Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE
L'INTÉRIEUR

Cadre de cohérence technique
du ministère de l'intérieur

Guide d'intégration

cctmi

Table des matières

Versions du document 1.1
Introduction 1.2
Pilier utilisateur 1.3
- Gestion de l'identité de l'usager 1.3.1
- Gestion de l'identité de l'agent 1.3.2
- Gestion de l'identité de la personne morale 1.3.3
- L'environnement numérique de travail de l'agent 1.3.4
- La qualité du parcours de l'utilisateur 1.3.5

Pilier données et API 1.4
- Données et services 1.4.1
- Gestion des échanges 1.4.2
- Analyser et valoriser les données 1.4.3
- Données personnelles 1.4.4
- Cycle de vie des données 1.4.5

Pilier sécurité 1.5
- SSI et homologation 1.5.1

Pilier fabrique de code 1.6
- Forges d'intégration et de déploiement continu 1.6.1

Pilier hébergement 1.7
- Mise en place d'un hébergement 1.7.1

Pilier services transverses 1.8
- Synthèse des services 1.8.1

Versions du document

Version du CCT	Date de modification du document	Auteurs
3.0	Mars 2019	JC Bastoul
3.0.2	Juin 2019	JC Bastoul
3.0.3	Décembre 2019	JC Bastoul
3.0.3a	Décembre 2019	JC Bastoul
3.0.4	Juillet 2020	JC Bastoul
3.0.5	Octobre 2020	JC Bastoul
3.0.6	Décembre 2020	JC Bastoul
3.1.0	Juillet 2023	D SCEMAMA
3.1.1	Août 2024	H DRISS
3.1.2	Juillet 2025	H DRISS
3.1.3	Septembre 2025	H Driss

Guide d'intégration d'une application dans l'écosystème ministériel

Introduction

Une application, avec son contexte qui lui est propre, doit pouvoir s'interfacer avec l'ensemble des outils, processus, chaînes de services, permettant d'assurer son maintien en condition au sein du système d'information du ministère, et de celui de l'État. Plus précisément :

- l'application aura tout bénéfice à utiliser des **communs**, composants et services existants qu'il convient de ne pas réécrire, avec pour ne citer que celles-ci, les fonctions d'identification et d'authentification des utilisateurs, les services de confiance (signature électronique, horodatage...), les services d'archivage, etc.
- l'application pourra, plutôt que de les recréer, réutiliser les **données** existantes, voire des traitements de ces données ; à l'inverse, elle peut être amenée à rendre disponible les données ou traitements qu'elle va créer,
- l'application doit être sécurisée,
- et bien sûr, l'application doit pouvoir être exploitée, hébergée, soutenue à moindre coût par les professionnels qui assurent ces services

Le guide d'intégration se focalise sur l'intégration de l'application au sein du SI de l'Administration. Il ne traite pas de son architecture technico-fonctionnelle.

Structure du document

Le guide liste les 6 piliers d'une intégration réussie :

1. les utilisateurs (usagers comme agents) - PU,
2. les données et les API - PD,
3. la sécurité - PS,
4. la fabrique de code - PF
5. l'hébergement - PH,
6. les services transverses - PA.

Chacun de ces piliers sera décliné en domaines et chaque domaine fait l'objet d'une fiche.

Chaque pilier est constitué de plusieurs Domaines, qu'il est nécessaire de couvrir pour favoriser l'homologation de l'application.

Chaque fiche, relevant d'un pilier et d'un domaine, est structurée de la façon suivante :

- le **principe recherché**
- les **impacts sur l'application**
- les **règles et recommandations** : nous conservons ici la même signification que dans le CCT historique (pré V3). Les règles s'imposent, les recommandations sont à comprendre comme des bonnes pratiques.
- **informations utiles** : le guide se veut avant tout une aide à l'acteur ministériel. Celui-ci trouvera dans ce pavé d'information tous les liens vers des éléments pouvant lui faciliter la tâche : contacts, offres de service, ressources utiles, zones d'échange et de collaboration ...

Les piliers de l'intégration

Le tableau qui suit liste les 6 piliers d'une intégration réussie, mentionnés plus haut, et les décline de façon plus précise en domaines à couvrir. Dans une phase de dégrossissage, ce tableau peut servir de check list pour le chef de projet et lui permettre d'éviter des surprises au moment de l'intégration ou de la mise en production.

Piliers	Fiches de domaine	Check
1 - Utilisateur (personne physique ou morale, usager ou agent) - PU	1 - Gestion de l'identité des usagers	
	2 - Gestion de l'identité des agents	
	3 - Gestion de l'identité des personnes morales	
	4 - L'environnement de travail numérique de l'utilisateur (ENTA pour l'agent)	
	6 - Qualité du parcours utilisateur	
2 - Données & API - PD	1 - Données et services	
	2 - Gestion des échanges	
	3 - Analyser et valoriser les données	
	4 - Données personnelles	
	5 - Cycle de vie de la donnée / Archivage	
3 - Sécurité - PS	1 - La sécurité (SSI, DISSIP, PSSI...) et l'homologation	
4 - Fabrique de code - PF	1 - Forges d'intégration et de déploiement continus	
5 - Hébergement - PH	1 - Mise en place d'un hébergement	
6 - (Autres) Service transverse -PA	1 - Synthèse des services transverses	

Remarque : a noter que les aspects "chaine de soutien utilisateur" (domaine 4 du pilier 1) et "services de supervision" (domaine 2 du pilier 5) n'ont pas été adressés dans cette version du document.

Pilier utilisateur - Introduction

L'utilisateur, qu'il soit un usager / citoyen, un agent, une entreprise ou une association (dans les deux cas une personne morale) doit être le premier souci du concepteur d'une nouvelle application.

Le service offert par l'application à l'utilisateur s'appuie sur 4 concepts structurants clés:

- L'usage de fonctions d'identification et d' authentification centralisés et externes à l'application
- L'environnement de travail (ou Environnement de Travail Numérique de l'Agent)
- Le soutien à l'utilisateur
- La prise en compte de l'expérience utilisateur et de l'accessibilité du service

A partir de ces 4 concepts clés, 6 domaines sont à mettre en œuvre :

1. Identification de l'usager / citoyen
2. Identification de l'agent
3. Identification d'une personne morale (association ou entreprise)
4. L'environnement de travail numérique de l'agent
5. [cf. remarque plus bas]
6. Prise en compte de l'expérience usager, tout au long du cycle de vie du service

PS : le domaine 5 (Mise en place d'une chaîne de soutien à l'utilisateur) n'est pas traité dans la version du CCT actuel.

Usager : gestion des identifications / authentifications

Principe recherché

Les applications ouvertes au public nécessitent une **identification** de l'usager, ainsi que son **authentification**. Ces fonctions sont fournies au travers des solutions centralisées, basées sur des protocoles standard du marché.

La DINUM, en utilisant le protocole sous-jacent OpenID Connect, a conçu un fédérateur de SSO nommé **FranceConnect**.

Il a été décliné en plusieurs variantes :

- **FranceConnect** (objet de la suite de la fiche)
- FranceConnect+ (FranceConnect à authentification forte pour les démarches plus sensibles)
- AgentConnect, variante réservée aux agents publics.

Choix de l'identité

L'usager, sur tous les services mettant en œuvre le « bouton » FranceConnect, peut s'identifier auprès du fournisseur d'identité de son choix (FI) dans une liste de fournisseurs agréés . **Plusieurs niveaux d'authentification sont possibles**. Conformément au règlement européen eIDAS, l'usager peut choisir trois niveaux d'authentification, sous réserve que ceux-ci soient offerts par ses fournisseurs d'identité :

- niveau **faible**, suffisant pour la majorité des services, dans lequel l'authentification de l'utilisateur s'appuie sur un seul secret, généralement son mot de passe ;
- niveau **substantiel**, dans lequel l'authentification de l'usager est renforcée par un second facteur : SMS, mot de passe à usage unique (OTP One time password) ..etc ;
- niveau **élevé**, dans lequel l'authentification de l'usager est renforcée par un second facteur mettant en œuvre des moyens de sécurité forts (carte à puce, token, biométrie).

FranceConnect ne propose qu'un niveau faible. FranceConnect+, lui, propose un niveau substanciel à élevé.

Qualité de l'identité

Quel que soit le fournisseur d'identité et le niveau d'authentification, la qualité de l'identité de l'usager est garantie grâce à son croisement avec celle présente dans le RNIPP(Répertoire National d'Identification des Personnes) tenu par l'INSEE. A noter que le referentiel RNIPP de l'INSEE n'étant pas totalement fiable, des anomalies peuvent survenir lors du croisement entre FranceConnect/FranceConnect+ et celui-ci.

Gestion de l'identité dans l'application

L'identité doit se conformer aux exigences de FranceConnect/FranceConnect+, notamment le RGI (Référentiel Général d'Interopérabilité)

Référence : https://www.numerique.gouv.fr/publications/interoperabilite/

Avec FranceConnect/FranceConnect+, l'application reçoit l'identité pivot définie dans le RGI (nom, prénom, genre, date de naissance, lieu de naissance), accompagnés d'autres attributs selon les possibilités du fournisseur d'identité (adresse, adresse de messagerie, téléphone...), du niveau d'authentification utilisé et d'un identifiant unique et opaque de la personne propre à l'application (FranceConnect/FranceConnect+ génère, pour une même personne, des identifiants applicatifs différents pour empêcher le croisement des fichiers).

Impact pour les applications

L'identification et l'authentification des usagers ne doivent plus être prises en charge « en silo » au sein de l'application. Ces fonctions peuvent maintenant être mutualisées, à moindres frais, dans l'offre étatique FranceConnect/FranceConnect+. Le chef de projet pourra trouver des informations pratiques sur la mise en œuvre des SSO (y compris FranceConnect) dans la fiche dédiée.

Dans le cadre d'un raccordement à FranceConnect, l'application doit être capable d'assurer les fonctions suivantes :

- le stockage de l'identifiant opaque de FranceConnect,
- la procédure de réconciliation à la première connexion, c'est à dire d'appairage de l'identité pivot de FranceConnect avec celle connue de l'application,
- la vérification du niveau d'authentification, qui doit être supérieur ou égal au niveau requis par l'application. Par exemple, une application exigeant un niveau d'authentification substantiel acceptera un usager authentifié au niveau élevé, mais refusera un usager authentifié au niveau faible,
- les secrets FranceConnect sur les serveurs (authentification mutuelle application/FranceConnect)
- la gestion des cas d'erreur

Règles et recommandations

Ref	Statut	Intitulé
1166	RG	Les accès du grand public aux téléservices se font obligatoirement en TLS.
1344	RG	Pour réaliser le maintien d'une session authentifiée, seuls les mécanismes de cookie de session gérés par le langage (HTTPSession en Java par ex.) sont acceptés.
1435	rc	L'appairage de l'identité pivot de FranceConnect avec une identité connue de l'application, également appelé processus de réconciliation, peut intégrer la fourniture par l'usager d'une information complémentaire, vérifiable par l'application, et permettant de lever de potentielles ambiguïtés. Exemple : fourniture du numéro de permis dans le cadre de la démarche télépoint.

Informations utiles

Pour plus d'information, consulter le portail de service de la DTNUM : https://pi.interieur.rie.gouv.fr/

Contacts utiles

FranceConnect a été conçu et est opéré par la DINUM. L'espace pour les contacter : https://franceconnect.gouv.fr/faq#CONTACT

Offres de service

Site dédié aux partenaires (publics ou privés), c'est à dire tout organisme désirant utiliser FranceConnect comme fournisseur de service ou de données, ou se positionner en fournisseur d'identité : https://partenaires.franceconnect.gouv.fr

Ressources

« Comment ca marche ? » : https://franceconnect.gouv.fr

Agent : gestion des identifications / authentifications / autorisations

Contexte

Les applications nécessitent généralement une quadruple fonction regroupée en 2 catégories :

- le contrôle d'accès: **identification**, **authentification,**
- l'attribution de droits :**autorisation** et **habilitation** des utilisateurs / agents

Ces fonctions sont fournies au travers des solutions centralisées, basées sur des protocoles standards du marché.

Différents SSO existent par nature de populations :

- 4 SSO web ministériels, affectés à des populations identifiées : gendarmes, policiers, personnels de la préfecture de police, et tous agents du MI et prestataires longue durée.
- L' ProConnect, fédérateur de fournisseurs d'identités des agents publics, dans ses deux instances (ProConnect internet et ProConnect RIE).
- Pour les besoins d'authentification des postes de travail et applications client-serveur, plusieurs solutions d'authentification sont disponible ,basé sur Kerberos : les AD (Active Directory) pour les parcs d'ordinateurs Windows, ainsi que l'instance de Kerberos mise en œuvre pour le parc de postes Linux de la gendarmerie.

En cas d'inadéquation fonctionnelle, d'autres alternatives peuvent être mises en œuvre (ex. LDAP) et soumises obligatoirement à une validation du Comité d'architecture.

La suite de cette fiche se focalise sur les SSO web (pour ces derniers, quelques éléments sont disponibles dans l'annexe SSO.

Passage2 est intégré à ProConnect. Cependant ce SSO en tant que fournisseur d'identité de ProConnect ne sera visible que si des services applicatifs positionnent ce Fournisseur d'identité comme moyen d'accès possible.

La stratégie suivante doit être appliquée : Toute application ministérielle pouvant être utilisée par des agents externes au ministère, doit prendre en charge à minima deux SSO (web), plus étant recommandé :

- **l'un des 4 SSO ministériels**, pour les agents du ministère
- **ProConnect**, pour des agents publics identifiables par cette solution, ou, dans le cas contraire,via une solution SSO maitrisée par le domaine Métier

Il est nécessaire de s'assurer que le SSO soit accessible pour les populations ciblées, selon le positionnement réseau de l'application.

Le tableau suivant fait une synthèse des SSO à prendre en compte par les applications du ministère selon deux critères : le type de population, et réseau d'accès.

