MINISTÈRE
DES OUTRE-MER

Liberté
Égalité
Fraternité

DIRECTION GENERALE DES OUTRE-MER

COMMANDEMENT DU SERVICE MILITAIRE ADAPTE

DEPARTEMENT ADMINISTRATION-FINANCES

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)

AYANT POUR OBJET LA

FOURNITURE, L'INTEGRATION, L'EXPLOITATION ET LE MAINTIEN EN CONDITION OPERATIONNELLE ET DE SECURITE DU SOCLE D'INFRASTRUCTURES DES SYSTEMES D'INFORMATION ET DE COMMUNICATION (SIC) DU SERVICE MILITAIRE ADAPTE (SMA)

Le présent CCTP comporte les trois annexes suivantes :

Annexe 1	Politique de sécurité des systèmes d'information de l'État (PSSIE)
Annexe 2	Guide d'hygiène informatique de l'ANSSI
Annexe 3	Catalogue des guides et référentiels techniques de l'ANSSI via portail Web

SOMMAIRE

ARTICLE I. MARCHÉ SOCLE « INFRASTRUCTURE DU SMA » **5**

I.1 OBJET DU MARCHE **5**
I.1.1 GESTION GLOBALE DES INFRASTRUCTURES SIC 6
I.1.2 MAINTIEN EN CONDITION OPERATIONNELLE (MCO) 6
I.1.3 MAINTIEN EN CONDITION DE SECURITE (MCS) 6
I.1.4 ÉVOLUTION ET MODERNISATION DU SOCLE 7
I.1.5 SUPERVISION ET HYPERVISION 7
I.1.6 CONTINUITE ET REPRISE D'ACTIVITE (PCA/PRA) 7
I.1.7 ACCOMPAGNEMENT DES ENTITES DU SMA 8
I.1.8 PERIMETRE GEOGRAPHIQUE ET CONTRAINTES 8
I.2 DECOUPAGE DES PRESTATIONS **9**
I.3 PHASE DU MARCHE **11**

ARTICLE II. PRÉSENTATION DU SERVICE MILITAIRE ADAPTÉ (SMA) **12**

II.1 LE SERVICE MILITAIRE ADAPTE (SMA) **12**
II.2 ORGANISATION DU SMA **13**
ORGANISATION GENERALE 13
IMPLANTATION GEOGRAPHIQUE 13
ROLE DU COMSMA 15
II.3 PRESENTATION DU DEPARTEMENT « SYSTEMES D'INFORMATION ET NUMERIQUE » (DSIN) **15**
II.3.1 DU SOCLE D'INFRASTRUCTURE SIC 16
II.3.2 DES SYSTEMES D'INFORMATION METIERS 16
II.3.3 SERVICES NUMERIQUES COLLABORATIFS 17
II.3.4 DE LA CYBERSECURITE 17
II.3.5 DU PILOTAGE ET DE LA TRANSFORMATION NUMERIQUE 18
II.4 PRESENTATION DES CELLULES SIC **18**
ROLE DES CELLULES SIC 18
RELATION AVEC LA DSIN 19

ARTICLE III. ARCHITECTURE DU SYSTÈME D'INFORMATION ET DU SOCLE NUMÉRIQUE DU SMA **20**

III.1 ARCHITECTURE GENERALE DU SOCLE **20**
III.2 ARCHITECTURE PHYSIQUE **21**
III.3 INFRASTRUCTURE DE VIRTUALISATION **23**
III.4 SAUVEGARDE ET REPLICATION **25**
III.5 ARCHITECTURE RESEAU DE LA SOLUTION **28**
III.5.1 ARCHITECTURE RESEAU GLOBALE 28
III.5.2 GESTION MULTI-ACCES ET RESILIENCE RESEAU 30
III.5.3 INTEGRATION DE LA SOLUTION SATELLITAIRE STARLINK 30
III.5.4 SECURISATION DES FLUX RESEAU 31
III.5.5 SUPERVISION DE LA CONNECTIVITE 31
III.5.6 GESTION DES FOURNISSEURS DE CONNECTIVITE 32
III.5.7 GESTION CAPACITAIRE DES ACCES INTERNET 33
III.5.8 CONNECTIVITE MICROSOFT 365 33
III.6 SUPERVISION ET HYPERVISION **34**
III.6.1 PRINCIPE GENERAL 34
III.6.2 SUPERVISION LOCALE ET CENTRALISEE 34
III.6.3 EXIGENCES RELATIVES A LA PLATEFORME DE SUPERVISION CHECKMK 35
III.6.4 SUPERVISION DES SERVICES MICROSOFT 365 36
III.7 OUTIL DE GESTION DE LA PRESTATION **37**
III.7.1 PRINCIPE GENERAL 37
III.7.2 FONCTIONNALITES ATTENDUES 38
III.7.3 INTEGRATION AVEC LES OUTILS DU SOCLE 39
III.7.4 ACCES ET UTILISATION 39
III.7.5 REPORTING ET PILOTAGE 40
III.7.6 EXIGENCES DE SECURITE ET DE CONFORMITE 41

ARTICLE IV. LAGON : SYSTÈME D'INFORMATION MÉTIER CENTRAL ET COEUR DU SMA **42**

IV.1 PRESENTATION GENERALE **42**
IV.2 ÉVOLUTION DU SYSTEME D'INFORMATION LAGON **43**
IV.3 CARACTERISTIQUES TECHNIQUES DE LA PLATEFORME AP4 ..... **44**
IV.4 IMPACTS SUR LE SOCLE D'INFRASTRUCTURE **46**

1. EXIGENCES EN MATIERE D'HEBERGEMENT 46
2. EXIGENCES RESEAU 47
3. EXIGENCES DE SECURITE 47
4. EXIGENCES DE SUPERVISION 47
5. EXIGENCES DE GESTION CAPACITAIRE 48
6. EXIGENCES DE SAUVEGARDE ET DE CONTINUITE D'ACTIVITE 48
IV.5 ARCHITECTURE D'HEBERGEMENT DU SI LAGON 49
IV.6 CONFIDENTIALITE ET SECURITE DES DONNEES 51

ARTICLE V. DÉCOUPAGE CONTRACTUEL DES PRESTATIONS ATTENDUES 53

V.1 PRINCIPES GENERAUX 53
V.2 PRESTATION N°1 : COMITOLOGIE 54
V.3 PRESTATION N°2 : MAINTIEN EN CONDITION OPERATIONNELLE (MCO) 57
V.3.1 ENGAGEMENTS DE SERVICE (SLA) 59
V.4 PRESTATION N°3 : MAINTIEN EN CONDITION DE SECURITE (MCS) 62
V.4.1 GESTION DES VULNERABILITES 62
V.4.2 SUPERVISION DE SECURITE 63
V.4.3 GESTION DES INCIDENTS CYBER 63
V.4.4 SECURISATION ET DURCISSEMENT 64
V.4.5 PROTECTION CONTRE LES RANSOMWARES 64
V.4.6 VEILLE ET CONFORMITE 65
V.5 PRESTATION N°4 : FORMATION ET TRANSFERT DE COMPETENCES 66
V.6 PRESTATION N°5 : REALISATION DE PROJETS SPECIFIQUES ET TRANSFORMATION NUMERIQUE 68
V.6.1 MODERNISATION DES INFRASTRUCTURES 68
V.6.2 DATACENTER DU CFSMA (PERIGUEUX) 68
V.6.3 CLOUD ET SOUVERAINETE 69
V.6.4 INTELLIGENCE ARTIFICIELLE 69
V.6.5 PLAN IMPACT DU COMSMA 70
V.6.6 ÉVOLUTIONS DU SI LAGON 70
V.6.7 ÉVOLUTIONS DES INFRASTRUCTURES DE CONNECTIVITE 70
V.7 PRESTATION N°6 : REVERSIBILITE 71
V.7.1 PLAN DE REVERSIBILITE 71
V.7.2 PERIMETRE 72
V.7.3 TRANSFERT DE CONNAISSANCE 72
V.7.4 PHASES DE REVERSIBILITE 73
V.7.5 REVERSIBILITE TECHNIQUE 73
V.7.6 CONTINUITE DE SERVICE 74
V.7.7 OBLIGATION DE COOPERATION 74

ANNEXES 75

ANNEXE 1 : POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DE L'ÉTAT (PSSIE) 76
ANNEXE 2 : GUIDE D'HYGIENE INFORMATIQUE DE L'ANSSI 77
1. GESTION DES ACCES 77
2. SECURISATION DES SYSTEMES 77
3. PROTECTION DES RESEAUX 77
4. GESTION DES POSTES ET SERVEURS 77
5. SAUVEGARDE ET RESILIENCE 77
6. SUPERVISION ET DETECTION 77
7. SENSIBILISATION ET ORGANISATION 78
ANNEXE 3 : CATALOGUE DES GUIDES ET REFERENTIELS TECHNIQUES DE L'ANSSI VIA PORTAIL WEB 79

Article I. MARCHÉ SOCLE « INFRASTRUCTURE DU SMA »

I.1 OBJET DU MARCHÉ

Le présent marché a pour objet la fourniture, l'intégration, l'exploitation, l'administration, le maintien en condition opérationnelle (MCO), le maintien en condition de sécurité (MCS), la supervision et l'évolution du socle d'infrastructures des systèmes d'information et de communication (SIC) du Service Militaire Adapté (SMA).

Ce socle, dénommé « infrastructure SMA » ou « socle numérique du SMA », constitue le cœur technique permettant l'hébergement, le fonctionnement, la sécurisation et l'interconnexion des systèmes d'information, des services numériques et des services collaboratifs du SMA.

Ce socle comprend :

- **l'infrastructure de serveurs ;**
- **la solution de virtualisation ;**
- **l'infrastructure de stockage ;**
- **la solution de sauvegarde ;**
- **la solution de sécurité ;**
- **l'infrastructure réseau ;**
- **le réseau d'entreprise du SMA (IntraSMA) ;**
- **les infrastructures d'accès à Internet et d'interconnexion des sites, reposant sur des solutions terrestres, mobiles et satellitaires ;**
- **les services de supervision et d'hypervision ;**
- **les services collaboratifs et de productivité numérique Microsoft 365.**

Il supporte notamment :

- **le système d'information LAGON**, SI principal du SMA, cœur du système d'information métier ;
- **le système d'information ASTECH**, dédié à l'administration et à la gestion des équipements du département PREV-LOG ;
- **le système d'information ALIZÉS**, dédié à la gestion et à l'administration de l'habillement du département DAF ;
- **le système d'information GLPI**, utilisé pour la gestion et l'administration des équipements numériques et multimédias du département DSIN ;
- **les services Microsoft 365 du SMA** reposant sur un tenant unique, comprenant notamment Exchange Online, Microsoft Teams, SharePoint Online, OneDrive Entreprise, Microsoft Entra ID, Microsoft Defender, Microsoft Purview et Microsoft Copilot ;
- ainsi que l'ensemble des **services transverses d'infrastructure** (annuaire, messagerie, stockage, supervision, sauvegarde, gestion des identités, services collaboratifs et outils d'administration etc…).

À ce titre, le titulaire devra assurer la cohérence globale du socle numérique du SMA afin de garantir la disponibilité, la performance, la sécurité, la résilience et l'évolutivité de l'ensemble des systèmes et services numériques hébergés.

I.1.1 Gestion globale des infrastructures SIC

Comprenant :

- les environnements serveurs (physiques et virtualisés) ;
- les infrastructures de stockage ;
- les systèmes de sauvegarde et de réplication ;
- les équipements réseau et de sécurité ;
- les infrastructures d'accès à Internet terrestres, mobiles et satellitaires ;
- les équipements de routage WAN, de répartition de charge et de bascule automatique ;
- les services d'interconnexion sécurisée entre les emprises du SMA ;
- les plateformes supportant les systèmes d'information LAGON, ASTECH, ALIZÉS et GLPI ;
- les services Microsoft 365 ;
- les services de gestion des identités et des accès numériques.

Le titulaire garantit la cohérence globale du socle permettant l'exploitation simultanée de l'ensemble des systèmes d'information, services collaboratifs et services numériques du SMA, avec une gestion maîtrisée des interdépendances et des flux de communication.

I.1.2 Maintien en condition opérationnelle (MCO)

Incluant :

- la garantie de disponibilité et de performance des SI hébergés ;
- la gestion des incidents et des problèmes ;
- la maintenance préventive et corrective ;
- le maintien à niveau des composants techniques (OS, hyperviseurs, middleware).

Une attention particulière sera portée à la **continuité de service des SI critiques**, notamment LAGON, ainsi qu'à la bonne qualité de service des SI de gestion (ASTECH, ALIZÉS, GLPI).

Le maintien en condition opérationnelle couvre également les services Microsoft 365, les infrastructures de connectivité WAN, les accès Internet multi-opérateurs, les services satellitaires et les solutions de supervision du SMA.

I.1.3 Maintien en condition de sécurité (MCS)

Conformément aux exigences réglementaires de l'État et aux référentiels en vigueur (notamment ANSSI), incluant :

- la gestion des vulnérabilités ;
- le durcissement des systèmes ;
- la segmentation des environnements (notamment entre SI) ;
- la supervision de sécurité ;
- la gestion des incidents cyber.

Le titulaire devra mettre en œuvre une approche **sécurité couvrant l'ensemble des SI hébergés**, en tenant compte de leurs spécificités fonctionnelles et de leur sensibilité.

Le maintien en condition de sécurité couvre également les services Microsoft 365, les mécanismes de gestion des identités, les accès conditionnels, les solutions de protection des postes et des données ainsi que les dispositifs de sécurité des infrastructures de connectivité.

I.1.4 Évolution et modernisation du socle

Le titulaire accompagne le SMA dans la transformation de son infrastructure en intégrant :

- l'évolution des architectures supportant les SI existants (LAGON, ASTECH, ALIZÉS, GLPI) ;
- l'intégration éventuelle de nouveaux SI ou services numériques ;
- le recours à des solutions **hybrides (on-premise / cloud de confiance)** lorsque pertinent ;
- l'automatisation des déploiements et de l'exploitation ;
- l'amélioration continue des performances et de la résilience ;
- l'intégration et l'évolution des services Microsoft 365 ;
- l'intégration des usages liés à l'intelligence artificielle, notamment Microsoft Copilot et les services numériques associés.

I.1.5 Supervision et hypervision

Le titulaire met en œuvre :

- une supervision unifiée de l'ensemble du socle ;
- une visibilité transverse sur l'ensemble des infrastructures, des systèmes d'information (LAGON, ASTECH, ALIZÉS, GLPI), des services Microsoft 365 et des infrastructures de connectivité ;
- une hypervision centralisée au niveau département systèmes d'information et numérique (DSIN) ;
- la production d'indicateurs de pilotage consolidés.

I.1.6 Continuité et reprise d'activité (PCA/PRA)

Le titulaire définit et maintient :

- des plans de continuité et de reprise adaptés aux différents SI ;
- des mécanismes de sauvegarde et de réplication ;

- des procédures de reprise testées régulièrement.

Les niveaux d'exigence peuvent être différenciés selon la criticité des SI, avec une priorité donnée au SI LAGON.

Les solutions d'accès Internet terrestres et satellitaires participent pleinement aux dispositifs PCA/PRA.

Le titulaire devra garantir la capacité de bascule automatique ou assistée vers les solutions alternatives de connectivité afin de maintenir les services critiques du SMA en cas de défaillance majeure d'un opérateur ou d'une infrastructure de télécommunication.

I.1.7 **Accompagnement des entités du SMA**

Le titulaire assure :

- le support aux équipes du département systèmes d'information et numérique (DSIN) ;
- l'appui aux cellules SIC en régiment ;
- l'assistance à l'exploitation des SI métiers (ASTECH, ALIZÉS, GLPI) ;
- l'accompagnement des utilisateurs et administrateurs des services Microsoft 365 ;
- le transfert de compétences dans les domaines de la cybersécurité, du cloud et des services collaboratifs.

I.1.8 **Périmètre géographique et contraintes**

Le marché couvre l'ensemble des emprises du SMA, en métropole et outre-mer, caractérisées par :

- une dispersion géographique importante,
- des niveaux de connectivité hétérogènes,
- une forte dépendance aux réseaux de télécommunications publics et satellitaires pour assurer les échanges entre les organismes du SMA ;
- des contraintes opérationnelles spécifiques.

Le titulaire devra garantir une **qualité de service homogène pour l'ensemble des SI déployés**, indépendamment de la localisation, ainsi que la continuité des communications numériques entre les emprises du SMA en s'appuyant sur les différentes solutions de connectivité disponibles (fibre, xDSL, 4G/5G et satellite).

I.2 DÉCOUPAGE DES PRESTATIONS

Le présent accord-cadre est agencé et structuré autour des prestations suivantes :

Prestation 1 : Comitologie

Cette prestation couvre l'ensemble des activités de gouvernance, de pilotage contractuel, de suivi des engagements de service, de reporting et d'amélioration continue.

Prestation 2 : Maintien en condition opérationnelle (MCO)

Cette prestation couvre l'exploitation, l'administration, la supervision, le support et le maintien en condition opérationnelle :

- des infrastructures serveurs ;
- des plateformes de virtualisation ;
- des infrastructures de stockage ;
- des solutions de sauvegarde ;
- des infrastructures réseau ;
- du réseau IntraSMA ;
- des infrastructures d'accès à Internet et de connectivité WAN ;
- des services satellitaires ;
- des outils de supervision et d'hypervision ;
- des services Microsoft 365.

