

SSCX_2420

FOURNITURE, MISE EN PLACE ET MAINTIEN EN CONDITION OPERATIONNELLE D'UNE SOLUTION DE COMMUNICATION UNIFIEE ET CENTRALISEE POUR L'ETABLISSEMENT FRANÇAIS DU SANG (EFS), FOURNITURE DE MATERIELS ASSOCIES ET RELISATION DE PRESTATIONS ASSOCIEES

Cahier des Clauses Techniques Particulières (CCTP)

1. Présentation de l'EFS	5
1.1. Missions principales de l'EFS	5
1.2. Autres missions de l'EFS.....	6
1.3. Organisation de l'EFS	6
1.4. Organisation de la Direction des Systèmes d'Information	8
1.5. Chiffres clés 2023	9
2. Détails du marché	10
2.1. Contexte et objet du marché	10
2.2. Périmètre du marché et phasage	10
2.3. Objectifs recherchés et enjeux	10
2.4. Parties prenantes du projet	10
2.5. Format et contenu des propositions	11
3. Obligations contractuelles	12
3.1. Obligations générales	12
3.2. Obligations techniques	12
3.3. Délais contractuels	12
4. Synthèse de l'existant	14
4.1. Acronyme / Glossaire.....	14
4.2. Infrastructure de communication	15
4.3. Réseaux informatiques	15
5. Description des besoins liés aux systèmes de communications à l'EFS : Applications annexes.....	16
5.1. Introduction	16
5.2. Définition de l'architecture cible	19
5.3. Prise en compte de l'architecture réseaux	20
5.4. Trunks SIP	20
5.5. Architecture du système de communications à installer	20
5.6. Outil d'administration, observation de trafic, alarmes	24
5.7. Annuaire système.....	26
5.8. Fonctionnalités téléphoniques.....	26
5.9. Gestion automatique des appels (SVI)	27
5.10. Messagerie vocale	28

5.11. Solution de Mobilité interne : réseau DECT	29
5.12. Communication unifiée	30
5.13. Télétravailleurs	31
5.14. Terminaux téléphoniques	31
5.15. Solution FAX/IP	33
5.16. Performances	33
5.17. Sécurisation de la plateforme	34
6. Prestations de déploiement, contrôles, tests EFS et recettes	35
6.1. Détail des prestations de déploiement	35
6.2. Vérification d’Aptitude au Bon Fonctionnement (VABF)	38
6.3. Vérification des Services Réguliers (VSR)	39
6.4. Dossier des ouvrages exécutés	39
6.5. Démontage et reprise des anciennes installations	40
7. Gestion des D.E.E.E. et revalorisation	41
7.1. Contexte et objectifs	41
7.2. Prestations attendues	41
7.3. Exigences techniques	42
8. Spécification des prestations de pilotage du marché	43
8.1. Démarche processus	43
8.2. Responsable opérationnel de compte	43
8.3. Animation des instances de pilotage	43
9. Garantie et Maintien en Condition Opérationnelle	44
9.1. Garantie des matériels et logiciels	44
9.2. MCO - Maintien en Condition Opérationnelle	44
9.3. Les moyens : Centre support Client	45
9.4. Critères de MCO – Plages horaires et délais associés	46
10. Réversibilité et transfert des acquis en début et en fin de marché	51
10.1. Généralités	51
10.2. Modalités de déclenchement	51
10.3. Modalités d'exécution	51
10.4. Délais de réalisation	52

10.5. Livrables	52
11. Exigences SSI	53
11.1. Glossaire	53
11.2. Introduction.....	53
11.3. Sécurité organisationnelle.....	54
11.4. Sécurité informatique.....	55
11.5. Maintenance	56
11.6. Relations avec les tiers	58
11.7. Fin du contrat.....	58
11.8. Plan de Continuité d'Activité (PCA).....	59
11.9. Plan d'Assurance Sécurité (PAS)	59
11.10. Sécurité physique des locaux	59
11.11. Fourniture de service SaaS (Software as a service)	61
11.12. Audits de sécurité.....	64
12. Annexes	65

1. Présentation de l'EFS

Sous tutelle du Ministère de la Santé et de la Prévention, l'Établissement Français du Sang est un établissement public de l'État créé le 1er janvier 2000. Opérateur civil unique de la transfusion sanguine en France, l'EFS veille à la satisfaction des besoins en matière de produits sanguins labiles dans le respect des principes éthiques du don de sang. L'EFS est chargé de promouvoir le don du sang, les conditions de sa bonne utilisation et de veiller au strict respect des principes éthiques par l'ensemble de la chaîne transfusionnelle : un don de sang volontaire, bénévole, et anonyme et l'absence de profit.

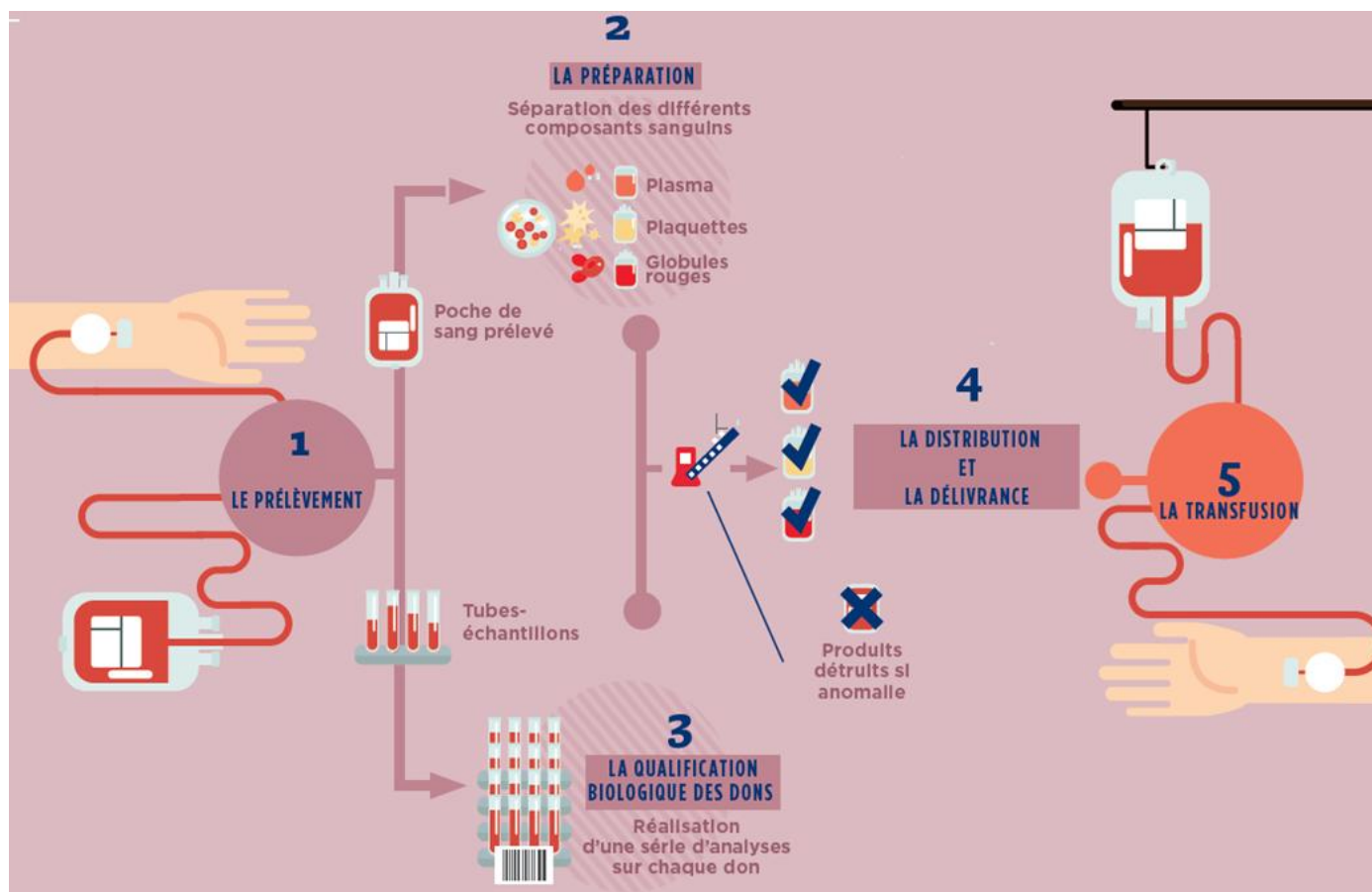
L'EFS participe à soigner 1 million de patients chaque année en approvisionnant 1500 établissements de santé publics et privés en produits sanguins labiles (PSL) issus de ces dons de sang éthiques.

Afin d'assurer une qualité optimale des produits sanguins préparés, l'EFS adapte en permanence l'activité de transfusion sanguine aux évolutions médicales, scientifiques et technologiques. Il veille au respect des bonnes pratiques transfusionnelles et au développement de la qualité pour tous les processus transfusionnels, de manière à assurer une qualité homogène sur l'ensemble du territoire.

L'EFS assure la gestion du service public transfusionnel et ses activités annexes.

1.1. Missions principales de l'EFS

Afin de mener à bien sa mission de service public, l'EFS bénéficie d'un monopole pour les activités de collecte du sang, de qualification biologique du don, de préparation, et de distribution des produits sanguins labiles aux établissements de soins privés et publics. Il organise ces activités ainsi que l'activité de délivrance et effectue le contrôle de qualité des produits sanguins.



Parcours d'une poche de sang

🔥 **Le prélèvement**

Le prélèvement est assuré dans 127 sites fixes de prélèvement en France ainsi que dans le cadre de 40 000 collectes mobiles organisées chaque année. L'EFS collecte soit du sang total soit certains composants du sang (plasma, plaquettes).

🔥 **La préparation**

La poche prélevée est dirigée vers un plateau de préparation. Le sang est séparé en ses différents composants par la centrifugation, puis déleucocyté (filtration des globules blancs véhiculant les virus et certaines bactéries). L'EFS compte 17 plateaux de préparation.

🔥 **Le contrôle qualité**

Le contrôle qualité permet de vérifier la conformité des produits préparés par rapport à des références de caractéristiques réglementaires ou des spécifications préétablies.

🔥 **La qualification des dons**

Au moment du prélèvement, des tubes sont également recueillis pour effectuer des tests immunologiques et sérologiques. La qualification permet de rechercher la présence des marqueurs viraux et de détecter toute anomalie du sang ou de ses composants. L'EFS compte 4 plateaux de qualification.

🔥 **La distribution et la délivrance**

Après vérification de l'absence d'anomalies sur le don ou de réactions positives aux tests de dépistage, les produits sanguins sont distribués aux établissements de santé et attribués au patient sur prescription médicale nominative. La durée de vie des produits est variable : 5 jours pour les plaquettes, 42 pour les concentrés de globules rouges, plusieurs mois pour le plasma congelé.

1.2. Autres missions de l'EFS

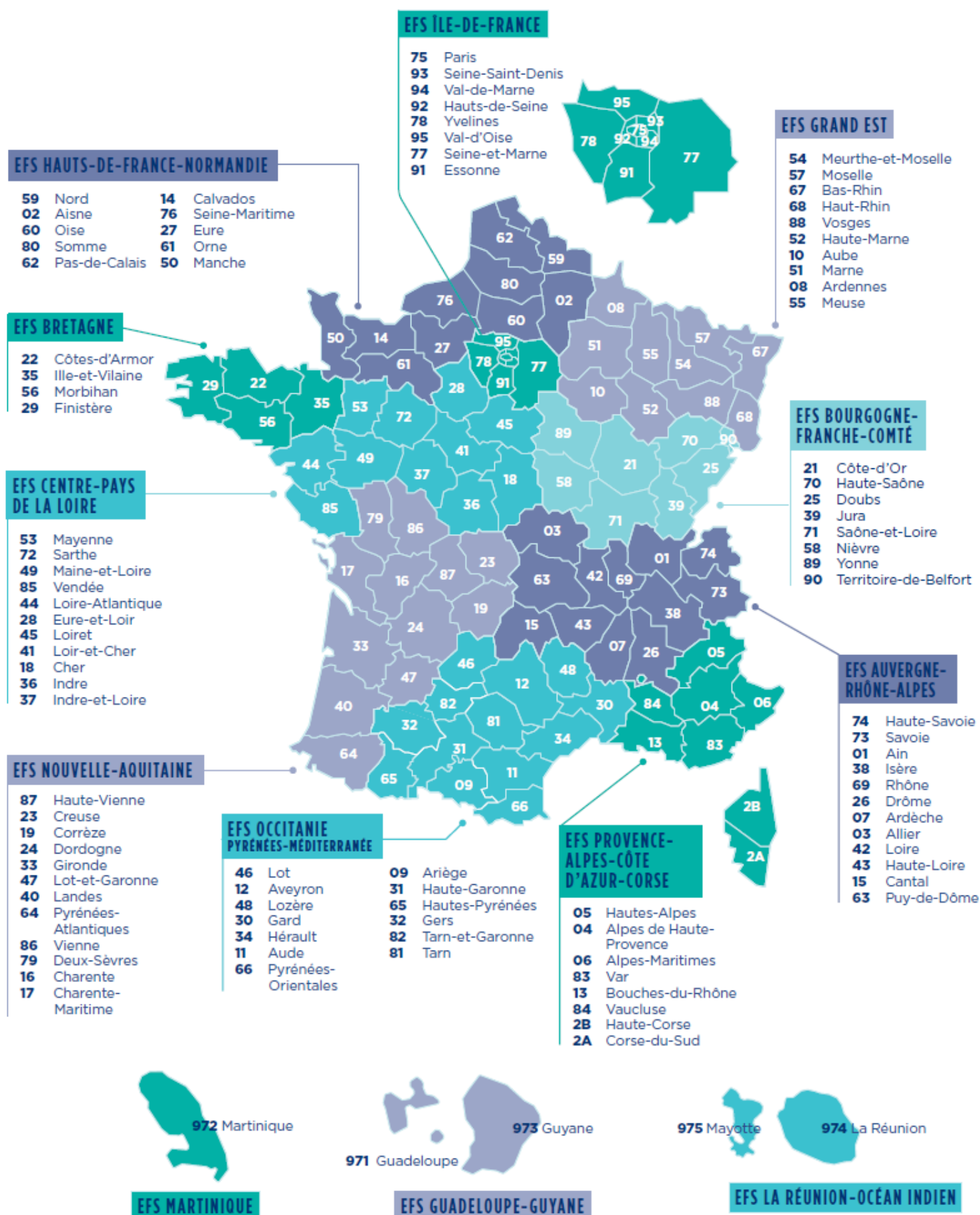
L'EFS a vocation à développer toute activité liée à la transfusion sanguine. Il peut à ce titre être autorisé à fabriquer, importer et exploiter des médicaments dérivés du sang.

L'Établissement français du sang peut, en outre, à titre accessoire, être autorisé à exercer d'autres activités de santé dont des activités de soins et de laboratoire de biologie médicale. A ce titre l'EFS effectue des examens d'immunohématologie "receveur" afin de vérifier la compatibilité entre les caractéristiques du receveur et celles du produit qui lui est destiné.

L'EFS assure également l'approvisionnement en plasma du Laboratoire Français de Fractionnement et des Biotechnologies (LFB) en vue de la fabrication de produits stables. A côté de ces activités de transfusion sanguine, l'EFS s'implique également dans d'autres activités comme l'ingénierie cellulaire, la biologie médicale, la banque de tissus...

1.3. Organisation de l'EFS

L'EFS est composé de 13 établissements de transfusion sanguine, sans personnalité morale répartis sur l'ensemble du territoire français.



1.4. Organisation de la Direction des Systèmes d'Information

La Direction des Systèmes d'Information (DSI) est en charge de la politique de l'établissement en matière de systèmes d'information. Au service des fonctions métiers et supports, des activités des Etablissements de Transfusion Sanguine (ETS), elle assure la gestion de l'ensemble du système d'information de l'Etablissement.

La DSI a pour mission :

- ◆ Le maintien en condition opérationnelle et le développement du SI dans l'ensemble de ses composantes fonctionnelles (médicotechnique, fonctions support, informatique décisionnelle, outils collaboratifs, échanges avec les partenaires externes) et techniques (exploitation, infrastructures informatiques, bureautiques et télécoms, ingénierie logicielle, sécurité du SI)
- ◆ L'unification et le développement de son SI métier
- ◆ La mise en place de l'organisation nationale de la DSI
- ◆ La mutualisation des infrastructures, des logiciels et des moyens comme source d'efficience
- ◆ D'assurer la maîtrise économique des évolutions du SI et plus globalement du coût de possession informatique.
- ◆ De garantir de façon optimale la sécurité du système d'information

La DSI est structurée en plusieurs départements, qui couvrent notamment :

Des départements de type SI Métiers :

- ◆ **Département SI Médicotechnique**, qui assure la responsabilité applicative (maintien en conditions opérationnelles, évolutions et projets) des applications métiers liées au Logiciel Médico-Technique (LMT INLOG et BNPI).
- ◆ **Département SI Relations Partenaires e-santé**, qui assure la responsabilité applicative des services relatifs à la e-santé (messagerie MSSanté) et l'interopérabilité avec les partenaires de santé de l'EFS (établissements de santé publics et privés, laboratoires, CTSA, LFB, Agence de la Biomédecine, etc.) ainsi que l'interopérabilité du LMT avec d'autres systèmes internes de l'EFS (Relations Donneurs, BNPI...).
- ◆ **Département SI Marketing et Communication**, qui assure la responsabilité applicative des solutions de gestion de la Relations Donneurs (prise de rendez-vous, application EFS, CRM, Marketing Automation, Centres de Contacts) et de la communication (sites internet, outils de communication interne...).
- ◆ **Département SI Connexes et Innovations**, qui assure la responsabilité applicative des logiciels régionaux historiques (applications connexes à la chaîne transfusionnelles, SI de laboratoires, Recherche, services techniques...), des applications transverses (ITSM-IWS, SharePoint), ainsi que des domaines d'activités tels que la définition des modalités de déploiement d'automates (QBD, IH, HLA...).
- ◆ **Département SI Gestion**, qui la responsabilité applicative des applications supportant les fonctions support de l'EFS (SAP et applications connexes, SI RH...)
- ◆ **Département Data et SI Qualité**, qui assure la responsabilité applicative du SI Décisionnel et SI Qualité et est en charge de répondre aux besoins de valorisation des données (cartographie, gouvernance, collecte, consolidation, mise en conformité, analyse, diffusion).
- ◆ **Département Etudes et Développement Spécifiques**, qui assure la réalisation des projets dont la nature nécessite un développement spécifique interne à l'EFS. Ces projets peuvent concerner l'activité médico-technique ou toute autre activité en fonction des besoins de l'EFS.

Des Départements de type Production et Support :

- ◆ **Département Production**, qui assure la coordination globale des activités de Production à l'aide de services Cyber sécurité, Système, Réseaux et Télécom, Middleware, Bases de Données, Supervision et Exploitation.
- ◆ **Département Support et Environnement de Travail Numérique**, a pour mission de fournir un support informatique global ainsi qu'un environnement de travail numérique (postes de travail, téléphonie, solutions bureautiques et collaboratives...) harmonisé, fiable, sécurisé et opérationnel à l'ensemble des collaborateurs de l'EFS, en lien avec les équipes de proximité.

Des Départements ou cellules de type Pilotage :

- ◆ **Département Architecture SI**, qui garantit la gestion du patrimoine IT, en cohérence avec les demandes métier mais aussi les catalogues de services des différentes équipes du SI, ainsi que la gestion de la conformité, via la validation et sécurisation des projets IT dans l'écosystème EFS, en respect des règles architecturales définies.
- ◆ **Cellule Gestion des Grands Projets**, qui regroupe les responsables SI de Grands Projets afin d'assurer la coordination globale des équipes informatiques mobilisées.
- ◆ **Cellule Pilotage Coordination Qualité**, qui assure un appui au pilotage et à l'organisation du SI, dans l'objectif de maximiser l'apport de valeur apportée par le SI et de veiller au respect des principes de gestion du SI.

1.5. Chiffres clés 2023

L'Institution :

- 1 opérateur civil unique de la transfusion sanguine
- 9 763 collaborateurs
- 143 sites EFS assurent la délivrance des produits sanguins labiles
- 29 225 collectes mobiles
- 4 étapes pour le parcours de la poche de sang : prélèvement, préparation, qualification, distribution
- 1 500 hôpitaux et cliniques approvisionnés en produits sanguins
- 1 million de malades soignés

Prélèvements :

- 2 702 432 prélèvements

Donneurs de sang :

- 1 545 814 donneurs
- 262 788 nouveaux donneurs

Pour en savoir plus, consultez le rapport d'activité de l'EFS sur www.efs.sante.fr, rubrique « L'EFS » => « Les publications de l'EFS ».

2. Détails du marché

2.1. Contexte et objet du marché

Compte tenu de la diversité et de l'ancienneté de ses infrastructures actuelles de téléphonies, l'EFS a décidé de lancer une consultation concernant la mise en place sur l'ensemble de ses sites d'un système de télécommunications sur IP centralisée au niveau national.

Le présent Cahier des Charges Techniques particulières (CCTP) décrit les contraintes techniques du marché à travers l'expression des besoins de l'EFS ainsi que les prestations attendues.

2.2. Périmètre du marché et phasage

Le nouveau système de communication sur IP devra reprendre les principales fonctionnalités d'un IPBX moderne avec les contraintes spécifiques suivantes :

- ◆ Mise en place d'une architecture de téléphonie centralisée évolutive jusqu'à 9000 terminaux ;
- ◆ Migration des accès opérateur télécom existant (groupement d'accès Primaire) vers Trunk SIP ;
- ◆ Intégration progressive des différentes Région dans la nouvelle architecture ;
- ◆ Remplacement de l'infrastructure DECT par une solution DECT/IP ;
- ◆ Intégration avec la solution de communication unifiée TEAMS.

Compte tenu des contraintes opérationnelles et techniques, le marché sera découpé en phases successives (cf. détail des phases en paragraphe 0) :

- ◆ Phase initiale : mise en place de l'architecture centralisée et validation de la maquette ;
- ◆ Phase pilote : intégration de deux Région pilote à la solution centralisée ;
- ◆ Phase intégration : intégration des différentes Région en fonction de leur taille.

2.3. Objectifs recherchés et enjeux

Les objectifs et les enjeux liés au projet sont :

- ◆ Bénéficier d'une infrastructure de communication moderne avec :
 - Un niveau de disponibilité et de sécurité à la hauteur des enjeux de continuité de services de l'EFS (99,9%) ;
 - Un engagement contractuel fort, de la part du futur titulaire, en termes de **maintien en condition opérationnelle** des solutions, notamment en ce qui concerne la garantie de temps de rétablissement (GTR) ;
 - Une flexibilité et une évolutivité permettant de prendre en compte les évolutions et projets de l'EFS ;
- ◆ Offrir aux télétravailleurs une facilité d'accès et d'usage des services disponibles sur la solution, tout en garantissant la sécurisation des échanges ;
- ◆ Maîtriser les coûts d'extension et de fonctionnement de la solution globale sur toute la durée du marché ;
- ◆ Disposer d'un outil de management permettant de gérer la solution en interne.

