser en conséquence pour assurer des montées de version sur une base annuelle et assurer</i>					

l'application des mises à jour dans l'intervalle (<https://www.suse.com/lifecycle#rke2>). C'est pourquoi, il est recommandé d'utiliser un gestionnaire de cluster afin d'être capable d'assurer le MCS et le MCO.

Moteur de conteneurisation	Containerd	CNCF	Par extension, tout moteur s'appuyant sur cet exécutable. Inclus dans la distribution RKE2 et retenu pour les offres de conteneurisation cloud C1 du Ministère.	A / N	Min Arm
Moteur de conteneurisation	Podman		Uniquement en mode rootless avec runtime runc, hors environnement de production	R / -	Intrasan
Moteur de conteneurisation	Docker	Docker	Uniquement avec runtime runc, hors environnement de production	A / -	Intrasan
HCI	Virtualization	CNCF/SUSE	Anciennement Harvester, solution sous licence libre pour clusters hyper convergés. Assujetti aux environnements ne disposant pas d'une solution apportée par le socle	A / N	Min Arm
Gestion de clusters	Rancher	CNCF/SUSE	Solution sous licence libre qui permet de piloter des ensembles de clusters et de gérer les ressources Kubernetes déployées. Retenu pour les offres de conteneurisation cloud C1 du Ministère.	A / N	Min Arm
<i>Commentaire : Rancher embarque un grand nombre de produits prépackagés sous formes de charts Helm disponibles dans le catalogue de l'application. En cas de déploiement via Rancher, la version à privilégier est la version proposée par Rancher. Toutefois les modules sont tous installables de façon indépendante, ce qui permet de remédier à une vulnérabilité. Dans le cas où aucune version n'est spécifiée pour un produit du fait d'un cycle d'évolution trop rapide, il conviendra de se reporter directement à la documentation du produit.</i>					
<i>Commentaire 2 : Rancher est une application en conteneur qui s'exécute dans un cluster dédié avec des composants imposés (INGRESS NGINX comme composant CNI par exemple). En conséquence, les composants listés ci-après ne sont utilisables que dans les autres clusters.</i>					
Interface réseau pour conteneurs	Cilium	CNCF/Isovalent	Greffon de gestion du réseau sur un cluster Kubernetes reposant sur l'eBPF et permettant la création de politiques réseaux avancées. Inclus dans la distribution RKE2 et retenu pour les offres de conteneurisation cloud C1 du Ministère.	A / N	Min Arm
Interface réseau pour conteneurs	Calico	CNCF/Tigera	Greffon de gestion du réseau sur un cluster Kubernetes reposant sur l'eBPF et permettant la création de politiques réseaux avancées. Inclus dans la distribution RKE2.	A / N	Min Arm
Contrôle d'admission	Kyverno	CNCF / Nirmata	Moteur de contrôle d'admission (gestion de la conformité et de la configuration)	A / N	Min Arm
Gestionnaire de backup	Velero	CNCF / SUSE	Solution de sauvegarde et restauration de clusters Kubernetes Choisir la version en fonction du support de la version Kubernetes (cf. documentation Velero)	A / N	Min Arm

Gestionnaire de backup	Kasten	CNCF / VEEAM	Solution de sauvegarde très fin et restauration de clusters et ressources Kubernetes. Permet d'offrir du « Backup as a service » en fonction de l'implémentation choisie. Permet également la migration simple de clusters.	A / N	Min Arm
Gestionnaire de backup	Px Backup	Pure Storage	Solution de gestion de stockage sur baies Pure Storage.	A / N	Min Arm
Stockage	Plugin CSI vSphere	VMWare	Permet de monter des disques vSphere sur les nœuds d'un cluster Kubernetes afin de créer des volumes persistants	A / N	Min Arm
Stockage	Portworx	Pure Storage	Solution de gestion de stockage sur baies Pure Storage.	A / N	Min Arm

★ / ★ pour les recommandations sur les versions voir le détail en annexe 8.2.1* **Pile logicielle : liste des produits**

Les systèmes et projets quel que soit leur domaine d'application (big data, projets applicatifs, ...) ne disposant pas dans l'environnement concerné d'une offre de service d'hébergement en orchestration de conteneurs et souhaitant mettre en œuvre ces technologies devront donc effectuer une demande de dérogation auprès du CND. Ceci permettra de recenser les usages envisagés et de vérifier, avec les équipes concernées, la pertinence du recours à la conteneurisation. Une attention toute particulière sera systématiquement portée sur la gestion et la maîtrise des images utilisées.

Document	Date	Origine	Type doc	Portée
Guide ANSSI de recommandations de sécurité relatives aux déploiements de conteneur docker version 1.0, cf. 4.5 Sécurisation des COTS	23 septembre 2020	ANSSI	Note technique	Toute admin.
<i>Commentaires : ce document présente les bonnes pratiques de sécurité relatives au déploiement et à l'exécution de conteneur Docker (le Docker daemon et la gestion des images Docker sont hors de périmètre de ce guide)</i>				

L'intérêt de la technologie d'orchestration des conteneurs réside également dans son intégration de la chaîne DevSecOps mise en place pour assurer un cycle rapide de déploiement des applications et de leurs mises à jour. Cet aspect, partie intégrante de la démarche de cloudification en cours, s'appuie sur des capacités GitOps côté production et un outillage CI/CD DevSecOps adossé à la plateforme PICSEL.

Dans les environnements de niveau secret⁵⁹, en attendant la mise en place d'une offre de service d'hébergement en orchestration de conteneurs mutualisée à même de garantir une exploitation maîtrisée de conteneurs en production, le recours aux conteneurs, demeure soumis à une demande de dérogation, notamment afin de s'assurer du bon emploi de la technologie et de la capacité à rejoindre les offres ministérielles dès lors qu'elles seront disponibles.

Par ailleurs, le recours à des conteneurs mis en œuvre sur serveurs lors des phases de développement et de test pour lesquelles ils sont parfaitement adaptés est pleinement autorisé. PICSEL dispose d'une offre Kubernetes à cet effet.

Enfin, l'utilisation de conteneurs sur le poste client (PC, tablette, ...) est, quant à elle, interdite (fonctionnement en mode serveur proscrit, complexité de l'exploitation du poste). Le paramétrage des postes clients Windows bloque toute exécution de conteneurs.

⁵⁹ à noter qu'Artemis.IA dispose d'une instance hébergée sur le réseau S-SF et offre une capacité d'hébergement en orchestration de conteneurs dédiée aux usages d'IA et de Big Data.

5.1.4 Poste terminal : fixe / mobile (portable, smartphone, tablette)

Configuration logicielle : cf. §3.1.1.5 Socle technique logiciel du poste de travail

Configuration matérielle : pas de référence identifiée à ce jour

Document	Date	Origine	Type doc	Portée
Recommandations de configuration matérielle de postes clients et serveurs x86 version 1.0, cf. 4.5 Sécurisation des COTS	25 mars 2015	ANSSI	Note technique	Toute admin.
<i>Commentaire : ce document traite essentiellement de mécanismes matériels présents ou prévus sur architecture x86 et de recommandations quant à leur usage. Il aborde également des éléments de configuration qu'il convient de vérifier lors du paramétrage du BIOS d'un ordinateur.</i>				

5.1.5 Impression et scanners

Cf. 3.1.3.3 Impression – édition multifonction [SU-IMP]

5.1.6 Stockage

Document	Date	Origine	Type doc	Portée
Concept d'emploi et SLR sur le stockage des données				
<i>Commentaire : ce document est référencé en §3.1.4 Gestion des données</i>				
Directive DIRISI n°245 relative à l'exploitation et au soutien d'IRIS version 1.0, cf. §3.1.4 Gestion des données	2 mai 2018	DIRISI	Directive	Intradef
<i>Commentaire : cette directive précise le service offert par IRIS, l'organisation et le fonctionnement de l'infrastructure IRIS ainsi que les éléments relatifs à l'exploitation, le soutien et les responsabilités des acteurs.</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Stockage	IRIS sur une base de Scality	CND	Stockage objet de fichiers et métadonnées au travers du protocole S3 et de données froides (archivage, sauvegarde)	R / S	Intradef
<i>Commentaire : cette solution (Infrastructure Résiliente et Intègre de Stockage) est un service d'infrastructure de stockage extensible de données non structurées (de taille supérieure à 60 ko) offrant plusieurs pétaoctets pour les besoins de l'infrastructure (sauvegardes, journaux d'événements applicatifs, ...) et des applications à travers différents protocoles (NFS, SMB v3 et S3), qu'il s'agisse de données froides (dépôt d'archives, de sauvegardes, d'images ISO, de vidéos...) ou non (stockage objet via le protocole S3). Le service offre plusieurs niveaux de redondance (local, national), suivant les besoins.</i> <i>Cette prestation est à demander par FEB hébergement et est incluse comme option dans les demandes d'hébergement sur l'offre CIDR.</i> <i>Une capacité est également disponible sur PICSEL pour faciliter le recours à ces technologies. Sa mise en oeuvre sur CINP fait également l'objet de travaux actuellement.</i>					
Stockage	IRIS-S-SF sur une base de Scality	CND	Stockage objet de fichiers et métadonnées au travers du protocole S3 et de données froides (archivage, sauvegarde)	E / S	SIA S-SF
<i>Commentaire : à date de rédaction, ce service est en cours de VABF et devrait être ouvert en production d'ici à fin 2026.</i>					
Stockage	MinIO	MinIO	Stockage objet de fichiers et métadonnées au travers du protocole S3 et de données froides (archivage, sauvegarde). A limiter à des cas d'emploi ne permettant pas de recourir aux instances IRIS existantes en prévoyant la	D / N	Min Arm

			souscription de licence dès lors qu'elle ne seront plus disponibles dans la version communautaire.		
<i>Commentaire: les changements récents opérés par la compagnie MinIO (arrêt des distributions binaires et des images de conteneurs, retrait de la gestion des clefs de connexion, des authentifications LDAP et OIDC et des fonctions d'administration de l'IHM de la version communautaire) incitent à la plus grande prudence quant à l'utilisation de ce logiciel. Dans l'attente de l'émergence d'une solution offrant davantage de garantie, il reste recommandé de s'appuyer sur les services de stockage du Ministère.</i>					

Présente sur l'Intradef, cette capacité est en cours de VABF sur le réseau S-SF (SIA) et également prévue dans l'environnement CINP ainsi que PICSEL pour faciliter les travaux de développement des systèmes d'information devant y avoir recours. Ce stockage n'est en revanche pas adapté aux cas d'usage suivants :

- hébergement de bases de données relationnelles (du fait des taux I/O élevés que cela nécessiterait) ;
- exécution de machines virtuelles.

5.1.7 Téléphonie

5.1.7.1 Téléphonie classique

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°7 portant sur la téléphonie sur le protocole internet publiée au Bulletin Officiel des Armées, cf. 3.1.8 Téléphonie	13 janvier 2009	DGSIC	Directive	Min Arm
Directive DGSIC n°11 du 8 janvier 2010 portant sur la sécurisation des autocommutateurs diffusée par lettre n°15/DEF/DGSIC/SDSSI du 8 janvier 2010	8 janvier 2010	DGSIC	Directive	Min Arm
<i>Commentaire : cette directive définit la politique à mettre en œuvre par les organismes du Ministère des armées responsables d'un service de téléphonie classique. Elle fournit les critères de décision pour l'acquisition, la réalisation, la mise en œuvre, le maintien en condition et la sortie de service d'un service de téléphonie classique. Cette directive est applicable aux systèmes d'information et de communication non classifiés de défense supports d'un service de téléphonie classique et à tous leurs composants, notamment leurs éléments actifs.</i>				
Directive DIRISI n°256 du 13 août 2018 relative à l'emploi et la configuration de la téléphonie professionnelle du ministère de la défense (TPDM)	8 janvier 2010	DIRISI	Directive	Min Arm
<i>Commentaire : cette directive a pour objet de définir un cadre d'emploi des différentes fonctionnalités de téléphonie professionnelle au sein du Ministère et de standardiser au maximum les configurations des PABX métropolitains ou non.</i>				
Directive de mise en œuvre de la téléphonie mobile au sein des bases de défense Note n° D-14-001374/DEF/EMA/CPCS/B.SOUT/SIC-SSI/NP du 04 février 2014	4 février 2014	EMA	Note	Intradef

5.1.7.2 Téléphonie chiffrée

Cf. 4.6.8

5.1.7.3 Radiotéléphonie (INPT)

Le réseau radio du futur (RRF) constitue un projet de réseau commun aux acteurs de la gestion de crise. Il a vocation à se substituer aux réseaux radios RUBIS et INPT actuellement utilisés, qui reposent sur des infrastructures détenues et exploitées par l'État et qui offrent des services rudimentaires.

Le RRF vise à remédier à ces limites en offrant une solution hybride, qui consiste à utiliser les réseaux 4G et 5G des opérateurs de réseaux mobiles, tout en bénéficiant d'une qualité de service différenciée par rapport à leurs autres clients.

Le RRF bénéficiera à de nombreux services de l'État (forces de sécurité intérieure, armées, services de secours, administration pénitentiaire, services douaniers, services de la navigation maritime ou aérienne, etc.), comme à certains opérateurs d'importance vitale et aux collectivités territoriales (police municipale, services départementaux d'incendie et de secours (SDIS)).

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°133 d'exploitation et de soutien de l'INPT /DIPAD : V1.0 du 16 juin 2014	16 juin 2014	DIRISI	Directive	Min Arm
<i>Commentaire : l'INPT (Infrastructure Nationale Partageable des Transmissions) est un réseau globalisé de radiotéléphonie numérique, de couverture nationale, offrant des services de voix et de données, et opéré par le Ministère de l'Intérieur et des Outre-Mer. Cette directive décrit les modalités d'exploitation du sous-réseau de l'INPT attribué au Ministère (DIPAD : Desserte Interarmées en PMR Accessibles à la Défense). A terme, la défense est concernée par 10000 terminaux.</i>				

5.2 Réseaux

Pas de référence identifiée à ce jour.

5.2.1 Généralités

5.2.1.1 Architecture des réseaux, IPV6

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°20 portant sur l'architecture des réseaux 'internet Protocol' publiée au Bulletin Officiel des Armées	24 août 2011	DGSIC	Directive	Min Arm
<i>Commentaire : cette directive définit les règles applicables au sein du Ministère pour l'architecture des réseaux internet protocol (IP) de défense relatives essentiellement aux réseaux de transit global IP (hors passerelles et enclaves), et ne concernent que la seule couche IP (hors réseaux supports, ou couches de transport ou applicatives).</i>				
Directive DGSIC n°22 portant sur la transition IPv6 publiée au Bulletin Officiel des Armées	20 déc. 2011	DGSIC	Directive	Min Arm
<i>Commentaire : cette directive traite de la stratégie de migration vers l'IPv6 et des règles relatives aux acquisitions et évolutions majeures de tous les systèmes d'information et de communication au regard de la transition vers IPv6.</i>				

5.2.1.2 Adressage IP

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.037 - Plans d'adressage IP, cf. 8.4.7 Adressage IP	13 mars 2025	DIRISI	Guide	Min Arm
<i>Commentaire : ce guide abroge la Directive DIRISI n°129. Ce document de politique d'adressage IP présente les plans d'adressage IPv4 et IPv6 globaux du Ministère. Il porte principalement sur : • l'allocation des plages et l'assignation des adresses ;</i> • les numéros de SAT ; • les numéros d'AS BGP ; • les communautés BGP ; • les VRF.				
Directive DIRISI n°109 portant sur la politique de routage des flux IP DEFENSE version 3, cf. 8.4.7 Adressage IP	26 mai 2018	DIRISI	Directive	Min Arm

Commentaire : cette directive expose la finalité recherchée dans la politique de gestion des flux. Elle présente les évolutions à mettre en œuvre pour la gestion des flux : • de nouveaux systèmes classifiés via OPERA ; • pour l'OME via l'emploi en nominal de la FON OME.				
Directive DIRISI n°134 relative à l'adressage IPV4 des réseaux protégés version 2.1, cf. 8.4.7 Adressage IP	25 juin 2014	DIRISI	Directive	Min Arm Réseaux Classifiés de défense
Commentaire : cette directive porte sur : • les équipements cautionnés (CHIP, Netasq, Arkoon, etc.) dès lors qu'une fonction de chiffrement est activée ; • les équipements relevant du domaine classifié de défense (ECHINOPS, TCE621, etc.).				

5.2.1.3 Bout en bout : QoS – Contrats de services – interconnexion – métrologie

5.2.1.3.1 Marquage – qualité de service

Document	Date	Origine	Type doc	Portée
Directive n°36 DGSIC relative au marquage des flux IP pour la qualité de service sur les réseaux IP au sein du ministère de la Défense	3 juillet 2015	DGSIC	Directive	Min Arm
Commentaire : cette directive définit les règles applicables pour la différenciation des flux IP au sein du Ministère pour la qualité de service (QoS) des flux réseaux IP.				

5.2.1.3.2 Routage inter-systèmes

Document	Date	Origine	Type doc	Portée
Directive n°38 relative au « routage inter-systèmes » [DIR-RIS] approuvée le 29 mars 2016 et diffusée par note n°173/DEF/DGSIC/DG/NP du 30 mars 2016	29 mars 2016	DGSIC	Directive	Min Arm Tout Intranet
Commentaire : cette directive énumère des modèles d'interconnexion de réseaux IP et traite de règles de bon usage ainsi que des aspects liés à la sécurisation des interconnexions aussi bien dans le domaine des connexions de type unicast que multicast. Elle concerne les aspects techniques et organisationnels relatifs aux équipements matériels de réseaux, aux éléments de sécurité, et aux applications.				
Bonnes pratiques de configuration de BGP	septembre 2013	ANSSI	Guide	Toute admin.
Commentaire : ce document de l'ANSSI réalisé avec la coopération d'opérateurs français, décrit les bonnes pratiques de configuration du protocole BGP (Border Gateway Protocol), protocole natif des routeurs. Il édicte des recommandations suivant les types d'interconnexions et de relations entre AS (Autonomous System).				

5.2.1.3.3 Métrologie – indicateurs

Document	Date	Origine	Type doc	Portée
Directive DGNUM n°42 relative à la métrologie réseau (DIR-METRO) 1ère édition	15 janvier 2019	DGNUM	Directive	Min Arm
Commentaire : cette directive regroupe un ensemble de recommandations pour améliorer l'efficacité de la supervision des réseaux militaires et apporter des capacités de suivi des contrats de service.				
EMO.DCES.R4.019 - Système de métrologie réseaux version 1.0	06 septembre 2021	DIRISI	Document cadre d'exploitation	Min Arm
Commentaire : cette directive consultable sur DIADEME a pour opbjet de fournir les éléments relatifs à l'exploitation des outils de métrologie du Ministère. Elle précise les responsabilités de l'opérateur CND et des clients, et les modalités de mise en oeuvre des demandes de prestation de métrologie et la fourniture de SLA.				

5.2.1.4 Problématique des réseaux contraints

Document	Date	Origine	Type doc	Portée
Recommandations à destination des responsables d'application devant déployer leur système sur des théâtres d'opération et bâtiments de la Marine , sous timbre n° 759/DEF/DGSIC/SDAU du 27 novembre 2014	27 novembre 2014	DGSIC	Note	Min Arm
<i>Commentaire : cette note fournit un ensemble de recommandations générales en matière de conception, d'architecture et de qualification des systèmes d'information pour la prise en compte de leur déploiement sur les théâtres d'opération, les bateaux et implantations outre-mer (limites des réseaux, liaisons satellitaires...)</i>				

5.2.2 Réseaux de transport WAN et routage

DESCARTES (DEploiement des Services de Communications et Architectures des Réseaux de Télécommunications Sécurisés) : les réseaux de transport du ministère des Armées s'appuient sur plusieurs composantes fonctionnelles s'appuyant sur la technologie IP :

- d'un réseau de transport IP d'usage général, opéré par un opérateur civil (OPERA, migration vers le RIE en cours d'étude) ;
- d'un réseau de transport métropolitain résilient et maîtrisé capable de fonctionner même en cas de crise grave (composante SOCRATE du programme DESCARTES portée par le marché SCR, rénovation du réseau historique résilient SOCRATE) ;
- d'une architecture de routage et de sécurité (composante POINCARE du programme DESCARTES portée par le marché ISR) constituée d'un système de points d'interconnexion (PI) sur les sites offrant les capacités de raccordement des réseaux de desserte, de chiffrement des flux (au niveau DIFFUSION RESTREINTE) et leur aiguillage selon leur classe et la résilience requise pour transiter sur le réseau d'usage général ou le réseau résilient ; cette composante standard est doublée d'une composante ATM (Air Trafic Management) sur les sites contribuant au contrôle aérien pour le routage spécifique de ces flux dédiés, qui est ségrégée pour pouvoir répondre aux exigences réglementaires liées à l'ATM ;
- d'un secours par satellite (COMCEPT) pour le transport vers les sites nécessitant de la résilience et n'ayant qu'un accès au réseau de transit IP d'usage général ;
- de divers supports tiers et Internet, notamment pour les sites OME ;
- d'une architecture de routage et de sécurité (POINCARE), constituée d'un système de points d'interconnexion (PI) sur les sites offrant les capacités de raccordement des réseaux de desserte, d'aiguillage et de chiffrement des flux.

Dans le cadre du programme DESCARTES, une spécification d'interface pour les clients au réseau DESCARTES a été établie. Elle définit les spécificités techniques du raccordement IP au réseau DESCARTES et les contraintes et exigences d'interconnexion à prendre en compte par les systèmes client.

Il est important de prendre en compte le MTU (Maximum Transmission Unit) pour les clients raccordés au réseau DESCARTES (ce MTU est de 1330 octets). Il s'agit également du MTU appliqué à l'Intrade.

Tout client / application se raccordant au réseau DESCARTES doit renseigner le fichier CAR (CANEvas des besoins Réseau) qui caractérise le type d'échange et les flux entre les différents sites et la QoS envisagée.

5.2.3 Services de réseaux de desserte

5.2.3.1 Maîtrise des flux réseau [MFR]

Pas de référence identifiée à ce jour.

5.2.4 Services des réseaux étendus : filtrage - passerelles [FIL-PAS]

Cf. 5.2.12 Câblage

5.2.5 ToIP / VoIP

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°7 portant sur la téléphonie sur le protocole internet : directive du 13 janvier 2009 publiée au Bulletin Officiel des Armées	13 janvier 2009	DGSIC	Directive	Min Arm
<i>Commentaire : cette directive définit la politique à mettre en œuvre avant le déploiement d'un service de téléphonie sur le protocole internet (ToIP) par les organismes du Ministère. Elle fournit les critères de décision pour l'acquisition, la réalisation et la mise en œuvre d'un service de ToIP. Elle est applicable aux systèmes d'information et de communication non classifiés de défense support d'un service de ToIP et à leurs composants, notamment leurs éléments actifs. Cette directive tient compte du projet de référentiel général d'interopérabilité prescrit par l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives et du référentiel général de sécurité.</i>				
Recommandations de sécurisation d'une architecture de téléphonie sur IP version 1.0 (cf. 4.5 Sécurisation des COTS)	23 décembre 2013	ANSSI	Note technique	Toute administration
<i>Commentaire : Cette note technique présente les risques ainsi que les mesures de sécurisation qui doivent accompagner la mise en œuvre d'une infrastructure de téléphonie sur IP.</i>				

5.2.6 Réseaux sans fils

5.2.6.1 Technologies sans fil (WIFI, Bluetooth, RFID, ZIGBEE, Lorawan)

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°23 portant sur la sécurité de réseaux sans fil Édition n°2 du 08/02/2024 diffusée par note n° 54/ARM/DGNUM/DG/NP	08 février 2024	DGSIC	Directive	Min Arm
<i>Commentaire : cette directive édicte les règles relatives à l'emploi et la mise en œuvre de technologies sans fil : Wi-Fi, Bluetooth, RFID, ZIGBEE, LORAWAN. Cette directive abroge l'ancienne version restreinte au Wifi du 6 février 2012 et le guide n°9 sur la mise en œuvre des réseaux Wifi.</i>				
Recommandations de sécurité relatives aux réseaux Wi-Fi version 1.2, cf. 4.5 Sécurisation des COTS	9 septembre 2013	ANSSI	Note technique	Toute admin.
<i>Commentaire : Cette note technique a pour objet de guider dans le choix des meilleurs paramètres pour la bonne sécurisation d'un réseau Wi-Fi.</i>				

5.2.6.2 RFID

Document	Date	Origine	Type doc	Portée
Politique interarmées pour l'emploi de systèmes d'identification par radiofréquences [PIA RFID] diffusée par note sous double timbre : n°D-17004828 ARM/EMA/SC et n°DGA01D17025073/ARM/DGA/DO/SMCO	06 octobre 2017	EMA DGA	Politique	Min Arm
Directive technique interarmées pour la mise en œuvre des technologies RFID [DTIA RFID] diffusée par note sous double timbre n°D-18005592 ARM/EMA/DSA/MCO/NP et n°DGA01D18054469/ARM/DGA/DO/SMCO/NP	15 octobre 2018	EMA DGA	Directive	Min Arm
Vademecum sur la RFID entretenu par DGA/DO/SMCO	14 novembre 2016	DGA	Guide	Min Arm
<i>Commentaire : ce guide RFID fournit une aide aux spécificateurs sur l'utilisation de cette technologie pour le soutien des opérations d'armement. Il peut aider soit en phase amont lors de la rédaction des documents contractuels (STB, CCTP, ...) ou en phase de réception des offres et de négociation avec les industriels afin de vérifier tous les aspects (questions, normes, ...) des solutions RFID proposées.</i>				

5.2.7 Liaison satellitaires

Pas de référence identifiée à ce jour.

5.2.8 Équipements : LAN, Routage, Switch, Pare feu, accélérateurs...

Document	Date	Origine	Type doc	Portée
Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu version 1.0, cf. 4.5 Sécurisation des COTS	30 mars 2013	ANSSI	Note technique	Toute admin.
<i>Commentaire : Cette note technique a pour objet de fournir les éléments organisationnels permettant de structurer la base de règles constituant la politique de filtrage réseau appliquée sur un pare-feu d'interconnexion. Cette note est indépendante de la fonction du pare-feu (accès internet, cloisement de datacenter, isolation d'un partenaire) ; elle fait l'abstraction des solutions techniques qui peuvent être employées (logiciel, équipement dédié) et ne tient pas compte de son mode d'administration (ligne de commande, interface web, client lourd).</i>				
Recommandations pour la sécurisation des commutateurs Ethernet et l'utilisation des VLAN , cf. 4.5 Sécurisation des COTS	22 février 2010	DGA MI	Guide technique	Min Arm

5.2.9 Équipements de chiffrement

Cf. 4.6.7 Équipements de chiffrement

5.2.10 VPN

Document	Date	Origine	Type doc	Portée
Recommandations de sécurité relatives à IPSec pour la protection des flux réseau version 1.1, cf. 4.5 Sécurisation des COTS	3 août 2015	ANSSI	Note technique	Toute admin.
<i>Commentaire : cette note technique précise les recommandations relatives à un usage sécurisé d'IPSec.</i>				

5.2.11 Baies

Pas de référence identifiée à ce jour.

5.2.12 Câblage

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.004 - Installation et nommage des composants d'infrastructure de télécommunications	21 juillet 2025	DIRISI	Guide	Min Arm hors BICES
<i>Commentaire : Ce guide consultable sur DIADEME formalise le nommage des équipements et instaure les règles de câblage des installations. Il décrit les éléments nécessaires à l'élaboration au maintien à jour de la base de données de la CMDB réseau, de GAS et du SI CARLA, tout en fixant des normes uniques d'installation pour le CND et l'ensemble des SIC du Ministère. Ce guide abroge la directive DIRISI DIR-073.</i>				
Directive DIRISI n°15 « infrastructure des réseaux de desserte du ministère de la défense V2.0 sous timbre n°502688/DEF/DIRISI/SCP du 21 octobre 2010	21 octobre 2010	DIRISI	Directive	Min Arm
<i>Commentaire : cette directive identifie les éléments du câblage générique, les normes et modalités de câblage des réseaux de desserte du ministère. Elle est constituée de deux parties : • partie 1 : relative à l'état de l'art en cours au ministère sur le câblage, les locaux techniques, les armoires techniques, le câblage du fédérateur, le câblage capillaire (postes terminaux) ainsi que les règles sur le cheminement, le repérage et le marquage de l'infrastructure et les procédures de contrôles ; • partie 2 : les normes retenues en matière de câblages, de résistance au feu, de courants forts et les normes techniques réseaux. Cet ensemble normatif est entretenu sous l'égide du Centre de Normalisation de la Défense (CND) via son site « Intranormes ».</i>				
Directive AND n°DGA01D21033009 - « Directive technique schéma directeur MODIP » version 2.0 du 12/10/2021	12 octobre 2021	AND	Directive technique	Min Arm MODIP
<i>*Commentaire : cette directive décrit les standards d'architecture et les standards d'implémentation à mettre en œuvre pour les réseaux de desserte des sites du Ministère dans le cadre MODIP. Elle n'est pas applicable aux réseaux RDIP, ATM, des datacenter ou non opéré par le CND. Elle abroge la directive 235.</i>				

6 CADRE FONCTIONNEL ET TECHNIQUE D'HEBERGEMENT

6.1 Plateformes d'hébergement

6.1.1 Références générales sur l'hébergement

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°32 portant sur la sécurité de l'hébergement des SI au sein du ministère cf. 4.8.7 Hébergement / Virtualisation	11/03/2014	DGSIC	Directive	Min Arm
<i>Commentaire : applicable à l'opérateur, et aux systèmes informatiques hébergés, en recommandation pour les applications ayant vocation à être hébergées à l'extérieur du Ministère.</i>				

Règle	Énoncé	Statut	Portée
CCT_R12_1	Il est INTERDIT d'héberger à des fins d'intégration, de pré-production ou de production un service ou un système d'information en dehors des plates-	I	Min Arm

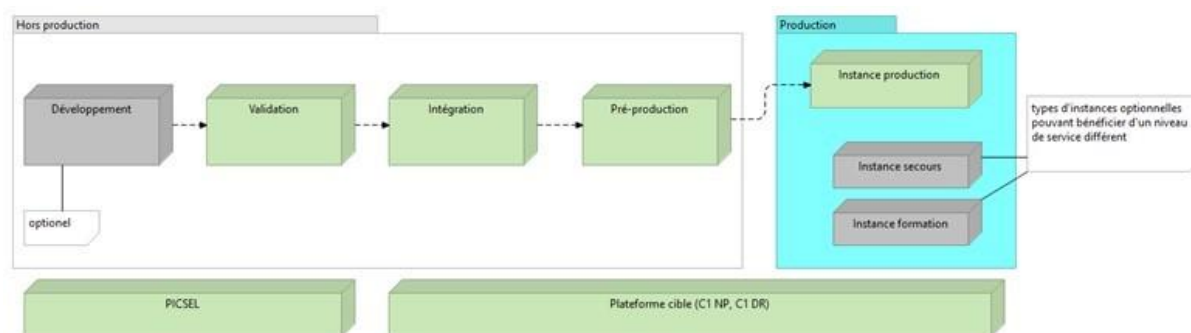
	formes de socle dès lors qu'une offre de service adaptée est disponible dans l'environnement considéré.		
CCT_R13_1	Pour le cas où une plateforme de socle n'est pas disponible ou pour des activités d'expérimentation ou de développement non réalisables sur PICSEL, il est OBLIGATOIRE d'obtenir une dérogation du CND.	O	Min Arm

Le CND appréciera la nécessité d'opérer des hébergements hors plates-formes du socle, sur des infrastructures en salle blanche et opérées par des tiers :

- les plates-formes d'hébergement du S2NA sont considérées comme appartenant au socle ;
- les activités de réalisation d'infocentre, de tableaux de bord ou d'entraînement de modèles d'intelligence artificielle sont qualifiées d' « intégration de données » et assimilées à des activités de production, à mener dans un environnement destiné à ce type d'activité, les instances de production du service utilisé devant prévoir ce cas d'usage et mettre à disposition les espaces et les ressources nécessaires (ex : instance d' « intégration de données » du service de visualisation de données Qlik Sense).

Hors activité de développement, les hébergements sur des plates-formes tierces restent assujettis aux autorisations de la gouvernance et à une homologation. Il en est de même des plates-formes elles-mêmes.

6.1.2 Typologie d'environnements sur les plateformes



Typologie des environnements sur les plateformes

Pour chaque SI déployé, différents environnements sont envisageables en fonction des visées et phases du projet.

Environnements SI dits « Hors production » :

- **Environnement de développement** : il est destiné aux projets pour implémenter leurs systèmes et est porté hors dérogation par la plate-forme PICSEL, quel que soit le niveau de classification visé au déploiement. Il porte également une logique de bac-à-sable ou d'expérimentation. C'est dans cet environnement que sera réalisé le contrôle qualité requis avant déploiement vers l'environnement cible ; ce contrôle qualité est destiné à valider avant déploiement la conformité du système aux contraintes et attendus d'hébergement (playbooks Ansible, conformités au CCT, pile maintenue et à jour, ...).
- **Environnement « Intégration SI »** : il est destiné aux équipes du SI (équipe projet et de développement qui ont la charge du déploiement et de l'exploitation de cet environnement, même en infogérance) pour tester les procédures de déploiement en environnement représentatif sur plateforme d'hébergement cible et valider le bon fonctionnement technique du SI (dans le cas d'une primo installation, d'évolutions ou d'application de correctifs de sécurité).

Environnement « Préproduction SI » : il est destiné aux équipes du RCP/RTS et aux infogérants pour tester les procédures d'exploitation et valider le bon fonctionnement du SI (VABF). L'équipe projet procède aux tests fonctionnels (dans le cas d'une primo installation ou d'évolutions du SI). Elle permet d'effectuer la mise en œuvre de tous les changements sans impacter le SI de production.

Environnement SI « Production » : il s'agit de l'environnement d'hébergement cible qui peut lui-même se voir adjoindre deux types d'instances complémentaires, dont le niveau de service apporté peut être différent de celui de l'instance de production principale. C'est sur cet environnement qu'est réalisé la VSR.

Instance SI « Secours » : elle permet la reprise ou la continuité du système (éventuellement en mode dégradé) de l'instance principale de production, dont elle est l'image y compris pour la partie « données », en cas d'incident majeur. Il convient de noter que le mécanisme de réplication des données devra être étudié et mis en place par le projet. Le PCI/PRI reste également de la responsabilité du bénéficiaire. L'instance de secours est nécessairement déployée sur un DataCenter différent de l'instance de production principale.

Instance SI « Formation » : ce type d'environnement, éventuellement à accès restreint, permet d'offrir un espace de formation aux utilisateurs finaux du SI, éventuellement pour préparer la mise en production d'une nouvelle version sur l'instance de production principale.

6.1.3 Les niveaux de service d'hébergement

Pour chaque offre, l'opérateur s'engage à mettre en œuvre tous les moyens disponibles pour assurer aux environnements de production le niveau de services découlant directement de la catégorisation DIMA :

Niveaux de services				
Arbitrage	i2 ou sans décision	i3bis	i3	i4
Prérequis d'architecture du SI	Plate-forme de secours non obligatoire	Plate-forme de secours non obligatoire	Plate-forme de secours exigée	Plate-forme de secours exigée sur site distant et en position « active automatisée »
Continuité	La résilience des infrastructures SIC du CND, la gestion des incidents, ainsi que la mise en place d'une sauvegarde suffisent à assurer un retour du service au regard de la DIMA		Un environnement de secours, ainsi qu'un PCI rédigé et testé sont exigés pour disposer d'une solution permettant le retour du service au regard de la DIMA. En cas d'absence de secours et de PCI, le SI sera pris en compte au maximum par le CND au niveau de service « Argent »	
Niveaux de services correspondants	 Bronze	 Argent	 Or	 Platine

Sont concernées la disponibilité, les sauvegardes et restaurations ainsi que la prise en compte des incidents et des demandes de changement.

6.1.4 Processus d'hébergement

Après expression du besoin d'hébergement par le bénéficiaire auprès du CND, le processus d'hébergement se déroule en 5 phases successives : attribution de l'hébergement une fois les pré-requis acquis, qualification du SI sur l'infrastructure CND, mise en pré-production, mise en production expérimentale puis opérationnelle et, à terme, arrêt des services d'hébergement.

Lors de la demande d'hébergement, il convient de prendre en compte l'ensemble de ses contraintes, besoins et services consommés (débits réseaux nécessaires, certificats, entrées DNS, NTP, supervision et supervision de sécurité, services d'authentification, de messagerie, passerelles, archivage ...). Des agents seront installés concomitamment pour répondre à certains besoins (supervision, sécurité, sauvegarde, gestion et contrôle de configuration ...). Selon le cas, des tests de montée en charge pourront en outre être demandés.

Enfin, pour être mis en production, il est rappelé qu'un système doit être homologué et faire l'objet d'une vérification d'architecture de la part de l'AGORA Tech et être homologué.

Le dossier d'architecture technique est un prérequis essentiel et structurant de tout échange avec le CND dont un modèle est disponible sur le portail hébergement du CND.

6.1.5 Hébergement sur Intradef

Périmètre	Offre	Utilisation / Restrictions	Statut	Portée
Hébergement de pré-production / production (dont formation et secours)	Infogérance Cloud C1DR	L'offre C1DR se substitue à l'offre SHSM DR pour les nouveaux projets. De manière exceptionnelle et transitoire ne sont désormais éligibles à un hébergement SHSM DR que les projets préexistant ne satisfaisant pas encore les prérequis C1DR. L'offre SHSM DR sera arrêtée au plus tard fin 2028.	R / S	Intradef
Hébergement d'intégration / pré-production / production (dont formation et secours)	VPS Cloud C1DR	L'offre C1DR se substitue à l'offre SHSM DR pour les nouveaux projets. De manière exceptionnelle et transitoire ne sont désormais éligibles à un hébergement SHSM DR que les projets préexistant ne satisfaisant pas encore les prérequis C1DR. L'offre SHSM DR sera arrêtée au plus tard fin 2028.	R / S	Intradef
Hébergement de pré-production / production CaaS "CAASTOR"	VPS CaaS Cloud C1DR	Offre d'hébergement de SI à base d'orchestration de conteneurs	R / S	Intradef
Hébergement de production / pré-production	Salle blanche	Réservé aux besoins en matériel spécifique	A / N	Intradef
Hébergement de production	HDS	Réservé aux systèmes d'information comportant des données de santé dans l'attente d'une reprise en hébergement sur C1DR.	A / S	Intradef
Hébergement de production	SIE	Intradef embarqué uniquement	R / S	Intradef
Hébergement de développement/expérimentation/validation	PICSEL	Les systèmes d'information doivent réaliser un contrôle qualité sur cette plateforme pour évaluer leur aptitude à un hébergement en production à destination de C1DR ou C1NP.	R / S	Intradef

6.1.5.1 Aspect réseaux

6.1.5.1.1 Gard

Sur Intradef, le réseau interne des datacenter (Bordeaux, Rennes, Suresnes, Toulon et Six-Fours) dispose d'une architecture hautement résiliente de type IP Fabric. Le projet Gard apporte une connectivité à l'accès de 10 et 25 Gbit/s et une automatisation de la configuration sur base de logiciel (SDN).

6.1.5.1.2 SARDaC⁶⁰

Les flux entrant/sortant dits « Nord-Sud » des datacenter sont désormais filtrés et ne laissent désormais circuler par défaut que :

- HTTPs : exposition des sites, applications web et API REST ou SOAP ;
- S3 : flux d'accès aux stockages objet ;
- SMTPs : flux de messagerie sécurisé ;
- DNS : flux d'interrogation des serveurs de nommage ;
- NTP : flux de synchronisation horaire ;
- LDAPs : flux d'authentification des postes de travail ;
- flux de réplication des infrastructures (Active Directory, réplication asynchrone des baies de stockage, réplication des bucket IRIS, SRM et vSphere)

Les flux existants sont examinés et ceux non conformes seront ensuite progressivement coupés.