Prestation 3 : Maintien en condition de sécurité (MCS)

Cette prestation couvre la protection des systèmes d'information et des services numériques du SMA conformément aux exigences réglementaires en vigueur, notamment :

- la gestion des vulnérabilités ;
- la supervision de sécurité ;
- la gestion des identités et des accès ;
- la sécurité des infrastructures de connectivité ;
- la sécurité des services Microsoft 365 ;
- la gestion des incidents cyber.

Prestation 4 : Formations et transfert de compétences

Cette prestation couvre les actions de formation, de sensibilisation et de transfert de compétences au bénéfice du DSIN, des cellules SIC et des utilisateurs autorisés.

Elle inclut notamment :

- les infrastructures SIC ;
- les outils de supervision ;
- les solutions Microsoft 365 ;
- les bonnes pratiques de cybersécurité ;
- les nouveaux services numériques déployés dans le cadre du marché.

Prestation 5 : Projets spécifiques et transformation numérique

Cette prestation couvre les évolutions majeures du système d'information et les projets ponctuels relevant notamment :

- des infrastructures numériques ;
- des réseaux et télécommunications ;
- du cloud de confiance ;
- de Microsoft 365 ;
- de l'intelligence artificielle et de Microsoft Copilot ;
- de la cybersécurité ;
- de la supervision ;
- des démarches d'homologation ;
- de la continuité et de la reprise d'activité ;
- de l'intégration de nouveaux systèmes d'information.

Prestation 6 : Réversibilité

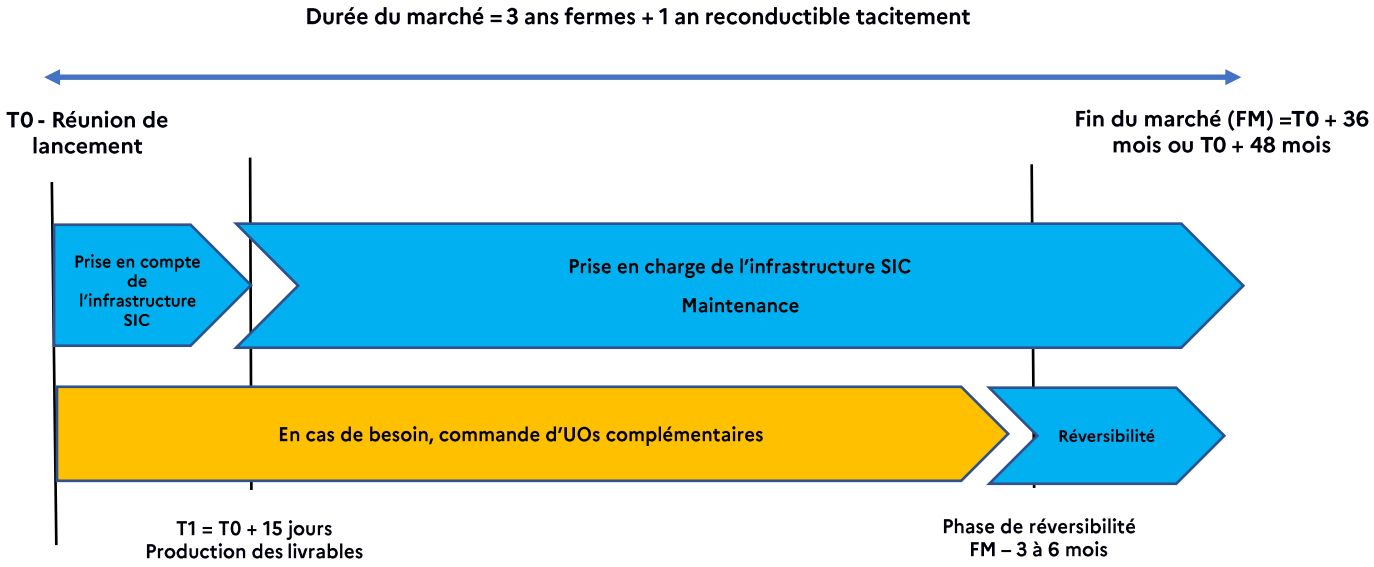
Cette prestation couvre la préparation, l'organisation et la réalisation de la réversibilité du marché, incluant l'ensemble des infrastructures, des données, des configurations, des documentations, des outils d'administration, des services Microsoft 365 et des moyens de connectivité du SMA.

Prestation 1	COMITOLOGIE
Prestation 2	MAINTIEN EN CONDITION OPERATIONNELLE (MCO)
Prestation 3	MAINTIEN EN CONDITION DE SECURITE (MCS)
Prestation 4	FORMATIONS ET TRANSFERT DE COMPETENCES
Prestation 5	PROJETS SPECIFIQUES ET TRANSFORMATION NUMERIQUE
Prestation 6	REVERSIBILITE

I.3 PHASE DU MARCHÉ

Les prestations décrites ci-dessus couvrent l'ensemble du cycle de vie du système d'information numérique du SMA, depuis son exploitation quotidienne jusqu'à son évolution et sa transformation.

Le titulaire devra garantir la cohérence globale des prestations afin d'assurer la disponibilité, la sécurité, la performance et l'évolutivité des infrastructures, des systèmes d'information métiers, des services collaboratifs Microsoft 365 et des infrastructures de connectivité du SMA.



Article II. PRÉSENTATION DU SERVICE MILITAIRE ADAPTÉ (SMA)

II.1 LE SERVICE MILITAIRE ADAPTÉ (SMA)

Le Service militaire adapté (SMA) est un dispositif relevant du ministère chargé des Outre-mer. Créé en 1961, il a pour mission principale de favoriser l'insertion socioprofessionnelle des jeunes ultramarins éloignés de l'emploi, en leur offrant un parcours de formation globale, à la fois professionnelle, éducative et civique.

À ce titre, le SMA accueille chaque année environ **6 000 volontaires**, âgés de 18 à 25 ans, dans les départements et collectivités d'outre-mer. Il leur propose un accompagnement individualisé visant l'acquisition de compétences professionnelles, le renforcement des savoirs fondamentaux et l'accès durable à l'emploi.

Le SMA repose sur :

- un **cadre militaire structurant**, favorisant discipline, cohésion et engagement ;
- une **approche globale de formation**, intégrant remise à niveau scolaire, formation professionnelle et accompagnement social ;
- une **finalité d'insertion durable**, mesurée notamment par le taux d'accès à l'emploi ou à la formation qualifiante.

Outre sa mission principale d'insertion, le SMA constitue également une **capacité d'appui aux autorités civiles et militaires**, notamment dans le cadre de plans d'urgence (catastrophes naturelles, soutien aux populations, opérations de secours).

Le SMA s'appuie désormais sur **un système d'information numérique structurant** permettant d'assurer le pilotage de ses activités, la gestion de ses ressources, la conduite des formations, la collaboration entre les organismes et le maintien de la continuité de ses missions sur l'ensemble de ses implantations.

Ce système d'information repose notamment sur :

- des infrastructures numériques réparties entre la métropole et les outre-mer ;
- des systèmes d'information métiers, dont le système LAGON ;
- des services numériques transverses ;
- des infrastructures de communication et d'interconnexion sécurisées ;
- un environnement collaboratif Microsoft 365 déployé au sein d'un tenant unique partagé par l'ensemble des organismes du SMA.

Compte tenu de la dispersion géographique des emprises, de l'éloignement de certains sites et de la criticité des activités conduites, la disponibilité, la sécurité, la résilience et la performance du système d'information constituent des enjeux majeurs pour le SMA.

II.2 ORGANISATION DU SMA

Le SMA est une organisation interarmées structurée autour d'un commandement central et d'unités déployées sur plusieurs territoires.

Organisation générale

L'ensemble de ces organismes s'appuie sur un système d'information unique permettant d'assurer la continuité des activités administratives, logistiques, financières, de gestion des ressources humaines, de formation et de pilotage du SMA.

Ce système d'information repose sur des infrastructures distribuées, des services numériques centralisés, un réseau d'entreprise sécurisé (IntraSMA) ainsi qu'un environnement collaboratif Microsoft 365 commun à l'ensemble des organismes du SMA.

Le dispositif comprend :

- **Le commandement du service militaire adapté (COMSMA)**, situé à Paris, chargé du pilotage global du dispositif ;
- **Les régiments du SMA (RSMA)**, implantés dans les territoires ultramarins ;
- **Un centre de formation en métropole (Périgueux)**, notamment dédié à la mobilité et à la formation complémentaire.

Implantation géographique

Le SMA est présent sur les principaux territoires d'outre-mer :

- Martinique
- Guadeloupe
- Guyane
- La Réunion
- Mayotte
- Nouvelle-Calédonie
- Polynésie française

ainsi qu'en métropole (structure de formation et d'appui).

Cette répartition géographique fait du système d'information du SMA l'un des systèmes d'information les plus répartis géographiquement de l'administration, avec des implantations situées sur plusieurs océans, fuseaux horaires et zones de connectivité hétérogène.

Les infrastructures numériques du SMA doivent ainsi permettre de garantir un niveau homogène de service et de sécurité malgré des contraintes importantes de distance, de transport, d'approvisionnement et de qualité des réseaux de télécommunications.

Les vingt-cinq (25) sites du SMA correspondant au périmètre du marché sont :

- **L'état-major du SMA (COMSMA)** est situé Paris, au sein des locaux du ministère des Outre-mer situés rue Oudinot, Paris 7ème ;
- **Le centre de formation du SMA (CFSMA)**, mono-site est situé à Périgueux ;
- **Le régiment du service militaire adapté de Martinique (RSMA-Mq)**, est réparti sur 2 sites :
  - Lamentin (site principal),
  - La maison du SMA (Fort de France).
- **Le régiment du service militaire adapté de Guadeloupe (RSMA-Ga)**, est réparti sur 2 sites :
  - Baie-Mahault (site principal),
  - La maison du SMA (Saint-Martin).
- **Le régiment du service militaire adapté de Guyane (RSMA-Gy)**, est réparti sur 3 sites :
  - Saint-Jean-du-Maroni (site principal),
  - Cayenne,
  - La maison du SMA (Saint-Laurent-du-Maroni).
- **Le régiment du service militaire adapté de Mayotte (RSMA-My)**, sera réparti sur 3 sites :
  - Combani (site principal),
  - Chirongui (site à venir),
  - La maison du SMA (Mamoudzou).
- **Le régiment du service militaire adapté de La Réunion (RSMA-Re)**, est réparti sur 4 sites :
  - Saint-Pierre (site principal),
  - Saint-Denis,
  - Bourg-Murat,
  - La maison du SMA (Saint-Denis).
- **Le régiment du service militaire adapté de Nouvelle-Calédonie (RSMA-Nc)**, sera réparti sur 5 sites :
  - Koumac (site principal),
  - Koné,
  - Bourail,
  - Nouméa (site à venir),
  - La maison du SMA (Nouméa).
- **Le régiment du service militaire adapté de Polynésie-Française (RSMA-Pf)**, est réparti sur 4 sites :
  - Arue (site principal),
  - Hiva Oa aux Marquises (1 500 Km de Tahiti),
  - Tubuaï aux îles Australes (700 Km de Tahiti),
  - Hao dans l'archipel des Tuamotu-Gambier (900 Km de Tahiti).

Cette organisation répartie confère au SMA une **forte dimension territoriale**, avec des contraintes spécifiques en matière :

- d'infrastructures ;

- de connectivité ;
- de continuité de service ;
- de soutien logistique.

Ces contraintes géographiques rendent indispensable la mise en œuvre de solutions de connectivité adaptées reposant notamment sur des accès Internet multi-opérateurs, des infrastructures de routage sécurisées, des solutions de continuité de service et, pour certains sites, des technologies satellitaires telles que Starlink.

Rôle du COMSMA

Le COMSMA assure la direction et la coordination de l'ensemble du dispositif. À ce titre, il :

- définit les orientations stratégiques du SMA ;
- pilote les ressources (humaines, financières et logistiques) ;
- assure la cohérence des actions menées par les régiments et le centre de formation ;
- garantit la performance globale du dispositif.

Il veille également à la cohérence des outils numériques, des systèmes d'information métiers et des services collaboratifs déployés au profit de l'ensemble des organismes du SMA.

Il s'appuie sur plusieurs départements et pôle fonctionnels, notamment :

- opérations (POPS) ;
- administration et finances (DAF) ;
- ressources humaines (DRH) ;
- logistique et prévention (DLOG-PREV) ;
- systèmes d'information et numérique (DSIN).

Dans ce cadre, le COMSMA porte la **gouvernance des systèmes d'information du SMA**, dont fait partie le socle d'infrastructure objet du présent marché.

Il définit les orientations stratégiques en matière de transformation numérique, de cybersécurité, de services collaboratifs, de modernisation des infrastructures et d'évolution des systèmes d'information.

À ce titre, il s'appuie notamment sur le département des systèmes d'information et du numérique (DSIN), responsable du pilotage technique du système d'information, de l'environnement Microsoft 365, de la cybersécurité et du socle numérique du SMA.

II.3 PRÉSENTATION DU DÉPARTEMENT « SYSTÈMES D'INFORMATION ET NUMÉRIQUE » (DSIN)

Le département « Systèmes d'Information et Numérique » (DSIN) relève du COMSMA et constitue l'entité centrale en charge de la conception, de la mise en œuvre, de l'exploitation, de la sécurisation et de l'évolution du système d'information du SMA.

À ce titre, la DSIN :

- définit les **orientations stratégiques en matière de systèmes d'information, de services numériques et de transformation numérique** ;
- assure la **gouvernance, l'urbanisation et la cohérence globale du système d'information** ;
- pilote les **marchés d'infrastructure, de services numériques et de cybersécurité** ;
- garantit la **cohérence technique, la sécurité, la résilience et la performance du système d'information à l'échelle de l'ensemble des organismes du SMA ;**
- assure la **gouvernance des services numériques collaboratifs et du tenant Microsoft 365 du SMA ;**
- accompagne **les projets de modernisation, de cloud, de valorisation de la donnée et d'intelligence artificielle**.

Il est notamment responsable :

II.3.1 Du socle d'infrastructure SIC

Le DSIN assure la gouvernance du socle numérique du SMA comprenant notamment :

- les infrastructures serveurs ;
- les environnements de virtualisation ;
- les infrastructures de stockage ;
- les systèmes de sauvegarde et de réplication ;
- les infrastructures réseau ;
- le réseau d'entreprise IntraSMA ;
- les infrastructures d'accès à Internet ;
- les solutions satellitaires ;
- les outils de supervision et d'hypervision.

À ce titre, il assure :

- la conception et l'évolution des architectures techniques ;
- l'exploitation centralisée et le pilotage des infrastructures ;
- le suivi des prestations MCO et MCS ;
- la définition des normes techniques ;
- le pilotage de la résilience et de la continuité de service.

II.3.2 Des systèmes d'information métiers

La DSIN assure ou coordonne l'administration technique des principaux SI du SMA :

- **LAGON** : système d'information principal du SMA, cœur métier ;
- **ASTECH** : système d'administration et de gestion des équipements (département PREV-LOG) ;
- **ALIZÉS** : système de gestion de l'habillement (département DAF) ;
- **GLPI** : système de gestion des équipements numériques et multimédias (DSIN).

Dans ce cadre, la DSIN garantit :

- la disponibilité et la performance technique des SI ;
- leur intégration dans le socle d'infrastructure ;
- leur sécurisation et leur conformité.

La DSIN assure également l'intégration de ces systèmes d'information avec les services numériques transverses du SMA, notamment les services collaboratifs Microsoft 365, les mécanismes d'authentification et les infrastructures de communication.

II.3.3 **Services numériques collaboratifs**

Le DSIN assure la gouvernance et l'administration du tenant Microsoft 365 unique du SMA.

À ce titre, il pilote notamment :

- Exchange Online ;
- Microsoft Teams ;
- SharePoint Online ;
- OneDrive Entreprise ;
- Microsoft Entra ID ;
- Microsoft Defender ;
- Microsoft Purview ;
- Microsoft Copilot ;
- Power Platform.

Dans ce cadre, la DSIN garantit :

- la cohérence des usages numériques ;
- la gestion des identités et des accès ;
- la sécurité des services collaboratifs ;
- l'intégration avec les systèmes d'information du SMA ;
- la maîtrise des licences et des services associés.

II.3.4 **De la cybersécurité**

- de la déclinaison des politiques de sécurité ministérielles ;
- de la mise en œuvre des mesures de protection ;
- du pilotage du maintien en condition de sécurité (MCS) ;
- de la sécurité des services Microsoft 365 ;
- de la gestion des identités numériques ;
- de la gouvernance des accès privilégiés ;
- du pilotage des dispositifs de détection et de protection ;
- de la conformité aux référentiels de l'État et de l'ANSSI ;
- du pilotage des démarches d'homologation de sécurité ;
- de la gestion des incidents de sécurité.

II.3.5 Du pilotage et de la transformation numérique

Le DSIN pilote les projets de modernisation du système d'information du SMA, notamment :

- La modernisation des infrastructures numériques ;
- l'intégration de solutions cloud ou hybrides ;
- l'automatisation de l'exploitation ;
- l'évolution des services Microsoft 365 ;
- le déploiement des services d'intelligence artificielle ;
- les projets liés à Microsoft Copilot ;
- la valorisation et l'exploitation des données ;
- l'amélioration continue de la qualité de service et de la performance numérique.