Le présent CCTP définit les contraintes techniques de l'ensemble des phases de mise en place et des services de maintenance associés à la solution.

Note importante : compte tenu des objectifs de haute disponibilité attendue, la solution pourra être soit hébergée dans les Datacenters de l'EFS, soit hébergée dans les Datacenters du Titulaire si cela permet d'obtenir une garantie d'atteinte des niveaux de disponibilité souhaitée.

Ainsi, il sera demandé aux candidats de valoriser au moins une des deux options d'hébergement dans le BPU afin de permettre à l'EFS de formaliser un choix final en toutes connaissances de causes. Les candidats qui souhaitent répondre aux deux options devront fournir à l'appui de leur offre, un argumentaire précisant les avantages et les inconvénients de ces deux options d'hébergement.

2.4. Parties prenantes du projet

La Direction des Systèmes d'Information de l'EFS (DSI) joue un rôle pivot dans la mise en œuvre d'une solution de téléphonie unifiée, en assurant la cohérence, la sécurité et l'efficacité du déploiement au sein de l'organisation. Son action s'inscrit à la fois sur des aspects techniques, organisationnels et de support au quotidien. La responsabilité de la solution sera portée par les équipes Téléphonies & Réseaux.

Le candidat détaillera comment il peut accompagner la DSI dans la réalisation de ces tâches.

2.4.1. Analyse des besoins métiers

- ◆ Recueil des besoins auprès des équipes métiers (accueil, direction, soins, terrain, etc.).
- ◆ Identification des usages spécifiques (mobilité, appels en situation critique, réception de fax sécurisés, etc.).
- ◆ Cartographie des équipements existants (autocom, postes, DECT, softphones, fax, etc.).

2.4.2. Choix de la solution

- ◆ Évaluation des solutions du marché
- ◆ Arbitrage technique, budgétaire et en matière de sécurité
- ◆ Prise en compte de la fin du RTC et des impacts associés.

2.4.3. Gouvernance et pilotage du projet

- ◆ Définition de la stratégie de déploiement : planning, priorités, sites pilotes.
- ◆ Coordination des parties prenantes : fournisseurs, équipes techniques, référents métiers.
- ◆ Préparation de la montée en charge et validation des performances (tests, qualification, recettes).

2.4.4. Mise en œuvre opérationnelle

- ◆ Supervision de l'intégration technique avec le SI
- ◆ Validation des prérequis réseau (QoS, bande passante, VLAN, sécurité).
- ◆ Préparation à la migration (formation, documentation, plan de bascule).

2.4.5. Organisation du support

- ◆ Réalisation du support N1 : assuré par les équipes techniques ou référents de site pour les demandes et incidents
- ◆ Appui au support N2/N3 en lien avec le fournisseur ou l'éditeur (diagnostic complexe, panne de passerelle, problématique Trunk SIP, interopérabilité fax, etc.).

2.4.6. Harmonisation et gestion du cycle de vie

- ◆ Constitution d'un catalogue de services téléphoniques : modèles de postes, solutions de fax, softphones, options de mobilité, services liés (SVI, conférence, enregistrement, etc.).
- ◆ Suivi du parc et des contrats (renouvellements, évolutivité, fin de vie).
- ◆ Mise à jour des politiques de sécurité et de continuité de service.

2.4.7. Accompagnement des utilisateurs

- ◆ Communication et conduite du changement : tutoriels, points d'étape, retours utilisateurs.
- ◆ Formation adaptée aux profils d'usage : accueil, administratif, mobilité, direction.

2.5. Format et contenu des propositions

Les propositions des candidats devront impérativement suivre le plan du présent CCTP afin de permettre une meilleure évaluation des offres. Les réponses devront faire clairement référence aux chapitres ou aux paragraphes du CCTP et comporter un récapitulatif des prix.

De la même manière, le candidat devra compléter la matrice de conformité au CCTP (conforme, partiel, non-conforme avec justifications/explications) via le fichier Excel fourni en annexe.

Les candidats pourront fournir des informations complémentaires ou des services à valeur ajoutée qui ne sont pas explicitement décrits par ce CCTP s'ils le jugent nécessaire et intéressant pour le projet.

Le titulaire explicitera clairement :

- ◆ La politique de licence logicielle de son système ;
- ◆ Les types de licences, les nombres de licences proposées et les modalités d'évolutions de ces licences. Il détaillera les coûts unitaires et la nécessité de licences par type de poste et par fonctionnalité.

3. Obligations contractuelles

3.1. Obligations générales

Les candidats sont informés au travers de ce CCTP et des annexes des différentes contraintes techniques, fonctionnelles et de sécurité auxquelles ils devront répondre lors la mise en place initiale de la solution mais également pendant toute la durée du marché.

Le titulaire exécute la totalité des opérations qui lui incombent, en particulier :

La fourniture et la mise en place des systèmes de communications et des applications annexes (messagerie vocale, DECT...) ;

Le raccordement de l'ensemble des sites sur le réseau de l'opérateur public et sur le réseau privé de l'EFS (LAN et WAN) ;

Le maintien en condition opérationnelle de l'ensemble des solutions fournies dans le cadre du marché ;

La mise à disposition d'un interlocuteur unique pour la gestion du contrat de service sur la durée du marché.

Le titulaire doit fournir, installer et paramétrer les différentes architectures techniques dans le respect des règles de l'art, dont il est le garant.

Les contraintes liées à la confidentialité, sécurité, sûreté, la continuité des services, cybersécurité, ainsi que les contraintes liées au site de l'EF sont spécifiées dans le document *Exigences SSI* en annexes 5

3.2. Obligations techniques

3.2.1. Spécifications minimums

Les spécifications techniques énoncées dans le présent CCTP (paragraphe 5) précisent les capacités et fonctionnalités **minimum** à mettre en œuvre dans le cadre du présent marché.

Le candidat doit fournir, installer et paramétrer les différentes architectures techniques en respectant la totalité de ces spécifications.

Le candidat a la possibilité de proposer des solutions plus complètes ou plus évoluées sous réserve du respect des contraintes minimums.

En particulier, le candidat devra préciser si les applications qu'il fournit sont **virtualisables** et sous quel environnement ; il indiquera précisément les **caractéristiques techniques des serveurs proposés** afin de permettre à l'EFS de juger de l'opportunité d'héberger la solution sur ses propres ressources systèmes.

L'ensemble des applications clientes mises à disposition des utilisateurs (communication unifiée, softphone, etc...) devra être compatible à minima avec les systèmes d'exploitation suivant : Windows pro à partir de la version 10.

3.2.2. Évolutivité

Le titulaire prévoit des systèmes et applications pouvant répondre aux évolutions potentielles de l'EFS, notamment en termes de :

- ◆ Extension du nombre d'équipements connectés : le système de communication devra pouvoir supporter une évolution du nombre de terminaux **d'au minimum 20%** par simple adjonction de terminaux téléphoniques et/ou de licences et sans remise en cause de l'infrastructure initiale ;
- ◆ Extension de l'infrastructure : au-delà de la limite précitée, l'évolution de l'infrastructure de communication devra pouvoir être réalisée par ajout de cartes, de modules et de licences sans remise en cause de la solution logicielle initiale ;

3.3. Délais contractuels

Les obligations sur les délais de réalisation et d'intervention sont fixées par défaut et **soumises à pénalités en cas de non-respect de celles-ci** (cf. CCAP) ; cela concerne :

3.3.1. Mise en service des différentes phases

La mise en service de l'ensemble de la solution devra être réalisée dans le respect du détail des prestations présenté au paragraphe 6.1 du présent CCTP.

Le candidat présentera le déroulement du déploiement à travers un calendrier d'exécution détaillé intégrant les phases successives suivantes :

Phase	Périmètre	Détails
initiale	Infrastructure socle en hébergement centralisé	Déploiement Système de communication et applications annexes ; Trunk SIP centralisé ; postes IP et Softphone pour test de la maquette
pilote	Intégration de deux Régions	Migration d'environ 700 terminaux IP et 300 Softphones Déploiement Passerelle média analogique et raccordement des postes ; interconnexion hôpitaux Portabilité SDA vers Trunk SIP central Validation des fonctionnalités SVI et connexion hôpitaux
intégration	Intégration successive des autres Régions : - jusqu'à 500 terminaux - de 501 à 800 terminaux - plus de 800 terminaux	Migration des terminaux IP et Softphones Déploiement Passerelle média analogique et raccordement des postes ; interconnexion hôpitaux Portabilité SDA vers Trunk SIP central

Les candidats détailleront le calendrier qu'il préconise pour la réalisation des deux premières phases.

3.3.2. Maintien en condition opérationnelle (MCO)

Le maintien en condition opérationnelle de la solution de communication prendra effet à l'issue de la réception des équipements concernés par chaque phase.

Le titulaire s'engagera sur une **Garantie de Temps de Rétablissement (GTR) de 4 heures** qui s'appliquera à l'ensemble du système de communication ; les applications annexes (messagerie vocale, solution DECT, ...) pourront bénéficier d'une GTR inférieure (8h).

Les obligations contractuelles sur les délais de GTR sont précisées au présent CCTP.

3.3.3. Couverture géographique

Le candidat devra couvrir un périmètre d'intervention projet & MCO sur l'ensemble des territoires de l'EFS, que ce soit en métropoles mais aussi en territoire ultramarins (Guadeloupe-Guyane, Martinique, La Réunion).

Le candidat devra préciser, si elles existent, les spécificités d'architectures, de délai, de qualité de service nécessaires pour l'ensemble des territoires.

4. Synthèse de l'existant

Le présent paragraphe décrit l'ensemble des infrastructures existantes afin de donner aux différents candidats une visibilité des équipements sur lesquels ils seront amenés à intervenir.

La majeure partie de ces équipements est à remplacer mais il subsistera une part de matériel à conserver et à réutiliser.

Afin de faciliter la compréhension du présent CCTP, le tableau ci-dessous résume les différents acronymes utilisés dans ce document :

4.1. Acronyme / Glossaire

Acronyme	Détail
ACD	Automatique Call Distribution (groupement de distribution d'appel)
DSI	Direction des Systèmes d'Information
EDI	Échanges de données informatisés (<i>entre les informatiques "métier" EFS et celles des établissements de soins partenaires, notamment</i>)
GTB	Gestion technique du bâtiment
GTC	Gestion technique centralisée
HNO	Heure non ouvrée
HO	Heure ouvrée
MOM	Mise en Ordre de Marche
QOS	Principe de classification des flux et acheminement selon leur criticité
ToIP	Téléphonie sur IP
VA	Vérification d'Aptitude
VLAN	Réseaux LAN virtuels destinés à isoler les flux applicatifs selon leur nature
VoIP	Voix sur IP
VPN	Virtual Private Network (réseau privé virtuel)
VSR	Vérification de Service Régulier
SBC	Session Border Controller
SVI	Serveur vocal interactif

4.1.1. Quadrigrammes des régions

- **AURA** – Auvergne Rhône Alpes
- **BFCT** – Bourgogne Franche-Comté
- **BRET** – Bretagne
- **CPDL** – Centre Pays de la Loire
- **GEST** – Grand est
- **HFNO** – Hauts de France Normandie
- **IDFR** – Île-de-France
- **LROI** – Réunion
- **MART** – Martinique
- **GUAD** – Guadeloupe
- **NVAQ** – Nouvelle Aquitaine
- **OCPM** – Occitanie Pyrénées-Méditerranée (ex "PYRE")
- **PACC** – PACA Corse (ex "ALPM", Alpes Méditerranée)
- **STDE** – Saint-Denis = siège national EFS

4.2. Infrastructure de communication

4.2.1. Organisation

Chaque région dispose de son propre système de téléphonie, mis en place au fil du temps selon ses compétences locales, ses contraintes organisationnelles et ses choix techniques.

Ces systèmes présentent une forte hétérogénéité :

- niveaux de centralisation variables (solutions locales ou déjà partiellement mutualisées),
- versions logicielles et matérielles différentes,
- configurations distinctes des Trunks SIP et de l'architecture réseau.

Il n'existe actuellement aucune interconnexion entre les systèmes de téléphonie des régions, ce qui limite les possibilités de simplification, de résilience et de rationalisation des coûts.

De plus, la gestion du MCO et de la maintenance est assurée de manière indépendante par chaque région, via des prestataires ou fournisseurs distincts, entraînant une absence de vision consolidée et des pratiques disparates.

4.2.1. Inventaire des Systèmes existants

Voir annexe 4

4.3. Réseaux informatiques

4.3.1. Réseau informatique

Le câblage informatique est par défaut en Catégorie 6.

Les équipements informatiques sont raccordés sur des switches de distribution (marques HPE, Aruba, Cisco...).

Les switches récents disposent d'alimentations POE : les prérequis sur la puissance unitaire et totale nécessaire aux terminaux devront être fournis par le candidat.

4.3.2. Fonctionnalités réseau : routage, règles de sécurités, disponibilité, plan d'adressage

Les équipements disposent tous de la possibilité de configurer des VLAN dédiés en fonction de la typologie de l'équipement.

Cela permet de restreindre les accès réseau au strict nécessaire et de limiter la surface d'exposition.

Les Règles d'autorisation et le routage sont effectués depuis les Pare-Feu qui portent les vlan (cœur de réseau).

Un serveur DHCP assure l'attribution automatiquement des adresses IP ainsi que les paramètres de configuration nécessaires (VLAN, serveur de provisioning, adresse du serveur SIP, etc.).

5. Description des besoins liés aux systèmes de communications à l'EFS : Applications annexes

5.1. Introduction

5.1.1. Constat

La téléphonie à l'EFS est un enjeu important car un certain nombre d'activités doivent pouvoir être joignable facilement, sur des périodes étendues (24/24, 7j/7), que l'interlocuteur soit à son bureau, dans le site ou en déplacement.

Point important dans l'organisation : les appels peuvent être à destination d'un service et pas forcément d'une personne, par conséquent on se retrouve avec de nombreux équipements qui ne sont pas nominatifs.

5.1.2. Cas d'usage

On étudiera de façon non exhaustive quelques enjeux autour de ce projet d'harmonisation et d'évolution du système de téléphonie.

On attendra du soumissionnaire qu'il détaille comment il prévoit d'accompagner l'EFS dans ce projet, comment répondre aux contraintes d'activités tout en offrant des nouveaux usages et en rationalisant les équipements.

Il est attendu que le soumissionnaire présente un plan de changement sur les études de cas expliquées ci-dessous.

A noter qu'en plus des contraintes métiers, certaines considérations sont à prendre en compte :

- La plupart des sites n'ont pas une couverture wifi à 100%
- Certains sites peuvent avoir des contraintes de réceptions du réseau mobile
- La sécurité informatique est un prérequis important et les impacts sur les ouvertures de flux, les accès DMZ, l'identification des équipements non EFS (ex : un terminal Android ou iPhone) doivent être explicités en détails.

5.1.3. Etude de cas

Cas	Profil	Besoins	Usages Actuels
Cas 1	Biologiste	Un(e) biologiste est une personne qui travaille dans un laboratoire, à son propre bureau, doit pouvoir être joignable dans le laboratoire pour validation. Les équipes doivent pouvoir facilement l'appeler et la retrouver via l'annuaire Cette personne peut être amenée à se déplacer sur des sites EFS ou non EFS et à faire des astreintes (soir & we)	Un téléphone fixe dans son bureau. Un DECT lorsqu'elle est en interne Un smartphone pour les astreintes
Cas 2	Technicien(ne) de laboratoire	Une personne qui travaille dans un lieu non nominatif, elle doit pouvoir répondre aux appels de son service La nuit, elle peut être seule dans le laboratoire, elle doit pouvoir répondre aux sollicitations téléphoniques sur le numéro du service. Elle doit avoir un DATI/PTI pour détecter tout incident	Différents postes DECT pour le service Téléphone portable avec application DATI / PTI
Cas 3	Service Vigilance	Personnel recevant des appels donneurs, il peut être sur site ou en télétravail et recevoir les appels sans soucis. Dans certains cas comme une mobilité sur son site, elle ne doit pas rater des appels.	Softphone & DECT pour la mobilité
Cas 4	Service de délivrance	Le service doit pouvoir être joignable pour des demandes urgentes. Si la téléphonie est inopérante, le site n'est plus joignable mais le personnel doit pouvoir récupérer les appels.	Mise en place de téléphone de secours type smartphone.

5.1.4. Proposition d'inventaire cible

Sur la base des inventaires remontés en région, un scénario a été défini pour rationaliser et transformer l'usage de la téléphonie, en prenant les hypothèses suivantes :

- Réduction de 10% des équipements fixes
- Réduction de nombre de postes analogiques, cela doit rester uniquement des exceptions
- Passage à 30% de softphone ou convergence fixe/mobile
- Réduction de 10% du nombre de DECT

Le soumissionnaire devra détailler comment il peut accompagner l'EFS dans cette transformation à travers des références de projets similaires ayant les mêmes enjeux sur la criticité de l'activité.

On attendra à la fois des informations techniques mais aussi comment réaliser cette conduite du changement.

Les quantitatifs du tableau ci-dessous sont ceux repris dans les DQE des régions.

Note importante :

Les candidats qui souhaitent réutiliser du matériel existant, de la même marque que celui qu'il propose, devront reporter la moins-value correspondante dans les lignes du DQE concernées.

Cette moins-value sera détaillée sous deux montants distincts : d'une part la moins-value globale concernant les passerelles média (passerelles opérateur, passerelle analogique) et d'autre part la moins-value globale pour réutilisation de postes IP, SIP ou DECT.

Ces réutilisations ne seront acceptées que si le candidat s'engage à assurer le maintien en condition opérationnelle des équipements réutilisés dans les mêmes conditions et sur la même durée que les équipements neufs correspondants.

Tableau d'inventaire cible (hypothèse hors régions outre-mer)

	EXISTANT					PREVISION				
Régions	total softphone	total postes IP	total postes numériques	total postes analogiques existant	total de postes DECT	total softphone final	qté poste type1	Qté poste type2	total analogique	Qté poste DECT final
AURA	80	327	25	75	435	123	58	230	50	392
BFCT	0	140	0	50	282	46	21	86	20	254
BRET	0	196	0	0	164	53	25	99	0	148
CPDL	0	398	0	230	345	153	72	286	60	311
GEST	100	264	0	0	251	98	46	183	0	226
HFNO	0	72	108	379	744	135	63	251	60	670
IDFR	0	0	378	302	208	165	77	307	70	187
NVAQ	30	690	18	151	350	233	109	435	25	315
OCPM	0	208	4	74	290	69	32	129	30	261
PACC	25	216	89	188	199	131	61	244	34	179
Siège	50	360	0	0	0	111	52	207	0	0
Total général	285	2871	622	1449	3268	1317	615	2459	349	2941

5.2. Définition de l'architecture cible

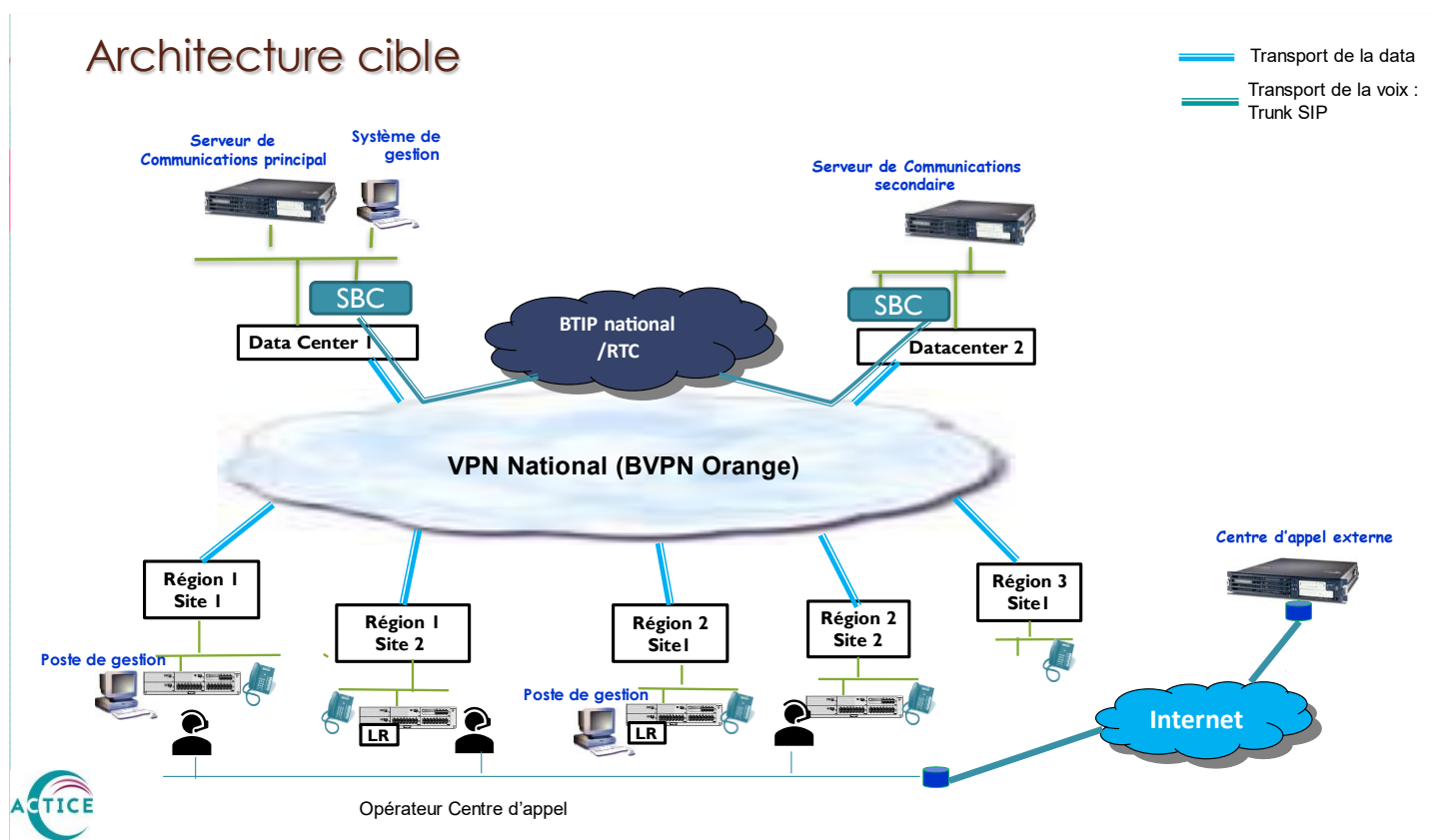
La solution proposée devra s'appuyer sur un système de communication IP totalement distribué, utilisant la commutation par paquets, en particulier pour le transport de la voix et de la signalisation sur un réseau IP.

Le système de communication doit être composé de deux parties distinctes, le logiciel gérant l'ensemble des communications et les composants matériels supportant les interfaces de communication et les accès opérateurs.

Afin d'assurer la continuité de services de l'ensemble des fonctionnalités, la solution de communication reposera sur **deux serveurs en mode actif/passif** repartis sur deux datacenters distincts, permettant de pallier aux éventuelles ruptures de service du serveur principal et/ou du lien d'interconnexion du réseau WAN.