Accès	Agents MI (4 catégories)	Agents État non MI	Agents autres fonctions publiques	Agents non identifiés par leur organisme de rattachement
Accès intranet	L'un des 4 SSO du ministère sur un critère population : - PROXIMA pour les gendarmes - CHEOPS NG pour les policiers - [PASSAGE PP pour certains agents PP] - PASSAGE2 pour tous les agents restants	Pour les agents de l'État Hors MI dont le FI est déjà interfacé avec ProConnect, utiliser cette solution . Pour les autres populations d'acteurs, intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier ProConnect-RIE en cible	Intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier ProConnect-RIE en cible	Intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier
Accès RIE (inter-ministériel)	Passage2 (RIE) pour les agents MI, incluant la fonction de fédération	Pour les agents de l'État dont le FI est déjà interfacé avec ProConnect-RIE, utiliser cette solution. Pour les populations non couvertes, intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier ProConnect-RIE en cible	Sauf exception, ces agents arrivent par Internet. Pour ces cas d'exception, intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier ProConnect-RIE en cible	Intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier
Accès Internet	Privilégier les accès extranet via les solutions nomades. Pour l'accès direct à une application métier en tant qu'agent du ministère: Intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier	Pour les agents de l'État Hors MI dont le FI est déjà interfacé avec ProConnect, utiliser cette solution . Pour les autres populations d'acteurs.Intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier	Intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier ProConnect-Internet en cible	Intégrer la population ciblée dans une solution SSO maitrisée par le domaine Métier

ProConnect

La section qui précède a documenté le cas d'usage le plus simple : un agent du MI accédant à une application du MI sur son Intranet. Le tableau des cas d'usage de l'introduction liste plusieurs autres cas. Le SSO qui y apparaît, en cible est le plus souvent ProConnect dans ses deux instances, ProConnect internet et ProConnect RIE.

Le tiers de confiance ProcConnect, a été conçu par la DINUM. Le ministère positionne Passage2 en tant que Fournisseur de Services (FS) au regard d'ProConnect.

ProConnect est interfacé avec des composants existants et maitrisés au sein du ministère :

- il s'appuie sur les FI (Fournisseurs d'Identité) existants dans les SSO ministériels
- le protocole standard d'ProConnect, **OpenID Connect**, supporté par les fournisseurs de services de nos SSO ministériels

Le fichier en annexe décrit les cas de connexion des agents au travers d'internet qui pourraient mettre en oeuvre ProConnect.

Règles et recommandations

Ref	Statut	Intitulé
-	-	le tiers de confiance doit admettre à minima 1 fournisseur d’identité pour la population ciblée. Dans le cas contraire, veuillez solliciter les responsables interministeriels de la solutions ProConnect pour intégrer les fournisseurs d’identité adéquats.
1436	RG	L'identification de l'agent doit être conforme aux identités pivot telles qu'elles sont décrites dans les documentations en ligne d'ProConnect. Cette conformité sémantique est très importante pour faciliter l'insertion de l'application dans l'approche état plateforme : c'est-à-dire lui permettre de s'intégrer à ProConnect et d'exposer si besoin des API de données.
1071	RG	Pour les cartes à puce à usage interne, il est obligatoire de s'appuyer sur le standard IAS-ECC, format retenu dans le cadre de l'IGC ministérielle.
1169	RG	Si une application du ministère est accessible à des utilisateurs d’une autre administration à partir de leur infrastructure (via RIE par exemple), l’authentification et la gestion des droits de ces utilisateurs ne peuvent être déléguées qu’à condition d’apporter des garanties de sécurité. Cette disposition est garantie intrinsèquement par ProConnect.
1167	RG	Les habilitations (par exemple les droits fins d’une application) associées aux utilisateurs doivent être contenues dans une base protégée.
1382	RG	Le RIO (Référentiel d'Identité et d'Organisation) est le référentiel socle des identités pour l'ensemble du ministère. Tout annuaire ou application utilisant l'identité d'un agent du ministère doit s'appuyer sur le RIO et au minimum intégrer le champ identifiant RIO.
1114	RG	Une application ne doit pas prendre en charge la fonction d'authentification de ses utilisateurs : elle doit déléguer cette fonction au SSO du ministère dont elle relève, ou à ProConnect quand le périmètre d'usage dépasse celui des agents du ministère.

Personne morale : gestion des identifications / authentifications / autorisations

Contexte

- Certaines applications ou traitement de données ne s'adressent pas à une personne physique, citoyen ou agent, mais à une **personne morale : une entreprise ou une association**. Dans ce cas de figure, il est nécessaire de identifier de façon unique la personne morale
- établir le lien avec le mandataire

Identité d'une entreprise

La base Sirene, opérée par l'Insee, est le fournisseur des données d'identité des entreprises et de leurs établissements. Celle-ci fait partie des données de référence du Service public de la donnée mis en place par la loi pour une République numérique. Cette identité a deux composantes :

- le SIREN : identifiant unique de l'unité légale (entreprise)
- le SIRET : identifiant unique d'un établissement - le SIRET est constitué du SIREN auquel on ajoute l'identifiant de l'établissement

Les entreprises peuvent être également référencées ou immatriculées dans d'autres registres :

- RCS (Registre du commerce et des sociétés), qui concerne les sociétés commerciales, opéré par Infogreffe pour le compte de l'ensemble des greffes des Tribunaux de commerce français.
- RM (Répertoire des métiers), qui concerne les entreprises artisanales, opérés par les chambres de métiers et de l'artisanat

Ces immatriculations contiennent toutes le n° SIREN de l'entreprise qui reste donc l'identifiant principal. Synthèse utile sur Service-public.fr

Règle : dans le cadre d'entreprise étrangère, ou travaillant à l'international, celle ci doit être identifiée au travers de :

- un European Unique identifier (EUID) au niveau de la communauté européenne
- un "Unique business identifier" à un niveau plus global

Identité d'une association

Lors de sa déclaration en préfecture, l'association reçoit automatiquement un numéro d'inscription au répertoire national des associations (RNA). Elle doit en outre demander son immatriculation au répertoire Sirene lorsqu'elle souhaite demander des subventions auprès de l'État ou des collectivités territoriales, lorsqu'elle emploie des salariés ou lorsqu'elle exerce des activités qui conduisent au paiement de la TVA ou de l'impôt sur les sociétés. Extrait service-public.fr

Règles et recommandations

Ref	Statut	Intitulé
1437	RG	L'identification d'une entreprise doit s'appuyer sur son SIREN (ou SIRET s'il s'agit des établissements). L'identification d'une association doit s'appuyer sur son SIREN (ou SIRET s'il s'agit des établissements) si elle un possède un. Elle s'appuiera sur son numéro RNA dans le cas contraire.
1438	rc	Le protocole a mettre en œuvre est OpenID Connect.

Agent : l'environnement numérique de travail (ENT)

Définition de l’ENT

L’Environnement Numérique de Travail (ENT) correspond à **l’ensemble des ressources, matériels, outils et services transverses mis à disposition des agents du Ministère de l’Intérieur et des Outre-Mer, leur permettant d’accéder aux informations, de créer ou modifier des fichiers, de communiquer, de collaborer sur des projets, en mobilité ou dans les locaux administratifs, dans un cadre sécurisé.**

L’ENT permet de faciliter les communications, la collaboration et les échanges quotidiens.

L’ENT doit répondre aux normes de sécurité imposées par l’ANSSI.

Le remplacement des applications client-serveur vers des services en ligne engendre de plus fortes implications de sécurité et de confidentialité des données. Avec la doctrine « Cloud au centre », la sécurisation de l’ENT est en enjeu majeur. Le chiffrement des outils nomades de type Noemi, Ubiquity (GN), Hesperis, Call-MI et NEO revêt par conséquent un caractère obligatoire.

Il convient également de rappeler et d’imposer à tous les Systèmes d’Information (SI) le respect des normes d’interopérabilité et de sécurité, et ce dès le début de la phase de développement (security by design). A ce titre, la maîtrise d’ouvrage de chaque SI est responsable de la compatibilité aux normes précitées pour les nouveaux SI comme pour les plus anciens qu’il conviendra de faire évoluer, pour garantir la sécurité des SI et permettre l’accès à l’ensemble des postes de travail, sans imposer la moindre adhérence à un logiciel, format, version, outil ou à un système d’exploitation.

Les API permettant la communication entre logiciels devront être de type API Rest.

Le développement des applications web devra obligatoirement intégrer le format "Responsive Web Design". L'UX Design devra également être associée aux projets applicatifs dès les premières phases du projet. L’accessibilité est un aspect clé de l’ENT car elle garantit que tous les utilisateurs, y compris les personnes en situation de handicap, puissent accéder à l’ensemble des fonctionnalités et services de l’ENT de manière équitable.

Il conviendra de :

- s’assurer de l’existence de fonctionnalités permettant d’ajuster la lisibilité des contenus à la convenance de l’utilisateur, par exemple en autorisant l’agrandissement des caractères, la présence d’alternatives textuelles aux médias (images, vidéos et podcasts), la bonne sonorisation des contenus par un formatage compatible avec les aides techniques employées par les agents (lecteurs d’écran et plages braille) ;
- s’assurer que les fonctionnalités de publication de contenus permettent de publier des contenus accessibles ;
- veiller à proposer des interfaces avec un contraste suffisant ;
- rédiger les contenus dans un langage facile à lire et à comprendre ;
- respecter le Référentiel Général d’Amélioration de l’Accessibilité (RGAA) pour les interfaces web et se conformer aux normes européennes EN 301 549, ou à défaut aux bonnes pratiques internationales, notamment le Référentiel de l’Accessibilité des Applications Mobiles (RAAM) pour les applications mobiles ;
- fournir la preuve de l’accessibilité en réalisant ou faisant réaliser un audit d’accessibilité et en publiant le rapport avec l’objectif d’atteindre un score de conformité égal à 100 % des critères du RGAA ou de la norme équivalente pour les fonctionnalités auditées.

Périmètre de l'ENT

Le périmètre de l’Environnement Numérique de Travail du Ministère de l’Intérieur et des Outre-Mer englobe les ordinateurs fixes et mobiles, sécurisés ou non, les smartphones et tablettes. Ces matériels, pour faire partie du périmètre de l’ENT, **doivent avoir été configurés ou masterisés à l’aide des images disques ou masters** créés et déployés par la DTNUM ou par les services SIC locaux.

Environnements bureautiques fixes

Les ordinateurs fixes ou portables, dits de bureau, et destinés à être **connectés uniquement sur le réseau du MIOM et du Réseau Interministériel de l'État (RIE)** seront configurés exclusivement avec les outils de la DTNUM, en respectant les versions préconisées et maintenues des systèmes d'exploitation et des logiciels.

Environnements bureautiques nomades

Les ordinateurs portables nomades sécurisés et chiffrés de type **Noemi ou Ubiquity (Gendarmerie Nationale), munis d'un VPN (réseau privé virtuel, tunnel sécurisant l'accès au réseau du MIOM depuis un réseau privé personnel)** seront déployés selon les règles définies par la DTNUM ou le STSI². Le site Noemi rassemble toutes les informations nécessaires (les prérequis, les documentations d'installations, les actualités) pour les techniciens support, mais offre également à tous les utilisateurs des réponses aux interrogations, des documentations, une assistance de type FAQ et fixe les restrictions d'usage.

Environnements d'administration de services

Les ordinateurs portables sécurisés destinés à l'utilisation du SPAN doivent être configurés selon les règles définies par la DTNUM. **Le SPAN est préconisé pour permettre l'administration à distance de serveurs** par des personnels qualifiés et ne sera déployé que pour cet usage particulier. Le site SPAN rassemble les informations nécessaires à son déploiement et au support associé.

Environnements Passerelles Internet

Les ordinateurs fixes ou portables communément appelés **« PC ADSL» ou « PC Internet »**, s'ils sont destinés à être **utilisés par le biais de Fournisseurs d'Accès Internet (FAI), ne doivent en aucun cas être exposés alternativement sur internet depuis les FAI et connectés sur le réseau du MIOM**. Ces machines seront configurées indépendamment de toute restriction par les directions qui les utiliseront, à l'exception de l'installation de l'antivirus officiel du MIOM version autonome, disponible sur le site de téléchargement de la DTNUM.

Environnements de developpement et d'administration technique

Les ordinateurs **dédiés aux développeurs et administrateurs techniques seront configurés sous Linux** et seront préparés et maintenus par la DTNUM ou les services SIC locaux. Un dépôt sera créé à la DTNUM et celui ci sera le seul dépôt autorisé (en complément du dépôt géré par la GN pour leurs besoins propres). La mise en place de ce service sera effective dans le courant de l'année 2023.

Appareils mobiles

Les smartphones et tablettes (Hesperis uniquement) déployés et maintenus par la DTNUM ou par les services SIC locaux permettent l'accès au service Hesperis, CallMI et NEO.

Ils permettent de bénéficier :

- d'une messagerie professionnelle, avec agenda et gestion des contacts
- de la téléphonie (appels, SMS, MMS),
- d'un accès internet via Orion,
- d'un accès intranet,
- d'un accès aux applications mobiles publiques et métiers validées par le C2MI.

Ils ne permettent pas :

- l'utilisation des réseaux sociaux comme Facebook, Twitter, instagram…
- d'utiliser des messageries instantanées (Whatsapp, Télégram).
- de se servir de son téléphone comme point d'accès mobile.

Rappel : l'utilisation du terminal CallMI est **destinée à un usage Diffusion Restreinte exclusivement (la voix, les sms et la Data sont sécurisés)**. En conséquence ce terminal n'est pas la solution à utiliser pour se tenir informé des dernières nouvelles ou autres activités de même nature.

Important : Toute demande de mise à disposition d'une **nouvelle application sur les smartphones et tablettes** devra nécessairement **passer par le Responsable de la Sécurité des Systèmes d'Information (RSSI)** du demandeur qui, une fois la requête analysée et filtrée, adressera la demande de validation au Service du Haut Fonctionnaire de Défense (SHFD), et plus précisément au **Centre de Cyberdéfense du Ministère de l'intérieur (C2MI)**, qui statuera et autorisera ou non le déploiement.

Systèmes d'exploitation autorisés

Seuls les systèmes d'exploitation **Windows et Linux (versions supportées et correctement sécurisées)** sont autorisés sur le réseau du MIOM et du RIE. Tout autre système d'exploitation sera nécessairement connecté hors réseau. **Android** est le seul système d'exploitation autorisé (version supportée et correctement sécurisée) **sur les smartphones et tablettes** configurés par la DTNUM ou les services SIC locaux.