Le DSIN constitue ainsi **l'autorité technique centrale du SMA** pour l'ensemble des sujets relatifs aux systèmes d'information, aux infrastructures numériques, aux services collaboratifs Microsoft 365, à la cybersécurité, à la transformation numérique et à la gouvernance des services numériques du SMA.

II.4 PRÉSENTATION DES CELLULES SIC

Au niveau local, chaque régiment et centre de formation du SMA dispose **d'une cellule SIC** chargée de la mise en œuvre opérationnelle, du maintien en condition des moyens numériques et de communication ainsi que du support de proximité au profit des utilisateurs.

Les cellules SIC constituent **le relais local** du département des systèmes d'information et du numérique (DSIN) pour l'exploitation des infrastructures, des services numériques et des systèmes d'information déployés au sein des organismes du SMA.

Rôle des cellules SIC

Les cellules SIC assurent notamment :

- le **support de proximité aux utilisateurs** ;
- **l'exploitation locale** des infrastructures numériques (postes de travail, réseaux locaux, équipements informatiques et moyens de communication) ;
- la participation **aux opérations de déploiement, de maintenance et de renouvellement des équipements ;**
- le **relais des actions** menées par le DSIN ;
- **l'accompagnement des utilisateurs** dans l'usage des services numériques du SMA ;
- le support de **premier niveau des services Microsoft 365** ;
- la participation à **la gestion des incidents et demandes de service** ;
- la contribution à **la supervision locale** des infrastructures et des services ;
- l'assistance à **la mise en œuvre des mesures de cybersécurité** définies par le DSIN.

Relation avec la DSIN

Les cellules SIC agissent en coordination permanente avec le DSIN selon un modèle :

- **centralisé pour la gouvernance,** la cybersécurité, les infrastructures cœur, les services Microsoft 365 et les systèmes d'information nationaux ;
- **décentralisé pour l'exploitation de proximité**, le support utilisateur et les interventions locales.

Le titulaire devra intégrer les cellules SIC dans son dispositif opérationnel afin de garantir une coopération efficace entre les équipes locales, le DSIN et les équipes du titulaire.

Les cellules SIC constituent un maillon essentiel du dispositif numérique du SMA. Elles participent notamment :

- à la remontée des incidents ;
- au suivi des performances ;
- à l'application des politiques de sécurité ;
- à la gestion des demandes de service ;
- au suivi des équipements et des infrastructures locales ;
- à la supervision de proximité ;
- à la continuité des activités numériques ;
- à l'accompagnement des utilisateurs dans l'usage des outils collaboratifs et des services Microsoft 365.

Elles contribuent à la qualité de service globale du système d'information du SMA et constituent les interlocuteurs privilégiés des utilisateurs sur les différents sites du périmètre du marché.

Dans le cadre du présent marché, le titulaire devra s'appuyer sur les cellules SIC pour la réalisation de certaines opérations locales, notamment :

- les interventions de proximité ;
- les déploiements de matériels ;
- les opérations de recette ;
- les actions de maintien en condition opérationnelle ;
- les formations de premier niveau ;
- les opérations de continuité d'activité ;
- les opérations de cybersécurité définies par le DSIN.

Le titulaire veillera à maintenir une coopération étroite avec les cellules SIC afin de garantir la qualité de service attendue sur l'ensemble des emprises du SMA.

Article III. ARCHITECTURE DU SYSTÈME D'INFORMATION ET DU SOCLE NUMÉRIQUE DU SMA

III.1 ARCHITECTURE GÉNÉRALE DU SOCLE

Le socle numérique du SMA constitue l'ensemble des infrastructures, plateformes et services numériques permettant l'hébergement, l'exploitation, l'interconnexion, la sécurisation et le pilotage du système d'information du Service Militaire Adapté.

Il repose sur une architecture distribuée et résiliente et sécurisée, organisée autour :

- de **plateformes d'hébergement locales** déployées au sein des régiments et du centre de formation ;
- d'un **pilotage centralisé assuré par le département des systèmes d'information et du numérique (DSIN)** ;
- d'une **interconnexion réseau sécurisée** des organismes du SMA reposant sur le réseau IntraSMA et des infrastructures de connectivité multi-opérateurs ;
- de **services numériques centralisés et mutualisés** ;
- de mécanismes permettant la **continuité et la reprise d'activité** ;
- **d'outils de supervision et d'hypervision centralisés**.

Le socle numérique supporte notamment :

- le système d'information LAGON (SI cœur) ;
- ASTECH ;
- ALIZÉS ;
- GLPI ;
- les services Microsoft 365 du SMA ;
- les services d'identités numériques ;
- les services collaboratifs ;
- les services de supervision ;
- les services numériques transverses nécessaires au fonctionnement du SMA.

L'environnement Microsoft 365 repose sur un tenant unique partagé par l'ensemble des organismes du SMA et constitue une composante à part entière du système d'information.

Les infrastructures de connectivité comprennent notamment :

- les réseaux locaux ;
- le réseau d'entreprise IntraSMA ;
- les accès Internet multi-opérateurs ;
- les infrastructures WAN ;
- les solutions satellitaires ;
- les dispositifs de routage, de répartition de charge et de bascule automatique des flux.

L'architecture devra permettre :

- une **haute disponibilité des services critiques** ;
- une **isolation logique des différents systèmes d'information** ;
- une **sécurisation cohérente de l'ensemble des composants** ;
- une **évolutivité (scalabilité) du système d'information** ;
- une **gestion centralisée tout en conservant une autonomie locale minimale** ;
- **l'intégration de nouveaux systèmes d'information et services numériques** ;
- **l'intégration de services cloud et de services d'intelligence artificielle** lorsque cela est pertinent ;
- une **résilience adaptée aux contraintes géographiques** propres aux implantations du SMA.

Le titulaire devra garantir la cohérence globale de cette architecture afin d'assurer la continuité des missions du SMA, indépendamment de la localisation des utilisateurs, des infrastructures ou des services numériques utilisés.

L'architecture cible du SMA repose sur le principe d'un système d'information hybride associant :

- des infrastructures locales ;
- des infrastructures centralisées ;
- des services numériques externalisés ;
- des services collaboratifs Microsoft 365 ;
- des solutions cloud de confiance ;
- des services d'intelligence artificielle.

Le titulaire devra prendre en compte cette trajectoire d'évolution dans l'ensemble de ses prestations et accompagner le SMA dans la modernisation progressive de son système d'information.

III.2 ARCHITECTURE PHYSIQUE

L'infrastructure du SMA repose sur des équipements répartis sur l'ensemble des emprises du Service militaire adapté, en métropole et outre-mer.

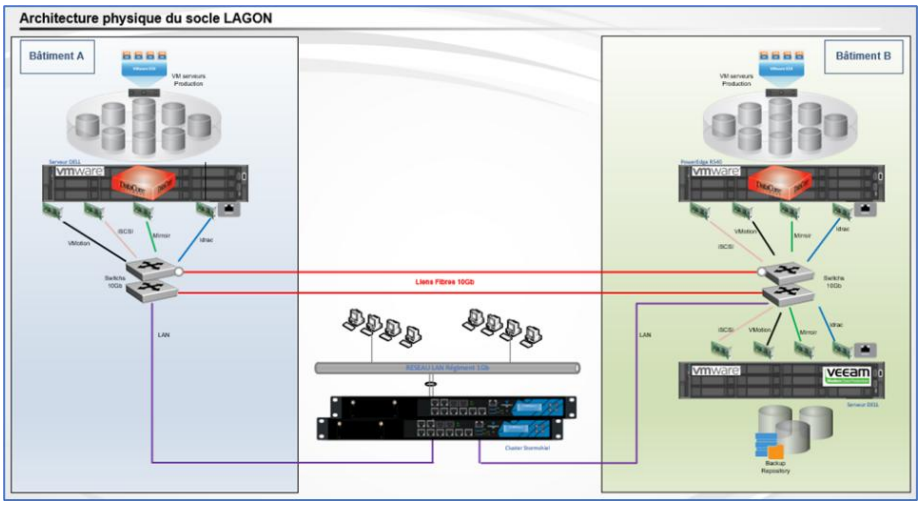
Cette infrastructure comprend notamment :

- des **serveurs physiques** hébergeant les environnements virtualisés ;
- des **baies de stockage** (SAN, NAS ou technologies équivalentes selon les sites) ;
- des **équipements réseau** (commutateurs, routeurs, pare-feux et équipements de sécurité) ;
- des **équipements de sécurisation électrique** (onduleurs, groupes électrogènes ou dispositifs équivalents selon les sites) ;
- des **terminaux satellitaires** ;
- des **équipements de connectivité opérateurs** ;
- des **équipements SD-WAN ou équivalents** ;

- des **dispositifs de secours télécoms** ;
- des **équipements dédiés à la supervision et à l'hypervision** ;
- des **équipements participant aux services d'authentification, d'annuaire et de gestion des identités numériques** ;
- des **équipements assurant l'interconnexion sécurisée des organismes du SMA via le réseau IntraSMA**.

Cette infrastructure est conçue pour assurer le fonctionnement des systèmes d'information métiers, des services numériques transverses, des services collaboratifs Microsoft 365 et des infrastructures de communication du SMA.

Les services Microsoft 365 et les éventuels services cloud de confiance s'appuient sur cette architecture physique via des infrastructures de connectivité sécurisées garantissant l'accès des utilisateurs aux services numériques centralisés.



Chaque emprise dispose d'un socle local permettant :

- l'hébergement des services essentiels lorsque cela est nécessaire ;
- le maintien d'une activité minimale en cas de perte de connectivité ;
- la continuité des opérations critiques ;
- le maintien des services locaux indispensables aux missions opérationnelles ;
- la résilience des communications avec les autres organismes du SMA.

Les architectures locales sont conçues pour fonctionner dans des environnements présentant des contraintes de connectivité variables et pour permettre une reprise rapide des activités en cas d'incident majeur.

Le titulaire devra garantir :

- la **redondance des composants critiques** (alimentation, stockage, réseau et connectivité) ;
- la **standardisation des architectures** entre sites ;
- la **maîtrise de l'obsolescence matérielle** ;

- la **cohérence des architectures locales et centralisées** ;
- la **capacité d'évolution des infrastructures** pour répondre aux besoins futurs du SMA ;
- la **compatibilité avec les architectures cloud hybrides et les services Microsoft 365** ;
- la **prise en compte des contraintes spécifiques des territoires ultramarins** ;
- la **résilience des infrastructures de communication et de connectivité**.

Le titulaire assure un suivi permanent de l'état des infrastructures physiques du SMA et formule toute recommandation permettant :

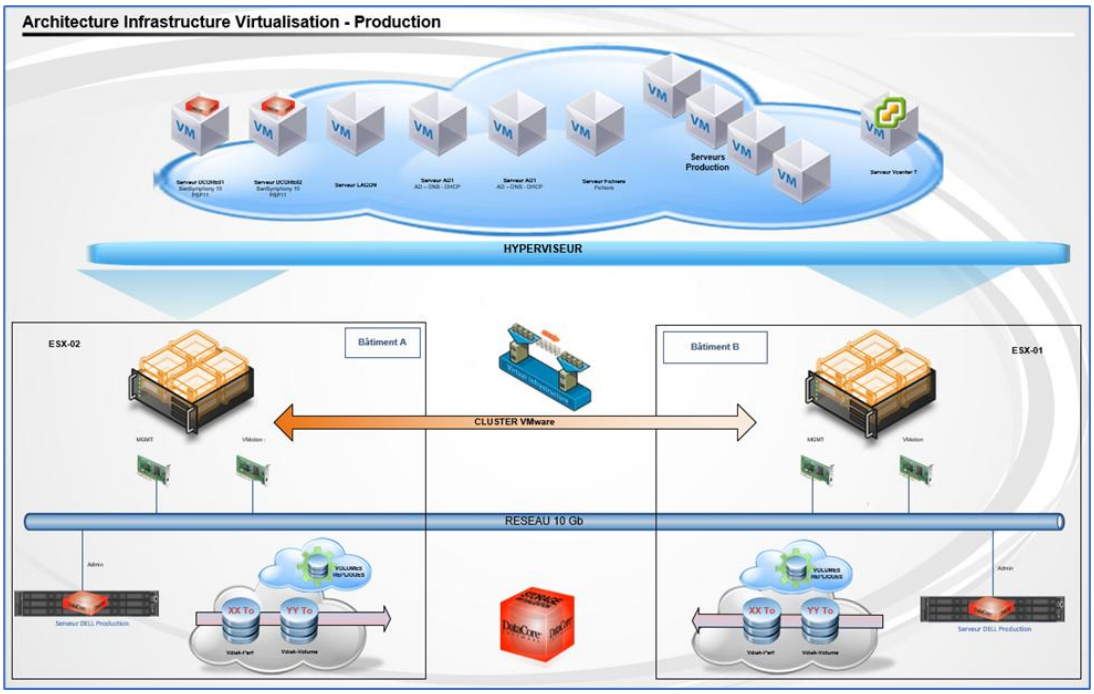
- d'améliorer la disponibilité des systèmes d'information ;
- d'augmenter la résilience des sites ;
- de réduire les risques d'obsolescence ;
- d'optimiser les coûts d'exploitation ;
- d'accompagner les évolutions des usages numériques, notamment liés aux services Microsoft 365, au cloud et à l'intelligence artificielle.

III.3 INFRASTRUCTURE DE VIRTUALISATION

Le socle numérique du SMA s'appuie sur une infrastructure de virtualisation permettant :

- la mutualisation des ressources matérielles ;
- la flexibilité de déploiement des systèmes d'information ;
- la haute disponibilité des services ;
- l'optimisation de l'exploitation des ressources informatiques ;
- l'évolutivité des infrastructures en fonction des besoins du SMA.

Cette infrastructure constitue le socle d'hébergement des systèmes d'information métiers, des services techniques transverses et des composants nécessaires au fonctionnement global du système d'information du SMA.



Le titulaire devra assurer :

- l'exploitation et l'administration de la plateforme de virtualisation ;
- la gestion des ressources (CPU, mémoire, stockage et réseau) ;
- la mise en œuvre des mécanismes de haute disponibilité (HA) ;
- la migration à chaud des ressources lorsque nécessaire ;
- la mise à jour et la sécurisation des hyperviseurs ;
- le suivi des performances et de la consommation des ressources ;
- la gestion des capacités et des projections d'évolution des plateformes ;
- la production des indicateurs nécessaires au pilotage de l'infrastructure.

Une attention particulière sera portée à :

- l'**optimisation des performances des systèmes d'information métiers** (LAGON, ASTECH, ALIZÉS et GLPI) ;
- la **segmentation des environnements** (production, qualification, recette, test et éventuellement développement) ;
- la **sécurisation des environnements virtualisés** ;
- la **maîtrise des consommations de ressources** ;
- la **résilience des plateformes d'hébergement** ;
- **l'intégration de solutions de conteneurisation** ;
- **l'intégration de plateformes applicatives** modernes reposant sur des architectures distribuées ;
- **l'évolution progressive vers des architectures hybrides** associant infrastructures locales et services cloud de confiance.

L'infrastructure de virtualisation devra être en capacité d'héberger les composants techniques nécessaires aux évolutions futures du système d'information du SMA, notamment :

- les plateformes applicatives de nouvelle génération ;
- les composants liés à l'évolution du système LAGON ;
- les outils de supervision et d'hypervision ;
- les services d'intégration avec Microsoft 365 ;
- les composants de sécurité ;
- les solutions de gestion de la donnée ;
- les futurs services d'intelligence artificielle.

Le titulaire devra veiller à maintenir un niveau de capacité suffisant afin de répondre à l'évolution des usages numériques et des besoins métiers du SMA.

Une attention particulière sera portée à la prise en charge des composants de la plateforme AP4 du système LAGON, notamment lorsqu'ils reposent sur des technologies de conteneurisation, de micro-services ou d'architectures distribuées.

Le titulaire réalisera un suivi régulier des capacités de l'environnement virtualisé et identifiera de manière proactive les risques de saturation affectant :

- les ressources processeur ;
- les ressources mémoire ;
- les capacités de stockage ;
- les performances réseau ;
- les besoins induits par l'évolution des systèmes d'information et des usages numériques.

III.4 SAUVEGARDE ET RÉPLICATION

Le titulaire met en œuvre une stratégie globale de sauvegarde, de réplication et de protection des données couvrant l'ensemble du système d'information du SMA.

Cette stratégie devra inclure :

- des **sauvegardes régulières des infrastructures virtualisées, des applications et des données ;**
- des mécanismes de **rétention adaptés aux besoins métiers et aux exigences réglementaires** ;
- des solutions de **réplication inter-sites** lorsque nécessaire ;
- des **tests réguliers de restauration** ;
- des mécanismes garantissant **l'intégrité et la traçabilité des sauvegardes** ;
- des **solutions de protection** contre les suppressions accidentelles, les erreurs humaines et les actes malveillants.

Les dispositifs de sauvegarde devront couvrir l'ensemble des composants critiques du système d'information du SMA, qu'ils soient hébergés localement, dans les infrastructures du socle ou au sein de services numériques externalisés.