6.1.5.1.3 Equilibreur de charge physique

La politique d'emploi des équilibreurs de charge d'entrée des datacenter a également fait l'objet d'une harmonisation entre les différents centres. Ces équipements portent actuellement trois fonctions principales :

- Equilibrage de charge (Loadbalancing ou LB),
- Chiffrement/déchiffrement des flux TLS,
- Authentification.

Désormais, ces fonctions sont assurées uniformément comme suit.

6.1.5.1.3.1 Equilibrage de charge

Les équipements assurent l'équilibrage de charge :

- pour les systèmes d'information « historiques » infogérés par le CND, en attendant la mise en œuvre d'une solution « NLB as a Service » sur C1DR ;
- pour les seuls composants du socle (portefeuille de la DSI Socle) concourant à l'activité d'hébergement ou à la sécurité.

Pour les systèmes d'information hébergés en VPS sur l'offre VPS Cloud C1 DR, cette fonction de répartition de charge doit être portée au niveau de leur couche logicielle et incluse dans leur architecture, en utilisant des solutions référencées et recommandées (HAProxy, httpd, NGINX, ...).

6.1.5.1.3.2 Chiffrement des flux

Le chiffrement des flux TLS consiste à la conversion du http vers le https dans le sens sortant, le certificat étant porté par l'équipement de répartition de charge. Cette fonction est maintenue pour :

- tous les systèmes d'information « historiques » qui ne peuvent pas assurer eux-mêmes cette fonction, et après obtention d'une dérogation de l'AGORA Tech ;

⁶⁰ Sécurisation des Accès Réseau DAtaCenter

- tous les systèmes d'information en https en infogérance DR et bénéficiant actuellement de ce service.

6.1.5.1.3.3 Authentification

Les équipements mutualisés d'équilibrage de charge ne doivent porter aucune fonction spécifique d'un système d'information spécifique, au premier rang desquelles l'authentification qui est, sauf dérogation AGORA Tech, de la responsabilité exclusive de la brique de socle MindefConnect Intradef.

En conséquence, les systèmes d'information « historiques » en infogérance DR ou non et utilisant ce mode d'authentification le conserveront jusqu'à leur migration vers le C1DR. Aucun nouveau système ne sera autorisé à utiliser ce mode d'authentification non conforme.

6.1.5.2 Hébergement Infogérance Cloud C1DR

Les systèmes d'information qui bénéficient de l'offre historique doivent intégrer la démarche « move to cloud » pour être transférés vers le C1DR avant le 31/12/2028, date d'arrêt du service SHSM DR.

Le CND assure l'administration technique et la supervision de la couche technique applicative (systèmes d'exploitation, serveurs applicatifs, serveurs de présentation, bases de données) sous réserve que ses composants soient déclarés soutenus par le CND dans le présent Cadre de Cohérence Technique.

Le CND assure une administration technique restreinte de la pile logicielle non déclarée comme « soutenue » dans le CCT, limitée à des actions réflexes telles que l'arrêt et relance des services, sous réserve de fourniture par le bénéficiaire d'une documentation technique suffisante.

L'administration fonctionnelle du SI incombe entièrement au bénéficiaire.

L'ensemble des enregistrements d'exécution (traces, journaux d'événements applicatifs et systèmes, ...) doit être rendu accessible au CND à des fins d'exploitation de la sécurité.

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.014 - Conditions Générales d'Hébergement de niveau DR (CGHD-DR) v4.0	11 juillet 2025	DIRISI	Guide	Intradef
<i>Commentaire : cette note décrit les conditions générales d'hébergement d'un système d'information DR dans le cadre de l'offre de service Cloud C1DR du CND, la sécurité et les obligations liées à cet hébergement.</i>				
Directive DIRISI n°239 d'administration de l'Intradef : v1 du 3 avril 2018, directive entretenue par le CND	3 avril 2018	DIRISI	Note	Intradef
<i>Commentaire : Cette directive fait suite à la désignation du Directeur du CND comme administrateur de l'Intradef. Elle décline les axes sur lesquels cette fonction s'exerce.</i>				
EMO.GUI.R4.032 Urbanisation des équipements dans les Datacenters de la DIRISI V1.0 du 01/04/2024	1 avril 2024	DIRISI	Guide	Intradef
<i>Commentaire : Ce document annule et remplace la directive DIRISI n°193 intitulée « Directive d'urbanisation des Datacenters et des salles informatiques auxiliaires ». Il s'adresse aux bénéficiaires d'un hébergement au sein des Datacenters principaux, des salles secondaires et auxiliaires du CND. L'objectif de ce document est de définir les étapes nécessaires à l'urbanisation d'un équipement, en tenant compte de l'ensemble des contraintes, de manière à assurer une installation efficace tout en respectant les règles de l'art. Les bénéficiaires doivent s'assurer que l'ensemble des prérequis énoncés dans ce document soient fournis et validés au moment de la demande d'hébergement.</i>				

Partie intégrante de l'offre de service Cloud (cf. 3.2.1.2 Démarche et principes liés), C1DR a remplacé les hébergements Infogérance DR, VPS DR et VPS-c DR.

Construit dans une recherche de maîtrise, de standardisation et d'automatisation, C1DR vise avant tout à simplifier et accélérer la mise en production des systèmes d'information mais ne modifie pas fondamentalement les principes et le cadre technologique en vigueur en œuvre sur les hébergements

Infogérance et VPS DR : hébergement en machines virtuelles avec les systèmes d'exploitation durcis du Ministère.

Il apporte toutefois un raccordement automatisé aux services du socle dont certains devaient précédemment être demandés séparément (NTP, DNS, sauvegarde, dépôts de mise à jour MEDUSA, antivirus, gestion des licences Windows et RedHat, supervision, contrôle de conformité, orchestrateur Ruche, inventaire, comptes de services, gestion des secrets et des certificats). D'autres services seront progressivement ajoutés à la liste (stockage objet IRIS, service d'observabilité ...).

La démarche de cloudification impose au système d'information de respecter quelques exigences qui sont rappelées ci-après et qui sont destinées à faciliter les automatisations et l'exploitabilité, donc améliorer le niveau de service offert, et d'en conserver la maîtrise dans la durée :

- disposer d'une pile logicielle à jour et soutenue en MCO/MCS (condition d'homologation) ;
- disposer de scripts de déploiements Ruche conformes (ceux de C1NP sont identiques à ceux d'Intradef, exigence précédemment en vigueur pour l'hébergement infogérance DR historique, étendue au VPS) ;
- s'adosser à l'authentification MindefConnect de l'environnement support ;
- respecter le format des journaux d'événement : le format attendu par le CALID constitue un prérequis à la mise sous supervision de sécurité ;
- exporter ses journaux d'événements applicatifs dans le puits de log (revient à produire des journaux d'événements qui seront exportés ensuite automatiquement par un agent installé à cet effet) ;
- instancier a minima l'API REST d'observabilité (l'instrumentation pourra être enrichie via développement mais c'est laissé à l'appréciation du projet de ses besoins en la matière) ;
- gérer ses secrets et ses certificats via le service de socle Gestion des secrets.

Les services offerts sur la plate-forme PICSEL ont été mis en place pour faciliter le développement et le test des quelques adaptations nécessaires et d'en contrôler la conformité avant déploiement sur C1DR.

6.1.5.3 Offre VPS DR

Les systèmes d'information qui bénéficient de l'offre historique doivent intégrer la démarche « move to cloud » pour y être transférés vers l'offre VPS Cloud DR avant le 31/12/2028, date d'arrêt du service.

Les prestations du CND concernent la fourniture et l'administration technique des couches basses telles que décrites dans les conditions générales d'hébergement.

6.1.5.4 Hébergement des données de santé (HDS)

La plateforme Hébergement des Données de Santé (HDS) a été mise en place par le CND pour assurer l'hébergement de données de santé (données à caractère personnel dites sensibles) et l'infogérance des systèmes d'information du SSA qui les produisent. Les modalités de reprise de ces fonctions par la plateforme Cloud C1DR sont en cours d'étude.

6.1.5.5 Hébergement Salle Blanche DR (réservé aux besoins en matériel spécifique)

Sous réserve d'obtention d'une dérogation permettant le recours à un tel hébergement, les prestations Salle Blanche du CND consistent en la fourniture d'un emplacement au sein d'une architecture matérielle CND électriques et informatiques.

L'achat, la livraison, l'installation, la maintenance et l'administration technique et fonctionnelle du matériel et des logiciels (y compris la sauvegarde, la restauration et le soutien en cas de défaillance) incombent entièrement au bénéficiaire.

Il incombe également au bénéficiaire de prendre attache avec le CND afin de bénéficier de l'installation de l'agent d'inventaire.

Le matériel fourni par le bénéficiaire doit obligatoirement être compatible avec les structures CND nécessaires pour l'accès aux datacenters et aux réseaux concernés.

L'ensemble des enregistrements d'exécution (traces, journaux d'événements applicatifs et systèmes, ...) doit être rendu accessible au CND à des fins d'exploitation de la sécurité.

Cette offre de service reste soumise à l'approbation technique du CND dont les modalités sont décrites dans le guide et les conditions générales d'hébergement.

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.032 Urbanisation des équipements dans les Datacenters de la DIRISI Directive n°193 Urbanisation des équipements dans les centres informatiques du CND V2.0 du 01/10/2016	1 avril 2024	DIRISI	Guide	Intradef
<i>Commentaire : Ce document annule et remplace la directive DIRISI n°193 intitulée « Directive d'urbanisation des Datacenters et des salles informatiques auxiliaires ». Il s'adresse aux bénéficiaires d'un hébergement au sein des Datacenters principaux, des salles secondaires et auxiliaires du CND. L'objectif de ce document est de définir les étapes nécessaires à l'urbanisation d'un équipement, en tenant compte de l'ensemble des contraintes, de manière à assurer une installation efficace tout en respectant les règles de l'art. Les bénéficiaires doivent s'assurer que l'ensemble des prérequis énoncés dans ce document soient fournis et validés au moment de la demande d'hébergement.</i>				

6.1.5.6 Hébergement sur SIE (Intradef Embarqué)

Les infrastructures embarquées du SIE permettent l'hébergement d'applications locales depuis la version Baltique. Ces infrastructures apportent des ressources limitées lié aux contraintes d'environnement (espace en baie, énergie, refroidissement, réseau contraint).

Le SIE offre 2 niveaux d'hébergement :

- intégré (mutualisation des services : frontal web, bases de données, télé-déploiement, etc.) ;
- hébergé (mise à disposition d'un espace pour une machine virtuelle entièrement gérée par la direction d'application).

Les directions d'application sont invitées à contacter l'équipe SIE pour connaître les spécifications à jour de l'hébergement sur SIE à prendre en compte.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°236 – SHeM embarqués (SHeMe)	01 mars 2018	DIRISI	Directive	SIE
<i>Commentaire : cette directive sera mise à jour et complétée d'un guide de gouvernance et de recommandation au développement des applications embarquées.</i>				

6.1.5.7 Hébergement de développement

Partie intégrante de l'offre de service Cloud (cf. 3.2.1.2), la composante PICSEL (Plateforme Interarmées pour héberger la production Continue sécurisée des SI Et Logiciels) met à disposition des Responsables de conduite de Projet, des Responsables Technique de Système et des Responsables de Réalisation de Projet des Directions d'application (DA), de projet (DP) ou de programme numérique une infrastructure hors espace de confiance.

Ceci permet de répondre aux enjeux de maîtrise induits par les activités de développement et d'expérimentation tout en donnant plus de libertés aux équipes projet et en facilitant l'accès aux

partenaires industriels dans les locaux du MinArm. Elle met enfin le contrôle qualité indispensable aux projets et programmes numériques du Ministère (MinArm) avant leur installation sur les environnements cibles.

PICSEL permet d'accélérer les étapes de développements, de validation / qualification et de mise à jour des applications (dont le move to cloud) avant le passage en intégration, pré-production et production de leurs applications sur C1DR ou C1NP. PICSEL doit également dérisquer et banaliser ces opérations et alléger les charges d'exploitation dans la durée.

Les standardisations et les contrôles effectués doivent enfin, par les garanties qu'ils apportent, permettre d'alléger les processus de gouvernance actuels associés à ce passage.

PICSEL propose des ressources informatiques sous forme de moyens, d'outils et d'espaces de développement (dénommés « zones projet ») :

- accès rapide à des ressources et en libre-service pour mener des travaux de développement, d'expérimentation ou de qualification dans le cadre d'un projet préalablement validé par la DSI d'appartenance ;
- mise à disposition d'outils et de services représentatifs des services de la production C1DR et C1NP paramétrés selon les normes du Ministère, administrés et exploités pour mener ces travaux ;
- des moyens et outils aux directions d'application pour réaliser un premier niveau de validation et d'intégration ;
- des moyens et outils aux exploitants et aux RSSI-A de s'assurer de la qualité des applications et services (qualité, sécurité, exploitabilité) avant qu'ils ne soient déployés dans les environnements cibles et in fine en production ;
- une chaîne CI/CD DevSecOps vers les environnements cibles (C1NP et C1DR et environnement historique DR dans une moindre mesure, travaux en cours) ;
- mutualisation de la gestion des dépôts de binaires de développement ;
- support à l'utilisation des services via une documentation centralisée et une équipe support.

Cette plateforme est par nature en constante évolution : son catalogue de services s'enrichit au fur et à mesure des décisions et des orientations techniques de la DSI Socle en réponse aux besoins exprimés par les DA/DP et l'ensemble des entités de développement du Ministère. Elle évolue également pour intégrer les évolutions et amélioration des services cloud offerts par les plateformes C1NP et C1DR qui y sont développés. L'intégration des capacités de tests de charges menées par le BEEI du Service projets du CND est également en cours d'étude.

Bien qu'il soit possible d'exposer sur Intradef les systèmes d'information et services qui y sont développés ou expérimentés, ceci doit se limiter à quelques utilisateurs à des fins de tests et de validation. PICSEL (comme toute plateforme de ce type) n'est pas destinée à héberger ou exposer des systèmes d'information ou des services en production utilisés en situation réelle depuis Intradef, même si l'accès en est limité à une population restreinte.

6.1.6 Hébergement sur Internet

Périmètre	Offre	Utilisation / Restrictions	Statut	Portée
Hébergement de production / pré-production	Infogérance Cloud C1NP	Offre d'hébergement Internet	R / S	Internet
Hébergement de production	C3 Internet	Soumis à visa AGORA Cloud CND	A / N	Internet

Document	Date	Origine	Type doc	Portée
Note provisoire n°2025/508/ARM/CND/GOUV STRAT/NP "appui aux DSI, création de l'offre de services AGORA" du 18/11/2025	18 novembre 2025	CND	Note provisoire	Min Arm

Instruction ministérielle n°2010/DEF/DGSIC/NP relative à la mise en œuvre de services en ligne ou de sites internet par le ministère de la défense diffusée par note n°458/DEF/DGSIC/DG/NP du 2 août 2016	2 août 2016	DGSIC	IM	Min Arm
<i>Commentaire : cette IM précise les modalités de demande ou de renouvellement d'agrément pour tout site internet du Ministère, réseaux sociaux inclus, en déclinaison de la circulaire du Premier ministre n° 5574/SG du 16 février 2012 relative à l'Internet de l'État.</i>				
Politique d'hébergement des SI et des données sur INTERNET édition approuvée le 18/07/2022 et diffusée par la note n°255/ARM/DGNUM/SDTN/NP	18 juillet 2022	DGNUM	Politique	Internet
<i>Commentaire : cette politique abroge les directives provisoires précédentes (Offres IaaS/PaaS et SaaS)</i>				
Directive DGSIC n°13 sur la sécurité des accès aux services de l'Internet et de l'hébergement des services Internet du ministère	30 juin 2010	DGSIC	Directive	Min Arm
<i>Commentaire : règles applicables aux accès au réseau et aux services de l'Internet ainsi qu'en matière d'hébergement de services internet. La partie hébergement des services Internet sur l'internet maîtrisé est traitée plus spécifiquement par la Directive DGNUM n°44.(voir ci-dessous)</i>				
Directive DGSIC n°32 portant sur la sécurité de l'hébergement des SI au sein du ministère cf. 4.8.7 Hébergement / Virtualisation	11/03/2014	DGSIC	Directive	Min Arm
<i>Commentaire : applicable à l'opérateur, et aux systèmes informatiques hébergés, en recommandation pour les applications ayant vocation à être hébergées à l'extérieur du ministère.</i>				

6.1.6.1 Hébergement C1NP

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.009 - Conditions Générales d'Hébergement de systèmes d'information sur le service Cloud NP (CGHD-DR) version 2.0	11/07/2025	DIRISI	Guide	Internet C1NP
<i>Commentaire : cette note décrit les conditions générales d'hébergement d'un système d'information NP dans le cadre de l'offre de service Cloud C1NP du CND, la sécurité et les obligations liées à cet hébergement.</i>				

Partie intégrante de l'offre de service Cloud (cf. 3.2.1.2 Démarche et principes liés), C1NP porte la fonction d'hébergement en infogérance NP.

Construit dans une recherche de maîtrise, de standardisation et d'automatisation, C1NP, tout comme C1DR, vise avant tout à simplifier et accélérer la mise en production des systèmes d'information : hébergement infogéré de machines virtuelles avec les systèmes d'exploitations durcis du Ministère. Les services d'authentification et d'échanges avec Intradef y sont également disponibles (PAPI v2.1, messagerie, MindefConnect Internet).

Il apporte toutefois une extension des technologies acceptées et un raccordement automatisé à un panel de services du socle étendu (NTP, DNS, sauvegarde, dépôts de mise à jour MEDUSA, antivirus, gestion des licences Windows et RedHat, supervision, orchestrateur Ruche identique à celui du C1DR, inventaire, comptes de services ainsi que gestion des secrets et des certificats non exposés sur Internet, mise sous observabilité des systèmes d'information accessible depuis Intradef, stockage objet). D'autres services seront progressivement ajoutés à la liste en cohérence avec C1DR et PICSEL (contrôle de conformité, hébergement en orchestration de conteneurs ...).

La démarche de cloudification impose au système d'information de respecter quelques exigences qui sont rappelées ci-après et qui sont destinées à faciliter les automatisations et l'exploitabilité, donc améliorer le niveau de service offert, et d'en conserver la maîtrise dans la durée :

- disposer d'une pile logicielle à jour et soutenue en MCO/MCS (condition d'homologation) ;
- disposer de scripts de déploiements Ruche conformes (ceux de C1NP sont identiques à ceux d'Intradef) ;
- s'adosser à l'authentification MindefConnect Internet ;

- respecter le format des journaux d'événements : le format attendu par le CALID constitue un prérequis à la mise sous supervision de sécurité ;
- raccordement à la solution d'observabilité dédiée aux systèmes d'information (incluant les journaux systèmes et applicatif) dont le tableau de bord est accessible directement depuis Intradef ;
- instancier a minima l'API REST d'observabilité (l'instrumentation pourra être enrichie via développement mais c'est laissé à l'appréciation du projet de ses besoins en la matière) ;
- gérer ses secrets et ses certificats non exposés sur Internet via le service de socle Gestion des secrets.

Les services offerts sur la plate-forme PICSEL ont été mis en place pour faciliter le développement et le test des adaptations nécessaires et d'en contrôler la conformité avant déploiement sur C1NP.

6.1.6.2 Recours offre C3 Internet

Cette acquisition de service doit se faire via le vecteur contractuel interministériel UGAP. Le CND est seul habilité à activer ce levier pour le Ministère.

Le recours à un service cloud en mode SaaS, que ce soit via le contrat OURANOS ou via les contrats d'unité d'œuvre, ou tout autre mode de contractualisation, est subordonné à une demande de visa auprès du CND. Un tel hébergement doit remplir certaines obligations liées à la souveraineté et la sécurité, RGPD inclus.

Dans ce cadre, un avis AGORA Tech est conseillé pour tout système déployé en offre C3 Internet mettant en œuvre des interfaces avec des systèmes d'information ou composants déployés sur des hébergements du Ministère (utilisation de passerelles d'échanges, mise en œuvre de flux de données inter segments, accès depuis des postes ISPT intradef, consommation ou exposition de services). Ce processus n'exonère pas le projet de conduire une démarche d'homologation.

Document	Date	Origine	Type doc	Portée
Politique d'hébergement des SI et des données sur INTERNET édition approuvée le 18/07/2022 et diffusée par la note n°255/ARM/DGNUM/SDTN/NP	18 juillet 2022	DGNUM	Politique	Internet
<i>Commentaire : cette politique abroge les directives provisoires précédentes (Offres IaaS/PaaS et SaaS)</i>				
Circulaire n° 6282/SG du 5 juillet 2021 portant la doctrine d'utilisation de l'informatique en nuage de l'Etat	5 juillet 2021	PM	Circulaire	Toute administration
<i>Commentaire : cette circulaire prévoit que l'administration en charge du système choisit la solution adaptée en fonction de ses propres critères et qu'elle doit privilégier une offre qualifiée et immunisée aux réglementations extracommunautaires</i>				
Référentiel d'exigence Prestataires de services de l'information en nuage (SecNumCloud) de l'ANSSI (version 3.2 du 8 mars 2022)	8 mars 2022	PM	Référentiel	Toute administration
Note provisoire n°2025/508/ARM/CND/GOUV STRAT/NP "appui aux DSL, création de l'offre de services AGORA"	18 novembre 2025	CND	Note provisoire	Min Arm

6.1.7 Hébergement mutualisé SIA sur les intranets classifiés

L'architecture de tout système d'information (architecture applicative et intégration sur le/les réseaux supports) doit être validée par la gouvernance technique (cf. 1.4 Gestion et gouvernance du CCT) (sur dossier ou en présentation) au moment de la revue de conception générale.

Hors cas dérogatoire, l'hébergement d'applications et de systèmes d'information au sein du SIA est structuré autour des moyens ISHM/MHS et permet ainsi aux applications de venir consommer l'offre de services proposée par le SIA (services communs, sauvegarde, stockage, ...). La consommation des

services du SIA ne présume pas du niveau d'infogérance proposé par l'opérateur à la direction d'application (Infogérance ou VPS).

L'hébergement d'une application au sein du SIA doit respecter certaines contraintes et consignes :

- l'application doit respecter le Référentiel d'hébergement, document mis à jour a minima annuellement. Ce document est disponible auprès du programme SIA ;
- l'application peut consommer l'ensemble des services communs du socle étendu fourni par le SIA.
- l'application est hébergée sur un OS basé sur un « *template* » fourni par le SIA.

Les conditions générales d'hébergement concernent essentiellement les offres Infogérance SIA et VPS SIA. Les hébergements en salle blanche ne sont pas la norme mais peuvent être traités au cas par cas.

En complément du présent CCT, les systèmes d'information doivent prendre en considération l'offre de service du SIA décrite par son référentiel d'hébergement.

6.1.8 Informatique décisionnelle

Voir aussi §3.2.6 Informatique décisionnelle traditionnelle (ou BI Corporate)

6.2 Opérations – processus

6.2.1 Gestion des configurations

La mise en place de processus et d'outils de gestion des configurations doit permettre de connaître la composition exacte et à tout moment du parc informatique de responsabilité CND et d'établir des analyses d'impact avant chaque changement.

Pour être efficace, la gestion de configuration doit définir :

- les éléments de configuration qui doivent être inventoriés et suivis en regard des services et processus qu'elle alimente ;
- les processus qui permettront de maintenir à jour les configurations ;
- les acteurs du processus.

Le CND met en œuvre une gestion des configurations sur le périmètre des systèmes d'information métier hébergés dont elle est opérateur.

Le contrôle qualité opéré sur PICSEL et l'API d'observabilité (cf. 6.2.7.4) désormais requis pour les hébergements C1NP et C1DR ainsi que le SI Conformité ont vocation à contribuer à cette gestion de configuration.

6.2.1.1 Base de connaissance de gestion CMDB [BCA]

La base de gestion des configurations (CMDB) a vocation à intégrer tous les systèmes d'information métier et services hébergés par le CND. Elle permettra d'établir la photo du parc matériel et applicatif, de mener des campagnes de rationalisation, d'améliorer la gestion des obsolescences logicielles et le suivi des évolutions.

Document	Date	Origine	Type doc	Portée
GUIDE EMO.GUI.R4.012 Description des systèmes d'Information dans la CMDB version 1.0	01/08/2022	DIRISI	Guide	Min Arm
<i>Commentaire : ce document a pour objet de préciser la description type d'un système d'information dans la CMDB des SI du CND pour permettre à l'exploitant de décrire un système ainsi que de préciser les règles de</i>				

nommage :

- des instances d'applications ;
- des changements uniquement liés à une demande d'hébergement.

6.2.1.2 Inventaire [INV]

Afin d'alimenter la CMDB de l'hébergement, le CND collecte les informations logicielles et matérielles sur les serveurs Windows et Linux. L'alimentation de la CMDB Bureautique utilise quant à elle les remontées MCM pour les postes utilisateurs.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Inventaire	MCM	Microsoft	Limité aux clients WINDOWS depuis 2019	R / S	Min Arm
Inventaire	ServiceNow	ServiceNow	Utilisé par l'opérateur pour alimenter sa CMDB	R / S	Intradef
Inventaire	OCS Inventory	OCS Inventory Team	Dans le cas de réseaux non opérés par le CND et ne disposant pas d'une infrastructure d'inventaire déjà en place. Pour les réseaux opérés ou sous la responsabilité du CND (notamment l'Intradef), soumis à l'approbation du CND	A / S	Min Arm
Inventaire	GLPI	GLPI		A / S	Min Arm

6.2.1.3 Dépôt d'artefacts

Le Ministère doit disposer d'un service qui centralise et sécurise ses artefacts binaires. Ce service a également vocation à faciliter sur l'Intradef, C1NP et PICSEL la récupération et la mise à jour des binaires, bibliothèques et packages issus d'internet ou mis à disposition suite à des développements internes ou de MOI tiers. Il permettra de cartographier les binaires utilisés dans les SI afin d'alerter les responsables des SI en cas d'utilisation de composants obsolètes, interdits ou considérés comme dangereux.

C'est la brique de socle MEDUSA qui est destinée à porter ce service. Elle reprend progressivement l'ensemble du périmètre couvert actuellement par DECOS et l'étend au fur et à mesure, à commencer par les templates d'OS durcis.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Dépôt correctif de sécurité	DECOS-S	DIRISI	Cf. 4.8.4 Maintien en condition de sécurité (MCS) - composant technique	R / S	Min Arm
Dépôt	MEDUSA	Min Arm	Mise à jour Et Dépôt Unifié de Systèmes et Applicatifs	R / S	Min Arm
Répertoire d'artefacts binaires	Artifactory	JFrog	Assujetti à tout autre cadre d'emploi que MEDUSA-RUCHE - nécessité de justifier le cadre d'emploi	A / E	Min Arm
<i>Commentaire : l'objectif pour le Ministère est d'acquérir la maîtrise des binaires de toutes natures mis en œuvre sur ses réseaux et de se constituer une source de vérité unique dans ce domaine. En conséquence, ajouter un autre dépôt vient à l'encontre de cette démarche et ne peut s'entendre que dans des environnements non couverts actuellement et dans l'optique d'une rejointe à terme. En conséquence, ceci nécessite d'être dûment justifié.</i>					

6.2.2 Gestion des demandes

L'hébergement d'un nouveau SI fait l'objet d'une demande dématérialisée dans le catalogue de service du CND.

L'offre hébergement est présentée dans la gamme éponyme du catalogue de services du CND.

6.2.3 Déploiement / Distribution / Orchestration

Dans un objectif de maîtrise des hébergements et des postes de travail, de réduction des délais et des coûts humains d'installation, de mise à jour et d'exploitation, le ministère s'oriente vers une automatisation et une orchestration des déploiements et de la distribution des logiciels.

Sur les systèmes Windows, elle s'appuie principalement sur WSUS et MCM (excluant de facto le recours aux technologies de type Java Webstart par exemple). Dans le cadre de la démarche de cloudification et dans la poursuite du projet Ruche, les installations manuelles des systèmes d'information sont remplacées par une orchestration à base de technologie ansible et de dépôts de binaires maîtrisés.

Ceci a pour objet d'éviter les actions manuelles, sujettes à erreurs, en suivant une documentation lourde à réaliser et difficile à fiabiliser, à standardiser les pratiques entre Datacenter notamment, à rendre reproductibles ces opérations délicates et à réduire drastiquement les délais de mise à disposition.

Ce mode de distribution s'applique aux durcissements de sécurité, aux briques logicielles standards du CCT et au déploiement des systèmes d'information.

Ce mode de déploiement est obligatoire dans les hébergements cloudifiés C1NP et C1DR, y compris pour les systèmes en VPS. Pour les niveaux salle blanche, il devient recommandé hors dérogation AGORA Tech : outre les gains pour les TME, ceci vise à préparer la migration inéluctable vers les hébergements cloudifiés.

Ce mode de déploiement s'appuie notamment sur :

- une bibliothèque de « collections Ansible » ministérielle progressivement enrichie et disponible en libre service sur Intradef ;
- un kit de développement contenant la structure attendue pour le projet ;
- le « guide d'utilisation du modèle de projet Gitlab » associé et deux projets de démonstration sont également disponibles.

Une liste synthétique des collections, des versions de middleware prises en charge et leur état sont disponibles sur la page de la météo des collections Ruche.

Dans le cas où l'offre existante des collections ne répondrait pas totalement au besoin, il est possible d'exprimer son besoin de modification voire de création dans le projet dédié de l'outil de suivi Tuleap afin que la demande soit instruite par le CND. Une collection développée par un projet peut également être proposée pour intégrer la bibliothèque : elle pourra alors être validée, adaptée à une utilisation mutualisée et intégrée.

Cette démarche de standardisation et d'automatisation, alignée sur les principes de l'infrastructure as code sera poursuivie notamment dans les domaines du provisionnement des ressources de type machines virtuelles via, par exemple, le recours à `terraform` (dans le cadre du SIA ou des C1DR et C1NP) ou dans celui de l'orchestration de conteneurs.

Document	Date	Origine	Type doc	Portée
GUIDE EMO.GUI.R4.017 - Offre d'automatisation des déploiements de SI version 1.0	01/10/2022	DIRISI	Guide	Min Arm
GUIDE EMO.GUI.R4.015 - utilisation du modèle de projet Gitlab pour la plateforme RUCHE version 1.0	01/08/2022	DIRISI	Guide	Intradef

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Déploiement	MCM / WSUS	Microsoft		R / S	Intredef
Déploiement	MCM / WSUS	Microsoft		A / S	S-SF SIA Frops
<i>Commentaire : Microsoft a annoncé que WSUS (Windows Server Update Services) était désormais déprécié, en conséquence plus aucune évolution fonctionnelle ne sera pas apportée au produit, au profit de solutions fonctionnant en mode connecté avec leur Cloud. Toutefois à date, Microsoft n'annonce pas de retrait et continue à fournir le service avec ses versions de Windows Server (dont 2025).</i>					
Déploiement	OCS Inventory	OCS Inventory Team	Assujetti aux configurations projetables SIA et dans le cas de réseaux non opérés par le CND et ne disposant pas d'une infrastructure de déploiement déjà en place. Toute autre utilisation est soumise à la stricte approbation du CND.	A / S	Min Arm
Orchestration	Puppet	Apache	Sur SIE (version Baltique), pour la distribution des configurations. Sur I3E, pour le contrôle périodique des configurations et le MCS. A titre transitoire (le temps de la migration C1DR), sur environnement S2NA-Intredef	A / -	Intredef dont SIE et I3E
<i>Commentaire : assujetti au titre de l'existant actuel, dans une optique à terme de rejointe d'une cible Ansible.</i>					
Déploiement	RUCHE	Min Arm		R / S	Min Arm
<i>Commentaire : RUCHE a pour vocation à fournir des services et une plateforme autour de la solution Ansible pour l'automatisation des déploiements de SI. Il vise un service optimisé aux exploitants et un changement dans le mode de livraison des SI infogérés. (cf. ci-dessous pour un premier niveau d'offre de service)</i>					
Orchestration	Ansible	REDHAT	Pour l'automatisation de l'installation et du déploiement de tout nouveau SI	R / S	Intredef Internet
<i>Commentaire : Ansible (au travers de Ruche, à chaque fois que le service est disponible sur le réseau support) est désormais le mode requis d'installation et de mise à jour des nouveaux systèmes d'information sur les plateformes du CND.</i>					
Provisionnement	Terraform	HashiCorp	Pour l'automatisation du provisionnement des ressources de type VM	A / -	Min Arm
Génération d'images	Packer	HashiCorp	Génération d'images machine identiques multi plateformes	R / -	Min Arm

6.2.4 Gestion du stockage

Dans les structures d'hébergement de l'Intredef, la gestion du stockage est actuellement assurée par les outils déployés dans chaque Infrastructure d'hébergement.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Stockage SAN	Pure Storage	Pure Storage	Structures d'hébergement	R / S	Intredef
Stockage SAN	Hitachi	Hitachi	Structures d'hébergement	R / S	Intredef
Stockage NAS	Hitachi	Hitachi	Structures d'hébergement	A / S	Intredef
Stockage NAS	Netapp	NetApp	Structures d'hébergement	A / S	S-SF SIA Frops
Stockage Objet	Scality Ring	Scality	Assujetti au recours à IRIS	A / S	Intredef

6.2.5 Synchronisation / Réplication / Déduplication

Pas de référence identifiée à ce jour.

6.2.6 Sauvegarde / restauration

La sauvegarde et restauration s'appuie sur les solutions logicielles ci-dessous suivant le type de données et la structure d'hébergement.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Sauvegarde	Time Navigator (TINA)	ATEMPO	Structures d'hébergement : Pour les données structurées avec sauvegarde sur bandes. Par défaut pour l'offre d'hébergement VPS Cloud	R / S	Intradef
Sauvegarde	MIRIA (ADA)	ATEMPO	Sauvegarde serveur de proximité	R / S	Intradef
Sauvegarde	VEEAM	VEEAM Software	Pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits	R / S	Intradef S-SF SIA FrOps Intrasan
Sauvegarde	Bareos	Bareos	Assujetti au contexte SIE. Outil sous licence libre AGPL v3, utilisé sur le SIE Baltique.	A / S	SIE
Sauvegarde	Elastic Curator	Elastic	Gestionnaire de snapshots Elasticsearch/Opensearch	A/N	Intradef S-SF SIA FrOps

6.2.6.1 Sauvegarde du poste de travail

Pour la sauvegarde du poste de travail, certains organismes (DGA, SIMMT...) ont mis en place une solution basée sur la solution LINA de la société ATEMPO.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Sauvegarde	Live Navigator (LINA)	ATEMPO	Solution de sauvegarde des postes de travail sur le périmètre DGA	A / S	Intradef

6.2.7 Observabilité

L'un des enjeux de la démarche de cloudification (cf. 3.2.1.2) est l'accroissement de maîtrise sur les infrastructures et systèmes d'information hébergés. Outre les aspects de conformité et de sécurité, la visibilité sur leur fonctionnement est également un axe qui doit être développé.

La capacité d'un système d'information à fournir des informations sur son fonctionnement interne à partir d'éléments qu'il émet s'appelle l'**observabilité**. Elle facilite la supervision et permet une identification et une résolution des problèmes plus rapides voire automatisées en vue de répondre aux attentes des utilisateurs et d'atteindre les niveaux de services (SLA ou Service Level Agreements) et autres exigences métier.

Le bénéfice principal de l'observabilité est qu'un système plus observable est plus facile à comprendre (en général et en détail), plus facile à superviser, plus facile et plus sûr à mettre à jour et plus facile à réparer.

Par extension, l'observabilité fait également référence aux outils logiciels et aux pratiques permettant d'agréger, de corréler et d'analyser un flux continu de données de fonctionnement des applications associées à celles du matériel et du réseau sur lesquels elles s'exécutent.

L'observabilité applicative se concentre sur 4 types principaux de données, dont les 3 communément désignés comme étant **les 3 piliers de l'observabilité** : les journaux d'événements applicatifs, les métriques et les traces applicatives auxquels s'ajoutent les dépendances :

- **journaux d'événements applicatifs (ou logs)** : enregistrements granulaires, horodatés, complets et immuables des événements applicatifs qu'on peut trouver sous 3 formats : texte, structuré ou binaire. Parmi tant d'autres, les journaux d'événements applicatifs peuvent être utilisés pour créer des enregistrements haute fidélité, milliseconde par milliseconde de chaque événement, complets avec le contexte associé que les développeurs peuvent « rejouer » à des fins de recherche de panne ou de débogage ;
- **métriques** : appelées parfois métriques « *time series* », ce sont des mesures fondamentales de la santé de l'application et du système sur une période de temps donnée, par exemple combien de mémoire ou de capacité de calcul une application utilise sur une période de 5 minutes ou encore avec quel délai de réponse une application répond lors d'un pic d'utilisation ;
- **traces** : les traces enregistrent le « voyage » de bout en bout de chaque requête utilisateur, depuis son interface ou son application mobile via toute l'architecture distribuée jusqu'au retour de la réponse ;
- **dépendances** : également appelées cartes de dépendances, elles indiquent de quelles autres composantes, applications ou ressources technologiques dépend une application.

Une fois collectées, ces informations sont agrégées en temps réel pour fournir une **information complète et contextuelle** : le **quoi**, **où** et le **pourquoi** de chaque événement. Ces informations multiples peuvent être découvertes automatiquement par des systèmes qui, pour traiter cette masse de données, peuvent s'appuyer sur de l'intelligence artificielle (AIOps) afin d'extraire des signaux – l'indication d'un problème réel – au milieu du bruit.

L'observabilité et la supervision, qu'elle soit applicative⁶¹ ou réseau⁶², sont deux concepts distincts mais complémentaires. La supervision collecte et analyse des données connues comme étant liées à des problèmes de performance de l'application, du système ou du réseau (les **known unknowns** : des conditions exceptionnelles qu'on sait devoir surveiller) alors que l'observabilité donne aux équipes des informations contextuelles nécessaires pour identifier et résoudre au plus tôt des problèmes dont elles n'étaient pas conscientes (**unknown unknowns**) et permettre des infrastructures de remédiation automatique et des infrastructures d'auto réparation des applications.

Le Ministère disposait déjà de capacités de supervision grâce au projet PISARO :

- **PISARO Supervision** (aspect *métriques*) : surveillance de l'état des infrastructures des SI hébergés par le CND,
- **PISARO Métrologie** (aspect *traces*) : suivi précis et proactif du fonctionnement des SI à fort enjeu de disponibilité.

En capitalisant sur ces capacités, le Ministère étend la démarche afin de prendre en compte :

- l'ensemble des dimensions de la supervision et de l'observabilité ;
- toutes les plateformes composant le cloud (C1NP, C1DR et PICSEL – y compris pour l'hébergement en orchestration de conteneurs).

Pour marquer cette extension de périmètre, l'ensemble des composantes contributrices (dont celles de PISARO) est regroupé au sein du projet « Observabilité ».

Sur le segment réseau Intrasan du SSA, la supervision système se fait au travers de Manage Engine OPM.

⁶¹ APM ou Application Performance Monitoring

⁶² NPM ou Network Performance Monitoring

6.2.7.1 Journaux d'événements applicatifs et système

Document	Date	Origine	Type doc	Portée
Recommandations de sécurité pour l'architecture d'un système de journalisation ANSSI-PA-012/ANSSI/SDE du 28/01/2022 : https://messervices.cyber.gouv.fr/guides/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation	28 janvier 2022	ANSSI	Guide	Toute admin.