Sécurité des postes de travail et des serveurs

Tout poste de travail ou serveur (Windows ou Linux) doit être équipé des antivirus qualifiés par le ministère à jour de sa base antivirale. Rien ne doit entraver le fonctionnement et la mise à jour de l'anti-virus et/ou de l'anti-espiogiciels et/ou du pare-feu.

Sécurité des supports de stockage

Le passage à la station blanche de tous les supports amovibles est indispensable lors des transferts de fichiers. La mise en place d'un système d'authentification des supports amovibles au travers de l'antivirus est fortement recommandé.

Sécurité reseaux

Une fiche pratique SSI relative à la sécurisation de l'accès internet par réseau ADSL (ou fibre) est établie par le SHFD. Celle ci est disponible en annexe réglementaire, il conviendra de s'assurer de la conformité de l'installation et de l'utilisation des PC ADSL ou Internet aux dispositions développées, notamment à la mise en place d'un portail d'authentification de type « Alcasar ».

Tous ces outils sont supportés par la DTNUM et peuvent faire l'objet d'une demande d'assistance uniquement s'ils ont été configurés et déployés par les services SIC locaux dépendant de la Direction de la Transformation Numérique. Il convient de respecter les préconisations établies dans ce document pour l'ensemble de l'ENT dépendant du périmètre du MIOM et des Directions Départementales Interministérielles sous responsabilité numérique du MIOM.

Les produits de l'ENT

Materiel

On considère que les produits matériels qui composent l'Environnement Numérique de Travail sont distingués en 4 parties :

- Les PC sécurisés, fixes ou portables : Solutions Noémi, SPAN, Ubiquity (GN) et Gendbuntu (GN)
- Les PC dits ADSL ou Internet : Machines exclusivement dédiées et connectées sur Internet
- Les ordinateurs pour les développeurs et administrateurs techniques : Machines disposant de composants particuliers dédiés aux développeurs et administrateurs techniques
- Smartphones et tablettes sécurisées : Solutions Hesperis, Call-MI et Neo
    - Modèles qualifiés Hesperis 2 disponibles sur le site intranet dédié : Ne sont autorisés que les téléphones de marque SAMSUNG, qui comportent une couche de sécurité optimisée avec le module KNOX et sont dotés d'un client adapté à nos usages Samsung Mail, le tout sur une version android supportée.
    - Modèles qualifiés Call-MI (solution DR) disponibles sur le site intranet dédié : Ne sont autorisés que les téléphones de marque SAMSUNG, qui comportent une couche de sécurité optimisée avec le module KNOX et sont dotés d'un client adapté à nos usages Samsung Mail, le tout sur une version android supportée.
    - Modèles qualifiés NEO pour les forces de sécurité intérieure

Logiciels / Services de l'Environnement numérique de Travail

Contexte réglementaire :

Le présent document s'appuie sur les textes référencés ci-après définissant la stratégie de l'État au niveau des systèmes d'information. Ainsi les critères de sélection des outils/services reprennent ces priorisations pour définir ceux dont l'usage sera autorisé au sein du ministère de l'Intérieur.

- La loi 2016-1321 du 7 octobre 2016 (article 16) encourageant l'utilisation des logiciels libres et les formats ouverts ;
- Le Référentiel Général d'Interopérabilité, RGI v1 - ordonnance n° 2005-1516 du 8 décembre 2005, RGI v2 - arrêté en date du 20 avril 2016;
- Le Référentiel Général de l'Amélioration de l'Accessibilité, arrêté du 20 septembre 2019 ;
- La circulaire Ayrault du 19 septembre 2012 relative aux orientations pour l'usage des logiciels libres dans l'Administration ;
- La circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État ;
- Le guide d'hygiène informatique de l'Agence Nationale de Sécurité des Systèmes d'Information,
- La Politique de Sécurité des Systèmes d'Information du Ministère de l'Intérieur et des Outre-Mer.
- La note de la Dinum sur la non conformité de Microsoft Office 365 à la doctrine "Cloud au centre".
- La fiche pratique SSI du Service du Haut Fonctionnaire de Défense relative à la sécurisation de l'accès internet par réseau ADSL (ou fibre).

Critères retenus pour la sélection des logiciels, outils ou services :

Critères	Attentes
Type de logiciel – Libre / Gratuiciel / Payant	Ré-utilisabilité, scalabilité, flexibilité, sécurité (transparence du code source), évolutivité (mutualisation possible des améliorations), pérennité, interopérabilité (usage des formats ouverts), potentiel encadrement des usage ou coût de licence pour un logiciel commercial.
Existence d'un support correctif O/N	Garantie d'assistance continue, mises à jour régulières aux fins d'amélioration de fonctionnalités et de corrections de bugs, permettant ainsi une stabilité d'usage sur le long terme. Un logiciel non supporté n'a plus vocation à être utilisé sur les postes du MIOM du fait de la non couverture de ses failles de sécurité.
Outil utilisé en Interministériel O/N	Facilité d'usage entre les systèmes utilisés dans d'autres administrations, possibilité de mutualisation en termes de support et de maintenance, partage des bonnes pratiques.
Version LTS ou ESR disponible O/N	Stabilité, disponibilité et maintien des correctifs sur le long terme, mises à jour de sécurité.
Version SSI validée O/N	Logiciels évalués et validés par l'ANSSI. Certification de conformité aux normes de sécurité.
Outil multi plateforme Windows/Linux/Android/Mac	Mutualisation, rationalisation, compatibilité matérielle, simplification d'appropriation de l'usage et continuité de travail dans un même outil.
Limitation d'usage dans le contexte ministériel	Définition de l'usage exclusif fixé pour le logiciel sur l'Environnement Numérique de Travail du MIOM.
Niveau d'accessibilité actuel (Pris en charge/Partiellement pris en charge/Non pris en charge)	Définition du niveau d'accessibilité du logiciel ou service, afin de valoriser les outils potentiellement adaptés aux agents porteurs de handicaps.
Conformité aux normes et standards O/N	Interopérabilité, meilleure expérience utilisateur (fiabilité des restitutions), non adhérence applicative, conformité réglementaire.
Licence open source reconnue par OSI (Open Source Initiative - organisation dévouée à la promotion des logiciels open source)	Transparence et confiance, les logiciels reconnus sont évalués pour leur conformité,leur flexibilité de modification et de distribution du code source, leur coopération communautaire et leur stabilité.
Type de licence si logiciel propriétaire (libératoire/par poste/par agent/sur volume)	Vise à limiter l'impact financier et en termes de gestion des dites licences, afin de faciliter la scalabilité de l'usage du logiciel et son coût à la cible.
Porteur de logiciel ou service	Détenteur de la solution (mono-acteur, taille, origine, ….) permettant de s'assurer de la pérennité de la solution dans la durée et couverture possible du risque.
Droit soumis à une licence UE O/N	Conformité réglementaire stricte en matière de protection des données, équité et transparence, garantie de la protection intellectuelle, soumis au droit européen.
Taille indicative du paquet	Taille du fichier à mettre en dépôt sur la plateforme de téléchargement. Information donnée à titre indicatif, à prendre toutefois en compte pour un large déploiement sur les systèmes d'information du MIOM.

A noter : Certains logiciels pourront être retenus malgré la « non conformité » à un ou plusieurs critères sur raison particulière et justifiée, sans toutefois être en opposition avec la Politique de Sécurité des Systèmes d'Information du MIOM et les principes de base pré-cités. La situation pourra ainsi être réévaluée au regard des nouvelles solutions qui pourraient voir le jour et apporteraient la couverture fonctionnelle attendue tout en répondant aux critères.

Tous les logiciels du poste de travail seront mis à disposition sur le site de téléchargement, à raison de 3 versions au maximum. Les logiciels installés sur l'ENT ne seront téléchargeables que depuis les plateformes officielles du MIOM ou à terme un outil de gestion centralisé, ou un dépôt Linux DTNUM ou GN.

Tout logiciel ne bénéficiant plus de mise à jour sera remplacé par une autre solution logicielle remplissant le même usage ; le support de la solution doit être assuré par la communauté ou l'éditeur.

Usages : La couverture fonctionnelle de la solution (logiciel ou service) sera par définition totale ou partielle, en fonction des besoins exprimés par les services demandeurs. La solution retenue devra néanmoins couvrir le spectre le plus large possible de l'usage qui lui est associé. Le choix des logiciels, outils et services sera basé sur les usages et les bonnes pratiques. L'objectif est de parvenir à proposer un seul outil/logiciel pour un usage. L'usage final non couvert par l'offre, correctement défini par le service demandeur, permettra de proposer de nouvelles solutions au CCT, par le biais d'un formulaire d'expression de besoin (FEB) dûment renseigné.

Politique de versions des logiciels, outils ou services :

Est appliquée l'ensemble des mises à jour de sécurité (au fil de l'eau), sauf en cas d'impact sur le fonctionnel du logiciel. Dans ce cas une analyse d'impact est pratiquée, au regard du risque couvert et une décision est prise concernant l'installation du dit correctif ou son ajournement.

Pour les logiciels majeurs du poste de travail des agents du ministère (navigateur, suite bureautique,..) le cycle de mises à jour prévisionnel est de 6 mois (avril et octobre).

S'appuyant sur la feuille de route du produit à déployer lorsque cette dernière est connue (une variation de quelques semaines peut être nécessaire, le temps de valider la version et selon la présence ou non de correctif suite à la découverte de problèmes dans la version proposée au téléchargement).

Pour les autres logiciels du poste de travail, une montée de version annuelle est prévue (avril ou octobre) sur la base des avancées fonctionnelles notables.

Les logiciels du poste de travail sont testés par un panel de testeurs sur les domaines AC, AT, ATE et PN durant 2 semaines avant mise en production.

Déploiement des logiciels :

Le poste de travail de type ordinateur de bureau, chiffré ou non, et destiné à être connecté au réseau du MIOM est fourni à l'agent avec un bouquet logiciel de base.

Les sections support locales chargées du déploiement et de l'installation auprès des agents installeront les outils complémentaires nécessaires à l'agent en fonction de son périmètre d'activité et de ses besoins.

Pour les machines dont le système d'exploitation est de type Microsoft Windows, les services locaux ont à leur disposition sur l'Active Directory, un groupe WPP présent dans chaque OU (Unité d'Organisation) permettant aux machines intégrées à ce groupe WPP (pc_standards) d'obtenir automatiquement et systématiquement la dernière version du socle logiciel de base du poste de travail (navigateur, suite bureautique, lecteur PDF, lecteur multimédia, éditeur de texte, retouche d'image, navigateur de visioconférences et client de messagerie). Ce socle sera étendu autant que faire se peut avec des outils qui seront définis comme faisant partie du bouquet logiciel de base fourni à l'agent.

La diffusion automatique des mises à jour du socle logiciel par WPP pourra être remplacée à l'avenir par un outil de gestion et de déploiement centralisé.

A terme, l'agent pourra par lui-même piocher dans un magasin d'application les outils disponibles et les installer sans génération de ticket de support ni besoin de compte administrateur.

Les logiciels ou applications pour les smartphones sont disponibles depuis le magasin accessible depuis chaque terminal ; leurs mises à jour est automatique ou manuel, paramétrable par chaque utilisateur (documentations disponibles sur les sites Hesperis2 et Call-MI)

Logiciels, outils et services retenus

Se référer au chapitre dédié dans le référentiel des produits

La feuille de route sur les produits de l'ENT est disponible au travers de ce lien.

Le tableau des critères utilisé par les services de l'ENT pour qualifier les produits.

Les usages les plus représentatifs de l'ENT sont distingués comme suit :


Documents bureautiques
Outil de gestion de projet
Authentification
Transfert fichiers volumineux
Outil d'enquête et de sondage
Wébinaire
Stockage/partage de documents
Planification des réunions / sondages
Visio conférence
Messagerie
Compression / décompression fichiers
Audio conférence
Messagerie instantanée
Logiciel de gestion de tâches
Annuaire interministériel
Plateforme collaborative
SI géographique
Signature des documents électroniques
Plateforme de communautés
Retouche d'images
Diagrammes
Chiffrement / déchiffrement
Editeur de texte/code source
Lecteur multimédia
Fichiers PDF
Prise de note
Gestion des mots de passe
Accessibilité
Sauvegarde de l'ENT
Capture son ou vidéo

Utilisateur : expérience utilisateur et accessibilité

Contexte

Un sujet essentiel

L'accessibilité et la qualité du parcours usager d'une application, d'un service, d'une démarche en ligne, sont essentiels et au cœur de la politique sociétale et d'inclusion des populations.

Les risques d'une non qualité d'un parcours usager sont nombreux :

- coût financier des correctifs après coup – toujours significativement plus important que le coût d'une prise en compte en amont
- risque de non adoption ou de rejet de la démarche en ligne
- risque d'exclusion des publics fragiles
- risque de dégradation d'image (campagne de presse, réseaux sociaux)
- risque de recours (par exemple des associations de personnes handicapées)

Cette qualité est mesurée, par l'État lui-même (cf section suivante) comme par la société civile (ex. associations de défense des personnes en situation de handicap, des étrangers ...etc).

Prise en compte

L'accessibilité et la qualité du parcours usager sont à prendre en compte en amont du projet, dès la phase de conception, indépendamment de la méthode projet, et tout au long de son cycle de vie.

Vérifier et mesurer

L'accessibilité et la qualité du parcours usager se doivent d'être vérifiée et mesurée dans une démarche d'amélioration continue, tout au long du cycle de vie de l'application. Cette mesure peut passer par différents outils de suivi d'audience, des enquêtes de satisfaction, propre à chaque ministère.

En complément, la satisfaction de l'usager se doit d'être également mesurée sous l'impulsion des services du premier ministre, DINUM et DITP au travers de deux dispositifs :

- Mesure à chaud : une fonction "Mon Avis" qui **doit obligatoirement** être intégré à la fin de chaque démarche en ligne. Les résultats statistiques de cette mesure sont publiés dans l'observatoire de la qualité des démarches en ligne (cf section suivante)
- Mesure à froid avec le dispositif VoxUsagers : site de VoxUsagers

L'observatoire de la qualité des démarches en ligne

La DINUM a mis en place un observatoire public : l'observatoire de la qualité des démarches en ligne. Il évalue finement, chaque trimestre, les 250 démarches en ligne les plus utilisées par des critères d'évaluation dont notamment :

- la satisfaction des usagers, collectée à chaud grâce au bouton "Mon Avis" obligatoirement intégré sur chaque démarche.
- l'accessibilité numérique (RGAA),
- la prise en compte du handicap,
- le critère "dites le nous une fois" (DLNUF)
- compatibilité avec les équipements mobiles
- disponibilité et rapidité
- l'intégration à FranceConnect

Ces critères d'évaluation sont détaillés sur le site de l'observatoire : critères d'évaluation.