Les objectifs de cette stratégie sont :

- garantir **l'intégrité, la disponibilité et la confidentialité des données** ;
- permettre une **reprise rapide et maîtrisée** des activités en cas d'incident ;
- répondre aux exigences **du PRA et du PCA** ;
- **limiter les impacts opérationnels** liés à une perte de données ;
- **renforcer la résilience du système d'information** face aux cyberattaques ;
- **garantir la continuité des missions du SMA.**

Une attention particulière sera portée :

- aux données critiques du SI LAGON ;
- aux données des SI ASTECH, ALIZÉS et GLPI ;
- aux données administratives, logistiques et financières du SMA ;
- aux services d'identité et d'authentification ;
- aux données hébergées dans l'environnement Microsoft 365 ;
- aux données documentaires et collaboratives ;
- à la protection contre les cybermenaces, notamment les ransomwares ;
- aux mécanismes de restauration rapide des services critiques.

Le titulaire devra prendre en compte la protection des données hébergées au sein du tenant Microsoft 365 du SMA.

À ce titre, il devra être en mesure de proposer et de mettre en œuvre des solutions permettant notamment :

- la sauvegarde des données Exchange Online ;
- la sauvegarde des espaces SharePoint Online ;
- la sauvegarde des contenus OneDrive Entreprise ;
- la sauvegarde des équipes Microsoft Teams ;
- la restauration granulaire ou globale des données en cas d'incident.

Le titulaire veillera à garantir la cohérence entre les mécanismes de sauvegarde du socle d'infrastructure et ceux concernant les services Microsoft 365.

Les mécanismes de réplication et de sauvegarde devront contribuer aux dispositifs de continuité et de reprise d'activité du SMA.

Le titulaire devra être en mesure d'identifier :

- les données critiques ;
- les objectifs de reprise (RTO) ;
- les objectifs de perte admissible de données (RPO) ;

- les dépendances entre infrastructures, applications et services numériques.

Les sauvegardes devront être protégées contre les compromissions provenant du système d'information de production.

Le titulaire veillera notamment à mettre en œuvre, lorsque cela est pertinent :

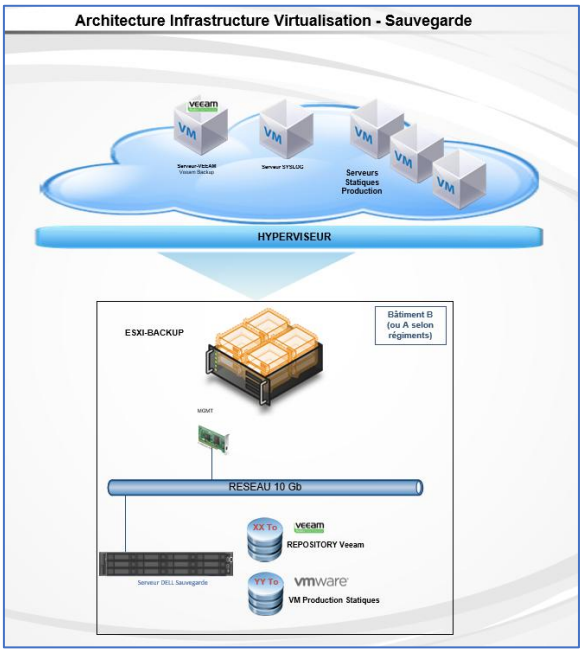
- des mécanismes d'isolation des sauvegardes ;
- des mécanismes de stockage immuable ;
- des contrôles d'accès renforcés ;
- une séparation des privilèges d'administration ;
- une supervision des opérations de sauvegarde et de restauration.

Les incidents affectant les sauvegardes devront faire l'objet d'une remontée immédiate au DSIN.

Le titulaire réalisera au minimum un exercice annuel de restauration et de reprise permettant de vérifier :

- l'intégrité des sauvegardes ;
- la cohérence des procédures ;
- les performances des mécanismes de restauration ;
- l'atteinte des objectifs de reprise définis par le SMA.

Un compte rendu détaillé sera remis au DSIN à l'issue de chaque exercice.



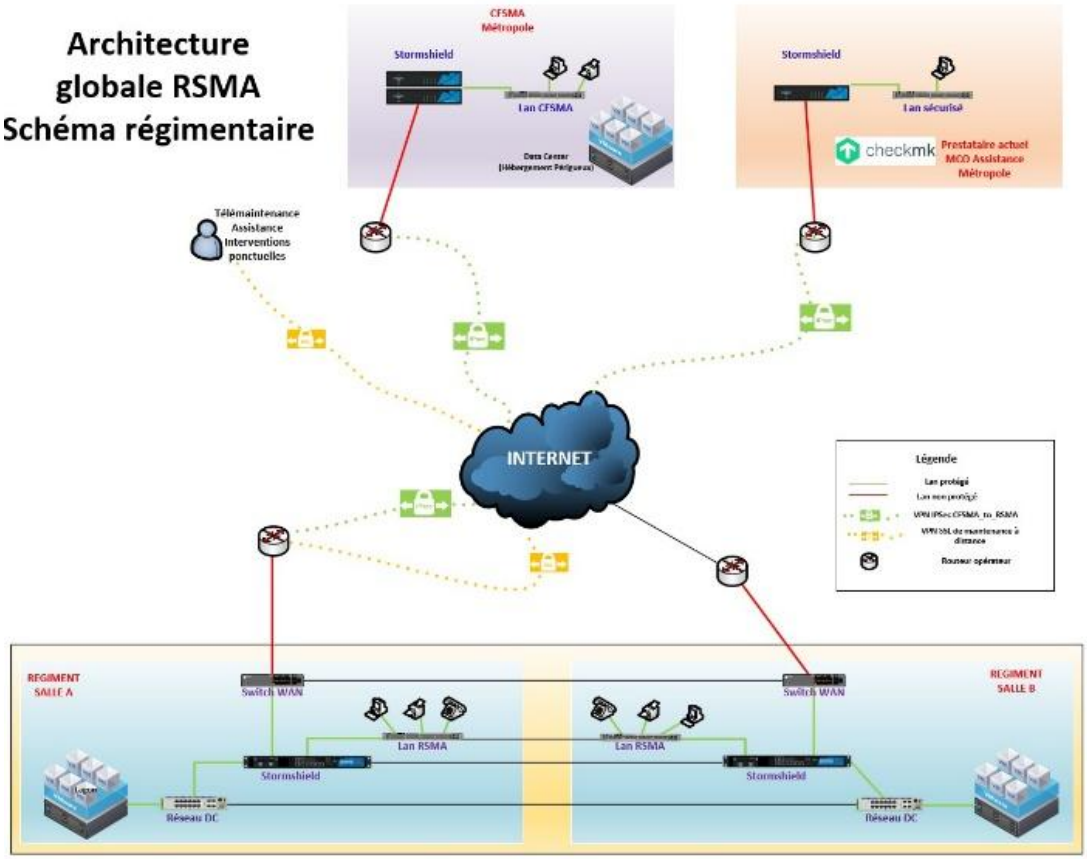
III.5 ARCHITECTURE RÉSEAU DE LA SOLUTION

III.5.1 Architecture réseau globale

Le réseau du SMA permet l'interconnexion :

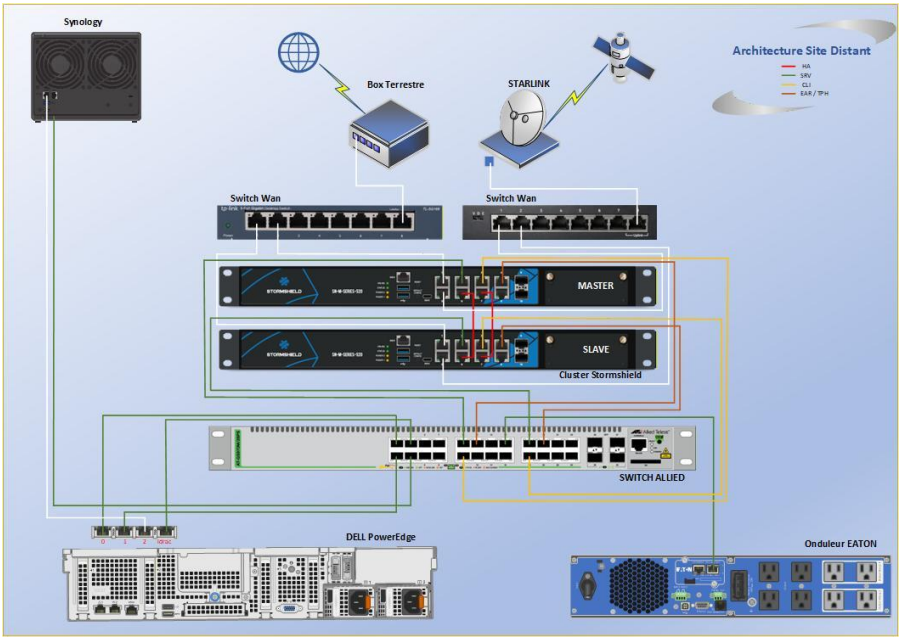
- du COMSMA ;
- des régiments ;
- du centre de formation ;
- des infrastructures hébergeant les systèmes d'information.

Chaque organisme du SMA dispose d'une architecture de connectivité reposant sur **plusieurs accès WAN**, permettant d'assurer la continuité de service et la résilience du système d'information.



À ce titre, chaque emprise bénéficie :

- de **deux fournisseurs d'accès à Internet (FAI)** :
  - généralement **1 à 2 liens fibre optique** selon les territoires,
  - complétés, le cas échéant, par un **accès mobile (4G/5G)** ;
- d'une **solution satellitaire Starlink**, déployée sur l'ensemble des sites à l'exception du RSMA de Polynésie française.



Cette architecture multi-accès et multi-opérateurs constitue un dispositif global visant à :

- garantir la **disponibilité des communications inter-sites** ;
- assurer la **continuité de service des SI critiques** ;
- renforcer la **résilience face aux défaillances des opérateurs terrestres** ;
- améliorer **les performances dans des zones à connectivité contrainte** ;
- garantir **l'accès aux services collaboratifs Microsoft** 365 ;
- garantir **l'accès aux services cloud de confiance** ;
- assurer **les usages de visioconférence, de téléphonie et de collaboration** ;
- accompagner les usages numériques émergents et **les futurs services d'intelligence artificielle**.

L'ensemble de ces infrastructures constitue le réseau d'entreprise du SMA (IntraSMA), permettant l'échange sécurisé des données, l'accès aux services numériques et la continuité des activités entre les différentes emprises.

Le réseau du SMA assure également l'accès sécurisé :

- aux services Microsoft 365 ;
- aux services numériques externalisés ;
- aux services cloud autorisés ;
- aux infrastructures de supervision et d'administration.

Il constitue une composante essentielle du fonctionnement du système d'information du SMA.

III.5.2 **Gestion multi-accès et résilience réseau**

Le titulaire devra mettre en œuvre une gestion avancée des accès WAN, permettant :

- la **priorisation des flux applicatifs** :
  - priorité élevée pour LAGON ;
  - priorité élevée pour les flux Microsoft 365 critiques (Teams, Exchange Online, SharePoint Online) ;
  - priorité adaptée pour ASTECH, ALIZÉS et GLPI ;
- la **gestion dynamique des liens** :
  - utilisation préférentielle des liens fibre ;
  - recours aux liens 4G/5G en complément ;
  - activation de Starlink en secours ou en renforcement ;
  - prise en compte des indicateurs de qualité de service des différents liens ;
  - optimisation dynamique des flux applicatifs lorsque les équipements le permettent.
- des mécanismes de :
  - **bascule automatique (failover)** en cas de perte d'un lien ;
  - **répartition de charge (load balancing)** lorsque pertinent ;
  - **maintien de session** pour les applications sensibles.

Le titulaire devra garantir :

- une **disponibilité optimale des SI**, indépendamment du type de lien utilisé ;
- une **continuité de service transparente pour les utilisateurs** ;
- une adaptation aux contraintes spécifiques des territoires ultramarins.

Le titulaire devra également garantir une qualité de connectivité compatible avec les usages collaboratifs, les services cloud et les futurs besoins liés à l'intelligence artificielle.

III.5.3 **Intégration de la solution satellitaire Starlink**

La solution Starlink constitue un **troisième niveau de connectivité**, venant renforcer les dispositifs existants.

Elle pourra être utilisée :

- en **lien de secours** en cas de défaillance des accès principaux ;
- en **lien complémentaire** pour améliorer les performances ;
- en **solution principale temporaire** dans des contextes dégradés.

Le titulaire devra assurer :

- l'intégration complète de Starlink dans l'architecture réseau,
- la compatibilité avec les mécanismes de routage et de bascule,
- la prise en compte des spécificités techniques :
  - latence variable ;
  - routage dynamique ;

- qualité de service.

Le titulaire veillera à intégrer les liens satellitaires dans la stratégie globale de continuité d'activité du SMA.

Les mécanismes de routage devront permettre une utilisation transparente des accès Starlink lors des bascules ou des dégradations de service.

III.5.4 **Sécurisation des flux réseau**

L'ensemble des communications, quel que soit le type de lien utilisé (fibre, 4G/5G, satellite), devra être sécurisé.

Le titulaire devra mettre en œuvre :

- des mécanismes de **chiffrement systématique des flux** (VPN IPSec ou équivalent) ;
- des dispositifs de **contrôle d'accès et d'authentification forte** ;
- une **segmentation réseau** adaptée aux différents SI ;
- une protection contre les menaces réseau (filtrage, inspection).

Le titulaire devra également assurer :

- la sécurisation des flux à destination des services Microsoft 365 ;
- la maîtrise des accès aux services cloud ;
- la protection des accès administrateurs ;
- le contrôle des échanges inter-sites ;
- la traçabilité des accès aux services critiques.

Les mécanismes de sécurité devront être compatibles avec les exigences des services Microsoft 365, des infrastructures cloud et des futures évolutions du système d'information.

Une attention particulière devra être portée à l'utilisation des liens satellitaires, qui devront respecter les exigences de sécurité imposées par les systèmes d'information de l'État.

III.5.5 **Supervision de la connectivité**

L'ensemble des liens WAN devra être supervisé via la solution **CheckMK**.

Le titulaire devra assurer :

- la supervision des différents accès :
  - liens fibre ;
  - liens 4G/5G ;
  - liens Starlink ;
- le suivi des indicateurs de performance :
  - disponibilité ;

    - latence ;
    - débit ;
    - taux de perte de paquets ;
    - gigue (jitter) ;
    - temps de rétablissement ;
    - qualité d'expérience des services critiques lorsque les outils le permettent ;
- la détection proactive des dégradations de service ;
- la génération d'alertes automatiques.

Les données de supervision devront être exploitées pour :

- le pilotage du MCO ;
- l'analyse des incidents réseau ;
- l'amélioration continue de la qualité de service.

Une attention particulière sera portée aux performances des flux Microsoft 365, notamment :

- Teams ;
- Exchange Online ;
- SharePoint Online ;
- OneDrive Entreprise ;
- Microsoft Copilot.

III.5.6 **Gestion des fournisseurs de connectivité**

Le titulaire assurera la gestion opérationnelle des fournisseurs d'accès Internet terrestres et satellitaires.

À ce titre, il devra :

- assurer le suivi des contrats et des abonnements,
- coordonner les opérations avec les opérateurs télécoms,
- ouvrir et suivre les incidents auprès des fournisseurs,
- assurer le pilotage des rétablissements,
- produire des indicateurs de qualité de service par opérateur,
- proposer les améliorations permettant d'accroître la résilience des liaisons.

Le titulaire participe également aux études d'évolution des offres de connectivité et formule toute recommandation permettant :

- d'améliorer la disponibilité ;
- d'augmenter les débits ;
- d'améliorer les performances des usages Microsoft 365 ;
- de renforcer la résilience du réseau IntraSMA ;
- d'optimiser les coûts de connectivité.

III.5.7 **Gestion capacitaire des accès Internet**

Le titulaire assure une analyse continue de la capacité des infrastructures du socle SIC.

Il réalise annuellement une étude capacitaire portant sur :

- les infrastructures systèmes ;
- les espaces de stockages ;
- les ressources de virtualisation ;
- les infrastructures de connectivité Internet.

Cette étude prend notamment en compte les évolutions de consommation liées :

- à l'évolution du trafic Internet ;
- aux usages Cloud ;
- aux usages Microsoft 365 ;
- aux usages collaboratifs (Teams, SharePoint, OneDrive) ;
- aux usages de visioconférence ;
- aux usages liés à Microsoft Copilot ;
- aux autres services d'intelligence artificielle ;
- aux besoins des SI LAGON, ASTECH, ALIZÉS et GLPI ;
- aux projets de transformation numérique du SMA ;
- aux évolutions du réseau IntraSMA ;
- aux nouveaux services numériques susceptibles d'être déployés pendant la durée du marché.

L'étude capacitaire devra comporter :

- un état des consommations actuelles ;
- une projection à 12 mois ;
- une projection à 24 mois ;
- une projection à 36 mois ;
- l'identification des risques de saturation ;
- les recommandations d'évolution.

Cette étude fera l'objet d'un rapport annuel transmis au DSIN.

Le titulaire formulera les recommandations nécessaires en matière de dimensionnement, de bande passante, de résilience et d'évolution des architectures.

III.5.8 **Connectivité Microsoft 365**

Le titulaire devra prendre en compte les prérequis de connectivité Microsoft 365 dans l'ensemble des architectures réseau du SMA.

À ce titre il devra :

- Assurer l'accessibilité permanente des services Microsoft 365 ;

- optimiser les flux Teams ;
- garantir des performances compatibles avec les usages collaboratifs ;
- maîtriser les impacts des mécanismes de sécurité sur les services Microsoft 365 ;
- accompagner les évolutions liées à Microsoft Copilot.

Le titulaire devra être en mesure de proposer toute évolution permettant d'améliorer les performances des services Microsoft 365 sur les sites du SMA.