Dans le cadre de la cloudification en général et du projet « Observabilité » en particulier, une infrastructure adossée à Elastic a été mise en place sur PICSEL et sur la composante C1NP. Son déploiement est également en cours sur le C1DR en vue d'une ouverture mi-2026 au profit des directions d'application. Le service fonctionne actuellement pour les SI sous RHEL ou Alma 8. Cette composante Observabilité C1DR a vocation à donner accès aux directions d'application aux données d'observabilité des systèmes d'information hébergés sur C1NP (dans l'attente, un accès à ces informations depuis Intradef a été mis en place). Les systèmes d'information et services y déverseront leurs journaux d'événements applicatifs et système, permettant ainsi une consultation et une interrogation centralisée au bénéfice des différents acteurs. L'adossement au stockage IRIS permet de les conserver conformément aux délais requis par la réglementation. Enfin, il alimente les outils de supervision de sécurité.

Plusieurs solutions du socle vont s'appuyer sur cette capacité (dont la PAPI v2.1, RUCHE et SARDaC).

6.2.7.2 Métriques

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Observabilité	Elastic Entreprise	Elastic	Mise en place pour la supervision des structures d'hébergement et des SI hébergés par le CND sur PICSEL, C1NP, C1DR	R / S	C1NP, C1DR, PICSEL
PISARO Supervision	Shinken Enterprise	Shinken	Mise en place pour la supervision des structures d'hébergement et des SI hébergés sur SHSM DR par le CND.	R / S	Intradef
Supervision/Hypervision	GSYS Solution basée sur Shinken		Solution de supervision apportée (et soutenu) par le SIA	A / S	S-SF SIA FrOps
Sonde NRPE	NRPE	Daemon Linux	Agent de supervision NRPE	R / S	Min Arm
Sonde NRPE	NSClient ++	NSClient	Agent de supervision NRPE. Périmètre de déploiement restreint aux serveurs Windows	A / S	Min Arm

S'adressant aux SI hébergés sur l'offre historique SSMH DR, alimenté par les métriques qu'il collecte, PISARO supervision (intégré à la solution Observabilité) couvre la surveillance du bon fonctionnement du système.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°263 relative à l'exploitation et au soutien PISARO (supervision)	01/11/2019	DIRISI	Directive	Intradef
<i>Commentaire : la directive présente l'architecture générale de la partie supervision de PISARO (métropole et outre-mer). Elle fournit à tous les acteurs des éléments quant à l'exploitation et au soutien de PISARO dans sa fonction de supervision. Elle précise les responsabilités et fonctions accessibles des différents acteurs.</i>				

6.2.7.3 Traces

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Observabilité	Elastic Entreprise	Elastic	Mise en place pour la collecte des traces des SI hébergés par le CND sur PICSEL, C1NP, C1DR	R / S	C1NP
PISARO Métrologie	Dynatrace	DynaTrace	• mise en place pour monitorer les applications identifiées comme critiques par le CND • utilisé aussi par le CASID lors des audits ou assistances des SI confrontés à des problèmes de performances (en collaboration avec le BEEI). Intégrée au projet Observabilité.	A / S	Intradef

Les traces permettent de mesurer la performance des sessions utilisateurs via le suivi des temps de réponse et la performance des processus métier via le suivi des transactions, etc.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°257 relative à l'exploitation et au soutien PISARO (métrologie)	01/11/2018	DIRISI	Directive	Intradef
<i>Commentaire : la directive fournit à tous les acteurs des éléments quant à l'exploitation et au soutien de PISARO dans sa fonction de métrologie. Elle précise les responsabilités des différents acteurs. Elle précise les critères d'éligibilité d'une mise sous métrologie d'un SI et le processus de mise en place. PISARO est intégrée à la solution Observabilité.</i>				

6.2.7.4 Dépendances (C1NP et C1DR)

Le suivi des dépendances est adressé travers des informations collectées dans la CMDB du CND ainsi que, de façon plus dynamique, à l'aide de l'API d'observabilité. Cette dernière a pour objet de :

- Faciliter la récupération d'informations relative à la gouvernance ayant un impact sur les hébergements (trigramme, version, niveau ARR, DSI d'appartenance ...) ;
- Améliorer l'observabilité des systèmes d'information en mettant à disposition un état synthétique de bon fonctionnement et de leur capacité à utiliser les services et autres systèmes d'information dont ils dépendent.

6.2.7.5 Sur les réseaux classifiés

Cf .6.1.7

6.2.8 PCA/PRA – PCI/PRI - Gestion de crise

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.010 Tests périodiques des Plans de Continuité d'Activité & Plans de Continuité Informatique version 2.0	20/04/2022	DIRISI	Guide	Min Arm
<i>Commentaire : ce guide consultable sur DIADEME a pour but de fixer les conditions de mise en œuvre des tests périodiques des Plans de Continuité d'Activité (PCA) du CND ; des Plans de Continuité Informatique (PCI) des systèmes d'information (SI) critiques, exploités par le CND au profit de ses clients ou à son propre bénéfice, d'autre part. Il vise donc à décrire les différents types de tests, leur fréquence, le rôle des acteurs,</i>				

les modalités d'établissement du calendrier des tests et les procédures de compte rendu. Il n'a pas vocation à fournir les modes opératoires de réalisation ni les modèles de rédaction des PCA et PCI.

Voir également § 4.8.2 PCA-PRA

6.2.9 Gestion d'exploitation et des capacités

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestion incidents	DIADEME	Service Now	Gestion des incidents. Basé sur Service Now	R / S	Min Arm
Commentaire : La déclaration d'un incident est réalisée via DIADEME [via ce formulaire].					

6.2.10 Hypervision

Pas de référence identifiée à ce jour.

6.2.11 Administration réseaux, performance réseaux et Télécommunications

Pas de référence identifiée à ce jour.

6.2.12 Surveillance et métrologie des salles

Pas de référence identifiée à ce jour.

7 CONCEPTION – DEVELOPPEMENT

7.1 Règles générales

Les applications conçues et développées aujourd'hui structurent le système d'information ministériel de demain. La conception d'une nouvelle application doit s'effectuer dans le cadre des concepts fondamentaux définis au §3.2.1.1 **Concepts fondamentaux** (indépendance technologique, rationalisation des techniques utilisées, interopérabilité native).

Dans le cas où le choix s'oriente vers un développement externalisé ou l'acquisition d'un progiciel « sur étagère », outre les concepts ci-dessus, de nombreux principes restent valables.

Cela se traduit par les recommandations suivantes :

- L'approche silo est proscrite, le choix doit être fait dans un contexte global, en tenant notamment compte de l'intégration du nouveau produit dans son environnement applicatif au sein du SI du Ministère ;
- Pour les développements externalisés, afin de permettre aux industriels postulants de s'inscrire dans la démarche de rationalisation technique du ministère, le présent CCT (dans sa version NP à diffusion réfléchie) doit être joint au CCTP, en tout ou partie selon les modalités proposées au §1.5 **Prise en compte dans le cadre des cahiers des charges** ;
- Pour les développements internes et externes un passage par le chaîne de pré intégration de PICSEL est requis ; il a notamment pour objet de vérifier la bonne prise en compte des prérequis des hébergements Cloud C1 ;
- Des règles de gouvernance, de conduite de projet ou de prise en compte de la SSI et d'hébergement s'appliquent aux maîtres d'ouvrage faisant réaliser des applications, qu'elles soient ou non basées sur des progiciels du commerce. Des règles d'autres domaines (archivage, etc.) peuvent également s'appliquer.

7.2 Analyse, modélisation

La modélisation métier est un préalable à toute démarche d'informatisation. Au sein du Ministère, cette démarche, qui s'inscrit dans un cadre étatique, repose sur la description d'un modèle d'entreprise conformément au langage retenu Archimate, et qui couvre quatre axes : Stratégique, Métier, Applicatif et Technique (contre 5 jusqu'à présent, la couche fonctionnelle se retrouvant dans les axes métier, applicatif et technique).

Cette démarche de modélisation est cadrée par un guide destiné aux architectes du Ministère.

L'utilisation de ce guide s'accompagne de la mise en œuvre d'outils ministériels accessibles localement sur chaque poste de travail :

- Archi (pour les représentations d'architecture, respect natif du langage Archimate), certains patterns seront fournis au travers de bibliothèques en libre disposition ;
- CAMUNDA (pour les modélisations des processus, selon le BPMN) ;
- Modélio (pour les diagrammes de données, selon UML) ;
- Draw.IO (pour les phases d'idéation).

Les travaux de modélisation réalisés dans le cadre d'un projet, de rédaction de schémas directeurs, etc. peuvent être importés dans le référentiel d'architecte d'entreprise (AE). L'alimentation du référentiel AE central se fera en conséquence selon un processus de gouvernance avec des contrôles de cohérence, l'analyse de la pertinence du contenu, notamment au regard des interfaces. La gestion de ce référentiel sera sous MEGA HOPEX.

Le référentiel AE central sera restreint en modification aux urbanistes CND, un accès sera ouvert aux architectes d'entreprise des DSI Domaines (un par DSI). Les modélisations seront toutefois accessibles en lecture au Ministère via un site web généré avec MEGA HOPEX.

Par ailleurs, l'annexe 8.7 Modèles d'architecture du présent CCT présente un catalogue des architectures recommandées, modélisées à l'aide d'un sous-ensemble simplifié et adapté aux besoins du Ministère de la spécification Archimate.

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
ARCHIMATE	Langage de modélisation ouvert d'architecture d'entreprise. Norme technique de l'OpenGroup. Choisi comme un standard recommandé pour décrire les architectures dans le référentiel OTAN NAF v4 . Cf. https://www.opengroup.org/archimate-forum/archimate-overview .	R	Min Arm

Document	Date	Origine	Type doc	Portée
Guide ministériel n°3 « export documentaire du plan d'occupation des sols du ministère des Armées » édition POS v6.0 mise à jour approuvée le 8 décembre 2025	8 décembre 2025	CND	Guide POS	Min Arm
<i>Commentaire : ce document décrit l'ensemble de secteurs qui composent le POS. La version 6.0 ajoute la zone fonctionnelle Cyber</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Modélisation métier	MEGA	MEGA	HOPEX	R	Min Arm
Modélisation métier	ARCHI	Archi	Implémente Archimate 3.2, préconisé pour la modélisation d'ensemble des SI.	R	Min Arm
Modélisation métier	CAMUNDA MODELER	CAMUNDA	Logiciel permettant de modéliser les processus métier au format	R	Min Arm

	(Open Source Desktop Modeler)		BPMN 2.0 et les modèles de décision au format DMN 1.1.		
Modélisation métier	MODELIO	MODELIO	Logiciel permettant de modéliser en UML 2.5 (préconisé pour les modèles de classes ou d'activités) 2.5 mais aussi en BPMN 2.0, Archimate 3.2.	R	Min Arm
Modélisation métier	DRAW.IO	Diagrams.net (JGraph)	Logiciel permettant de modéliser librement (mode idéation), qui est une alternative à Microsoft Visio avec en natif des artefacts de différents langages de modélisation (UML partiel, BPMN, etc.).	R	Min Arm

7.3 Développement

Dans sa version actuelle, ce paragraphe s'applique aux développements internes du Ministère. Néanmoins, les documents référencés constituent des guides de règles et bonnes pratiques pour tout développement, à ce titre il est possible d'y faire référence dans les documents contractuels.

Par ailleurs, il est rappelé que de nombreux usages reposent sur le passage par des réseaux contraints, spécificité qu'il importe de prendre en compte dès les phases de développement (cf. 5.2.1.4).

7.3.1 Outils de développements internes

7.3.1.1 Environnement DevSecOps ministériel

7.3.1.1.1 Ambitions et orientations DEVSECOPS

Différents travaux sont en cours de réalisation pour consolider la plateforme de développement dotée d'une chaîne DEVSECOPS pérenne au profit de l'ensemble du Ministère.

Dans un premier temps, une capacité de déploiement automatisé et d'intégration automatisée a été mise en place sur PICSEL⁶³ ainsi que d'une capacité d'intégration et de déploiement continu vers les composantes C1NP et C1DR du cloud, avec des améliorations à venir (amélioration et simplification, automatisation complète du déploiement vers C1NP et C1DR).

En parallèle une primo capacité CI/CD sur base d'orchestration de conteneurs a été réalisée sur PICSEL et est disponible entre PICSEL et C1DR.

Ces travaux sont réalisés en étroite interaction avec RUCHE, le référentiel unifié de code source mis en place en relation avec le pôle hébergement. RUCHE est le dépôt git national (a minima pour les collections ansible et autres éléments propres aux déploiements).

Offrant une première capacité de CI/CD⁶⁴, la chaîne actuelle comprend :

- la génération à la demande et le management de Zones Projets, permettant aux équipes projet (ou centre de développement / exploitation) d'avoir un environnement de développement, d'expérimentation et à terme de pré-intégration (plateforme PICSEL) ;
- la mise à disposition d'un orchestrateur de déploiement (Ansible) permettant aux équipes projet d'automatiser leurs déploiements en réutilisant et en spécialisant les productions du pôle hébergement (collections de RUCHE) ;

⁶³ Plateforme InterArmées pour héberger la production Continue Sécurisée des SI Et les Logiciels

⁶⁴ Continuous Integration/Continuous Delivery

- la mise à disposition d'un orchestrateur d'intégration continue (Gitlab CI), associé à l'écosystème habituel des chaînes de développement (Analyse statique SonarQube, tests de conformité et de sécurité SCAP...) ;
- la mise à disposition de dépôts sécurisés et mis à jour (MEDUSA) permettant le déploiement des applications et des machines à utiliser.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Environnement de développement	PICSEL	Min Arm	Plateforme DevSecOps de développement et d'expérimentation, assurant le contrôle qualité requis pour un hébergement sur C1DR et C1NP. Cf. 6.1.1	R / S	Min Arm
Environnement de développement	ShemDev	Min Arm	Capacité résiduelle de fournitures de ressources à des fins de développement assujettie aux cas d'usage non encore couverts par PICSEL	D / -	Min Arm
Gestionnaire de version	Gitlab	Gitlab		A / -	Min Arm
Gestionnaire de version	Bitbucket	Atlassian		D / -	Tout intranet
<i>Commentaire : L'éditeur ATlassian abandonne progressivement le support de Bitbucket on premise jusqu'en 2029. Au delà, les données ne seront plus accessibles qu'en lecture. Cf le NeMO CND/GOUV STRAT/GOUV NUM n°2025/66 du 27/10/2025.</i>					
Gestionnaire de version	Forgejo	Codeberg	Fork libre de Gitea qui a changé de licence. Gestionnaire de version pour des besoins modestes	A / N	Min Arm
<i>Commentaires : le 22 octobre 2022, le projet Gitea a annoncé la création de l'entreprise Gitea Limited et le transfert de la marque et du domaine du projet à celle-ci afin d'assurer le futur du projet. Cette annonce a généré quelques réticences de la part de contributeurs et utilisateurs, notamment au travers d'une lettre ouverte, conduisant en décembre 2022 le développeur actif de Gitea à créer un fork appelé Forgejo.</i>					
Intégration Continue	GitlabCI	Gitlab	Assujetti au besoin d'une instance dédiée hors PICSEL ou RUCHE	A / S	Intradef
Qualimétrie	SonarQube	SonarSource	Assujetti au besoin d'une instance hors PICSEL	A / -	Min Arm
Orchestration	RedHat automation controller	Red Hat	Assujetti au besoin d'une instance dédiée hors PICSEL ou RUCHE	A / -	Min Arm
Orchestration	Molecule	opensource	Utilisation pour test des collections Ansible	A / -	Min Arm
<i>Commentaire : dès lors que la plateforme ministérielle de déploiement automatisé est en capacité d'opérer dans l'environnement considéré, celle-ci doit être utilisée. Les composants ci-dessus complètent le dispositif sur les environnements non équipés.</i>					

7.3.1.1.2 Plateforme de développement PICSEL

Pile logicielle : Annexe 8.2 (Cf 8.2.1)

7.3.1.2 CALI et OBEO Designer (anciennement dans S@fran)

OBEO Designer et CALI (catalogue d'architectures logiciels industrialisés) forment un système de modélisation et de développement Low-Code permettant d'homogénéiser les démarches de développement, standardiser les outils et normaliser la production logicielle. Ce générateur a été conçu pour les développements en JAVA et applications de type client web.

Cette plateforme est destinée au maintien de SI legacy et interdite pour tout nouveau projet.

7.3.2 Développement en Java

Document	Date	Origine	Type doc	Portée
Guide de règles et de recommandations relatives au développement d'applications de sécurité en Java, https://cyber.gouv.fr/publications/securite-et-langage-java	2009	ANSSI	Guide	Min Arm
<i>Commentaire : Ce guide élaboré dans le cadre du projet JAVASEC sous l'égide de l'ANSSI présente des règles et recommandations pour le développement d'applications JAVA avec un bon niveau de prise en compte de la sécurité. Même si ce guide date un peu, nombre de préconisations de développement restent d'actualité. Les éléments de ce guide sont sur le site de l'ANSSI : https://messervices.cyber.gouv.fr/guides/securiser-un-environnement-dexecution-java-sous-windows</i>				

Le framework Spring est recommandé pour le développement backend en Java. Il est très complet et permet une très grande variété d'intégration avec d'autres frameworks si besoin. Les principaux composants à privilégier sont :

- Spring MVC (pour le développement d'applications web),
- Spring Security (pour gérer l'authentification, les habilitations et la protection contre diverses attaques),
- Spring Data (qui simplifie l'accès aux bases de données en fournissant une abstraction pour travailler avec différentes sources de données, telles que les bases de données relationnelles et NoSQL).

Sur le plan de l'architecture, Spring fournit un conteneur IoC (pour la gestion des objets et de leur cycle de vie. Il prend en charge l'injection de dépendances, la configuration des beans, et la gestion des transactions). Enfin, Spring prend en charge la programmation par aspect (AOP) ce qui permet de séparer la logique métier des aspects techniques et transverses comme par exemple la gestion de la sécurité, des transactions, de la sécurité, ou encore de la journalisation d'événements.

Spring Boot est un projet Spring qui simplifie et accélère la création d'applications Java en fournissant une configuration automatique (avec différents profils possibles qui définissent des dépendances préconfigurées appelées « starters ») qui réduit fortement la complexité d'une configuration manuelle.

JHipster (Java Hipster) est un générateur d'applications Spring Boot. Ses principaux avantages pour améliorer la productivité des développeurs sont :

1. Configuration : JHipster génère une configuration initiale complète pour une application Spring Boot comprenant notamment la structure du projet, la configuration de la base de données, la sécurité avec Spring Security (supporte OpenID Connect), la gestion des utilisateurs (gestion de profils utilisateurs), Elasticsearch, et bien d'autres. JHipster intègre également la configuration du Frontend et supporte Vue.js, React et Angular (supporte également la création d'application PWA) ;
2. Scaffolding : JHipster peut générer automatiquement le code source de l'application, les entités, les contrôleurs et services REST, les modèles de vues ;
3. Base de données : JHipster prend en charge plusieurs systèmes de gestion de base de données, notamment MariaDB, MySQL, PostgreSQL, MongoDB. Il génère également des scripts de migration pour les modifications de schéma de base de données (supporte les outils Flyway ou le très simple dbDeploy qui peut s'intégrer dans le code en tant que Spring Bean) ;
4. Outils de développement : JHipster intègre divers outils de développement, tels que des outils de test, de gestion de base de données et de génération de code. Il possède également, avec le « JHipster Domain Language » (JDL), un langage de description pour l'application, ses entités et relations utilisable dans un IDE (Eclipse, IntelliJ ou VS Code) ;
5. Déploiement : JHipster génère des fichiers de configuration pour le déploiement y compris pour des conteneurs (par exemple pour un cluster Kubernetes).

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Environnement Java	Jakarta EE	Eclipse(Licence Publique Eclipse 2.0)		★ / ★	Min Arm
Framework de développement	Spring	VMWare (licence Apache 2.0)	Framework d'infrastructure pour les applications d'entreprise Java à utiliser préférentiellement avec l'OpenJDK 8/17.	R / -	Min Arm
<i>Commentaire : A noter que la fin du support de la version 5.3 a été atteinte le 31/12/2024⁶⁵ (une extension de 2 ans supplémentaires est possible au travers d'un support commercial), la version 6.2 (tout comme Spring Boot 3.5) atteint sa fin de support en juin 2026 (extension de support de 6 ans possible via support commercial). La version majeure actuellement active est la version 7 (avec Spring Boot 4.0) et nécessite d'utiliser au minimum le JDK 17. De plus, la version 5.3 prenait en charge les versions 7 et 8 de Java EE sous namespace javax tandis que la version 6 passait aux versions 9 et 10 de Jakarta EE sous namespace jakarta. Avec la version 7, c'est désormais Jakarta EE 11 qui est à utiliser (Servlet 6.1, JPA 3.2 et Bean Validation 3.1).</i> Il est donc recommandé aux projets utilisant cette technologie ne l'ayant pas encore fait de procéder rapidement à une montée de version majeure.					
Framework de développement	Spring Boot	VMWare (licence Apache 2.0)	Outil d'aide à la création d'application Spring, simplifiant la gestion des dépendances et la configuration ; la fonction permettant d'embarquer un serveur d'application Tomcat, Jetty ou Undertow ne doit pas être utilisée (hors des environnements de développement ou d'hébergement en orchestration de conteneurs).	★ / -	Min Arm
Framework de développement	JHipster	Projet communautaire (Licence Apache 2.0)	Générateur de projet d'application Spring Boot intégrant la réalisation d'un frontend avec Vue.js, React ou Angular.	R / -	Min Arm
Framework de développement	Quarkus	Projet communautaire (Licence Apache 2.0) avec Red Hat comme principal contributeur.	Quarkus est un framework Java conçu pour les applications cloud-native et les microservices. Il se distingue par sa rapidité de démarrage et sa faible consommation de mémoire, ce qui le rend particulièrement adapté aux environnements de conteneurs comme Kubernetes. Son usage au Ministère est assujéti à l'usage de conteneurs.	A / -	Min Arm

★ pour les recommandations sur les versions voir le détail en annexe §8.2.1 Pile logicielle : liste des produits.

7.3.3 Développement en PHP

Document	Date	Origine	Type doc	Portée
Cadre technique relatif au développement PHP au sein du ministère de la Défense diffusé sous timbre n°185/DEF/DGSIC/DG/NP du 6 avril 2016 (Nemo n°2016/2016/99)	6 avril 2016	DGSIC	Cadre technique	Min Arm
<i>Commentaire : ce document cadre, désormais obsolète, précise les conditions de réalisation technique d'applications développées en PHP au sein du ministère : il précise les règles techniques à respecter, émet</i>				

⁶⁵ <https://spring.io/projects/spring-framework#support>

des préconisations en matière d'outils de développement et énonce les bonnes pratiques en conformité avec l'état de l'art. Il est applicable aux centres de développement du Ministère.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Framework de développement	Symfony	Symfony SAS (licence MIT)		★ / -	Min Arm
Framework de développement	Laravel	Communauté (licence MIT)		R / -	Min Arm
Framework de développement	Drupal	(licence GNU GPL 2)		R / -	Min Arm

★ pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits.

7.3.4 Développement en C# et .NET

Le framework .Net, ainsi qu'un système d'exploitation Windows, font partie des prérequis pour développer en C#. L'environnement de développement est Microsoft Visual Studio, auquel il est possible d'ajouter des plugins, et la gestion du cycle de vie peut se faire via TFS (*Team Foundation Server*) qui gère le versioning des sources, la réservation de code, la gestion des tâches, les builds, etc. Une instance de SQL Server est indispensable au fonctionnement de TFS. Enfin, la gestion des dépendances nécessite Nuget.

7.3.5 Développement HTML5-Javascript-CSS

Pour ce type de développement, il est recommandé de privilégier la réalisation d'application SPA (*single page application*). Ceci afin d'améliorer la performance de l'application en réduisant les sollicitations vers un serveur de présentation et donc de la bande passante réseau.

Règle	Énoncé	Statut	Portée
RT_DEV_10_1	Pour la réalisation d'applications web, il est RECOMMANDÉ de privilégier un développement de <i>Single Page Application</i> [SPA].	R	Min Arm

Il est également recommandé de réaliser le rendu des pages côté serveur plutôt que côté client (SSR) pour améliorer la performance de l'application et la mise en cache des pages. Cette approche est nécessaire pour améliorer le référencement d'un site si nécessaire (SEO). La génération de sites statiques (*Static Site Generator* : SSG) est également à privilégier à l'installation lorsque c'est envisageable pour améliorer la performance et la sécurité.

Règle	Énoncé	Statut	Portée
RT_DEV_11_1	Pour la réalisation d'applications web, il est RECOMMANDÉ de réaliser le rendu des pages côté serveur [SSR].	R	Min Arm

La génération de sites statiques est également à privilégier lorsque c'est envisageable pour améliorer la performance et la sécurité.

Règle	Énoncé	Statut	Portée
RT_DEV_12_1	Pour la réalisation de pages web globalement statiques, il est RECOMMANDÉ de recourir à la génération de sites statiques [SSG].	R	Min Arm

La technologie PWA (*progressive web app*) est recommandée pour permettre le fonctionnement en mode temporairement déconnecté d'un SI réalisé en client-léger.

Règle	Énoncé	Statut	Portée
RT_DEV_13_1	Pour les besoins de fonctionnement en mode temporairement déconnecté d'un système d'information en client léger, il est RECOMMANDÉ de recourir au développement d'une progressive web app [PWA].	R	Min Arm

☆☆☆☆☆
 Pour la réalisation d'applications mobiles, privilégier le développement de PWA (progressive Web Apps). Développement en mode natif soumis à dérogation.
 ☆☆☆☆☆

Actuellement, deux frameworks pérennes s'imposent pour le développement d'application en Javascript : Vue.js et React. Le premier est à privilégier car il est le plus simple à maîtriser tout en étant suffisamment complet pour la plupart des SI du Ministère. React est aussi complet et bénéficie d'un bon support éditeur sur les vulnérabilités critiques.

Angular, précédemment recommandé, est dorénavant assujéti à la maintenance des SI existants en production, à des développements réalisés par des équipes internes déjà formées et expérimentées sur Angular, ou à l'engagement de la DSI à suivre le rythme des montées de versions. Le support des versions LTS étant désormais de 18 mois⁶⁶, le maintien à jour est moins coûteux. C'est un framework qui est plus complexe et exigeant à maîtriser que Vue.js ou React sans qu'il apporte des fonctionnalités majeures qui ne seraient pas réalisables avec Vue.js ou React (avec si besoin des bibliothèques complémentaires disponibles dans les écosystèmes de ces frameworks, voire des frameworks tels que Nuxt.js ou Next.js).

Le développement en JavaScript pour le backend nécessite l'environnement d'exécution Node.js (cf. 3.2.2.2.5 *Environnement d'exécution JavaScript*). Pour la partie web associée, le framework recommandé est Express. Son remplacement par le framework Fastify est assujéti à un besoin de très fortes performances ou de traitements complexes en mode asynchrone. Express est un framework simple et performant qui dispose d'un écosystème très important de bibliothèques et framework complémentaires permettant d'apporter des fonctionnalités prêtes à l'emploi. Parmi celles-ci, et pour éviter une trop grande diversité de framework, il est conseillé de privilégier les frameworks Parse Server (à la condition express de découpler les API REST servies du schéma de base de données et de les rendre conformes au cadre technique des API REST du Ministère) ou Nest.js. Leur utilisation reste assujéti car il est préférable de privilégier la simplicité d'Express qui est suffisante dans la plupart des applications WEB.

Il est de plus recommandé de réaliser les développements en Typescript qui apporte un typage statique permettant de renforcer la qualité et la robustesse du code face à des erreurs qui peuvent être détectées dès la compilation du code Typescript en Javascript plutôt qu'à l'exécution.

Règle	Énoncé	Statut	Portée
RT_DEV_14_1	Il est RECOMMANDÉ de réaliser les développements en Typescript plutôt que directement en Javascript.	R	Min Arm

Enfin, JQuery, dont seule la dernière version mineure de la série 4.0.0 (la dernière version mineure de la série 3 ne recevra désormais que les correctifs pour les failles et bugs critiques) est encore maintenue activement a vu les fonctions offertes reprises par les API Javascript des navigateurs ou par des microframeworks. Malgré les immenses services rendus par le passé, cette technologie est désormais sans réelle plus-value, en fin de vie et ne doit plus être utilisée. Les greffons ou frameworks qui l'utilisent doivent être identifiés et progressivement remplacés par des équivalents n'ayant pas d'adhérence avec JQuery. De plus, une version 4 étant désormais disponible, il est nécessaire d'effectuer la montée de version (impliquant des réécritures de code du système d'information concerné attendu que la version 4 contient des changements rompant la compatibilité ascendante), compte-tenu du fait que la 3 ne sera soutenue que pour « une période de temps limitée⁶⁷ ».

⁶⁶ <https://angular.dev/reference/releases#actively-supported-versions>

⁶⁷ <https://jquery.com/support/>

Document	Date	Origine	Type doc	Portée
Recommandations pour la mise en œuvre d'un site Web : maîtriser les standards de sécurité côté navigateur cf. 4.5 Sécurisation des COTS	28 avril 2021	ANSSI	Note technique	Toute admin.
Commentaire : Guide accessible sur le site MesServicesCyber de l'ANSSI.				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Framework de développement	JQuery	JQuery Foundation		★ / -	Min Arm
Framework de développement	Angular	Google (licence MIT)	Assujetti à la maintenance des applications déjà en production, aux projets réalisés par des équipes internes ou aux DSI aptes à assurer le MCO/MCS sur tout la durée du système d'information malgré le cycle de vie court de ce composant : 1 nouvelle version majeure tous les 6 mois avec un support de 18 mois pour les versions LTS.	A / -	Min Arm
Framework de développement	React	Meta (licence MIT)		R / -	Min Arm
Framework de développement	Next.js	Vercel (licence MIT)	Assujetti à la réalisation avec React de SI exposés sur Internet et pour lesquels l'optimisation du référencement par les moteurs de recherche (SEO) est un besoin métier majeur.	A / -	Min Arm
Framework de développement	Vue.js	Evan You (licence MIT)	Solution à privilégier pour les nouveaux projets	★ / -	Min Arm
Framework de développement	Nuxt.js	NuxtJS (licence MIT)	Version en fonction de la version Vue utilisée. Assujetti à la réalisation avec Vue.js de SI exposés sur Internet et pour lesquels l'optimisation du référencement par les moteurs de recherche (SEO) est un besoin métier majeur.	A / -	Min Arm
Framework de développement	Electron	OpenJS Foundation	Assujetti aux cas nécessitant impérativement le développement d'un client lourd et une capacité à réaliser un MCS très fréquent (au moins 2 fois par an).	A / -	Min Arm
Commentaire : le cycle de vie de la solution Electron est particulièrement court, ce qui va imposer a minima au projet une charge de MCO/MCS conséquente afin de la maintenir à jour et dans une version supportée. Avec une nouvelle version toutes les 8 à 10 semaines et un support de 6 mois, un nouveau package CNCI est donc à refaire au moins tous les 6 mois.					
Framework de développement	Express.js	OpenJS Foundation	Framework WEB pour développement Javascript	R / S	Min Arm
Framework de développement	Fastify	OpenJS Foundation	Framework WEB assujetti à des enjeux de performance ou de traitements complexes en mode asynchrone.	A / -	Min Arm
Framework de développement	Parse server	Parse-community (License BSD)	Framework complémentaire à Express. Assujetti à un développement d'application mobile pour faciliter la gestion des utilisateurs, la communication en temps réel par websockets et les notifications Push aux appareils mobiles.	A / -	Min Arm
Framework de développement	Nest.js	Open collective (Licence MIT)	Pour un développement backend métier important, plutôt que d'utiliser Express et un nombre conséquent de modules complémentaires dont la liste varierait d'un SI à l'autre, il est préférable de	A / -	Min Arm

			choisir un framework intégré et suffisamment complet pour réaliser un SI métier complexe entièrement en Javascript. Nest.js est le framework à privilégier dans ce cas d'usage. Il fonctionne avec Express ou Fastify et est agnostique au framework frontend. Il peut être utilisé avec Vue.js, React ou Angular.		
--	--	--	--	--	--

7.3.6 Réalisation d'applications mobiles

Le cadre relatif à la réalisation des applications mobiles identifie trois manières de réaliser des applications mobiles :

- Webapp en faisant appel à un navigateur ;
- Applications développées en natif ;
- Applications dites hybrides.

L'évolution technologique, et notamment les capacités actuelles des navigateurs et des protocoles sur lesquels ils reposent, incitent désormais à recommander fortement l'usage de « **progressive web apps** » (PWA)⁶⁸ pour la réalisation d'applications mobiles.

Les applications web progressives utilisent des API web modernes ainsi qu'une stratégie d'amélioration progressive pour créer des applications web multiplateformes qui fonctionnent partout et possèdent des fonctionnalités qui donnent aux utilisateurs les mêmes avantages que les applications natives, y compris pour un fonctionnement en mode déconnecté.

Les solutions développées en natif ou dites hybrides restent envisageables dès lors que l'approche PWA ne permet pas de répondre au besoin.

Lorsque l'accès aux SDK natifs est nécessaire, le framework Ionic associé à Capacitor ou Cordova et qui est compatible avec les frameworks Angular, React et Vue pourra être utilisé.

Règle	Énoncé	Statut	Portée
CCT_R14_1	Pour la réalisation d'applications mobiles, il est RECOMMANDÉ de privilégier un développement de Progressive Web Apps [PWA] plutôt qu'un développement en mode natif.	R	Min Arm

Document	Date	Origine	Type doc	Portée
Cadre technique relatif à la réalisation des applications mobiles au sein du ministère de la Défense , diffusé par note n°141 /DEF/DGSIC/DG/NP (Nemo n°2016/69)	3 mars 2016	DGSIC	Cadre technique	Min Arm
<i>Commentaire : ce document précise les conditions de réalisation technique des applications mobiles au sein du Ministère : il en définit les cas d'usage retenus, précise les règles techniques à respecter, et émet des préconisations en matière de choix technologiques.</i>				
Spécification d'interface SMOBI à l'attention des SI version 1.2 Cadre d'architecture et contraintes de configuration pour un système d'information accessible sur un terminal SMOBI Cf. 3.1.6 Mobilité [SU-AN, SU-ITN]	8 Décembre 2022	AND	Note technique	Intradef
<i>Commentaire : ce document constitue le cadre de cohérence technique pour les applications ayant vocation à être utilisées sur des terminaux SMOBI (PC Windows et smartphones/tablettes Android). Il s'adresse</i>				

⁶⁸ À noter que l'annonce de l'arrêt du support des PWA sur Firefox ne concerne que la version Desktop, et pas les versions sur Android qui, elles, continuent à fonctionner.

essentiellement aux directions d'applications (chefs de projets MOA et MOE internes ou externes). Il décrit les règles à respecter et les pratiques à éviter pour assurer le bon fonctionnement de ces applications en mobilité.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Framework de développement	Ionic	Licence MIT	Développement d'applications mobiles nécessitant un accès aux SDKs natifs.	A / -	Min Arm
Framework de développement	Capacitor		Développement d'applications s'appuyant sur Ionic	A / -	Min Arm
Framework de développement	Cordova		Développement d'applications s'appuyant sur Ionic	A / -	Min Arm

7.3.7 Développement à l'aide d'outils « low-code » ou « no-code »

Document	Date	Origine	Type doc	Portée
Directive n°49 encadrant l'emploi des solutions peu de code / sans code au Ministère des armées édition v1.0, diffusée par note n° 564/ARM/DGNUM/SDTN/NP	28/09/2023	DGNUM	Directive	Min Arm Hors projets sous IM 1618
<i>Commentaire : ce document a pour objet de fixer les règles d'emploi des solutions de Low Code / No Code au sein du Ministère des armées, en lien avec le cadre de cohérence technique et la gouvernance associée des projets de systèmes d'information. S'applique aux plates-formes qui ont vocation à mutualiser différentes expérimentations et applications ainsi que leur MCO/MCS sur une même solution.</i>				

Le *no-code* ou *low-code* consiste à développer des applications sans avoir besoin d'écrire de code (*no-code*) ou avec peu de code (*low-code*). Les outils *no-code* sont généralement pensés dès leur conception pour générer des applications sans avoir à écrire de code, alors que les outils *low-code* sont plus souvent des extensions d'outils existants, davantage orientés vers le monde de l'entreprise. Tous mettent en avant la simplicité avec laquelle il est possible de développer une application.

L'utilisation de tels produits permet de masquer la complexité technique en se focalisant sur la partie métier. Ces outils nécessitent des formations spécifiques à la solution utilisée mais permettent ensuite à un acteur fonctionnel d'être relativement autonome pour réaliser des cas d'usage peu complexes.

Ainsi, selon les objectifs et les besoins du projet il peut être pertinent d'utiliser un outil de type « *low-code* » ou « *no-code* » lors de la phase d'idéation ou de cadrage fonctionnel afin de réaliser des POC. Cela peut permettre de mieux inclure les acteurs métier dans la réalisation et de faire mûrir le besoin fonctionnel, dans le cadre d'une démarche centrée sur l'utilisateur.

Néanmoins, ces produits ne permettent pas toujours d'obtenir la maîtrise nécessaire de l'application ainsi créée. La structuration du code sous-jacent, son éclatement au sein des différents ateliers et son suivi en version, tous spécifiques, obèrent les capacités d'appropriation et de MCO par les équipes de développement du Ministère, mêmes formées sur ces produits. Aussi, même si les promesses de simplicité de l'approche *low-code* / *no-code* peuvent sembler tentantes, notamment du point de vue fonctionnel, ce mode de production des applications n'est pas adapté à tous les cas d'usage.

L'utilisation de ces outils est assujettie aux projets fonctionnellement très simples, aux POC et aux phases d'idéation sur une durée déterminée avant un passage à l'échelle hors d'outils *low-code* / *no-code*. De plus, lorsque les applications créées sont destinées à la production, le MCS de l'ensemble de la pile logicielle doit être assuré sur toute leur durée de vie.

Par conséquent, la réalisation d'une solution basée sur un outil de *low-code* / *no-code* est soumise à une vérification par l'AGORA Tech afin de garantir le MCO et le MCS sur toute la durée d'utilisation du produit. Le recours à des plateformes de *low-code* / *no code* pour des applications structurantes du ministère ou ayant un besoin de disponibilité supérieur à I2 est jugé risqué et

fortement déconseillé. Il est même interdit pour réaliser des applications critiques qui nécessitent une sécurité renforcée et une haute fiabilité.

Pour mémoire, il existe des services du socle numérique (Démarche Simplifiée, Tuleap) et des outils de développements référencés dans le présent CCT (Drupal WebForm, Jhipster, chaîne CI/CD et outillage PICSEL) qui permettent de mener rapidement des développements maîtrisables dans la durée.

Au-delà de ces considérations, la directive référencée ci-dessus énonce un certain nombre de règles de gouvernance des plates-formes et des développements, organisationnelles, de sécurité et techniques dont :

- Limiter aux expérimentations et aux applications non critiques de taille réduite, ne requérant pas plus qu'une disponibilité I2 et sans besoin de sécurité renforcée ou de haute fiabilité ;
- Calculer le retour sur investissement et élaborer un document de justification ;
- Conformité au [RGAA](#), ainsi qu'avec le CCT, quel que soit le type d'hébergement et recours à des frameworks standards si possible OpenSource ;
- Effectuer les échanges interapplicatifs via API Rest, utiliser des certificats IGCg NG ;
- Absence de développements spécifiques ;
- Mise en œuvre par du personnel formé maîtrisant la technologie ;
- Plate-forme distincte de celle de production pour les activités de développement ;
- Suivre une démarche d'homologation standard.