Accessibilité numérique

L'accessibilité numérique (RGAA) est une composante légale de la qualité d'une démarche en ligne.

Les ressources et outils disponibles au sein des services cités ci-dessous peuvent être utilisés pour réaliser des démarches conformes au RGAA.

- la DAE (Direction des Achats de l'État) a mis en place un ensemble complet de prestations d'accompagnement, d'audit et formation
- la DILA fournit des ressources aux développeurs sur le site PIDILA : https://design.numerique.gouv.fr/outils/checklist-pidila/
- la DINUM fournit les ressources pour mettre en oeuvre les exigences du RGAA : https://accessibilite.numerique.gouv.fr/
- les ressources financières avec le fond pour l'insertion des personnes handicapées dans la fonction publique (FIPHFP)

Pour toute demande complémentaire, ou pour tout accompagnement sur ce sujet, les chefs de projet peuvent contacter leur référent accessibilité de proximité ou le référent du ministère à l'adresse dnum-transformation-numerique@interieur.gouv.fr

Règles et recommandations

Ref	Statut	Intitulé
	RG	Toute mise à jour majeure d'une application doit faire l'objet d'un audit de conformité aux critères du RGAA.
	RG	Tous les services développés doivent viser un taux de conformité au RGAA égal à 100%.
	RG	L'achat d'un outil doit se faire en tenant compte du taux de conformité au RGAA (i.e. outil accessible ou proposer une solution complémentaire accessible) et que toute prestation de réalisation technique doit se soumettre aux mêmes exigences de respect des critères du RGAA que précédemment évoquées (i.e. conformité à 100%)
1219	RG	La charte graphique de DSFR (Design de Système de l'État) s'applique aux applications WEB.
1230	RG	Toutes les applications doivent se conformer, sans conditions, aux critères du Référentiel Général d'Amélioration de l'Accessibilité (RGAA) disponible sur le site : https://accessibilite.numerique.gouv.fr/

Pilier données et API - Introduction

Toute application offre des services et manipule des données, des concepts métier, qui jouent souvent un rôle plus large et plus durable que l'application elle-même. Toute application doit adresser, sans conditions, les 5 questions élémentaires suivantes :

1. **Concevoir une application orientée service et données** - couvert par plusieurs questions :
2. **Réutilisation** Les données que doit manipuler mon application existent elles déjà ailleurs et ai je envisagé une réutilisation ?
3. **Exposition des données** - L'application est elle pensée pour faciliter la réutilisation des données qu'elle crée ou transforme ?
4. **Exposition des traitements** - Au delà d'une exposition brute de données, mes traitements sur les données eux mêmes peuvent être exposés ? Sont-ils exposés en vue d'une réutilisation possible ?
5. **Gestion des échanges** - Les échanges, internes comme externes, sont pris en charge par des dispositifs ministériels ou interministériels dédiés. Ont-ils été pris en compte ?
6. **Analyser et valoriser les données** - Les données sont un patrimoine indépendamment des traitements qui leur sont appliqués. Elle doivent pouvoir être notamment croisées, analysées, anonymisées, parfois recyclées en données ouvertes. Toutes les mesures ont elles été prises pour faciliter cette valorisation ultérieure?
7. **Données personnelles** - Le cadre juridique relatif au traitement des données personnelles a-t-il été bien pris en compte (cf. notamment RGPD) ?
8. **Archivage** - Le cycle de vie complet des données manipulées par l'application a-t-il été pensé ?

Données et API -- Concevoir une application orientée données et services

Les données

Les données sont un patrimoine de l'État. Leur portée et leur importance peuvent déborder du traitement de l'application qui va les exploiter. Il est donc important, dès la conception d'un nouveau traitement ou d'une nouvelle application, de formaliser une réponse structurée, aux interrogations suivantes :

Sujet	Quelle question doit on se poser ?
Réutilisation (consommation de données déjà existantes)	les données que doit manipuler mon application existent-elles déjà ailleurs et ai je envisagé une réutilisation ?
Exposition des données	l'application est elle pensée pour faciliter la réutilisation des données qu'elle crée ou transforme ?
Exposition de traitements	Au-delà d'une exposition brute de données, les **traitements** sur les données peuvent être exposés. Sont-ils exposés en vue d'une réutilisation possible ?

Les services

Réutiliser des données, exposer des données, exposer des traitements : ces actions sont des **services**. Ceux-ci sont « exposés » aux travers d'interfaces, ou API (Application Programming Interface). L'API est un service WEB qui utilise le protocole http(s) et un style d'architecture REST ou REST full.

Le type d'interface dont il sera question dans la suite de la fiche sera ce type d'API HTTP/REST.

La Stratégie d'API du CCT décrit la démarche dans toute sa dimension : architecture, design, sécurité et gouvernance.

Réutilisation

Rappel de la question initiale : les données que doit manipuler mon application existent-elles déjà ailleurs ? Ai-je envisagé leur réutilisation ?

Le traitement de cette question nécessite de croiser les données métier manipulées par l'application avec les données réutilisables, au niveau ministériel comme interministériel.

Il peut s'agir :

- de données de référence, souvent qualifiés de "communs", exposés sur des dispositifs de type MDM (Master Data Management) - Il peut s'agir du GDR (Gestion de Données de Référence) de la DTNUM, ou les données de référence exposées par le SIR du ST(SI)² pour la sécurité intérieure ;
- de données exposées dans le SI de l'État, dans le cadre État Plateforme et de FranceConnect Plateforme. Exemple : l'API Entreprise ;
- de données exposées par d'autres applications ;
- de données ouvertes.

Deux types de vérifications sont à réaliser pour chaque donnée manipulée :

1. existence de la donnée au sein du ministère de l'Intérieur;
2. réutilisation de la donnée dans le contexte de l'application

Existence de la donnée au sein du ministère de l'Intérieur

Plusieurs sources de données sont disponibles au sein du ministère de l'Intérieur :

- les données ouvertes de l'État dans data.gouv.fr
- le référentiel patrimonial des applications du Ministère de l'intérieur, CANEL
- le catalogue des données du ministère de l'intérieur : catalogue.data.minint.fr
- les catalogues d'API (la majorité des API exposent des données plus que des traitements) : **api.minint.fr** pour l'accès aux données en interne pour le ministère et api.gouv.fr pour l'État.

Réutilisation de la donnée dans le contexte de l'application

En cas de réutilisation, il est nécessaire de s'assurer que :

- sa sémantique soit compatible,
- sa qualité soit satisfaisante,
- la qualité de service de l'exposition soit compatible avec les exigences de l'application,
- les performances soient suffisantes,
- qu'une solution de repli ait été prévue en cas d'interruption de service, le cas échéant qu'un contrat de service ait été établi avec le fournisseur.

Exposition des données

Rappel de la question initiale : l'application contribue t elle à la réutilisation des données qu'elle crée ou transforme ?

Une application peut produire des données métier qui peuvent contribuer à la réutilisation de données, au-delà du contexte de l'application. Conformément à l'approche État Plate-forme avec ses API données, il est obligatoire de prévoir une exposition de ces données pour une ré-utilisation éventuelle.

Modalités d'exposition : une exposition par API, quand elle ne participe pas à un inter-ou intra-applicatif planifié, doit utiliser les services d'une plateforme d'échange et sa brique de gestion d'API (API Management) pour intégrer un certain nombre de services tels que :

- la gestion de la performance (il est possible de limiter les appels par acteurs - throttling, quotas)
- le contrôle d'accès s'il est nécessaire
- la contractualisation avec l'offre de service MonComptePro de la DINUM
- la traçabilité et l'accounting
- de la conversion (API SOAP en API REST par exemple)

Une donnée de référence est définie par les propriétés suivantes :

- utilisation fréquente par un grand nombre d'utilisateurs, internes et externes
- qualité critique pour un grand nombre de processus
- sémantique partagée et relativement stable dans le temps
- durée de vie qui va au-delà des processus opérationnels qui les utilisent
- facilité d'accès à ces données est critique

Si la donnée entre dans cette catégorie des données de référence, il est nécessaire de la traiter comme telle, et d'utiliser un système d'exposition dédié : GDR ou SIR.

Exposition de traitements

Rappel de la question initiale : Au-delà d'une exposition brute de données, les **traitements** sur les données peuvent être exposés ? Sont-ils exposés en vue d'une réutilisation possible ?

L'exposition public d'un traitement via une API REST-Full est requise pour tout partage inter-applicatif.

Ces API doivent être exposés dans une passerelle d'API (INES, SIR) et décrite au travers d'un catalogue. Le catalogage interne MI se fait sur http://api.minint.fr/ , le catalogage sur internet se fait sur https://api.gouv.fr/

Règles et recommandations

Pour information, il existe des règles pertinentes dans le périmètre des référentiels de données dans le Cadre Commun d'Architecture des Référentiels de données.

Le référentiel "stratégie d'API" est lui même un recueil de règles et de recommandations (ou bonnes pratiques) : Stratégie d'API - Règles et recommandations

Ref	Statut	Intitulé
1445	RG	Pour toute donnée, les conditions d'une possible réutilisation doivent être envisagées. Réutilisation en mode différé sous forme de publication de jeu de données ouvertes, et exposition au fil de l'eau sous forme d'API.
1446	RG	Toute nouvelle API susceptible d'être réutilisée, doit être cataloguée et documentée sur le catalogue api du ministère (api.minint.fr) si son usage est strictement restreint au ministère, sinon sur celui de l'état (data.gouv.fr).
1447	rc	Toute nouvelle API susceptible d'être réutilisée devrait être exposée via l'une des plateformes d'API Management du ministère.
1448	RG	En cas de consommation d'API externe, l'intermédiation d'une plateforme d'échange doit être privilégiée.
1360	RG	Il est obligatoire de réutiliser les données existantes
1100	RG	Les composants fonctionnels manifestement communs à plusieurs applications doivent être développés sous forme de services réutilisables.

Données et API -- Gestion des échanges

Principe recherché

Les applications s'intègrent dans un écosystème ministériel, voire interministériel (SI de l'État), voire au-delà (SI collectivités, partenaires, usagers ..) avec lesquels elles échangent des données. Celles-ci peuvent être des données externes qu'elles consomment, ou des données internes qu'elles exposent (à la consommation des autres applications).

Interfaces d'échange - ou API

Dans la stratégie de l'État plateforme, qui s'aligne en cela sur des pratiques généralisée dans l'Internet, les données sont échangées selon le profil recommandé P1 « Fondations État Plateforme » défini dans le Réglement Général d'Interopérabilité (RGI) qui préconise des interfaces API basées sur le protocole https, le style d'architecture REST, le format de données JSON, et le protocole d'authentification OpenID Connect. Un certain nombre de bonnes pratiques ont été définies pour ces échanges, notamment au niveau ministériel avec la stratégie API qui définit le niveau sémantique des API REST.

L'usage d'interface sous forme webservices SOAP est proscrite pour toutes nouvelles ou évolutions majeures de l'application.

Une tolérance, soumise sans condition à validation par le Comité d'architecture, existe pour d'autres modes d'échange :

- échanges par fichier -- Encore très répandus, notamment pour les données ouvertes.
- CFT, RMI/JRMP, PeSIT

Les plateformes d'échange

Le ministère structure ses échanges autour de deux plate-formes d'échange :

- INES, opérée par la DTNUM
- SIR (Système d'Interface et de Référence), opérée par l'ANFSI

Les autres DSI (PP, ANTS, ANTAI ...) ne se sont pas dotées de plateforme d'échange référencé par le Ministère de l'intérieur

Par ailleurs, d'autres plateformes d'échange interministériel peuvent être utilisées, si les besoins de l'application ne peuvent être couverte par les plateformes d'échange du Ministère de l'intérieur :

- La plateforme d'API Gateway/Management de l'AIFE : PISTE (https://piste.gouv.fr/).

Règle :

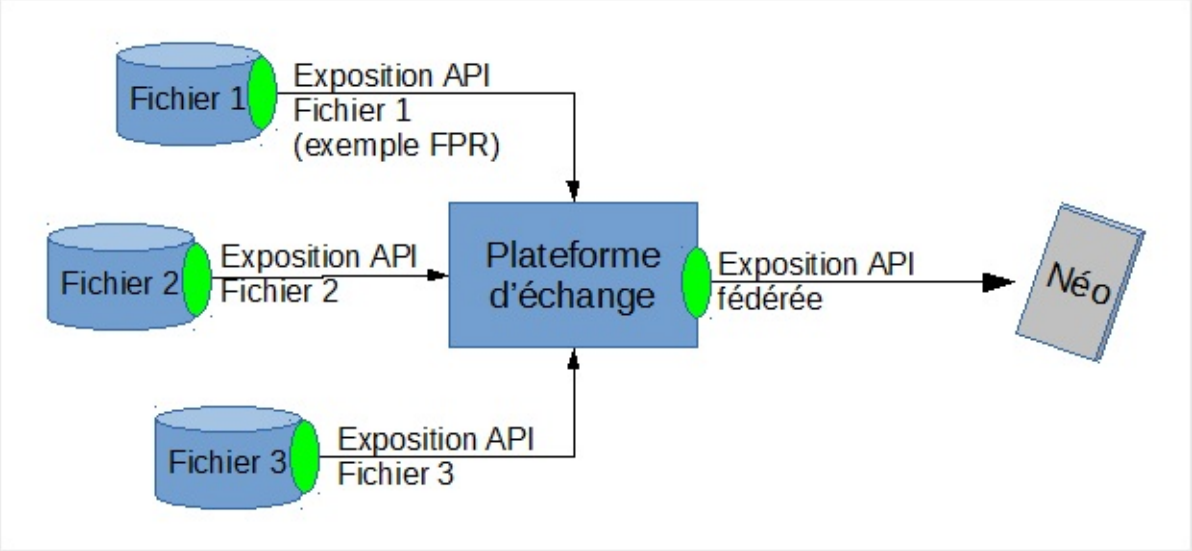
Indépendamment de la plateforme d'échange, qu'elle soit ministèriel ou inter-ministériel, en cas d'exposition d'une API sur Internet, Il est recommandé d'utiliser la solution de contractualisation de la DINUM :MonComptePro (https://moncomptepro.beta.gouv.fr)

Le composant majeur des plateformes d'échange est l'**API Gateway / API Management**. Celui-ci offre un certain nombre de fonctions essentielles telles que :

- **Passerelle d'API** avec des fonctions d'exposition des services et des ressources, de sécurisation des flux, de régulation du trafic (seuils, quotas), de contrôle des identités et des droits (par jetons)
- **Magasin d'API** avec des fonctions de publication, des API, de souscription aux API, de tableau de bord pour les développeurs -- Cette fonction est portée au ministère par un autre composant : http://api.minint.fr
- **Editeur d'API** avec des fonctions de gouvernance (cycles de vie, versioning) , facturation, monitoring, autorisation
- **ESB (Enterprise Service Bus)**. Ces bus de services sont capables de prendre en charge des transformations ainsi que des agrégations de flux dans des contextes d'échanges inter-applicatifs.
- **SAS fichier**

Fonctions d'intermédiation des plateformes d'échange.