III.6 SUPERVISION ET HYPERVISION

La supervision du système d'information du SMA a pour objectif de garantir la disponibilité, la performance, la sécurité et la résilience des infrastructures, des systèmes d'information et des services numériques.

Elle repose sur une organisation permettant une surveillance continue des infrastructures techniques, des réseaux, des applications, des services numériques et des services de connectivité.

Le titulaire devra prévoir la possibilité d'évolution du dispositif vers un modèle de type SOC (Security Operations Center), incluant :

- centralisation des logs,
- corrélation des événements,
- exploitation sécurité.

III.6.1 Principe général

La supervision des infrastructures SIC repose sur la solution **CheckMK**.

Cette solution permet :

- une **supervision technique complète** (serveurs, réseaux, applicatifs),
- une **centralisation des informations de supervision**,
- une **corrélation des événements**,
- une **production d'indicateurs de performance et de disponibilité**.

III.6.2 Supervision locale et centralisée

La supervision est organisée selon deux niveaux :

Supervision locale (cellules SIC)

Les cellules SIC assurent :

- La surveillance des équipements locaux ;
- le contrôle de premier niveau des infrastructures et des services ;
- la gestion de premier niveau des incidents ;
- la remontée des alertes vers le niveau central ;
- la contribution au diagnostic des incidents affectant leur organisme ;

- le suivi de proximité des performances et de la disponibilité des services numériques.

Hypervision centralisée (DSIN)

Le DSIN dispose d'une vision consolidée de l'ensemble du système d'information grâce aux dispositifs de supervision et d'hypervision mis en œuvre.

Cette hypervision permet notamment :

- la consolidation des événements issus de l'ensemble des sites ;
- la supervision transverse des infrastructures ;
- la supervision transverse des SI (LAGON, ASTECH, ALIZÉS, GLPI) ;
- le suivi des infrastructures WAN et des accès Internet ;
- le suivi des infrastructures satellitaires ;
- le suivi des services Microsoft 365 ;
- le pilotage global de la performance du socle numérique ;
- l'analyse des incidents majeurs ;
- le suivi des indicateurs de qualité de service ;
- l'identification proactive des risques de dégradation.

L'hypervision devra permettre au DSIN de disposer d'une vision unifiée de l'état du système d'information du SMA comprenant :

- les infrastructures systèmes ;
- les infrastructures réseau ;
- les services de connectivité ;
- les services de sécurité ;
- les applications métiers ;
- les services Microsoft 365 ;
- les capacités techniques ;
- les indicateurs contractuels du marché.

Les données collectées devront être exploitables à des fins d'analyse opérationnelle, capacitaire et décisionnelle.

III.6.3 Exigences relatives à la plateforme de supervision CheckMK

Le titulaire devra :

- assurer l'**exploitation, l'administration et l'évolution de la solution CheckMK** ;
- garantir la **couverture complète du périmètre supervisé** comprenant notamment :
    - infrastructures systèmes,
    - infrastructures virtualisées ;
    - infrastructures de stockage ;
    - équipements réseau ;
    - infrastructures WAN ;
    - accès Internet ;

    - accès satellitaires ;
    - équipements de sécurité ;
    - services applicatifs ;
    - services d'authentification et d'annuaire ;
    - composants critiques Microsoft 365 lorsqu'ils sont supervisables ;
    - services numériques du SMA.
- configurer :
    - les seuils d'alerte ;
    - les règles de supervision ;
    - les tableaux de bord ;
- mettre en place :
    - des **alertes automatisées** ;
    - des **tableaux de bord adaptés** :
        - au DSIN ;
        - aux cellules SIC ;
        - aux responsables de prestations ;
        - aux responsables de la cybersécurité ;
        - aux responsables du pilotage du marché.
    - des **rapports périodiques de supervision** qui devront notamment comporter :
        - les taux de disponibilité ;
        - les incidents majeurs ;
        - les tendances de capacité ;
        - les événements récurrents ;
        - les analyses de causes principales ;
        - les recommandations d'amélioration.

Il devra également :

- assurer l'intégration de CheckMK avec les outils de gestion de la prestation (ITSM) ;
- permettre l'export des données de supervision pour le suivi des KPI et SLA ;
- garantir la sécurisation de la plateforme de supervision ;
- assurer la sauvegarde des configurations de supervision ;
- maintenir la documentation de la plateforme ;
- garantir la traçabilité des actions d'administration ;
- contribuer aux études de capacité et d'évolution du système d'information.

III.6.4 **Supervision des services Microsoft 365**

Le titulaire devra mettre en œuvre des mécanismes permettant d'assurer le suivi de la disponibilité et des performances des services Microsoft 365 utilisés par le SMA.

Lorsque les interfaces et API disponibles le permettent, la supervision devra notamment prendre en compte :

- Exchange Online ;

- Microsoft Teams ;
- SharePoint Online ;
- OneDrive Entreprise ;
- Microsoft Entra ID ;
- Microsoft Copilot.

Ces informations devront être intégrées aux tableaux de bord d'hypervision afin de fournir au DSIN une vision consolidée du fonctionnement des services numériques.

Les données issues de la supervision devront contribuer aux démarches de gestion capacitaire du SMA.

Le titulaire exploitera ces données afin :

- d'identifier les tendances de consommation ;
- d'anticiper les saturations ;
- de dimensionner les infrastructures futures ;
- d'accompagner les projets de transformation numérique ;
- d'évaluer les impacts des nouveaux usages, notamment liés à Microsoft 365, au cloud et à l'intelligence artificielle.

III.7 OUTIL DE GESTION DE LA PRESTATION

III.7.1 Principe général

L'outil de gestion de la prestation (ITSM) constitue la plateforme de référence pour le pilotage opérationnel, technique et contractuel du marché.

Il permet d'assurer le suivi, la traçabilité, la gouvernance et le pilotage de l'ensemble des activités réalisées dans le cadre des prestations de maintien en condition opérationnelle (MCO), de maintien en condition de sécurité (MCS), de transformation numérique et de gestion des infrastructures du SMA.

L'outil devra couvrir l'ensemble du périmètre du marché comprenant notamment :

- les infrastructures systèmes ;
- les infrastructures réseau ;
- les services de connectivité ;
- les services Microsoft 365 ;
- les services de cybersécurité ;
- les outils de supervision ;
- les systèmes d'information métiers ;
- les projets spécifiques ;
- les activités de continuité et de reprise d'activité.

L'ensemble des prestations réalisées dans le cadre du marché devra être tracé dans cet outil afin de garantir une vision consolidée de l'activité au profit du DSIN.

L'outil devra être accessible :

- au **département des systèmes d'information et du numérique (DSIN)**,
- aux **cellules SIC des organismes du SMA (RSMA et CFSMA)**,
- le cas échéant, à d'autres acteurs autorisés.

III.7.2 **Fonctionnalités attendues**

L'outil devra à minima proposer les fonctionnalités suivantes :

Gestion des incidents et demandes

L'outil devra permettre la catégorisation des incidents et demandes selon les domaines suivants :

- systèmes ;
- réseaux ;
- cybersécurité ;
- Microsoft 365 ;
- connectivité Internet ;
- infrastructures satellitaires ;
- applications métiers ;
- services utilisateurs.

Les statistiques produites devront permettre une analyse consolidée par domaine fonctionnel et technique.

Gestion des changements

Les changements devront être classifiés selon leur criticité :

- changement standard ;
- changement normal ;
- changement majeur ;
- changement d'urgence.

L'outil devra permettre le suivi des validations, des impacts, des risques et des fenêtres de mise en production.

Gestion des configurations (CMDB)

La CMDB devra permettre la gestion centralisée des éléments de configuration composant le système d'information du SMA.

Elle devra notamment référencer :

- les serveurs ;
- les équipements réseau ;
- les équipements de sécurité ;
- les machines virtuelles ;

- les infrastructures de stockage ;
- les équipements WAN ;
- les accès Internet ;
- les abonnements opérateurs ;
- les équipements Starlink ;
- les plateformes Microsoft 365 ;
- les composants applicatifs ;
- les systèmes d'information métiers ;
- les composants de supervision ;
- les dépendances techniques existantes entre les différents composants.

La CMDB devra permettre de représenter les relations entre les infrastructures, les applications, les services numériques, les sites du SMA et les prestataires associés.

Concernant Microsoft 365, la CMDB devra permettre le suivi :

- des licences ;
- des services activés ;
- des composants administrés ;
- des espaces collaboratifs ;
- des dépendances avec les infrastructures du SMA ;
- des interfaces avec les systèmes d'information métiers.

Gestion des niveaux de service (SLA)

- suivi des engagements contractuels,
- calcul automatique des indicateurs,
- alertes en cas de dérive.

III.7.3 **Intégration avec les outils du socle**

L'outil devra également pouvoir être interfacé avec :

- Microsoft Entra ID ;
- Microsoft 365 lorsque les interfaces disponibles le permettent ;
- les outils de supervision de sécurité ;
- les outils de reporting retenus par le DSIN ;
- les référentiels documentaires du SMA.

Le titulaire devra garantir la cohérence des données entre l'ensemble des systèmes interconnectés.

III.7.4 **Accès et utilisation**

L'authentification des utilisateurs devra pouvoir s'appuyer sur les mécanismes de gestion des identités définis par le DSIN.

Les habilitations devront être attribuées selon le principe du moindre privilège et faire l'objet d'une revue régulière.

Le titulaire devra mettre à disposition :

- un **portail web sécurisé**,
- des profils d'accès différenciés (DSIN, SIC, administrateurs),
- des tableaux de bord personnalisés.

L'outil devra permettre :

- la saisie des tickets par les utilisateurs autorisés,
- le suivi en temps réel des demandes,
- la consultation de l'historique.

III.7.5 **Reporting et pilotage**

L'outil devra permettre la production d'indicateurs de pilotage, notamment :

- nombre d'incidents par type ;
- nombre d'incidents par site ;
- nombre d'incidents par système d'information ;
- nombre d'incidents Microsoft 365 ;
- nombre d'incidents liés à la connectivité ;
- taux de respect des SLA ;
- délais moyens de traitement ;
- disponibilité des infrastructures ;
- disponibilité des services numériques ;
- disponibilité des accès WAN ;
- disponibilité des services Microsoft 365 ;
- volume des changements réalisés ;
- état des capacités ;
- qualité de service globale.

Ces indicateurs devront être :

- consolidés au niveau du DSIN ;
- présentés lors des instances de pilotage (COPIL, COSUI) ;
- utilisés dans une logique d'amélioration continue.

Gestion capacitaire

L'outil devra permettre l'exploitation des données nécessaires aux études capacitaires du SMA.

Les informations collectées devront permettre :

- l'identification des tendances de consommation ;

- la détection des risques de saturation ;
- le suivi de la croissance des infrastructures ;
- l'analyse de l'impact des nouveaux usages numériques ;
- l'accompagnement des projets de transformation du SMA.

Gestion Microsoft 365

L'outil devra permettre le suivi des incidents, demandes, problèmes et changements relatifs aux services Microsoft 365.

Lorsque cela est possible, il devra permettre :

- l'identification du service concerné ;
- le suivi des interruptions de service ;
- le suivi des incidents récurrents ;
- la production d'indicateurs spécifiques ;
- le suivi des actions correctives.

Les données associées devront être intégrées aux tableaux de bord de pilotage du DSIN.

III.7.6 **Exigences de sécurité et de conformité**

L'outil devra respecter les exigences de sécurité applicables aux systèmes d'information de l'État :

- authentification sécurisée,
- gestion des habilitations,
- traçabilité des accès et actions,
- conservation des journaux.

Le titulaire devra garantir :

- la confidentialité des données ;
- leur intégrité ;
- leur disponibilité ;
- leur traçabilité ;
- leur conservation conformément aux exigences du SMA.

L'ensemble des actions réalisées dans l'outil devra faire l'objet d'une journalisation permettant les opérations d'audit, de contrôle et d'investigation.
Les journaux devront être conservés selon les durées définies par le DSIN et rester accessibles durant toute la durée du marché.

L'outil ITSM constitue le référentiel opérationnel du marché.

Sauf accord contraire du DSIN, l'ensemble des incidents, demandes, changements, problèmes, actifs, événements significatifs, indicateurs de pilotage, plans d'actions et éléments de reporting devront être enregistrés dans cet outil afin de garantir une traçabilité complète des prestations réalisées.

Article IV. LAGON : SYSTÈME D'INFORMATION MÉTIER CENTRAL ET COEUR DU SMA

IV.1 PRÉSENTATION GÉNÉRALE

Le système d'information **LAGON** constitue le système d'information métier principal du Service militaire adapté (SMA).

Il est au cœur des processus de gestion, de pilotage et de suivi des activités du SMA et contribue directement à l'exécution de ses missions opérationnelles, administratives et de formation.

Il permet notamment de couvrir les besoins fonctionnels liés :

- à la gestion des volontaires ;
- au suivi des parcours de formation ;
- à la gestion administrative des personnels ;
- au pilotage des activités des organismes du SMA ;
- à la gestion des processus métiers ;
- à la production d'indicateurs de pilotage et d'aide à la décision ;
- à la consolidation des données nécessaires au pilotage du SMA.

À ce titre, LAGON occupe une position centrale dans le système d'information du SMA et repose sur le socle numérique décrit au chapitre III du présent CCTP.

Le système est interconnecté avec les différentes composantes techniques du système d'information du SMA, notamment :

- les infrastructures d'hébergement ;
- les services d'authentification et de gestion des identités ;
- les infrastructures réseau et de connectivité ;
- les services de supervision ;
- les services Microsoft 365 lorsque les besoins métiers le nécessitent.

Le maintien en condition opérationnelle de ce système présente un caractère critique et nécessite un niveau élevé de disponibilité, de performance, de sécurité et de résilience.

Toute interruption significative du fonctionnement de LAGON est susceptible d'avoir un impact direct sur les activités de gestion, de pilotage et de formation conduites par le SMA.

Le titulaire devra porter une attention particulière à l'exploitation, à la supervision, à la sécurisation et à l'évolution des infrastructures supportant LAGON afin de garantir la continuité des missions du Service militaire adapté.

Dans le cadre de la transformation numérique engagée par le SMA, le système LAGON constitue une plateforme stratégique appelée à évoluer régulièrement afin de répondre aux nouveaux besoins fonctionnels, réglementaires et techniques.

Le titulaire devra accompagner ces évolutions en garantissant la compatibilité permanente des infrastructures du socle avec les exigences de la plateforme LAGON et de ses futures évolutions technologiques.

LAGON constitue l'un des principaux consommateurs des ressources du socle numérique du SMA et représente une charge prioritaire pour les dispositifs de supervision, de sauvegarde, de continuité d'activité, de cybersécurité et de gestion capacitaire décrits dans le présent marché.

IV.2 ÉVOLUTION DU SYSTÈME D'INFORMATION LAGON

Dans le cadre du renouvellement du marché du système d'information LAGON, dont le titulaire est la société ANAKEEN depuis mars 2026, le système d'information fait l'objet d'une évolution majeure de son architecture fonctionnelle et technique.

Cette évolution repose sur l'intégration de la plateforme **Anakeen Platform 4 (AP4)**, destinée à moderniser le système d'information métier du SMA et à accompagner les futurs besoins de transformation numérique.

AP4 constitue une plateforme moderne de développement et d'exécution d'applications métiers permettant notamment :

- la gestion du cycle de vie documentaire (GED) ;
- l'automatisation des processus métiers (BPM) ;
- la création d'applications sur mesure en mode low-code / no-code ;
- l'intégration avec des systèmes tiers via des API REST ;
- l'exposition et la consommation de services numériques ;
- le développement d'interfaces modernes et évolutives ;
- l'intégration facilitée avec les services collaboratifs et les plateformes numériques du SMA.

Cette plateforme s'appuie notamment sur les principes suivants :

- Security by Design ;
- Privacy by Design ;
- architecture orientée services (SOA) ;
- interopérabilité par API ;
- modularité des composants ;
- approche agile et évolutive ;
- compatibilité avec les architectures distribuées et conteneurisées.

L'évolution vers AP4 constitue un axe majeur de modernisation du système d'information du SMA et devra être prise en compte par le titulaire dans l'ensemble des prestations d'exploitation, de supervision, de sécurisation, de sauvegarde et d'évolution du socle numérique.

Cette évolution implique une augmentation des besoins d'interopérabilité, de supervision, de performance, de sécurité et de gestion capacitaire.

Le titulaire devra maintenir une coordination permanente avec le titulaire du marché LAGON afin de garantir la compatibilité des infrastructures du socle avec les exigences techniques actuelles et futures de la plateforme AP4.

La plateforme AP4 est susceptible d'intégrer à terme de nouveaux services numériques, services documentaires, mécanismes d'automatisation, interfaces applicatives et composants d'intelligence artificielle.

Les infrastructures du SMA devront donc conserver un niveau d'évolutivité suffisant pour accompagner ces transformations tout au long de la durée du marché.

IV.3 CARACTÉRISTIQUES TECHNIQUES DE LA PLATEFORME AP4

La plateforme AP4 introduit une rupture technologique significative par rapport aux versions précédentes du système d'information LAGON.

Elle repose sur une architecture moderne, modulaire et distribuée permettant d'améliorer l'évolutivité, l'interopérabilité, les performances et la maintenabilité des applications métiers du SMA.