De la même façon, la solution de communication devra pouvoir gérer un accès opérateur de type Trunk SIP sur chacun des datacenters.

Schéma de l'architecture attendue :



Comme indiqué précédemment (cf. § 2.3), deux solutions d'hébergement de la solution peuvent être valorisées par le candidat : dans les Datacenters de l'EFS ou dans ceux du candidat s'il dispose de cette possibilité. Dans le premier cas, l'ensemble des serveurs nécessaires à l'hébergement de la solution sera chiffré au titre du BPU et le candidat en précisera les spécifications exhaustives en termes de vCPU, vRAM et espace disque.

De même, le candidat précisera le type de lien VPN nécessaire à l'hébergement de la solution dans ses propres Datacenters ainsi que le mode de raccordement des Trunk SIP de l'EFS qui seront dans tous les cas fournis par l'opérateur titulaire du marché télécom en cours (Orange).

En synthèse, le candidat devra proposer 1 ou 2 offres :

- Une architecture dite « On Prem », hébergés dans les datacenters de l'EFS
- Une architecture dite « hybride » type UCaaS avec hébergement des serveurs hors EFS et en intégrant la contrainte du raccordement Trunk SIP fourni par l'EFS

Dans ces deux offres, le candidat détaillera le périmètre de responsabilité et de maintenance des équipements.

5.3. Prise en compte de l'architecture réseaux

Les équipements de distribution (commutateur) existants seront utilisés en l'état ou mise à niveau par l'EFS.

Même s'il ne sera pas amené à intervenir sur ces équipements, le titulaire est informé qu'il doit disposer des compétences nécessaires afin de **fournir les prérequis** de configuration de ces commutateurs et qu'il devra s'assurer de la compatibilité des équipements existants avec l'architecture qu'il préconise.

L'acceptation de recourir à l'usage de ces équipements l'engage, en cas de mauvaise évaluation de sa part, à procéder à l'adaptation du matériel à sa charge.

Tous les postes téléphonique IP seront configurés dans un sous réseau virtuel (VLAN) dédié à la voix sur IP.

Le candidat précisera les **contraintes de configuration de Vlan** liées à sa solution ainsi que les conditions de configuration de 'Boot' des postes IP.

5.4. Trunks SIP

Situation actuelle

Toutes les régions ne disposent pas encore d'un Trunk SIP local. Les architectures sont donc hétérogènes, certaines reposant encore sur des configurations historiques ou sur des solutions hybrides.

Cible

L'objectif est de converger vers un Trunk SIP unique et centralisé, afin de simplifier l'architecture, sécuriser les flux et optimiser la gestion de la téléphonie à l'échelle nationale. Il est attendu une solution de Trunk SIP en mode haute disponibilité avec 2 accès comportant chacun 300 canaux, évolutif à 500 canaux.

Attendus du candidat

Le candidat devra proposer un plan de migration progressif, permettant le transfert des Trunks SIP régionaux vers cette solution centralisée, en garantissant la continuité de service et en intégrant les contraintes locales (sites sensibles, astreintes, continuité des appels d'urgence).

Initialisation du projet

Dès le lancement du projet, la construction de l'offre de téléphonie nationale devra intégrer la mise en place de ce Trunk SIP centralisé, fourni par l'opérateur Orange (*à date*) dans le cadre d'une offre BTIP, portée par le réseau WAN de l'EFS.

5.5. Architecture du système de communications à installer

5.5.1. Logiciel de communication

Le logiciel de communication devra fournir à minima :

- ◆ Les fonctions de communications téléphoniques modernes pour les postes fixes (IP, analogique) et mobiles (DECT/IP et/ou WIFI) ;
- ◆ La gestion des appels sur les accès opérateurs à travers des connexions de type Trunk SIP et de type T2 ;
- ◆ L'interfaçage avec tout type d'application de communication connexe : IP Softphone, système de taxation, centre de contact multimédia, messagerie unifiée, annuaire à reconnaissance vocale, CTI, serveur de notification ... ;
- ◆ Le prise en charge du dialogue entre IPBX hétérogènes au minimum conforme à la norme QSIG ou Trunk SIP privé ;
- ◆ Une organisation des domaines de communications en mode multi-entité : chaque région dispose de son propre domaine au niveau administration.

Le logiciel de communications sera implanté sur deux serveurs physiques distincts installés dans des deux datacenters distincts.

Le basculement du contrôle des communications d'un serveur à l'autre devra pouvoir s'opérer **sans rupture des communications** en cours.

Seules les communications en phase d'établissement pourront être interrompues et relancées par le nouveau serveur actif.

Le basculement de serveur devra être **notifié à l'administrateur** du système afin que ce dernier puisse vérifier les causes du changement et rétablir le service normal.

Le système devra également pouvoir s'interfacer avec des serveurs de données (fax, annuaire, etc..) via un réseau Interne ou un réseau privé virtuel, et sur toutes les natures de médias disponibles.

5.5.2. Spécification de la communication sur IP

Les équipements téléphoniques (téléphones IP, gateways, serveurs SIP, etc.) seront raccordés dans des VLAN dédiés en fonction de la typologie de l'équipement.

Une matrice de flux spécifique au projet doit être définie, en s'appuyant sur les besoins réels de communication entre les différents équipements, et non sur une approche générique. Les éléments nécessaires à la priorisation des flux (QOS) devront être précisés pour qu'elle soit activée au sein du réseau informatique.

Qualité de service

Les caractéristiques fondamentales du transport de la voix sur IP du système proposé porteront à minima sur les mécanismes suivants :

- La compatibilité avec les protocoles de codage de la voix sur IP : H323, H345, SIP, afin de garantir l'interopérabilité des équipements ;
- La prise en compte des mécanismes de qualité de service et la priorisation du trafic RTP/SIP via la QoS (marquage DSCP sur les switches et routeurs),
- La connexion par protocole RTP direct entre les terminaux IP pour les communications intersites et intra-sites (commutations directes entre postes distants) ;
- La flexibilité de l'accès utilisateur en termes de type d'équipement et de localisation dans le réseau IP (DHCP)
- la sécurisation des communications (chiffrement SIP/TLS et SRTP) et la segmentation stricte via des règles de pare-feu limitant les communications à ce qui est strictement nécessaire,
- la supervision des flux voix pour détecter les anomalies (jitter, latence, perte de paquets),

Le système proposé supportera nativement la communication sur IP en direct ou « Peer to Peer », seule la signalisation téléphonique doit remonter vers le gestionnaire de communications, la parole commutée par le réseau IP s'échangeant directement de client à client. Les trames Voix et Signalisation devront être marquées afin d'être reconnues et classifiées par le réseau.

Les standards de marquage supportés seront les suivants :

- Niveau 2 : IEEE 802.1p/Q ;
- Niveau 3 : TOS/DiffServ.

Dans le cas d'un PC raccordé à un poste téléphonique IP, les trames émises par le PC ne doivent pas être marquées aux niveaux 2 et 3, et doivent être restituées de manière transparente par le poste IP au commutateur de rattachement.

Client DHCP

Les postes téléphoniques IP supporteront soit un adressage IP fixe (gérable à partir du terminal) ou un adressage dynamique par Client DHCP compatible avec le serveur de l'entreprise. Le candidat documentera dans sa réponse les éléments à gérer dans le serveur DHCP pour supporter les clients IP Voix.

Compatibilité SIP

Le système proposé devra permettre l'utilisation de terminaux SIP avec les autres terminaux et lignes externes privées ou publiques de l'entreprise. Le logiciel SIP devra être conforme à l'architecture normalisée et intégré dans le gestionnaire de communication temps réel afin de bénéficier des services de duplication existants. Les modules SIP sont les suivants :

- SIP Proxy ;
- SIP Registrar ;
- SIP Gateway.

Les terminaux SIP peuvent indifféremment utiliser les protocoles UDP ou TCP pour communiquer. Les standards supportés doivent être conforme aux RFC suivantes :

- RFC 3261 ;
- RFC 3262 ;
- RFC 3264 ;
- RFC 3265.

Ainsi que les RFC en élaboration (draft) tel que :

- Transfer : draft-ietf-sip-refer-06.txt, draft-ietf-sip-replaces-02.txt, draft-ietf-sip-cc-transfer-05.txt ;
- Message en attente : draft-ietf-sipping-mwi-01.txt;
- Draft-ietf-sip-session-timer-09;
- RFC 2833 : données utiles RTP pour les chiffres DTMF.

Support des terminaux SIP

Le système proposé devra permettre aux terminaux SIP de l'entreprise de s'enregistrer sur le système via le module proxy SIP et se voir attribuer un numéro d'annuaire dans le serveur de communication de manière à être joint par les terminaux téléphoniques traditionnels. Les services téléphoniques suivants doivent être offerts aux terminaux SIP :

- ◆ Nom et numéro de l'appelant ou du demandeur (sur l'écran du terminal) ;
- ◆ mise en garde ;
- ◆ reprise de garde ;
- ◆ transfert ;
- ◆ renvoi inconditionnel ;
- ◆ renvoi conditionnel sur occupation ou sur non-réponse ;
- ◆ conférence à trois ;
- ◆ ne pas déranger ;
- ◆ tonalités DTMF (dans ou hors de la bande selon le protocole RFC 2833) ;
- ◆ notification de message en attente par le système de messagerie vocale ;
- ◆ tickets de taxation pour communications externes et internes.

Authentification

Une procédure d'authentification HTTP Digest (MD5) doit pouvoir être définie entre le terminal et le proxy SIP de l'entreprise ou toute autre passerelle SIP ou proxy SIP externes lors de l'initiation d'un appel ou dans des messages en cours d'appel. D'une manière générale, toutes les communications, signalisations, échanges devront être sécurisé par un protocole adapté et à jour (TLS etc...)

Communications externes SIP

Les terminaux SIP de l'entreprise ainsi que les postes IP devront pouvoir communiquer avec des équipements se trouvant derrière une passerelle SIP ou un proxy SIP externe (de classe opérateur ou entreprise). Tous les appels SIP doivent passer par le proxy SIP du système, ce proxy contrôle le nombre maximal d'appels. Il doit être également possible par configuration d'interdire les appels en provenance de terminaux SIP inconnus avec tous les postes de l'installation.

5.5.3. Équipement de connexion aux Médias

Le système devra offrir des passerelles média et/ou SBC (Session Border Contrôler) disposant d'une grande flexibilité de configuration : les mêmes composants matériels devront permettre de multiples configurations en termes d'interfaces de connexions.

Le système devra en outre pouvoir supporter une architecture totalement distribuée sur IP. Dans cette architecture, les passerelles déportées seront dotées de capacité de commutation interne non bloquante et supporteront les interfaces téléphoniques nouvelles générations ou traditionnelles pour certains usages, soit :

- ◆ Interface réseau public de type T2 RNIS et Trunk SIP ;
- ◆ Interface LAN / WAN ;
- ◆ Liaison privée de type E1/PRI, complet ou fractionné, en mode QSIG ;
- ◆ Liaison privée de type Trunk SIP et T2 privé ;
- ◆ Interface analogique à détection de fréquence vocale.

Les passerelles dédiées aux accès opérateur principaux devront fonctionner en **partage de charge** pour l'accès aux ressources des Trunks SIP des opérateurs.

Le candidat précisera le mode de répartition du trafic sortant ainsi que les configurations nécessaires au niveau de l'opérateur pour la gestion du trafic entrant.

Pour faciliter l'intégration avec les systèmes de câblage structurés, il est souhaitable de disposer de passerelles media au standard 19 pouces, rackables et empilables, et présentant en face avant des connexions standard au format RJ 45, permettant de fédérer les éléments voix et données au sein d'un câblage unifié.

5.5.1. Capacité des équipements d'infrastructure

Infrastructure centrale :

Désignation des équipements	Capacité équipé	Capacité extensible
Application/Serveur de communication principal et secondaire <ul style="list-style-type: none">- Nombre de licences de poste IP/SIP supporté :- Nombre de licences de poste DECT supporté :- Nombre de passerelles média pouvant être gérées :- Nombre de licences de poste analogique supporté :	5000 3000 150 500	6000 3500 200 800
Passerelles Média ou SBC 'Opérateur' : Accès centralisé au réseau public par Trunk SIP <ul style="list-style-type: none">- Passerelle 1- Passerelle 2	300 canaux 300 canaux	500 canaux 500 canaux

Passerelles média utilisateurs et réseau privé :

Désignation des équipements	Capacité équipé	Capacité extensible
Passerelle numérique interface T2 privé	1 T2 – 30 canaux	2 T2- 60 canaux
Passerelle analogique pour poste classique	8 ports	32 ports
Passerelle analogique pour liaison hôpital <ul style="list-style-type: none">- Port poste analogique (FXS)- Port réseau analogique (FXO)	2 ports 2 ports	8 ports 8 ports

5.5.2. Configurations multisites

Le candidat décrira les solutions qu'il propose pour le transport des communications IP entre les sites à travers le réseau WAN de l'EFS (VPN MPLS) :

- ♦ Type de protocole utilisé (H323, SIP)
- ♦ Type de compression (G711, G729, G729A....)
- ♦ Contrainte de QOS,
- ♦ etc.

La solution de communication devra pouvoir acheminer, de manière totalement transparente, le trafic **depuis les Trunk SIP centralisées vers les postes téléphoniques distribués sur les sites en régions.**

5.5.3. Plan de numérotation

Il est demandé au titulaire de reprendre les **plans de numérotation actuels** des postes de l'EFS et de les adapter pour en faire le plan référence du futur système.

Les codes d'activation des fonctions (renvoi, consultation d'appel en attente, etc.) seront à 2 chiffres maximum. De même, les numéros SDA existants seront réutilisés dans les mêmes conditions qu'actuellement. Le plan de numérotation doit être homogène, modifiable et adaptable aux besoins futurs ou conjoncturels de l'EFS.

5.5.4. Alimentation électrique des équipements

Les serveurs de communication et serveurs annexes (messagerie unifiée, gestion/taxation, etc...) ainsi que chaque passerelle « Media » du système seront raccordées aux réseaux secours (240Vac) des sites de l'EFS.

L'EFS fournira et installera, dans le coffret d'alimentation ou de distribution des locaux concernés, les disjoncteurs nécessaires au raccordement des équipements du prestataire.

Ce dernier sera responsable de fournir et d'installer les câbles d'alimentation entre ce coffret et ses équipements

Le candidat devra préciser les prérequis de ces équipements en termes d'énergie : nombre d'alimentations et puissance globale.

5.5.5. Implantation du matériel

Les conditions d'environnement des serveurs liés aux applications de communications et des passerelles Média seront précisées par le candidat et les contraintes suivantes seront stipulées :

- ◆ Espace requis au sol pour l'installation des baies informatiques d'hébergement des équipements ;
- ◆ Dégagement calorifique dans les locaux ;
- ◆ Climatisation : limite inférieure et supérieure de température, gradient admissible ;
- ◆ Protection nécessaire contre les perturbations électromagnétiques et électriques : foudre, tubes fluorescents, revêtements synthétiques, ondes radioélectriques, etc. ;
- ◆ Ventilation du local batteries (le cas échéant).

Le prestataire devra la fourniture des baies d'hébergements de ses équipements dans l'ensemble des locaux techniques hormis ceux des datacenters dans lesquels il devra intégrer ses matériels dans les baies existantes. Le candidat confirmera le nombre de 'U' dont il a besoin pour l'hébergement de sa solution dans les baies de l'EFS ainsi que la profondeur minimum des équipements.

5.6. Outil d'administration, observation de trafic, alarmes

5.6.1. Configuration générale

L'application d'administration du système sera basée sur les dernières technologies Internet et devra être accessible en mode Web par un client léger.

L'application d'administration devra en outre permettre les services suivants :

- ◆ Possibilité de connexion par au moins 3 sessions simultanées ;
- ◆ Gestion des droits d'accès aux différents services de configuration ;
- ◆ Configuration de l'ensemble des services du système de communication ;
- ◆ Observation des trafics en temps réels ;
- ◆ Statistiques de trafics sur une période donnée ;
- ◆ Alarmes système connectées aux systèmes de supervision ;
- ◆ Mise en place de solution permettant le contrôle et la limitation d'usages non autorisés ou pouvant amener une surfacturation (plafond de consommations / quota, appels à l'étranger, numéro surtaxé etc...) ;
- ◆ Etc.

De plus l'outil d'administration devra permettre de configurer une organisation géographique reprenant le périmètre de chacune des Régions (mode multi entité). Ainsi, l'administrateur pourra intervenir sur le paramétrage d'une région sans impacter les autres.

La solution doit permettre ce type d'arborescence logique :

- Organisation → Régions → Sites → Activités / Services.

L'accès à l'outil d'administration devra être protégé par une identification basée sur un nom d'utilisateur et un mot de passe. La DSI de l'EFS fournira au titulaire un compte dans l'active Directory (AD) du siège ainsi qu'un accès VPN lui permettant d'accéder à l'outil d'administration de l'IPBX.

L'association du nom d'utilisateur avec le mot de passe permettra de créer des profils utilisateurs ouvrant droits à une gestion par domaine.

On pourra s'appuyer sur une approche RBAC pour définir des profils / rôles aux utilisateurs étant amenés à opérer la solution.

La gestion par domaine devra pouvoir être définie par un administrateur principal ayant accès à l'ensemble des services et informations contenues dans l'application d'administration (y compris les numéros masqués et les codes personnels). Cet administrateur principal aura le droit de créer des profils utilisateurs définissant les niveaux suivants :

- ◆ Droit d'accès à une ou plusieurs domaines : (ex : configuration, statistique, gestion des droits) ;
- ◆ Niveau d'accès aux applications : Lecture ou Lecture/Écriture ;
- ◆ Création/suppression dans les bases de données
- ◆ Etc.

5.6.2. Gestion système

L'outil d'administration du système de communications devra permettre la gestion de la totalité des paramètres en mode graphique et disposera des caractéristiques suivantes :

- ◆ Indépendance par rapport aux versions logicielles du système de communication et synchronisation automatique avec les nouvelles versions ;
- ◆ Configuration possible en mode « Batch » via des utilitaires d'Import/Export ;
- ◆ Sélection d'items à l'aide de filtres et modification automatique de tout ou partie des items sélectionnés ;
- ◆ Configuration des paramètres d'un Item (ex : usager) à partir d'une fenêtre unique ;
- ◆ Configuration des terminaux IP sur une vue graphique ;
- ◆ Configuration de la messagerie vocale directement à partir de l'application ;
- ◆ Liste d'événements de gestion donnant la date et le détail des opérations.

5.6.3. Observation des trafics

Le gestionnaire du système de communication devra pouvoir accéder, à tout moment, aux informations relatives au trafic de l'installation, l'usage des exploitations téléphoniques et le fonctionnement global du système.

Ces observations sont destinées à mesurer le degré d'utilisation du système et de détecter d'éventuels problèmes de dimensionnement.

L'application présentant les résultats devra être de type graphique.

Le candidat présentera et décrira les différentes observations possibles. Les besoins particuliers du présent cahier des charges sont les suivants :

- ◆ Observation par ½ heure, jour et par mois des éléments suivants :
 - Temps de réponse des postes appelés,
 - Trafic des postes de l'installation,
 - « Top 10 » usagers par durée
 - Trafic des groupes d'opératrices,
 - Temps moyen d'attente sur les opératrices,
 - Trafic des lignes externes regroupées en faisceaux,
 - Trafic individuel des lignes externes,
- ◆ Observation des organes assurant le bon fonctionnement de l'IPBX (taux de disponibilité).
- ◆ Observation de trafic des communications IP par client (poste ou passerelle média) ou entre deux adresses IP définies par le gestionnaire donnant les informations suivantes :
 - Le nombre de trames échangées,
 - Le nombre de trames perdues,
 - La gigue,
 - Le délai de transit.

Le candidat précisera également les possibilités d'analyse du trafic interne à l'EFS, en particulier celui transitant sur le réseau WAN.

Il est souhaité que les données de l'observation de trafic soient sauvegardées, par période, sur un dispositif permettant le rechargement et la consultation ultérieure des informations.

5.6.4. Gestion des Alarmes Systèmes

L'outil d'administration devra permettre la centralisation des alarmes et événements relatifs au système de communication ainsi que celles générées par l'outil d'administration lui-même. Ces événements et alarmes doivent être filtrés et affichés en temps réel en fonction des besoins du gestionnaire.

Ces alarmes devront être catégorisées suivant la définition faite par l'ISO soit 6 niveaux de sévérité identifiés par des couleurs différentes permettant une lecture directe. Chaque alarme devra avoir une signification détaillée en deuxième niveau, outre les causes probables, l'application devra indiquer les actions techniques nécessaires pour solutionner le problème.

En cas d'alarme majeure, un e-mail doit être automatiquement émis vers un ou plusieurs gestionnaires du système. Les listes d'alarmes et d'événements ainsi que leur signification détaillée doivent être imprimables et archivables. Des statistiques pourront être réalisées via un générateur de rapports.

L'application devra permettre un accès MIB afin de récupérer les informations système dans un outil de gestion centralisé tiers.

5.6.5. Edition des rapports

L'application de management devra permettre l'édition automatique à date récurrentes de tout type de rapport ainsi que l'envoi par e-mail desdits rapport en différents formats tel que :

- Format texte : .TXT
- Format PDF : PDF file
- Format HTML
- Format Excel : XLS file

5.6.6. Supervision

La solution devra intégrer une supervision avancée de l'ensemble des composants et services de la plateforme de téléphonie.

Deux approches seront possibles :

- Via SNMP, en mettant à disposition des MIB complètes et documentées.
- Via l'installation d'agents sur les serveurs, permettant une collecte plus fine des métriques. Dans ce cas, le développement et la mise à disposition des scripts de supervision devront être prévus et validés dès la phase d'intégration.

La supervision devra couvrir aussi bien les aspects techniques (état des serveurs, services applicatifs, Trunks SIP, QoS des communications) que les aspects fonctionnels (suivi des flux d'appels, disponibilité des services critiques, détection d'anomalies).

5.7. Annuaire système

L'annuaire interne du système de communication devra permettre l'enregistrement de **10 000 numéros minimum** à la fois interne (numéros des postes IP de l'EFS avec SDA associé) et externe (numéros client et fournisseurs).

L'annuaire du système de communication devra pouvoir être synchronisé avec la base contact de **l'EFS ; à savoir la capacité de se synchroniser avec SAP, que ce soit pour le personnel mais aussi pour les services.**

Le candidat détaillera les connecteurs ou API disponibles et les éventuels prérequis, contraintes de sécurités, etc.

Le candidat précisera notamment les possibilités **d'automatisation de l'attribution des numéros** internes et SDA à partir de la création d'un nouvel utilisateur dans l'annuaire AD de l'entreprise, de façon à permettre un **provisionnement automatique** des postes IP.