La plateforme d'échange et d'intermédiation est porté par la plateforme. Elle offre un service d'intermédiation entre un consommateur et plusieurs fournisseurs.

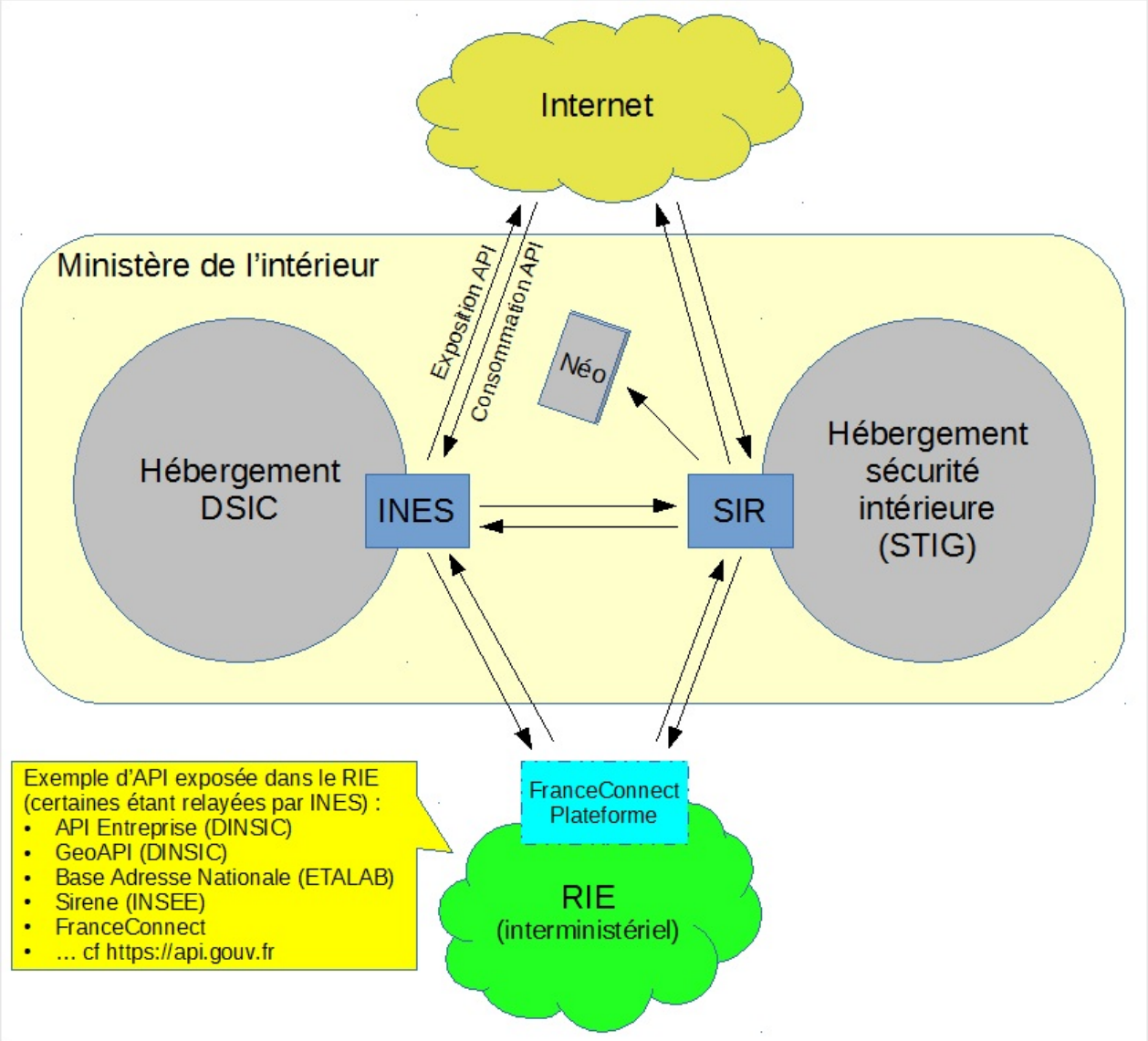


L'exemple ci-dessus montre un cas d'intermédiation avec la possibilité pour une application mobile du smartphone Néo qui équipe les forces de l'ordre d'interroger plusieurs fichiers de police en une seule demande sur une API fédérée.

API Entreprise de la DINUM est un autre exemple d'intermédiation et de service à valeur ajoutée en ce qu'elle agrège des informations de l'INSEE (Sirene) et d'Infogreffe.

INES - DTNUM	SIR - ANFSI
La plateforme INES met en œuvre 3 composants : - API management (tel que décrit ci-dessus) - ESB (Bus de service) qui permet de transformer ou d'agréger des flux. - SAS fichier La plateforme INES est appelée à prendre en charge tous les flux d'API internes au applications hébergées par la DTNUM. La plateforme INES mutualise le raccordement au RIE et à Internet. C'est elle qui permet de « consommer » des API externes, comme par exemple l'API entreprise, la BAN, l'API INSEE …etc. INES est raccordé au SIR et route les flux destinés aux applications de sécurité interieure hébergées au STIG	La plateforme SIR est basée sur un ESB (Bus de service) qui permet notamment d'assurer le routage, la sécurisation, et des agrégations de flux d'API. La plateforme SIR prend en charge les flux d'API sortant du périmètre du centre d'hébergement de la sécurité intérieure (STIG). Le SIR ne prend pas en charge les flux internes au STIG. SIR est raccordé à INES et route les flux destinés aux applications de hébergées dans le centre d'hébergement de la DTNUM. Le SIR route et agrège tous les flux API avec les équipements mobiles des forces de l'ordre, notamment les applications des smartphones Neo (interrogation de fichier ..etc). Cf schéma ci-dessus.

Urbanisation des flux



Les deux plateformes d'échanges sont dédiées aux deux principaux hébergements nationaux : INES pour l'hébergement DTNUM et SIR pour l'hébergement STIG de la sécurité intérieure.

Règle : Les flux inter-applicatifs transitant entre les deux hébergements doivent être relayés (contrôlés, sécurisés ...) via INES et SIR.

Impacts sur les applications

Tout échange entre application doit transiter au travers d'une plateforme d'échange.

Règles et recommandations

Ref	Statut	Intitulé
1449	rc	La consommation d'API interne devrait passer par une fonction d'API gateway pour avoir une bonne visibilité sur l'ensemble des flux de consommation.
1450	RG	Les flux inter-applicatifs inter-centres d'hébergement transitent par INES et SIR.
		La plateforme INES est le point

1451	RG	d'entrée pour les API interministérielles (API entreprise, API INSEE, BAN ...etc). Grâce à son API management, elle est garante du respect du contrat de service établi avec les fournisseurs extérieurs.
1363	RG	Le format de présentation et d'échange d'une adresse postale doit respecter la norme AFNOR XPZ 10-011.
1047	rc	Si l'échange entre deux applications nécessite une transformation des données, il est recommandé de s'appuyer sur les plateformes d'échange du ministère.
1048	RG	Tous échanges asynchrones doivent être réalisés au travers d'une plateforme d'échange du ministère, ou interministériel.
1065	RG	Tous les échanges par Web Service ou par API doivent être authentifiés.
1072	RG	Tout fichier XML doit être accompagné de son schéma.
1074	RG	Les formats PNG et JPEG doivent être utilisés pour échanger les informations graphiques et les images fixes.
1075	RG	Les flux audiovisuels, doivent respecter les formats MPEG-2 ou MPEG-4.
1076	RG	En complément du RGI, pour tous les échanges de documents bureautiques internes et externes, seuls les formats OpenDocument et PDF sont autorisés.
1078	RG	Le format d'échange des fichiers géographiques retenu est le format ShapeFile.
1120	RG	Tout échange d'informations avec un SI externe au ministère doit faire l'objet d'un traitement particulier par des serveurs proxy déployés au sein d'une DMZ (conformément aux recommandations de l'ANSSI) afin de vérifier l'innocuité et l'intégrité des flux ou des fichiers. Les infrastructures nationales existantes (ex : SIR, INES) doivent être systématiquement privilégiées.
1165	RG	Les interconnexions avec des partenaires externes doivent être réalisées en priorité à l'aide de VPN IPSEC, selon les recommandations de configuration ANSSI. A défaut, l'usage du protocole TLS, basé sur l'authentification mutuelle par certificat, sera utilisé.

Données et API - Analyser et valoriser les données

Principe recherché

La maîtrise de la donnée, de la science de la donnée et de l’intelligence artificielle est identifiée par le Gouvernement comme un enjeu stratégique.

Toute application qui sera amenée à alimenter une plateforme technique de valorisation de données, devra intégrer:

- **des extracteurs de données** - permettant de sortir les données opérationnelles de l'application pour les intégrer au sein de la plateforme technique.
- des mécanismes d'**anonymisation des données**, avant d'alimenter la plateforme technique de valorisation des données, dans le respect des exigences réglementaires et normatives

Gestion des données personnelles

Contexte

Les dispositions de l'article 4 du RGPD précisent : «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Au vu de cette définition, la majorité des applications du ministère de l'intérieur traitent des données personnelles. La protection des données personnelles relève de plusieurs cadres juridiques :

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil
- La sûreté de l'État et le renseignement

Le RGPD

Le règlement européen renforce de façon significative les droits de l'usager sur ses données personnelles, notamment :

- Droit d'accès aux données, de rectification
- Selon les circonstances : droit à l'effacement, opposition
- Pour certains traitements (et très rare au MI) : portabilité des données

Politique de conformité des données personnelles du ministère de l'intérieur (PCDP-MI)

Les dispositions du RGPD ne parlent pas d'« application informatique » *stricto sensu* mais plutôt de « **traitement** »* . *Un traitement selon les dispositions de l'article 4 du RGPD constitue «* toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ». Il s'agit donc d'une définition très large qui désigne toute action sur les données personnelles. Un traitement peut être automatisé (une ou plusieurs applications) ou non (par exemple l'utilisation de la messagerie électronique pour envoyer un mail). Le RGPD s'applique donc à tout traitement, ainsi qu'à tous les fichiers (dont un simple tableau Excel), même papier.

Selon le RGPD, tout traitement doit avoir un **responsable de traitement** : dans la pratique celui qui détermine la finalité et les moyens du traitement, tel qu'un préfet d'un département, ou le directeur d'une administration centrale.

Règle : Chaque responsable de traitement a l'obligation de maintenir un *registre* des traitements dont il a l'initiative (ce qui exclut les traitements nationaux dont il n'est qu'utilisateur). Ce registre pourra être audité par la CNIL, et également, en tant que document administratif, communiqué sur demande citoyenne après occultation des mentions relatives à la sécurité (Cf annexe 2 de la note du DPD).

Lorsqu'un traitement est susceptible "d'engendrer un risque élevé pour les droits et les libertés des personnes physiques" (art 35 du RGPD), **le responsable du traitement doit faire mener une analyse d'impact du traitement sur la protection des données à caractère personnel**.

Remarque : l'analyse d'impact est souvent nommée PIA, Privacy Impact Assesment ou encore Étude d'Impacts sur la Vie Privée. (Cf annexe 3 de la note du DPD). Elle doit comporter l'avis du délégué ministériel à la protection des données avant sa validation par le responsable du traitement. L'analyse permet de vérifier la conformité juridique du traitement, d'évaluer les risques, et de mettre en place les mesures de sécurité appropriées. Si une homologation SSI est menée, il est recommandé de la coupler à l'analyse d'impact RGPD : les deux vont recenser les mêmes risques (notamment SSI), et elles différeront sur le périmètre des enjeux : impact sur les droits et libertés pour la PIA, impact sur le ministère pour l'homologation SSI.

La loi 78-17 Informatique et libertés

L'entrée en vigueur du RGPD a entraîné l'abrogation de certaines dispositions de cette loi. Toutefois, certaines autres dispositions restent en vigueur afin de préciser les marges de manœuvre nationales du RGPD.

Ainsi, le chapitre II de la loi fixe les conditions de licéité des traitements de données à caractère personnel ; le chapitre III contient les dispositions relatives à la Commission nationale de l'informatique et des libertés (CNIL).

Impacts pour l'application

La protection des données à caractère personnel, que celle-ci relève du RGPD ou de la loi n° 78-17 du 6 janvier 1978 (périmètre sécurité publique et infractions pénales) a un **impact important pour l'application** dans l'ensemble de son cycle de vie (conception, exploitation, décommissionnement). Ainsi que le spécifie le RGPD dans l'article 25, la protection des données doit être prise en compte **dès la conception, et par défaut** (*privacy by design*, *privacy by default*).

Le guide méthodologique de la CNIL « Analyse d'impact relative à la protection des données / La méthode», la démarche de mise en conformité s'appuie sur deux piliers :

- les **principes et droits fondamentaux**, sont réglementaires, et de facto obligatoires sans condition. On peut citer parmi les droits fondamentaux, l'information des personnes concernées, l'exercice des droits selon les situations (d'accès, de rectification, d'effacement, de limitation du traitement ....)
- la **gestion des risques sur les droits et libertés des personnes**, qui permet de déterminer les mesures techniques appropriées.