1. Une architecture applicative moderne

La plateforme AP4 repose sur des technologies Web modernes permettant :

- le développement d'applications de type SPA (Single Page Application) et PWA (Progressive Web Application) ;
- l'exécution d'une partie de la logique métier côté client ;
- l'amélioration de l'expérience utilisateur ;
- la réduction des temps de réponse ;
- l'optimisation des échanges entre le navigateur et les services applicatifs.

Cette architecture est susceptible d'augmenter les besoins de connectivité et de performances réseau entre les utilisateurs et les composants applicatifs.

2. Une architecture ouverte et interopérable

- l'exposition de services via des API REST ;

- l'utilisation de technologies modernes telles que JavaScript, Vue.js et les composants associés ;
- l'intégration facilitée avec les systèmes d'information existants ;
- l'échange de données avec des services tiers ;
- l'intégration avec des plateformes numériques et collaboratives.

Cette approche favorise l'interopérabilité avec les autres systèmes d'information du SMA ainsi qu'avec les services numériques déployés dans le cadre des projets futurs.

3. Une structuration avancée des données et des processus

La plateforme AP4 intègre :

- une gestion centralisée des modèles de données (Smart Data Engine) ;
- des workflows métiers intégrés ;
- des mécanismes d'automatisation des traitements ;
- des fonctionnalités avancées de gestion documentaire ;
- des capacités d'orchestration des processus métiers.

Cette architecture contribue à améliorer la cohérence des données, la traçabilité des opérations et l'automatisation des activités métier du SMA.

4. Une architecture distribuée et conteneurisée

La plateforme AP4 repose sur une architecture distribuée pouvant s'appuyer sur des technologies de conteneurisation telles que Docker ou technologies équivalentes.

Elle repose notamment sur :

- la séparation des composants applicatifs ;
- l'isolation des services ;
- l'utilisation de services backend dédiés ;
- l'exploitation de composants de traitement asynchrones ;
- la séparation des bases de données et services documentaires.

Cette architecture permet :

- une meilleure résilience ;
- une plus grande souplesse d'exploitation ;
- une évolutivité facilitée ;
- une montée en charge progressive des composants.

La plateforme peut être déployée :

- sur des infrastructures hébergées localement (on-premise) ;
- sur des environnements virtualisés ;
- sur des infrastructures cloud ou PaaS ;

- dans des architectures hybrides associant plusieurs modes d'hébergement.

IV.4 IMPACTS SUR LE SOCLE D'INFRASTRUCTURE

L'intégration de la plateforme AP4 implique des évolutions significatives du socle numérique supportant le système d'information LAGON.

Compte tenu de son caractère critique pour les activités du SMA, le titulaire devra garantir la compatibilité permanente des infrastructures avec les exigences techniques actuelles et futures de la plateforme AP4.

Le titulaire du présent marché devra assurer une coordination étroite avec le titulaire du marché du SI LAGON (actuellement société ANAKEEN), notamment pour :

- l'intégration technique de la plateforme AP4 ;
- la gestion des incidents impliquant conjointement l'infrastructure et l'applicatif ;
- la qualification et l'analyse des incidents complexes ;
- la planification des évolutions techniques ;
- la conduite des opérations de maintenance ;
- la résolution conjointe des anomalies ;
- les opérations de recette et de validation des évolutions ;
- le suivi des performances et des capacités.

Les modalités de coopération entre les deux titulaires devront permettre une identification rapide des responsabilités et une résolution efficace des incidents affectant le système d'information LAGON.

Le titulaire du présent marché devra également prendre en compte les éléments suivants :

1. Exigences en matière d'hébergement

Le titulaire devra garantir :

- prise en charge d'architectures **multi-composants** (frontend, backend, workers, base de données) ;
- la gestion d'environnements conteneurisés ;
- un dimensionnement adapté aux charges applicatives ;
- la haute disponibilité des composants critiques ;
- la capacité d'évolution des ressources d'hébergement ;
- la séparation des environnements de production, de qualification, de recette et de test ;
- la résilience des plateformes d'exécution ;
- la compatibilité avec les évolutions futures de la plateforme AP4.

Une attention particulière sera portée aux capacités processeur, mémoire, stockage et réseau nécessaires au bon fonctionnement de l'ensemble des composants de la plateforme.

2. Exigences réseau

Le titulaire devra garantir :

- la prise en compte des flux applicatifs entre composants ;
- l'optimisation des performances réseau ;
- l'adaptation aux contraintes multi-sites ;
- la maîtrise de la latence applicative ;
- la disponibilité des services exposés ;
- la qualité des échanges entre composants applicatifs ;
- la compatibilité avec les infrastructures WAN du SMA ;
- la compatibilité avec les dispositifs de résilience réseau du SMA.

Les infrastructures de connectivité devront permettre de préserver les performances attendues du système LAGON y compris dans les contextes de bascule opérateur ou d'utilisation de liens satellitaires.

3. Exigences de sécurité

Le titulaire devra garantir :

- la sécurisation des API exposées ;
- la gestion des identités et des accès ;
- la conformité aux exigences de sécurité applicables au SMA ;
- l'application des principes Security by Design et Privacy by Design ;
- la sécurisation des flux entre composants ;
- la protection des mécanismes d'authentification ;
- la journalisation des événements de sécurité ;
- la prise en compte des recommandations de l'ANSSI ;
- la correction des vulnérabilités affectant les composants d'infrastructure supportant AP4.

Les mesures de sécurité mises en œuvre devront être compatibles avec les mécanismes de supervision, de sauvegarde et de continuité d'activité du SMA.

4. Exigences de supervision

La plateforme AP4 devra être intégrée au dispositif de supervision basé sur **CheckMK**.

Cette supervision devra permettre notamment :

- la supervision des services applicatifs ;
- la supervision des conteneurs ;

- la supervision des ressources système ;
- le suivi des performances applicatives ;
- le suivi des dépendances techniques ;
- la supervision des bases de données associées ;
- la remontée automatisée des alertes ;
- la production d'indicateurs de disponibilité et de performance.

Les événements remontés devront pouvoir être intégrés au dispositif ITSM du titulaire afin de faciliter le traitement des incidents et le suivi des engagements de service.

5. Exigences de gestion capacitaire

Le titulaire devra assurer un suivi régulier des capacités nécessaires au fonctionnement de la plateforme AP4.

Il devra notamment suivre :

- les consommations processeur ;
- les consommations mémoire ;
- les volumes de stockage ;
- les performances réseau ;
- les besoins liés aux composants conteneurisés ;
- les évolutions de charge applicative.

Toute évolution susceptible d'impacter les performances ou la disponibilité du système LAGON devra faire l'objet d'une analyse et de recommandations transmises au DSIN.

6. Exigences de sauvegarde et de continuité d'activité

Le titulaire devra garantir l'intégration des composants AP4 dans les dispositifs de sauvegarde, de réplication, de continuité et de reprise d'activité du SMA.

Les procédures de restauration devront couvrir :

- les composants applicatifs ;
- les bases de données ;
- les composants documentaires ;
- les configurations techniques ;
- les environnements conteneurisés.

Les objectifs de reprise devront rester cohérents avec la criticité du système d'information LAGON.

IV.5 ARCHITECTURE D'HÉBERGEMENT DU SI LAGON

Le système d'information LAGON repose sur une architecture distribuée, modulaire et évolutive permettant de répondre aux exigences de disponibilité, de performance, de sécurité et de résilience du SMA.

Cette architecture peut notamment comprendre :

- un frontend applicatif assurant les interfaces utilisateurs ;
- des services applicatifs backend ;
- des services de traitement asynchrone (workers) ;
- une ou plusieurs bases de données ;
- des composants de gestion documentaire (GED) ;
- des composants d'authentification et d'échange avec les services transverses ;
- des composants conteneurisés lorsque l'architecture AP4 le nécessite.

Les différents composants peuvent être répartis sur plusieurs environnements physiques ou virtualisés afin de garantir les performances, la disponibilité et la résilience du système.

Le titulaire devra garantir :

- la disponibilité de l'ensemble des composants ;
- la cohérence des environnements de production, qualification, recette et test ;
- la capacité de montée en charge de l'infrastructure ;
- la tolérance aux pannes ;
- la haute disponibilité des composants critiques ;
- la maîtrise des performances applicatives ;
- la cohérence des flux entre les différents composants ;
- la compatibilité avec les évolutions futures de la plateforme AP4 ;
- l'intégration des composants dans les dispositifs de supervision, de sauvegarde et de sécurité du SMA.

Le dimensionnement de l'infrastructure devra permettre d'absorber les évolutions du système d'information LAGON pendant toute la durée du marché.

Le titulaire devra suivre en permanence :

- la consommation des ressources processeur ;
- la consommation mémoire ;
- les performances des bases de données ;
- les capacités de stockage ;
- les performances réseau ;
- les temps de réponse applicatifs.

Toute dégradation significative devra faire l'objet d'une analyse, d'un plan d'actions et de recommandations transmises au DSIN.

L'architecture d'hébergement devra être compatible avec les dispositifs de continuité et de reprise d'activité définis pour le système d'information LAGON.

Le titulaire devra garantir :

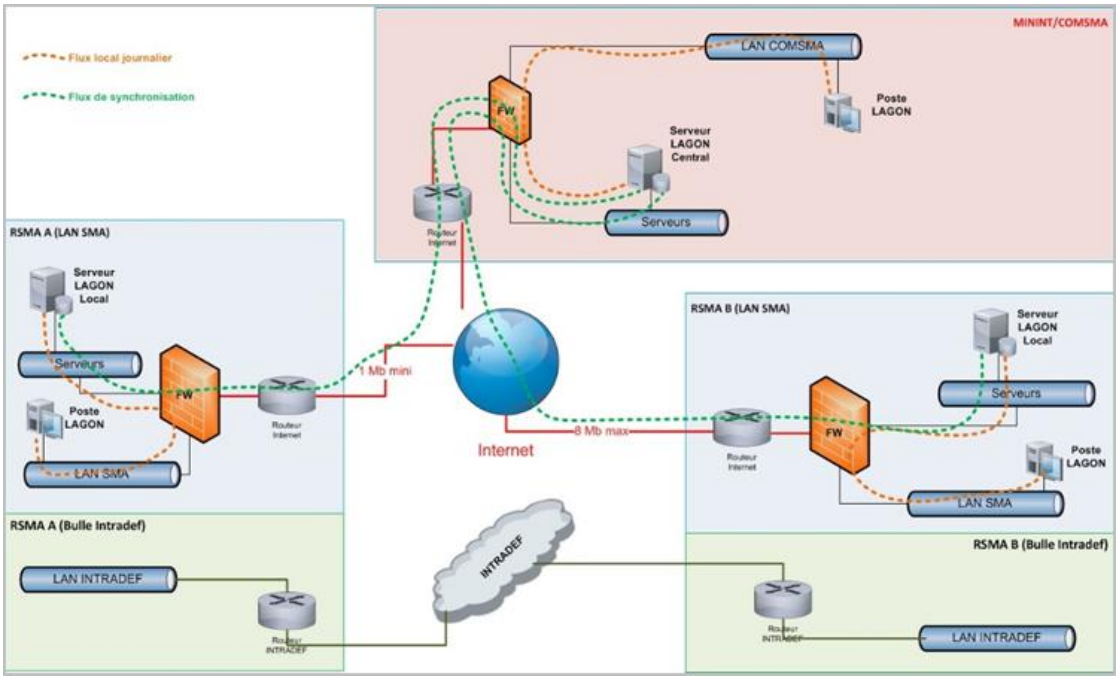
- la sauvegarde des composants applicatifs ;
- la sauvegarde des bases de données ;
- la sauvegarde des composants documentaires ;
- la restauration cohérente de l'ensemble des services ;
- le respect des objectifs de reprise définis par le SMA.

L'architecture d'hébergement devra permettre les échanges avec les autres composants du système d'information du SMA, notamment :

- les services d'authentification ;
- les infrastructures de supervision ;
- les outils ITSM ;
- les services Microsoft 365 lorsqu'ils sont utilisés dans le cadre des processus métiers ;
- les services numériques transverses du SMA.

Le titulaire devra veiller à préserver ces interconnexions lors de toute opération de maintenance ou d'évolution.

Actuellement, le réseau utilisé pour le SI LAGON peut être modélisé de la manière suivante :



IV.6 CONFIDENTIALITÉ ET SÉCURITÉ DES DONNÉES

Le système d'information LAGON traite des données sensibles relatives aux activités du Service militaire adapté (SMA), à ses personnels, à ses volontaires, à ses activités de formation et à ses activités opérationnelles.

Compte tenu de la criticité de ces informations, le titulaire devra garantir un niveau élevé de protection des données tout au long de leur cycle de vie.

Le titulaire devra garantir :

- la confidentialité des données ;
- leur intégrité ;
- leur disponibilité ;
- leur traçabilité ;
- leur protection contre les accès non autorisés ;
- leur protection contre les pertes, altérations ou destructions accidentelles ;
- leur conformité aux exigences réglementaires applicables ;
- leur prise en compte dans les dispositifs de sauvegarde, de continuité et de reprise d'activité.

L'ensemble des composants du système d'information LAGON devra respecter les principes suivants :

- Security by Design ;
- Privacy by Design ;
- moindre privilège ;
- défense en profondeur ;
- séparation des responsabilités ;
- traçabilité des accès et des actions ;
- sécurisation des échanges entre composants ;
- protection des données sensibles.

Gestion des identités et des accès :

Le titulaire devra veiller à la mise en œuvre de mécanismes garantissant :

- l'authentification des utilisateurs ;
- la gestion des habilitations ;
- le contrôle des accès aux données ;
- la traçabilité des connexions ;
- la revue régulière des droits d'accès.

Les mécanismes de gestion des identités devront demeurer compatibles avec les services d'authentification du SMA et les évolutions décidées par le DSIN.

Journalisation et audit :

Le titulaire devra garantir la journalisation des événements de sécurité affectant les composants d'infrastructure supportant le système LAGON.

Les journaux devront permettre notamment :

- l'identification des accès ;
- la traçabilité des opérations d'administration ;
- l'analyse des incidents ;
- les investigations de sécurité ;
- les opérations d'audit.

Les événements de sécurité devront pouvoir être exploités dans le cadre des dispositifs de supervision et d'hypervision du SMA.

Protection des échanges :

Les échanges de données entre les différents composants du système LAGON devront être protégés par des mécanismes adaptés de chiffrement et de contrôle des accès.

Une attention particulière devra être portée :

- aux communications entre composants applicatifs ;
- aux interfaces d'administration ;
- aux API exposées ;
- aux échanges avec les services externes ;
- aux flux transitant sur les infrastructures de connectivité du SMA.

Gestion des vulnérabilités :

Le titulaire devra mettre en œuvre les mesures nécessaires afin de maintenir un niveau de sécurité compatible avec les exigences du SMA.

À ce titre, il devra notamment :

- appliquer les correctifs de sécurité relevant de son périmètre ;
- contribuer au traitement des vulnérabilités identifiées ;
- participer aux opérations de remédiation ;
- informer le DSIN des risques susceptibles d'affecter la sécurité du système LAGON.

Le titulaire veillera à ce que les infrastructures hébergeant le système LAGON demeurent conformes aux exigences de sécurité applicables aux systèmes d'information de l'État ainsi qu'aux politiques et directives définies par le SMA et le DSIN.

Toute anomalie de sécurité susceptible d'affecter la confidentialité, l'intégrité ou la disponibilité des données devra faire l'objet d'une remontée immédiate au DSIN et être traitée conformément aux procédures de gestion des incidents de sécurité du SMA.

Article V. DÉCOUPAGE CONTRACTUEL DES PRESTATIONS ATTENDUES

V.1 PRINCIPES GÉNÉRAUX

Le présent marché est structuré en prestations couvrant l'ensemble du cycle de vie du système d'information et du socle numérique du SMA, depuis leur exploitation quotidienne jusqu'à leur modernisation et leur évolution.

Ces prestations couvrent notamment :

- les infrastructures systèmes ;
- les infrastructures réseau ;
- les infrastructures de connectivité Internet et WAN ;
- les services satellitaires ;
- les services de cybersécurité ;
- les services de supervision et d'hypervision ;
- les systèmes d'information métiers ;
- les services Microsoft 365 ;
- les dispositifs de continuité et de reprise d'activité ;
- les projets de transformation numérique.

Ces prestations s'inscrivent dans un contexte de :

- transformation numérique du SMA ;
- modernisation continue des infrastructures ;
- évolution du système d'information LAGON vers la plateforme AP4 ;
- développement des usages collaboratifs Microsoft 365 ;
- renforcement des exigences de cybersécurité ;
- montée en puissance des usages numériques et de la donnée ;
- évolution vers des architectures hybrides et des services cloud de confiance ;
- intégration progressive de services d'intelligence artificielle ;
- augmentation des besoins de connectivité entre les emprises du SMA.

Le titulaire devra adopter une approche :

- orientée qualité de service ;
- fondée sur des engagements mesurables (SLA, KPI et OLA le cas échéant) ;
- intégrant une logique d'amélioration continue ;
- reposant sur l'anticipation des risques techniques, opérationnels et de sécurité ;
- privilégiant l'automatisation lorsque celle-ci apporte un gain de qualité ou de performance ;
- conforme aux référentiels et bonnes pratiques en vigueur (ITIL, ANSSI et référentiels de l'État).

Le titulaire devra garantir une vision cohérente et transverse du système d'information du SMA en prenant en compte les interdépendances existantes entre les infrastructures, les

systèmes d'information métiers, les services Microsoft 365, les infrastructures de connectivité et les dispositifs de cybersécurité.