5.8. Fonctionnalités téléphoniques

5.8.1. Fonctionnalités standards

Le système de communication proposé devra intégrer à minima les fonctionnalités suivantes :

Fonctionnalité	Utilisation
Présentation du nom, du numéro	sur tous les postes compatibles (IP et DECT) avec masquage possible poste par poste
Transfert / Renvoi	Renvoi vers ligne extérieure Public : autorisé avec limitation des numéros émis
Interception	avec interception sur groupement
Rappel Automatique	configurable par poste
Restrictions d'appels	configurable par poste
Groupements de postes	groupement simple et en mode ACD
Filtrage Patron-Secrétaire	
Boîte vocale / messagerie unifiée	Boîte vocale sur tous les postes sauf poste analogique

Fonctionnalité	Utilisation
Poste Multilignes	utilisé sur poste accueil
Annuaire / Appel par le nom	avec une synchronisation avec annuaire AD (cf. 5.7)
Couplage messagerie électronique	avec Office 365 et utilisation Outlook en fonction du niveau de licence E1 et E3 (cf. 5.10.8)

5.8.2. Fonctionnalités spécifiques

Renvois extérieurs

Pour un suivi exact des coûts de communication, le renvoi d'un terminal vers un numéro externe ne fera pas appel au complément de service de l'opérateur. La gestion de ce renvoi sera assurée par l'IPBX et pourra s'établir indifféremment via le raccordement au réseau public téléphonique ou via l'accès Internet de l'EFS (renvoi vers Softphone par exemple).

De manière à préserver les coûts générés par cette fonctionnalité, il devra être possible de ne renvoyer uniquement que les appels en provenance de l'extérieur, les appels locaux suivant un traitement interne prédéfini.

Message de patience

Le système de communication devra pouvoir intégrer **plusieurs messages de patience** pouvant être affectés **sur une ou plusieurs entités de l'EFS**.

Les messages et les musiques de patience devront pouvoir être enregistrés directement par l'administrateur sur un support numérique (tout support magnétique étant exclu).

Le candidat pourra proposer une solution soit en version intégrée dans le système soit en dispositif externe.

Le candidat prendra à sa charge le premier enregistrement par un studio professionnel pour la musique générale de patience de l'EFS.

Groupement d'appels ACD

Plusieurs services disposent de groupements de postes pour lesquels les appels sont gérés à travers des files ACD (Automatique Call Distribution). Chacune de ces files ACD dispose d'un message de dissuasion en cas de saturation des files d'attentes.

5.9. Gestion automatique des appels (SVI)

Le système de communication proposé devra être équipé d'une application dite "standard automatique" ou **serveur vocal interactif (SVI)**, permettant sous certaines conditions l'accueil des correspondants extérieurs en leur proposant de manière interactive l'orientation vers un service ou un correspondant pré défini.

Le dialogue interactif sera à base de codes à fréquence vocale Q23, les cas d'erreurs (codes erronés) seront traités par un message d'information et retour au message courant de l'arborescence. Si aucun code Q23 n'est reçu, l'appel débordera automatiquement, après une temporisation paramétrable vers un numéro pré défini.

Cette application sera utilisée aussi bien pendant et en dehors des heures de présence des postes d'accueil des entités concernés et devra pouvoir être exploitée avec des **configurations différentes suivant les entités**.

La solution proposée devra pouvoir supporter **un SVI** par site EFS. Les films sonores des annonces existantes pourront être fournis par l'EFS afin que le futur titulaire les intègre dans la nouvelle solution.

5.9.1. Configuration SVI

Les besoins des entités concernés sont les suivants :

Arborescence de jour :

- ◆ 2 niveaux de rubrique,
- ◆ 4 choix minimum par rubrique,
- ◆ 1 message d'erreur,
- ◆ 1 message d'excuse.

Arborescence de nuit :

- ◆ 1 niveau de rubrique,
- ◆ 4 choix- par rubrique,
- ◆ 1 message d'excuse.

Le basculement du message de nuit au message de jour doit être automatique et lié au basculement du(es) poste(s) d'accueil du site concerné. Le transfert d'un appel vers un correspondant interne ou un service (groupe de postes) doit être supervisé par l'application. Si le demandé est libre ou renvoyé, la communication sera transférée ; si le demandé est occupé, l'appelant recevra la tonalité d'occupation ou sera orienté vers la messagerie vocale, si le demandé bénéficie de ce service.

Cette application étant destinée à traiter des appels entrant sur des périodes horaires où le trafic peut être important, il est nécessaire de disposer d'un système capable de traiter **32 connexions simultanées**. Le candidat précisera si le système proposé est intégré ou extérieur à l'IPBX ; les capacités d'extension ainsi que les modularités de la solution seront décrites.

5.9.2. Renvoi de nuit automatique

Le renvoi de nuit sera activé, de manière automatique, par une horloge système. Il est souhaité, dans le présent appel d'offres, d'élargir la notion de "renvoi de nuit" à des états intermédiaires, afin de mieux s'adapter à l'organisation de l'entreprise.

Exemple de fonctionnement souhaité, en jours ouvrés, du lundi au vendredi :

- De 8h00 à 18h00, l'installation est en fonctionnement normal, les SVI prennent en charges le trafic entrant en mode jour, l'acheminement SDA est actif sur l'ensemble de l'installation ;
- De 18h00 à 8h00, l'installation bascule en renvoi de nuit : les appels entrants sont orientés vers une arborescence dite de "nuit" du SVI ; l'acheminement des SDA reste normal. Les droits d'accès des usagers aux appels externes sont conservés pour tous les postes installés en espaces fermés mais sont réduits à l'appel des numéros d'urgence (pompiers, police, etc.) pour tous les postes en espaces librement accessibles.
- Le samedi et le dimanche, l'installation sera en renvoi de nuit permanent.

5.9.3. Blocage des numéros entrant sur appel intempestif

La solution de communication devra permettre le blocage des appels entrants depuis certains numéros identifiés comme sources d'appel intempestif. Cela peut correspondre à des appels de fax mal dirigé, des appels publicitaires, etc. Le candidat précisera le mode de blocage qu'il peut mettre en place : détection automatique des porteuses de fax, blocage automatique sur récurrence d'appel, saisie d'un code service pour blocage de la réception, etc...

5.10. Messagerie vocale

Le système de communications devra être équipé d'une application de **messagerie vocale**.

Le candidat décrira la totalité des services proposés aux utilisateurs et au gestionnaire de la messagerie, les capacités maximales de celle-ci en boîtes vocale, en capacité d'enregistrements et en accès simultanés.

Les besoins particuliers du présent cahier des charges sont de **1000 boîtes aux lettres vocales, 16 accès simultanés Voix et 100 heures d'enregistrement**, ainsi que les services décrits ci-après.

La capacité de la messagerie vocale devra pouvoir être étendue à **1500 boîtes maximum** par simple adjonction de licences complémentaires. De même la capacité d'enregistrement devra pouvoir être doublée.

5.10.1. Fonction répondeur ou répondeur/enregistreur

Le dispositif devra offrir au choix des titulaires de boîtes vocales les deux fonctions répondeur ou répondeur/enregistreur horodatant les messages.

5.10.2. Annonces personnalisables

Lors de la validation d'un renvoi vers la messagerie vocale, le titulaire pourra choisir entre deux annonces personnalisées. Dans le cas où les annonces personnalisées ne sont pas enregistrées, l'annonce standard sera automatiquement substituée.

5.10.3. Appel renvoyé vers la messagerie vocale

Le transfert automatique vers la messagerie vocale, d'un appel en réception, pourra s'établir soit immédiatement, dans le cas d'un appel sur un poste renvoyé volontairement, ou après une temporisation de non-réponse. Après l'écoute de l'annonce, l'appelant pourra soit déposer un message, soit décider de déborder vers les positions de réponse ou un poste particulier.

5.10.4. Indication de messages en attente

Le titulaire est averti de la présence de messages par une lampe allumée sur son poste (poste IP ou analogique équipé d'une lampe message). Concernant les terminaux ne disposant pas de lampe message, il serait souhaitable qu'au décroché un message vocal informe l'utilisateur de la présence de messages. Le candidat décrira les modes opératoires de cette exploitation.

5.10.5. Consultation des messages

Le titulaire peut consulter ses messages en attente à partir d'un poste interne quelconque ou d'un poste extérieur via le réseau téléphonique général. A partir d'un terminal IP, il est demandé, en cours de consultation, une interactivité entre l'afficheur et les services courants exemple : avance rapide, stop retour, archivage, suite, message précédent, etc.

5.10.6. Confidentialité d'accès

La confidentialité dans l'enregistrement des annonces personnalisées et dans la consultation des messages sera assurée par un code personnel à minima à 4 chiffres (idéalement 6).

5.10.7. Archivage des messages

Le système de messagerie archivera automatiquement les messages ; seule une demande d'effacement volontaire de l'utilisateur annulera ces derniers dans une période définie par le gestionnaire du système. Au-delà de cette période de stockage les messages les plus anciens seront automatiquement effacés.

5.10.8. Fonctionnement en mode Unifiée

Afin de simplifier la gestion des boîtes vocales des utilisateurs de l'EFS, la fonctionnalité minimum attendue est que les messages vocaux reçus par les postes fixes puissent être **transférer vers la boîte mail** de l'utilisateur de façon automatique.

Afin de limiter l'espace nécessaire au stockage des messages, le système de messagerie vocale devra effacer automatiquement les messages les plus anciens au profit des nouveaux.

5.10.1. Sécurité

Les messageries vocales devront avoir un niveau de sécurité satisfaisant pour ne pas permettre une utilisation frauduleuse par un tiers (code pin par défaut, etc. – cf. **Exigences de Sécurité des Systèmes d'Information (SSI) pour les candidats ou titulaires de l'EFS**).

5.11. Solution de Mobilité interne : réseau DECT

L'EFS dispose aujourd'hui de mobilité Voix basée sur des bornes DECT majoritairement connectées sur des ports numériques.

Le titulaire devra proposer le remplacement de cette infrastructure par une solution de type DECT sur IP ; les terminaux existants pourront être réutilisés si compatibles.

Les besoins en mobilité DECT sont les suivants :

- Nombre de mobiles : environ 3000
- Nombre de bornes : 727 bornes intérieures.

La solution de mobilité devra répondre aux critères suivants :

- ♦ Commutation inter-borne (handover) fluide, sans coupure d'appel lors des déplacements ;
- ♦ Capacité par borne : au minimum 4 à 8 appels simultanés (selon le modèle proposé) ;
- ♦ Scalabilité : possibilité d'ajouter des combinés ou bornes sans modification majeure de l'architecture ;
- ♦ Compatibilité SIP pour intégration avec le système de téléphonie IP existant ;
- ♦ Support des terminaux en mode GAP ;
- ♦ Administration centralisée de l'infrastructure DECT (provisioning, mises à jour, supervision) ;
- ♦ Intégration à l'annuaire d'entreprise (LDAP ou autre) pour composer les numéros internes facilement ;
- ♦ Sécurité des communications : chiffrement entre les combinés et les bornes si disponible.

Le candidat fournira une liste de postes DECT/IP qui répondra aux critères suivants

- ♦ Combinés robustes adaptés à un usage professionnel (IP65 ou supérieur selon les environnements).
- ♦ Autonomie des combinés : minimum 12 à 15 heures en conversation.
- ♦ Fonctionnalités PTI / DATI intégrées pour certains postes :
 - Bouton d'alarme manuel.
 - Détection de chute / perte de verticalité.
 - Détection d'immobilité prolongée.
 - Transmission automatique d'alertes vers un dispositif de supervision ou d'intervention.

5.12. Communication unifiée

Le candidat devra proposer une solution de communication unifiée exploitable indifféremment avec un poste fixe ou un softphone ; il précisera également les possibilités d'intégration avec un client de messagerie électronique (Exchange).

5.12.1. Intégration dans le poste client

Le candidat précisera le type de client utilisé sur chaque PC : client lourd installé sur le poste de travail ou accès en mode Web.

Dans le premier cas, le candidat précisera les besoins en termes de ressources internes (espace disque, mode de fonctionnement) ainsi que la méthodologie de déploiement.

Le candidat indiquera le niveau de compatibilité de sa solution avec les matériels PC et les OS existants (Windows 7, 8 et 10, Mac OS...).

5.12.2. Fonctionnalité de base

Le candidat précisera parmi les fonctionnalités listées ci-dessous celles qui pourraient être accessible directement depuis un client de messagerie écrite (Outlook, ...) :

- ♦ Numéroteur universel depuis divers documents électronique (bureautique, messagerie, internet, etc....)
 - Click-to-call
 - Glisser / déplacer (ou copier / coller) avec nettoyage du numéro
- ♦ Traitement des appels entrants et sortants
 - Fonctions : décrocher-raccrocher, dévier, mise en attente, conférence
 - Résolution de nom
 - Routage d'appels en fonction de la présence Calendrier.
- ♦ Journaux d'appels
 - Appels entrants / sortant / manqués.
- ♦ Gestion de contacts (annuaires externes)
 - Actions sur un contact : appel, prise de notes, envoi de mail, SMS, Chat
 - Partage de contact
- ♦ Informations de présence
 - Intégré à l'outil avec commande manuelle
 - Synchronisé avec le Calendrier de la messagerie écrite
 - Suivant l'état du poste Téléphonique ;
- ♦ Suivant l'état du poste de travail (connecté, verrouillé, etc..).

Le candidat devra de plus préciser le coût de l'option de fonctionnement avec **Teams** et avec quel niveau de **licence** les services décrits ci-dessus sont accessibles. Le candidat devra préciser les fonctionnalités offertes par ce couplage avec Teams, s'il permet une unification de l'usage de Teams et du softphone par exemple.

5.12.3. Convergence fixe-mobile

Dans le cadre de l'évolution future des besoins liés à la mobilité, certains utilisateurs équipés de téléphone GSM de type Smartphone (iPhone, Android, ...) devront pouvoir accéder à des fonctionnalités de convergence fixe-mobile avec les possibilités suivantes :

- ♦ Attribution d'un numéro unique de téléphonie fixe permettant de joindre indifféremment l'utilisateur sur son poste fixe de bureau et sur son GSM ;
- ♦ Gestion d'une boîte de messagerie vocale unique fixe-mobile ;
- ♦ Attribution de fonctions spéciales sur le réseau GSM : conférence à trois, transfert d'appels, gestion de présence grâce à l'installation de l'application de convergence sur les GSM.

Le candidat décrira les fonctionnalités et possibilités liées aux fonctions de convergence fixe-mobile et donnera une liste des prérequis et terminaux compatibles.

De même, il devra indiquer si ces fonctionnalités sont liées à **un complément d'abonnement Data (3G/4G)** sur les postes mobiles GSM.

Le candidat devra intégrer dans son offre l'ensemble des équipements nécessaires à la connexion des mobiles GSM avec le système de communication à travers le réseau public Internet. Il devra entre autres prévoir les systèmes de sécurisation à déployer dans la zone DMZ de l'accès Internet de l'EFS.

5.12.4. Communication sur le Réseau Wifi

Compte tenu de la disponibilité d'un **réseaux Wifi étendu** sur plusieurs sites de l'EFS, le candidat présentera le type de **solution Voix sur IP** qu'il propose dans cet environnement.

Le candidat devra clairement indiquer dans son offre les contraintes et les limites d'utilisation des terminaux Wifi ainsi que toutes les ressources nécessaires (licences, compresseur IP, etc...).

Il devra également indiquer les prérequis nécessaires pour l'utilisation de terminaux type Smartphone en tant que poste mobile interne au système de communication.

5.13. Télétravailleurs

L'EFS souhaite pouvoir répondre au nouvel enjeu du télétravail en proposant aux utilisateurs concernés des terminaux et/ou des solutions de Softphones permettant une exploitation à distance des ressources du système de communication.

Les fonctionnalités attendues pour les postes de télétravailleurs sont les suivantes :

- ◆ Mise à disposition d'un numéro interne et externe (SDA) ;
- ◆ Gestion des appels à distance, à travers une connexion sécurisée avec le système de communication : le candidat décrira le mode de connexion proposée ;
- ◆ Transfert des appels reçus vers l'utilisateur sur le poste de son choix : vers poste IP Fixe ou Softphone, vers mobile entreprise ;
- ◆ Accès à la messagerie vocale d'entreprise ;
- ◆ Accès à la solution de communication unifiée : préciser les limites fonctionnelles ;
- ◆ Gestion des appels sortants à travers le système de communication de l'EFS avec l'édition des tickets de taxation correspondants dans le système de gestion des couts opérateurs.

Le candidat décrira précisément le mode de fonctionnement de l'application dédiée aux télétravailleurs ainsi que les ressources nécessaires pour son hébergement sur le système d'information de l'EFS et en particulier le type de connexion VPN utilisé.

Concernant l'utilisation de Softphone, le candidat précisera notamment si le VPN nécessaire au fonctionnement du Softphone peut cohabiter sur le PC de l'utilisateur avec **un VPN Data de type IPsec ou SSL**.

5.14. Terminaux téléphoniques

5.14.1. Postes téléphoniques IP

Le candidat présentera sa gamme de terminaux IP. Parmi les postes proposés, le candidat devra disposer d'au moins deux terminaux répondant, à minima, aux caractéristiques suivantes :

- ◆ Télé alimentation au **standard 802.3af Classe POE-1 ou POE-2 maximum** ; alimentation locale 220 volts possible ;
- ◆ Switch interface Ethernet 100/1000 auto-sensing;
- ◆ Port PC intégré en Gigabit ;
- ◆ QoS interne au poste et priorité à la voix ;
- ◆ Marquage des trames voix niveau 2 : 802.3 p/ Q et niveau 3 : DSCP ToS/ DiffServ ;
- ◆ Restitution transparente des trames PC associé (pas de marquage des trames PC par le poste) ;
- ◆ Allocation fixe ou dynamique de l'adresse IP par client DHCP ;
- ◆ Compatible avec l'usage du protocole 802.1x.

5.14.2. Gamme des postes IP

Il est souhaité, dans la présente consultation plusieurs types de postes IP et/ou SIP.

Type 1 (IP) poste de Direction ou utilisateur à fort trafic :

- ◆ Afficheur graphique 3,5 pouces minimum, rétroéclairé ;
- ◆ Clavier alphanumérique physique ou virtuel sur afficheur tactile pour la recherche de numéros interne et externe ;
- ◆ Réglage du contraste de l'afficheur ;
- ◆ 4 touches contextuelles minimum liées à cet afficheur ;
- ◆ 4 touches programmables minimum (renumérotation, fonction secret, accès messagerie, etc..) ;
- ◆ Signalisation associée à chaque touche par symboles de type icônes ou texte court ;
- ◆ Voyant de signalisation de la messagerie (vocale et texte) ;
- ◆ Main libre et écoute amplifiée ;
- ◆ Réglage du volume de l'écouteur du combiné ;
- ◆ Service d'aide à la programmation intégré ;
- ◆ Prise casque ;
- ◆ Options possibles : Boîtiers de touches additionnelles (jusqu'à 50 touches), fonctionnalités Bluetooth pour connexion d'un casque Bluetooth.

Type 2 (IP ou SIP) poste d'agent :

- ◆ Afficheur graphique noir et blanc : 3 lignes minimum ;
- ◆ Réglage du contraste de l'afficheur ;
- ◆ 4 touches contextuelles minimum liées à cet afficheur ;
- ◆ Signalisation associée à chaque touche par symboles de type icônes ou texte court ;
- ◆ Voyant de signalisation de la messagerie (vocale et texte) ;
- ◆ Écoute amplifiée ;
- ◆ Service d'aide à la programmation intégré ;
- ◆ Options possibles : prise casque.

Type 3 (IP ou SIP) poste de conférence :

- ◆ Afficheur graphique de configuration ;
- ◆ Clavier de numérotation directe ;
- ◆ Main libre omnidirectionnel haute-fidélité ;
- ◆ Touches « Secret », touche renumérotation ;
- ◆ Système de détection de parole avec réduction des bruits ;
- ◆ Sortie son pour amplificateur externe ;
- ◆ Option : de 1 à 3 micros supplémentaires.

Module de touche pour poste IP

Le candidat décrira le type de module de touche qu'il est à même de proposer (module IP ou connexion direct sur le poste) ainsi que le nombre et le mode de configuration des touches programmables.

Les touches programmables directement par l'utilisateur devront permettre de chaîner plusieurs fonctions (exemple : préfixe de renvoi + Numéro extérieur, etc..), et pour répondre aux problèmes d'organisation spécifiques de l'EFS, il serait souhaitable de pouvoir verrouiller les touches de certains terminaux afin de figer des configurations particulières (profils).

Le quantitatif des terminaux est indiqué au DQE.

5.14.3. Terminaux analogiques

Les terminaux analogiques (postes téléphonique, platine interphone, télécopieur, ...) devront pouvoir être pris en compte par adjonction d'interfaces spécifiques sur les Passerelle média ou par adaptateur IP multiports. Les interfaces de raccordement pourront recevoir indifféremment des terminaux à numérotation décadique ou à numérotation à fréquence vocale Q23, la reconnaissance du type de numérotation par l'équipement sera automatique.

Lors de la phase de collecte, le recensement de ces équipements sera nécessaire, l'opportunité de les remplacer par des équipements IP pourra être étudié en fonction des impacts.

5.14.4. Softphone

Le système de communications devra pouvoir accepter des terminaux de type « Soft Phone ». Ils disposeront au minimum des caractéristiques suivantes :

- Interface permettant d'accéder à l'ensemble des fonctionnalités téléphoniques à partir du réseau LAN ou depuis un accès extérieur (VPN opérateur, Internet Sécurisé, etc...) ;
- Accessibilité complète à la messagerie vocale de l'entreprise ;
- Prise en charge des fonctions Click-to-call (depuis des pages Web ou des contacts de messagerie) ;
- Support des environnements Microsoft Windows en version française, ainsi que MacOS / Linux / Android.

Le candidat devra clairement préciser le **mode d'intégration du Softphone** sur le PC de l'utilisateur : client lourd installé sur la machine ou client léger accessible en HTML, ainsi que les **limites fonctionnelles** de chaque mode d'intégration.

Le titulaire devra intégrer dans le contrat de maintenance de la solution, la mise à jour des versions logicielles des Softphones au fur et à mesure des mises à jour de l'application de communication (cf. paragraphe 9.4.4).

5.15. Solution FAX/IP

Afin d'assurer le transport des flux FAX indépendamment des Trunk SIP centraux et pour des raisons de compatibilités avec les équipements fax existant, une passerelle média avec interface type T2 sera installée, dans un des datacenters supportant les Trunk SIP centralisés, pour le raccordement sur accès de type T2/IP avec 30 canaux de communications.

Cette passerelle restera conforme aux prescriptions techniques indiquées au paragraphe 5.5.3 et devra pouvoir supporter en extension un T2 supplémentaire.

5.16. Performances

Le candidat détaillera les prérequis pour atteindre le niveau de service présenté ci-dessous

5.16.1. Exigences réseaux minimales

Bande passante par appel

- Minimum requis : **100 kbps symétriques par appel simultané** (codec G.711).
- La solution doit s'adapter dynamiquement à des codecs plus compressés (ex. G.729, Opus) si besoin.

Latence (aller-retour)

- Latence RTT (round-trip time) maximale : **≤ 150 ms** entre le terminal et le SBC (Session Border Controller).

Jitter (variation du délai)

- Jitter maximal autorisé : **≤ 30 ms**.
- Une **mise en tampon adaptative (jitter buffer)** doit être gérée côté passerelle ou softphone.