La mise en conformité nécessite la mise en place d'un ensemble de mesures, d'ordre fonctionnel, organisationnel, ou de mise en place de processus et techniques Ces dernières relèvent du présent cadre de cohérence technique.

Les relations avec les sous-traitants qui traitent des données personnelles pour le compte du ministère sont également impactées (nouveaux devoirs du sous-traitant). Le cadre juridique impose de :

- mettre en conformité avec l'article 28 du RGPD l'ensemble des contrats de sous-traitance;
- sécuriser les données ; à ce titre, la mise en place d'un dispositif de journalisation participe à cette sécurisation. La CNIL a émis une recommandation en 2021 en ce sens (cf. délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation.
- pour tous les traitements : mettre en place du concept de limitation du traitement des données (marquage de certaines données pour empêcher leur utilisation, sans toutefois les effacer).

La CNIL a édité un catalogue des mesures de mise en conformité (Analyse d'impact relative à la protection des données / Les bases de connaissance). Le tableau ci-dessous synthétise dans ce catalogue les mesures techniques relevant du CCT.

Mesures de protection des données (extrait guide CNIL cité ci dessus)	Mesures techniques
2 - Anonymisation	Identifier les données pertinentes et supprimer les données inutiles, sur les données. Sur les éléments d'identification directe ou à valeur rare, anonymiser selon la technique adéquate : randomisation ou généralisation.
3 - Archivage	La protection des données à caractère personnelle a des impacts sur la politique d'archivage. Cf fiche cycle de vie de la donnée. (offre de service Maarch RM, VITAM, chiffrement des données)
4 - Chiffrement	Le référentiel de composant du CCT préconise des composants de chiffrement, comme les composants PRIM'S
8 - Contrôle des accès logiques	Cf Fiches identification et authentification de l'agent et de l'usager
11 - Exercice des droits de l'usager	Ces nouveaux droits de l'usager induisent principalement des mesures organisationnelles.Du point de vue technique, la mise en œuvre des droits de l'usager nécessite un bon niveau d'authentification de celui-ci. _Cette fonction pourrait être utilement mutualisée par un téléservice au niveau ministériel (ou au-delà).
19 - Gestion des postes de travail	La protection des données à caractère personnelles implique le poste de travail. Cf fiche ETNA

Remarque : Le CCT préconise d'utiliser les mesures proposées par la CNIL comme un guide, dans le respect du contexte de l'application et du Ministère de l'Intérieur

Le guide CNIL « Analyse d'impact relative à la protection des données » dans son volet base de connaissance est un catalogue des mesures destinées respecter les exigences légales du RGPD et à traiter les risques.

Cycle de vie de la donnée et archivage

Principe recherché

Modalité d’archivage par nature de donnée

La donnée au sens large (document, donnée structurée ou non) a un cycle de vie, représentée par une température.

- "chaude" lorsqu'elle est utilisée quasi-quotidiennement par son service producteur et ses consommateurs. Durant cette phase, elle doit être pleinement disponible, dans les respects de la sécurité Si et de la protection des données personnelles.
- "tiède" à la fin de son usage public mais qu'elle reste à disposition du service producteur
- "froide" lorsque la donnée n'est plus utilisée qu'à des fins historiques scientifiques ou statistiques.

Selon le code du patrimoine article L 211-1 la définition de l’archivage est le suivant : 'Les archives sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité'.

Toutes les données sont considérées comme des archives dès leur création.

Impact sur les applications

L'application doit prendre en compte dans sa conception le cycle de vie de la donnée. C'est à dire les trois phases de l'archivage : courant, intermédiaire et définitif.

1. L'application détient exploite utilise des données chaudes, ou archives **courantes** dans la langue des archivistes.
2. Les données "tièdes" doivent être versées à un système prenant en charge les archives **intermédiaires**. Le ministère est doté d'un système d'archivage intermédiaire et il convient de s'assurer que le versement pourra être mis en place avec un minimum d'effort (respect des interfaces).
3. La dernière phase concerne l'archivage **définitif** - ou la destruction, le scénario est sous la responsabilité du responsable des archives ministérielles - Les archives définitives sont externalisées

Règles et recommandations

Ref	Statut	Intitulé
-	RG	Toute application doit prévoir dans sa conception le versement des données aux archives intermédiaires du ministère, selon la nature des données. Ce versement doit être conçu dans le respect de l'interface SEDA.
1129	RG	Lorsqu'une application comporte des données actives et des données historiques, elles doivent être stockées dans des bases ou des fichiers différents.
1444	RG	Toute application nécessitant un archivage des données doit prévoir dans sa conception le versement des données aux archives intermédiaires du ministère, dans le respect de l’interface SEDA.

Pilier sécurité

SSI et homologation

Principe recherché

La **sécurité (SSI)** d'une application est obligatoire, et une des conditions qui lui permettront d'offrir le service attendu en garantissant la disponibilité, la confidentialité et l'intégrité de l'information.

Le souci de la SSI concerne toutes les applications, elle ne se limite pas aux **SI « vitaux » ou « essentiels »** tels que les définit le SHFD.

La SSI doit être prise en compte dès la conception de l'application et jusqu'à son dé-commissionnement. Sa prise en compte est inscrite dans le projet par une **démarche d'intégration de la sécurité des systèmes d'information dans les projet, ou DISSIP**.

Dans le prolongement de la DISSIP, la sécurité de l'application est attestée, avant sa mise en production, par son **homologation de sécurité**. L'homologation permet à un responsable, s'appuyant sur l'avis des experts, de s'informer et d'attester aux utilisateurs d'un système d'information que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés. La décision d'homologation constitue donc un acte formel par lequel l'Autorité :

- atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;
- en accepte les risques résiduels

Le responsable de l'homologation de sécurité est l'AQSSI (Autorité Qualifiée pour la SSI, directeur ou directeur général nommé par arrêté ministériel) de la MOA du projet qui, pour piloter cette démarche, s'appuie sur son Conseiller à la Sécurité Numérique (CSN) conformément à l'IGI 1337 . Le chef de projet MoE et le RSSI MoE ont un rôle de support et d'accompagnement (sauf lorsque la MOE et sa propre MOA comme c'est le cas pour la DTNUM)

Les principaux acteurs de la SSI sont :

- Le Service du Haut Fonctionnaire à la Défense (SHFD)
- La chaîne SSI (RSSI…) qui irrigue l'ensemble du ministère, préfectures comme directions centrales, maîtrises d'œuvre (les DSI / acteurs SIC) comme maîtrises d'ouvrages (directions métier).

Impacts sur les applications

Pour être mise en production une application doit:

- être homologuée, sur la base d'un dossier contenant à minima :
  - une analyse de risque de type EBIOS Risk Manager
  - un ou des rapports d'audits (tests d'intrusion systèmatiques, de code, d'architecture, voire organisationnel pour les SI les plus sensibles)
  - un plan d'action SSI permettant de réduire les risques identifiés lors de l'analyse de risques et des audits
  - un support présenté à la commission d'homologation (présidé par l'AQSSI ou son représentant, le FSSI ou son représentant, CSN, MOA, MOE, RSSI)
- être en conformité vis a vis du RGPD :
  - avec éventuellement, et en parallèle de l'analyse de risques, une analyse d'impact au sens protection des données à caractère personnel / RGPD.

L'ensemble de ces livrables doivent donc être anticipés et provisionnés dans le budget de l'application, notamment

- l'éventuelle sous-traitance de l'analyse de risque EBIOS RM ou FEROS
- l'audit **PASSI**(Prestation d'Audit SSI) par un partenaire agréé ANSSI.

Le produit doit mettre en œuvre des composants de sécurité, selon les objectifs de sécurité établis durant la réalisation des démarches d'homologation et de conformité réglementaire . Ces composants de sécurité sont spécifiés dans le référentiel de produits du CCT (Partie 4 : Sécurité & interopérabilité), ainsi que dans les offres de services existantes, que celles-ci soient ministérielles ou interministérielles.

Par ailleurs, il est important d'appliquer les procédures d'exploitation de la sécurité (PES) qui définissent les règles et bonnes pratiques de sécurité applicables à tous les systèmes de la DTNUM et des SGAMIs : http://dtnum.minint.fr/index.php/la-s-s-i/pes

Règles et recommandations

Ref	Statut	Intitulé
-	RG	Rappel de la règle INT-HOMOLOG-SSI de la PSSI de l'État (Homologation de sécurité des systèmes d'information). Tout système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies.
-	RG	La sécurité de l'information (ou SSI) doit être prise en compte dès la conception de l'application. Cette prise en compte est structurée par la DISSIP, démarche d'intégration de la sécurité des systèmes d'information.
1385	RG	Il est OBLIGATOIRE d'identifier et de hiérarchiser les exigences de sécurité applicables au développement de l'application. Les arbitrages et les évolutions seront formalisés et tracés dans la documentation technique de réalisation ou le dossier de sécurité et d'homologation. Les exigences de sécurité applicables au développement sont constituées des éléments suivants : - La politique de sécurité des systèmes d'information applicable. - La sensibilité (confidentialité, intégrité, disponibilité) des données traitées et traitantes (code source, paramétrages, etc.). - L'analyse de risques exprimant les besoins et identifiant les objectifs de sécurité. - Les exigences de sécurité issues de la fiche d'expression rationnelle des objectifs de sécurité (EBIOS RM FEROS). - Les éventuelles menaces prises en compte au cours de l'analyse de risque. - Les éventuelles réglementations applicables (protection du secret, données personnelles, etc.). Ces exigences de sécurité sont exprimées par les directions métier aux équipes de projet (ou aux prestataires) concernées en amont du développement. Elles sont accompagnées d'une métrique convenue permettant de les hiérarchiser, et d'effectuer des arbitrages le cas échéant, en termes d'impacts métier.
		Il est OBLIGATOIRE d'identifier et de définir l'ensemble des rôles (métier et technique) et des privilèges strictement nécessaires et suffisants, pour le développement et la mise en oeuvre de l'application. Les rôles et privilèges associés aux acteurs du développement,

1386	RG	aux utilisateurs et aux exploitants de l'application tant sur le plan fonctionnel (métier), que sur le plan technique (MOE, équipe projet, administrateur, opérateur sauvegarde, etc.) doivent être formalisés au sein de la documentation technique du projet (cahier des charges fonctionnel, doctrine d'emploi, etc.) ou du dossier de sécurité et d'homologation (matrice de couverture des risques, dossier d'administration et d'utilisation, etc.).
1387	RG	Il est OBLIGATOIRE d'identifier et de définir les responsabilités (métier, technique, sécurité) des différents acteurs impliqués dans le développement. Les responsabilités des différents acteurs doivent être formalisées au sein du plan de management (ou équivalent) de projet de développement : - dans le domaine fonctionnel pour la partie métier ; - dans le domaine technique pour la partie architecture, programmation, intégration, etc. ; - dans le domaine de la vérification (revue de code, tests, etc.).
1388	RG	Il est OBLIGATOIRE d'identifier au sein de l'équipe de projet un correspondant sécurité garant de la prise en compte de l'ensemble des questions de sécurité pour le projet de développement.
1398	RG	Il est INTERDIT d'utiliser des protocoles, services ou algorithmes obsolètes pour la conception de nouvelles applications Exemples de services, protocoles ou algorithmes obsolètes et vulnérables : - rlogin, rsh, telnet, SNMP v1, SSH v1. - SSL, TLS v1.0, TLS v1.1. - RC4, MD5, SHA1, DES, 3DES. - LM, NTLM v1.
1420	RG	Il est OBLIGATOIRE de contrôler les données, à traiter et traitées, en entrée et en sortie des modules et des fonctionnalités développés et codés. Afin de prévenir les risques de types injection, les données doivent être : - filtrées en rejetant les caractères non autorisés et non pris en compte ; - normalisées en les réduisant à leur représentation la plus simple ; - validées en vérifiant le format, le type, l'origine ou encore la longueur des données attendues ; - encodées selon le contexte de traitement.
1433	RG	Il est INTERDIT de livrer une application informatique ou un logiciel incluant des paramètres d'authentification par défaut dans les codes sources ou les fichiers de configuration.
		L'application doit être conçue et

1110	RG	développée dans le strict respect des règles de sécurité en vigueur au Ministère en particulier, pour les applications Web, veiller à ne pas être sensible aux 10 principales menaces identifiées par l'OWASP (Open Web Application Security Project)
1334	RG	De manière à mettre en place le principe de moindre privilège, il est nécessaire de définir, au niveau du SGBD, des comptes de connexion correspondants aux différents rôles définis (type administrateur, relecteur, contributeur, …).
1336	RG	De manière à se prémunir des attaques dites XSS, et en sus du filtrage des données non sûres, l'encodage des mots clé de la grammaire HTML (HTML entity encoding) doit être effectué avant stockage ou affichage de données.
1342	RG	L'ensemble des informations relatives aux sessions (variables de l'utilisateur, droits d'accès, etc.) doivent être stockées côté serveur en les associant à un identifiant de session, qui doit être la seule information envoyée au client. En particulier, il est proscrit de transmettre ces données, par sérialisation par exemple, vers le client dans l'objectif d'assurer une persistance de ces données.
1337	RG	De manière à se prémunir du vol de cookie de session ou contenant des informations sensibles (authentification ou données) par attaque de type XSS, le mécanisme HTTPOnly doit être utilisé pour sécuriser l'emploi de ces cookies.
1348	RG	Des mécanismes de nettoyage des bases de données doivent être prévus afin de supprimer tout contenu illégitime (ex : existence de scripts en lieu et place d'une chaîne de caractère)
1434	rc	En cas de DISSIP renforcée il est RECOMMANDE d'armer la comitologie projet d'un COSEC (Comité Sécurité) dont le but serait de conduire la DISSIP, de préparer l'homologation et qui serait animé par le correspondant sécurité du projet.
1194	RG	La traçabilité des actions de gestion des utilisateurs et de leurs droits doit être assurée.

