fObjet	DECLARATION DE PRATIQUE GENERALE 1.3.6.1.4.1.62714.41.11.1.1

Version *	Date	Modifications	Rédacteur
0.1	04/09/25	Création du document	GBA
1.0	03/03/2025	Finalisation de la version initiale	GBA

* *<Version>.<Edition>* *Changement de version = évolution majeure* *Changement d'édition = évolution mineure*

Durée de validité	*Nbre de versions à conserver*
1 an	Minimum 2 (actuelle + précédente)

Niveau de diffusion	*Liste de diffusion si Restreint ou Confidentiel*
Public	

	Fonction	Date & Signature
Vérificateur 1	DSSC GBA	Signature manuscrite – version officielle conservée
Vérificateur 2	Responsable d'AC SPA	Signature manuscrite – version officielle conservée
Approbateur	Administrateur Délégué LCA	Signature manuscrite – version officielle conservée

Sommaire

1. Introduction

1.1. Présentation générale

BE YS TRUSTED SOLUTIONS LUXEMBOURG, ci-après le Prestataire, s'est positionnée comme prestataire de service de confiance à destination de ses clients et partenaires, en offrant des services supports à la confiance numérique, de manière à leur permettre généralement de sécuriser l'ensemble de leurs échanges.

Le Prestataire a défini cette Déclaration de Pratique générale afin de mutualiser et simplifier le suivi du respect de la norme ETSI EN 319 401 pour chacun de ses Services de Confiance.

1.2. Objet du document

La présente Déclaration des Pratiques Générale (DPG) a pour objet de décrire l'ensemble des pratiques, procédures et mesures mises en œuvre par le Prestataire afin d'assurer la conformité de son organisation, de ses systèmes et de ses activités aux exigences de la norme ETSI EN 319 401 – "General Policy Requirements for Trust Service Providers".

Ce document établit le cadre de sécurité, d'organisation et de gouvernance applicable à l'ensemble des services de confiance exploités par le Prestataire.

Il définit les principes communs relatifs à :

- la gestion de la sécurité de l'information et des actifs critiques ;
- la fiabilité de l'organisation et la séparation des rôles et responsabilités ;
- la sécurité des systèmes et des opérations ;
- la gestion du personnel, des fournisseurs et de la chaîne d'approvisionnement ;
- la conformité aux exigences légales, normatives et contractuelles applicables.

Cette DPC Générale constitue une référence commune pour les différentes Déclarations de Pratiques de Certification spécifiques à chaque service de confiance (ex. service de signature électronique, de cachet électronique, d'authentification, d'horodatage, d'archivage ou d'émission de certificats).

Chaque DPC spécifique peut (sans obligation) ainsi s'y référer pour les éléments transverses de sécurité et de gouvernance, et préciser les pratiques opérationnelles propres au service concerné.

La DPC Générale s'inscrit dans le système de management de la sécurité du Prestataire et s'articule avec :

- la Politique applicable à chaque Service de Confiance;
- les procédures internes de sécurité et d'exploitation ;
- les référentiels normatifs ETSI EN 319 401.

L'objectif de cette DPC Générale est de démontrer que le Prestataire met en œuvre des mesures techniques, organisationnelles et procédurales cohérentes et proportionnées, garantissant la confiance, la conformité et la continuité de ses services de confiance qualifiés ou non qualifiés.

1.3. Périmètre d'application

La présente Déclaration des Pratiques Générale (DPG) s'applique à l'ensemble des activités, systèmes, ressources et personnels impliqués dans la fourniture des services de confiance opérés par le Prestataire, qu'ils soient qualifiés ou non qualifiés au sens du règlement (UE) n°910/2014 (eIDAS).

Elle ne s'applique que si le Service de Confiance concerné fait référence à cette DPG dans sa politique ou sa déclaration de pratiques.

Elle couvre les dispositions organisationnelles, techniques et procédurales communes à tous les services de confiance, et notamment :

- la gouvernance et la structure organisationnelle du Prestataire ;
- la gestion de la sécurité physique, logique et opérationnelle des systèmes ;
- la gestion des accès, des identités et des rôles de confiance ;
- la gestion des risques, des incidents et de la continuité d'activité ;
- la gestion du cycle de vie des clés et dispositifs cryptographiques ;
- la protection des informations, des actifs et des données à caractère personnel ;
- la gestion des relations avec les fournisseurs et sous-traitants ;
- la conformité aux exigences légales, réglementaires et normatives applicables.

Cette DPG constitue le socle de conformité aux exigences de la norme ETSI EN 319 401, et fournit le cadre de référence pour toutes les DPC spécifiques associées à chaque service de confiance exploité par le Prestataire, notamment :

- La DPC du Service de Signature à distance

Les DPC spécifiques décrivent les modalités particulières de mise en œuvre et les processus propres à chaque service, tandis que la présente DP Générale définit les principes transverses de sécurité, d'organisation et de conformité applicables à l'ensemble du périmètre.