Taux de perte de paquets

- Taux de perte de paquets admissible : **< 1 % sur 10 secondes d'appel**.
- Une **correction d'erreur ou compensation (PLC - Packet Loss Concealment)** est souhaitée.

Le soumissionnaire devra préciser les prérequis nécessaires pour obtenir ces taux de performances ainsi que le maintien de ces performances lors de montée en charge / pic d'activités.

5.16.2. Tolérance réseau & continuité de service

En cas de coupure de lien WAN ou interco SIP, la solution doit proposer :

- un **basculement automatique** (failover) vers un autre lien ou un autre SBC,
- ou un mode **local survivability** (ex. via un relais local, autocom ou passerelle SIP).

Le système doit être capable de **répartir dynamiquement la charge** entre plusieurs Trunks SIP ou SBC.

5.16.1. Expérience utilisateur

Les niveaux de performances suivants sont attendus pour pouvoir permettre une expérience utilisateur satisfaisante :

- Objectif de qualité audio : **MOS (Mean Opinion Score) $\geq 4,0$** (Acceptable ou Excellent)
- Codec par défaut : **G.711**
- Le délai de signalisation entre la composition du numéro et la sonnerie ne doit pas dépasser **2 secondes**
- Bascule entre deux trunks SIP (ou SBC) : **< 5 secondes**
- Capacité à rediriger un appel vers un numéro de secours en cas de perte de connexion pendant l'appel

5.17. Sécurisation de la plateforme

Le candidat devra proposer son plan de sécurisation de la plateforme de téléphonie, en précisant d'éventuels impacts sur la solution de téléphonie.

- Modification de tous les accès/mots de passe par défaut
- Mise en place des protocoles de sécurité (TLS, HTTPS)
- Mise en place de certificat et processus de renouvellement
- Désactivation des services inutiles
- Désactivation des protocoles obsolètes / non sécurisés (ex : SNMP V1...)
- Activation de double authentification
- Détection d'anomalies ou de tentative de brute-force : ex : blocage lors de X authentification en erreur

(Cf. Exigences de Sécurité des Systèmes d'Information (SSI) pour les candidats ou titulaires de l'EFS, en annexe).

5.17.1. Matrice de flux

Le soumissionnerai devra fournir dans son document d'architecture la liste des flux, ports, protocoles à ouvrir ainsi que la description et le rôle de ces flux.

Lors de la phase projet, ces flux devront être adaptés au strict besoin de l'EFS.

6. Prestations de déploiement, contrôles, tests EFS et recettes

Les prestations de déploiement décrites au présent paragraphe concernent la mise en place de la solution de communication ainsi que les phases de recette VABF et VSR associées.

L'organisation du déploiement devra être conforme aux prescriptions détaillées dans la suite de ce paragraphe et tenir compte du phasage retenu.

Conjointement aux prestations de déploiement et pour chaque phase concernée, le titulaire devra également assurer :

- Le Pilotage du déploiement tel que décrit au paragraphe 8
- Le Contrôle qualité tel que décrit au document Annexe 1 ;

6.1. Détail des prestations de déploiement

Pour réaliser la mise en œuvre des systèmes de communication, les prestations générales du titulaire doivent être au minimum :

- La définition du cahier d'étude technique pour la réponse aux besoins fonctionnels exprimés dans le présent Cahier des Clauses Techniques ;
- La collecte des données de configuration des systèmes existants ;
- Le **déploiement des systèmes de communications et applications annexes** ainsi que le paramétrage des applications **en phase de maquetage** ;
- Le déploiement de l'ensemble des équipements complémentaires à la phase de maquetage (poste IP, passerelles médias, postes analogique...) ;
- Le **raccordement de la nouvelle solution** aux réseaux opérateurs télécoms (Trunk SIP) et au réseau privé (LAN et VPN MPLS) ;
- Le câblage et/ou l'extension de câblage pour la connexion de nouveaux terminaux (cf. BPU) ;
- Les formations des utilisateurs, opérateurs et gestionnaires.

6.1.1. Plan de migration

Le plan de migration des infrastructures de communication pressenti pour chaque phase est le suivant :

Phase initiale :

- Mise en place des serveurs de communication centraux en Datacenter ;
- Déploiement de postes IP et softphones pour validation maquette ;
- Configuration des SVI et des groupements ACD pour validation maquette ;
- Connexion des Trunk SIP centralisés ;
- Connexion de la passerelle dédiée aux communications Fax ;
- Intégration avec Teams ;
- Formation administrateurs.

Phase pilote (sur 2 Régions présélectionnées dont IDFR) :

- Déploiement des postes administratifs IP et/ou softphones (en remplacement de postes numériques et analogiques) soit environ 700 terminaux IP et 300 Softphones.
- Déploiement Passerelle média analogique et raccordement des postes ;
- Mise en place de passerelles vers les hôpitaux ;
- Migration de l'infrastructure DECT/IP ;
- Test et validation des configurations avant migration (prestation globale reportée au DQE IDFR) ;
- Portabilité SDA vers Trunk SIP central ;
- Portabilité des numéros de Fax vers la passerelle centralisée ;
- Formations utilisateurs ;
- Dépose des anciens équipements.

Phase intégration (sur les Régions restantes) :

- Migration des postes administratifs (numériques et analogiques) vers postes IP et/ou softphones ;
- Déploiement Passerelle média analogique et raccordement des postes ;
- Mise en place de passerelles vers les hôpitaux ;
- Migration de l'infrastructure DECT/IP ;
- Portabilité SDA vers Trunk SIP central ;
- Portabilité des numéros de Fax vers la passerelle centralisée ;
- Formations utilisateurs ;
- Dépose des anciens équipements.
- ... ;

6.1.2. Calendrier d'intervention et plan de charge en homme/jour

Avant la mise en œuvre de chaque phase, l'EFS exige du titulaire la production d'un **calendrier précis tenant compte des contraintes de l'EFS** et indiquant les délais de réalisation de chaque étape de migration ainsi que les périodes de vérification d'aptitude (VA) et de services réguliers (VSR) après la mise en production.

A chacune des étapes décrites dans ce paragraphe, le titulaire doit prendre les dispositions nécessaires pour garantir la continuité du service rendu aux utilisateurs l'EFS, et en particulier la possibilité de procéder à certaines migrations en HNO (heure non ouvrée) ou de nuit.

En complément du calendrier de déploiement, le titulaire fournira le plan de charge des interventions techniques (en homme/jour) avec le profil des intervenants (architecte, expert, technicien, etc.) ainsi que la charge correspondante pour les équipes techniques de l'EFS.

Le candidat joindra à son offre le calendrier de déploiement qu'il prévoit pour chacune des phases ainsi que les plans de charge correspondants.

Ces documents seront remis à jour en accord avec l'EFS au démarrage de chaque phase.

Le candidat proposera un ordonnancement des régions en fonction des critères qui lui semblent pertinents (complexité, taille, obsolescence etc...). Cette proposition sera étudiée par l'EFS et pourra être revue en fonction des contraintes opérationnelles.

6.1.3. Collecte de données

Sur la base des documents qu'il aura fournis avec son offre, le titulaire aura la charge de procéder à la saisie complète de l'ensemble des éléments qu'il aura à collecter. Pour cela il devra exécuter les tâches suivantes :

- ◆ Rédiger et personnaliser les fiches de collecte de données ;
- ◆ Faire la présentation auprès du chef de projet client des objectifs de la collecte ;
- ◆ Editer les fiches de saisies pour validation ;
- ◆ Prendre en compte les modifications ou compléments ;
- ◆ Proposer un **nouveau plan de numérotation** au niveau national ;
- ◆ Éditer la collecte pour acceptation.

La collecte doit être la plus exhaustive possible, mais ne doit pas provoquer trop d'excès de charge des personnels de l'EFS. Chaque étape nécessite la validation des services concernés de l'EFS.

Concernant le plan d'adressage IP des différents VLAN nécessaires à la configuration du système global, le titulaire devra effectuer une demande auprès des équipes de l'EFS selon un descriptif précis des besoins d'architecture détaillée. Le titulaire devra se conformer aux plans d'adressage définis par l'EFS.

6.1.4. Vérification des matériels

Le titulaire est tenu de procéder, pendant l'exécution des prestations, aux vérifications techniques qui lui incombent :

- ◆ Pour le matériel et les logiciels, ils s'assurent que les produits commandés et livrés sont conformes à la commande, aux normes, ainsi qu'aux spécifications du CCTP ;
- ◆ Ils réalisent les vérifications et essais imposés par les normes, D.T.U. et les règles professionnelles, ainsi que ceux exigés par le CCTP

Les résultats de ces vérifications seront consignés dans un procès-verbal, intégrant la liste exhaustive des matériels fournis, qui sera transmis pour examen à l'EFS.

6.1.5. Phase de Test et Maquettage

La phase de test et de maquettage avant mise en production permet d'évaluer les possibilités de migration dans de bonnes conditions. Le titulaire fournit les moyens nécessaires permettant de mesurer le niveau de la prestation.

Le titulaire a la responsabilité de l'installation et de la mise en service de la configuration de test. Il fournira les plans et la méthodologie d'installation de la maquette à l'EFS qui les validera avant de démarrer les travaux.

Les éventuels prérequis à l'installation seront transmis dans un délai raisonnable pour que l'EFS puisse s'organiser.

Le titulaire doit proposer une procédure de tests pour validation à l'EFS. Elle doit comporter les essais fonctionnels, tests de sécurisation (redondance), etc.

Le résultat des tests de fonctionnement sera ensuite consigné dans un procès-verbal de vérification d'aptitude de la phase 'maquette' rédigé par le titulaire et approuvé par l'EFS.

Détail des tests de validation de la maquette :

Périmètre	Détail
Solution de communication	Vérification de la configuration par rapport à la collecte des données
Passerelle Média opérateur	Etablissement de communications avec un accès Trunk SIP de test
Passerelle analogique	Test de communication avec poste analogique en numérotation, simulation d'appel vers hôpital
Poste IP	Test de communication avec poste interne et numéro externe, mise en attente, conférence, transfert, etc.
FAX	Test d'émission et réception FAX
Serveur vocal interactif	Test d'une arborescence type
Intégration Teams	Test du fonctionnement de la communication unifiée avec Teams
Système de management	Vérification des accès et des droits administrateur

Les retards dans l'acceptation de la phase de maquettage, consécutifs à une qualité insuffisante ou une non-conformité, ne constituent pas une cause de report du délai contractuel sauf en présence d'un cas de force majeure ayant empêché l'exécution du marché par le titulaire. Le titulaire encourt donc des pénalités si de tels retards sont constatés.

Après validation de la vérification d'aptitude, le titulaire peut passer à la phase de mise en ordre de marche.

6.1.6. Migration et mise en ordre de marche

Pour chacune des phases successives de déploiement, le titulaire devra au titre de la mise en ordre de marche :

- ♦ L'installation des passerelles media et des postes IP sur sites ;
- ♦ Le raccordement des postes sur les passerelles analogiques ;
- ♦ Le raccordement des passerelles dédiées pour les hôpitaux ;
- ♦ Le raccordement et test des accès opérateurs public et privé ;
- ♦ Le contrôle du câblage nécessaire entre les systèmes de communications et les éléments suivants :
 - Les alimentations d'énergie ;
 - L'arrivée des accès opérateur ;
 - Le répartiteur général ou les baies de brassage ;
 - Les terminaux téléphoniques ;
 - Les systèmes annexes.
- ♦ Le repérage et le marquage complet de tous les tenants et aboutissants de l'installation.

L'EFS attire l'attention des candidats sur les contraintes de migration liées aux disponibilités des prises informatiques dans les locaux ne permettant pas toujours une coexistence des solutions de téléphonie à remplacer et à venir :

- ♦ Certain poste de travail ne dispose que d'une seule prise RJ45 informatique, ce qui peut conduire à un raccordement en cascade du poste de travail (PC) derrière le poste téléphonique IP ;
- ♦ Les prises RJ45, sur lesquelles des postes numériques sont raccordés, pourront être réutilisées pour la connexion d'un terminal IP après vérification du câblage et raccordement sur un port de switch.

Au vu de l'activité de l'EFS, ayant un fonctionnement critique et 24h/24, une attention toute particulière sera à prévoir pour la continuité d'activité lors de cette mise en place (perte d'appels, organisation du service...). Le candidat devra détailler sa démarche projet et l'accompagnement des utilisateurs.

6.1.7. Formations

La formation est incluse dans l'offre de base et sera détaillée dans le mémoire technique du candidat.

Elle sera dispensée par un personnel qualifié pour cette tâche et aura lieu conformément au planning établi en accord avec l'EFS.

La formation sur l'exploitation et l'utilisation des postes téléphoniques IP sera effectuée auprès de relais utilisateurs. Ces relais utilisateurs seront chargés eux-mêmes de dispenser les formations aux utilisateurs finaux.

Les gestionnaires du système de communication à l'issue de leur formation, devront être en mesure d'assurer la gestion courante de l'installation telles que :

- création et suppression de poste, modification des paramètres principaux : nom, type de poste, catégorie d'exploitation, catégorie d'accès, centre de frais, groupement de postes,
- gestion de la numérotation abrégée ;
- gestion des système SVI.

Ils devront aussi connaître la signification des alarmes et savoir déterminer l'échelle de gravité d'un incident.

Les temps minima indispensables de formation seront de :

- 1 heure minimum pour les utilisateurs classiques, par groupe de 6 à 8 personnes (cf. : nombre de groupe dans BPU) ;
- 2 heures minimum pour les profils fort communicant, par groupe de 6 à 8 personnes (cf. : nombre de groupe dans BPU) ;
- 2 jours pour la gestion/ annuaire/topologie/observation des trafics du système de communication pour un groupe de 6 à 8 utilisateurs, + 1h de rappel avant la fin de VSR.

En complément à ces formations, il est demandé au titulaire de prévoir un transfert de compétence vers certains personnels de l'EFS (expert Telecom) afin que ces derniers puissent assurer les interventions de maintenance Niveau 1 tel que : remplacement de postes IP, configuration de Softphone, remplacement de passerelles analogiques, etc.

Ce transfert de compétence sera précédé d'une formation constructeur (chiffrée distinctement au BPU) sur l'ensemble des équipements déployés dans la solution finale.

Le titulaire devra valoriser le nombre de jours nécessaire pour la formation de 2 équipes de 8 personnes.

Hormis la formation constructeur, les modules de formation et les supports seront réalisés sur site, suivant le personnel de destination. Le contenu de ces formations sera délivré par le titulaire et soumis à l'approbation de l'EFS.

Une proposition de formation type « e-learning » peut être proposée par le titulaire.

De plus, le titulaire rédigera un **mode d'emploi personnalisé** pour chacun des postes proposés qui pourra être **consultable en ligne sur l'Intranet** de l'EFS. Il en présentera un modèle dans son mémoire technique.

L'ensemble des formations (hors transfert de compétence) devra avoir été réalisé **avant la phase de vérification d'aptitude** au bon fonctionnement (VABF).

6.2. Vérification d'Aptitude au Bon Fonctionnement (VABF)

Cette vérification s'appliquera au **déploiement lié à la phase pilote et à celui de chaque Région**, ou, le cas échéant, aux migrations résultant de changements importants dans l'infrastructure proposée par le titulaire.

Pour la réception des prestations, le titulaire doit fournir l'installation complète et fonctionnelle, en parfaite conformité avec les règlements et les règles de l'art, sans pouvoir considérer comme limitatives les indications du présent CCTP.

Lorsque qu'il a procédé à la mise en service (en préproduction) de l'infrastructure et aux essais et mises au point technique, le titulaire avise l'EFS de la possibilité de procéder à la vérification d'aptitude. Il fournit alors à l'EFS un Procès-Verbal de Vérification d'Aptitude que l'EFS complète et signe après une période de test sur plusieurs jours ouvrés. L'EFS peut émettre des réserves ou signer le PV sans remarques.

Dans le cas où une quelconque non-conformité se révèle, avant ou après la vérification d'aptitude de l'installation, le titulaire est tenu d'exécuter la mise aux normes à ses frais.

La vérification d'aptitude doit être effectuée dans des conditions les plus proches possibles des conditions opérationnelles. Elle débouche sur la mise en production.

Les opérations de vérification d'aptitude comprennent :

Pour le déploiement de la phase initiale et pour chaque région :

- Les tests de bon fonctionnement de l'ensemble des matériels et des logiciels pour les fonctions requises ;
- La vérification des performances exigées et annoncées par le prestataire en termes de service sur une **période de 5 jours ouvrés**, à compter de la mise en service (en préproduction) ;

Pour le déploiement de la phase initiale uniquement :

- La vérification de la notice actualisée présentant les modalités d'accès au Service 'Hotline' du titulaire. Ces documents doivent être rédigés par le titulaire et livrés à l'EFS avant le démarrage de la VA.
- La vérification de la notice actualisée présentant les modalités pratiques de gestion des changements. Ces documents doivent être rédigés par le titulaire et livrés à l'EFS avant le démarrage de la VA.

Le prestataire aura à sa charge l'organisation des opérations de vérification d'aptitude au bon fonctionnement et les documents en découlant.

Ceux-ci doivent apporter la preuve que les opérations de contrôle qui garantissent un fonctionnement de qualité ont bien été effectuées et fournir les moyens nécessaires permettant de mesurer le niveau de la prestation.

La mise en production des nouveaux matériels et services ne peut être réalisée qu'à l'issue de la vérification d'aptitude et après accord entre le titulaire et l'EFS sur les modalités et le planning de basculement vers la solution cible retenue.

6.3. Vérification des Services Réguliers (VSR)

Elle ne s'applique qu'à la migration initiale, ou, le cas échéant, aux migrations résultant de changements importants dans l'infrastructure proposée par le titulaire.

Durant la période de vérification de service régulier qui s'étalera sur **10 jours ouvrés**, le titulaire fournit à l'EFS les moyens nécessaires permettant de mesurer la conformité de la prestation par rapport à ses engagements.

L'EFS s'engage à mettre à la disposition du titulaire, les emplacements suffisants pour recevoir les équipements nécessaires à la mise en œuvre de sa prestation.

Le titulaire prend à sa charge toute adjonction technique aux équipements existants qui s'avérerait nécessaire pour la mise en œuvre de la prestation.

6.4. Dossier des ouvrages exécutés

Avant de procéder à la réception définitive de chaque phase d'installations, le titulaire sera tenu de remettre à l'EFS le dossier des ouvrages exécutés (DOE) en conservant l'historique des prestations préalablement réalisées de façon à assurer une traçabilité des événements techniques (modèle présenté en annexe)

Un exemplaire des DOE sera transmis à l'EFS après chaque mise à jour ; le titulaire en conservera un double pour ses propres besoins.

Une relecture et une mise à jour annuelle est réalisée sur toute la durée du marché. Cette opération est actée par l'évolution de la « version » du document. Ce dossier sera constitué des pièces suivantes :

- les schémas détaillés des installations, intégrant la liste des équipements déployés, leurs notices techniques complètes et détaillées, ... ;
- les plans complets d'implantation des équipements dans les baies informatiques du client avec le repérage des raccordements sur les panneaux RJ45 et avec les références apparaissant sur les plans et les schémas concernés ;
- les manuels et notices d'exploitation des applications déployées ;
- les instructions de mise en service des installations ;
- les documents permettant la maintenance des installations ;
- les notices logicielles, leurs numéros de version, les options implantées, la capacité des verrous logiciels ;
- les listings de programmation sur support informatique ;
- les notices d'exploitation des postes téléphoniques, fournies par le constructeur en langue française. Elles seront remises aux utilisateurs à la mise en service ;
- les fichiers de numérotation comportant le numéro d'annuaire, le point de raccordement côté IPBX, le plan d'adressage IP des équipements ;
- deux (2) jeux de sauvegarde des configurations systèmes installés ;
- un registre d'interventions où seront consignés tous les événements intervenant durant la vie des systèmes de communications et des équipements réseaux.

Cette liste documentaire n'est pas exhaustive, le titulaire établira au plus tard 60 jours après le début du contrat une liste de documents applicables (LDA). Cette LDA devra être complétée lors de la phase de définition d'étude

système et pourra n'être que préliminaire pour les phases de conception détaillées. Elle sera donc remise à jour sur une base régulière.

Le suivi de la production de la documentation sera inclus dans les rapports mensuels d'avancement.

Les plans concernés par cette prestation seront créés et/ou modifiés en format électronique.

Les textes seront fournis au format Word et les tableaux au format **Excel**, **CSV** ou compatibles.

Le titulaire devra mettre à disposition une plateforme de gestion documentaire accessible via navigateur sécurisé (login et mot de passe).

6.5. Démontage et reprise des anciennes installations

Le titulaire assurera le démontage des anciens matériels et, sauf demande explicite de l'EFS, procédera à leur enlèvement (se référer également à la gestion des DEEE décrite ci-dessous)

Le titulaire explicitera dans son offre la méthode qu'il propose pour le retrait et l'enlèvement des anciens matériels.

Cette opération devra être réalisée à l'issue de chacune des phases de déploiement.

7. Gestion des D.E.E.E. et revalorisation

Le titulaire devra répondre aux exigences prévues au CCAP. Le titulaire s'engage notamment à assurer la collecte, le tri, la dépollution, et la valorisation des équipements de télécommunication conformément à la réglementation en vigueur. Il fournira un rapport mensuel détaillant les tonnages traités, les taux de réutilisation et de recyclage, ainsi que les certificats de destruction des données pour les équipements sensibles. Les équipements réutilisables seront prioritairement orientés vers des filières de reconditionnement agréées.

7.1. Contexte et objectifs

- **Cadre réglementaire** : Respect de la directive européenne 2012/19/UE et du Code de l'environnement (articles R. 543-172 à R. 543-206).
- **Objectifs** :
 - Assurer une collecte sélective et traçable des D.E.E.E.
 - Maximiser la réutilisation et le recyclage des matériaux
 - Réduire l'impact environnemental des déchets

7.2. Prestations attendues

7.2.1. Collecte des DEEE

- **Modalités** :
 - Enlèvement sur site
 - Mise à disposition de contenants sécurisés
 - Organisation de tournées régulières ou sur demande pour les sites générant des volumes importants
- **Fréquence** : À définir selon les besoins et à inscrire dans le PAQ.
- **Types de D.E.E.E. concernés** : Équipements informatiques et de télécommunication (catégorie 4)
 - Téléphones fixes
 - Routeurs, modems, switchs, serveurs de téléphonie
 - Câbles et accessoires
 - Équipements de transmission

7.2.2. Réutilisation et reconditionnement

- **Test et reconditionnement** :
 - Vérification de la fonctionnalité des équipements
 - Nettoyage, remise en état, et reconditionnement pour la revente ou le don
- **Effacement des données** :
 - Suppression certifiée des données stockées (normes ISO 27001 ou RNCP pour les éventuelles données sensibles)
 - Fourniture d'un certificat de destruction des données en fonction de la nature des équipements détruits (obligatoire pour équipement de stockage de données).