7.3.8 Autres langages

Document	Date	Origine	Type doc	Portée
Règles de programmation pour le développement sécurisé de logiciels en langage C v1.4	24/03/2022	ANSSI	Guide	Toute admin.
Commentaire : ce document est disponible en anglais sur le site MesServicesCyber de l'ANSSI (la version française étant la v1.2 plus ancienne).				
Shell Style guide	2025	Google	Guide	Min Arm
Commentaire : Faute d'un guide MinArm ou industriel, le développement de scripts shell bash devra suivre les règles de codage " Shell Style Guide " de Google. Le but est de réduire les mauvaises pratiques en matière d'écriture de script, et d'éviter les bugs courants en suivant un ensemble de règles de codage, et d'améliorer la maintenabilité générale de ces scripts. En complément de ce guide, il est fortement recommandé d'utiliser des outils d'analyse statique de code, un choix possible étant le logiciel opensource "shellcheck" (rpm disponible pour la distribution AlmaLinux : ShellCheck-0.6.0-3.el8.x86_64.rpm). D'autres règles de codage peuvent être utilisés : elles doivent à minima adresser toutes les problématiques exposées dans le Google "Shell Style guide"				
Règles de programmation pour le développement d'applications sécurisées en Rust v1.0	09/06/2020	ANSSI	Guide	Toute admin.
Commentaire : ce document est disponible sur le site MesServicesCyber .				

7.3.9 Sécurisation du code

Les données que traitent nos applications font l'objet de convoitises plus ou moins aiguës selon leur criticité ou l'intérêt qu'elles présentent, et le risque de vol d'informations ou de données sensibles est réel. La façon dont un programme informatique est conçu peut impacter sa disponibilité, compromettre l'intégrité et la confidentialité des données traitées, et ainsi engager la responsabilité pénale de son propriétaire, de son promoteur ou des équipes qui en ont assuré la conception et la réalisation.

Les mesures de sécurisation des réseaux et des serveurs ne sont pas absolues et la surface d'attaque représentée par un code mal conçu (cf. top 10 de l'OWASP⁶⁹) doit être considérée comme critique. La démarche de sécurisation du code doit en conséquence être pleinement intégrée au cycle de vie des applications, de leur conception à leur retrait de service. La robustesse du code doit être testée et vérifiée avant toute mise en production, ainsi qu'à chaque évolution.

Ces contrôles sont par exemple rendus disponibles dans la chaîne d'intégration continue de PICSEL.

La sécurisation du code ne doit pas être confondue avec la démarche, réglementairement obligatoire, d'homologation, pour laquelle il convient de se référer au § 4.2.1.

L'ensemble des acteurs impliqués, maîtrise d'ouvrage comme équipes de conception, réalisation et maintien en condition opérationnelle, doit comprendre les enjeux de cette démarche et mettre correctement en œuvre les recommandations en la matière, ou faciliter cette mise en œuvre : bonnes pratiques de codage (génériques et spécifiques aux technologies et langages employés), utilisation d'interfaces de programmation connues, documentées et soutenues, utilisation d'outils de vérification de qualité du code, etc.

Des travaux de veille et d'animation sur la robustesse du code sont réalisés par le CASID⁷⁰.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°40 portant sur le développement des applications informatiques et des logiciels robustes du ministère de la Défense [DIR DEV.SEC]	17/05/2017	DGSIC	Directive	Min Arm
<i>Commentaire : ce document présente un ensemble d'exigences et de règles permettant de réaliser au profit du Ministère des développements d'applications informatiques ou des logiciels robustes capables de fonctionner correctement en présence d'événements inattendus (valeurs hors normes ou mal formatées, etc.).</i>				

7.3.10 Développement à partir de grands modèle de langage (LLM)

Document	Date	Origine	Type doc	Portée
Guide de l'ANSSI portant sur les RECOMMANDATIONS DE SÉCURITÉ POUR UN SYSTÈME D'IA GÉNÉRATIVE version 1.0	29/04/2024	ANSSI	Guide	Tout
<i>Commentaire : Les projets intégrant de l'IA générative sont appelés à prendre connaissances et à appliquer le guide de l'ANSSI portant sur les recommandations de sécurité pour un système d'IA générative</i>				

Règle	Énoncé	Statut	Portée
CCT_R15_1	Pour la réalisation de développement à partir de modèle LLM, il est RECOMMANDE d'utiliser sur les modèles validés par l'AMIAD	R	Min Arm
CCT_R16_1	Pour la réalisation de développement à partir de modèle LLM, il est RECOMMANDE de s'appuyer sur les services d'IA génératifs en exploitation sur Intradef (GenIAI Intradef)	R	Intradef
CCT_R17_1	Dans le cas où les modèles validés par l'AMIAD ne remplissent pas le cas d'emploi du développement à réaliser, et dans le cas d'utilisation de modèles dont la provenance est hors MINARM, il est OBLIGATOIRE de vérifier a minima la provenance du modèle et l'applicabilité de la licence avec la direction des affaires juridiques du Ministère, la provenance du modèle (pays d'origine, industriel), la sécurité, les biais et	O	Min Arm

⁶⁹ Open web association security project (<http://owasp.org/www-chapter-france/>) : communauté, libre et ouverte à tous, travaillant sur la sécurité des applications web. Le « top ten » est un projet visant à lister les 10 risques de sécurité applicative les plus critiques. Ce classement fait référence et est aujourd'hui cité par de nombreuses organisations, dont certaines gouvernementales.

⁷⁰ Centre d'Appui aux Systèmes d'Information de la Défense

	les risques de contournement des mesures de sécurité et d'éthique (jailbreaking).		
--	---	--	--

7.4 Test et intégration (pré-intégration, intégration continue)

Dans sa version actuelle, ce paragraphe s'applique aux développements internes du Ministère et est fortement recommandé pour les développements réalisés à l'extérieur.

Dans un cadre professionnel, et d'autant plus au Ministère, tout développement implique la réalisation de tests logiciels automatisés. La démarche de cloudification renforce encore cet impératif en rendant tout système d'information qui n'en serait pas doté inapte à tirer un quelconque bénéfice des nouveaux environnements de développement (déploiement automatisé fiable et rapide notamment).

Ces tests automatisés s'organisent sous forme d'une pyramide :

- tests unitaires: ne testent qu'une seule fonction ou méthode, en isolation de tout composant externe à celle-ci ;
- tests d'intégration et d'API ;
- tests d'IHM, tests de bout en bout, tests fonctionnels ;
- tests de sécurité, de charge et tests métier.

Les premiers sont les nombreux, les plus simples, robustes et rapides à exécuter, les derniers sont les moins nombreux, les plus complexes, fragiles et lents à exécuter.

Ils doivent être intégrés et joués dans une chaîne d'intégration continue, typiquement celle de PICSEL.

Le développement dirigé par les tests (TDD ou Test Driven Development) et dirigé par le comportement (BDD ou Behaviour Driven Development) sont des pratiques fortement recommandées qui permettent d'améliorer significativement la qualité du code produit, son adéquation au besoin et de calibrer au juste besoin le nombre de tests à produire.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
BDD Testing	Cucumber	OpenSource		R / -	Min Arm
<i>Commentaire : le recours à Gherkin comme langage de spécification des tests constitue en la matière une bonne pratique.</i>					
TDD Testing	Cypress	Cypress.io		R / -	Min Arm
Automatisation de tests d'IHM	Selenium IDE	SeleniumHQ	Pour la production de scripts servant à la mesure des métriques associées à un scénario fonctionnel complet à travers une IHM Web.	R / -	Min Arm

7.4.1 Tests unitaires

Un test unitaire (ou de composants) vérifie le fonctionnement individuel de logiciels, modules, composants ou autres unités de code (classes, méthodes, programmes) testables séparément. Le test unitaire doit se faire de manière isolée du reste du système (en utilisant éventuellement des bouchons, pilotes et simulateurs).

7.4.2 Tests d'intégration des composants

L'intégration est un processus combinant des composants ou systèmes avec une interaction. Le terme intégration doit toujours être précisé. Il peut concerner entre autres :

- l'intégration de composants dans une application ;

- l'intégration d'une application dans son environnement ;
- l'intégration logiciel-matériel d'un SI dans son environnement physique.

7.4.3 Intégration continue

L'intégration continue est un ensemble de pratiques utilisées en génie logiciel consistant à vérifier à chaque modification de code que le résultat est conforme aux standards de développement et que les modifications ne produisent pas de régression dans l'application développée.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Intégration continue	PICSEL (Gitlab)	Min Arm	Outil retenu dans le cadre de la cloudification (PICSEL, C1DR et C1NP)	R / S	Min Arm
Intégration continue	Jenkins	Jenkins	Assujetti à des cas d'usages hors PICSEL	D / -	Min Arm
<i>Commentaire : Jenkins demeure un excellent outil, Gitlab lui a seulement été préféré à des fins de rationalisation des outils, car permettant de mutualiser plusieurs fonctions au sein d'un même service (CI/CD, gestion des dépôts git, gestion des tickets de développement, Wiki ...).</i>					

7.4.4 Tests de performance

Les tests de performance, de montée en charge peuvent être mis en œuvre par le BEEI⁷¹ (CND). Des travaux sont en cours pour intégrer ses infrastructures de test à l'environnement PICSEL afin d'alléger les opérations d'installation des systèmes d'information à tester et de bénéficier d'instances représentatives de services socle des environnements C1DR et C1NP.

Document	Date	Origine	Type doc	Portée
Offre de campagne de tests de performance : accompagnement, réalisation et analyse des résultats		CND	DIADEME	Min Arm
<i>Commentaire : Ce service accessible de DIADEME permet aux équipes projets (RCP, DADP) de réaliser des tests de performance de leur SI prioritairement de niveau DR, avec la possibilité éventuelle d'effectuer des simulations pour le niveau NP, sur un environnement dédié au plus proche de la production.</i>				

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Tests de charge	JMeter	Apache Software Foundation	Sollicitation intensive et parallélisée de services simples : • webservices ; • tests JUnit ; • méthode d'un bean managé ; • SQL ; • navigation simple dans une IHM Web.	R	Min Arm
<i>Commentaire : à utiliser uniquement sur un environnement dédié aux tests de charge</i>					
Tests de charge	Gatling	Gatling Corp	Tests de charge et de performance pour applications web (sous licence Apache 2.0). Disponible sur PICSEL.	R	Min Arm
<i>Commentaire : à utiliser uniquement sur un environnement dédié aux tests de charge</i>					

⁷¹ Bureau Expertise pour l'Évaluation et l'Intégration

7.5 Qualité logicielle

Dans sa version actuelle, ce paragraphe s'applique aux développements internes du Ministère et est fortement recommandé pour les développements réalisés à l'extérieur.

7.5.1 Qualité du code

La qualité logicielle est un ensemble d'indicateurs portant sur des critères multiples : qualité du code source, facilité de maintenance, qualité perçue, facilité d'apprentissage, etc.

Pour les logiciels, la qualité ne se mesure pas. C'est la non-qualité qui sert de base aux calculs des indicateurs. On mesure de fait le nombre de dysfonctionnements rencontrés impactant un des critères de qualité et le logiciel est considéré comme étant « de qualité » si ces dysfonctionnements ne dépassent pas un seuil fixé selon les attentes du projet ou du Ministère vis-à-vis de ce logiciel ou de cette typologie de développement.

Norme / Standard	Description / Utilisation / Restrictions	Statut	Portée
ASCRM V1.0 (OMG Document Number : formal/2016-01-03) (OMG Document Number : Formal/2016-01-04) (OMG document Number : formal/2016-01-02)	Automated Source Code Reliability Measure. Janvier 2016. Cette norme de l'OMG définit les éléments de mesure de la qualité interne du code dans le domaine de la fiabilité (disponibilité, tolérance aux pannes et capacité de récupération). https://www.omg.org/spec/ASCRM/1.0/PDF	R	Min Arm
ISO/IEC 25010:2023 édition 2	Ingénierie des systèmes et du logiciel — Exigences de qualité et évaluation des systèmes et du logiciel (SQuARE) — Modèles de qualité du produit	R	Min Arm
<i>Commentaire</i> : cette norme n'est disponible qu'en anglais: https://www.iso.org/fr/standard/78176.html			
ISO/IEC 5055:2021 édition 1	Nouvelle norme fournissant un ensemble de règles permettant d'évaluer les systèmes logiciels selon quatre facteurs : sécurité, fiabilité, maintenabilité et efficience. Réf : Téléchargeable ici .	R	Min Arm
CWE	Common Weakness Enumeration, liste des vulnérabilités logicielles maintenue par le MITRE (organisation à but non lucratif américaine). Réf : https://cwe.mitre.org	R	Min Arm
NIST Risk Management Framework	Ensemble de critères visant à sécuriser les systèmes informatiques du gouvernement américain. Réf : https://csrc.nist.gov/projects/risk-management/sp800-53-controls	R	Min Arm
<i>Commentaire</i> : le cadriciel Risk Management Framework (RMF) développé par la Joint Task Force offre un processus qui intègre des activités de gestion des risques de sécurité, de confidentialité, et de la chaîne logicielle durant le cycle de vie des logiciels en tenant compte les contraintes induites par les lois, directives, stratégies, standards ou règles applicables.			
OWASP top 10 2021	Liste des failles de sécurité les plus courantes et les plus exploitées. Réf : https://owasp.org/www-project-top-ten	R	Min Arm
<i>Commentaire</i> : 2025 est à date le dernier top 10 disponible. Il existe sur le site OWASP d'autres Top Ten d'intérêt (Kubernetes, Machine Learning, Large Language Model Applications, AI, API, mobile, CI/CD ...)			
Modèle qualimétrique du CISQ	Standard pour mesurer les critères de qualité des logiciels et les règles de développements à utiliser, développé par le Consortium for IT Software Quality. Réf : https://www.it-cisq.org/coding-rules/	R	Min Arm

Commentaire : les 5 dernières références sont mesurées par la plateforme CAST mise en œuvre par le CASID.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Qualité du code	CAST AIP	CAST SOFTWARE	Outil particulièrement adapté à l'évaluation du code des prestataires extérieurs ou aux opérations de transférabilité / réversibilité. A réserver en priorité aux SI structurants, selon arbitrage CND.	R / -	Min Arm
Commentaire : les principaux intégrateurs disposant de cette plateforme, il est opportun de prévoir dans les marchés la communication des résultats de l'analyse. La version souhaitable est celle du ministère afin de pouvoir effectuer éventuellement des mesures contradictoires en s'appuyant sur la norme ISO 5055. Il est recommandé de contrôler en continue la qualité du code avec SonarQube et de réserver les mesures avec CAST AIP aux livraisons majeures. CAST AIP nécessite un temps de traitement plus long mais offre des résultats plus poussés avec des mesures de remédiation qui peuvent être complétées par un plan d'amélioration et un accompagnement du CASID. .					
Qualité du code	SonarQube LTS	Open Source	PICSEL va proposer ce composant comme service horizon mi 2026 et intégrer progressivement ses mesures au rapport qualité préalable au déploiement en production des systèmes d'information.	R / S	Min Arm

7.5.2 Performance - Métrologie

La supervision permet de s'assurer du bon fonctionnement permanent d'un service ou d'une application en fonction d'indicateurs définis par le client. La métrologie de la performance ajoute la notion de mesures dans le but d'optimiser l'infrastructure d'hébergement, le code et les performances vis-à-vis de l'utilisateur final. Il est possible de faire appel au composant Observabilité déployé notamment sur PICSEL.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Performance-métrologie	Vmstat : Version fournie par le système d'exploitation	Open source	Pour l'observation ponctuelle d'un serveur. Limité aux systèmes Linux.	R	Min Arm
Performance-métrologie	sar – ksar :	Open source	Version fournie par le système d'exploitation Pour : • historiser l'activité de plusieurs serveurs ; • effectuer des mesures durant une campagne de tests ; • faire des comparaisons dans le temps. Limité aux systèmes Linux.	R	Min Arm
Performance-métrologie	perfmon	Microsoft	Version fournie par le système d'exploitation Même cas d'utilisation que sar et ksar mais pour un serveur Windows.	R	Min Arm
Performance-métrologie	XDebug	Open source	Mesure des performances des applications PHP https://xdebug.org/	R	Min Arm
Performance-métrologie	JavaMelody	Open Source	Composant logiciel open source, dédié au monitoring d'applications Java.	R	Min Arm
Performance-observabilité	EDOT	Open Source	Elastic Distributions of OpenTelemetry permettant d'instrumenter des systèmes d'information développés notamment dans les principaux langages utilisés et recommandés	R	Min Arm

			par le Ministère (Java, PHP, Javascript, Python, mais aussi .NET et les technologies Android, iOS ou .NET). https://www.elastic.co/docs/reference/opentelemetry		
--	--	--	--	--	--

7.6 Gestion des anomalies

Dans sa version actuelle, ce paragraphe s'applique aux développements internes du ministère et est fortement recommandé pour les développements réalisés à l'extérieur.

Les anomalies peuvent notamment être caractérisées par :

- des règles de gestion mal comprises ou interprétées ;
- de mauvais comportements ergonomiques ;
- des erreurs de charte graphique ;
- des erreurs de libellés ou d'affichage.

Niveaux de criticité

On distingue trois niveaux de criticité :

- MINEUR : les anomalies de ce niveau n'entravent pas le fonctionnement de l'application. Ce peut être par exemple des erreurs d'affichage, de libellé, de message ou d'affichage graphique ;
- MAJEUR : ces erreurs, plus graves, touchent le bon fonctionnement de l'application, par exemple une règle de gestion erronée sans toutefois bloquer la recette du produit ;
- CRITIQUE : ce sont les erreurs les plus graves, qui bloquent la recette du produit.

Cette définition de criticité permet :

- de donner un bilan global de la qualité de la livraison ;
- de pouvoir prioriser les corrections, et planifier le travail de correction.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestion d'anomalies	Tuleap	Tuleap		R / S	Intradef
<i>Commentaire : soutenu et exploité par le CASID</i>					
Gestion d'anomalies	Gitlab	Gitlab		R / S	Min Arm
<i>Commentaire : l'instance déployée sur PICSEL permet aux développeurs des projets qui y sont développés de suivre les anomalies logicielles à corriger, en lien avec le gestionnaire de code source. Des instances ad hoc peuvent également être déployées pour des usages spécifiques non couverts par des outils de socle qui y seraient déjà présents.</i>					
Gestion d'anomalies	DooNAF-Mantis Bug Tracker	DGA	Assujetti au contexte des programmes d'armement (DGA).	A / S (★)	Min Arm
<i>Commentaire : DooNAF est l'atelier d'ingénierie système (IS) mis à disposition par la DGA. Il regroupe un ensemble d'outils d'ingénierie système utilisés lors du déroulement d'une opération d'armement. Mantis Bug Tracker personnalisé pour la DGA fait partie de la suite d'outils soutenus sur le plan fonctionnel par la communauté IS et sur le plan système par le S2NA.</i>					
Gestion d'anomalies	JIRA	Atlassian		D	Tout intranet
<i>Commentaire : L'éditeur ATlassian abandonne progressivement le support de JIRA on premise jusqu'en 2029. Au delà, les données ne seront plus accessibles qu'en lecture. Cf le NeMO CND/GOUV STRAT/GOUV NUM n°2025/66 du 27/10/2025.</i>					

8 ANNEXES

8.1 Changements notables de la présente édition

8.1.1 Mise à jour et actualisation (hors pile logicielle)

Sujets transverses :

- Création du CND
- Création des AGORA
- Évolution de la gouvernance (Déclaration d'Engagement et Plateau d'Intégration)
- Passage en déconseillé des produits Atlassian (Confluence, Jira, Bitbucket) suite à l'abandon progressif de l'éditeur du support on premise
- Détails sur les services disponibles sur intrasan, ainsi que les briques recommandées
- Mise à jour des échéances
- SBOM à demander dans les CCTP
- Ajout de FranceConnect et mise à jour de ProConnect

Paragraphe 3 (Services communs)

- Ajout de Rust
- Ajout de Nuxeo
- Ajout de Prometheus
- Ajout de Fluentd
- Ajout de leaflet
- Web services INA : arrivée du service Personnes (équivalent d'User_Info dans Annudef)
- Web Analytic : Matomo recommandé sur Internet et retrait d'Eulerian
- Passage de MinIO en déconseillé
- Passage d'OnlyOffice en déconseillé suite à la décision de la DPID
- Mise à jour GDS
- Mise à jour route API

Paragraphe 5 (Infrastructure)

- Ajout de l'offre CaaStor

Paragraphe 7 (Conception – Développement)

- Retrait de Visio et Project. Ce retrait n'implique pas une interdiction de leur usage. Pour rappel, il convient de privilégier l'usage d'alternatives recommandées au CCT s'il y en a.

Paragraphe 8 (Annexes)

- Actualisation pile logicielle

8.1.2 Mise à jour et actualisation de la pile logicielle

Cf. 20260216_NP_Changelog_3.6.1-3.7.0.xlsx

8.2 Glossaire / liens utiles

Le Guide n°7 DGNUM – intégration de la sécurité numérique dans les projets comprend un glossaire portant sur les termes en matière de sécurité numérique.

8.3 Piles logicielles du développement sur PICSEL

À date, les principaux composants sont les suivants :

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Gestionnaire de version	Gitlab	Gitlab	Version entreprise	S	PICSEL
Intégration Continue	Gitlab	Gitlab	Gitlab-CI utilisé par des runners en zone projet PICSEL Version entreprise	S	PICSEL
Qualimétrie	SonarQube	SonarSource	Sonar dédié en zone projet PICSEL, intégré au Jenkins	S	PICSEL
Orchestration	Ansible Automation Platform	Red Hat		S	PICSEL
Sécurité	Vault Enterprise	Hashicorp	Version entreprise (composant Gestion Des Secrets)	S	PICSEL
Observabilité	Elastic	Elastic		S	PICSEL
Sécurité	MEDUSA	MinArm	Dépôts de binaires contrôlés (Artifactory et XRay)	S	PICSEL

8.4 Règles de nommage

8.4.1 Nommage des fichiers

Document	Date	Origine	Type doc	Portée
Directive DGNUM n°31, édition n°2 portant sur le nommage des fichiers numériques au MINARM	30 octobre 2023	DGNUM	Directive	MinArm
<i>Commentaire : règles relatives au nommage des fichiers émis en interne ou externe au ministère, archivés ou publiés. Exception : règles de nommage des fichiers relatifs à la procédure des marchés publics destinés à transiter par la place Chorus et qui sont régis par les règles du service des achats de l'État (SAE).</i>				

8.4.2 Annuaire - Identifiant unique - Adresse messagerie

Document	Date	Origine	Type doc	Portée
Directive de nommage des annuairescf. 3.3.4.1 Annuaires / référentiels	12 juin 2012	EMA	Note	MinArm
<i>Commentaire : mise en forme des informations d'annuaire et des adresses de messagerie électronique.</i>				
Schéma d'annuaire des Intranets de la Défense &cf. 3.3.4.1 Annuaires / référentiels	26 nov. 2012	SC²A	Référentiel	MinArm

8.4.3 Nommage DNS

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.016 « nommage DNS » Version 1.0	01/09/2022	DIRISI	Guide	MinArm

8.4.4 Nommage des serveurs

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.019 « nommage des serveurs » Version 2.0	01/10/2022	DIRISI	Guide	MinArm
<i>Commentaire : Cette directive donne des règles homogènes de nommage des serveurs, physiques et virtuels, du ministère des armées, de façon à en garantir l'unicité du nom. Elle concerne tous les nouveaux serveurs sur tous les intranets, ceux déjà en production ne sont pas concernés sauf dans un cadre d'uniformisation ou d'amélioration de l'exploitation. Dans le cadre du STC-IA, le nommage physique est reproduit comme nom de la ressource dans Active Directory. Trigrammes de SI : le nommage recourt à un trigramme définissant le système d'information concerné, la gestion des trigrammes de SI relève de cette directive (la gestion des trigrammes de sites relève de la directive DIRISI n°67).</i>				
Directive n°149 « nommage des configurations STC-IA v0.5 » Version 0.8	01/03/2015	DIRISI	Directive	SIA
<i>Commentaire : Afin d'identifier tous les sites logiques métropoles SIA du Ministère qui accueillent le socle technique commun SIA S-SF, ce document définit une procédure d'identification basée sur une clé primaire codée sur trois caractères, nommée trigramme de configuration SIA, en complément du trigramme de site physique d'hébergement. Ce trigramme de configuration SIA répond à un besoin de mise en place de règles particulières de nommage complémentaire au profit du Socle Technique Technique Commun InterArmée v0.5 (STC-IA v0.5), devenu depuis SIA S-SF dans une stratégie de déploiement de plusieurs configurations SIA sur un même site géographique d'hébergement.</i>				
EMO.GUI.R4.024 « nommage des serveurs projetables du SIA » Version 1.0	01/07/2023	DIRISI	Guide	SIA
<i>Commentaire : Le nommage de serveurs des configurations projetables du SIA est réalisé sur la base d'un trigramme de site établi conformément au guide EMO.GUI.R4.019. Ce guide a pour objectif de définir le nommage des serveurs des configurations projetables du SIA et fixe l'emploi unique du trigramme [SCZ] comme identifiant des serveurs du socle (hors serveurs SI métiers).</i>				

8.4.5 Nommage composants d'infrastructure de télécommunication

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°73 d'installation et de nommage des composants d'infrastructure de télécommunication version 4.1	01/09/2018	DIRISI	Directive	IntradeIntraced
<i>Commentaire : Cette directive bien qu'établie pour la durée de vie d'OGIT reste la référence pour le Ministère. Elle donne des règles homogènes de nommage de tous les équipements sous la responsabilité de la DIRISI (métropole, outremer et étranger) : zone technique, répartiteurs, baies, câblage, équipements actifs, terminaux, ... Cette directive précise aussi des règles de câblage des installations.</i>				

CARLA : La description des réseaux physiques locaux de niveau NP et DR (éléments de réseau, éléments de distribution, infrastructure bâtie...) est réalisée au travers de CARLA (Cartographie des Réseaux Locaux). Le système d'information CARLA permet d'avoir une gestion précise et rigoureuse de l'architecture filaire et optique d'un site (infrastructure de câblage courant faible, desserte des locaux) et de donner aux techniciens réseaux les moyens de répondre aux sollicitations multiples des utilisateurs dans des délais très courts, surtout en cas de panne d'une liaison.

Solution	Produit	Fournisseur	Utilisation / Restrictions	Statut	Portée
Référentiel	CARLA	DIRISI R3WEB	Gestion des données relatives aux infrastructures de télécommunication, réseaux locaux NP et DR.	R	IntradeIntraced

8.4.6 Nommage VLAN

Document	Date	Origine	Type doc	Portée
Guide EMO.GUI.R4.005 « Format des VLAN » Version 1.0	01/03/2022	DIRISI	Guide	MinArm
<i>Commentaire : à pour objet de définir et de permettre de contrôler l'utilisation des VLAN opérés par la DIRISI et mis en oeuvre pour les réseaux de desserte des sites du ministère des Armées (tous niveaux de classification en métropole, outremer, à l'étranger, en OPEX et sur les bâtiments de la Marine nationale) et de définir de manière normée la définition :</i> • <i>du périmètre d'utilisation des VLAN ;</i> • <i>du standard de nommage des VLAN ;</i> • <i>des principes d'attribution des ID VLAN ;</i> • <i>des principes de mise en relation de l'adressage réseau entre le 3ème octet d'adressage avec l'utilisation des VLAN ;</i> • <i>du processus des demandes de création de VLAN.</i> <i>Le nouveau système GARD (Gestion Automatisée des Réseaux des Datacenter) gère de façon automatisée les VLAN des Datacenters. Ce document ne s'applique donc pas aux Datacenters où GARD est mis en oeuvre.</i>				

8.4.7 Adressage IP

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°129 portant sur l'adressage IPV4 du ministère de la défense : version 2.1 diffusée par note n°922077/DEF/DIRISI/SCOE/EXP/NP du 7 mai 2014	7 mai 2014	DIRISI	Directive	MinArm
Directive DIRISI n°109 portant la politique de routage des flux IP sur l'IP DEFENSE : version 3.0	26 mai 2018	DIRISI	Directive	MinArm
<i>Commentaire : Ces directives présentent le plan d'adressage IPV4 global du ministère des armées ainsi que l'adressage et le routage VPN 2010. Elles s'appliquent à l'ensemble des organismes du ministère des armées. Ces directives référencent par ailleurs les principales références concernant les plans d'adressage IP relative aux divers réseaux et sous-réseaux du ministère des armées.</i>				
Directive DIRISI n°134 relative à l'adressage IPV4 des réseaux protégés : version 2.1 du 25 juin 2014	25 juin 2014	DIRISI	Directive	MinArmRéseaux Classifiés de défense
<i>Commentaire : Cette directive précise les éléments relatifs à l'adressage des équipements cautionnés (Chip, Netasq, Arkoon...) et des équipements relevant du classifié de défense (Echinops, TCE621, ...) en métropole, OME, etc. Mais elle ne traite pas des topologies (contextes et associations), et ne concerne ni les CHIP du RCDG (SOCRATE, RTRAN) ni RIFAN 2.</i>				

8.4.8 Marquage de la sensibilité des informations numériques

Document	Date	Origine	Type doc	Portée
Guide Marquage de la sensibilité des informations numériques diffusée par la note n°365ARM/DGNUM/DG du 3/10/2022	3/10/2022	DGNUM	guide	MinArm
<i>Commentaire : Le guide a pour objet de fournir à l'ensemble des utilisateurs et les directions applications du Ministère une sensibilisation avancée sur le marquage de la sensibilité des informations numériques des données. Le marquage de la sensibilité consiste en l'apposition d'un marqueur visuel compréhensible par une personne, sur une information ou un ensemble de données, structurées (notamment dans les bases de données) ou non (fichiers, le guide présente les différents niveaux de protection, et expose les principes à mettre en œuvre pour le marquage numérique de la sensibilité des données informations numériques au ministère des Armées, courriels, etc.)</i>				

8.5 Référentiels / Nomenclatures

8.5.1 Cartographie des services

Le Cadre Commun d'Urbanisation de l'État (CCU) élaboré par la DINUM propose une structuration de la couche infrastructure applicative (NRA : Nomenclature de Référence Applicative) et matérielle (NRI : Nomenclature de Référence Infrastructure).

Document	Date	Origine	Type doc	Portée
Cadre Commun d'Urbanisation de l'État V1.0 diffusé par lettre n°2012-SU-132 du 16 novembre 2012 Nomenclature de Référence Applicative [NRA] Nomenclature de Référence Infrastructure [NRI]	26 octobre 2012	SGMAP DINSIC	Référentiel	MinArm

Le ministère des armées s'est doté d'une cartographie des services communs des intranets plus détaillée.

Document	Date	Origine	Type doc	Portée
Cartographie des services communs des intranets de la défense diffusée par note n°489/DEF/DGSIC/SDAU/NPO du 22 septembre 2015 et D-15-005981/DEF/EMA/CPI/NP du 22 septembre 2015	22 sept. 2015	DGSIC - EMA/CPI	Référentiel	MinArm
<i>Commentaire : cette cartographie permet de classer et détailler les services des intranets.</i>				

8.5.2 Catalogue des OID

Paragraphe laissé vide.

8.5.3 Trigrammes de sites géographiques

Document	Date	Origine	Type doc	Portée
Guide EMO.GUI.R4.034 « Gestion des trigrammes de site du ministère des Armées » Version 1.0	1er octobre 2024	DIRISI	Guide	MinArm
<i>Commentaire : Ce guide remplace la Directive n°67 v1.3 du 16/06/2015 La directive décrit les modalités de gestion des trigrammes de sites géographiques utilisés accueillant des sites d'information et de communication (routeur, data center, équipements de commutation, système d'information...) voir les sites interconnectés avec ceux du ministère des armées. Point de contact : le POLE OPS RTD gère la liste et les demandes de nouveaux trigrammes. Ce guide ne concerne pas la gestion des trigrammes attribués aux SI (décrit dans le document EMO.GUI.R4.019), ni ceux correspondant aux trigrammes de configuration SIA (décrit dans la directive DIRISI DIR-149), ni ceux attribués aux Bases de Défense.</i>				
Référentiel des trigrammes de sites	-	DIRISI	Référentiel	MinArm

8.5.4 Mots clés d'attribution (MCA)

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°121 relative à la gestion de la liste unique des mots clés d'attribution (MCA) version 3.0 du 21 mars 2014	21 mars 2014	DIRISI	Directive	MinArm

8.6 Critères d'éligibilité des produits et solutions

8.6.1 Objectifs et contraintes

Le cadre de cohérence technique du ministère a pour objet d'établir et de maintenir dans la durée l'équilibre entre plusieurs besoins et contraintes qui s'opposent par nature. Citons par exemple :

- évolutions et innovations technologiques pouvant offrir un avantage opérationnel ou un gain de ressources ;
- souveraineté en matière de système d'information ;
- interopérabilité ;
- sécurité des systèmes d'information ;
- maîtrise du système d'information ;
- exploitabilité, passage à l'échelle ;
- rationalisation des choix technologiques du ministère.

Si une nouvelle technologie semble présenter des opportunités susceptibles d'apporter un avantage opérationnel ou un gain en ressources pour le Ministère, il est indispensable de s'assurer qu'elle offre un certain nombre de garanties avant de pouvoir l'adopter.

Le domaine de l'informatique évolue à un rythme extrêmement rapide qu'un organisme tel que le Ministère des armées, du fait de la taille de son système d'information et de ses ressources humaines ne peut suivre aveuglément.

Par exemple :

- est-elle pérenne ? L'histoire de l'informatique regorge d'exemples de technologies qui se sont avérées de fausses bonnes idées ou ont été rapidement supplantées par d'autres technologies répondant plus efficacement au besoin (applets Java, technologie Flash, WAP ...) ;
- garantit-elle la maîtrise du système d'information ? une technologie propriétaire ou exclusivement maintenue par un seul acteur est susceptible de mettre le ministère dans une situation de dépendance inacceptable (en terme de souveraineté, de sécurité ou de coût financier à assumer par la suite) ;
- est-elle mature ? Le monde de l'informatique évolue extrêmement rapidement et même si une innovation semble devoir s'imposer durablement, elle peut mettre un peu de temps avant de se stabiliser et de trouver une implémentation durable. Adopter trop vite une technologie peut donc présenter le risque de retenir une implémentation mort-née ;
- est-elle structurellement solide ? des solutions fonctionnellement intéressantes peuvent s'avérer fragiles: défaut de conception, code de mauvaise qualité provoquant des dysfonctionnements, des problèmes de performance, des failles de sécurité ou rendant très difficile ou coûteuse la montée de version ;
- est-elle maîtrisable par le ministère ? Le ministère doit mettre en œuvre et exploiter les technologies à l'aide des ressources, notamment humaines, dont il dispose. Son personnel doit pouvoir les maîtriser, ce qui implique des formations à programmer et un niveau de complexité adapté. En conséquence, il n'est pas envisageable de multiplier les technologies pour répondre à un même besoin. Ceci peut aussi conduire à estimer la réversibilité des solutions retenues et la capacité du Ministère à les reprendre à son compte.

8.6.2 Critères généraux d'appréciation

En déclinaison des orientations précitées, les demandes d'intégration de nouveaux produits ou solutions dans le CCT ou de dérogation sont appréciées au travers de critères dont les principaux sont donnés ci-après :

- **privilégier à iso-fonctionnalités** les produits et solutions sous licence libre, possiblement sans coût de licence associé ; dans tous les cas, il conviendra que le code source puisse être accessible à des fins d’audit ou faire l’objet d’une analyse de sécurité ;
- **fonctionnalités :**
 - pas de doublon fonctionnel avec un autre logiciel ou solution déjà présente au CCT (au-delà du besoin de maintenir des options alternatives quand cela est jugé nécessaire) ;
 - pas de doublon avec des services du réseau support (authentification, supervision applicative, statistiques de fréquentation, etc.) ;
 - pas de produit ou de solution offrant des fonctions de développement, d’exploitation ou d’exécution de code arbitraire à un utilisateur standard ;
- **support :**
 - gestion par une organisation ou un groupe de contributeurs actifs dont l’appartenance à une organisation ou l’éventail de profils offre des garanties suffisantes (sécurité, absence de monopole, politique suggérant la possibilité d’une mise en dépendance technologique et/ou financière voire un abandon, ...) ;
 - vitalité suffisante : l’activité est évaluée par exemple au nombre de livraisons de corrections et évolutions, à la date des dernières livraisons de code ou de sortie des dernières versions, à la rapidité de traitement des bugs et problèmes ;
 - adoption par un nombre suffisant d’acteurs permettant d’assurer une pérennité acceptable de l’écosystème ;
 - versions à durée de vie longue (par exemple versions dites LTS ou long term support) ou, à défaut, disposant d’une durée de support annoncée compatible avec les contraintes du ministère et les durées des projets de systèmes d’information ;
 - version stable : les versions Release Candidate (RC), beta ou alpha ne sont pas autorisées (ainsi que celle ayant recours à un composant en dépendance lui-même en version RC, beta ou alpha) ;
- **sécurité :**
 - nombre de vulnérabilités signalées, vitesse de traitement ;
 - fréquence des signalements ;
 - pas d’échange de données avec l’extérieur (vers des serveurs externes au Ministère, à des fins de statistiques ou de gestion des licences ou pour récupérer des ressources de type scripts javascript, polices de caractères, feuilles de style, images par exemple) ;
 - pas d’exécution de code à la volée ;
 - pas de fonctionnement en mode “boîte noire” (installation en image de VM, en conteneur ou en « fat jar » par exemple) ;
 - existence d’audits ou de certification ;
- **qualité :**
 - présence d’une documentation, si possible en français ;
 - qualité du code (évaluée via SonarQube ou CAST par le CASID par exemple) ;
- **capacité d’intégration** dans le système d’information du Ministère :
 - adéquation avec les orientations du Ministère (technologie web en client léger, présence d’API RESTful, authentification utilisation de MindefConnect pour l’authentification (voire Kerberos pour les réseaux autres que NP et DR), « API first », « secure by design » ...) ;
 - compétences internes disponibles ou pouvant être acquises par le personnel concerné dans des délais adaptés ;
 - compatibilité avec les infrastructures du Ministère (capacités d’hébergement, des infrastructures réseaux, des équipements de sécurité, des services du socle ...) ;
 - interopérabilité et réversibilité ;
 - capacité à communiquer avec les autres briques du système d’information ;
 - possibilité pour le ministère de reprendre ou de faire reprendre le MCO et le MCS (mise à disponibilité du code source immédiate ou possible, notamment) ;

- nombre de dépendances : les dépendances doivent également être inscrites au CCT et en nombre raisonnable (ce critère adresse également des préoccupations de support et de sécurité, voire de qualité).

8.6.3 Critères d'éligibilité pour des modules de CMS

Concernant les solutions de CMS (Content Management System), pour être éligible, un module doit vérifier, outre les exigences communes à tous les produits ou solutions (cf. ci-dessus § 8.6.2), les exigences spécifiques suivantes :

1. **Apport fonctionnel suffisant**: Pas de module dont l'apport fonctionnel est suffisamment minime pour ne pas justifier le recours à un module (exemple : si le module fait 3 lignes de code, la fonctionnalité peut être directement implémentée dans le site sans qu'il soit besoin d'un module) ;
2. **Support**
 - Gestion par une organisation (pour DRUPAL, elles sont désignées comme Drupal services provider) ou un groupe de contributeurs actifs dont l'appartenance à une organisation ou l'éventail de profils offre des garanties suffisantes ;
 - Non référencé en tant qu'Abandonware pour Joomla ;
3. **Sécurité**
 - Nombre de vulnérabilités signalées, vitesse de traitement, fréquence des signalements :
 - <https://www.drupal.org/security>
 - <https://extensions.joomla.org/vulnerable-extensions/about/>
 - Pour DRUPAL, couverture par la security advisory policy.
 - Pour wordpress :
 - <https://www.easyhoster.com/aide/choisir-plugin-wordpress>
 - <https://make.wordpress.org/plugins/>
 - <https://wpmarmite.com/installer-plugin-wordpress/>
4. **Qualité** : pas d'adhérence au noyau du CMS (i.e. pas de modification du noyau mais utilisation des API proposées par le framework du CMS)

8.7 Modèles d'architecture

8.7.1 Introduction aux modèles d'architecture

8.7.1.1 Qu'est-ce qu'un modèle d'architecture ?

Un modèle ou « pattern » est un modèle dont le but est de décrire une « bonne pratique » afin d'assurer la capitalisation et la diffusion des connaissances dans un domaine métier donné.