L'ensemble des prestations devra contribuer à l'amélioration continue de la disponibilité, de la performance, de la sécurité, de la résilience et de l'évolutivité du système d'information du SMA.

Le titulaire est tenu à une obligation de conseil durant toute la durée du marché.

À ce titre, il devra :

- alerter le DSIN de tout risque technique, sécuritaire ou opérationnel ;
- proposer les évolutions permettant d'améliorer les performances du système d'information ;
- contribuer aux études de capacité ;
- identifier les risques d'obsolescence ;
- accompagner les projets de transformation numérique ;
- formuler toute recommandation susceptible d'améliorer la qualité de service ou la résilience du système d'information du SMA.

V.2 PRESTATION N°1 : COMITOLOGIE

Le titulaire participe aux instances de gouvernance du marché et assure le pilotage contractuel, opérationnel et technique des prestations réalisées.

Les instances de gouvernance comprennent notamment

- **le comité de direction (CODIR)** : validation des orientations stratégiques ;
- **le comité de pilotage (COPIL)** : suivi global des prestations et des SLA ;
- **le comité de suivi (COSUI)** : pilotage opérationnel ;
- **toute réunion technique ou comité spécifique demandé par le DSIN**.

Le titulaire prépare, anime et assure le suivi des actions décidées lors de ces instances.

Comité de direction (CODIR) :

Le CODIR constitue l'instance de pilotage stratégique du marché.

Il permet notamment :

- la validation des orientations stratégiques ;
- le suivi des projets majeurs ;
- le suivi des risques ;
- la validation des trajectoires d'évolution du système d'information ;
- l'examen des indicateurs consolidés du marché.

Comité de pilotage (COPIL) :

Le COPIL assure le suivi global de l'exécution du marché.

Il permet notamment :

- le suivi des prestations ;
- le suivi des engagements de service ;
- l'analyse des indicateurs de qualité ;
- l'examen des incidents majeurs ;
- le suivi des plans d'actions ;
- le suivi des études d'évolution.

Comité de suivi (COSUI) :

Le COSUI constitue l'instance de pilotage opérationnel du marché.

Il permet notamment :

- le suivi des activités MCO ;
- le suivi des activités MCS ;
- le suivi des incidents ;
- le suivi des changements ;
- le suivi des actions correctives ;
- le suivi des demandes en cours.

Le titulaire devra fournir pour chaque instance :

- un ordre du jour ;
- un support de présentation ;
- un compte rendu ;
- un relevé de décisions ;
- un suivi des actions ouvertes ;
- les tableaux de bord associés.

Il devra également produire :

- des tableaux de bord consolidés ;
- des indicateurs de performance ;
- des indicateurs SLA et KPI ;
- des analyses des incidents majeurs ;
- des analyses de tendances ;
- des plans d'amélioration ;
- des indicateurs de capacité ;
- des indicateurs de cybersécurité ;
- des indicateurs de disponibilité des services.

Gestion des risques :

Le titulaire tiendra à jour un registre des risques du marché.
Ce registre devra notamment identifier :

- les risques techniques ;
- les risques de sécurité ;
- les risques capacitaires ;
- les risques d'obsolescence ;
- les risques liés aux fournisseurs ;
- les risques susceptibles d'affecter la disponibilité des services.

Une synthèse de ces risques sera présentée lors des COPIL

Performance environnementale et sobriété numérique :

Le titulaire accompagnera le SMA dans une démarche de sobriété numérique et d'amélioration continue de la performance environnementale du socle SIC.

À ce titre il devra notamment :

- optimiser l'utilisation des ressources de calcul, de stockage et de réseau ;
- contribuer à la réduction des consommations énergétiques des infrastructures ;
- privilégier les solutions permettant le réemploi et l'allongement de la durée de vie des équipements ;
- favoriser les interventions à distance lorsque cela est compatible avec la qualité de service ;
- limiter la production documentaire papier ;
- proposer annuellement des recommandations d'amélioration environnementale.

Le titulaire présentera annuellement un bilan environnemental portant notamment sur :

- les actions réalisées ;
- les indicateurs de suivi ;
- les gains constatés ;
- les recommandations proposées au DSIN.

Amélioration continue :

Le titulaire proposera et suivra un plan d'amélioration continue portant notamment sur :

- la qualité de service ;
- la performance des infrastructures ;
- la résilience du système d'information ;
- la cybersécurité ;
- les services Microsoft 365 ;
- les infrastructures de connectivité ;

- les processus d'exploitation.

L'état d'avancement des actions sera présenté lors des instances de gouvernance.

Les instances de pilotage devront également permettre le suivi spécifique :

- du système d'information LAGON et de la plateforme AP4 ;
- des services Microsoft 365 ;
- des infrastructures de connectivité WAN ;
- des accès Internet multi-opérateurs ;
- des services satellitaires Starlink ;
- des projets de transformation numérique en cours.

Le titulaire désignera un responsable de contrat unique chargé de représenter le titulaire lors des instances de gouvernance et d'assurer l'interface permanente avec le DSIN.

V.3 PRESTATION N°2 : MAINTIEN EN CONDITION OPÉRATIONNELLE (MCO)

Le titulaire assure l'exploitation, l'administration et le maintien en condition opérationnelle de l'ensemble du socle numérique du SMA, afin de garantir la disponibilité, la performance, la résilience et la continuité des services numériques.

Le titulaire assure notamment :

- la supervision via CheckMK ;
- l'administration des infrastructures systèmes ;
- l'administration des infrastructures réseau ;
- l'administration des plateformes de virtualisation ;
- l'exploitation des solutions de sauvegarde ;
- la gestion des incidents et des problèmes ;
- la gestion des changements relevant du périmètre du marché ;
- l'exploitation du réseau IntraSMA ;
- l'exploitation des infrastructures d'accès Internet ;
- l'exploitation du multi-FAI et de Starlink ;
- le suivi opérationnel des services Microsoft 365 relevant du périmètre du marché ;
- l'exploitation des outils de supervision et d'hypervision.

Le titulaire assure également :

- le suivi de l'obsolescence des composants ;
- la gestion des maintenances préventives ;
- la gestion des mises à jour d'infrastructure ;
- la veille technique sur les composants exploités ;
- la production de recommandations d'amélioration ;
- la coordination avec les autres titulaires intervenant sur les systèmes d'information du SMA.

Il garantit :

- la disponibilité des infrastructures ;
- la continuité de service multi-sites ;
- la performance des systèmes d'information ;
- le maintien des capacités nécessaires au fonctionnement du SMA ;
- la cohérence globale des composants du socle ;
- la qualité des services numériques délivrés aux utilisateurs ;
- la résilience des infrastructures techniques.

Dans le cadre du maintien en condition opérationnelle du socle SIC du SMA, le titulaire assure une gestion proactive de la capacité des infrastructures afin de garantir l'adéquation permanente entre les ressources disponibles et les besoins actuels et futurs du Service militaire adapté.

À ce titre, le titulaire réalise annuellement une étude capacitaire couvrant l'ensemble du socle SIC, comprenant notamment :

- les infrastructures serveurs ;
- les ressources de virtualisation ;
- les infrastructures de stockage ;
- les infrastructures réseau ;
- les services Microsoft 365 ;
- les plateformes applicatives associées au SI LAGON/AP4 ;
- les infrastructures d'accès à Internet et d'interconnexion des sites reposant sur des solutions terrestres, mobiles et satellitaires.

Cette étude devra notamment prendre en compte :

- les évolutions des usages Microsoft 365 ;
- les consommations liées à Teams, SharePoint et OneDrive ;
- les impacts des futures évolutions de LAGON/AP4 ;
- l'évolution des volumes de trafic Internet observés sur l'ensemble des emprises ;
- les consommations de bande passante des systèmes d'information LAGON, ASTECH, ALIZÉS et GLPI,
- les usages des services cloud et des architectures hybrides,
- les usages collaboratifs, multimédias et de visioconférence,
- les évolutions liées aux services d'intelligence artificielle, notamment Microsoft Copilot ou tout autre service numérique équivalent,
- les contraintes spécifiques liées aux implantations ultramarines,
- les perspectives d'évolution du système d'information du SMA.

Le titulaire devra identifier les risques de saturation, les points de contention éventuels et les limitations susceptibles d'affecter les performances ou la disponibilité des services.

À l'issue de chaque étude, le titulaire remettra au DSIN un rapport de capacité comprenant :

- un état des lieux détaillé des consommations observées,
- une projection des besoins à 12, 24 et 36 mois,
- une analyse des impacts des projets en cours ou programmés,
- des recommandations de dimensionnement,
- des propositions d'évolution des infrastructures, des capacités réseau et des accès Internet,
- une estimation budgétaire des évolutions recommandées.

Le rapport devra également identifier :

- les risques d'obsolescence ;
- les dépendances critiques ;
- les seuils d'alerte capacitaires atteints ou prochainement atteints ;
- les investissements recommandés.

Le titulaire s'engage à formuler toute recommandation permettant d'améliorer la performance, la résilience, la disponibilité et la qualité de service du socle SIC du SMA.

Amélioration continue :

Le titulaire met en œuvre une démarche d'amélioration continue du maintien en condition opérationnelle.

À ce titre, il :

- analyse les incidents récurrents ;
- identifie les causes profondes ;
- propose des actions correctives ;
- mesure l'efficacité des actions engagées ;
- présente les résultats lors des instances de pilotage.

V.3.1 **Engagements de service (SLA)**

Le non-respect des SLA pourra faire l'objet de pénalités définies dans le CCAP.

Le titulaire assure un service de support, de maintenance et d'exploitation permettant le traitement des incidents affectant les infrastructures SIC du SMA.

Les engagements du titulaire sont définis selon les critères suivants :

- temps de rappel ;
- garanties de temps d'intervention (DTI) ;
- garantie de temps de rétablissement (GTR).

Temps de rappel :

Le titulaire accuse réception de toute demande ou incident dans un délai maximal de quatre (4) heures ouvrées à compter de son enregistrement dans l'outil ITSM.

Garantie de temps d'intervention (GTI) :

La GTI correspond au délai maximal entre l'ouverture de l'incident et le début effectif des actions de diagnostic ou d'intervention du titulaire.

Garantie de temps de rétablissement (GTR) :

La GTR correspond au délai maximal permettant de rétablir un fonctionnement nominal ou dégradé acceptable du service.

Classification des incidents :

Anomalie bloquante :

Incident entraînant l'arrêt complet d'un service critique ou l'impossibilité d'exécuter une mission essentielle.

Sont notamment concernées :

- indisponibilité du SI LAGON ;
- indisponibilité d'un hyperviseur ;
- indisponibilité d'un service d'authentification ;
- interruption des communications inter-sites ;
- panne critique de stockage ;
- incident cyber entraînant une indisponibilité.

Anomalie majeure :

Incident entraînant une dégradation importante du service sans arrêt complet.

Anomalie mineure :

Incident n'empêchant pas le fonctionnement normal des activités mais nécessitant une correction ou une intervention.

Les engagements minimaux attendus sont les suivants (C.F. tableau ci-dessous) :

Gestion des incidents

Unité	Localisation	Temps de rappel	GTI	GTR (Hors temps livraison pièces*)		
				Anomalie bloquante	Anomalie majeure	Anomalie mineure
COMSMA	Paris	4h	J+1	J+2	J+5	J+7
CFSMA	Périgueux	4h	J+1	J+2	J+5	J+7
RSMA-Mq	Lamentin Fort de France	4h	J+1	J+2	J+5	J+7
RSMA-Ga	Guadeloupe Saint-Martin	4h	J+1	J+2	J+5	J+7
RSMA-Gy	Saint-Jean-du-Maroni Saint-Laurent-du-Maroni Cayenne	4h	J+1	J+3	J+5	J+7
RSMA-Re	Saint-Pierre Saint-Denis (2 sites) Bourg-Murat	4h	J+1	J+3	J+5	J+7
RSMA-My	Combani Chirongui Mamoudzou	4h	J+1	J+3	J+5	J+7
RSMA-Nc	Koumac Bourail Koné Nouméa (2 sites)	4h	J+2	J+4	J+5	J+7
RSMA-Pf	Arue Hiva Oa Tubuaï HAO	4h	J+2	J+4	J+5	J+7

Réseau multi-FAI

- bascule automatique < 5 minutes ;
- maintien des services critiques en mode dégradé ;
- supervision continue des mécanismes de bascule ;
- vérification périodique du bon fonctionnement des liens de secours ;
- maintien de la connectivité des services critiques du SMA.

V.4 PRESTATION N°3 : MAINTIEN EN CONDITION DE SÉCURITÉ (MCS)

Le titulaire met en œuvre un dispositif de maintien en condition de sécurité (MCS) couvrant l'ensemble du périmètre du marché.

Ce dispositif s'applique notamment :

- aux infrastructures systèmes ;
- aux infrastructures réseau ;
- aux infrastructures de connectivité ;
- aux services Microsoft 365 ;
- aux composants du système d'information LAGON ;
- aux systèmes ASTECH, ALIZÉS et GLPI ;
- aux outils de supervision ;
- aux solutions de sauvegarde ;
- aux services d'authentification et de gestion des identités.

Le titulaire veille au maintien permanent d'un niveau de sécurité compatible avec les exigences du SMA, les référentiels de l'État et les recommandations de l'ANSSI.

V.4.1 Gestion des vulnérabilités

Le titulaire assure la gestion des vulnérabilités affectant les infrastructures, systèmes, composants logiciels et services couverts par le marché.

À ce titre, il devra :

- réaliser des scans de vulnérabilités réguliers, au minimum mensuels ;
- réaliser des scans complémentaires en cas de menace particulière ;
- analyser et qualifier les vulnérabilités détectées ;
- suivre leur remédiation ;
- produire un reporting périodique au DSIN.

Les délais de traitement maximum sont fixés à :

- vulnérabilités critiques : moins de 7 jours ;
- vulnérabilités majeures : moins de 30 jours ;
- vulnérabilités modérées : selon analyse de risque validée avec le DSIN.

Le titulaire assurera également une veille spécifique relative aux composants LAGON/AP4, Microsoft 365 et aux infrastructures exposées sur Internet.

V.4.2 **Supervision de sécurité**

Le titulaire met en œuvre une supervision de sécurité permettant :

- la détection d'événements suspects ;
- la corrélation des alertes ;
- l'identification des comportements anormaux ;
- le suivi des événements critiques ;
- l'analyse des incidents de sécurité ;
- l'intégration avec les dispositifs de supervision existants.

Les mécanismes de supervision devront couvrir notamment :

- les infrastructures systèmes ;
- les équipements réseau ;
- les accès Internet ;
- les services Microsoft 365 ;
- les services d'identité ;
- les composants critiques du système LAGON.

Les informations de sécurité devront être exploitables dans les outils de supervision et d'hypervision du SMA.

V.4.3 **Gestion des incidents cyber**

Le titulaire devra disposer de procédures documentées permettant la prise en compte des incidents de sécurité.

À ce titre :

- détection : moins de 1 heure ;
- alerte immédiate du DSIN ;
- qualification de l'incident ;
- mise en œuvre des premières mesures de confinement ;
- coordination avec les acteurs concernés ;
- suivi jusqu'au retour à la normale.

Un rapport d'incident devra être transmis au DSIN dans un délai maximal de cinq jours ouvrés après clôture de l'incident.

Ce rapport devra notamment présenter :

- la chronologie des événements ;

- les causes identifiées ;
- les impacts observés ;
- les actions correctives réalisées ;
- les recommandations permettant d'éviter la récurrence.

V.4.4 **Sécurisation et durcissement**

Le titulaire assure le durcissement des infrastructures conformément aux recommandations de l'ANSSI.

Les mesures mises en œuvre comprennent notamment :

- le hardening des systèmes ;
- la segmentation des réseaux ;
- la sécurisation des API de LAGON/AP4 ;
- le chiffrement des flux ;
- la limitation des services exposés ;
- la protection des interfaces d'administration ;
- la réduction de la surface d'attaque ;
- la sécurisation des mécanismes d'authentification ;
- la gestion des comptes à privilèges ;
- la revue régulière des configurations de sécurité.

Gestion des identités et des accès :

Le titulaire contribue au maintien en condition de sécurité des mécanismes d'identité et d'authentification relevant du périmètre du marché.
Une attention particulière sera portée :

- aux comptes administrateurs ;
- aux accès privilégiés ;
- aux mécanismes d'authentification forte ;
- aux services Microsoft Entra ID ;
- aux accès aux infrastructures critiques.

Le titulaire devra appliquer le principe du moindre privilège et signaler toute anomalie constatée au DSIN.

V.4.5 **Protection contre les ransomwares**

Le titulaire met en œuvre les mesures permettant de limiter les risques liés aux rançongiciels.

Ces mesures comprennent notamment :

- des sauvegardes isolées ;

- des mécanismes de stockage immuable lorsque cela est pertinent ;
- des tests réguliers de restauration ;
- des contrôles d'accès renforcés ;
- la séparation des privilèges d'administration ;
- des dispositifs de détection précoce ;
- des procédures de reprise d'activité.

Les mécanismes mis en œuvre devront permettre la restauration des services critiques du SMA dans les délais compatibles avec les exigences du PCA/PRA.

V.4.6 **Veille et conformité**

Le titulaire assure une veille permanente portant notamment sur :

- les publications CERT-FR ;
- les publications de l'ANSSI ;
- les vulnérabilités affectant les technologies exploitées ;
- les alertes de sécurité Microsoft ;
- les vulnérabilités touchant les composants AP4 et LAGON.