7.2.3. Recyclage et valorisation

- **Démantèlement** :
 - Séparation des matériaux (métaux précieux, plastiques, verre, etc.)
 - Extraction des composants valorisables (circuits imprimés, métaux rares)
- **Valorisation matière** :
 - Recyclage des métaux (or, argent, cuivre, etc.) via des filières agréées
 - Valorisation des plastiques et autres matériaux
- **Élimination des résidus** :
 - Traitement des fractions non recyclables en filière agréée (incinération avec récupération d'énergie en dernier recours)

7.2.4. Traçabilité et reporting

- **Suivi des flux** :
 - Fourniture de bordereaux de suivi (BSDA pour les DEEE dangereux)
 - Traçabilité des équipements depuis la collecte jusqu'au traitement final

- **Rapports périodiques :**
 - Tonnages collectés et traités par catégorie
 - Taux de réutilisation, recyclage, et valorisation
 - Preuves de conformité réglementaire (attestations de traitement par des centres agréés)

7.2.5. Sensibilisation et formation

- **Actions de sensibilisation :**
 - Campagnes d'information pour les utilisateurs (affiches, guides, webinaires)
 - Formation des agents à la manipulation des équipements (risques électriques, données sensibles)
- **Communication :**
 - Mise à disposition de supports pour informer sur les bonnes pratiques (ex. : où déposer les équipements, pourquoi les recycler)

7.2.6. Exigences spécifiques aux télécommunications

- **Sécurité des données :**
 - Garantie de confidentialité pour les équipements contenant des données (ex. : téléphones, serveurs)
 - Preuve de destruction ou d'effacement sécurisé des données
- **Respect des normes :**
 - Conformité aux normes environnementales (ISO 14001, EMAS)
 - Respect des réglementations sectorielles (ex. : RGPD pour les données, directive D.E.E.E.)

7.2.7. Critères de performance

- **Indicateurs clés :**
 - Taux de réutilisation des équipements (%)
 - Taux de valorisation matière (%)
 - Délai moyen entre la collecte et le traitement
 - Nombre d'incidents (perte, vol, non-conformité)

7.3. Exigences techniques

- **Matériel :**
 - Véhicules adaptés (ex : bennes étanches, compartimentées...)
 - Équipements de protection individuelle (EPI) pour les agents
- **Installations :**
 - Centre de tri agréé et conforme à la réglementation
 - Partenariats avec des éco-organismes agréés

8. Spécification des prestations de pilotage du marché

Ce chapitre décrit les activités de pilotage attendues pendant toute la durée du marché objet du présent CCTP et est complété par une annexe détaillant les spécificités des différents comités.

Les candidats sont réputés avoir pris connaissance des contraintes techniques de tous ordres imposés par l'environnement technique et applicatif existant dans les sites et bâtiments de l'EFS, ainsi que des conditions de réalisation des différentes prestations.

Le pilotage du marché par le Titulaire s'applique transversalement aux différentes activités. Il regroupe les activités liées aux réunions de pilotage et de contrôle.

La direction des systèmes d'information de l'EFS associera le Titulaire aux évolutions du Système d'Information. Ce dernier pourra faire des propositions d'évolution sur les moyens utilisés (suggestions de rationalisation et d'évolution des matériels et logiciels existants).

8.1. Démarche processus

Le Titulaire devra mettre en place une démarche orientée processus pour la délivrance de ses prestations. Cette démarche pourra être de type ITIL V3 voire V4,

Cette approche processus devra permettre :

- ♦ De clarifier les rôles et responsabilités des parties prenantes (interne au Titulaire, équipes de Direction des systèmes d'information et des services généraux, autres Titulaires),
- ♦ D'assurer un vocabulaire, une compréhension et une collaboration efficace des différentes prestations,
- ♦ De disposer d'un niveau de pilotage synthétique et efficace avec la notion d'indicateurs de processus.

Cette approche, par les processus, sera déployée progressivement de manière itérative en accord avec l'EFS. Le détail de ce déploiement sera décrit dans une convention de service.

8.2. Responsable opérationnel de compte

Le Titulaire devra désigner un interlocuteur privilégié appelé Responsable Opérationnel de Compte (ROC) qui sera chargé d'assurer le pilotage de la prestation ainsi que le suivi de la qualité de service associé. Le ROC sera l'interlocuteur privilégié de la direction des systèmes d'information.

8.3. Animation des instances de pilotage.

Le Titulaire devra assurer le pilotage et le contrôle du marché à minima au travers des comités suivants :

- ♦ Réunion d'initialisation du marché (réunion de lancement),
- ♦ Comité Stratégique,
- ♦ Comité de Pilotage,
- ♦ Comité Technique.

D'autres comités pourront être sollicités si besoin.

L'annexe 1 décrit l'ensemble des comités ainsi que les prestations attendues pour chacun d'eux.

Ces différents comités pourront avoir lieu à l'EFS ou en visioconférence (selon les souhaits de l'EFS). Les frais de transport ou de communications sont à la charge du Titulaire.

Le candidat remettra dans son offre un exemple de rapport d'activité et de suivi de pilotage.

9. Garantie et Maintien en Condition Opérationnelle

Compte tenu des enjeux liés au système de communications de l'EFS, le seul choix d'une architecture hautement sécurisée ne peut suffire à répondre à l'ensemble des besoins en termes de disponibilité et de continuité de services.

L'EFS souhaite donc que le Titulaire l'accompagne sur les deux axes suivants :

➤ Le maintien en condition opérationnelle du système de communication

Pour ce faire, le titulaire mettra en place un service guichet unique dès la mise en service définitive permettant la prise en compte des dépannages pour assurer une continuité de service et une gestion optimum des solutions matérielles et logicielles concernant :

- ♦ Le système de communications et ses composants ;
- ♦ Les applications annexes.

➤ Les prestations d'exploitation courante des installations.

Pour ce faire, le titulaire fournira des ressources techniques en ligne ou sur site pour assister l'EFS lors de modifications importantes de configuration ou pour des opérations lourdes de déménagements (par exemple).

Ce service sera fourni à travers une offre de **tickets services** reprenant les différentes opérations pouvant être prises en charge ainsi que le nombre de tickets consommés par intervention.

Pendant toute la durée du marché, le Titulaire s'engage à entretenir et à maintenir en ordre de marche l'ensemble des éléments techniques objet du présent CCTP ainsi qu'à informer l'EFS des cycles de vie des différents équipements fournis (end of life). Ces informations de fin de vie devront être transmises à l'EFS au moins 6 mois avant la date d'échéance, de manière à ce que l'EFS puisse prendre les mesures adéquates (commande matériel, changement de solution, ...).

Le Titulaire fournira également les engagements du constructeur sur la pérennité des systèmes et des applications fournies pour **une durée de 10 ans**.

Le candidat détaillera dans son offre, ses services de maintenance, et en particulier le lieu géographique du Service Après-vente, ainsi que les moyens humains mis à disposition.

9.1. Garantie des matériels et logiciels

A dater de la VSR de chacune des phases de déploiement, les installations complètes (matériels et logiciels) seront entretenues et/ou remplacés par le titulaire dans le cadre des prestations de maintien en condition opérationnelle (MCO) décrites au présent chapitre.

Les garanties du constructeur sur le matériel seront d'une durée de 1 an minimum.

Les garanties des matériels porteront sur :

- ♦ Les applications de communication et leurs composants ;
- ♦ Les passerelles média (Gateway) et leur connectique ;
- ♦ Les serveurs et applications connexes (SVI, Taxation, etc...),
- ♦ Les postes IP ;
- ♦ Les systèmes DECT.

Le Titulaire assurera toutes les réparations de matériel, le remplacement en cas de panne irréversible ainsi que le remplacement provisoire sur un matériel en cours de réparation.

Ces prestations s'effectueront **dans les mêmes conditions et contraintes** que celles exigées au titre de la prestation de « maintien en condition opérationnelle » (MCO).

9.2. MCO - Maintien en Condition Opérationnelle

Le terme général MCO « Maintien en condition opérationnelle » couvrira l'ensemble des prestations « correctives », « préventives », « évolutives » et de « sécurité ».

La MCO garantit le maintien en condition opérationnelle du système de communication dans son intégralité. Elle intègre et s'appuie en termes d'exigences sur une **Garantie de temps de rétablissement (GTR)**.

La responsabilité de la MCO est assurée par le Titulaire avec obligation de résultat : **le niveau de haute disponibilité attendu est de 99,9 %** (8 heures d'interruption par an maximum).

Les prestations de MCO s'appliquent dès la mise en exploitation d'un équipement et de la solution technique liée à son fonctionnement.

A l'issue du déploiement de la dernière phase, le contrat de MCO sera assuré pour une durée d'au moins trois ans.

Au titre de la MCO, le titulaire doit entres-autres corriger toute malfaçon constatée et signalée ; il doit ainsi procéder, dans le cadre du marché :

- ◆ Au démontage, remplacement et installation des matériels, pièces, modules, sous-ensembles, ou éléments constatés défectueux, hormis pour le cas de détériorations consécutives à un non-respect des conditions normales d'utilisation du matériel ;
- ◆ Prendre à sa charge les frais de déplacements, de transports, de démontage, de remontage et de mise au point ;
- ◆ Assurer la mise à jour et/ou à la correction de logiciels ou de programmes remédiant aux défaillances de fonctionnement mis en évidence ;
- ◆ Garantir et s'engager sur des délais de réparation tel que demandé dans les critères de maintien en condition opérationnelle (MCO § 9.4) ;
- ◆ Maintenir le système à niveau technique, en appliquant au fur et à mesure de leur disponibilité les **mise à jour majeures et mineures** de programmes logiciels ;
- ◆ Mettre en place un dispositif de télémaintenance efficace et sécurisé qui permettra de prendre la main sur l'ensemble des systèmes, périphériques compris, pour assurer entre autres la sauvegarde périodique des données ainsi que le chargement de celles-ci, en assurant leur intégrité, en cas de défaillance du système.

Le périmètre du Maintien en condition opérationnelle concerne les équipements et logiciels du système de communication et plus particulièrement les éléments suivants :

9.2.1. Périmètre Matériel

- ◆ Serveurs de communication,
- ◆ Passerelle Média,
- ◆ Serveur et PC d'applications :
- ◆ Systèmes vocaux
- ◆ Systèmes de Taxation
- ◆ Système de management
- ◆ Postes opérateurs, le cas échéant.

9.2.2. Périmètre Logiciel

- ◆ Les systèmes d'exploitation fournis sur les plates-formes matérielles ;
- ◆ Les applications et logiciels :
- ◆ Application de téléphonie
- ◆ Application connexe (SVI...)
- ◆ Application de management.

9.3. Les moyens : Centre support Client

Le Titulaire mettra à disposition de l'EFS un guichet de contact unique permettant l'accès à son **centre support client (Hot Line) 24h/24 et 7j/7**. Ce dernier sera accessible via un numéro unique de téléphone ou par mail ou à travers un service WEB.

9.3.1. Déclaration des pannes et dysfonctionnements

Le guichet unique devra pouvoir prendre en compte tous les appels de type opérationnel passés par les entités techniques de l'EFS (DSI) et/ou par les responsables sur chaque site distant de l'EFS (expert télécom.).

Le candidat fournira dans son offre une description des processus/procédures de prise en charge et d'escalade ainsi que l'organisation autour de ce centre d'appel.

9.3.2. Gestion des incidents par le Titulaire

Les appels au support technique du Titulaire génèrent systématiquement l'ouverture d'un ticket. Le candidat décrira dans son offre l'ensemble des moyens qu'il mettra à disposition de l'EFS pour le suivi de résolution des tickets.

Un incident a pour définition « Tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service. »

Sans que la liste ne soit exhaustive, les incidents peuvent être d'origine :

- ♦ applicative : application non disponible, lenteurs ;
- ♦ matérielle : système HS, saturé, instable, perte d'énergie.

Dans le cadre du marché, le Titulaire assurera la gestion des incidents par la remise en service des applications et services, dans les délais les plus courts, en minimisant l'impact sur les utilisateurs.

Le cycle de vie de l'incident et les étapes de la Gestion des incidents sont les suivants :

- ♦ Détection et enregistrement ;
- ♦ Classification et support initial ;
- ♦ Investigation ;
- ♦ Résolution ;
- ♦ Clôture.

9.4. Critères de MCO – Plages horaires et délais associés

Le titulaire devra assurer les services de MCO dans les conditions décrites aux chapitres suivants. Chaque intervention sur site fera l'objet d'un rapport consigné dans un registre d'intervention, dont un exemplaire sera remis à l'EFS.

Toute demande de services sera suivie et tracée dans une base de données du Titulaire. Ces données pourront être consultables dans un extranet.

Les tableaux ci-dessous défini les plages horaires et les critères de MCO attendus :

Désignation	Plage d'intervention
Période HO (heures ouvrées)	Du lundi au vendredi en jours ouvrés ; De 8h00 à 18h00
Période HNO (heures non ouvrées)	Jours non-ouvrés de 8h00 à 18h00 Toutes les nuits de 18h à 8h00

Par définition, la couverture **24/7** correspond au cumul des couvertures en HO et HNO sur la période donnée.

Le prestataire s'engagera sur des délais de GTR minimale selon 3 seuils d'urgence :

Qualification incident	Degré d'urgence	Plage horaire	Contraintes de GTR
Bloquant	Critique	24/7	4h après déclaration (*)
Non Bloquant	Urgent	HO	de 4h à 8h après déclaration (*)
Mineur	Peu urgent	HO	24h après début intervention

Nota (*) : niveau de GTR par équipement précisé au BPU.

La qualification de la panne et donc de l'urgence sera actée de fait selon le descriptif suivant :

- **Incident bloquant** : concerne un incident généralisé pour lequel il n'existe aucune solution palliative ou de contournement
 - Panne globale du système de communication (hors problèmes opérateurs, courants forts, réseau LAN), générant une indisponibilité totale du service ou limitée à un ou plusieurs sites ;
 - Pannes répétitives, non forcément bloquantes par rapport aux critères ci-dessous mais qui ont fait l'objet de plusieurs signalements et corrections non stables avec persistance et/ou réapparition trois fois ou plus sur une période d'un mois ;
 - Dégradation des performances (saturation du système de communications, temps de réponse, etc.) entraînant une impossibilité de communication vers certains services ;
 - Faille de sécurité.
- **Incident non-bloquant** : Tout dysfonctionnement ne relevant pas d'un incident bloquant :
 - Une fonction essentielle de l'exploitation est défaillante mais reste limitée en termes de propagation ;
 - Sauvegarde des équipements impossible ;
 - Qualité des communications dégradée.
- **Incident mineur** : Toute demande ne relevant pas d'un dysfonctionnement décrit ci-avant.

9.4.1. Prestations correctives

Les prestations de MCO correctives s'appliquent à toutes les installations et périphériques que le Titulaire aura mis en place dans le cadre du marché et ont pour objectif de répondre à un dysfonctionnement éventuel, perturbant ou empêchant l'usage partiel ou total des systèmes.

Les composants défectueux sont remplacés par du matériel neuf, identique ou au moins équivalent.

En cas de problème d'approvisionnement ou de cessation de fabrication, un modèle équivalent sera présenté à l'EFS. Les éventuelles adaptations de mise en œuvre restent à la charge du Titulaire.

Les opérations de maintenance corrective pourront être traitées exceptionnellement par télémaintenance pour les problèmes mineurs ou pouvant être corrigés de cette manière.

Le recours à la télémaintenance pour diagnostic pourra être la première opération menée avant le déplacement d'un technicien. Si les opérations par télémaintenance ne s'avèrent pas efficaces, un technicien devra être dépêché sur place sous contrainte de respect des engagements de GTR.

Les prestations de MCO se prolongeront sans interruption jusqu'à résolution complète de l'incident et le retour au service normal sans qu'un second ticket ne soit ouvert.

Le Titulaire s'engage à remplacer ou à modifier tout élément technique, objet du présent CCTP et sous sa responsabilité, pour assurer la continuité de service.

Détail des prestations en HO

Les opérations correctives en HO peuvent être consécutives à :

- Une visite périodique préventive ;
- Un appel sur dysfonctionnement, émanant des moyens généraux ;
- Une évolution permettant de corriger et/ou améliorer un Process ou une fonctionnalité.

Dans le cadre des interventions en **HO**, celles sur site ou à distance sont à inclure dans la prestation globale de MCO et à assurer sans limitation de nombre ou de durée pour maintenir l'installation en bon état de fonctionnement. Il en est de même pour le remplacement ou la réparation de toutes pièces composant le matériel.

Si lors de ses investigations, le Titulaire est amené à mettre en cause des organes non couverts par le contrat de maintenance établi entre l'EFS et lui, il devra tout de même en faire le diagnostic et prendre toutes dispositions pour informer la direction des systèmes d'information de l'EFS.

Détail des prestations en HNO

Les prestations de MCO correctives en **HNO** ont pour objectif de répondre à **une panne bloquante** empêchant l'usage partiel ou total des systèmes. Elles pourront être traitées exceptionnellement par télémaintenance.

Dans le cadre des interventions en **HNO**, celles sur site ou à distance sont à inclure dans la prestation à travers l'utilisation d'un système prédéfini en nombre de tickets.

Un certain nombre de tickets « Astreinte », acquis sur la base des tarifs précisés au BPU, sera affecté aux prestations en **HNO**.

Périmètre des prestations réalisables en HO et HNO

Périmètre concerné	Prise en compte en HO	Prise en compte en HNO
L'ensemble des équipements du système de communication	Oui	Oui
Le signalement après vérification des pannes d'accès opérateurs	Oui	Oui
La participation aux tests avec les opérateurs lors d'un constat de défaut ;	Oui	Non
La participation aux tests avec les intégrateurs du système d'information de l'EFS	Oui	Non
La remise en route des équipements du système de communication ayant fait l'objet d'interventions	Oui	Oui
Le remplacement et la réinstallation des pièces défectueuses	Oui	Oui
L'intervention sur site : la main d'œuvre, les déplacements	Oui	Oui
La télé interventions	Oui	Oui

9.4.2. Prestations correctives sur Logiciel

La maintenance logicielle corrective concerne les parties logicielles. Un logiciel présentant des dysfonctionnements sera modifié par correctif logiciel ou par implémentation d'une version complète et stable du logiciel.

Dans le cas où ces corrections demandent une ou plusieurs migrations ou évolutions matérielles d'un des éléments constituant le système de communication, celles-ci devront être incluses.

Le Titulaire s'engage à appliquer uniquement des correctifs garantis par l'éditeur du logiciel.

Les prestations portent sur :

- ♦ La mise en place des correctifs logiciels sur l'ensembles des applications constituant la solution de communication ;
- ♦ La mise à niveau des équipements nécessaires au support des correctifs logiciels ;
- ♦ La reprogrammation des équipements dans leurs configurations avant les dysfonctionnements ;
- ♦ Les participations aux tests ;
- ♦ Les interventions sur site et les télé interventions ;
- ♦ La main d'œuvre et les déplacements ;

9.4.3. Prestations préventives

Détail des prestations

Les visites préventives ont pour objectif de vérifier, en dehors de toutes pannes, que les équipements ne présentent pas de risque de dysfonctionnement lié à une surcharge d'exploitation ou une mauvaise utilisation.

Elles devront également permettre de porter à la connaissance de l'EFS toutes les évolutions logicielles proposées par le constructeur et/ou l'éditeur.

Le Titulaire consigne dans un rapport l'exécution et les résultats des actions et opérations de maintenance préventive. Le document « rapport de maintenance préventive » sera remis et visé systématiquement par le responsable du marché (ou son représentant). Il sera communiqué à l'EFS cinq (5) jours ouvrés après la fin de la dernière action réalisée dans le cadre de cette maintenance.

Les tâches sur lesquelles porteront les actions de maintenance préventive sont, entre autres :

- ♦ Contrôle visuel des éléments constituant le local technique : le câblage des éléments, les diverses connexions et raccordements, l'état des différents coffrets ou baies et l'état général du local technique (température, poussière, hydrométrie) ;
- ♦ Vérification des éventuels dépannages et réparations effectués depuis la dernière visite préventive ;
- ♦ Test du plan de reprise d'activité (PRA) :
 - Test de redondance des équipements à travers les situations suivantes : coupure d'un lien WAN, arrêt de serveur principal, isolement d'un accès opérateur ;
 - Test de restauration des données.

- Test et contrôle des dispositifs de report d'alarme ;
- Vérification et mise à jour de la base documentaire ;
- Contrôle de bon fonctionnement des systèmes de communication : Il s'agit du contrôle de l'intégrité des systèmes à travers la vérification des indicateurs d'incidents systèmes, vérification des faisceaux opérateurs, contrôle de l'organe de télémaintenance ;
- Test de fonctionnement de systèmes périphériques : SVI, outil de gestion...
- Tenue à jour de la documentation ;
- Contrôle de fonctionnement des sauvegardes automatiques ; réalisation d'une sauvegarde de toutes les données sur un support magnétique ou optique.

La consignation des actions d'entretien préventif, les essais réalisés et les anomalies constatées seront portés sur un « rapport de maintenance préventive ». Pour chaque résultat d'essai non conforme aux normes définies pour chaque équipement, il sera mentionné par écrit quelle a été l'action apportée ou quelle est celle à prévoir si cette dernière devait générer une indisponibilité.

Périodicité des interventions

La périodicité de la visite préventive est annuelle. Elle se déroule sur la base d'un planning validé par l'EFS. La première visite préventive sera réalisée à la fin de la première année d'exploitation des solutions techniques mise en œuvre par le Titulaire dans le cadre du déploiement de la nouvelle solution.

9.4.4. Prestations évolutives ou mise à niveau technique

Le Titulaire informera l'EFS des éventuels changements de normes par les opérateurs et/ou constructeurs ou de réglementation en vigueur, ainsi que des incidences techniques et financières sur les installations en place. La direction des systèmes d'information de l'EFS avisera alors des suites à donner.

Le Titulaire est réputé être au fait des modifications apportées par le constructeur et/ou l'éditeur, pour des raisons d'amélioration et de fiabilité, à un organe ou groupe d'organes reconnus défectueux.

Dans tous les cas, **le titulaire devra intégrer** dans son offre de MCO, les **mise à jour majeures** de l'application de communication de façon à maintenir la solution dans la dernière version validée par l'éditeur.

Ces mises à jour devront faire l'objet de tests de non-régression en version plateforme avant d'effectuer le changement sur le système actif.

9.4.5. Sauvegardes

Le Titulaire assurera une sauvegarde quotidienne des données de configuration des systèmes, incluant l'ensemble des composants et périphériques.

D'autres sauvegardes seront effectuées systématiquement :

- à chaque visite de maintenance préventive ;
- à chaque intervention ayant un impact sur le contenu des données internes aux systèmes ;
- à chaque demande du service informatique.

Ces sauvegardes sont indépendantes de celles qui sont effectuées dans le cas de son exploitation courante.