Pilier fabrique de code

Forges d'intégration et de déploiement continu

Principe recherché

La construction d'une nouvelle application, d'un nouveau produit, ou d'une évolution fonctionnelle s'appuie aujourd'hui dans une chaîne d'**intégration continue** puis de **déploiement continu**. Les hébergements cloud, du ministère (PI), ou de l'État (PI ou NUBO) renforcent cette tendance.

La **chaîne d'intégration continue** vise à la production, d'un paquetage déployable de l'application ou d'un produit.

La **chaîne de déploiement continu** vise à automatiser les opérations de déploiement réalisées manuellement par une équipe d'exploitation. Cette automatisation permet de fiabiliser le déploiement et d'augmenter la fréquence des livraisons, et des mises en production.

Les chaînes d'intégration et de déploiement s'appuient sur une usine de développement, ou forge, constituée d'un ensemble d'outils prenant en compte le contexte du Ministère de l'Intérieur.

Les services du numérique du ministère de l'intérieur (DTNUM, ANFSI, DSI de la PP et des SGAMI, ...) ont mis en place ces forges d'intégration et ou de déploiement.

Au sein du Ministère de l'Intérieur, deux usines logicielles sont disponibles :

- la forge [/DC] DTNUM, usine d'automatisation permettant les déploiements sur des offres IaaS.
- L'offre DevSecOps, usine logicielle Cloud Native, supportant le déploiements fréquents sur des offres de conteneurisation, et les besoins d'agilité des équipes projet

Dans la cadre du CCT traditionnel, la **forge DNUM [/ DC]**, dont les fonctions recouvrent à la fois intégration et déploiement, est décrite ci après.

La forge DNUM [/ DC]

La forge DNUM est l'offre de service de la DTNUM qui propose l'outillage nécessaire à l'intégration continue, au déploiement continu, et au suivi des projets **sur les offres IaaS cloud** :

- gitlab dépôt de code git des scripts de déploiement et autres configurations
- openstack, son API, et des fichiers d'architecture YAML permettant de piloter le cloud PI.
- ansible et python les langages de scripts
- CLI forge DC l'outil en ligne de commande qui assiste l'intégrateur et l'exploitant dans l'automatisation des commandes
- gitlab runner l'ordonnanceur utilisé pour automatiser les actions, à prendre en charge par le projet
- nexus le dépôt de binaires et proxy cache des dépôts applicatifs de l'internet (maven, npm, composer, ...)

Les fonctions d'intégration continue de la forge DNUM

La forge DNUM permet de créer des paquetages déployables, au travers une image de contenaire de manière privilégié. Le paquetage déployable à privilégier au sein de la forge DNUM est l'image Docker stockée sur le dépôt Nexus. La reconstruction de cette image Docker et sa validation est effectuée par un pipeline gitlab runner et des scripts Ansible. Outre ce paquetage déployable, les livrables suivant sont aussi obligatoirement présent sur le dépôt Gitlab :

- le code source de l'application
- une version incluse dans l'application (par exemple sur une page)
- une requête runtime de test
- les scripts de build (utilisés pour construire le paquetage)
- les scripts de test introduisant des conditions d'acceptabilité des User Story et qui incluent nécessairement des conditions d'exploitabilité du déploiement

Il est possible de synchroniser la forge DNUM avec des dépôts externes au ministère de l'intérieur de manière autonome au sein de son projet, par exemple dans un pipeline d'intégration continue. Il s'agit d'opération de type "pull" et à sens unique (l'intérieur va chercher ce qu'il y a à l'extérieur).

A cet effet, il est **OBLIGATOIRE** de reconstruire les binaires en interne au ministère de l'intérieur à partir des sources, des scripts, et des dépendances. Dans ces configurations hybrides (interne/externe), l'homogénéité des configurations influe sur la compatibilité développement/production. La chaîne d'intégration et notamment ses tests automatisés sont les garants de la livraison d'un paquetage déployable opérationnel en production.

Les fonctions de déploiement continu de la forge DNUM

La fonction de déploiement de la forge DNUM s'appuie sur les images gérées par le service Glance d'OpenStack. le CAEX (cahier d'exploitation) est aussi l'un des objectif de livrable de la forge DNUM. La forge DC nécessite la mise à disposition d'un CAEX (cahier d'exploitation) par application, qui référence les commandes permettant de démarrer, arrêter, sauvegarder, restaurer, superviser, déclencher un PRA, ... L'équipe de la forge DC normalise et accompagne l'exploitant en simplifiant ces procédures.

D'autres outils sont enfin actuellement utilisés au delà du déploiement pour gérer l'exploitation au titre de la sauvegarde et archivage, supervision. Il est obligatoire d'en tenir compte dans les scripts de déploiement pour entrer dans le cadre de l'offre d'exploitation du ministère :

- fournir une sauvegarde régulière en précisant son emplacement, sa fréquence, sa taille et son augmentation, ses règles d'archivage, et le processus de restauration
- fournir une ou plusieurs transaction de test sous la forme d'une URL retournant l'état de fonctionnement de l'application et un message éventuel ciblant le problème relevé

Impacts sur l'application de la Forge et de l'offre DevSecOps

Le ministère doit pouvoir conserver la maîtrise de ses applications et ses produits, que ceux-ci soient développés en interne ou en participation avec de prestataires externes. Cette maitrise passe par la détention du code source, des licences appropriées, des scripts de compilation et de paquetage, des scripts de construction des infrastructures et de déploiement. En définitive la capacité à reconstruire complètement l'application en cas de perte.

Les usines d'intégration et de déploiement du ministère sont un moyen d'atteindre cet objectif. Celles-ci permettent par ailleurs de mettre à disposition des concepteurs des composants réutilisables.

Règles et recommandations

Ref	Statut	Intitulé
-	RG	Le ministère doit pouvoir conserver la maîtrise de ses applications et ses produits. En conséquence il doit en détenir les codes sources ainsi que tous les scripts permettant leur reconstruction. Cette règle s'applique également à des produits non hébergés sur un site du ministère.
		Il est OBLIGATOIRE de définir et de formaliser un suivi rigoureux des dérogations, des bogues, des anomalies et des vulnérabilités tout au long du développement. Ce suivi, adossé à la matrice de couverture des risques, permettra d'évaluer le niveau de sécurité de l'application à la livraison, et de hiérarchiser les corrections à apporter. Les outils de suivi de développement

1389	RG	utilisés doivent intégrer les aspects bogues, anomalies et vulnérabilités afin de suivre l'état de sécurité de l'application tout au long de son cycle de vie, de la conception au retrait de service. Ils doivent intégrer les critères de causes et de conséquences des bogues de sécurité. Les critères de causes et de conséquences des bogues de sécurité doivent s'inspirer des sources ouvertes (OWASP, CWE, etc.). Ces éléments d'information viendront enrichir le dossier de vulnérabilités résiduelles du dossier de sécurité et d'homologation.
1399	RG	Il est OBLIGATOIRE de réaliser et maintenir à jour un inventaire des codes externes (bibliothèques, framework, API, etc.) utilisés par l'application.
1418	RG	Il est OBLIGATOIRE de disposer de conventions et de règles de codage adaptées au langage utilisé et de les appliquer dans le cadre du développement. Ces règles et conventions contribuent à la lisibilité et à la qualité du développement de l'application. Elles doivent être jointes à la documentation technique du projet de développement et constituent un référentiel de vérification lors des revues de code. Elles sont idéalement vérifiables à l'aide d'un outil adapté.
1423	RG	Il est OBLIGATOIRE de mettre en œuvre les fonctions de gestion (création, allocation, libération, etc.) et de manipulation (lecture, écriture, etc.) des ressources informatiques (mémoire, fichier, etc.) au plus près de leur utilisation effective.
1429	RG	Il est OBLIGATOIRE de réaliser des revues des codes sources pendant la phase d'implémentation et de programmation.
1430	RG	Il est OBLIGATOIRE de décrire et de formaliser les tests unitaires pour chaque unité de code lors de la phase d'implémentation et de programmation.
1431	RG	Il est OBLIGATOIRE de mettre en œuvre un processus d'intégration des modules l'application qui permet de vérifier l'absence de tout dysfonctionnements d'ordre fonctionnel et et technique sur le service lui-même, avec les services qu'il consomme et vis à vis de son contexte d'exécution.
1432	RG	Il est OBLIGATOIRE de gérer les anomalies détectées lors du processus d'intégration via les outils de suivi des bogues et des vulnérabilités utilisés pour l'application.
1104	RG	La gestion des anomalies (bug tracking) doit s'appuyer sur les outils

		recommandés par le CCT.
1106	RG	La documentation propre à chaque base de données centrale doit être constituée au minimum d'un dictionnaire de données, d'un ensemble de règles de gestion, et d'un modèle conceptuel de données (ou d'un diagramme de classe). Cette documentation, actualisée en fonction d'éventuelles mises à jour, doit être consultable.
1229	RG	Toute application développée à l'initiative et sous la responsabilité des échelons décentralisés doit: - ne répondre qu'à un besoin local dans le domaine applicatif ; - être réalisée avec les logiciels mentionnés dans le CCT ; - être maintenue localement ; - être en conformité avec la loi informatique et libertés et notamment faire l'objet des déclarations CNIL adaptées en fonction des traitements automatiques effectués ; - faire l'objet d'une utilisation limitée à un réseau local ; - faire l'objet d'une étude de sécurité pour elle-même et vis à vis du système d'information et de communication du ministère.
1428	rc	Il est RECOMMANDÉ d'effectuer des analyses statiques des codes sources pendant la phase d'implémentation et de programmation.
1107	rc	Le cadre de cohérence technique RECOMMANDE de respecter : - la démarche générale pour le développement des logiciels, - les règles de nommage et de codage, - les règles pour les journaux et les traces applicatives, - les règles pour la gestion des exceptions, - les règles pour la documentation du code source.
1108	rc	Le langage UML doit être privilégié pour la modélisation.
1391	RG	Il est OBLIGATOIRE d'utiliser un outil de gestion de version pour gérer et stocker les fichiers (codes sources, scripts, etc.) des applications.
1246	RG	Le code source d'une application ne doit pas être adhérent à un EDI.
1250	RG	L'usage de fichiers dits plats est déconseillé au profit de données structurées (JSON, XML...). L'utilisation de format autre que le XML doit être explicitement justifiée.
1265	RG	Les codes sources et la documentation des applications doivent être versionnés et centralisés à l'aide d'un outil de gestion de configuration référencé au CCT.
		Les applications PHP ou JAVA doivent

1279	RG	utiliser un framework de développement respectant au possible le modèle MVC et référencé au CCT.
1345	RG	Les jeux de tests permettant d'effectuer les vérifications de bon fonctionnement et de non régression de l'application doivent être fournis conformément à la procédure projet en vigueur en vue d'assurer la qualification des piles logicielles.

Pilier hébergement et exploitation

Mise en place d'un hébergement

Contexte

Grandes tendances

Le métier de l'hébergement est en pleine mutation sous l'effet de plusieurs tendances :

- Des **tendances technologiques**
  - de la virtualisation au cloud,
  - de la machine virtuelle au conteneur
  - avec comme dénominateur commun la mise en place des mécanismes d'automatisation : intégration continue, déploiement continu des applications comme des infrastructures.
- Des **tendances métier**
  - interpénétration du métier des "dev" (développeurs) et de celui des "ops" (exploitants hébergeurs) - le DevOps,
  - interpénétration des métiers et des développeurs avec l'expansion des méthodes agiles.
- Des **tendances organisationnelles au niveau de l'état**,
  - qui structure de façon croissante la production informatique sur un petit nombre de sites,
  - et qui travaille activement à l'intégration et à l'ouverture de tous les SI jusqu'ici gérés en silos.

Doctrine de l'Etat

Ces tendances se sont matérialisées par

- La "circulaire du 8 novembre 2018 relative à la doctrine d'utilisation de l'informatique en nuage par l'Etat" publiée sur LEGIFRANCE.
- La "circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État" publiée sur LEGIFRANCE.

Le tableau qui suit synthétise les deux solutions d'hébergement étatiques, cloud interne (cercle 1) et cloud externe ou commercial (cercle 3), avec leur conditions d'usage :

Cercle de solution	Condition d'usage	Nature du service	Disponibilité de offre	Catalogue
Cloud interne (cercle 1)	Données et traitements sensibles jusqu'à classification DR, Besoins régaliens	Service de type IaaS et PaaS, sur une base OpenStack, Service de type Caas sur une base Openshift/Kubernetes infrastructure interne (Cloud-PI et Nubo [MINEFI/DGFIP]). Conformité au référentiel SecNumCloud Essentiel de l'ANSSI	Cloud-PI : redondé sur deux sites, en cours de bascule sur une nouvelle architecture (GEN2)	Cloud-PI : PI - catalogue de services numériques du Ministère de l'Intérieur Nubo : offre de service
Cloud externe/commercial (cercle 3)	Données et traitements non sensibles	Service de type SaaS, sur cloud public	Marché Cloud Cercle 3 notifié depuis la fin du 1er semestre 2020.	[**Catalogue UGAP**] Une convention entre l'UGAP et la DTNUM est signée depuis début novembre 2020 pour le périmètre du ministère de l'Intérieur.
Cloud commercial de confiance (cercle 3 SecNumCloud)	Données et traitements peu sensibles	Service de type SaaS, sur cloud public	Marché Cloud Cercle 3 notifié depuis la fin du 1er semestre 2020.	[**Catalogue UGAP**] Une convention entre l'UGAP et la DTNUM est signée depuis début novembre 2020 pour le périmètre du ministère de l'Intérieur.

Les échanges sont autorisés entre clouds de cercle différent, dans le respect du contexte de l'application, des réglementations et cadres normatifs.

Impact sur les applications

La doctrine d'utilisation de l'informatique en nuage par l'État a des impacts importants sur l'hébergement d'une application. Le positionnement d'une application sur un cloud de 1er ou 3ème cercle dépend avant tout du niveau de sensibilité des données qu'il manipule. La décision peut aussi varier en fonction d'éléments contextuels comme des accords commerciaux ou des tensions diplomatiques.