La description de « patterns » permettant de réutiliser des « bonnes pratiques » de conception pour réaliser un nouveau projet (dans le domaine du BTP) a été popularisé avec le livre « *A Pattern Language* » paru en 1977⁷².

⁷² A pattern language: towns, buildings, construction de Christopher Alexander, Sara Ishikawa, Murray Silverstein, 1977 (0-19-501919-9)

A Pattern Language

Towns · Buildings · Construction



Christopher Alexander

Sara Ishikawa · Murray Silverstein

WITH

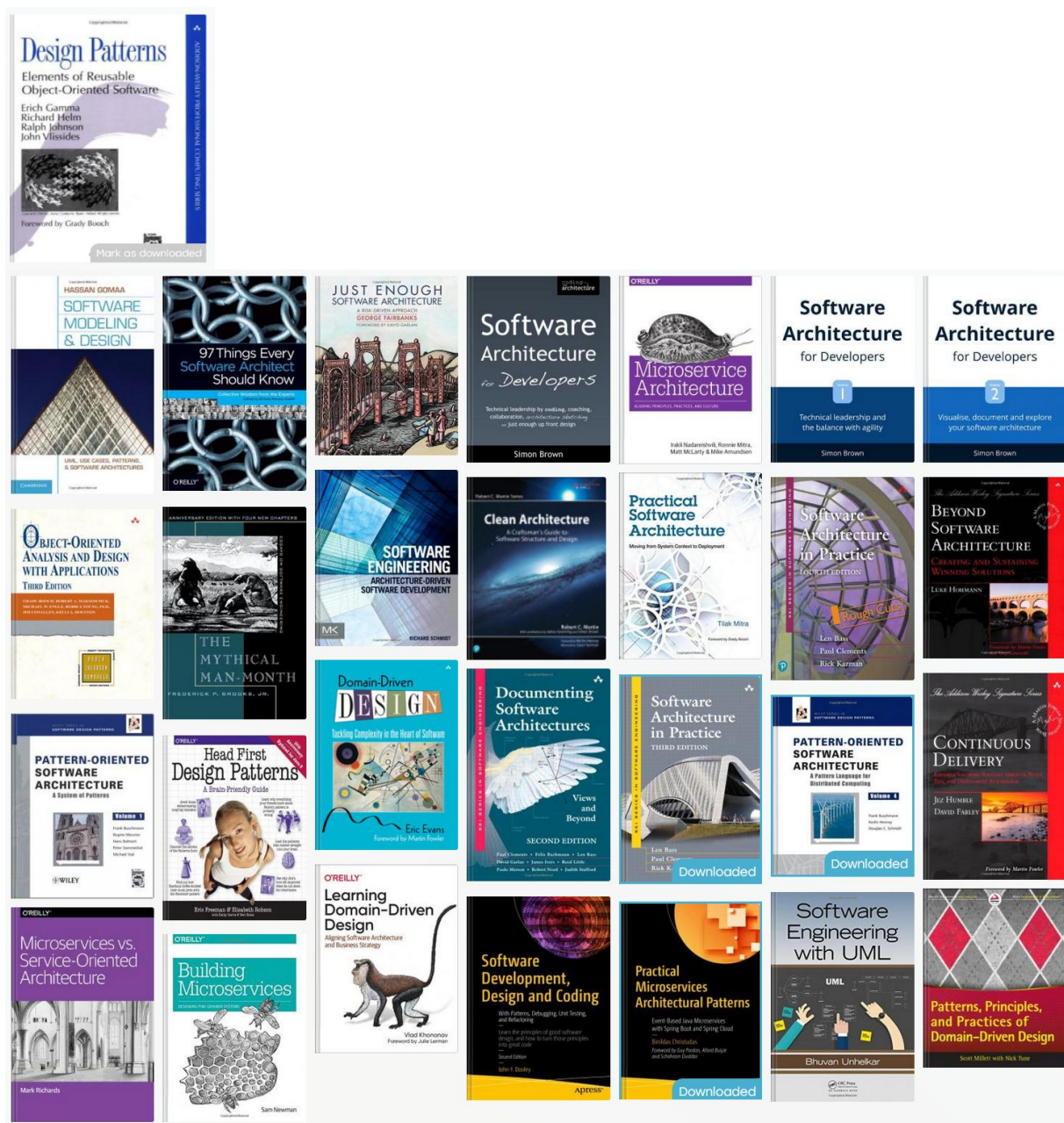
Max Jacobson · Ingrid Fiksdahl-King

Shlomo Angel

A Pattern Language

C'est le livre « Design Patterns » en 1994 qui a généralisé son usage en informatique avec des centaines de livres qui en proposent depuis cette date⁷³.

⁷³ Design Patterns, Elements of Reusable Object-Oriented Software, Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides



Un modèle d'architecture (terme utilisé dans cette annexe pour traduire « design pattern ») peut être décrit :

- **sous diverses formes** (par exemple sous forme de schéma, de texte descriptif, de spécification, de code spécifique, ...) ;
- **à différents niveaux de granularité** (par exemple le schéma général d'un système complexe, un couplage faible entre 2 SI, l'implémentation d'un proxy en Java, ...) ;
- **mais le but d'un modèle d'architecture, c'est d'avoir un modèle qui décrit la résolution d'un problème récurrent par une communauté d'experts, mis à disposition des non experts.**

Un modèle d'architecture pour le CCT ne décrit pas tous les détails des technologies du MinArm, mais des éléments clefs de conception qu'il faut connaître pour faire un bon usage du CCT.

Cette annexe traite des modèles d'Architecture Applicative et introduit les technologies ayant un statut « Recommandé » au CCT. Les nombreuses technologies ayant un statut « assujéti », « déconseillé », « interdit » ou « émergent » signalées dans le présent CCT ne figurent donc pas dans ces modèles d'architecture.

Le public visé : les RCP et architectes projets (juniors, nouveaux arrivants ou externes).

Pour approfondir le sujet des modèles d'architecture applicative et logicielle, parmi les nombreux livres qui traitent de cette question, la lecture des 5 tomes de « Pattern-oriented software architecture » aux éditions Wiley peut être recommandée :



Pattern Oriented Software Architecture

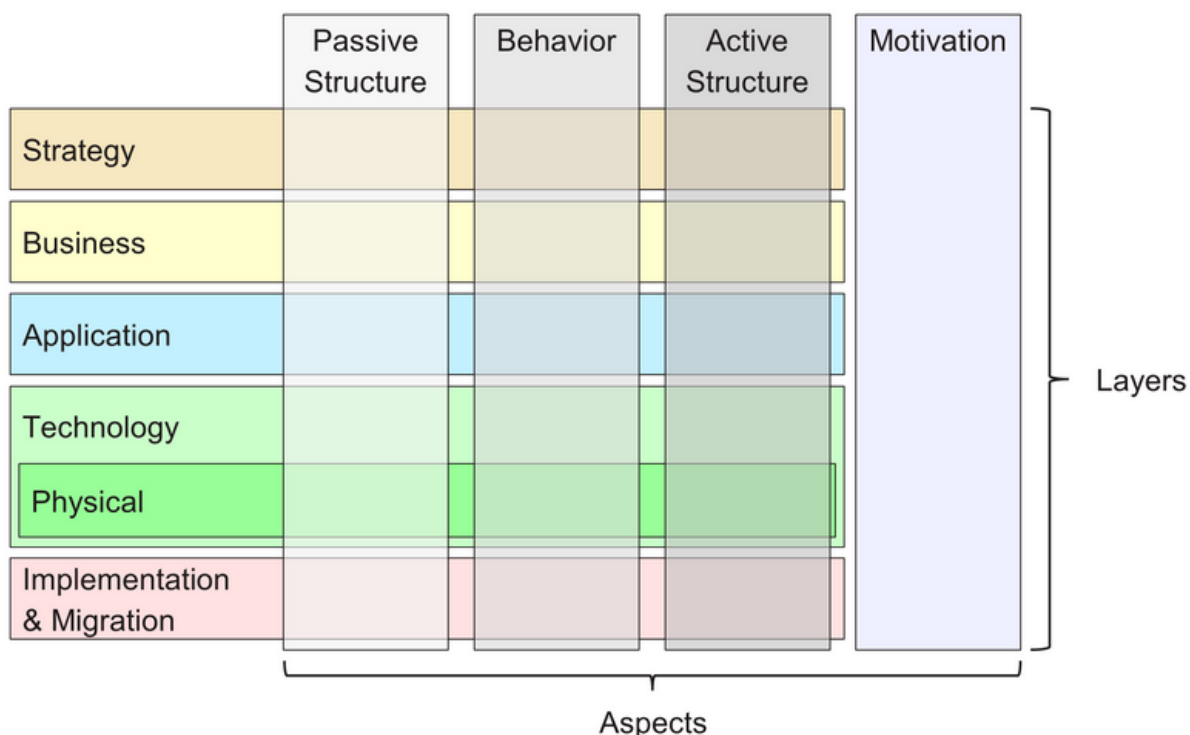
8.7.2 Modélisation des SI avec Archimate

8.7.2.1 Qu'est-ce que archimate ?

Archimate est un standard de l'Open Group qui est défini par une spécification (actuellement en version 3.2). Cette spécification décrit un langage et une notation graphique permettant de modéliser des systèmes d'information.

Ce langage introduit des concepts et des relations entre ces concepts dont la sémantique est précisée par un meta-modèle. Son utilisation pour modéliser un système donné utilise une notation graphique propre à Archimate.

Archimate permet de décrire un SI selon divers points de vue, de sa finalité stratégique à son implémentation. Dans les modèles d'architecture applicative, le focus est fait sur la couche « Application » et les technologies « recommandées » dans le CCT.



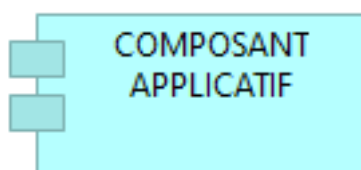
8.7.2.2 Les concepts Archimate utilisés pour les modèles d'architecture CCT

Archimate est un standard de description d'architecture essentiellement à destination des architectes. Or, le meta-modèle décrivant le point de vue applicatif dans Archimate introduit divers concepts qui ne sont pas tous indispensables pour décrire les modèles d'architecture d'intérêt pour le Ministère.

Ainsi, le choix a été fait de réduire le nombre de notations Archimate, dans le but d'en faciliter la compréhension par un responsable de conduite de projet (RCP).

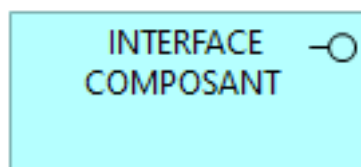
Par simplification, ne seront utilisés que les 4 concepts et notations suivants dans les modèles d'architecture.

Le composant applicatif :



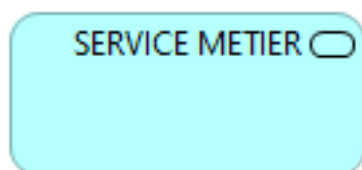
Composant Applicatif

L'interface de composant applicatif pour illustrer le principe de « boîte noire » (nommée en architecture *principe de « couplage faible »* ; ou en programmation *principe « d'encapsulation »*) qui indique que si un composant A appelle un composant B, il le fera via une interface du composant B. La réalisation (que l'on nomme « implémentation ») du composant B restant non visible du composant A (d'où l'appellation de « boîte noire ») :



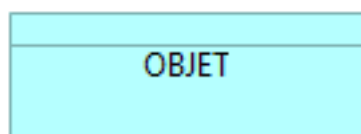
Composant Interface

Le **service** qui est une interface « publique » (c'est-à-dire visible de l'extérieur du SI) et qui permet à un composant B d'être appelé depuis un composant A qui est dans un autre SI :



Service Métier

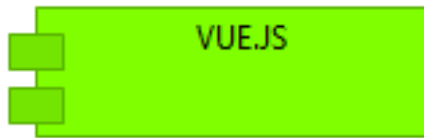
Les **objets** qui vont permettre la persistance des données du SI :



Objet

Pour introduire dans les modèles d'architecture les technologies ayant le statut de « recommandé » dans le CCT, également des concepts Archimate du point de vue technologique sont également utilisés.

A nouveau par souci de simplification, cette couche n'est pas reprise dans les modèles d'architecture applicatifs mais les services technologiques apparaissent en vert dans les schémas avec les notations du modèle applicatif (utilisation d'un composant pour un Framework plutôt que d'introduire une notation supplémentaire spécifique aux services technologiques). A titre d'illustration, le framework Vue.js qui est une technologie facilitant le développement d'application en Javascript sera représenté comme suit :

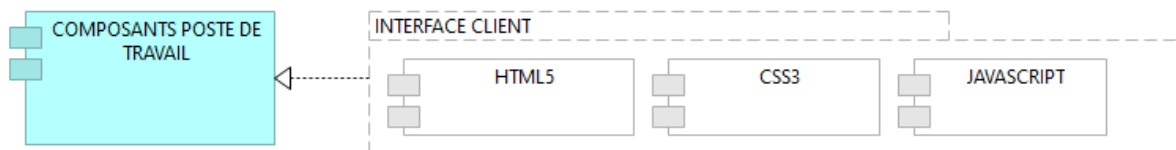


Framework VueJS

8.7.2.3 Les relations Archimate utilisées pour les modèles d'architecture CCT

Archimate définit 11 types de relation ; toujours par souci de simplification, seules 4 d'entre elles seront utilisées dans les modèles d'architecture.

La **réalisation** qui fait le lien entre un concept du modèle logique et sa réalisation par des technologies recommandées au CCT. Par exemple, est figuré ici que les composants qui s'exécutent sur un poste de travail sont *réalisés* avec les technologies HTML5, CSS3 et Javascript. Cet ensemble constitue ce qui est nommé une « interface client » :



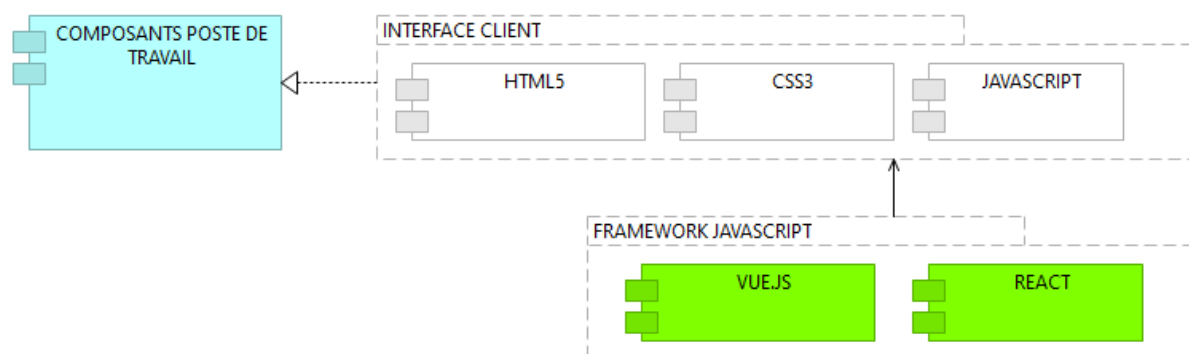
Réalisation

L'**association** est un lien structurel. Par exemple, est signifié ci-après que le framework Spring Boot s'utilise en association avec le framework Spring :



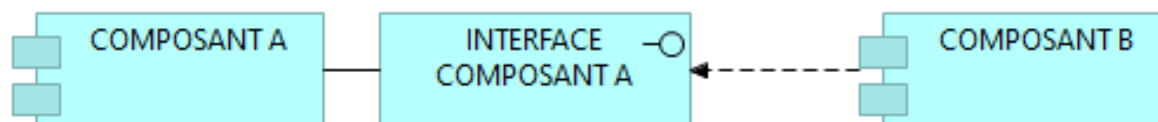
Association

Le **lien de service** montre les dépendances entre le code applicatif et les frameworks dont il dépend. Par exemple, pour réaliser le code d'une interface client, il est représenté ici qu'il est possible d'utiliser les framework javascript Vue.js ou React :



Lien Service

Le **lien dynamique** permet de montrer des flux de données lors de l'exécution de l'application et donc la logique de fonctionnement de l'architecture. Par exemple, à l'exécution, un composant applicatif B appelle une fonction d'un composant A via l'interface applicative associée :



Lien dynamique

8.7.3 Modèles d'architectures logiques de référence

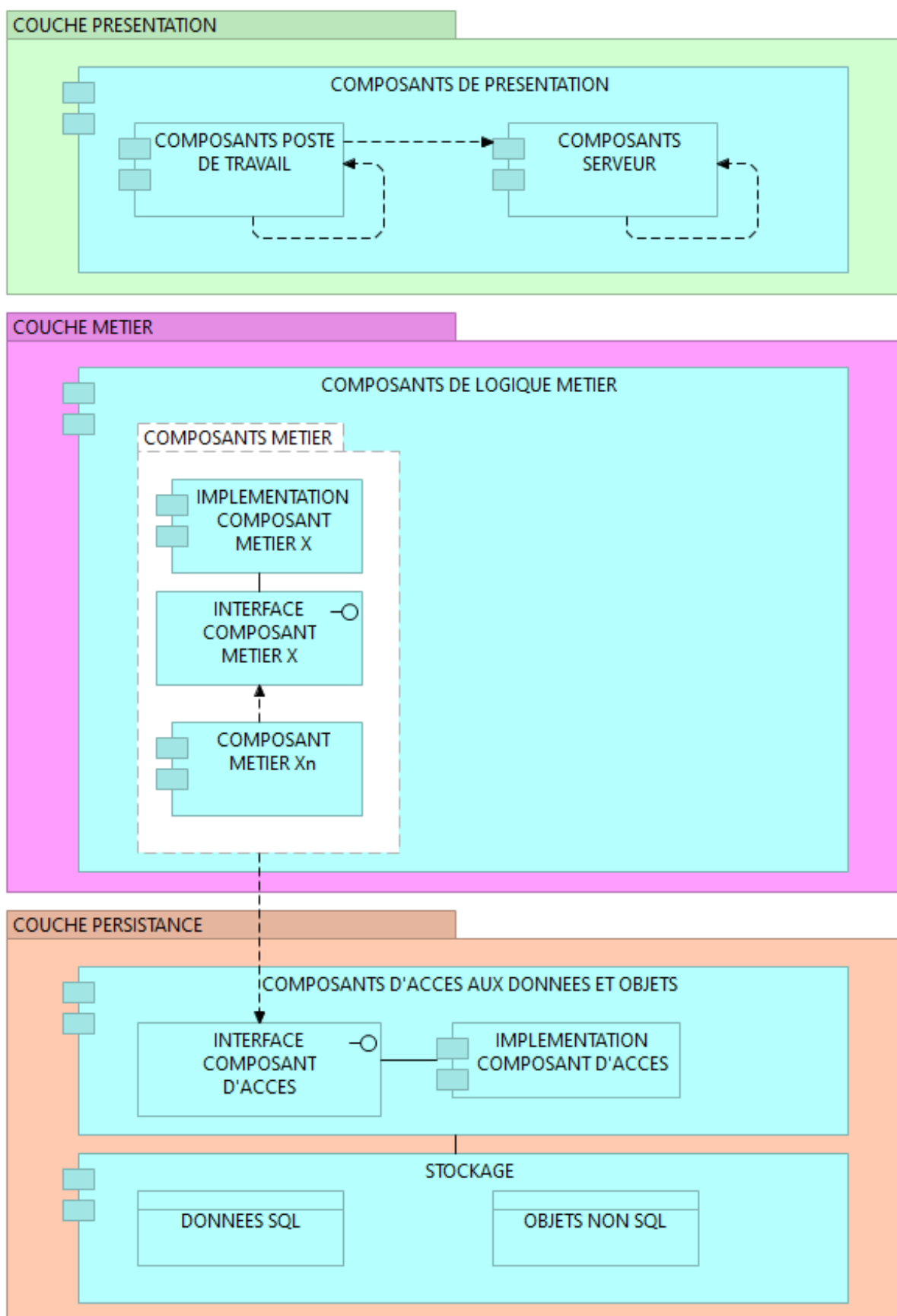
8.7.3.1 Définition et intérêt d'une architecture logique

Une architecture logique décrit une architecture applicative dont les éléments correspondent à une logique d'usage sans qu'il soit fait mention des technologies qui seront utilisées pour les implémenter, ce qui permet de décrire une logique commune pour toute architecture SI quelles que soient les technologies mises en œuvre pour un SI particulier. Ainsi, un SI réalisé en Java, PHP ou Javascript peut s'inscrire dans un modèle standard ayant une logique commune.

8.7.3.2 Modèle de référence

Ce modèle décrit un SI et son interopérabilité au travers de services de médiation conformément au principe de couplage faible dans une architecture orientée services (SOA). Au ministère des Armées, ce service de médiation est apporté par un composant « socle », la PEM (Plateforme d'Exposition et de Médiation). Le couplage faible induit permet de faire évoluer les composants associés à un service, indépendamment des clients de ce service, tant que l'interface de service reste inchangée, facilitant la maintenance et favorisant l'évolutivité globale.

Une architecture applicative se décrit précisément à l'aide de 5 couches. A des fins de simplification, seules les 3 suivantes seront utilisées pour les modèles d'architecture du CCT :



Architecture applicative

La « **couche de présentation** » représente la partie du SI qui gère les interfaces (généralement des écrans) avec lesquelles interagissent directement les utilisateurs (le terme « IHM » qui signifie « interfaces homme-machine » est également utilisé) ainsi que le contrôle de la cinématique d'enchaînement de ces écrans. Ce schéma logique permet à la fois une approche « client lourd » ou « client léger » ou les 2 à la fois dans le cas d'un « client léger » permettant un mode déconnecté. Dans une architecture « client lourd » (non recommandée), tous les composants nécessaires s'exécutent sur le poste de travail (« Composants poste de travail »). Dans une architecture « client léger », il s'établit un dialogue entre les composants qui s'exécutent sur le poste de travail (dans un navigateur) et des composants hébergés sur serveur (« Composants serveur »). Les composants serveur contrôlent la bonne logique d'enchaînement des pages, leur constitution et leur diffusion à destination du poste de travail pour affichage. Les flèches en pointillés sur le schéma représentent, de façon simplifiée, ces flux d'information entre composants. La flèche entre composant client et composant serveur illustre ce dialogue client-serveur. Une fois celui-ci instauré, le serveur transmet à son tour des flux à destination du poste de travail (qui ne figurent pas ici pour simplifier et souligner qui a l'initiative de ce dialogue).

La « **couche métier** » contient la logique métier du SI, traite les flux provenant de la « couche de présentation » et assure l'accès à la « couche de persistance » qui gère les données du SI. La couche métier illustre des aspects fondamentaux de l'architecture applicative : une architecture est un assemblage de composants, tout composant applicatif (« Implémentation composant métier X » sur le schéma) dispose d'une interface d'accès (interne au SI, donc privée et donc ni exposable, ni utilisable par un SI tiers) qui permet à un autre composant de ce même SI de l'invoquer (il est possible de gérer des niveaux plus fins à l'intérieur du SI pour préciser quels composants peuvent utiliser cet accès, mais ce niveau de précision n'est pas nécessaire pour les patterns présentés dans le CCT). Les technologies pour implémenter l'interface et le protocole d'appel à utiliser pour l'invoquer seront généralement spécifiques au langage choisi, mais la logique reste la même. Une application métier qui veut exposer des services (« Public API Service ») doit le faire avec un standard indépendant des langages de programmation. Le MinArm a choisi le standard « OpenAPI » qui requiert l'usage d'API selon le pattern REST. Chaque API doit être décrite dans un fichier « OpenAPI » que l'on nomme aussi fichier « swagger » (en respectant les règles de conception du MinArm et soumis à validation préalable du SAND), puis est publiée sur le service de médiation (PEM) pour pouvoir être invoquée par un autre SI. Ce service sert d'interface publique pour masquer l'appel du ou des composants métiers qui réalisent le service. C'est ce que montre le modèle complété ci-dessous.

Ce schéma montre également qu'un composant de la couche de présentation peut appeler un composant de la couche métier via son interface et que le bon usage d'un service de médiation ne concerne que le dialogue entre couches métiers de SI différents. Il est courant que les composants des couches de présentation et métier utilisent le même langage et dans ce cas le protocole d'appel est généralement lié au langage employé. Ceci implique que ces composants sont tous des composants « serveur ». Lorsque ce n'est pas le cas (par exemple dans le cas où la couche « présentation » est développée avec le framework Vue.js en javascript et s'exécute donc côté « client » dans un navigateur web et où la couche « métier » a été développée avec le framework Spring Boot en langage Java et s'exécute côté « serveur »), on utilise alors en général un protocole agnostique au langage tel que « https ». C'est aussi bien sur le cas entre composants exécutés sur le poste de travail et composants hébergés sur serveur de présentation. Le schéma montre également qu'un composant sur le poste de travail ne doit pas échanger directement avec un composant métier côté « serveur » afin que le dialogue reste toujours sous la supervision du contrôleur de l'application qui fait partie de la couche de présentation.

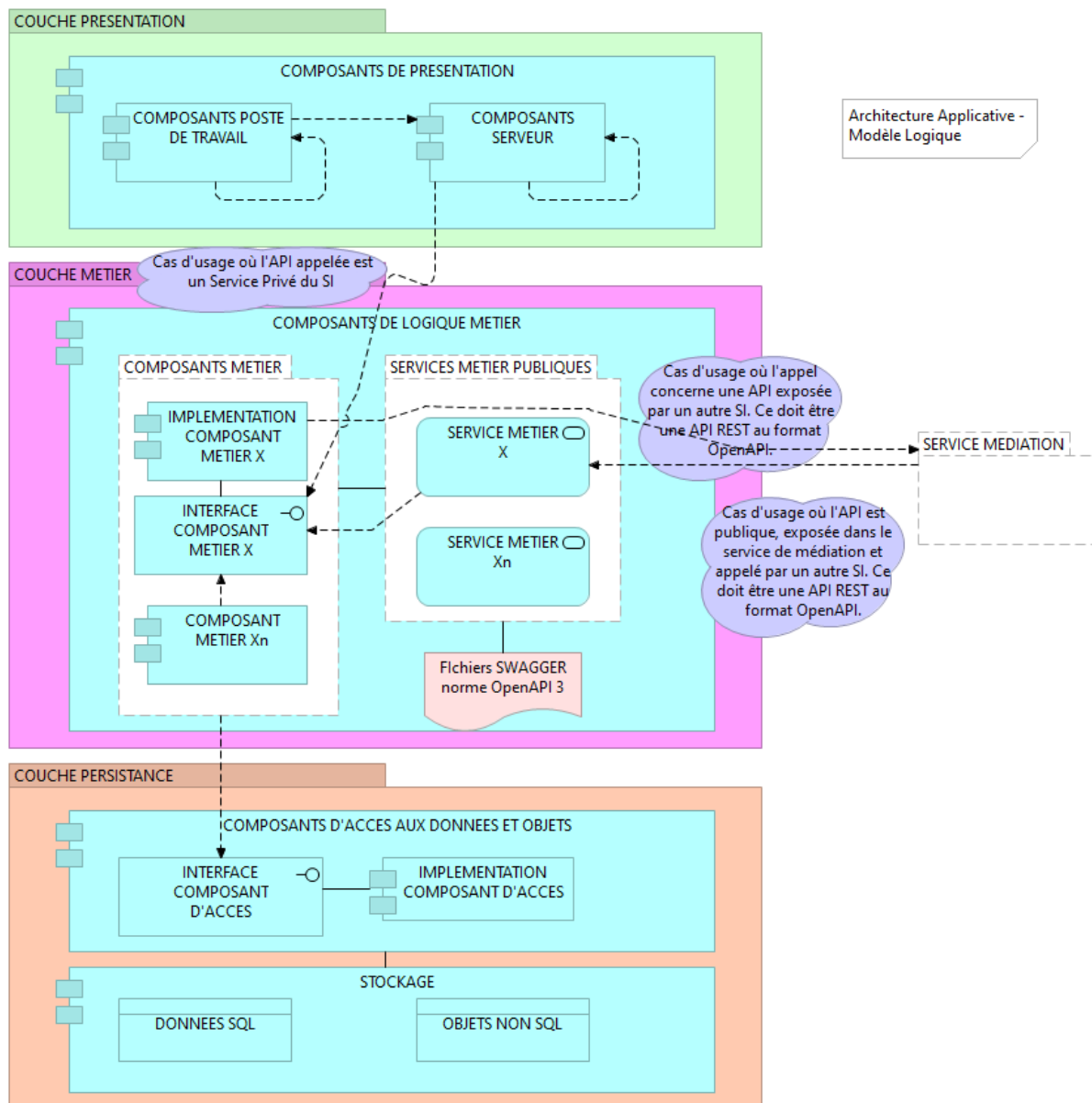
La « **couche de persistance** » contient les composants qui gèrent l'accès aux données (SQL et NO-SQL) avec les solutions qui en assurent le stockage telles que des systèmes de gestion des bases de données (ou d'**objets**). Un composant d'accès aux données est dit « de base » s'il ne contient que des fonctions d'accès de base aux données (fonctions appelées également « CRUD » pour « create », « read », « update » et « delete », termes qui se traduisent respectivement par « création », « lecture », mise à jour » et « suppression ») sans l'ajout de contrôles ou règles métier. À des fins de découplage, un composant d'accès va recourir à un intermédiaire (ou « proxy ») pour interagir avec la solution de stockage. Par exemple, un pilote de bases de données ou un framework assurant la correspondance

(nommé « mapping ») entre les données stockées au format relationnel dans la « base de données » et les objets manipulés par l'application (ces frameworks s'appellent des ORM).

Les interfaces des composants d'accès dans la couche de persistance peuvent également être implémentées par des API REST. C'est notamment le cas le plus usuel dans une architecture Javascript. Pour autant ces API REST, comme indiqué dans le schéma, ne doivent pas être exposées dans la PEM. Ce sont des API privées d'une application. La raison à cela étant que l'intégrité des données et des objets stockés en base de données requiert l'application de règles métier qui ne sont pas dans des composants « de base » mais dans des composants métier (qui eux, comme vu précédemment, sont potentiellement exposables dans la PEM en tant que services via des API REST).

Par conséquent, la création, la consultation, la mise-à-jour et la suppression de données ne peuvent être réalisées que par une seule application (plus précisément, par un composant métier unique appelé « service métier » dès lors qu'il est exposé via une interface publique), composant métier qui est généralement composé de plusieurs autres composants métiers de l'application et qui communiquent avec un ou plusieurs composants d'accès aux données.

La cohérence métier des données (appelée également « intégrité des données ») étant sous la responsabilité d'un service applicatif dédié, il est dès lors aisé de passer à un déploiement en mini ou micro-services (uniquement lorsque c'est pertinent de le faire, raison pour laquelle ces architectures restent « assujetties ») : en effet, la couche métier de l'application peut se découper selon ses services métier (chacun contenant ses composants métier et de persistance et étant responsables des données ou objets qu'ils gèrent) et chaque service peut être hébergé sur des serveurs virtuels ou containers différents selon les technologies d'hébergement adoptées.



Architecture applicative (modèle logique)

À noter que sont également utilisés les termes « frontend » pour la partie de l'architecture qui fait référence à la couche de présentation et « backend » pour la partie qui contient la couche métier et la couche de persistance.

8.7.4 Catalogue des modèles d'architecture applicatives

Les schémas suivants ont pour objet de montrer comment l'architecture applicative d'un SI peut être réalisée avec des langages de programmation spécifiques (Javascript ou PHP par exemple) en « client-léger » et comment réaliser un mode déconnecté. Les composants du schéma logique sont implémentés en utilisant des technologies recommandées décrites dans le CCT.

Les architectures présentées mettent en œuvre soit des solutions du marché, soit du code source pouvant provenir pour partie de frameworks logiciels. Le code couleur permet de les différencier :

- en blanc, les composants développés spécifiquement pour l'application ;

- en vert, le code réutilisé provenant d'un framework logiciel ou une solution logicielle ayant le statut « recommandé » au CCT.

Dans le schéma, les composants logiciels qui constituent l'application (codes sources plus les codes issus de frameworks) sont regroupés dans des rectangles blancs afin de les différencier des solutions logicielles qui offrent des « services techniques sur étagère » tels qu'un serveur d'application ou un système de gestion de bases de données.

8.7.4.1 Le modèle d'architecture PHP

Le modèle d'architecture pour des architectures développées en PHP met en évidence pour la couche de présentation que le code réalisé et exécuté sur le poste de travail (dans le navigateur) est développé en Javascript tandis que l'interface de présentation est décrite en HTML5/CSS3.

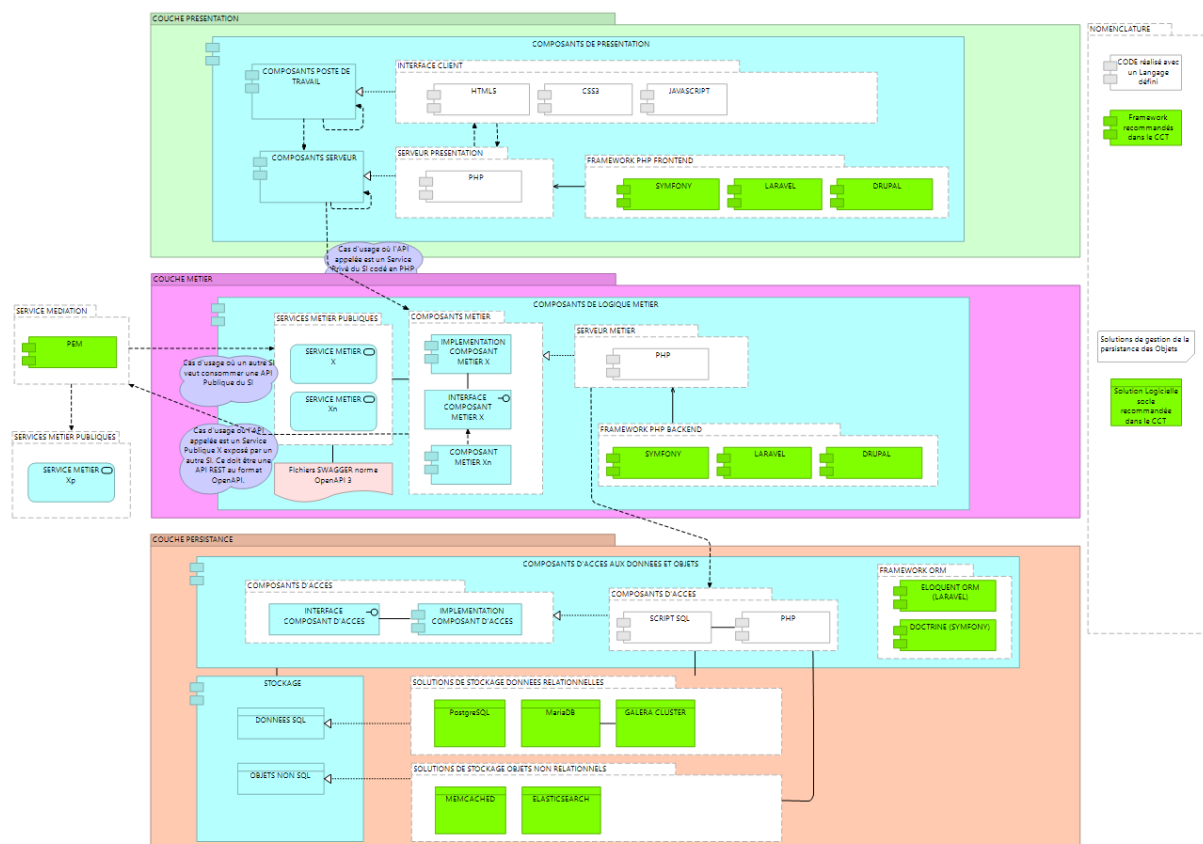
Côté serveur de présentation, le code est écrit en PHP avec, au choix, le framework Symfony, Laravel ou Drupal (idem pour le code de la couche métier).

L'accès aux données peut s'appuyer sur un ORM pour les framework Laravel et Symfony.

Les solutions de stockage relationnel recommandées et donc représentées ici sont PostgreSQL et MariaDB. Pour cette dernière, un cluster Galera est utilisable si besoin.

Le stockage non relationnel pour une mise en cache en mémoire peut être réalisé avec Memcached (stockage clef/valeur) ; celui recommandé pour stocker, indexer et rechercher de grandes quantités de données de manière rapide est Elasticsearch.

Il n'y a pas d'autres solutions recommandées pour le stockage non relationnel. Le CCT décrit plusieurs solutions utilisables mais qui sont assujetties à certains cas d'usage spécifiques.



Modèle d'architecture PHP

8.7.4.2 Le modèle d'architecture Javascript

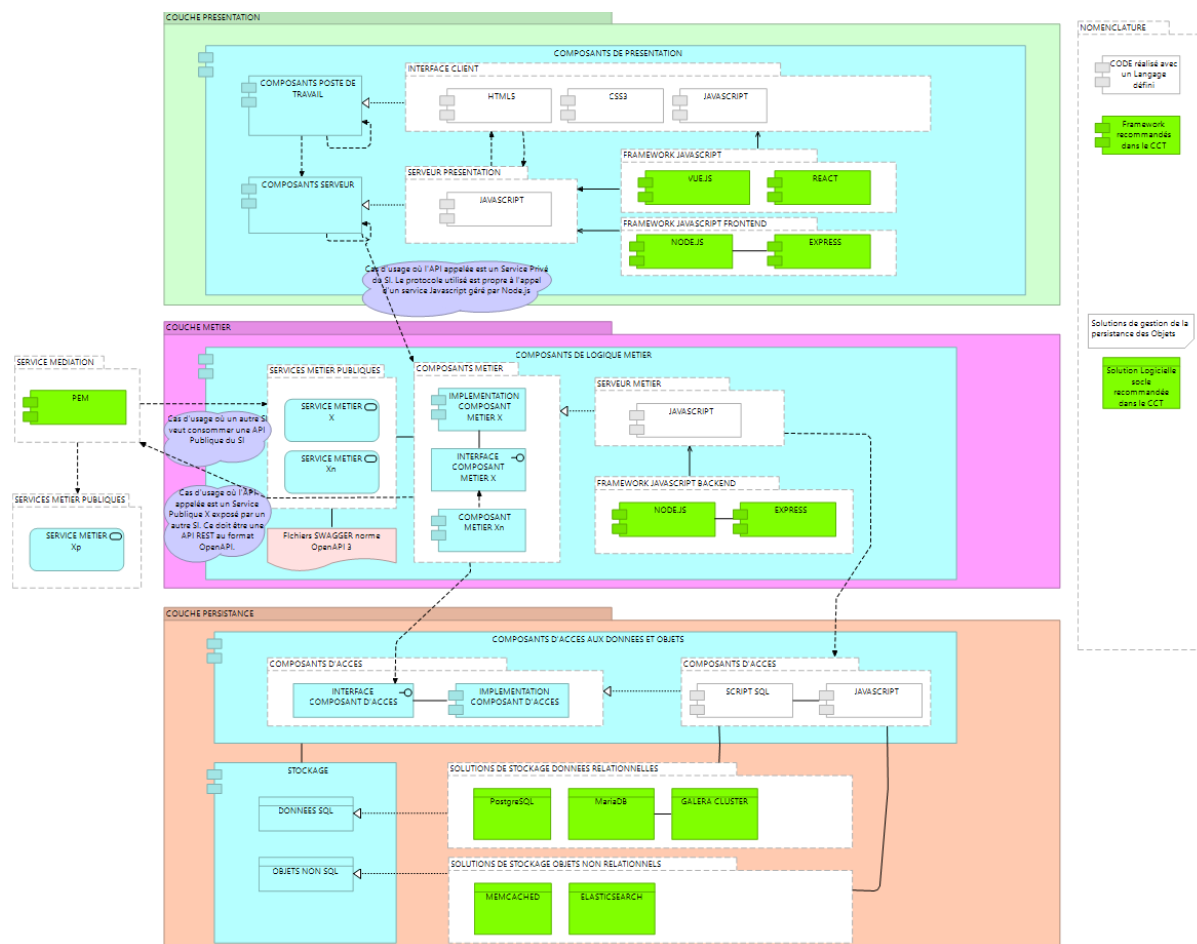
Le modèle d'architecture pour des architectures développées en Javascript met en évidence pour la couche de présentation, que le code réalisé et exécuté sur le poste de travail (dans le navigateur) est développé en Javascript tandis que l'interface de présentation est décrite en HTML5/CSS3. Le code est réalisé avec le framework Vue.js ou React.