Le support contenant la sauvegarde sera stocké dans un lieu indiqué par l'EFS ; le support sera étiqueté avec la date de sauvegarde et un descriptif du contenu. La gestion des sauvegardes en termes de suivi et de rotation des versions est à la charge du titulaire. Les opérations de sauvegarde font partie de l'exploitation régulière. Le niveau de sauvegarde minimale demandé est :

Données à sauvegarder	Fréquence recommandée	Mode de sauvegarde
Configuration du système IPBX (numéros, plans, règles, utilisateurs)	Quotidienne (au minimum)	Sauvegarde automatisée, versionnée, externalisée
Enregistrements des appels (logs de traçabilité)	Quotidienne	Archivage sécurisé (audit & conformité)
Messages de messagerie vocale	Quotidienne	Sauvegarde incrémentale / redondance système
Bases de données utilisateurs et profils	Quotidienne	Backup complet avec rotation
Paramètres de sécurité (certificats, clés)	Après chaque modification	Export sécurisé
Journaux système (logs d'administration)	Quotidienne	Archivage sécurisé

9.4.1. RTO

Dans le cadre de la solution de téléphonie d'entreprise (hébergée sur serveurs en datacenter ou en mode hybride), nous fixons un RTO (Recovery Time Objective) maximal de 4 heures.

Cela signifie qu'en cas d'incident majeur affectant la plateforme (panne matérielle, coupure réseau, défaillance applicative), le service de téléphonie doit être rétabli et pleinement opérationnel en moins de 4 heures.

Cet engagement garantit la continuité des communications essentielles pour l'activité, limite l'impact sur les équipes support et les utilisateurs finaux, et répond aux exigences de disponibilité d'un service critique comme la téléphonie.

Le respect de ce RTO implique des mécanismes de redondance, des plans de reprise documentés et des processus de supervision proactifs pour détecter et corriger rapidement toute anomalie. Le soumissionnaire détaillera sa capacité, à remonter partiellement ou totale les services de téléphonie.

9.4.2. Limites de prestations

Les prestations forfaitaires et le périmètre inclus

Le Titulaire interviendra sur l'ensemble des installations et éléments techniques objet du présent CCTP.

Le Titulaire est responsable des liaisons vers l'extérieur des sites jusqu'aux têtes de câbles appartenant aux Opérateurs de téléphonie.

Toutefois, le Titulaire ne saurait être tenu pour responsable des dérangements affectant ces lignes à l'extérieur de l'installation et dont la remise en service incombe à un opérateur. Il interviendra sur les lieux de l'installation et assurera la coordination avec les représentants des Opérateurs en vue de procéder à un dépannage complet.

Le Titulaire interviendra sur l'affectation, l'installation, le raccordement, le remplacement, le paramétrage de l'ensemble des composants techniques objet du présent CCTP

Si la panne constatée ne peut être réparée sur site et nécessite le recours à la garantie, le Titulaire procède au remplacement de l'équipement en panne en utilisant le matériel de maintenance mis à sa disposition par l'EFS. Le matériel défectueux est alors renvoyé à ses frais par le Titulaire en utilisant ses moyens logistiques. Cette prestation est comprise dans la part forfaitaire.

Les prestations et périmètres exclus

Sont exclus du périmètre de maintenance :

- ◆ Les faisceaux vers les opérateurs de la téléphonie (T2, T0 ou Trunk SIP) ;
- ◆ Le câblage inter sites et entre locaux techniques (Cuivre – FO) ;
- ◆ La fourniture et installation des baies informatiques et réseaux en dehors de celles fournies dans le cadre du marché ;
- ◆ Les alimentations électriques ;
- ◆ Les anciens PABX, leurs licences, les postes téléphoniques raccordés aux anciens PABX (le cas échéant).

Toute autre prestation non détaillée dans le présent CCTP doit être inscrite dans le PAQ.

10. Réversibilité et transfert des acquis en début et en fin de marché

10.1. Généralités

En complément du transfert de compétences qui se déroulent à chaque fin de réalisations, cette prestation a pour but d'organiser en fin de marché un transfert de connaissance du titulaire aux personnels désignés par l'EFS ou tout autre tiers désigné par celui-ci.

Le titulaire assure, sur demande de l'EFS et sur un temps imparti, une totale réversibilité de l'ensemble des prestations de maintenance de l'application ou du groupe d'applications concerné aux équipes de l'EFS ou à celles proposées par lui (autre prestataire). Il s'interdit de faire obstacle à cette décision et s'engage à apporter toute l'assistance nécessaire à la bonne fin de cette opération.

Cette prestation de réversibilité comprend à minima les activités suivantes :

L'organisation de sessions de travail sur les domaines suivants :

- ◆ L'architecture applicative ;
- ◆ L'architecture technique ;
- ◆ L'ensemble des outils développés autour de l'application ;
- ◆ La description de l'organisation de la documentation de référence ;
- ◆ L'assistance technique pendant une période permettant la prise en charge de la maintenance applicative et matériel par l'EFS ou par une personne désignée.

On distinguera :

- Réversibilité entrante (initialisation)

Le titulaire devra reprendre l'historique auprès des prestataires et des équipes présentes au démarrage de la prestation :

- ◆ Prise de connaissance de la documentation
- ◆ Montée en compétence suffisante pour la compréhension du contexte et des enjeux de l'EFS sur sa stratégie et ses usages digitaux ainsi que ses pratiques des outils du présent marché
- ◆ Reprise éventuelle des outils / Rites et Rythmes pour le pilotage des projets et prestations
- ◆ Rétro- engineering le cas échéant pour les parties les moins documentées
- ◆ Durée réversibilité à déterminer conjointement entre le titulaire sortant et l'EFS

- Réversibilité sortante

La mise en place d'une réversibilité sortante devra être réalisée avec les prestations suivantes :

- ◆ Accompagnement de la montée en compétence des personnes entrantes sur les outils et l'organisation mise en place pour la gestion de ces derniers,
- ◆ Livraison d'une documentation à jour
- ◆ Prise de connaissance par le titulaire entrant de la documentation et des contacts en place chez le titulaire sortant pour la gestion des prestations et des projets liés aux outils
- ◆ Accompagnement de la montée en compétence des personnes entrantes sur les activités et les projets liés aux outils
- ◆ Accompagnement de la montée en compétence des personnes entrantes sur les éventuels Rites et Rythmes pour le pilotage des projets et des prestations
- ◆ La durée de réversibilité est à déterminer conjointement entre le titulaire sortant et l'EFS

N.B : La réversibilité sortante pourra être prolongée au-delà de l'échéance du marché et tant que de besoin dans le respect du CCAP.

10.2. Modalités de déclenchement

Cette prestation n'est pas déclenchée par l'émission d'un bon de commande auprès du titulaire.

10.3. Modalités d'exécution

Le transfert de connaissance se déroule dans les locaux de l'EFS ou par session distante avec accord de l'EFS.

La méthodologie d'exécution proposée par le titulaire dans son plan de transfert devra être acceptée et validée par l'EFS.

Deux mois minimum avant la fin du marché l'EFS informera le titulaire de sa volonté d'organiser le transfert de connaissance ; le titulaire disposera d'un délai de 14 jours ouvrés pour proposer la méthodologie d'exécution de la prestation de transfert. Le plan de transfert fera l'objet d'un accord sous 14 jours ouvrés par l'EFS.

Pendant toute la période de réversibilité, les niveaux de services exigés dans le CCTP, PAQ, SLA, restent opposables au titulaire.

10.4. Délais de réalisation

La prestation de réversibilité doit être réalisée dans le délai convenu entre l'EFS et le titulaire.

Les dispositions du présent CCTP survivront au terme ou à la résiliation de ce dernier pour les besoins, le cas échéant de la finalisation des opérations de réversibilité.

10.5. Livrables

Le plan de transfert présentant la méthodologie de transfert de connaissance (Thèmes abordés, Planning, livrables...)

Bilan de fin de marché est un document qui permet de s'assurer de la réalisation de toutes les actions et décisions issues de différentes demandes, commandes et réunions prévues dans ce marché. Il marque la fin du marché.

11. Exigences SSI

11.1. Glossaire

AES	<i>Advanced Encryption Standard</i>
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
APSAD	Assemblée Plénière des Sociétés d'Assurance Dommage
EFS	Etablissement Français du Sang
IA	Intelligence Artificielle
PAS	Plan d'Assurance Sécurité
PCA	Plan de Continuité d'Activité
Prescripteur	Client Interne de l'EFS
RGS	Référentiel Général de Sécurité
RGPD	Le règlement général sur la protection des données
RNSSI	Responsable National de la Sécurité des Systèmes d'Information
SAAS	<i>Software as a service</i> ¹ (Logiciel en tant que service)
SI	Systèmes d'Information

11.2. Introduction

L'Etablissement Français du Sang (EFS), est conscient de sa mission en tant qu'opérateur unique de la transfusion sanguine en France mais aussi de son obligation de protéger les données personnelles de ses donneurs, les receveurs et de son personnel.

A ce titre, l'EFS doit assurer la continuité de la transfusion sanguine en France et se doit de vérifier que les activités confiées à des tiers partenaires ou à des sous-traitants se déroulent dans le respect des conditions de disponibilité, intégrité et confidentialité, fiabilité et authentification imposées par les obligations légales de son activité dépendante de son système d'information.

Le présent document comporte les exigences de Sécurité des Systèmes d'Information de l'EFS applicables aux prestations prévues au marché. Les volets relatifs à la sécurité organisationnelle, la sécurité physique des locaux, la sécurité informatique, les exigences SaaS, la télémaintenance, la relations avec les tiers et le plan de continuité d'activité y sont présentés.

Les candidats sont invités à prendre connaissance des mesures de sécurité indiquées et à y apporter une réponse dans le cadre de réponse relatif aux exigences SSI annexée au présent document (Matrice de conformité). Cette réponse fera l'objet d'une analyse afin de déterminer la conformité ou non du candidat à chacune des exigences et sera notée sur la base du critère prévu au règlement de la consultation.

Le candidat doit garder à l'esprit que la non-conformité n'est pas un blocage pour devenir le titulaire et participer à cette consultation. Le titulaire aura le temps nécessaire pour attendre la conformité et sera guidé, en cas de besoin pour l'atteindre.

Le tableau ci-dessous doit vous guider pour la réponse aux exigences en vous précisant le résultat recherché sur chaque grand domaine des exigences.

¹ Ce service concerne la mise à disposition par le candidat d'applications hébergées sur une plateforme partagée. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente. Le candidat gère de façon transparente pour le commanditaire l'ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d'effectuer quelques paramétrages métier dans l'application

DOMAINE	OBJECTIF/RESULTAT RECHERCHE
Sécurité Organisationnelle	Réponse obligatoire pour tout type de prestation. L'objectif est de savoir comment la sécurité est intégrée à votre organisation et fonctionne dans votre entreprise. De plus, l'EFS souhaite avoir une idée représentative des moyens mis en œuvre.
Sécurité Informatique	Réponse obligatoire pour les prestations de développement informatique, exploitation de service ou toute autre prestation nécessitant une connexion au système d'information de l'EFS. Ces exigences doivent être intégrées dès les premières étapes de la conception et développement et être appliquées tout au long du cycle de vie des systèmes pour garantir une sécurité robuste et durable face aux menaces en constante évolution. Les exigences de ce domaine sont valables dans le cas d'une prestation de développement pour le produit livré dans le cadre de cette prestation.
Relations avec les tiers	Obligation de réponse dans le cadre d'intervention de tout sous-traitant. Ce dernier doit appliquer et respecter nos exigences de sécurité des systèmes d'information.
Plan de Continuité d'Activité	Obligation de réponse pour toute prestation d'exploitation et/ou de service.
Plan d'Assurance Sécurité	Obligation de réponse uniquement si le candidat devient le Candidat du service

En réponse à nos exigences il est impératif de :

- Les intégrer dans la conception et/ou réalisation des produits ou prestations ;
- Remplir la matrice de conformité jointe en annexe des exigences.

Pour toute question complémentaire, nous restons à votre entière disposition selon les conditions indiquées dans les prestations prévues au marché.

NB : Les exigences ci-après doivent être complétées en fonction de l'option retenue :

- Hébergement dans les datacenters de l'EFS, remplir la partie « *Mesures socle à remplir indépendamment de l'option retenue* »
- Hébergement dans les datacenters du Titulaire, remplir les deux parties « *Mesures socle à remplir indépendamment de l'option retenue* » et « *Mesures à remplir si hébergement dans les datacenters du Titulaire* »

----- Mesures socle à remplir indépendamment de l'option retenue -----

11.3. Sécurité organisationnelle

SECORG1 : Le candidat doit présenter une politique de sécurité formalisée dont le périmètre couvre les risques de continuité de service et de malveillance auxquels il est exposé au titre de la prestation.

SECORG2 : L'organisation du candidat doit comprendre au moins un responsable sécurité pour l'ensemble des domaines concourant au bon déroulement de la prestation.

SECORG3 : Les moyens mis à disposition des responsables sécurité doivent leur permettre de faire appliquer la politique de sécurité.

SECORG4 : Tout collaborateur du candidat participant à l'activité de l'EFS doit respecter les procédures et les règles de sécurité applicables dans le cadre de la réalisation de la prestation.

SECORG5 : Tout collaborateur du candidat participant à l'activité de l'EFS doit avoir signé un engagement personnel de confidentialité dans le cadre de son contrat de travail.

SECORG6 : Le candidat doit documenter et mettre en œuvre une organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l'information au sein de son organisation.

SECORG7 : Le candidat doit sensibiliser à la sécurité de l'information et aux risques liés à la protection des données l'ensemble des personnes impliquées dans la fourniture du service.

SECORG8 : Le candidat doit obligatoirement faire appliquer les exigences de sécurité à l'ensemble des sous-traitants participant à la délivrance du service.

SECORG9 : Le candidat doit documenter et mettre en œuvre un plan de formation concernant la sécurité de l'information adapté au service et aux missions des personnels. Le responsable de la sécurité des systèmes d'information du prestataire doit valider formellement le plan de formation concernant la sécurité de l'information

11.4. Sécurité informatique

11.4.1. Spécificités pour le développement informatique

SECDEV-GESTIDEN1 : Pour la gestion des identités et des accès, le candidat doit s'assurer que seules les bonnes personnes peuvent accéder au système et aux données.

SECDEV-GESTIDEN2 : Pour la gestion des identités il doit aussi mettre en place une authentification forte et gérer les permissions d'accès aux systèmes.

SECDEV-AUTHENCENTRALE : le candidat doit utiliser des technologies standardisées comme LDAP, OAuth ou SSO pour gérer l'accès à plusieurs systèmes de manière cohérente et sécurisée et assurer une authentification centralisée

SECDEV-CHIFFREDATA1 : Pour le chiffrement des données, le candidat doit rendre les données illisibles pour toute personne non autorisée. Il doit également utiliser des mécanismes de chiffrement pour les données en transit et au repos ; ainsi que protéger les données envoyées sur Internet avec des connexions sécurisées.

SECDEV-CHIFFREDATA2 : Dans la suite du chiffrement des données, le candidat doit ainsi stocker les informations sensibles sous forme chiffrée.

SECDEV-JOURNAUX : Pour les journaux et suivi des activités, le candidat doit Implémenter des journaux d'audit pour détecter et analyser les changements non autorisés. Ainsi, il doit garder la trace des actions importantes pour détecter les problèmes ou abus afin de pouvoir obtenir les informations sur les actions sensibles telles que ;

- Les connexions ;
- Les modifications de données ;
- Les erreurs ou les comportements inhabituels ;
- Voir les modifications ou la suppression des journaux.

SECDEV- PROTECAPPLI1 : Concernant la sécurisation de l'application, le candidat doit s'assurer que le système fonctionne comme prévu, sans permettre de mauvaises utilisations. Il doit aussi s'assurer qu'un utilisateur malveillant n'envoie pas des informations dangereuses.

SECDEV- PROTECAPPLI2 : Le candidat doit donner par ailleurs un minimum d'autorisations aux composants du système pour limiter les dégâts en cas de problème et surtout effectuer une séparation des environnements de test et de production.

SECDEV-PROTECDATASEN : Pour la protection des données sensibles, le candidat doit limiter l'accès aux données de ce type uniquement aux personnes qui en ont besoin. Il doit dans la mesure du possible anonymiser les données sensibles.

SECDEV-SECUAPPLI : Pour la protection des applications contre les vulnérabilités et attaques courantes, le candidat, doit effectuer des tests d'intrusion réguliers et des analyses statiques ou dynamiques du code pour identifier et corriger les failles.

SECDEV-SECURISE : Pour le développement sécurisé, le candidat doit suivre les bonnes pratiques reconnues, comme les recommandations OWASP, pour prévenir les vulnérabilités des telles que les injections SQL ou les scripts intersites (XSS).

SECDEV-VALIDDATA ; Le candidat doit valider les données. Il doit contrôler systématiquement toutes les données saisies par les utilisateurs pour éviter les attaques par injection.

SECDEV-MOINDREPRIV : Principes de moindre privilège. Le candidat doit limiter les droits d'accès au strict nécessaire pour chaque utilisateur ou processus.

SECDEV-BIBLIOEXT : Pour les dépendances et bibliothèques externes, le candidat doit s'assurer que les outils ou morceaux de code utilisés sont sûrs. Il doit maintenir les bibliothèques et frameworks à jour pour éviter les vulnérabilités connues.

SECDEV-SECUSRVRS : Quant à la sécurisation des serveurs et réseaux, le candidat doit protéger les machines qui hébergent le système et les connexions entre elles ainsi que limiter les connexions non autorisées

SECDEV-REAINCIDENTS : Pour la réaction aux incidents de sécurité, le candidat doit être en mesure de détecter et répondre rapidement en cas d'attaque ou de problème (panne importante ou piratage). Il doit prévoir des mécanismes de sauvegarde et de redondance. Et finalement mettre en œuvre des solutions contre les attaques par déni de service (DDoS).

SECDEV-VERSIONNING : Le candidat doit effectuer le contrôle des versions. Il doit mettre en œuvre des systèmes de versionnage permettant de suivre et restaurer les versions antérieures des fichiers ou des applications en cas de corruption.

SECDEV-REGLESNORMES : Concernant le respect des règles et normes, le candidat doit s'assurer que le système respecte les lois et bonnes pratiques (suivi des réglementations et méthodes de travail).

SECDEV-ANACODE : Pour l'analyse de code, le candidat doit effectuer des tests de sécurité pendant le cycle de développement (ex. : SAST, DAST).

SECDEV MAJ DEPEND : Pour la mise à jour des dépendances, le candidat doit maintenir les bibliothèques et Framework à jour pour éviter les vulnérabilités connues.

SECDEV-TESTAUDITS : Pour les tests et audits réguliers, le candidat doit effectuer des tests de pénétration : et simuler des attaques pour identifier les failles.

SECDEV-AUDITCONFO : le candidat doit dans les aspects d'audits de conformité, de vérifier régulièrement que le SI respecte les politiques de sécurité définies par son entité

SECDEV-CRYPTO : Le candidat doit utiliser des protocoles sécurisés pour les communications réseaux TLS/SSL.

SECDEV-GESCLES : Le candidat doit, dans la cadre de la gestion des clés, mettre en place une infrastructure de gestion des clés (KMS).

SECDEV-FORMSENS : Le candidat doit assurer la formation des développeurs aux pratiques de codage sécurisé incluant les risques liés au code source généré par l'IA. Il doit aussi faire en sorte que tout le monde dans son équipe comprenne l'importance de la sécurité.

SECDEV-ANALYSE : Le candidat doit faire effectuer des tests d'intrusion réguliers et des analyses statiques ou dynamiques du code pour identifier et corriger les failles.

SECDEV-SVGDHSITE : Sauvegardes hors site : Le candidat doit réaliser des copies régulières des données sur des sites géographiquement éloignés pour limiter les pertes.

SECDEV-IA1 : Le candidat doit systématiquement contrôler le code source généré par IA (interdiction d'exécution, de *commit* automatiques de code source généré par IA, innocuité des bibliothèques, contrôles réguliers par un humain).

SECDEV-IA2 : Le candidat s'engage à ne pas utiliser l'IA pour générer du code source pour des modules critiques de système d'information – comme par exemple : modules de cryptographie (authentification, chiffrement, signature, etc.), de gestion des droits d'accès (utilisateurs et administrateurs), de traitement des données confidentielles.

11.5. Maintenance

Dans le cadre du maintien de la sécurité de son système d'information, l'EFS exige le respect des règles ci-dessous dans le cadre des différentes opérations de maintenances.

11.5.1. Généralités

MAINTEN1 : Si le candidat propose un système de supervision destiné au maintien en condition opérationnelle et de sécurité du système d'information, il devra en décrire précisément les catégories de données transférées. La protection de ces dernières devra être encadrée.

MAINTEN2 : L'EFS interdit strictement toute récupération de Données à Caractère Personnel (DCP²) ou données de santé.

MAINTEN3 : Les données techniques (configuration des équipements) de l'EFS exploitées par les équipes de support chez le candidat doivent être protégées et ne doivent pas être divulguées.

MAINTEN4 : Le candidat indiquera dans sa réponse où (pays, région, type d'hébergement) sont hébergées les données prélevées. Le candidat indiquera par ailleurs obligatoirement les certifications et habilitations de sécurité dont lui ou ses sous-traitants sont candidats.

MAINTEN5 : Au niveau des postes de travail standard de l'EFS, aucun outil de prise de contrôle à distance ne peut être installé ou exécuté. Le seul outil de prise de contrôle à distance autorisé est celui de l'EFS.

MAINTEN6 : Il est de la responsabilité du candidat d'assurer la sécurité de sa plateforme d'intervention à distance (locaux, matériels, données, logiciels, habilitations), notamment mise à jour des correctifs de sécurité et dispositif de protection contre les codes malveillants.

MAINTEN7 : Il est de la responsabilité du candidat de connaître en toutes circonstances les actions et l'identité de toute personne qui se connecte ou s'est connectée sur le SI de l'EFS et d'en assurer la traçabilité. Cette traçabilité devra être communiquée sur demande de l'EFS.

MAINTEN8 : Il est de la responsabilité du candidat de veiller à ce que toutes les informations résiduelles inutiles à l'issue d'une intervention soient supprimées en application du principe de minimisation des données.

MAINTEN9 : Le candidat réalise un suivi permanent des incidents et vulnérabilités liés aux dispositifs fournis et met à disposition les correctifs et préventifs nécessaires dans les délais appropriés.

MAINTEN10 : Le candidat s'engage à effectuer des tests de robustesse et de non-régression à chaque évolution du matériel ou du logiciel. Les impacts d'une défaillance qui serait néanmoins constatée seraient de la responsabilité du candidat, la correction et la prise en charge des impacts à sa charge. Les résultats des tests pourront être communiquées sur demande à l'EFS.

MAINTEN11 : Toute clé USB destinée à être connectée sur un équipement doit préalablement subir un contrôle antivirus réalisé par un agent de l'EFS

MAINTEN12 : Le titulaire doit informer la RNSSI de l'EFS de tout incident de sécurité concernant ses dispositifs connectés ou son SI pouvant impacter son matériel, le service ou les données de l'EFS. Le candidat s'engage à mobiliser les ressources nécessaires pour assurer le traitement de l'incident de sécurité sur les dispositifs déployés dans l'EFS. Si l'incident concerne un traitement relatif au RGPD, les dispositions relatives au traitement des incidents s'appliqueront aussi.