Mise en place d'un hébergement

Sachant que les conventions de service de ministère à ministère sont appelées à se multiplier, cette fiche CCT de l'hébergement prend le parti de d'aligner l'offre de service d'hébergement ministérielle à l'offre de service inter-ministérielle telle qu'elle est décrite dans le schéma directeur des infrastructures d'hébergement inter-ministériel, réalisé sous l'égide de la DINUM avec les DSI ministérielles. Ce catalogue de service, issus de ce schéma directeur, décrit les types de prestations assurées dans le cadre d'une convention entre l'offreur de service et sont bénéficiaire. Cette description couvre les domaines suivants :

- la description du service
- le périmètre de la prestation
- la responsabilité des acteurs
- les modalités de mise en œuvre et de gestion des services considérés
- les engagements sur les niveaux de qualité de service.

Ce document de référence, reconnu au niveau inter-ministériel (CINUM), décrit des engagements de service standard, susceptibles d'être complétés par chaque offreur. La présente fiche, comme le catalogue dont elle s'inspire, est structurée selon une vue « bénéficiaire ». Elle adresse plusieurs types de bénéficiaires : des maîtrises d'oeuvre, consommatrice de services d'infrastructure (offre IaaS d'un cloud par exemple), des responsables de projets SI, et finalement des utilisateurs finaux (offres de type SaaS).

Remarque : cet hébergement peut ne concerner qu'une partie de l'application concernée.

Service offert par les hébergeurs

Les services d'hébergement et d'exploitation offerts au sein du ministère sont structurés par le catalogue sus-nommé qui en établit le cadre, et complétés par les services propres à chaque hébergeur. Ces offres s'appuient sur des infrastructures techniques dont l'architecture est exposée par chaque offreur de service.

Qui sont les hébergeurs du ministère

Le ministère possède aujourd'hui deux instances d'hébergement centrales ainsi que des instances d'hébergement zonales. Les instances d'hébergement centrales :

- Celui du centre d'hébergement (CH) de la DTNUM, qui héberge les plateformes ISOCELE et CLOUD PI, et opère trois sites :
  - le **SIR (Service informatique de Rosny)**, qui opère les salles B021 et B015 qui a une vocation interministérielle,
  - le **SIL (Service informatique de Lognes)**
  - le **SIVM (Service informatique du Val Maubouée)**.
- Celui du STIG, avec les centres de Rosny et Nogent. Le STIG a aujourd'hui une forte orientation sécurité intérieure.

Les instances d'hébergement zonales : les SGAMI, dont la préfecture de police de Paris et le SGAMI EST.

Outre leur centre d'hébergement zonal, Les SGAMI peuvent être Centre de Compétence national (CCN) sur des compétences qui leur sont spécifiques. Le chapitre des informations utiles liste les fonctions d'hébergement et d'exploitation des SGAMI et de leurs CCN.

Cycle de vie d'un hébergement et convention

La mise en place d'un hébergement est matérialisée par une demande d'hébergement, puis par l'élaboration et la signature d'une convention avec un hébergeur. Cf liens en fin de fiche. Ces actions s'intègrent dans un cycle de vie de l'hébergement

1. le bénéficiaire évalue ses besoins fonctionnels, les services nécessaires
2. le bénéficiaire fait une demande d'hébergement (cf formulaire en fin de fiche)
3. mise au point de la convention et de ses annexes et signature de la convention (cf conventions type en fin de fiche)
4. mise en place de l'hébergement et mise en production
5. fonctionnement courant
6. phase de réversibilité ou de dé-commissionnement

Règles et recommandations

Ref	Statut	Intitulé
-	RG	L'hébergement et l'exploitabilité d'une application sont à prendre en compte dès la phase amont du projet. Le centre d'hébergement doit être impliqué en amont du projet pour pouvoir assurer l'hébergement dans de bonnes conditions.
-	RG	Les DBA des hébergeurs ne sont pas habilités à répondre à des demandes d'extraction de données. Il appartient au concepteur de l'application de prévoir ses propres mécanismes d'extraction de données en conformité

		avec la loi ou les règlements européens.
-	RG	Les demandes d'hébergement d'application nationale sont traitées par le BPAH (DTNUM/SDAS). Les demandes sont à adresser au BRM (à l'adresse dnum-brm-contacts@interieur.gouv.fr)
-	RG	Les hébergements doivent être pensés « Cloud First ».
1347	RG	La journalisation doit être prévue dès la conception de l'application en indiquant notamment les personnes autorisées à y accéder, le mode d'administration et la durée de conservation.
1000	RG	Lorsque l'application comporte des chemins différents entre deux composants, le fichier de paramètres doit systématiquement contenir les éléments nécessaires à l'établissement du chemin principal, mais également à l'établissement d'un chemin de secours.
1008	RG	Une application utilisant un socle technique donné doit être développée dans un souci de compatibilité avec les autres applications utilisant ce même socle.
1009	RG	Les chefs de projets des services techniques centraux doivent respecter les dispositions relatives à la gestion de la plate-forme de production centralisée décrites en annexe du CCT.
1012	RG	La sauvegarde des données applicatives s'appuie sur des solutions mutualisées mises en œuvre par le ministère.
1014	RG	Les outils d'ordonnancement ne doivent pas être utilisés à des fins d'orchestration de processus métier.
1019	RG	Les journaux doivent respecter le format défini par le ministère conformément aux « Normes d'exploitation » dont les éléments nécessaires seront fournis aux titulaires.
1020	RG	"L'application doit disposer d'un mode trace, qui permet, en cas de défaillance, de comportement suspect, ou de test intensif, de suivre pas à pas son déroulement (horodatage du début et de la fin de chaque module applicatif au minimum). Ce mode trace doit ainsi permettre : - de suivre pas à pas le déroulement des opérations, à un niveau très fin (opération unitaire de donnée stockée, de transfert de message, de traitement) - de fournir le contenu des données liées aux opérations précédentes - d'indiquer précisément la position de l'opération dans le programme - de détailler précisément toutes les erreurs, ou problèmes, même internes - de fournir un niveau d'importance aux fonctions tracées, et aux erreurs - d'être activé, et de ne garder que le

		niveau d’information choisi (niveau du point précédent) - d’archiver les informations sur une période assez longue (compte tenu du niveau choisi), de l’ordre de plusieurs jours à plusieurs semaines - d’archiver ces informations et de les purger, ceci de manière automatique."
1021	RG	Le mode trace ne doit pas être dépendant d’un outil de développement particulier. Il doit être intégré dans le produit final, comme une option de fonctionnement.
1022	RG	Le mode trace doit pouvoir être activé/supprimé dynamiquement. Le niveau de détail du mode trace doit pouvoir être spécifié/modifié dynamiquement.
1023	RG	Tout processus d’une application doit «journaliser» le moment où il est lancé et le moment où il s’arrête. En cas de fin anormale, un message d’erreur doit être journalisé. La description de ce message doit être contenue dans la documentation de mise en exploitation.
1051	RG	Les journaux doivent être stockés sur les disques locaux des serveurs. L'application doit permettre de les dupliquer vers un système externe.
1052	RG	La journalisation technique repose aujourd'hui sur : l'association NAGIOS/application PROLOG ou SYSLOG. Le cahier des charges techniques précisera,en fonction du centre d'hébergement retenu, les spécifications .
1053	RG	Les environnements virtualisés doivent se faire sur les produits référencés au CCT.
1054	RG	Les disques d'un serveur connectés en architecture DAS (Direct Attached Storage) ont pour vocation de n'accueillir que le système d'exploitation et les logiciels de base.
1349	RG	Toute application (ou sous-application) doit: - être identifiée par un trigramme; - correspondre à une arborescence normalisée par environnement (production, développement, ...) sur un espace de stockage dédié; - l'espace de stockage peut comprendre un à plusieurs groupes de volumes (ou disques) et systèmes de fichiers.
1007	RG	Les informations/traitements sensibles doivent être hébergés sur des serveurs physiquement distincts des serveurs hébergeant des informations/traitements non sensibles.
1015	RG	Les opérations de télémaintenance par un prestataire externe, quand elles sont autorisées doivent systématiquement être réalisées avec le système SPAN

1002	rc	La répartition des flux est assurée par les équipements réseaux en frontalité de la ferme des serveurs de présentation.
1003	rc	Les mécanismes de haute disponibilité et de répartition de charge entre les serveurs de présentation et les serveurs d'application sont ceux présents nativement dans les technologies utilisées.
1004	rc	Pour le 'tiers' serveur base de données, les solutions de haute disponibilité unifiées, standard, et industrielles à disposition dans les centres de service sont privilégiées. A défaut les solutions fournies par les moteurs SGBD seront utilisées.
1010	rc	Les bases de données et les fichiers, doivent pouvoir (si le système de gestion de données le permet), être sauvegardés dynamiquement (sauvegardes dites bases «ouvertes»). L'application doit offrir la possibilité de verrouiller les mises à jour, tout en maintenant les consultations actives.
1013	rc	La sauvegarde des bases des données - soit sensibles et volumineuses - soit accessibles 24h/24 s'effectue à chaud en utilisant l'une des technologies suivantes : - les snapshots des solutions de stockage disque - l'agent spécifique du logiciel de sauvegarde lorsqu'il est disponible.
1018	rc	Dans le cas de journaux applicatifs répartis, il faut garantir le respect de la chronologie des opérations (exemples : horodatage, numéro de séquence, ...).
1099	RG	Toutes les actions contribuant au lancement ou à l'arrêt de l'application, doivent pouvoir être déclenchées par une commande unique et s'enchaîner ensuite automatiquement.
1220	RG	L'application ne doit ni imposer, ni embarquer de solution d'ordonnancement liées aux travaux d'exploitation et d'administration.
1289	RG	L'application doit permettre les points de synchronisation assurant une cohérence fonctionnelle pour les sauvegardes de contextes entiers.
1297	RG	Tous les paramètres de l'application doivent être regroupés dans un fichier.
1299	RG	L'application doit fournir une commande permettant d'interdire toute nouvelle connexion utilisateur, sans perturber les connexions en cours.
1300	RG	L'application doit fournir une commande permettant l'arrêt de toutes les connexions utilisateur en cours.
		"Toutes les actions d'exploitation et de

1302	RG	pilotage de l’application doivent pouvoir être déclenchées : - manuellement en mode «expert» (mode commande) ou en mode «novice» (interface graphique), - et automatiquement par un automate (soumission de scripts sans aucune intervention humaine)."
1303	RG	Le fonctionnement normal et quotidien d’une application ne doit pas solliciter une intervention directe d’un opérateur.
1304	RG	Tous les logs des applications doivent être tracés dans un fichier au format ASCII.
1319	RG	L’application ne doit pas imposer des composants logiciels qui seraient incompatibles avec la solution de sauvegarde mutualisée mise en oeuvre par le service d'exploitation.
1301	rc	L'application doit fournir une commande permettant de passer, à tout moment, en mode «consultation».
1035	RG	Dans les centres d'exploitation, les données ne sont pas stockées sur les serveurs mais sur des systèmes partagés (exemple SAN/NAS).

Pilier services transverses

Certaines offres du Ministères de l’intérieur sont à portée inter-ministériel – telles que l’offre DevSecOps et Cloud PI. En complément, des offres inter-ministérielles sont également disponibles à la consommation (ex. VITAM).

Services transverses

Contexte

Il est rappelé que la consultation des offres de services existantes est nécessaire dans le cadre de la conception de nouveaux produits ou de nouvelles applications. La mise en œuvre d'offres de service existantes, sous réserve de leur adéquation au besoin, est un facteur important de cohérence du SI de l'État, de non redondance, et d'économie des deniers publics.

Les DSI centrales proposent toutes des offres de service nationales. Certaines d'entre elles ont même un périmètre élargi au SI de l'État, comme par exemple le service d'horodatage, ou certains services de supervision. Ces offres de service sont présentées dans les catalogues de services des DSI et le CCT n'a pas vocation à se substituer à ces catalogues de service (cf chapitre ressources ci-dessous).

Les SGAMI peuvent également déployer des offres de services nationales. Ils le font sous le pilotage de l'une des deux DSI centrales (DTNUM ou ANFSI), avec un statut reconnu de Centre de Compétences Nationales (CCN).

Offres de service

Les offres sont disponibles via le portail de services PI:

- Produits de l'Intérieur (PI) _ Le catalogue de services numériques du Ministère de l'Intérieur

Liste des Centres de Compétences Nationales (CCN)

CCN	SGAMI chef de file	Commentaire
Référent outil de supervision LAN Télémétrobox	SGAMI Ouest	Lettre de mission du 29 juin 2016
Outils CMS - Content Management Systems (logiciel de gestion de contenus destinés à la création de sites Web Internet ou Intranet	SGAMI Ouest	Lettre de mission du 26 juillet 2017
Virtualisation en environnement WINDOWS	SGAMI Ouest	Lettre de mission du 7 mai 2018
Système d'information INPT (GOTI)	SGAMI Est	Lettre de mission du 16 février 2016
Cartographie : référentiel grande échelle (RGE)	SGAMI Est	Lettre de mission du 1er juillet 2016
Expertise outillage Gestion de parc (OCS-GLPI)	SGAMI Est	Lettre de mission du 3 octobre 2016
Cellule ingénierie et servitudes (CCNIS)	SGAMI Sud	Note du 14 janvier 2016
Expertise Réseaux Air/Sol – réseaux radio	SGAMI Sud	Lettre de mission du 9 janvier
Système d'information de sûreté de sites	SGAMI Nord	Lettre de mission du 19 décembre 2016
Système d'information de sûreté de sites	SGAMI Nord	Lettre de mission du 19 décembre 2016
Centre d'exploitation et de supervision de l'INPT (CESI)	SGAMI Sud-Est	Note du 19 février 2016
Renvoi d'images / flux vidéo	SGAMI Sud-Est	Lettre de mission du 27 avril 2016
Expertise Bureau distant (terminaux légers)	SGAMI Sud-Est	Lettre de mission du 27 juin 2016
Offre de gestion électronique de courrier Maarch	SGAMI Sud-Ouest	Lettre de mission du 13 juin 2016
Maarch	SGAMI Sud-Ouest	Présentation du CCN et des offres Maarch
CESAR	DILT PP	Formalisé depuis 2014. À actualiser dans le cadre du secours mutuel avec le CESI. En cours de finalisation par la PP/SDSICIF à date de parution des DNO 2019
Expertise Moyens de transmissions	DILT PP	A finaliser par la PP/SDSICIF à date de parution des DNO 2019