Par défaut, Vue.js comme React sont des framework Javascript qui s'exécutent côté client, c'est-à-dire dans le navigateur web de l'utilisateur. Il n'est donc pas nécessaire d'utiliser Node.js ou Express.js pour les mettre en œuvre côté client, il suffit simplement d'inclure les fichiers Javascript de Vue.js ou de React dans les pages HTML et les exécuter dans le navigateur.

Cependant, du code doit être présent sur le serveur dès lors que qu'il est nécessaire de bénéficier de services qu'il doit exécuter pour effectuer le rendu des pages (SSR), pratique recommandée, ou plus systématiquement pour la gestion de l'authentification et des autorisations. Sur le serveur, le code est écrit en Javascript avec au choix, le framework Vue.js ou React. Le code utilise Node.js comme environnement d'exécution ainsi que le framework Express.

Il n'y a pas d'ORM recommandé pour l'accès aux données.

Les solutions de stockage sont les mêmes que celles utilisées pour PHP (cf. modèle d'architecture PHP ci-dessus).



Modèle d'architecture Javascript

8.7.4.3 Le modèle d'architecture Java

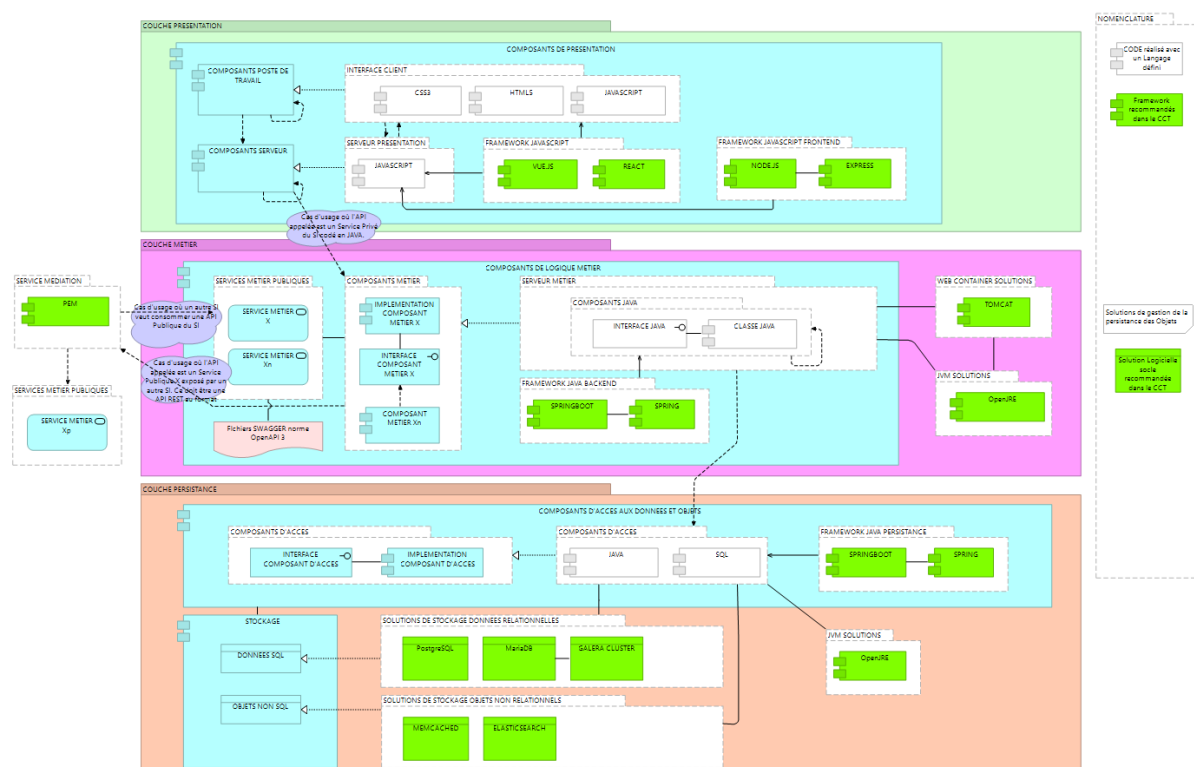
Le modèle d'architecture pour la couche de présentation des architectures développées en Java est similaire à celui du modèle d'architecture Javascript bien que les deux technologies soient parfaitement distinctes.

Le code de la couche métier utilise Spring Boot et les bibliothèques du Framework Spring. Le principal composant utilisé ici est Spring IoC qui fournit un conteneur responsable de la gestion des objets et de leurs cycles de vie. Il prend en charge l'injection de dépendances, la configuration des beans et la gestion des transactions.

L'accès aux données est également réalisé avec Spring Boot en utilisant le composant Spring Data qui offre un nombre important de possibilités pour des accès SQL et NoSQL. Spring Data offre de surcroît des accès pour Memcached et Elasticsearch. Les accès aux bases de données relationnelles peuvent recourir à Spring Data JDBC ou Spring Data JPA. Les solutions de stockage sont les mêmes que celles présentées pour PHP (cf. modèle d'architecture PHP ci-dessus).

A noter que cette architecture basée principalement sur Spring IoC et Spring Data n'a pas besoin d'un serveur d'application Jakarta EE, un simple Tomcat étant largement suffisant. Ceci a pour avantage de simplifier l'administration, l'exploitation et le MCS du SI en production. Tomcat et la machine virtuelle Java (OpenJRE) sont indiqués dans le schéma en dehors des regroupements « composants de logique métier » et « composants d'accès aux données et objets » car ils ne font pas partie de l'application elle-même. Ce sont des composants externes nécessaires à l'exécution du code Java.

L'architecture résultante est orientée API (la couche métier fournit des services à la couche de présentation en mode API REST) avec un frontend en Javascript et un backend en Java.

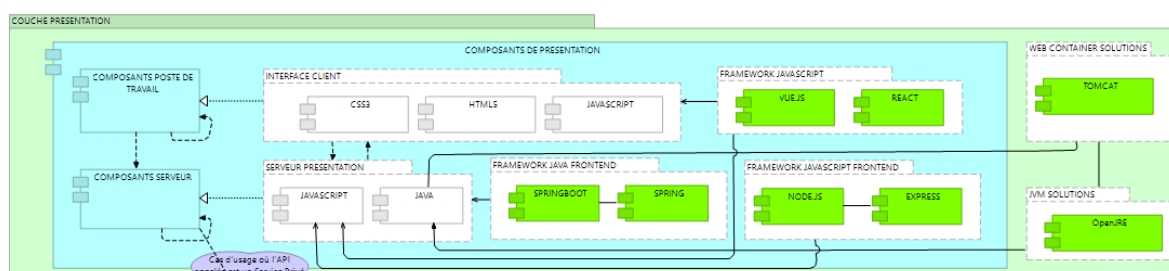


Modèle d'architecture applicative Javascript sur le Frontend et Java en Backend

Une architecture alternative pourrait consister à n'avoir que du code Java sur le serveur de présentation en utilisant les bibliothèques JSP ou JSF de Jakarta EE mais ce type d'architecture n'est plus recommandé. C'est néanmoins l'architecture de nombreux SI « historiques » du Ministère. Se pose alors la question de la façon de moderniser progressivement le frontend d'un tel SI pour le remettre en conformité.

8.7.4.4 Le modèle d'architecture de modernisation progressive d'un SI « historique » Java

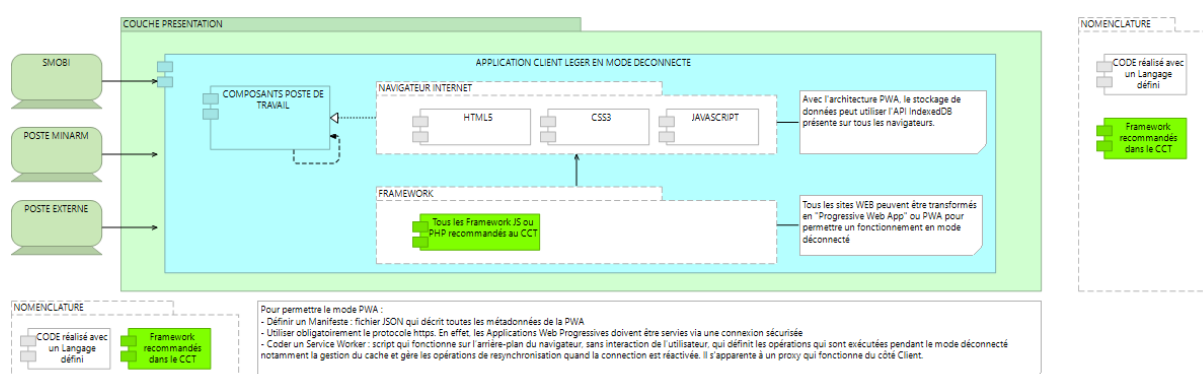
Spring MVC peut servir dans une stratégie de modernisation progressive d'un système d'information « historique » réalisé en JSP ou JSF. La première étape consiste à réaliser une migration technique vers Spring MVC (le principe général est « les vues sont conservées, le contrôleur est modernisé ») puis la couche de présentation est réécrite progressivement avec un Framework Javascript (tel que Vue.js) en faisant cohabiter les nouvelles pages avec les anciennes réalisées en Java, Spring Boot assurant la configuration de l'ensemble. Le framework Javascript assure le routage côté client et Spring MVC gère le routage côté serveur (plus précisément, Spring MVC assure la configuration des routes Vue.js ou React et un contrôleur Spring MVC gère les requêtes pour ces routes). Quand tout le frontend aura été réécrit, le code Java de la couche de présentation pourra être retiré et dès lors le système d'information sera devenu conforme au modèle d'architecture Java recommandé.



Modèle d'architecture applicative de transition permettant d'assurer la modernisation progressive d'un SI « historique » Java

8.7.4.5 Le modèle d'architecture « Client-léger » permettant un mode déconnecté

Pour disposer d'un mode déconnecté, l'architecture PWA⁷⁴ est recommandée. Ceci est réalisé en exploitant les fonctionnalités d'un navigateur internet supportant ce mode. Le modèle d'architecture ci-dessous décrit les éléments clefs de cette architecture. Les seules technologies recommandées dans le CCT pour la couche de présentation des applications en client-léger sont Javascript et PHP. Ces technologies permettent ce type d'architecture.



Modèle d'architecture « client-léger » permettant un mode déconnecté

⁷⁴ Une **progressive web app (PWA, application web progressive** en français) est une application web constituée de pages ou de sites web et qui peuvent se présenter à l'utilisateur de la même manière que les applications natives ou les applications mobiles. Ce type d'application tente de combiner les fonctionnalités offertes par la plupart des navigateurs modernes avec les avantages de l'expérience utilisateur offerte par les appareils mobiles.

8.8 Produits / Piles logicielles d'exécution

8.8.1 Modules pour CMS Drupal, Joomla ! et Wordpress

Les sites d'informations (CMS) peuvent recourir à des modules complémentaires pour étendre les fonctionnalités offertes. Ceci concerne notamment les CMS Drupal, Joomla ! et Wordpress.

Les modules retenus permettent de réaliser la majeure partie des fonctions liées à un CMS et répondent à une analyse au regard des critères d'éligibilité.

Voir l'annexe **8.6.3 Critères d'éligibilité pour des modules de CMS** pour les critères d'éligibilité des modules.

8.8.2 Pile logicielle : liste des produits

Cette annexe reprend et précise les choix de produits logiciels cités dans le présent CCT, notamment en terme de version.

Légende :

Reco SC2	Soutien
Recommandé	Soutenu
Emergent	Envisagé
Assujéti	Obsolascant
Deconseilla	Non soutnu
Interdit	-
-	

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Agent de messages	ActiveMQ	Apache Software Foundation	5.18	I	N	I	N	I	N	I	N	I	N	I				
Agent de messages	ActiveMQ	Apache Software Foundation	5.19	R	S	R	S	R	S	R	S	R	S	R				Compatible Java 11+
Agent de messages	ActiveMQ	Apache Software Foundation	6.0	I	N	I	N	I	N	I	N	I	N	I				
Agent de messages	ActiveMQ	Apache Software Foundation	6.1	R	S	R	S	R	S	R	S	R	S	R				Compatible Java 17+
Agent de messages	Kafka	Apache Software Foundation	3.6	I	N	I	N	I	N	I	N	I	N	I				Fin de vie : lors de la sortie de la 3.9
Agent de messages	Kafka	Apache Software Foundation	3.7	D	N	D	N	D	N	D	N	I	N	I				
Agent de messages	Kafka	Apache Software Foundation	3.8	D	O	D	O	D	O	D	O	I	N	D				Fin de vie : lors de la sortie de la 4.1
Agent de messages	Kafka	Apache Software Foundation	3.9	R	S	R	S	R	S	R	S	R	S	R				Fin de vie : lors de la sortie de la 4.2

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Agent de messages	Kafka	Apache Software Foundation	4.0	R	S	R	S	R	S	R	S	R	S	R				Fin de vie : lors de la sortie de la 4.3
Agent de messages	Kafka	Apache Software Foundation	4.1	R	S	R	S	R	S	R	S	R	S	R				
Agent de messages	Nats	Apache Software Foundation				A												Assujetti à un besoin d'agent de message pour conteneur
Agent de messages	RabbitMQ	Pivotal Software	3.12	I	N	I	N					I	N	I		22/02/24	31/12/24	
Agent de messages	RabbitMQ	Pivotal Software	3.13	D	O	I	N					D	O	D		18/09/24	31/12/27	Soutenu après accompagnement et assistance par premiers projets pour montée en compétence. Le support étendu est possible sous réserve d'acquittement d'une licence payante.
Agent de messages	RabbitMQ	Pivotal Software	4.0	D	O	D	O					D	O	D		15/04/25	30/09/27	Le support étendu est possible sous réserve d'acquittement d'une licence payante.
Agent de messages	RabbitMQ	Pivotal Software	4.1	D	O	D	O					D	O	D		15/04/25	30/04/28	Le support étendu est possible sous réserve d'acquittement d'une licence payante.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Agent de messages	RabbitMQ	Pivotal Software	4.2	R	S	R	S					R	S	R		31/07/26	30/10/28	Le support étendu est possible sous réserve d'acquittement d'une licence payante.
Analyse	Matomo			R	S	R	S					R	S					
Annuaire	Active Directory	Microsoft		R	S	R	S	R	S	R	S			R				Aligné sur le support des versions windows server
Annuaire	Meibo	Ilex						A	S	A	S							
Annuaire	OpenLDAP	OpenLDAP project	2	R	S	R	S	R	S	R	S	A	S	R				version 2.4 disponible dans les dépôts Alma 8.10, et .6 dans les dépôts Alma 9.x
Base de données NOSQL	ArangoDB	ArangoDB	3.11	I	N	I	N	I	N	I	N	I	N	I				BD multi-modèles (graphes, documents, clés-valeurs) open-source sous licence Apache. Version communautaire https://arangodb.com/subscriptions/end-of-life-notice/
Base de données NOSQL	ArangoDB	ArangoDB	3.12	A	N	A	N	A	N	A	N	I	N	A				BD multi-modèles (graphes, documents, clés-valeurs) open-source sous licence Apache. Version communautaire
Base de données NOSQL	Cassandra	Apache Software Foundation	3.11	I	N	I	N					I	N	I				

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Base de données NOSQL	Cassandra	Apache Software Foundation	4.0	D	O	I	N					I	N	D				Cas d'usage : Grands volumes de données et des besoins de bases distribuées hautement disponibles et décentralisées, sous réserve de prendre en compte les impacts réseau
Base de données NOSQL	Cassandra	Apache Software Foundation	4.1	D	O	I	N					I	N	D				Même status pour les versions 4.x hors 4.0.
Base de données NOSQL	Cassandra	Apache Software Foundation	5.0	A	S	A	S							A				Cas d'usage : Grands volumes de données et des besoins de bases distribuées hautement disponibles et décentralisées, sous réserve de prendre en compte les impacts réseau
Base de données NOSQL	Clickhouse	Yandex		A		A		A		A				A				

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Base de données NOSQL	CouchDB	Apache Software Foundation	3	A	N	A	N	A	N	A	N	I	N	A				CouchDB offre une réplication multi-master, ce qui signifie que plusieurs bases de données CouchDB peuvent se synchroniser entre elles de manière bidirectionnelle. Cela permet une grande tolérance aux pannes et la distribution des données sur plusieurs serveurs.
Base de données NOSQL	Elasticsearch	Elastic	6	I	N	I	N	I	N	I	N	I	N	I		09/08/22		
Base de données NOSQL	Elasticsearch	Elastic	7	D	O	D	O	D	O	D	O	I	N	D		15/01/26		Statut valable pour la 7.17. Les versions mineures précédentes (7.x) sont d'ores et déjà interdites.
Base de données NOSQL	Elasticsearch	Elastic	8.17	I	N	I	N	I	N	I	N	I	N	D				Les versions mineures précédentes (8.x) sont interdites. Le maintien de la 8.17 se terminera à la sortie de la 8.19. Il faut utiliser le JDK fournit pas la distribution linux plutôt que le JDK embarqué dans Elasticsearch. Elle est compatible OpenJDK 17 et 21.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Base de données NOSQL	Elasticsearch	Elastic	8.18	D	O	D	O	D	O	D	O	D	O	D				L'emploi de la version 8.19 est à privilégier. La 8.18 est supportée jusqu'à la sortie d'Elasticsearch 9.2. Il faut utiliser le JDK fournit pas la distribution linux plutôt que le JDK embarqué dans ElasticSearch. Elle est compatible OpenJDK 17 et 21.
Base de données NOSQL	Elasticsearch	Elastic	8.19	R	S	R	S	R	S	R	S	R	S	R				Future version LTS. Sera maintenue jusqu'à la version 10.0.0. Il conviendra de passer à cette version quand elle sera disponible. Il faut utiliser le JDK fournit pas la distribution linux plutôt que le JDK embarqué dans ElasticSearch. Elle est compatible OpenJDK 17 et 21.
Base de données NOSQL	Elasticsearch	Elastic	9	A	N	A	N	A	N	A	N			A				Version non recommandée. Cycle de vie rapide. Assujetti à la capacité à le maintenir en version.
Base de données NOSQL	MemCached	Danga Interactive	1.6	R	S	R	S					R	S	R				

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Base de données NOSQL	MongoDB	MongoDB, Inc	6.0	I	N	I	N					I	N	I		30/06/25		Préférer PostgreSQL, sauf quand ces fonctionnalités JSON ne répondent pas au besoin. Sur internet, il est interdit d'offrir des fonctionnalités de ce programme en tant que service.
Base de données NOSQL	MongoDB	MongoDB, Inc	7.0	A	S	A	S					A	S	A		31/08/26		Préférer PostgreSQL, sauf quand ces fonctionnalités JSON ne répondent pas au besoin. Sur internet, il est interdit d'offrir des fonctionnalités de ce programme en tant que service. Les versions mineures hors 7.0 sont interdites.
Base de données NOSQL	MongoDB	MongoDB, Inc	8.0	A	S	A	S					A	S	A				Préférer PostgreSQL, sauf quand ces fonctionnalités JSON ne répondent pas au besoin. Sur internet, il est interdit d'offrir des fonctionnalités de ce programme en tant que service. Les versions mineures hors 8.0 sont interdites.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Base de données NOSQL	Neo4J	Neo4j	2025	D	N	D	N					I	N	D				Base de type graphe . En version entreprise car la version communautaire n'a pas de gestion de privilège (un seul rôle d'admin) Version avec cycle de vie court.
Base de données NOSQL	Neo4J	Neo4j	4	I	N	I	N					I	N	I		29/06/25		Base de type graphe . En version entreprise car la version communautaire n'a pas de gestion de privilège (un seul rôle d'admin)
Base de données NOSQL	Neo4J	Neo4j	5.26	A	N	A	N					I	N	A				Base de type graphe . En version entreprise car la version communautaire n'a pas de gestion de privilège (un seul rôle d'admin) Les versions mineures précédentes (5.x) sont interdites.
Base de données NOSQL	OpenSearch	AWS	2	A	N	A	N	A	N	A	N			A				Alternative Elasticsearch
Base de données NOSQL	OpenSearch	AWS	3	A	N	A	N	A	N	A	N			A				Alternative Elasticsearch

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Base de données NOSQL	PouchDB	Apache Software Foundation	9	A		A		A		A		A		A				PouchDB est principalement utilisé pour le stockage de données côté client, ce qui signifie qu'il peut être utilisé pour stocker des données localement dans un navigateur web ou dans un environnement Node.js. PouchDB est conçu pour la réplication bidirectionnelle de données entre la base de données locale et une base de données distante. Cela permet de maintenir les données synchronisées entre différentes instances de l'application, même en cas de déconnexion.
Base de données NOSQL	Redis	Redis Labs	7.0	I	N	I	N					I	N	I				Sur internet, il est interdit d'offrir des fonctionnalités de ce programme en tant que service.
Base de données NOSQL	Redis	Redis Labs	7.2	D	O	D	O	D	O	D	O	I	N	D		28/02/26		Sur internet, il est interdit d'offrir des fonctionnalités de ce programme en tant que service.
Base de données NOSQL	Redis	Redis Labs	7.22	A	S	A	S					A	S	A				Sur internet, il est interdit d'offrir des fonctionnalités de ce programme en tant que service.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Base de données NOSQL	Redis	Redis Labs	7.4	A	S	A	S					A	S	A		30/11/26		Sur internet, il est interdit d'offrir des fonctionnalités de ce programme en tant que service.
Base de données NOSQL	Redis	Redis Labs	7.8	A	S	A	S					A	S	A		30/05/27		Sur internet, il est interdit d'offrir des fonctionnalités de ce programme en tant que service.
Base de données NOSQL	Solr	Apache Software Foundation	8	I	N	I	N					I	N	I				Les versions 8.10 et inférieures sont en fin de vie, et interdites. 8.11 : D/O. Elle peut encore recevoir des correctif de bugs critiques.
Base de données NOSQL	Solr	Apache Software Foundation	9	A	S	A	S					A	S	A				Cas d'usage : implémentation de moteurs de recherches évolués
Base de données orientée vecteurs	PgVector	PostgreSQL Global Development Group		A	S	A	S	A	S	A	S	A	S	A				Outils de recherche de similarités vectorielles pour postgresQL
BPM	Bonita	Bonitasoft	2024 (10.2)	D		D		D		D		D		D				Nécessite java 17. Compatible OIDC. Déconseillé parce qu'outils de low code, et du fait de la fréquence élevée des mises à jours.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
BPM	Camunda	Camunda	7.24	A	N	A	N	A	N	A	N			A		31/03/30	31/03/32	À n'utiliser que lorsque WebFlow et StateMachines pour les applications en java, ou Symfony-Workflow ou Laravel-Workflow pour les applications en PHP, ne peuvent être mises en œuvre. Le support étendu jusqu'en 2032 nécessite d'utiliser la version entreprise, payante.
BPM	Camunda	Camunda	8	A	N	A	N	A	N	A	N			A				À n'utiliser que lorsque WebFlow et StateMachines pour les applications en java, ou Symfony-Workflow ou Laravel-Workflow pour les applications en PHP, ne peuvent être mises en œuvre.
BPM	Flowable	Flowable	7	A	E	A	E							A				
Bureautique	7-zip	Igor Viktorovitch Pavlov	24	R		R		R		R		R		R				
Bureautique	Acrobat Reader	Adobe	2020	I		I		I		I		I		I		05/01/25		
Bureautique	Acrobat Reader	Adobe	25	R		R		R		R		R		R				
Bureautique	Libre Office	The Document Foundation	25.2	I		I						I		I		30/11/25		

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOps		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Bureautique	Libre Office	The Document Foundation	25.8	R		R						E		R		12/06/26		
Bureautique	Office	Microsoft	2007	I		I		I		I		I		I		08/10/12	09/10/17	Même statut pour les versions antérieures.
Bureautique	Office	Microsoft	2010	I		I		A		A		I				12/10/15	12/10/20	Assujetti : A la demande et aux
Bureautique	Office	Microsoft	2013	I		I		I		I		I		I		09/04/18	10/04/23	
Bureautique	Office	Microsoft	2016	R		R		D		D				R		12/10/20	13/10/25	
Bureautique	Office	Microsoft	2019	D		D		D		D						10/10/23	14/10/25	
Bureautique	Office	Microsoft	2024	R		R		R		R						09/10/29		
CI/CD	Gitlab		17	I	N	I	N	I	N	I	N			I				localement construites Version CE ou EE identiques sauf niveau de support
CI/CD	Gitlab		18	A	N	A	N	A	N	A	N			A				localement construites Version CE ou EE identiques sauf niveau de support
Communication instantanée	Jabber							A	E									Communication OTAN (Cf. WEBEX partie serveur)
Communication instantanée	JChat	OTAN		A		A		A		A				A				Assujetti au contexte : Interop OTAN / FrOps À utiliser avec le JRE Temurin.
Communication instantanée	Lync	Microsoft	2010	I		I		I		I		I		I		11/04/16	12/04/21	Cf Microsoft Office 2010

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Communication instantanée	Olvid			I		I						R		I				Interdit sur intradef, sauf à mettre en œuvre une instance homologuée, sur décision du COMCyber (NeMO N°2024/691 du 18/10/2024)
Communication instantanée	Prosody																	Assujetti au SIE
Communication instantanée	Skype for business	Microsoft	2016	D	O	D	O	R		R		I				12/10/20	13/10/25	ESU jusqu'au14/04/2026
Communication instantanée	Skype for business	Microsoft	2019	D	O	D	O									08/01/24	13/10/25	ESU jusqu'au14/04/2026
Communication instantanée	Skype for business	Microsoft	SE	R	S	R	S											
Communication instantanée	Tchap	DINUM										R						
Communication instantanée	Webconférence de l'État (Webconf)	DINUM																Service internet soutenu par la DINUM https://www.numerique.gouv.fr/outils-agents/webconference-etat/

[illegible]

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Décisionnel Agile / Analyse et visualisation	PowerBI Server	Microsoft		D	N	I	N	I	N	I	N	I	N	D				
Décisionnel Agile / Analyse et visualisation	QlikSense	QlikSense		A	N	A	N							A				Assujetti à l'impossibilité d'utiliser la plateforme ministérielle QlikSense.
Décisionnel Agile / Analyse et visualisation	Tableau	Tableau Software		D	N	I	N					I	N	D				
Décisionnel Analyse prédictive	Elasticsearch module machine learning	Elastic		A	S	A	S							A				
Décisionnel Analyse prédictive	POCEAD	MinArm		D	O	R	S							D				
Décisionnel Analyse prédictive	Predictive Analysis	SAP		D	O	I	N					I	N	D				

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Décisionnel Analyse prédictive	Suite SAS	SAS	9.4	D	O	I	N					I	N	D		01/02/28		La date de fin de vie n'est valable que pour la "Maintenance Release" 8. Les précédentes ne sont plus soutenues et sont donc interdites.
Décisionnel traditionnel	BO Lumira	SAP	2	D	O	I	N					I	N	D		30/11/25	30/11/27	
Décisionnel traditionnel	Business Object	SAP	4.2	I	N	I	N					I	N	I		30/11/22	30/11/24	
Décisionnel traditionnel	Business Object	SAP	4.3	D	O	I	N					I	N	D		30/11/25	30/11/27	Migration vers QlikSense à étudier.
Décisionnel traditionnel	Crystal Report	SAP	2016	D	O	I	N					I	N					
Décisionnel traditionnel	Fast Track	Bull		D	O									D				Il est recommandé d'utiliser le SI HERMOD.
Décisionnel traditionnel	HERMOD	MinArm		E	S													Infrastructure de mise en œuvre de la gestion de la donnée ; succède à la plateforme infocentre basée sur fastrack. Envisagé S2 2026.
Décisionnel traditionnel	Jaspersoft BI	Tibco		D	N	I	N					I	N	D				Édition Communautaire
Décisionnel traditionnel	Pentaho	Hitachi		D	N	I	N					I	N	D				Édition Communautaire

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Décisionnel traditionnel	SQL Server BI SSRS and SAAS	Microsoft		D	N	I	N					I	N	D				Outil de restitution et d'analyse des données (WEBI)
Déploiement	GLPI	Teclib	10.0	A	N	A	N					I	N	A				Uniquement pour les parcs non gérés par la DIRISI.
Déploiement	GLPI	Teclib	9.5	I	N	I	N					I	N	I		30/06/23		Uniquement pour les parcs non gérés par la DIRISI.
Déploiement	OCS Inventory	OCS Inventory Team	2	A	N	A	N	A		A		I	N	A				Assujetti aux cas d'usage S2NA
Déploiement / Distribution	Helm		3			A												Assujetti à Artemis.IA et domaine 3E
Déploiement / Distribution	MCM	Microsoft	2403	I	N	I	N	I	N	I	N			I		22/10/25		
Déploiement / Distribution	MCM	Microsoft	2409	D	O	D	O	D	O	D	O			D		06/06/26		
Déploiement / Distribution	MCM	Microsoft	2503	D	O	D	O	D	O	D	O			D		30/09/26		
Déploiement / Distribution	MCM	Microsoft	2509	R	S	R	S	R	S	R	S			R		12/05/27		
Déploiement / Distribution	ORCIDE	MinArm						A	S	A	S							Assujetti : aux configurations projetables du SIA sur théâtres et bâtiments
Distribution	RKE2	CNCF/SUSE	1.31	I	N	I	N	I	N	I	N			I		27/10/25		
Distribution	RKE2	CNCF/SUSE	1.32	D	N	D	N	D	N	D	N			D		28/02/26		
Distribution	RKE2	CNCF/SUSE	1.33	D	N	D	N	D	N	D	N			D		28/06/26		
Distribution	RKE2	CNCF/SUSE	1.34	A	N	A	N	A	N	A	N			A		27/10/26		

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
DNS	Bind	Internet Systems Consortium	9.16	I	N	I	N	I	N	I	N	I	N	I		30/04/24		
DNS	Bind	Internet Systems Consortium	9.18	D	O	D	O	D	O	D	O	I	N	D		30/04/26		
DNS	Bind	Internet Systems Consortium	9.20	R	S	R	S	R	S	R	S	I	N	R		30/04/28		
Échanges	GraphQL					A		A		A		A						Assujetti à des échanges internes au SI uniquement
Échanges	gRPC	Google				A		A		A		A						Assujetti à des échanges internes au SI uniquement
E-formation	ILIAS	Ilias	10	R	S	R	S	R	S	R	S	R	S			31/12/26	31/12/27	
E-formation	ILIAS	Ilias	8	I	N	I	N	I	N	I	N	I	N			31/12/24	31/12/25	
E-formation	ILIAS	Ilias	9	R	S	R	S	R	S	R	S	R	S			31/12/25	30/06/27	
E-formation	Moodle	Moodle HQ	4.4	I	N	I	N					I	N			20/04/25	07/12/25	Même status pour les versions antérieures
E-formation	Moodle	Moodle HQ	4.5	R	S	R	S					R	S			05/10/26	05/10/27	Version LTS
E-formation	Moodle	Moodle HQ	5.0	D	O	D	O					I	N			20/04/26	05/10/26	
E-formation	Moodle	Moodle HQ	5.1	D	O	D	O					I	N			05/10/26	05/04/27	
E-formation	Suite SCENARI	UTC		R	S	R	S					R	S					
Enquêtes et Sondages	Isidate	DGA		R	S	R	S											Sondage sur une date
Enquêtes et Sondages	LimeSurvey	LimeSurvey	5	I	N	I	N					I	N			31/05/23	31/05/24	remplace la 5.4 du dernier CCT (maj de sécurité)

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Enquêtes et Sondages	LimeSurvey	LimeSurvey	6	R	S	R	S					R	S					dernière version
Enquêtes et Sondages	Sherlock	SGA		R	S	R	S											
Environnement Java	Jakarta Enterprise Edition	Oracle	10	A		A		A		A		A		A				Version actuellement à privilégier pour le framework Jakarta EE mais reste assujetti car l'usage du Framework Spring reste la solution Java backend recommandée
Environnement Java	Jakarta Enterprise Edition	Oracle	7	I		I		I		I		I		I				Même status pour les versions antérieures
Environnement Java	Jakarta Enterprise Edition	Oracle	8	D		I		D		D		I		D				Uniquement pour des systèmes historiques en maintenance. Interdit pour un nouveau développement.
Environnement Java	Jakarta Enterprise Edition	Oracle	9.0	I		I		I		I		I		I				Version de transition, rapidement remplacée par la 9.1 pour un support de Java 11 LTS.
Environnement Java	Jakarta Enterprise Edition	Oracle	9.1	A		A		A		A		A		A				Version actuellement à privilégier pour le framework Jakarta EE mais reste assujetti car l'usage du Framework Spring reste la solution Java backend recommandée

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement	JDK	Oracle	11	I	N	I	N	I	N	I	N	I	N	I				
Environnement	JDK	Oracle	17	I	N	I	N	I	N	I	N	I	N	I				
Environnement	JDK	Oracle	21	D	N	D	N	D	N	D	N	D	N	D				Passage en interdit en septembre
Environnement Java	JDK	Oracle	24	I	N	I	N	I	N	I	N	I	N	I				Même statut pour les versions non-LTS, ie celles non inscrites au CCT.
Environnement	JDK	Oracle	25	A	S	A	S	A	S	A	S	A	S	A				
Environnement	JDK	Oracle	8	I	N	I	N	I	N	I	N	I	N	I		30/03/22	30/12/30	
Environnement	OpenJDK	Almalinux OS	11	D	O	D	O	D	O	D	O	I	N	D		31/10/24	31/10/27	Interdit sur des postes clients.
Environnement	OpenJDK	Almalinux OS	17	R	S	R	S	R	S	R	S	R	S	R		31/10/27		Interdit sur des postes clients.
Environnement	OpenJDK	Almalinux OS	21	R	S	R	S	R	S	R	S	R	S	R		31/12/29		Interdit sur des postes clients.
Environnement	OpenJDK	Almalinux OS	25	E	E	E	E	E	E	E	E	E	E	E		31/12/30		Interdit sur des postes clients.
Environnement	OpenJDK	Almalinux OS	8	D	O	D	O	D	O	D	O	I	N	D		30/11/26	31/12/30	Interdit sur des postes clients.
Environnement Java	OpenJDK	Eclipse Adoptium	11	A	S	A	S	A	S	A	S	A	S	A		30/10/27		Aussi appelé TemurinJDK (anciennement AdoptOpenJDK). Assujetti à l'usage sur windows, ou à la fin de vie de la version disponible dans les dépôts de la distribution linux Pour un usage client : Tout package bureautique doit utiliser Eclipse Adoptium (Temurin).

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement Java	OpenJDK	Eclipse Adoptium	17	A	S	A	S	A	S	A	S	A	S	A	S	30/10/27		Aussi appelé TemurinJDK (anciennement AdoptOpenJDK). Assujetti à l'usage sur windows, ou à la fin de vie de la version disponible dans les dépôts de la distribution linux Pour un usage client : Tout package bureautique doit utiliser Eclipse Adoptium (Temurin).
Environnement Java	OpenJDK	Eclipse Adoptium	21	A	S	A	S	A	S	A	S	A	S	A	S	29/09/31		Aussi appelé TemurinJDK (anciennement AdoptOpenJDK). Assujetti à l'usage sur windows Pour un usage client : Tout package bureautique doit utiliser Eclipse Adoptium (Temurin).
Environnement Java	OpenJDK	Eclipse Adoptium	24	I	N	I	N	I	N	I	N	I	N	I	N	30/09/25		Même statut pour les versions non-LTS, ie celles non inscrites au CCT.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement Java	OpenJDK	Eclipse Adoptium	25	A	S	A	S	A	S	A	S	A	S	A	S	30/09/31		Aussi appelé TemurinJDK (anciennement AdoptOpenJDK). Assujetti à l'usage sur windows Pour un usage client : Tout package bureautique doit utiliser Eclipse Adoptium (Temurin).
Environnement Java	OpenJDK	Eclipse Adoptium	8	A	S	A	S	A	S	A	S	A	S	A	S	01/01/30		Aussi appelé TemurinJDK (anciennement AdoptOpenJDK). Assujetti à l'usage sur windows, ou à la fin de vie de la version disponible dans les dépôts de la distribution linux Pour un usage client : Tout package bureautique doit utiliser Eclipse Adoptium (Temurin).