11.5.2. Télémaintenance

TELEMAIN1 : Les accès en télémaintenance sont autorisés uniquement via les systèmes (réseau, VPN, prise en main à distance, etc...) validés par l'EFS.

TELEMAIN2 : La connexion de télémaintenance du candidat doit se faire via un serveur sécurisée mise à disposition par l'EFS conformément à sa politique de sécurité.

TELEMAIN3 : Tout accès fera l'objet d'une demande d'approbation au moment de la connexion par le tiers.

TELEMAIN4 : Tout accès sera tracé (horodatage de la connexion et des actions réalisées par le tiers).

² Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Il peut s'agir d'un nom, d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'une empreinte, d'un enregistrement vocal, d'un numéro de sécurité sociale, d'un mail, etc.

TELEMAIN5 : Selon les besoins d'intervention l'accès aux systèmes à maintenir ou exploiter sera ouvert et fermé par l'établissement l'EFS à la demande (du mainteneur ou de la personne habilitée selon le protocole défini dans les conditions de la maintenance).

TELEMAIN6 : Le formulaire d'habilitation transmis par l'EFS devra être dûment complété par le tiers avant la création d'un accès en télémaintenance.

TELEMAIN7 : Tout compte d'accès doit être nominatif et fera l'objet d'une fiche d'habilitation individuelle.

TELEMAIN8 : Le tiers s'engage à informer sans délai l'EFS en cas mouvement de personnel.

TELEMAIN9 : Lors de sa création, la date de validité d'un accès sera égale à la date de fin du contrat. A défaut, la durée sera positionnée à un (1) an.

TELEMAIN10 : Le tiers devra procéder à une revue d'habilitation annuelle des comptes actifs

TELEMAIN11 : L'EFS se réserve le droit de couper, sans préavis, son accès internet en cas de force majeure.

TELEMAIN12 : Tout accès à distance devra se solder par un compte-rendu d'intervention qui sera transmis par messagerie électronique sous 8 heures au demandeur à l'origine de la demande d'intervention.

TELEMAIN13 : L'accès distant ne sera permis que depuis des plages d'adresses IP déclarées par le télémainteneur.

11.6. Relations avec les tiers

RELSTIERS1 : Le candidat doit tenir à disposition du commanditaire la liste de l'ensemble des tiers qui peuvent accéder aux données et l'informer de tout changement de sous-traitants au sens de l'article 28 du [RGPD] afin que le commanditaire puisse émettre des objections à cet égard.

RELSTIERS2 : Le candidat doit exiger des tiers participant à la mise en œuvre du service, dans leur contribution au service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il doit le faire au travers d'exigences, adaptées à chaque tiers et à sa contribution au service, dans les cahiers des charges ou dans les clauses de sécurité des accords de partenariat. Le candidat doit inclure ces exigences dans les contrats conclus avec les tiers.

RELSTIERS3 : Le candidat doit contractualiser, avec chacun des tiers participant à la mise en œuvre du service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences du présent document.

RELSTIERS4 : Le candidat doit définir et attribuer les rôles et les responsabilités relatives à la modification ou à la fin du contrat le liant à un tiers participant à la mise en œuvre du service.

RELSTIERS5 : Le candidat doit documenter et mettre en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service pour respecter les exigences de ce recueil d'exigences.

RELSTIERS6 : Le candidat doit documenter et mettre en œuvre une procédure permettant de réviser au moins annuellement les exigences en matière d'engagements de confidentialité ou de non-divulgaration vis-à-vis des tiers participant à la mise en œuvre du service.

11.7. Fin du contrat

FINCONTR1 : À la fin du contrat liant le candidat et le commanditaire, que le contrat soit arrivé à son terme ou pour toute autre cause, le candidat doit assurer un effacement sécurisé de l'intégralité des données du commanditaire. Cet effacement peut être réalisé suivant l'une des méthodes suivantes, et ce dans un délai précisé dans le contrat :

- effacement par réécriture complète de tout support ayant hébergé ces données ;
- effacement des clés utilisées pour le chiffrement des espaces de stockage du commanditaire ;
- recyclage sécurisé, dans les conditions énoncées dans l'exigence FINCONTR 3.

FINCONTR2 : À la fin du contrat, le candidat doit supprimer les données techniques relatives au commanditaire (annuaire, certificats, configuration des accès, etc.)

FINCONTR3 : Le candidat doit documenter et mettre en œuvre des moyens permettant d'effacer de manière sécurisée par réécriture de motifs aléatoires tout support de données mis à disposition d'un commanditaire. Si l'espace de stockage est chiffré, l'effacement peut être réalisé par un effacement sécurisé de la clé de chiffrement.

FINCONTR4 : La suppression des données ne pourra être réalisée qu'une fois la réversibilité finalisée et un procès-verbal signé par le client.

11.8. Plan de Continuité d'Activité (PCA)

PCA1 : Un plan de continuité d'activité, formalisé et testé doit permettre de prévenir ou de subvenir à toute panne grave ou à tout sinistre impactant les obligations définies dans le Contrat.

Ce plan de continuité assure à minima la sauvegarde régulière des informations et applications.

11.9. Plan d'Assurance Sécurité (PAS)

PASSEC1 : Une fois la fin de la consultation et le choix d'un candidat, ce dernier produira un plan d'assurance sécurité avec les exigences de sécurité indiquées dans ce document, en fonction de sa prestation.

Le PAS doit décrire les mesures de sécurité de l'EFS et mises en œuvre ainsi que leurs modalités d'application, sans que cette description ne puisse en aucun cas limiter l'obligation de résultat souscrite par le candidat de respecter le niveau minimal de sécurité.

PASSEC2 : Le PAS sera appliqué et tenu à jour par le candidat.

PASSEC3 : Un tableau de bord indiquant l'état de la conformité des exigences de sécurité doit être fourni par le candidat à une fréquence définie en commun accord entre le RSSI du candidat et la RNSSI de l'EFS. Si des écarts sont constatés, le candidat devra indiquer un plan d'action afin que l'exigence soit couverte. Des réunions de suivi devront être planifiées pour démontrer la couverture de l'exigence.

----- Mesures à remplir si hébergement dans les datacenters du Titulaire -----

11.10. Sécurité physique des locaux

Mise en garde : si vous faites appel à un prestataire d'hébergement pour votre solution, les réponses à ces exigences doivent être les siennes. Vous devez obtenir une réponse de sa part

A contrario, si vous hébergez votre solution dans votre propre Datacenter, c'est à vous qu'incombe la réponse à ces exigences.

11.10.1. Exposition aux risques

SECPHY-ER1 : L'implantation géographique des locaux ne doit pas être exposée à des risques naturels ni à des risques sociaux ou industriels. Toutefois, si les locaux sont implantés dans une zone présentant des risques, le candidat devra décliner la manière dont ces risques sont pris en compte pour assurer la continuité de service.

11.10.2. Référentiels applicables

SECPHY-RA1 : En complément des dispositions législatives et réglementaires en vigueur, toutes les installations concourant à la sécurité physique des locaux doivent respecter les règles françaises APSAD (Assemblée Plénière des Sociétés d'Assurance Dommage).

11.10.3. Protection contre l'intrusion

SECPHY-PL1 : Les locaux du candidat doivent être équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements doivent être opérationnels 24h/24h et 7j/7j.

Les moyens de protection doivent être adaptés aux moyens de détection et de réaction.

SECPHY-PL2 : Les accès physiques doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du candidat.

SECPHY-PL3 : Le système de vidéosurveillance, s'il existe, doit être configuré de manière à permettre l'exploitation des enregistrements quelles que soient les conditions d'éclairage. Les images doivent être d'une qualité suffisante pour permettre de reconnaître les personnes quelles que soient les conditions.

SECPHY-PL4 : Le candidat doit assurer la traçabilité des incidents de sécurité.

11.10.4. Télésurveillance

SECPHY-TSV1 : Si la surveillance des locaux est confiée à une société de télésurveillance, ses délais d'intervention sur site ne doivent pas dépasser 20 minutes. Les alarmes qui lui sont transmises doivent être différenciées en fonction des événements, au minimum :

- Incendie ;
- Intrusion ;
- Dégâts des eaux si détection de liquides ;
- Autres alarmes critiques de gestion technique centralisée du bâtiment.

11.10.5. Sécurité incendie

SECPHY-SI1 : Les installations de protection incendie doivent respecter les dispositions législatives et réglementaires et être conformes aux règles APSAD³.

SECPHY-SI2 : Les locaux doivent être protégés contre les effets directs et indirects de la foudre.

SECPHY-SI3 : Les travaux sur points chauds (soudure, meulage, ...) doivent donner lieu à la rédaction d'un permis de feu et faire l'objet d'une vigilance particulière.

SECPHY-SI4 : L'accès aux extincteurs doit être dégagé en permanence. Une signalétique appropriée doit permettre de les localiser.

SECPHY-SI5 : Le candidat veille à éliminer quotidiennement tout potentiel calorifique inutile de ses locaux (emballages, palettes, déchets de toute nature). Les conteneurs de déchets (bennes) et les stocks de palettes doivent être disposés à une distance minimale de 10 mètres des locaux.

11.10.6. Protection contre les dégâts des eaux

SECPHY-PGE1 : Le cheminement des canalisations doit se faire hors des locaux sensibles.

SECPHY-PGE2 : Les zones à caractère stratégique doivent être équipées d'un système de détection

SECPHY-PGE3 : Les canalisations apparentes doivent être protégées contre les chocs.

SECPHY-PGE4 : Les installations de plomberie doivent faire l'objet d'un contrat de maintenance.

SECPHY-PGE5 : Les gouttières, avaloirs, exutoires d'eau pluviale, etc. doivent être curés au minimum une fois par an, de préférence en fin d'automne pour éliminer les feuilles mortes.

11.10.7. Maintien en conditions opérationnelles des équipements de sécurité

SECPHY-MCO1 : L'infrastructure technique des bâtiments (distribution d'énergie et de fluides, climatisation des locaux) doit être redondante.

SECPHY-MCO2 : Les équipements de sécurité (incendie, intrusion, surveillance vidéo, ...) doivent disposer d'une alimentation électrique de secours d'une autonomie minimale de 4 heures.

SECPHY-MCO3 : L'ensemble des équipements qui concourent à la sécurité et à la continuité des opérations doit faire l'objet d'un contrat de maintenance préventive et doit satisfaire aux visites périodiques de contrôle telles que prévues dans les règles APSAD et dans la réglementation française.

SECPHY-MCO4 : En particulier, les installations électriques doivent faire l'objet d'un contrôle annuel renforcé par thermographie infrarouge.

³ Assemblée Plénière de Sociétés d'Assurances Dommages

SECPHY-MCO5 : Le candidat tient à jour un registre de sécurité regroupant les certificats de conformité, les procès-verbaux de visites réglementaires et le compte rendu des actions correctives réalisées, sur lequel doivent figurer l'identité des personnes les ayant réalisées et à quelle date.

11.11. Fourniture de service SaaS⁴ (Software as a Service)

11.11.1. Généralités

Le prestataire mettra en œuvre les mesures de sécurité suivantes :

SAAS-GEN1 : Le prestataire doit faire signer la charte informatique à l'ensemble des personnes impliquées dans la fourniture du service.

SAAS-GEN2 : Dans la mesure où un projet affecte ou est susceptible d'affecter le niveau de sécurité du service, le prestataire doit avertir le commanditaire et l'informer par écrit des impacts potentiels, des mesures mises en place pour réduire ces impacts ainsi que des risques résiduels le concernant

SAAS-GEN3 : Le prestataire doit, sur demande d'un commanditaire, lui rendre accessible le règlement intérieur et la charte d'éthique. Le commanditaire doit la rendre accessible ensuite à la RNSSI de l'EFS

11.11.2. Gestion des actifs

SAAS-GESACT1 : Lorsque le commanditaire confie au prestataire des données soumises à des contraintes légales ou réglementaires, le prestataire doit identifier les besoins de sécurité spécifiques associés à ces contraintes.

SAAS-GESACT2 : Il est recommandé que le prestataire documente et mette en œuvre une procédure pour le marquage et la manipulation de toutes les informations participant à la délivrance du service, conformément à son besoin de sécurité défini à l'exigence précédente.

SAAS-GESACT3 : Lorsque des supports amovibles sont utilisés sur l'infrastructure technique ou pour des tâches d'administration, ces supports doivent être dédiés à un usage.

11.11.3. Contrôle d'accès et gestion des identités

SAAS-CTLACC1 : Le candidat doit réviser annuellement la politique de contrôle d'accès et à chaque changement majeur pouvant avoir un impact sur le service.

SAAS-CTLACC2 : Le candidat doit documenter et mettre en œuvre une procédure d'enregistrement et de désinscription des utilisateurs s'appuyant sur une interface de gestion des comptes et des droits d'accès. Cette procédure doit indiquer quelles données doivent être supprimées au départ d'un utilisateur.

SAAS-CTLACC3 : Le candidat doit documenter et mettre en œuvre une procédure permettant d'assurer l'attribution, la modification et le retrait de droits d'accès aux ressources du système d'information du service.

SAAS-CTLACC4 : Le candidat doit tenir à jour l'inventaire des utilisateurs sous sa responsabilité disposant de droits d'administration sur les ressources du système d'information du service.

SAAS-CTLACC5 ; Le candidat doit être en mesure de fournir, pour une ressource donnée mettant en œuvre le service, la liste de tous les utilisateurs y ayant accès, qu'ils soient sous la responsabilité du candidat ou du commanditaire ainsi que les droits d'accès qui leur ont été attribués.

SAAS-CTLACC6 : Le candidat doit être en mesure de fournir, pour un utilisateur donné, qu'ils soient sous la responsabilité du candidat ou du commanditaire, la liste de tous ses droits d'accès sur les différents éléments du système d'information du service.

SAAS-CTLACC7 : Le candidat doit proposer au commanditaire des moyens d'authentification à multiples facteurs pour l'accès des utilisateurs finaux.

⁴ Ce service concerne la mise à disposition par le candidat d'applications hébergées sur une plateforme partagée. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente. Le candidat gère de façon transparente pour le commanditaire l'ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d'effectuer quelques paramétrages métier dans l'application

SAAS-CTLACC8 : Lorsque des comptes techniques, non nominatifs, sont nécessaires, le candidat doit mettre en place des mesures obligeant les utilisateurs à s'authentifier avec leur compte nominatif avant de pouvoir accéder à ces comptes techniques.

SAAS-CTLACC9 : Les comptes d'administration sous la responsabilité du candidat doivent être gérés à l'aide d'outils et d'annuaires distincts de ceux utilisés pour la gestion des comptes utilisateurs placés sous la responsabilité du commanditaire.

SAAS-CTLACC10 : Les interfaces d'administration utilisées par le candidat ne doivent pas être accessibles à partir d'un réseau public et ainsi ne doivent permettre aucune connexion des utilisateurs sous la responsabilité du commanditaire.

SAAS-CTLACC11 : Si des interfaces d'administration sont mises à disposition du commanditaire avec un accès via un réseau public, les flux d'administration doivent être authentifiés et chiffrés avec des moyens en accord avec les exigences du chapitre Cryptologie.

SAAS-CTLACC12 : Le candidat doit mettre en place un système d'authentification à double facteur pour l'accès : aux interfaces d'administration utilisées par le candidat et aux interfaces d'administration dédiées aux commanditaires.

SAAS-CTLACC13 : Les interfaces d'administration mises à disposition des commanditaires doivent être différenciées des interfaces permettant l'accès des utilisateurs finaux.

SAAS-CTLACC14 : Le candidat doit mettre en œuvre des mesures de cloisonnement appropriées entre ses commanditaires.

SAAS-CTLACC15 : Le candidat doit mettre en œuvre des mesures de cloisonnement appropriées entre le système d'information du service et ses autres systèmes d'information (bureautique, informatique de gestion, gestion technique du bâtiment, contrôle d'accès physique, etc.).

SAAS-CTLACC16 : Le candidat doit concevoir, développer, configurer et déployer le système d'information du service en assurant au moins un cloisonnement entre d'une part l'infrastructure technique et d'autre part les équipements nécessaires à l'administration des services et des ressources qu'elle héberge.

11.11.4. Cryptologie

Mise en garde ; pour les exigences SAAS-CRYPTO3, SAAS-CRYPTO4 et SAAS-CRYPTO5, vous devez répondre uniquement aux protocoles que vous utilisez. Pour les restantes indiquer dans la colonne Observations « NON CONCERNE »

SAAS-CRYPTO1 : Le candidat doit définir et mettre en œuvre un mécanisme de chiffrement empêchant la récupération des données du commanditaire en cas de réallocation d'une ressource ou de récupération du support physique. Cet objectif pourra être atteint en utilisant un chiffrement applicatif dans le périmètre du candidat, avec au moins une clé par commanditaire.

SAAS-CRYPTO2 : Le candidat doit utiliser une méthode de chiffrement des données respectant les règles et recommandations de l'ANSSI concernant le choix et le dimensionnement des mécanismes cryptographiques, version en vigueur.

SAAS-CRYPTO3 : Si le protocole *Transport Layer Security* (TLS) est mis en œuvre, le candidat doit appliquer les recommandations de l'ANSSI relatives à TLS, note technique n° SDE-NT-35/ANSSI/SDE/NP du 19 août 2016.

SAAS-CRYPTO4 : Si le protocole IPsec est mis en œuvre, le candidat doit appliquer les recommandations de l'ANSSI relatives à IPsec, note technique n° DAT-NT003/ANSSI/SDE/NP du 3 août 2015.

SAAS-CRYPTO5 : Si le protocole SSH est mis en œuvre, le candidat doit appliquer les recommandations de l'ANSSI : relatives à un usage sécurisé d'(Open)SSH, note technique n° DAT-NT-007/ANSSI/SDE/NP du 17 août 2015.

SAAS-CRYPTO6 : Le candidat doit mettre en place un chiffrement des données sur les supports amovibles et les supports de sauvegarde amenés à quitter le périmètre de sécurité physique du système d'information du service, en fonction du besoin de sécurité des données (voir exigence SAAS-ACT1 et SAAS-ACT2.).

11.11.5. Sécurité de l'exploitation

SAAS-SECEXPLOIT1 : Le candidat doit informer au plus tôt le commanditaire de toute modification à venir sur les éléments du service dès lors qu'elle est susceptible d'occasionner une perte de fonctionnalité pour le commanditaire.

SAAS-SECEXPLOIT2 : Le candidat doit documenter et mettre en œuvre les mesures de détection, de prévention et de restauration pour se protéger des codes malveillants. Le périmètre d'application de cette exigence sur le système d'information du service doit nécessairement contenir les postes utilisateurs sous la responsabilité du candidat et les flux entrants sur ce même système d'information.

SAAS-SECEXPLOIT3 : Le candidat doit documenter et mettre en œuvre une sensibilisation de ses employés aux risques liés aux codes malveillants et aux bonnes pratiques pour réduire l'impact d'une infection.

SAAS-SECEXPLOIT4 : Le candidat doit documenter et mettre en œuvre une politique de journalisation incluant au minimum les éléments suivants :

- la liste des sources de collecte ;
- la liste des événements à journaliser par source ;
- la fréquence de la collecte et base de temps utilisée ;
- la durée de rétention locale et centralisée ;
- les mesures de protection des journaux (dont chiffrement et duplication) ;
- la localisation des journaux.

SAAS-SECEXPLOIT5 : Le candidat doit générer et collecter les événements suivants : les activités des utilisateurs liées à la sécurité de l'information, la modification des droits d'accès dans le périmètre de sa responsabilité, les événements issus des mécanismes de lutte contre les codes malveillants, les exceptions, les défaillances et tout autre événement lié à la sécurité de l'information.

SAAS-SECEXPLOIT6 : Le candidat doit conserver les événements issus de la journalisation pendant une durée minimale de six mois sous réserve du respect des exigences légales et réglementaires.

SAAS-SECEXPLOIT7 : Le candidat doit fournir, sur demande d'un commanditaire, l'ensemble des événements le concernant.

SAAS-SECEXPLOIT8 : Le candidat doit protéger les équipements de journalisation et les événements journalisés contre les atteintes à leur disponibilité, intégrité ou confidentialité.

SAAS-SECEXPLOIT9 : Le candidat doit mettre en place une sauvegarde des événements collectés suivant une politique adaptée.

SAAS-SECEXPLOIT10 : Le candidat doit exécuter les processus de journalisation et de collecte des événements avec des comptes disposant de privilèges nécessaires et suffisants. Il doit limiter l'accès aux événements journalisés conformément à la politique de contrôle d'accès.

11.11.6. Incidents de sécurité des systèmes d'information

SAAS-INCSSI : Le Candidat doit assurer la traçabilité des incidents de sécurité des systèmes d'information et prévenir le RNSSI de l'EFS. Si un incident survient, cela implique un écart avec une ou plusieurs exigences de sécurité des systèmes d'information. Un rapport précis devra être produit et indiquer les actions à mettre œuvre pour remettre à niveau la ou les exigences et cela en commun accord entre le RSSI du Candidat et la RNSSI de l'EFS.

11.11.7. Localisation des données

SAAS-LOC DATA1 : Le candidat doit documenter et communiquer au commanditaire la localisation du stockage et du traitement des données.

SAAS-LOC DATA2 : Le candidat doit stocker et traiter les données du commanditaire au sein la France ou l'Union Européenne.

SAAS-LOC DATA3 : Les opérations d'administration et de supervision du service doivent être réalisées depuis la France ou l'Union Européenne.

11.12. Audits de sécurité

AUDSEC1 : L'EFS se réserve la possibilité de réaliser des audits de sécurité destinés à vérifier le respect par le candidat de son obligation de respecter le niveau de sécurité exigé par l'EFS et notamment de la bonne application du plan d'assurance sécurité. Le candidat sera prévenu de l'occurrence d'un audit au moins 5 jours ouvrés avant sa réalisation.

AUDSEC2 : Un plan d'actions doit être soumis par le candidat à l'EFS pour approbation du RNSSI au plus tard 15 jours après la livraison du rapport.

AUDSEC3 : Les écarts constatés avec le plan d'assurance sécurité et, plus généralement, tout non-respect du niveau de sécurité de l'EFS devra être régularisés dans un délai convenu en commun accord entre les deux parties.

AUDSEC4 : l'EFS se réserve le droit d'accès à l'ensemble des documents relatifs à la sécurité du candidat dans le cadre de sa prestation.

AUDSEC5 : Les écarts importants constatés avec le plan d'assurance sécurité et, plus généralement, ou non-respect du niveau de sécurité demandé par l'EFS peuvent être une cause de rupture de contrat dans les conditions prévues dans le DCE.

AUDSEC6 : Afin de vérifier le respect des engagements définis dans le contrat, l'EFS peut procéder ou faire procéder à des audits et des contrôles des procédures mises en œuvre par le candidat.

AUDSEC7 : Les vulnérabilités identifiées lors de tests de sécurité devront être comblées par des mesures appropriées sur la base d'un plan d'actions validé par l'EFS (notamment le RNSSI) et le PAS sera mis à jour en conséquence

12. Annexes

- Annexe 1 : Comitologie
- Annexe 2 : Inventaire détaillé
- Annexe 3 : Matrice de conformité SSI
- Annexe 4 : Inventaire des systèmes existants