Le titulaire assure également :

- la mise à jour des configurations de sécurité ;
- la prise en compte des évolutions réglementaires ;
- le maintien de la conformité aux référentiels applicables ;
- la production des éléments nécessaires aux audits de sécurité demandés par le DSIN.

Le titulaire devra se conformer aux référentiels de sécurité applicables aux systèmes d'information de l'État, notamment :

- la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) ;
- les guides de l'ANSSI ;
- les recommandations CERT-FR ;
- les politiques, procédures et directives de sécurité définies par le SMA et le DSIN.

Le titulaire est tenu à une obligation d'alerte en cas de découverte d'une vulnérabilité, d'une menace ou d'un incident susceptible d'affecter la confidentialité, l'intégrité ou la disponibilité des systèmes d'information du SMA.

V.5 PRESTATION N°4 : FORMATION ET TRANSFERT DE COMPÉTENCES

Le titulaire assure la montée en compétence des équipes du SMA afin de leur permettre de maîtriser les infrastructures, les services numériques et les outils relevant du périmètre du marché.

Les actions de formation et de transfert de compétences sont réalisées au profit :

- du DSIN ;
- des cellules SIC des régiments ;
- des administrateurs habilités ;
- des utilisateurs désignés par le SMA lorsque nécessaire.

Les formations devront notamment porter sur :

- la solution de supervision CheckMK ;
- l'outil ITSM retenu dans le cadre du marché ;
- les plateformes de virtualisation ;
- les technologies de conteneurisation ;
- les infrastructures réseau ;
- les infrastructures WAN ;
- les solutions de connectivité Internet ;
- les infrastructures Starlink ;
- les procédures de sauvegarde et de restauration ;
- les mécanismes de supervision et d'hypervision ;
- les bonnes pratiques d'exploitation ;
- les procédures de continuité et de reprise d'activité ;
- les principes de cybersécurité appliqués au SMA.

Le titulaire devra également contribuer au transfert de compétences relatif aux services Microsoft 365 relevant du périmètre du marché, notamment :

- Microsoft Entra ID ;
- Microsoft Teams ;
- SharePoint Online ;
- OneDrive Entreprise ;
- Microsoft Defender ;
- Microsoft Copilot lorsque celui-ci est déployé au sein du SMA.

Ces actions de transfert de compétences seront réalisées en coordination avec le DSIN.

Lorsque les évolutions du système d'information LAGON impactent les infrastructures du socle, le titulaire devra assurer le transfert de compétences nécessaire concernant :

- les architectures techniques AP4 ;
- les exigences d'hébergement ;

- les mécanismes de supervision ;
- les exigences de sécurité ;
- les impacts sur les infrastructures du SMA.

Le titulaire fournit et maintient une documentation complète, à jour et exploitable comprenant notamment :

- les dossiers d'architecture ;
- les procédures d'exploitation ;
- les procédures d'administration ;
- les procédures de sauvegarde et de restauration ;
- les procédures de supervision ;
- les procédures de continuité et de reprise d'activité ;
- les procédures de sécurité ;
- les guides utilisateurs et administrateurs ;
- les supports de formation.

Les sessions de formation pourront être réalisées :

- à distance ;
- sur site ;
- sous forme d'ateliers techniques ;
- sous forme d'accompagnements opérationnels.

Le titulaire adaptera le contenu des formations au niveau de compétence des participants et aux besoins exprimés par le DSIN.

Le titulaire veillera à assurer un transfert progressif et continu des connaissances tout au long de la durée du marché.

L'objectif est de permettre au DSIN et aux cellules SIC de conserver un niveau suffisant d'autonomie dans l'exploitation, le pilotage et l'administration des infrastructures et services numériques du SMA.

Chaque action de formation fera l'objet :

- d'un support pédagogique ;
- d'une feuille de présence ou d'un justificatif de participation ;
- d'un bilan de formation ;
- d'une mise à disposition des supports auprès du DSIN.

V.6 PRESTATION N°5 : RÉALISATION DE PROJETS SPÉCIFIQUES ET TRANSFORMATION NUMÉRIQUE

Cette prestation couvre les opérations d'évolution, de modernisation et de transformation du système d'information du SMA.

Elle permet la réalisation de projets techniques, fonctionnels ou organisationnels visant à améliorer la performance, la sécurité, la résilience, l'évolutivité et la qualité des services numériques du SMA.

Le titulaire apporte son expertise technique et assure un rôle de conseil auprès du DSIN dans le cadre des projets de transformation numérique.

Le titulaire devra proposer et mettre en œuvre, lorsque cela est pertinent, des solutions d'automatisation de l'exploitation (scripts, orchestration, Infrastructure as Code), visant à améliorer :

- la fiabilité ;
- la reproductibilité ;
- la rapidité des déploiements ;
- la qualité des opérations d'exploitation ;
- la réduction des erreurs humaines ;
- la standardisation des configurations ;
- la traçabilité des opérations techniques.

Les solutions proposées devront être documentées, maintenables et transférables au DSIN.

V.6.1 **Modernisation des infrastructures**

La prestation peut notamment couvrir :

- le renouvellement des infrastructures SIC ;
- la modernisation des infrastructures serveurs ;
- l'évolution des plateformes de virtualisation ;
- les études relatives aux technologies VMware, Hyper-V ou solutions équivalentes ;
- les architectures hyperconvergées ;
- l'évolution des infrastructures réseau ;
- la modernisation des infrastructures de stockage ;
- l'automatisation des infrastructures ;
- l'amélioration de la résilience des architectures.

V.6.2 **Datacenter du CFSMA (Périgueux)**

Le titulaire pourra être amené à accompagner les projets d'évolution du datacenter du CFSMA, notamment :

- la montée en puissance des capacités d'hébergement ;
- la mutualisation des ressources ;

- la haute disponibilité des services ;
- le renforcement des dispositifs PRA/PCA ;
- l'intégration de nouveaux systèmes d'information ;
- l'accueil de nouvelles plateformes applicatives.

V.6.3 **Cloud et souveraineté**

Le titulaire accompagne le SMA dans ses réflexions et projets relatifs aux architectures cloud.

À ce titre, il pourra être amené à réaliser :

- des études d'opportunité ;
- des études d'architecture ;
- des études de sécurité ;
- des études capacitaires ;
- des migrations vers des solutions cloud de confiance ;
- des projets d'architectures hybrides.

Une attention particulière sera portée :

- aux solutions cloud de confiance ;
- au projet Bleu (Capgemini / Orange) ou à toute solution équivalente ;
- aux exigences de souveraineté ;
- aux contraintes de cybersécurité ;
- aux exigences de réversibilité.

V.6.4 **Intelligence artificielle**

Le titulaire accompagne le SMA dans l'étude et l'intégration des solutions d'intelligence artificielle.

À ce titre, il peut être amené à contribuer :

- à l'intégration de Microsoft Copilot ;
- à l'intégration d'autres services d'intelligence artificielle autorisés ;
- à l'automatisation des tâches d'exploitation ;
- à la valorisation des données ;
- à l'aide à la décision ;
- à l'amélioration des processus internes.

Le titulaire réalise les études nécessaires concernant :

- les impacts sur les infrastructures ;
- les impacts sur les capacités réseau ;
- les impacts sur les ressources de calcul ;

- les impacts sur la cybersécurité ;
- les impacts sur les données.

V.6.5 **Plan IMPACT du COMSMA**

Le titulaire pourra contribuer aux projets inscrits dans le cadre du plan IMPACT du COMSMA.

Cette contribution peut notamment porter sur :

- les axes stratégiques de transformation ;
- la modernisation numérique ;
- l'innovation technologique ;
- l'amélioration des processus ;
- l'intégration de nouveaux services numériques ;
- les projets d'optimisation des infrastructures.

V.6.6 **Évolutions du SI LAGON**

Le titulaire accompagne les évolutions du système d'information LAGON en coordination avec le titulaire du marché applicatif.

À ce titre, il pourra intervenir sur :

- l'adaptation des infrastructures à la plateforme AP4 ;
- la prise en charge des environnements conteneurisés ;
- l'évolution des architectures d'hébergement ;
- l'optimisation des performances ;
- les évolutions de capacités ;
- les besoins de supervision ;
- les exigences de sécurité ;
- l'interopérabilité avec les autres systèmes d'information ;
- l'intégration avec les services Microsoft 365 lorsque cela est nécessaire.

V.6.7 **Évolutions des infrastructures de connectivité**

Le titulaire pourra être amené à conduire des projets portant sur :

- les infrastructures WAN ;
- les architectures multi-opérateurs ;
- les solutions satellitaires ;
- les solutions SD-WAN ;
- les infrastructures IntraSMA ;
- l'optimisation de la qualité de service ;
- l'amélioration de la résilience des communications.

Ces projets pourront inclure des études, des maquettes, des expérimentations ou des déploiements opérationnels.

Attendus :

Pour chaque projet spécifique confié au titulaire, celui-ci devra produire, selon les besoins exprimés par le DSIN :

- une étude préalable ;
- un dossier d'architecture ;
- une analyse des risques ;
- un planning prévisionnel ;
- un dossier de mise en œuvre ;
- un dossier de recette ;
- une documentation technique ;
- un dossier de transfert de compétences.

Les livrables attendus seront précisés dans les bons de commande ou marchés subséquents associés aux projets concernés.

V.7 PRESTATION N°6 : RÉVERSIBILITÉ

Le titulaire garantit la réversibilité complète, progressive et sécurisée de l'ensemble des prestations réalisées dans le cadre du marché.

Cette réversibilité doit permettre au SMA, ou à tout titulaire désigné par celui-ci, de reprendre l'exploitation, l'administration, la supervision et le maintien en condition opérationnelle et de sécurité des infrastructures sans dégradation de la qualité de service.

Le titulaire coopère pleinement avec le DSIN et le futur titulaire durant toute la période de réversibilité.

V.7.1 Plan de réversibilité

Le titulaire fournit un plan de réversibilité dès le début du marché.

Il comprend notamment :

- la cartographie complète du système d'information ;
- l'inventaire détaillé des actifs ;
- l'inventaire des services exploités ;
- l'identification des dépendances techniques ;
- les procédures de transfert ;
- les risques liés à la réversibilité ;
- les modalités de transfert de compétences ;
- les ressources nécessaires à la phase de réversibilité.

V.7.2 **Périmètre**

La réversibilité couvre l'ensemble des éléments exploités dans le cadre du marché, notamment :

- les infrastructures serveurs ;
- les infrastructures de stockage ;
- les infrastructures réseau ;
- les infrastructures WAN ;
- les accès Internet multi-opérateurs ;
- les équipements Starlink ;
- les plateformes de virtualisation ;
- les solutions de sauvegarde et de réplication ;
- les plateformes de supervision CheckMK ;
- l'outil ITSM ;
- les dispositifs de sécurité ;
- les composants d'exploitation associés au système d'information LAGON ;
- les connecteurs et interfaces techniques ;
- les documentations et procédures ;
- les données de pilotage du marché.

Lorsque les prestations du titulaire portent sur des services Microsoft 365, la réversibilité devra également couvrir :

- les configurations réalisées ;
- les documentations d'exploitation ;
- les procédures associées ;
- les tableaux de bord ;
- les éléments de supervision et de reporting produits dans le cadre du marché.

V.7.3 **Transfert de connaissance**

Le titulaire assure un transfert complet des connaissances vers le SMA et/ou le titulaire entrant.

Ce transfert comprend notamment :

- la documentation d'exploitation ;
- la documentation d'administration ;
- la documentation d'architecture ;
- les procédures de supervision ;
- les procédures de sauvegarde et de restauration ;
- les procédures de sécurité ;
- les procédures de gestion des incidents ;
- les procédures de gestion des changements ;
- les procédures relatives à la continuité d'activité.

Le titulaire organise les sessions de transfert nécessaires afin de garantir l'appropriation des connaissances par les équipes désignées par le DSIN.

V.7.4 **Phases de réversibilité**

La réversibilité est organisée selon les phases suivantes :

1. Préparation :

- validation du plan de réversibilité ;
- mise à jour des inventaires ;
- préparation des livrables.

2. transfert documentaire :

- transmission des documentations ;
- transmission des procédures ;
- transmission des cartographies ;
- transmission des référentiels.

3. transfert opérationnel :

- présentation des environnements ;
- transfert des connaissances ;
- accompagnement du repreneur ;
- prise en main progressive.

4. Assistance à la reprise :

- assistance technique ;
- support du repreneur ;
- correction des écarts constatés ;
- accompagnement renforcé durant la phase de transition.

La durée de la phase de réversibilité est estimée entre trois et six mois.

La durée exacte sera définie par le SMA en fonction du contexte du marché et des besoins identifiés lors de la préparation de la réversibilité.

V.7.5 **Réversibilité technique**

Le titulaire garantit :

- la restitution des données dans des formats standards et exploitables ;
- la restitution complète des configurations ;

- la restitution des scripts et automatisations développés dans le cadre du marché ;
- la restitution des paramètres de supervision ;
- la restitution des bases documentaires ;
- la restitution des inventaires techniques ;
- l'absence de verrou technologique empêchant la reprise des prestations.

Toutes les informations remises devront être directement exploitables par le SMA ou le titulaire entrant.

V.7.6 **Continuité de service**

Le titulaire garantit la continuité des services pendant toute la période de transition.

À ce titre, il assure :

- le maintien des prestations MCO ;
- le maintien des prestations MCS ;
- le respect des SLA contractuels ;
- la gestion des incidents ;
- la supervision des infrastructures ;
- la continuité des opérations d'exploitation.

La réversibilité ne devra entraîner aucune interruption non planifiée des services du SMA.

V.7.7 **Obligation de coopération**

Le titulaire est tenu à une obligation de coopération avec le SMA et le titulaire entrant.

Il fournit dans les délais demandés l'ensemble des informations, documentations, configurations et éléments techniques nécessaires à la bonne reprise des prestations.

Aucune restriction technique, contractuelle ou organisationnelle ne devra empêcher ou retarder la reprise des activités par le SMA ou par un nouveau prestataire.

ANNEXES

ANNEXE 1 :
Politique de sécurité des systèmes d'information de l'État (PSSIE)

La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) constitue le référentiel de sécurité applicable aux systèmes d'information du SMA.

À ce titre :

- le titulaire devra **respecter l'ensemble des exigences de la PSSIE**,
- il devra garantir la conformité de ses prestations avec :
    - les règles de sécurité,
    - les exigences organisationnelles,
    - les exigences techniques définies dans ce référentiel.

La PSSIE s'applique notamment :

- à la gestion des accès et des identités,
- à la protection des données,
- à la continuité d'activité,
- à la traçabilité des actions,
- à la gestion des incidents de sécurité.

Le titulaire devra :

- prendre connaissance de la version en vigueur de la PSSIE,
- intégrer ses exigences dans :
    - les activités de MCO,
    - les activités de MCS,
    - les projets d'évolution.

La PSSIE est réputée connue et opposable au titulaire.

ANNEXE 2 :
Guide d'hygiène informatique de l'ANSSI

Le guide d'hygiène informatique publié par l'ANSSI constitue un socle de bonnes pratiques en matière de cybersécurité.

Le titulaire devra appliquer ces recommandations dans le cadre de ses prestations, notamment sur les axes suivants :

1. Gestion des accès

- authentification forte,
- gestion des habilitations,
- suppression des comptes inutilisés.

2. Sécurisation des systèmes

- durcissement des systèmes (hardening),
- limitation des services exposés,
- gestion des correctifs.

3. Protection des réseaux

- segmentation des réseaux,
- filtrage des flux,
- sécurisation des interconnexions (VPN).

4. Gestion des postes et serveurs

- mise à jour régulière des systèmes,
- protection antivirus/EDR,
- surveillance des comportements.

5. Sauvegarde et résilience

- sauvegardes régulières,
- tests de restauration,
- protection contre les ransomwares.

6. Supervision et détection

- surveillance des événements,
- détection des anomalies,
- traitement des alertes.

7. Sensibilisation et organisation

- bonnes pratiques utilisateurs,
- organisation de la réponse à incident.

Le titulaire devra démontrer :

- la prise en compte de ce guide dans son dispositif MCS,
- sa capacité à appliquer ces recommandations de manière opérationnelle.

Ce référentiel constitue une **exigence minimale obligatoire**.

ANNEXE 3 :
Catalogue des guides et référentiels techniques de l'ANSSI via portail Web

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) met à disposition un ensemble de guides, recommandations et outils destinés à renforcer la sécurité des systèmes d'information des organisations publiques et privées.

Ces ressources sont accessibles en ligne via :

- le portail officiel de l'ANSSI :
  https://cyber.gouv.fr
- la page dédiée aux guides et services :
  https://cyber.gouv.fr/offre-de-service/guides-services-numeriques-et-outils/
- la plateforme MesServicesCyber :
  https://messervices.cyber.gouv.fr

Ces ressources comprennent notamment :

- des **guides techniques de sécurisation**,
- des **recommandations de configuration**,
- des **guides de gestion de crise cyber**,
- des **outils opérationnels de cybersécurité**,
- des référentiels de bonnes pratiques.

Le titulaire devra :

- se tenir informé des référentiels ANSSI applicables,
- intégrer ces recommandations dans ses prestations MCO et MCS,
- adapter ses pratiques aux évolutions de ces guides pendant toute la durée du marché.

Les guides ANSSI sont réputés **connus et opposables au titulaire**.