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement Java	OpenJDK	Oracle	11	D	O	D	O	D	O	D	O	I	N	D		29/09/23	30/01/32	Pour un usage serveur : nécessite donc une licence, ainsi qu'un environnement physique dédié à prévoir pour l'hébergement. Uniquement pour bénéficier du support d'un éditeur de solution refusant d'assurer le soutien sur une autre version binaire de ce JDK. Pour un usage client : nécessite également une licence payante. Les outils propriétaires doivent être désactivés ainsi que toute mise à jour automatique

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement Java	OpenJDK	Oracle	17	D	O	D	O	D	O	D	O	I	N	D		29/09/26	29/09/29	Pour un usage serveur : nécessite donc une licence, ainsi qu'un environnement physique dédié à prévoir pour l'hébergement. Uniquement pour bénéficier du support d'un éditeur de solution refusant d'assurer le soutien sur une autre version binaire de ce JDK. Pour un usage client : nécessite également une licence payante. Les outils propriétaires doivent être désactivés ainsi que toute mise à jour automatique

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement Java	OpenJDK	Oracle	21	A	S	A	S	A	S	A	S	I	N	A		30/09/28	30/09/31	Est disponible sous licence OTN gratuite jusqu'en septembre 2026. Au delà, il faudra avoir basculer en version 25, ou souscrire à une licence payante. (Cf commentaire java 17) Assujetti à une feuille de route de migration vers une autre distribution, vers le JRE Oracle 25, ou à la prise en compte du besoin d'achat de licence, voire de serveur physique selon le cas d'usage.
Environnement Java	OpenJDK	Oracle	24	I	N	I	N	I	N	I	N	I	N	I				Même statut pour les versions non-LTS, ie celles non inscrites au CCT.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement Java	OpenJDK	Oracle	25	A	S	A	S	A	S	A	S	I	N	A		30/09/30	30/09/33	Est disponible sous licence OTN gratuite jusqu'à un an après la sortie de la prochaine version LT, donc jusqu'à septembre 2028. Au delà, il faudra avoir basculer en version 29, ou souscrire à une licence payante. (Cf commentaire java 17) Assujetti à l'impossibilité d'utiliser un Temurin sur les postes windows, ou la distribution portée par Alma ou RHEL côté serveur.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement Java	OpenJDK	Oracle	8	D	O	D	O	D	O	D	O	I	N	D		30/03/22	30/12/30	Cette version LTS a un support exceptionnel de 16 ans du fait de l'étendue du parc logiciel qui utilise cette version. Composant soumis à licence (pour le MCS et le support) Pour un usage serveur : nécessite donc une licence, ainsi qu'un environnement physique dédié à prévoir pour l'hébergement. Uniquement pour bénéficier du support d'un éditeur de solution refusant d'assurer le soutien sur une autre version binaire de ce JDK. Pour un usage client : nécessite également une licence payante. Les outils propriétaires doivent être désactivés ainsi que toute mise à jour automatique
Environnement Java	OpenJDK	Redhat	11	I	N	I	N	I	N	I	N	I	N	I		31/10/24	31/10/27	Nécessiterait une souscription payante, en plus de celle pour l'utilisation de RHEL. Interdit sur des postes clients.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement Java	OpenJDK	Redhat	17	R	S	R	S	R	S	R	S	R	S	R		31/10/27		Le support étendu nécessite une souscription payante, en plus de celle pour l'utilisation de RHEL. Interdit sur des postes clients. Si l'usage de cette version est acceptable, il convient néanmoins de privilégier l'usage de la v21 chaque fois que possible.
Environnement Java	OpenJDK	Redhat	21	R	S	R	S	R	S	R	S	R	S	R		31/12/29		Le support étendu nécessite une souscription payante, en plus de celle pour l'utilisation de RHEL. Interdit sur des postes clients.
Environnement Java	OpenJDK	Redhat	25	E	E	E	E	E	E	E	E	E	E	E		31/12/30		Le support étendu nécessite une souscription payante, en plus de celle pour l'utilisation de RHEL. Interdit sur des postes clients.
Environnement Java	OpenJDK	Redhat	8	D	O	D	O	D	O	D	O	I	N	D		30/11/26	31/12/30	Le support étendu nécessite une souscription payante, non envisagée à date, en plus de celle pour l'utilisation de RHEL. Interdit sur des postes clients. Il est recommandé de migrer en version 21.
Environnement JavaScript	Express.js	OpenJS Foundation	4	R		R		R		R		R		D				

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement JavaScript	Express.js	OpenJS Foundation	5	R		R		R		R		R		D				
Environnement JavaScript	Fastify	OpenJS Foundation	4	I		I		I		I		I		I				
Environnement JavaScript	Fastify	OpenJS Foundation	5	A		A		A		A		A		A				Compatible avec Node.js version 20 et plus récente.
Environnement JavaScript				R	S	R	S	R	S	R	S	R	S	R				
Environnement JavaScript	Parse server	Parse Platform	5	A		A		A		A		A		A				Framework complémentaire à Express. Assujetti à un développement d'application mobile pour faciliter la gestion des utilisateurs, la communication en temps réel par websockets et les notifications Push aux appareils mobiles.
Environnement JavaScript	Parse server	Parse Platform	6	A		A		A		A		A		A				Framework complémentaire à Express. Assujetti à un développement d'application mobile pour faciliter la gestion des utilisateurs, la communication en temps réel par websockets et les notifications Push aux appareils mobiles.
Environnement PHP	PHP	The PHP Group	7.3	I	N	I	N	I	N	I	N	I	N	I		27/11/20	05/12/21	
Environnement PHP	PHP	The PHP Group	7.4	D	O	I	N	D	O	D	O	I	N	D		27/11/21	27/11/22	Déconseillé sur linux mais interdit sur windows

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement PHP	PHP	The PHP Group	8.0	D	O	I	N	D	O	D	O	I	N	D		25/11/22	25/11/23	Déconseillé sur linux mais interdit sur windows
Environnement PHP	PHP	The PHP Group	8.1	D	O	I	N	D	O	D	O	I	N	D		24/11/23	24/11/24	Déconseillé sur linux mais interdit sur windows
Environnement PHP	PHP	The PHP Group	8.2	D	O	D	O	D	O	D	O	I	N	D		07/12/24	07/12/25	Déconseillé sur linux mais interdit sur windows
Environnement PHP	PHP	The PHP Group	8.3	R	S	R	S	R	S	R	S	R	S	R		31/12/25	31/12/27	
Environnement PHP	PHP	The PHP Group	8.4	R	S	R	S	R	S	R	S	R	S	R		31/12/26	31/12/28	
Environnement PHP	PHP	The PHP Group	8.5	R	S	R	S	R	S	R	S	R	S	R		31/12/27	31/12/29	
Environnement PHP	PHP-FPM	The PHP Group		R	S	R	S	R	S	R	S	R	S	R				Pour des sites en PHP devant subir des charges importantes (inclut avec
Environnement Python	Python	Python Software Foundation	2.7	I	N	I	N	I	N	I	N	I	N	I		31/12/19		Même statut pour les versions antérieures.
Environnement Python	Python	Python Software Foundation	3.10	A	S	A	S	A	S	A	S	A	S	A		03/10/26		Emploi à justifier.
Environnement Python	Python	Python Software Foundation	3.11	A	S	A	S	A	S	A	S	A	S	A		23/10/27		Emploi à justifier.
Environnement Python	Python	Python Software Foundation	3.12	A	S	A	S	A	S	A	S	A	S	A		01/10/28		Emploi à justifier.
Environnement Python	Python	Python Software Foundation	3.13	A	S	A	S	A	S	A	S	A	S	A		31/10/29		Emploi à justifier.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Environnement Python	Python	Python Software Foundation	3.14	A	S	A	S	A	S	A	S	A	S	A		31/10/30		Emploi à justifier.
Environnement Python	Python	Python Software Foundation	3.9	I	N	I	N	I	N	I	N	I	N	I		04/10/25		Emploi à justifier.
Environnement	Ruby		3.1	I	N	I	N	I	N	I	N	I	N	I			30/03/25	
Environnement Ruby	Ruby		3.2	D	N	D	N	D	N	D	N	I	N	D		01/04/25	30/03/26	Assujetti au seul cas de mise en œuvre du service de socle Démarche Simplifié et à l'outillage Puppet dans l'attente d'une migration vers Ruche
Environnement Ruby	Ruby		3.3	A	N	A	N	A	N	A	N	A	N	A			31/03/27	Assujetti au seul cas de mise en œuvre du service de socle Démarche Simplifié et à l'outillage Puppet dans l'attente d'une migration vers Ruche
Environnement Ruby	Ruby		3.4	A	N	A	N	A	N	A	N	A	N	A				Assujetti au seul cas de mise en œuvre du service de socle Démarche Simplifié et à l'outillage Puppet dans l'attente d'une migration vers Ruche
ERP	HR Access Suite	HR Access Solutions (Sopra)		A	N	A	N					I	N	A				
ERP	SAP ECC	SAP		D	N	I	N					I	N	D				

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
ERP	SAP HANA / SAP S/4HANA	SAP		A	N	A	N					I	N	A		18/01/38		
ESB	ServiceMix	Apache Software Foundation	7	I	N	I	N	I	N	I	N	I	N	I				Uniquement pour les applications s'appuyant sur le framework du SIA
ESB	Talend Open Studio for ESB	Talend		I	N	I	N	I	N	I	N	I	N	I				Abandonné par l'éditeur. Il n'y a donc ni support, ni évolution de prévu.
ETL	Data Integrator	Oracle	12.1	I	N	I	N					I	N	I		30/11/17	30/11/19	Assujetti aux SI déjà déployés et aux cas d'usage ne pouvant pas être satisfaits par des briques recommandées.
ETL	Data Integrator	Oracle	12.2	A	N	A	N					I	N	A		30/11/26	30/11/27	Assujetti aux SI déjà déployés et aux cas d'usage ne pouvant pas être satisfaits par des briques recommandées.
ETL	Data Integrator	Oracle	14.1	A	N	A	N					I	N	A		01/12/29	01/12/32	Assujetti aux SI déjà déployés et aux cas d'usage ne pouvant pas être satisfaits par des briques recommandées.
ETL	Logstash	Elastic	7	I	N	I	N	I	N	I	N	I	N	I				
ETL	Logstash	Elastic	8.17	D	O	D	O	D	O	D	O	I	N	D				Les versions mineures précédentes (8.x) sont interdites. Le maintien de la 8.17 se terminera à la sortie de la 8.19.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
ETL	Logstash	Elastic	8.18	A	S	A	S	A	S	A	S	A	S	R				L'emploi de la version 8.19 est à privilégier. La 8.18 est supportée jusqu'à la sortie d'Elasticsearch 9.2.
ETL	Logstash	Elastic	8.19	R	S	R	S	R	S	R	S	R	S	R				Version LTS. Sera maintenue jusqu'à la version 10.0.0.
ETL	Logstash	Elastic	9	A	N	A	N	A	N	A	N			A				Version non recommandée. Cycle de vie rapide. Assujetti à la capacité à le maintenir en version.
ETL	SQL Server Integration Services (SSIS)	Microsoft		A	S									A		12/07/21	13/07/26	Bull Fast Track (Assujetti à un infocentre en MS). L'actuel infocentre opéré par la DIRISI n'intègre plus de nouveaux SI) Cf SQL server pour les versions et leur fin de vie.
ETL	Talend open studio for Data Integration	Talend		I	N	I	N	I	N	I	N	I	N	I				Abandonné par l'éditeur. Il n'y a donc ni support, ni évolution de prévu.
ETL	Talend Platform Data Integration (TPDI)	Talend		R	S									R				
ETL	Talend Platform Data Management	Talend	7.3	I	N	I	N					I	N	I		31/10/24		

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
ETL	Talend Platform Data Management	Talend	8	R	S	R	S					A	S	R				
Forum	PhpBB	phpBB limited	3.3	A	N									A				
Framework de développement	.NET	Microsoft	10	A		A		A		A		A		A		14/11/28		Assujetti au déploiement sur windows
Framework de développement	.NET	Microsoft	7	I		I		I		I		I		I		14/05/24		
Framework de développement	.NET	Microsoft	8	D		D		D		D		D		D		10/11/26		
Framework de développement	.NET	Microsoft	9	D		D		D		D		D		D		10/11/26		
Framework de développement	.NET Core	Microsoft																Cf la version équivalent de .NET pour le statut des versions. L'assujettissement pour les versions à jour est au déploiement sous Linux.
Framework de développement	.NET Framework	Microsoft	3.5	R	S	R	S	R	S	R	S	R	S	R		08/01/29		SP1

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	.NET Framework	Microsoft	4.6.1	I	N	I	N	I	N	I	N	I	N	I		25/04/22		Même status pour les versions suivantes : 4, 4.5, 4.5.1, 4.5.2, 4.6
Framework de développement	.NET Framework	Microsoft	4.6.2	R	S	R	S	R	S	R	S	R	S	R		11/01/27		
Framework de développement	.NET Framework	Microsoft	4.7	R	S	R	S	R	S	R	S	R	S	R				Le support de .NET 4.7 suit la même politique de cycle de vie que le système d'exploitation parent.
Framework de développement	.NET Framework	Microsoft	4.8	R	S	R	S	R	S	R	S	R	S	R				Le support de .NET 4.8 suit la même politique de cycle de vie que le système d'exploitation parent.
Framework de développement	Adobe Integrated Runtime (AIR)			D		I		I		I		I		D				Migration vers des technologies web recommandé. Sera refusé pour toutes nouvelles applications.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Angular	Google	18	I		I		I		I		I		I		22/11/24	22/11/25	Assujetti à la maintenance des applications déjà en production, aux projets réalisés par des équipes internes ou aux DSI aptes à assurer le MCO/MCS sur tout la durée du système d'information malgré le cycle de vie court de ce composant : 1 nouvelle version majeure tous les 6 mois avec un support de 18 mois
Framework de développement	Angular	Google	19	D		D		D		D		D		D		28/05/25	19/05/26	Assujetti à la maintenance des applications déjà en production, aux projets réalisés par des équipes internes ou aux DSI aptes à assurer le MCO/MCS sur tout la durée du système d'information malgré le cycle de vie court de ce composant : 1 nouvelle version majeure tous les 6 mois avec un support de 18 mois

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Angular	Google	20	A		A		A		A		A		A		21/11/25	21/11/26	Assujetti à la maintenance des applications déjà en production, aux projets réalisés par des équipes internes ou aux DSI aptes à assurer le MCO/MCS sur tout la durée du système d'information malgré le cycle de vie court de ce composant : 1 nouvelle version majeure tous les 6 mois avec un support de 18 mois
Framework de développement	Angular	Google	21	A		A		A		A		A		A		19/05/26	19/05/27	Assujetti à la maintenance des applications déjà en production, aux projets réalisés par des équipes internes ou aux DSI aptes à assurer le MCO/MCS sur tout la durée du système d'information malgré le cycle de vie court de ce composant : 1 nouvelle version majeure tous les 6 mois avec un support de 18 mois
Framework de développement	Bootstrap		4	I	N	I	N	I	N	I	N	I	N	I		31/12/22		Dernière version : 4.6.2

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Bootstrap		5	R		R		R		R		R		R				
Framework de développement	Capacitor		6	I		I		I		I		I		I		20/07/25	20/01/26	Développement d'applications s'appuyant sur Ionic
Framework de développement	Capacitor		7	A		A		A		A		A		A				Développement d'applications s'appuyant sur Ionic
Framework de développement	Cordova	Apache Software Foundation	12	A		A		A		A		A		A				Développement d'applications s'appuyant sur Ionic
Framework de développement	Django		5.2	I	N	R	S	R	S	R	S	R	S	I		30/11/25	31/03/28	Ce framework est recommandé pour réaliser une application WEB avec le langage Python. Les versions précédentes sont interdites. L'usage des versions non LTS (X.0 et X.1) est déconseillé.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Electron		38	D		D		D		D		I		D		10/03/26		Assujetti aux cas nécessitant impérativement le développement d'un client lourd et une capacité à réaliser un MCS très fréquent (au moins 2 fois par an). Attention : cette version est annoncée pour mars, et n'est pas encore disponible à la publication de cette version du CCT.
Framework de développement	Electron		39	A		A		A		A		A		A		05/05/26		Assujetti aux cas nécessitant impérativement le développement d'un client lourd et une capacité à réaliser un MCS très fréquent (au moins 2 fois par an). Attention : cette version est annoncée pour mars, et n'est pas encore disponible à la publication de cette version du CCT.
Framework de développement	FastAPI			R		R		R		R		R		R				Ce framework est recommandé pour réaliser des API avec le langage Python avec un besoin accru de performances.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Flask		3	R		R		R		R		R		R				Ce framework est recommandé pour réaliser des API avec le langage Python. Il est facile à apprendre et adapté à des API simples.
Framework de développement	Ionic		7	I		I		I		I		I		I		17/04/24	17/04/25	Développement d'applications mobiles nécessitant un accès aux SDKs natifs.
Framework de développement	Ionic		8	A		A		A		A		A		A				Développement d'applications mobiles nécessitant un accès aux SDKs natifs.
Framework de développement	JHipster		8	R		R		R		R		R		D				Générateur de projet d'application Spring Boot intégrant la réalisation d'un frontend avec Vue.js, React ou Angular.
Framework de développement	jQuery		2	I		I		I		I		I		I				
Framework de développement	jQuery		3	D		D		D		D		D		D				Assujetti à l'usage d'un composant tiers lui-même adhérent à jQuery. Seule la dernière version mineure disponible est tolérée.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	jQuery		4	A		A		A		A		A		A				Assujetti à l'usage d'un composant tiers lui-même adhérent à jQuery. Seule la dernière version mineure disponible est tolérée.
Framework de développement	Laravel	Laravel	10	I		I		I		I		I		I		06/08/24	06/02/25	Compatible PHP 8.1-8.3
Framework de développement	Laravel	Laravel	11	D		D		D		D		I		D		05/08/25	03/02/26	Compatible PHP 8.2, 8.3 et 8.4
Framework de développement	Laravel	Laravel	12	R		R		R		R		R		R		16/08/26	24/02/27	Compatible PHP 8.2, 8.3 et 8.4
Framework de développement	Leaflet			R		R		R		R		R		R				Framework javascript de gestion des cartes
Framework de développement	NestJS		11	A		A		A		A		A		A				
Framework de développement	Next.js		15	I		I		I		I		I		I				Comporte une faille de sécurité critique (CVE-2025-55182). Les versions précédentes sont également interdites.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Next.js		16	A		A		A		A		A		D				Assujetti à la réalisation avec React de SI exposés sur Internet et pour lesquels l'optimisation du référencement par les moteurs de recherche (SEO) est un besoin métier majeur. Les versions antérieures à la 16.07 comportent une faille critique (CVE-2025-55182) et sont donc interdites.
Framework de développement	Node.js	OpenJS Foundation	18	I	N	I	N	I	N	I	N	I	N	I		29/04/25		
Framework de développement	Node.js	OpenJS Foundation	20	D	O	D	O	D	O	D	O	I	N	D		29/04/26		
Framework de développement	Node.js	OpenJS Foundation	22	R	S	R	S	R	S	R	S	R	S	R		30/04/27		
Framework de développement	Node.js	OpenJS Foundation	24	R	S	R	S	R	S	R	S	R	S	R		06/11/27		

[illegible]

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Quarkus	Redhat		I		I		I		I		I		I				L'usage de la dernière version non LTS disponible est déconseillé du fait de son cycle de vie extrêmement court, de l'ordre du mois. L'usage des autres versions non LTS est interdit. Il est recommandé d'utiliser la version LTS, maintenue un an.
Framework de développement	Quarkus	Redhat	3.15	I		I		I		I		I		I		25/09/25		Quarkus est un framework Java conçu pour les applications cloud-native et les microservices. Il se distingue par sa rapidité de démarrage et sa faible consommation de mémoire, ce qui le rend particulièrement adapté aux environnements de conteneurs comme Kubernetes. Son usage au MinArm est assujetti à l'usage de conteneurs.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOps		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Quarkus	Redhat	3.20	D		D		D		D		I		D		26/03/26		Quarkus est un framework Java conçu pour les applications cloud-native et les microservices. Il se distingue par sa rapidité de démarrage et sa faible consommation de mémoire, ce qui le rend particulièrement adapté aux environnements de conteneurs comme Kubernetes. Son usage au MinArm est assujetti à l’usage de conteneurs. Version LTS
Framework de développement	Quarkus	Redhat	3.27	A		A		A		A				A		24/09/26		Quarkus est un framework Java conçu pour les applications cloud-native et les microservices. Il se distingue par sa rapidité de démarrage et sa faible consommation de mémoire, ce qui le rend particulièrement adapté aux environnements de conteneurs comme Kubernetes. Son usage au MinArm est assujetti à l’usage de conteneurs. Version LTS

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	React		19	R		R		R		R		R		R				Les versions 19.0.0, 19.1.0, 19.1.1 et 19.2.0 comportent une faille critique (CVE-2025-55182) et sont donc interdites.
Framework de développement	Ruby on Rails			I	N	A	S	A	S	A	S	A	S	I				
Framework de développement	Spring	VMWare	5.2	I		I		I		I		I		I		30/12/21	30/12/23	Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Compatibilité java 8 et 11
Framework de développement	Spring	VMWare	5.3	D		D		D		D		A		D		30/06/23	30/06/29	Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Il est obligatoire de prendre ce support pour avoir l'autorisation d'utiliser cette version. Compatibilité java 8 - 11 et 17 et javaEE 7 et 8.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Spring	VMWare	6.0	I		I		I		I		I		I		30/06/24	30/06/25	Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Compatibilité java 17 et jakartaEE 9 et 10.
Framework de développement	Spring	VMWare	6.1	D		I		D		D		I		D		30/06/25	30/06/26	Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Compatibilité java 17 et jakartaEE 9 et 10.
Framework de développement	Spring	VMWare	6.2	A		A		A		A		A		A		30/06/26	30/06/32	Assujetti à la souscription au support étendu payant. Compatibilité java 17 et jakartaEE 9 et 10.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Spring	VMWare	7.0	R		R		R		R		R		R		30/06/27	30/06/28	Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Compatibilité java 17 à 25 et jakartaEE 11. Les prérequis sont les suivants : Servlet 6.1 (Tomcat 11.0, Jetty 12.1), JPA 3.2 (Hibernate ORM 7.1/7.2), Bean Validation 3.1 (Hibernate Validator 9.0/9.1)

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Spring Boot	VMWare	3.2													31/12/24	31/12/25	La fonction permettant d’embarquer un serveur d’application ne doit pas être utilisée (hors des environnements de développement ou en hébergement en orchestration de conteneurs). Nécessite également de monter un certain nombre de versions de frameworks en dépendance (Hibernate 6.2, Elasticsearch client 8.7, SLF4J 2.0 ... par exemple). Il est donc recommandé aux projets utilisant cette technologie de planifier une montée de version majeure dans leur feuille de route. Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Compatibilité java 17 - 20

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Spring Boot	VMWare	3.3	D		D		D		D		I		D		30/06/25	30/06/26	La fonction permettant d’embarquer un serveur d’application ne doit pas être utilisée (hors des environnements de développement ou en hébergement en orchestration de conteneurs). Nécessite également de monter un certain nombre de versions de frameworks en dépendance (Hibernate 6.2, Elasticsearch client 8.7, SLF4J 2.0 ... par exemple). Il est donc recommandé aux projets utilisant cette technologie de planifier une montée de version majeure dans leur feuille de route. Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Compatibilité java 17 - 21

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOps		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Spring Boot	VMWare	3.4	A		A		A		A		A		A		31/12/25	31/12/26	Assujetti à l'impossibilité d'utiliser la 4.0, ou la 3.5 avec un support commercial. La fonction permettant d’embarquer un serveur d’application ne doit pas être utilisée (hors des environnements de développement ou en hébergement en orchestration de conteneurs). Nécessite également de monter un certain nombre de versions de frameworks en dépendance (Hibernate 6.2, Elasticsearch client 8.7, SLF4J 2.0 ... par exemple). Il est donc recommandé aux projets utilisant cette technologie de planifier une montée de version majeure dans leur feuille de route en 2024. Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Compatibilité java 17 - 21

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Spring Boot	VMWare	3.5	R		R		R		R		R		R		30/06/26	30/06/32	La fonction permettant d’embarquer un serveur d’application ne doit pas être utilisée (hors des environnements de développement ou en hébergement en orchestration de conteneurs). Nécessite également de monter un certain nombre de versions de frameworks en dépendance (Hibernate 6.2, Elasticsearch client 8.7, SLF4J 2.0 ... par exemple). Il est donc recommandé aux projets utilisant cette technologie de planifier une montée de version majeure dans leur feuille de route. Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Compatibilité java 17 - 21

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Spring Boot	VMWare	4.0	R		R		R		R		R		R		31/12/26	31/12/27	La fonction permettant d’embarquer un serveur d’application ne doit pas être utilisée (hors des environnements de développement ou en hébergement en orchestration de conteneurs). Attention support étendu disponible uniquement sur souscription d'une offre commerciale. Compatibilité java 17 et +.
Framework de développement	Symfony	Symfony SAS	5.4	D		D		D		D		D		D		29/11/24	29/11/29	Il n'y a plus de correction de bug en support étendu, mais juste des correctifs de sécurité. Il est donc recommandé de privilégier la version LTS 7.4 pour tout nouveau développement.
Framework de développement	Symfony	Symfony SAS	6.4	R		R		R		R		R		R		29/11/26	29/11/27	Il est recommandé de privilégier la version LTS 7.4 pour tout nouveau développement. Il n'y aura plus de correction de bug en support étendu, mais juste des correctifs de sécurité.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Framework de développement	Symfony	Symfony SAS	7.4	R		R		R		R		R		R		29/11/28	29/11/29	Il est recommandé de privilégier la version LTS 7.4 pour tout nouveau développement. Il n'y aura plus de correction de bug en support étendu, mais juste des correctifs de sécurité.
Framework de développement	Symfony	Symfony SAS	8.0	I		I		I		I		I		I				Même status pour les autres versions non LTS
Framework de développement	Vue.js	Evan You	2	I		I		I		I		I		I		30/12/23		
Framework de développement	Vue.js	Evan You	3	R		R		R		R		R		R				
Framework d'intégration	Camel		4	R		R		R		R		R		R				Il ne fait pas partie de Spring Framework mais il est recommandé de s'en service avec Spring Boot afin de bénéficier de l'infrastructure Spring (Conteneurs IoC, gestion de transactions, sécurité, ...). Il met en œuvre les principes et patterns d'intégration d'entreprise, appelés EIP.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Gestion d'anomalies	Mantis Bug Tracker		2	D	O	D	O	D	O	D	O	I	N	D				Embarque des frameworks obsolètes (jQuery 2 et Bootstrap 3). La communauté en charge de son soutien ne prévoit pas de corriger ces obsolescences. En conséquence, il est demandé d'étudier son remplacement par TULEAP.
Gestion de clusters	Rancher	CNCF/SUSE	2.10	D	N	D	N	D	O	D	O			D		19/06/25	19/06/26	Permet de piloter des ensembles de clusters et de gérer les ressources Kubernetes déployées. Retenu pour les offres de conteneurisation cloud C1 du Ministère, et intranets IST et 3E.
Gestion de clusters	Rancher	CNCF/SUSE	2.11	D	N	D	N	D	N	D	N			D		24/10/25	24/10/26	Permet de piloter des ensembles de clusters et de gérer les ressources Kubernetes déployées. Retenu pour les offres de conteneurisation cloud C1 du Ministère, et intranets IST et 3E.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Gestion de clusters	Rancher	CNCF/SUSE	2.12	A	N	A	N	A	N	A	N			A		28/02/26	28/02/27	Permet de piloter des ensembles de clusters et de gérer les ressources Kubernetes déployées. Retenu pour les offres de conteneurisation cloud C1 du Ministère, et intranets IST et 3E.
Gestion de clusters	Rancher	CNCF/SUSE	2.8	I	N	I	N	I	N	I	N			I			22/07/25	Permet de piloter des ensembles de clusters et de gérer les ressources Kubernetes déployées. Retenu pour les offres de conteneurisation cloud C1 du Ministère, et intranets IST et 3E.
Gestion de clusters	Rancher	CNCF/SUSE	2.9	D	N	D	N	D	N	D	N			D		26/02/25	26/02/26	Permet de piloter des ensembles de clusters et de gérer les ressources Kubernetes déployées. Retenu pour les offres de conteneurisation cloud C1 du Ministère, et intranets IST et 3E.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Gestion des schémas des BDD	Liquibase			A		A		A		A		A		A				Assujetti à l'impossibilité d'utiliser Flyway
Gestionnaire de backup	Kasten	CNCF/VEEAM		A	N	A	N	A	N	A	N			A				Solution de sauvegarde très fin et restauration de clusters et ressources Kubernetes. Permet d'offrir du « Backup as a service » en fonction de l'implémentation choisie. Permet également la migration simple de clusters.
Gestionnaire de	Px Backup	Pure Storage		A	N			A	N	A	N			A				Solution de gestion de stockage sur
Gestionnaire de backup	Velero	CNCF/SUSE	1	A	N	A	N	A	N	A	N			A				restauration de clusters Kubernetes Choisir la version en fonction du support de la version Kubernetes (cf documentation Velero)
Gestionnaire de version	Forgejo	Codeberg	11	A		A		A		A		A		A				Fork libre de Gitea qui a changé de licence Gestionnaire de version pour des besoins modestes
Gitops	ArgoCD	CNCF	3			A	N	A	N	A	N			A				Solution de déploiement automatique d'applications en conteneur.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
HCI	Virtualization	CNCF/SUSE	1	A		A		A		A		A		A				Anciennement Harvester. Assujetti à l'absence d'offre d'hébergement dans le contexte visé. Cela implique de monter son propre hébergement en salle blanche.
Hypervision / Virtualisation	ESXi	VMWare	7.0	I	N	I	N	I	N	I	N	I	N	I		01/04/25		
Hypervision / Virtualisation	ESXi	VMWare	8.0	A	S	A	S	A	S	A	S	A	S	A		10/10/27		Assujetti à des infrastructures existantes. Pour de nouvelles infrastructures, il est nécessaire de passer en Agora tech pour vérifier la disponibilité d'une solution recommandée.
Hypervision / Virtualisation	ESXi	VMWare	9.0	A	S	A	S	A	S	A	S	A	S	A				Assujetti à des infrastructures existantes. Pour de nouvelles infrastructures, il est nécessaire de passer en Agora tech pour vérifier la disponibilité d'une solution recommandée.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Hypervision / Virtualisation	Hyper-V	Microsoft	2012R2	I	N			I	N	I	N			I			31/12/24	Assujetti à l'absence d'offre d'hébergement dans le contexte visé ou à des configuration projetables (théâtre et bâtiments tous intranets et sites de proximité STC-IA V02). Cela implique de monter son propre hébergement en salle blanche.
Hypervision / Virtualisation	Hyper-V	Microsoft	2016	A	S			A	S	A	S			A		10/01/22	11/01/27	Assujetti à l'absence d'offre d'hébergement dans le contexte visé ou à des configuration projetables (théâtre et bâtiments tous intranets et sites de proximité STC-IA V02). Cela implique de monter son propre hébergement en salle blanche.
Hypervision / Virtualisation	Hyper-V	Microsoft	2019	A	S			A	S	A	S			A		08/01/24	08/01/29	Assujetti à l'absence d'offre d'hébergement dans le contexte visé ou à des configuration projetables (théâtre et bâtiments tous intranets et sites de proximité STC-IA V02). Cela implique de monter son propre hébergement en salle blanche.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Hypervision / Virtualisation	Proxmox VE	Proxmox Server Solutions GmbH	9.1	A	N	I	N	A	N	A	N	I	N					Assujetti à un besoin de gérer un faible nombre de VMs (de l'ordre de la dizaine). L'usage de conteneurs LXC est interdit. Assujetti à l'absence d'offre d'hébergement dans le contexte visé. Cela implique de monter son propre hébergement en salle blanche.
Hypervision / Virtualisation	Workstation Pro	VMWare	17															Assujetti aux réseaux IST/I3E uniquement
IA/ Big Data	Conda	Anaconda																Assujetti aux environnements de développement Big Data
IA/ Big Data	Flink	Apache Software Foundation				E	N											
IA/ Big Data	Jupyter		7															Assujetti aux environnements de développement Big Data
IA/ Big Data	NiFi	Apache Software Foundation	1	I	N	I	N	I	N	I	N	I	N	I				
IA/ Big Data	NiFi	Apache Software Foundation	2	R	S	R	S	R	S	R	S	R	S	R				

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
IA/ Big Data	Spark	Apache Software Foundation	3.4	I	N	I	N	I	N	I	N	I	N	I				Cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.
IA/ Big Data	Spark	Apache Software Foundation	3.5	A	N	A	N	A	N	A	N			A				Cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.
IA/ Big Data	Spark	Apache Software Foundation	4.0	A	N	A	N	A	N	A	N			A				Cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.
IA/ Big Data	Trino					A	S	A	S									Assujetti aux usages Artemis.IA
Identification de la langue parlée	Vocapia (VoxSigma LID)	Vocapia Research		E	E	E	E	E	E	E	E	E	E					Brique unique intégrant l'identification de plus de 120 langues, variantes et dialectes (dont langues d'intérêt MINARM), API REST, OS Linux, mode SaaS ou on-premise
IGC	IGC-G	MinArm		D	O	I	N	D	O	D	O			D				Infrastructure de gestion de clés ancienne génération - Dépréciée, lui préférer IGC-G NG

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
IGC	IGC-G NG	MinArm		R	S	R	S	R	S	R	S			R				Nouvelle infrastructure de gestion de clés - A privilégier
Interface réseau pour conteneurs	Calico	CNCF/Nirmata	3	A	N	A	N	A	N	A	N			A				Greffon de gestion du réseau sur un cluster Kubernetes reposant sur l'eBPF et permettant la création de politiques réseaux avancées. Inclus dans la distribution RKE2.
Interface réseau pour conteneurs	Cilium	CNCF/Isovalent	1	A	N	A	N	A	N	A	N			A				Greffon de gestion du réseau sur un cluster Kubernetes reposant sur l'eBPF et permettant la création de politiques réseaux avancées. Inclus dans la distribution RKE2 et retenu pour les offres de conteneurisation cloud C1 du Ministère. Apporte la gestion des network policies sur les noms de domaine contrairement à Calico (à vérifier)
Logiciel de	Keepalived		2	R	S	R	S	R	S	R	S	R	S	R				
MDM/DQM	PGDR	MinArm		R	S													À vocation ministérielle, l'offre de service concerne tout référentiel de données et SI NP/DR quel que soit le domaine métier.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Messagerie	Cyrus IMAP	Université Carnegie-Mellon	3.12	A	S							I	N	A				Utilisé en serveur SMTP/IMAP d'appoint, assujetti à une dérogation sur le cadre d'emploi
Messagerie	NEMO	MinArm	2	R	S													Addon outlook
Messagerie	NEMO	MinArm	3					R	S	R	S							Addon outlook
Messagerie	Outlook	Microsoft	2010					D		D						12/10/15	12/10/20	Cf Office 2010
Messagerie	Outlook	Microsoft	2016	R		R		R		R						12/10/20	13/10/25	Cf Office 2016
Messagerie	OWA	Microsoft		R		R												Outlook Web Access est une fonctionnalité portée par les serveurs Microsoft Exchange. Cf ce dernier pour les dates de fin de support.
Messagerie	postfix	Postfix.org	3.10	A	S			A	S	A	S	I	N	A				Assujetti a une dérogation sur le cadre d'emploi. Utilisé dans SIE et NEMO (bordure du système)
Messagerie	postfix	Postfix.org	3.6	I	N			I	N	I	N	I	N	I				Assujetti a une dérogation sur le cadre d'emploi.
Messagerie	postfix	Postfix.org	3.7	D	O			D	O	D	O	I	N	D				Assujetti a une dérogation sur le cadre d'emploi. Utilisé dans SIE et NEMO (bordure du système)
Messagerie	postfix	Postfix.org	3.8	A	S			A	S	A	S	I	N	A				Assujetti a une dérogation sur le cadre d'emploi.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Messagerie	postfix	Postfix.org	3.9	A	S			A	S	A	S	I	N	A				Assujetti a une dérogation sur le cadre d'emploi. Utilisé dans SIE et NEMO (bordure du système)
Messagerie	SOGGo			A										A				Assujetti au contexte SIE : Webmail pour le SIE (Baltique/Celtique), connectable avec le client Outlook et offrant des fonctions de partage de calendriers et de carnets d'adresses. Application responsive accessible sur SMOBI tablette ou smartphone.
Messagerie	Thunderbird	Mozilla	128	A										A				Version ESR
MessagerieAge	Exchange	Microsoft	2010	I	N	I	N	I	N	I	N	I	N			12/10/20		Même status pour les versions antérieures
MessagerieAge	Exchange	Microsoft	2016	D	O	D	O	D	O	D	O	I	N			13/10/20	13/10/25	ESU jusqu'au14/04/2026
MessagerieAge	Exchange	Microsoft	2019	D	O	D	O	D	O	D	O					08/12/24	13/10/25	ESU jusqu'au14/04/2026
MessagerieAge	Exchange	Microsoft	SE	R	S	R	S	R	S	R	S							
Métrologie	Dynatrace	Dynatrace	1	R	S	R	S							R				
Moniteur de transfert	CFT	Axway		A	S	A	S							A				Assujetti à des échanges avec des partenaires hors MinArm

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intredef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Moteur de conteneurisation	Containerd	CNCF	2	A	N	A	N	A	N	A	N			A				Par extension, tout moteur s'appuyant sur cet exécutable. Inclus dans la distribution RKE2 et retenu pour les offres de conteneurisation cloud C1 du Ministère.
Moteur de	Sinequa	Sinequa		A	S	A	S	R	S	R	S			A				Assujetti sur Intradef lorsque Syriam
Moteur de	SYRIARM	MinArm		R	S	R	S											
Multimédia	VLC	Videolan		R		R						R		R				
Navigateur	Edge	Microsoft		R		R		E		E				R				
Navigateur	Firefox	Mozilla	102	I		I		D		D		I		I		25/07/22	25/09/23	Version ESR
Navigateur	Firefox	Mozilla	115	I		I		I		I		I		I		31/07/23	30/09/24	Version ESR
Navigateur	Firefox	Mozilla	128	D		D		D		D		I		D		16/09/25		Version ESR
Navigateur	Firefox	Mozilla	140	E		E						R		R		13/10/26		Version ESR
Navigateur	Internet Explorer	Microsoft	11	I		I		I		I		I		I		14/06/22		Déconseillé par Microsoft

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Orchestrateur	Kubernetes	CNCF	1.31	I	N	I	N	I	N	I	N			I		27/10/25		Orchestrateur de conteneurs de référence, développé initialement par Google et retenu pour les offres de conteneurisation cloud C1 du Ministère. Une nouvelle version de Kubernetes est publiée tous les 4 mois et est soutenue pour environ 1 an. Les directions de projet doivent donc organiser en conséquence pour soutenir ce rythme de mise à jour. La complexité des écosystèmes nécessaires pour faire fonctionner l'ensemble des briques nécessaire à l'orchestration de conteneurs plaide pour le recours à une distribution.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Orchestrateur	Kubernetes	CNCF	1.32	D	N	D	N	D	N	D	N			D		28/02/26		Orchestrateur de conteneurs de référence, développé initialement par Google et retenu pour les offres de conteneurisation cloud C1 du Ministère. Une nouvelle version de Kubernetes est publiée tous les 4 mois et est soutenue pour environ 1 an. Les directions de projet doivent donc organiser en conséquence pour soutenir ce rythme de mise à jour. La complexité des écosystèmes nécessaires pour faire fonctionner l'ensemble des briques nécessaire à l'orchestration de conteneurs plaide pour le recours à une distribution.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Orchestrateur	Kubernetes	CNCF	1.33	D	N	D	N	D	N	D	N			D		28/06/26		Orchestrateur de conteneurs de référence, développé initialement par Google et retenu pour les offres de conteneurisation cloud C1 du Ministère. Une nouvelle version de Kubernetes est publiée tous les 4 mois et est soutenue pour environ 1 an. Les directions de projet doivent donc organiser en conséquence pour soutenir ce rythme de mise à jour. La complexité des écosystèmes nécessaires pour faire fonctionner l'ensemble des briques nécessaire à l'orchestration de conteneurs plaide pour le recours à une distribution.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Orchestrateur	Kubernetes	CNCF	1.34	A	N	A	N	A	N	A	N			A		27/10/26		Orchestrateur de conteneurs de référence, développé initialement par Google et retenu pour les offres de conteneurisation cloud C1 du Ministère. Une nouvelle version de Kubernetes est publiée tous les 4 mois et est soutenue pour environ 1 an. Les directions de projet doivent donc organiser en conséquence pour soutenir ce rythme de mise à jour. La complexité des écosystèmes nécessaires pour faire fonctionner l'ensemble des briques nécessaire à l'orchestration de conteneurs plaide pour le recours à une distribution.
Orchestration	Ansible	Redhat	2.14	I	N	I	N	I	N	I	N	I	N	I		19/05/24		

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Orchestration	Ansible	Redhat	2.15	R	S	R	S	A	N	A	N	R	S	A		30/11/24		L'usage d'AAP (Ansible Automation Platform) permet de prolonger le support d'Ansible. La version actuelle d'AAP utilisée pour Ruche porte le support étendu d'Ansible v2.15 jusqu'au 30/06/2026. Il est prévu de monter en version 2.16 à l'été 2026. Le cycle de vie d'Ansible dans Ruche est décrit dans la [documentation PICSEL](https://docs.picsel.defense.gouv.fr/3_guide_utilisation_services_techniques/39_service_ruche/391_fil_actu/index.html) Est assujetti sur les segments ne pouvant disposer de Ruche à l'usage d'AAP.
Orchestration	Ansible	Redhat	2.16	E	E	E	E	A	N	A	N	E	E	A		31/05/25		Version envisagé sur Ruche à l'été 2026. Est assujetti sur les segments ne pouvant disposer de Ruche à l'usage d'AAP.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Orchestration	Ansible	Redhat	2.17	I	N	I	N	D	N	D	N	I	N	D		30/11/25		N'est acceptable que sur un segment ne permettant pas l'usage de Ruche, et sous réserve d'être utilisé avec AAP. Même dans ce cas particulier, il est recommandé de plutôt utiliser Ansible 2.18. Dans tout autre cas, l'usage de cette version est interdit.
Orchestration	Ansible	Redhat	2.18	I	N	I	N	A	N	A	N	I	N	A		31/05/26		Assujetti au cas d'usage hors Ruche. Il est recommandé de l'utiliser avec les versions d'AAP 2.5 ou 2.6, qui portent respectivement son support étendu au 02/10/2027 et 02/10/2028.
Orchestration	Ansible	Redhat	2.19	I	N	I	N	D	N	D	N	I	N	D		01/12/26		N'est acceptable que sur un segment ne permettant pas l'usage de Ruche, et sous réserve d'être utilisé sans AAP. Même dans ce cas, il est plutôt recommandé d'utiliser la dernière version disponible.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Orchestration	Ansible	Redhat	2.20	I	N	I	N	A	N	A	N	I	N	A		01/12/26		N'est acceptable que sur un segment ne permettant pas l'usage de Ruche, et sous réserve d'être utilisé sans AAP, ou avec AAP 2.6 quand il la supportera, vers le S2 2026.
Orchestration	Ansible Automation Platform	Redhat	2.4	I	N	I	N	D	N	D	N	I	N	D		01/10/24	30/06/26	Utilisé dans le cadre et conformément à Ruche. Également soutenu sur PICSEL
Orchestration	Ansible Automation Platform	Redhat	2.5	I	N	I	N	R	N	R	N	I	N	R		02/10/25	02/10/27	Utilisé dans le cadre et conformément à Ruche. Également soutenu sur PICSEL
Orchestration	Ansible Automation Platform	Redhat	2.6	I	N	I	N	R	N	R	N	I	N	R		01/10/26	01/10/28	Utilisé dans le cadre et conformément à Ruche. Également soutenu sur PICSEL
Orchestration	Puppet	Puppet Labs	7	I										I		28/02/25		Sur SIE, pour la distribution des configurations. À titre transitoire, sur environnement S2NA Utilisé dans l'infrastructure des Intranets 3E-IST, pour le contrôle périodique des configurations et le MCS.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Orchestration	Puppet	Puppet Labs	8	A										A				Sur SIE, pour la distribution des configurations. À titre transitoire, sur environnement S2NA Utilisé dans l'infrastructure des Intranets 3E-IST, pour le contrôle périodique des configurations et le MCS.
Pare feux	Palo Alto	Palo Alto		R	S	R	S	R	S	R	S	R	S	R				
Partage de données géospatial	Geoserver		2	A	N	A	N	A	N	A	N			A				
PEM API	PEM Internet	MinArm										E	E					Passerelle d'échange mutualisée (basée sur la solution WSO2 API MANAGER). Usage obligatoire dans le cadre des échanges inter applicatifs (format API) au sein de l'internet maîtrisé mais également dans le cadre des échanges inter applicatifs entre Internet maîtrisé et Internet public.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
PEM API	PEM Intradef	MinArm		R	S	R	S											Passerelle d'échange mutualisée (basée sur la solution WSO2 API MANAGER). Usage obligatoire dans le cadre des échanges inter applicatifs (format API) au sein de l'intradef.
PEM API	WSO2 API Manager	WSO2	4.1.0	D	N	D	N							D		10/04/27		Version recommandée pour tout usage hors instances ministérielles mutualisées. Cas d'usage et utilisation à justifier.
PEM API	WSO2 API Manager	WSO2	4.5.0	A	N	A	N							A		18/03/28		Version recommandée pour tout usage hors instances ministérielles mutualisées. Cas d'usage et utilisation à justifier.
Plugin	Flash player	Adobe	32	I		I		I		I		I		I		30/12/20		Interdit pour tout nouveau projet. Désactivé sur tous les navigateurs à partir de début 2021. Même statut pour les versions inférieures.
Plugin	Silverlight	Microsoft	5	I		I		I		I		I		I		11/10/21		
Portail	Drupal	Drupal	10.4	I	N	I	N					I	N	I		31/12/25		
Portail	Drupal	Drupal	10.5	R	S	R	S					R	S	R		30/06/26		
Portail	Drupal	Drupal	11.1	I	N	I	N					I	N	I		31/12/25		
Portail	Drupal	Drupal	11.2	R	S	R	S					R	S	R		30/06/26		

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Portail d'information	Joomla!	Joomla!	5.3	I	N	I	N					I	N	I		15/10/25		Même status pour les versions antérieures
Portail	Joomla!	Joomla!	5.4			R	S					R	S	R		12/10/27		LTS
Portail d'information	Joomla!	Joomla!	6.0	D	N	D	N					I	N			14/04/26		La v6.0 est maintenue jusqu'à la sortie de la 6.1. À partir de là, c'est la 6.1 qui sera déconseillée, et la 6.0 passera en interdit. Il est préférable d'utiliser la version LTS (5.4)
Portail d'information	Wordpress	Wordpress Foundation	6.2	I	N	I	N	I	N	I	N	I	N	I		07/08/23		Assujetti aux cas d'usages non couverts par Joomla et Drupal. Seule la dernière version majeure est supportée. Patches de sécurité non garantis sur cette version et versions inférieures Versions de PHP supportées : 7.4 à 8.2.
Portail d'information	Wordpress	Wordpress Foundation	6.6	A	E	A	E	A	E	A	E			A				Assujetti aux cas d'usages non couverts par Joomla et Drupal. Seule la dernière version majeure est supportée. Version PHP supportées : 7.4 à 8.2
Portail	Liferay Portal	Liferay	7.4	R	S	R	S	R	S	R	S	R	S	R				

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Portail personnalisable	Sharepoint	Microsoft	2013	I	N	I	N	I	N	I	N	I	N			09/04/18	10/04/23	Assujetti aux seules configurations projetables (théâtres et bâtiments) du STCIA V0.5 incr 4
Portail personnalisable	Sharepoint	Microsoft	2016	D	S	D	S	A	S	A	S	I	N			12/07/21	13/07/26	Il est recommandé de partir sur la version SE, du fait de la fin prochaine du support étendu.
Portail personnalisable	Sharepoint	Microsoft	2019	D	S	D	S	A	S	A	S	I	N			23/01/24	13/07/26	Il est recommandé de partir sur la version SE, du fait de la fin prochaine du support étendu.
Portail personnalisable	Sharepoint	Microsoft	Subscription Edition	A	S	A	S	A	S	A	S	I	N					
Préparation et analyse des données	Data Science Studio	Dataiku		A	N	A	N	A	N					A				Assujetti à l'usage de la plateforme dataiku de l'Armée de l'Air et de l'Espace. Envisagé en tant que brique du socle sur le C1DR.
Provisionnement	Terraform	Hashicorp	1.10	I	N			I	N	I	N			I		14/05/25		
Provisionnement	Terraform	Hashicorp	1.11	D	N			D	N	D	N			D				Recommandé pour les hébergements en salle blanche uniquement
Provisionnement	Terraform	Hashicorp	1.12	R	E			R	E	R	E			R				Recommandé pour les hébergements en salle blanche uniquement

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Qualimétrie	SonarQube		10	D				D		D				D				Uniquement toléré en cas de besoin d'une instance hors PICSEL. La version 10.9 sera recommandée et soutenue. Avant sa sortie, les deux dernières versions mineures seront déconseillées. Les versions mineures antérieures sont quant à elles interdites.
Qualimétrie	SonarQube		8	I		I		I		I		I		I		06/02/23		Sonar dédié en zone projet PICSEL intégré à la CI/CD
Qualimétrie	SonarQube		9.9	A				A		A				A				Assujetti au besoin d'une instance hors PICSEL. Les versions mineures précédentes (9.8, 9.7, etc) sont interdites.
Qualimétrie	Squashtest	Squash	8															Recommandé hors environnement de production
Qualité des données	InfoSphere Information Server	IBM	14	A	E									A				
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	2.2	I	N	I	N	I	N	I	N	I	N	I		06/07/25		Même status pour les versions précédentes et les versions mineures (2.x) impaires

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	2.4	D	O	D	O	D	O	D	O	I	N	D		30/06/26		
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	2.6	R	S	R	S	R	S	R	S	R	S	R		30/06/27		
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	2.8	R	S	R	S	R	S	R	S	R	S	R		30/06/28		
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	3.0	R	S	R	S	R	S	R	S	R	S	R		30/06/29		
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	3.2	R	S	R	S	R	S	R	S	R	S	R		30/06/30		

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
RPA	UiPath	UiPath	2022.10	I	N	I	N							I		26/10/24	26/10/25	Cette technologie devant être considérée comme un moyen temporaire d'amélioration du fonctionnement de dispositifs anciens, son usage est assujéti à une demande de dérogation justifiant d'une rejoin te vers un environnement non déroga toire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n'exonère pas du respect des règles de l'Intradef et de facto, n'autorise pas son emploi au travers d'ISPT.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
RPA	UiPath	UiPath	2023.10	D	O	D	O							A		01/11/25	01/11/26	Cette technologie devant être considérée comme un moyen temporaire d’amélioration du fonctionnement de dispositifs anciens, son usage est assujetti à une demande de dérogation justifiant d’une rejointe vers un environnement non dérogatoire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n’exonere pas du respect des règles de l’Intradef et de facto, n’autorise pas son emploi au travers d’ISPT

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
RPA	UiPath	UiPath	2023.4	D	O	D	O							D		26/04/25	26/04/26	Cette technologie devant être considérée comme un moyen temporaire d’amélioration du fonctionnement de dispositifs anciens, son usage est assujetti à une demande de dérogation justifiant d’une rejointe vers un environnement non dérogatoire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n’exonere pas du respect des règles de l’Intradef et de facto, n’autorise pas son emploi au travers d’ISPT

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
RPA	UiPath	UiPath	2024.10	A	S	A	S							A		24/10/26	24/10/27	Cette technologie devant être considérée comme un moyen temporaire d’amélioration du fonctionnement de dispositifs anciens, son usage est assujetti à une demande de dérogation justifiant d’une rejointe vers un environnement non dérogoaire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n’exonere pas du respect des règles de l’Intradef et de facto, n’autorise pas son emploi au travers d’ISPT

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
RPA	UiPath	UiPath	2025.10	A	S	A	S							A		27/10/27	27/10/28	Cette technologie devant être considérée comme un moyen temporaire d'amélioration du fonctionnement de dispositifs anciens, son usage est assujetti à une demande de dérogation justifiant d'une rejointe vers un environnement non dérogoaire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n'exonere pas du respect des règles de l'Intradef et de facto, n'autorise pas son emploi au travers d'ISPT
Sauvegarde	MIRIA (ADA)	Atempo	3.15	D	O	I	N											
Sauvegarde	MIRIA (ADA)	Atempo	4.2	R	S	R	S											
Sauvegarde	Proxmox Backup Server	Proxmox Server Solutions GmbH	3	A	N	I	N	A	N	A	N	I	N					Assujetti à l'usage de Proxmox VE
Sauvegarde	Time Navigator (TINA)	Atempo	4.7	I	N	I	N							I		30/11/24		Pour les données structurées avec sauvegarde bande / Par défaut en offre VPS

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Sauvegarde	Time Navigator (TINA)	Atempo	4.8	R	S	R	S							R				Pour les données structurées avec sauvegarde bande / Par défaut en offre VPS
Sauvegarde	Veeam Backup & Replication	Veeam	11	I	N	I	N	I	N	I	N			I		31/01/23	31/01/24	
Sauvegarde	Veeam Backup & Replication	Veeam	12	R	S	R	S	R	S	R	S			R			31/01/26	
Sécurité	Sysmon	Microsoft		R	S	R	S	R	S	R	S	R	S	R				Gestion de l'activité système
Serveur d'application	Tomcat	Apache Software Foundation	10.0	I	N	I	N	I	N	I	N	I	N	I		30/10/22		Version obsolète Même statut sur intrasan
Serveur d'application	Tomcat	Apache Software Foundation	10.1	R	S	R	S	R	S	R	S	R	S	R				implémente les spécifications Java EE 10 : Servlet 6.0, JSP 3.1, EL 5.0 et WebSocket 2.1 Compatible java 11 et + Même statut sur intrasan
Serveur d'application	Tomcat	Apache Software Foundation	11	R	S	R	S	R	S	R	S	R	S	R				Compatible java 17 et + Même statut sur intrasan
Serveur d'application	Tomcat	Apache Software Foundation	8.5	I	N	I	N	I	N	I	N	I	N	I		30/03/24		implémente les spécifications Java EE 7 : Servlet 3.1, JSP 2.3, EL 3.0 et WebSocket 1.0 Compatible java 7 et + Même statut sur intrasan

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Serveur d'application	Tomcat	Apache Software Foundation	9	R	S	R	S	R	S	R	S	R	S	R		03/10/27		implémente les spécifications Java EE 8 (JASPIC 1.1) : Servlet 4.0, JSP 2.3, EL 3.0 et WebSocket 1.1 Compatible java 8 et + Même statut sur intrasan
Serveur d'impression	CUPS	OpenPrinting																Service d'impression bord du SIE. Assujetti au SIE.
Serveur HTTP / Proxy HTTP / Cache HTTP	HTTP Server	Apache Software Foundation	2.2	I	N	I	N	I	N	I	N	I	N	I				Même statut sur Intrasan
Serveur HTTP / Proxy HTTP / Cache HTTP	HTTP Server	Apache Software Foundation	2.4	R	S	R	S	R	S	R	S	R	S	R				Même statut sur Intrasan
Serveur HTTP / Proxy HTTP / Cache HTTP	IIS	Microsoft	10													11/01/27		Assujetti au déploiement de solutions adhérentes à l'écosystème Microsoft. Cf la version de windows serveur utilisée pour le statut et les dates de fin de vie.
Serveur HTTP / Proxy HTTP /	IIS	Microsoft	8.5	I	N	I	N	I	N	I	N	I	N	I		09/10/23		Version pour Windows Server 2012 R2
Serveur HTTP / Proxy HTTP / Cache HTTP	Nginx	Nginx	1.26	I	N	I	N	I	N	I	N	I	N	I				Même statut pour les versions mineures paires (1.x) précédentes.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Serveur HTTP / Proxy HTTP / Cache HTTP	Nginx	Nginx	1.27	I	N	I	N	I	N	I	N	I	N	I				Les versions impaires sont des versions mainline, et peuvent contenir des modules expérimentales. À ce titre, seules les versions paires, dites stables, sont autorisées.
Serveur HTTP / Proxy HTTP / Cache HTTP	Nginx	Nginx	1.28	R	S	R	S	R	S	R	S	R	S	R				Largement utilisé sur l'Internet . À justifier par rapport à Httpd Apache. Assujetti sur Intrasan
Serveur HTTP / Proxy HTTP /	Varnish Cache	Varnish Software	6.0	R	S	R	S	R	S	R	S	R	S					Les versions mineures suivantes sont interdites.
Serveur HTTP / Proxy HTTP / Cache HTTP	Varnish Cache	Varnish Software	7.6	I	N	I	N	I	N	I	N	I	N			15/09/25		Les versions mineures précédentes sont interdites.
Serveur HTTP / Proxy HTTP / Cache HTTP	Varnish Cache	Varnish Software	7.7	D	N	D	N	D	N	D	N	I	N			15/03/26		Les versions mineures précédentes sont interdites.
Serveur HTTP / Proxy HTTP / Cache HTTP	Varnish Cache	Varnish Software	8.0	D	N	D	N	D	N	D	N	D	N			15/09/26		Les versions mineures précédentes sont interdites.
Serveurs d'application Java	Jetty	Eclipse	11	I	N	I	N					I	N	I		31/12/23		Assujetti à des cas d'usage de micro-services implémente les spécifications Java EE 9 : Servlet 5.0. Nécessite un openJDK en version 11 ou +.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Serveurs d'application Java	Jetty	Eclipse	12	A	N	A	N							A				Assujetti à des cas d'usage de micro-services implémente les spécifications Java EE 8, 9 et 10. Nécessite un openJDK en version 17 ou +.
Serveurs d'application Java et d'EJB	Glassfish	Oracle	6	D	O	I	N					I	N	D				Privilégier Payara / Wildfly À partir de la version 6.1, implémente JakartaEE 9.1. Nécessite openJDK 11 ou 17.
Serveurs d'application Java et d'EJB	Glassfish	Oracle	7	D	O	I	N					I	N	D				Privilégier Payara / Wildfly Implémente JakartaEE 10. Nécessite openJDK 11 ou 17 ; le 17 est nécessaire à l'utilisation de MicroProfile.
Serveurs d'application Java et d'EJB	Jboss EAP	Redhat	6	I	N	I	N					I	N	I		29/06/19	29/06/22	Assujetti à une exigence de support.
Serveurs d'application Java et d'EJB	Jboss EAP	Redhat	7	D	O	D	O					I	N	D		29/06/25	29/11/26	Assujetti à l'usage de JakartaEE et à une exigence de support.
Serveurs d'application Java et d'EJB	Jboss EAP	Redhat	8	A	S	A	S					A	S	A		05/02/31	05/02/33	Assujetti à l'usage de JakartaEE et à une exigence de support. Même statut sur Intrasan
Serveurs d'application Java et d'EJB	Payara Server	Payara Services Ltd	5	I	N	I	N					I	N	I		29/11/22		Implémente JakartaEE 8. Nécessite un OpenJDK en version 8, 11 ou 17.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Serveurs d'application Java et d'EJB	Payara Server	Payara Services Ltd	6	D	O	I	N					I	N	D		31/12/27	31/12/32	Implémente JakartaEE 10. Nécessite un OpenJDK en version 11, 17 ou 21. La fin de vie jusqu'en 2032 n'est valable que pour un JRE 11. Pour les JRE 17 et 21, leur fin de vie respective sont 30/09/2029 et 30/09/2031.
Serveurs d'application Java et d'EJB	TomEE	Apache Software Foundation	10	A	S	A	S					A	S	A				Assujetti à l'usage de JarkartaEE.
Serveurs d'application Java et d'EJB	TomEE	Apache Software Foundation	9	I	N	I	N					I	N	I		31/12/24		Tomcat reconfiguré pour supporter aisément les EJB
Serveurs d'application Java et d'EJB	Wildfly	Redhat	37	I	N	I	N	I	N	I	N	I	N	I				Attention : seule la dernière version mise à disposition par l'éditeur est tolérée. Le cycle de vie d'une version (2-3 mois) est plus court que celui du CCT. En conséquence, la version affichée comme déconseillée dans le CCT peut être de facto interdite. Pour une application Jakarta EE, il faut mieux utiliser TomEE ou JBOSS EAP. Cette dernière solution est soumise à une licence payante.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Serveurs d'application Java et d'EJB	Wildfly	Redhat	38	D	O	I	N	D	O	D	O	I	N	D				Attention : seule la dernière version mise à disposition par l'éditeur est tolérée. Le cycle de vie d'une version (2-3 mois) est plus court que celui du CCT. En conséquence, la version affichée comme déconseillée dans le CCT peut être de facto interdite. Pour une application Jakarta EE, il faut mieux utiliser TomEE ou JBOSS EAP. Cette dernière solution est soumise à une licence payante.
SGBDR	Galera Cluster	Codership		R	S	R	S					R	S	R				Versions : celles embarquées dans les versions recommandées de MariaDB.
SGBDR	MariaDB	MariaDB Foundation	10.11	A	S	A	S	A	S	A	S	A	S	A		15/02/28		Assujetti à l'impossibilité d'utiliser PostgreSQL Même statut sur Intrasan
SGBDR	MariaDB	MariaDB Foundation	10.6	D	O	D	O	D	O	D	O	I	N	D		05/07/26		Assujetti à l'impossibilité d'utiliser PostgreSQL Assujetti sur Intrasan
SGBDR	MariaDB	MariaDB Foundation	11.4	A	S	A	S	A	S	A	S	A	S	A		29/05/29	16/01/33	Assujetti à l'impossibilité d'utiliser PostgreSQL Le support étendu est un support commercial, et donc payant.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
SGBDR	MariaDB	MariaDB Foundation	11.7	I	N	I	N	I	N	I	N	I	N	I				Version non LTS - déconseillée. Même status pour les versions antérieures, sauf mention contraire.
SGBDR	MariaDB	MariaDB Foundation	11.8	A	S	A	S	A	S	A	S	A	S	A		04/06/28	15/10/33	Assujetti à l'impossibilité d'utiliser PostgreSQL. Attention, suite à un changement de politique, le support communautaire de la 11.8 se termine avant celui de la 11.4. Le support étendu est un support commercial, et donc payant.
SGBDR	MySQL	Oracle	8.0	D	N	I	N	D	N	D	N	I	N			31/03/25	31/03/26	Qu'est-ce qu'on en fait ? On le passe en interdit, et on espère que MariaDB tienne le coup ? On le conserve en déconseillé et on temporise ? Si on temporise, on peut accepter la version 8.4 (LTS). Et je dois rajouter un commentaire pour préciser que sauf mention contraire, les autres versions sont interdites. Interdit sur Intrasan

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
SGBDR	MySQL	Oracle	8.4	D	N	D	N	D	N	D	N	D	N					Les autres versions sont interdites. Le recours à postgresSQL, ou à défaut à mariaDB, doit être systématiquement privilégié. Interdit sur Intrasan
SGBDR	Oracle Database	Oracle	12.2	I	N	I	N					I	N	I		30/07/18	30/03/22	Dernière version : 12.2.0.1 La fin du support étendue est valable avec ES/ULA. Emploi à dûment justifier pour les nouveaux projets, migration à envisager pour les anciens. (*) Soutien uniquement sur structures mutualisées (Exadata)
SGBDR	Oracle Database	Oracle	19c	D	O	D	O					D	O	A		31/12/29	31/12/32	L'usage d'une base de données Oracle nécessite une licence adaptée à un déploiement sur un environnement virtualisé mutualisé. À défaut, il faut partir sur une infrastructure dédiée, donc en salle blanche. Pour rappel, un déploiement en salle blanche implique de prévoir une TME. Interdit sur Intrasan
SGBDR	Oracle Database	Oracle	21c	I	N	I	N					I	N	I				Version innovation (non LTS)

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
SGBDR	Oracle Database	Oracle	23ai	D	O	D	O					D	O			31/12/31		L'usage d'une base de données Oracle nécessite une licence adaptée à un déploiement sur un environnement virtualisé mutualisé. À défaut, il faut partir sur une infrastructure dédiée, donc en salle blanche. Pour rappel, un déploiement en salle blanche implique de prévoir une TME.
SGBDR	pgAdmin4	PostgreSQL Global Development Group	8	A										A				Assujetti aux usages non couverts par DBeaver
SGBDR	PostGIS	PostGIS	3.0	I	N	I	N					I	N	I		12/11/25		Compatible postgresQL 11, 12 et 13.
SGBDR	PostGIS	PostGIS	3.1	D	O	D	O					I	O	D		11/11/26		Compatible postgresQL 11, 12, 13 et
SGBDR	PostGIS	PostGIS	3.2	A	S	A	S					A	S	A		10/11/27		Compatible postgresQL 11, 12, 13, 14
SGBDR	PostGIS	PostGIS	3.3	A	S	A	S					A	S	A		08/11/28		Compatible postgresQL 11, 12, 13,
SGBDR	PostGIS	PostGIS	3.4	A	S	A	S					A	S	A		08/11/28		Compatible postgresQL 12, 13, 14, 15
SGBDR	PostGIS	PostGIS	3.5	A	S	A	S					A	S	A		08/11/29		Compatible postgresQL 12, 13, 14,
SGBDR	PostGIS	PostGIS	3.6	A	S	A	S					A	S	A				Compatible postgresQL 12, 13, 14,
SGBDR	PostgreSQL	PostgreSQL Global Development Group	13	I	N	I	N	I	N	I	N	I	N	I		12/11/25		Version : 13 dans Ruche Sur HELISS-NG : version portée par Redhat 7 et Redhat 8

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
SGBDR	PostgreSQL	PostgreSQL Global Development Group	14	D	O	D	O	D	O	D	O	I	N	D		29/09/26		Recommandé sur Intrasan
SGBDR	PostgreSQL	PostgreSQL Global Development Group	15	R	S	R	S	R	S	R	S	R	S	R		10/11/27		Recommandé sur Intrasan
SGBDR	PostgreSQL	PostgreSQL Global Development Group	16	R	S	R	S	R	S	R	S	R	S	R		09/11/28		Recommandé sur Intrasan
SGBDR	PostgreSQL	PostgreSQL Global Development Group	17	R	S	R	S	R	S	R	S	R	S	R		08/11/29		Recommandé sur Intrasan
SGBDR	SQL Server	Microsoft	2012	I	N	I	N	I	N	I	N	I	N	I		10/07/17	11/07/22	Un changement de version ou une sortie doit être envisagée. Dernier service pack : SP4
SGBDR	SQL Server	Microsoft	2014	I	N	I	N					I	N	I		08/07/19	08/07/24	Dernier service pack : SP3
SGBDR	SQL Server	Microsoft	2016	A	S	A	S	A	S	A	S			A		12/07/21	13/07/26	Dernier service pack : SP3
SGBDR	SQL Server	Microsoft	2017	A	N	A	N	A	N	A	N			A		10/10/22	11/10/27	
SGBDR	SQL Server	Microsoft	2019	A	S	A	S	A	S	A	S	A	S	A		27/02/25	07/01/30	Sur C1NP : A/S si déployé sur linux Même statut sur Intrasan
SGBDR	SQL Server	Microsoft	2022	E		E		E		E						10/01/28	10/01/33	

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
SGBDR	SQLite	SQLite		A										A				Même statut sur Intrasan
SSO	FranceConnect Particulier	DINUM																Pour un besoin générique sans nécessité de savoir que l'utilisateur est un agent ou un ayant droit du ministère. Est soutenu par la DINUM. Est disponible au travers de MindefConnect Internet ou directement sur le C3NP.
SSO	Kerberos	Microsoft		A	S	A	S	R	S	R	S	I	N	A				
SSO	Keycloak	Redhat	25	I	N	I	N					I	N	I		03/10/24		Assujetti pour tout autre usage que MindefConnect sur intradef
SSO	Keycloak	Redhat	26	A	S	A	S					I	N	A				Assujetti pour tout autre usage que MindefConnect sur intradef
SSO	MindefConnect Internet	MinArm										R	S					Basé sur RedHatSSO
SSO	MindefConnect Intradef	MinArm		R	S	R	S											Basé sur RedHatSSO
SSO	MindefConnect Secret	MinArm						E	E									Basé sur RedHatSSO.
SSO	Red Hat Single Sign-On	Redhat	7	I	N									I		29/06/22	29/06/25	Assujetti pour tout autre usage que MindefConnect si besoin de support Changement de nom : devient RHBK (RedHat Build of Keycloak)

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
SSO	RHBK	Redhat	26	A	S	A	S							A		13/05/26	13/11/26	Red Hat Build for Keycloak, anciennement Red Hat SSO Assujetti pour tout autre usage que
SSO	Sign&Go	Ilex	5.1					A	S	A	S							Assujetti aux cas d'utilisation en cours.
SSO/Authentification mutualisée	FreelPA		4															Assujetti aux réseaux IST/I3E uniquement
SSO/Authentification mutualisée	Web services Annudef	MinArm		D	O	I	N							D				
Stockage	CSI vSphere	VMWare		A	N			A	N	A	N			A				Permet de monter des disques vSphere sur les nœuds d'un cluster Kubernetes afin de créer des volumes persistants. Infra hors cloud C1, requis quand sous-jacent VMWare notamment pour Kasten et Velero.
Stockage	IRIS	MinArm		R	S	R	S	E	E									Stockage objet de fichiers et métadonnées au travers du protocole S3 et de données froides (archivage, sauvegarde). En cours d'intégration sur le SIA.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Stockage	MinIO			D	N	D	N	D	N	D	N	D	N	D				Stockage objet de fichiers et métadonnées au travers du protocole S3 et de données froides (archivage, sauvegarde). Assujetti à des cas d'emploi ne permettant pas de recourir aux instances IRIS existantes
Stockage	Portworx	Pure Storage	3.1	I	N	I	N	I	N	I	N			I		31/07/24	31/07/25	Solution de gestion de stockage sur
Stockage	Portworx	Pure Storage	3.2			D	N	D	N	D	N			D		30/04/25	30/04/26	Solution de gestion de stockage sur
Stockage	Portworx	Pure Storage	3.3			I	N	I	N	I	N			I		23/12/25		Solution de gestion de stockage sur
Stockage	Portworx	Pure Storage	3.4			A	N	A	N	A	N			A		08/03/26	08/03/27	Solution de gestion de stockage sur
Stockage	Scality Ring			A	S			E	E					A				Pour IRIS.
Supervision	Fluentd	CNCF	6.0	A	N	I	N	A	N	A	N	I	N			31/12/27		Solution d'uniformisation de collecte et de centralisation de logs La version indiquée est celle de fluent package. Cf Prometheus pour les cas d'usage.
Supervision / Observabilité	Prometheus	CNCF	2.53	I	N	I	N	I	N	I	N	I	N			31/07/25		Solution de collecte et centralisation de métriques

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Supervision / Observabilité	Prometheus	CNCF	3.5	A	N	I	N	A	N	A	N	I	N			31/07/26		Solution de collecte et centralisation de métriques. Seules les versions LTS sont acceptables. Est assujéti à des contextes ne permettant pas l'usage du SI Observabilité, et à l'emploi du mode push-based
Synchronisation	NTP	Meinberg	4.2.8	A	N	A	N	A	N	A	N			A				
Synchronisation	NTPd/Chronyd			R	S	R	S	R	S	R	S	R	S	R				Sur les OS Linux
Système d'exploitation	Android	Google	10	I										I		05/03/23		Assujéti aux SMOBI Nom alternatif de la version : Queen Cake
Système d'exploitation	Android	Google	11	D										D		05/02/24		Assujéti aux SMOBI Nom alternatif de la version : Red Velvet Cake
Système d'exploitation	Android	Google	12	I										I		31/03/25		Assujéti aux SMOBI Nom alternatif de la version : Snow Cone
Système d'exploitation	Android	Google	13 (Tiramisu)	A										A				Assujéti aux SMOBI
Système d'exploitation	Android	Google	14 (Upside-down cake)	A										A				Assujéti aux SMOBI

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Système d'exploitation	Android	Google	15 (Vanilla Ice Cream)	E										E				Les premiers SMOBI en v15 sont attendus pour le T1 2026
Système d'exploitation	RedHat Enterprise Linux	Redhat	10			E	E	E	E	E	E	E	E					
Système d'exploitation	RedHat Enterprise Linux	Redhat	7	I	N	I	N	I	N	I	N	I	N	I		29/06/24		Même statut sur Intrasan
Système d'exploitation	RedHat Enterprise Linux	Redhat	8.10	A	S	A	S					R	S			30/05/29		Les versions mineures (8.x) précédentes sont interdites. Il est préconisé de favoriser l'usage d'Alma Linux sur intradef. 8.9 Assujetti sur Intrasan
Système d'exploitation	RedHat Enterprise Linux	Redhat	9	A	S	A	S					A	S			30/05/29		Assujetti à l'impossibilité d'utiliser la 8.10. Seule la dernière version mineure est autorisée (9.x). Les versions mineures paires (9.2, 9.4...) peuvent bénéficier d'un support commercial de deux ans. Recommandé sur Intrasan

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Système d'exploitation	Ubuntu	Communauté Ubuntu	22.04									A	S			31/03/27	31/03/32	Uniquement pour les postes surf ASTEL-I Nom alternatif de la version : Jammy Jellyfish
Système d'exploitation	Ubuntu	Communauté Ubuntu	24.04									A	S			31/03/29	31/03/34	Uniquement pour les postes surf ASTEL-I Nom alternatif de la version : Noble Numbat
Système d'exploitation	Windows	Microsoft	10	D				R		R				R				Pour les intranets classifiés, sauf exception dûment justifiée, c'est la branche SAC qui est préconisée
Système d'exploitation	Windows	Microsoft	11	R				E		E				R				Master LTSC 2024 attendu sur le Secret fin S2 2026. De manière générale, l'emploi du canal LTS pour des postes hors gestion CND est recommandée.
Système d'exploitation	Windows	Microsoft	7	I		I		A		A		I		I		12/01/15	13/01/20	Assujetti à un emploi sur le segment Secret et FrOps. Migration vers windows 10 en cours. Windows 7 sera interdit à l'issue
Système d'exploitation	Windows	Microsoft	8	I		I		I		I		I		I			11/01/16	
Système d'exploitation	Windows	Microsoft	8.1	I		I		I		I		I		I		08/01/18	09/01/23	

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Système d'exploitation poste client	Windows	Microsoft	xp	I		I		I		I		I		I		13/04/09	07/04/14	
Système d'exploitation serveur	AlmaLinux	Almalinux OS	10			E	E	E	E	E	E	E	E	E				Une nouvelle version sort tous les 6 mois.
Système d'exploitation serveur	AlmaLinux	Almalinux OS	8.10	R	S	R	S	E	E	E	E	E	E	R		30/05/29		Assujetti sur Intrasan
Système d'exploitation serveur	AlmaLinux	Almalinux OS	9			A	S	E	E	E	E	A	S	A		30/05/32		Seule la dernière version mineure (9.x) est acceptable. Une nouvelle version sort tous les 6 mois.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Système d'exploitation serveur	CentOS	Communauté CentOS	7.9	D	O			D	O	D	O	D	O	D		29/06/24		Les versions mineures précédentes (7.8 et précédentes) sont interdites. Le support des systèmes d'exploitation Centos a été arrêté par RedHat en juin 2024. La DIRISI a toutefois souscrit une prolongation de support LibertyLinux de 3 ans de Centos 7.9 afin de permettre aux systèmes d'information de satisfaire à l'ensemble des prérequis C1DR sans passer par une étape intermédiaire de montée en version de système d'exploitation. Cette prolongation ne sera pas reconduite.
Système d'exploitation serveur	CentOS	Communauté CentOS	8	I	N	I	N	I	N	I	N	I	N	I				Le support de CentOS est abandonné par RedHat/IBM à partir de décembre 2021. L'usage de CentOS 8 est donc désormais interdit.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Système d'exploitation serveur	Debian	Communauté Debian	10	I	N	I	N					I	N	I		09/09/22	29/06/24	DEBIAN uniquement recommandé sur SIE (embarqué Marine nationale) - Attention distribution en fin de vie. Nom alternatif de la version : Buster
Système d'exploitation serveur	Debian	Communauté Debian	11	D	N	I	N					I	N	D		30/06/24	29/06/26	Elle reste strictement assujettie à une justification du cadre d'emploi sur l'Intradef et la prise en charge du MCO/MCS Nom alternatif de la version : Bullseye
Système d'exploitation serveur	Debian	Communauté Debian	12	D	N	I	N					I	N	D		09/06/26	09/06/28	DEBIAN assujetti aux cas d'usage sur SIE (embarqué Marine nationale) et aux composants du socle technique. Nom alternatif de la version : Bookworm
Système d'exploitation serveur	Debian	Communauté Debian	13	A	N	I	N					I	N	D		09/08/28	30/06/30	DEBIAN assujetti aux cas d'usage sur SIE (embarqué Marine nationale) et aux composants du socle technique. Nom alternatif de la version : Trixie

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Système d'exploitation serveur	Windows Server	Microsoft	2012 R2	I	N	I	N	I	N	I	N	I	N	I		08/10/18	09/10/23	3 extensions de mises à jour de sécurité sont attendues. la dernière, "Extended Security Update Year 3", prévu pour le 15/10/2025, étendra le support jusqu'au 13/10/2026. Interdit sur Intrasan
Système d'exploitation serveur	Windows Server	Microsoft	2016	D	O	D	O	D	O	D	O	I	N	D		10/01/22	11/01/27	Assujetti au déploiement de solutions adhérentes à l'écosystème Microsoft. Sur intradef, il n'est disponible que sur l'hébergement historique, et pas sur le C1DR. Il est préférable de partir sur une version plus récente. Interdit sur Intrasan
Système d'exploitation serveur	Windows Server	Microsoft	2019	A	S	A	S					A	S	A		08/01/24	08/01/29	Assujetti au déploiement de solutions adhérentes à l'écosystème Microsoft Même statut sur Intrasan
Système d'exploitation serveur	Windows Server	Microsoft	2022	A	S	A	S			E	E			A		12/10/26	13/10/31	Assujetti aux briques du socle adhérentes à l'écosystème Microsoft. Recommandé sur Intrasan

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Système d'exploitation serveur	Windows Server	Microsoft	2025			E	E					E	E			13/11/29	14/11/34	Assujetti aux briques du socle adhérentes à l'écosystème Microsoft.
Tableau Blanc	Lync Live	Microsoft		I	N	I	N	D		D		I	N	I				

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Traducteur Ruby en Java	JRUBY			A		A		A		A		A		A				Nécessaire pour pour traduire en bytecode Java une application Ruby pour la Production Le langage Ruby et RAILS sont marginaux dans le domaine des SIAG. C’est pourquoi, il n’est pas recommandé ici. Néanmoins, dès lors que la pré-intégration sur PICSEL permet de réaliser un BUILD avec JRuby et une Production ensuite dans un environnement d’exécution Java, cette option de développement devient autorisée. Par « assujetti », on entend vérifier si un autre langage que Ruby peut être utilisé pour le SI Cible concerné et si Ruby est confirmé, que JRuby sera effectivement employé. Comme certains GEMs Ruby sont incompatibles avec JRuby, il est de la responsabilité de la DSI Domaine et de l’équipe projet de vérifier que de tels GEMs ne seront pas utilisés pendant le développement.

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Traduction	REVERSO	Reverso						D		D								
Traduction	SYSTRAN Pure Neural Server (SPNS)		9	A	S	A	S	A	S					A				- Traduction neuronale disponible pour 55 langues, portail de traduction, web services (API REST) - Intègre nativement un OCR, en option connecteur possible vers un outil de transcription de la parole - Mode SaaS (souverain européen OVH) ou on-premise (CPU ou GPU) - Outil non soumis à des restrictions export ni à des juridictions extra-européennes - Intégré dans ARTEMIS.IA

Annexe CCT v3.7.0 - 2026- Pile logicielle générale				Intradef		C1DR		SIA S-SF		SIA FrOpS		C1NP		I3E				
Catégorie	Logiciel	Éditeur	Version	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Recom. AGORA	Soutien CND	Date de fin de support	Date de fin de support étendu	Commentaire
Transfert de données volumineuses	France Transfert	DINUM																Service internet soutenu par la DINUM https://www.numerique.gouv.fr/outils-agents/france-transfert/
Wiki	DokuWiki																	Assujetti au contexte SIE : Déployé dans le cadre du SIE
Wiki	MediaWiki	Wikimedia Foundation	1.39	I	N	I	N							I		29/11/25		Assujetti à l'usage de wikidefense ou de TULEAP LTS
Wiki	MediaWiki	Wikimedia Foundation	1.43	A	N	A	N							A		31/12/27		Assujetti à l'usage de wikidefense ou de TULEAP LTS
Wiki	xWiki		15	I	N	I	N	I	N	I	N	I	N	I				
Wiki	xWiki		16.10	A	N	A	N	R	N	R	N	R	N	A				Les autres versions mineures (16.1, 16.2...) sont interdites. Sur intradef, il est assujetti aux cas d'usage non satisfaits par TULEAP.
Wiki	xWiki		17	D	N	I	N	D	N	D	N	I	N	D				La 17.10 passera en assujetti sur Intradef et C1DR, et en Recommandé sur les autres segments.