1.4. Références réglementaires et légales

Renvoi	Document
[RGPD]	Règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[EIDAS]	Règlement européen eIDAS

1.5. Références normatives

Renvoi	Document	Version
[319401]	ETSI EN 319 401 : Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers	3.1.1

1.6. Définitions, acronymes et abréviations

1.6.1. Définitions

Terme	Définition

Autorité de Gouvernance (AG) ***[Governance Authority (GA)]***	Entité responsable de l'ensemble des fonctions de l'IGC avec pouvoir décisionnaire
Cérémonie des Clés ou Key Ceremony (KC)	Réunion spéciale des personnes autorisées pour générer le Certificat d'une AC ou d'un Client (KC Client). La Bi-clé de ce Certificat doit être générée avec toutes les précautions nécessaires (voir la DPC) pour éviter sa compromission
Chiffrement ***[Encryption]***	Transformation cryptographique d'un ensemble de données (clair) en vue de produire un ensemble chiffré (dit cryptogramme)
Client	Entité cliente ayant décidé de souscrire au Service du Prestataire, qu'elle utilise pour ses propres besoins ou qu'elle met à disposition des Utilisateurs.
Composante du Service de Confiance	Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction du Service de Confiance
Confidentialité ***[Confidentiality]***	Propriété d'une *information* ou d'une *ressource* de n'être accessible qu'aux utilisateurs autorisés (création, diffusion, sauvegarde, archivage, destruction)
Déchiffrement ***[Decryption]***	Transformation d'un cryptogramme en vue de retrouver les données originelles en clair
Déclaration des Pratiques de Certification (DPC) ***[Certification Pratice Statement (CPS)]***	Document qui identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les PC qu'elle s'est engagée à respecter
Horodatage ***[Time-stamping]***	Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé
Infrastructure de Gestion de Clés (IGC) ***[Public Key Infrastructure (PKI)]***	Ensemble de composants, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs Certificats utilisés par des services de confiance. Une IGC peut être composée d'une AC, d'un OC, d'une AE centralisée et/ou locale, de MC, d'une entité d'archivage, d'une entité de publication
Intégrité ***[Integrity]***	Propriété d'exactitude, de complétude et d'inaltérabilité dans le temps des *informations* et des *fonctions* de l'information traitée
Module cryptographique matériel ***[Hardware Cryptographic Module (HSM)]***	Matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clés cryptographiques
Non-répudiation ***[Non-repudiation]***	Impossibilité pour un Porteur, un Utilisateur ou une Application utilisatrice de nier sa participation à un échange d'information ; cette participation porte tant sur l'origine de l'*information* (*imputabilité*) que sur son contenu (*intégrité*)
Politique de Certification (PC) ***[Certification Policy (CP)]***	Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une Autorité de Certification se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et

	exigences portant sur les autres intervenants, notamment les Porteurs et les Applications utilisatrices de certificats
Produit de sécurité	Dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité
Promoteur d'application	Fournisseur d'une offre de service sécurisé (échanges dématérialisés)
Service de Confiance	Service fournit par le Prestataire définit dans le règlement européen eIDAS [EIDAS]
Service du Prestataire	Un des services de la gamme d'offres de services de dématérialisation et de confiance du groupe du Prestaire, déployé en tout ou partie
Uniform Resource Locator (URL)	Adresse d'un site internet
Utilisateur	Voir « Application utilisatrice »

1.6.2. Acronymes et Abréviations

Acronyme FR	Acronyme EN	Définition
AC	**CA**	**Autorité de Certification [Certification Authority]**
AG	GA	Autorité de Gouvernance [Governance Authority]
CC	CC	Critères Communs [Common Criteria]
CEN		**Comité Européen de Normalisation**
CSP		Cryptographic Service Provider
DN		**Distinguished Name**
DPC	CPS	Déclaration des Pratiques de Certification [Certification Practice Statement]
EAL		**Evaluation Assurance Level**
ETSI		European Telecommunications Standards Institute
HSM		**Hardware Security Module**
KC		**Cérémonie des clés [Key Ceremony]**
OID		**Object Identifier**
PC	CP	Politique de Certification [Certification Policy]
PP	PP	Profil de Protection [Protection Profile]
RSA		Rivest Shamir Adelman
SSI		**Sécurité des Systèmes d'Information**
URL		Uniform Resource Locator

1.7. Identification du document

La présente déclaration de pratique est nommée « Déclaration des Pratiques de Certification Communes aux Services du Prestataire de Service de Confiance BYLUTS».

Elle repose sur la norme « Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers» [319401].

L'OID de ce document est 1.3.6.1.4.1.62714.41.11.1.1

Le préfixe d'OID de ce document répond aux principes de nommage suivant :

Iso(1).member-body(3).beystslu(6.1.4.1. 62714).igc(41).common(11).ps(1). version(1)

Le terme *ps* est utilisé pour Practice Statement, Déclaration de pratique en français.

2. Contexte organisationnel

2.1. Présentation du Services de Confiance

Pour chaque Service de Confiance référençant cette DPG, le prestataire présentera dans la Politique ou dans la Déclaration de Pratique le Service de Confiance ainsi qu'une vision générale de l'organisation en ayant la charge.

2.2. Rôles et responsabilités

Pour chaque Service de Confiance référençant cette DPG, le prestataire présentera dans la Politique ou dans la Déclaration de Pratique :

- Les entités chargées de la mise à disposition des informations publiques concernant le service (Politique, Conditions Générales d'Utilisation, …)
- La liste des informations devant être publiées
- Les délais et fréquence de publication

L'ensemble des informations publiées est du niveau de confidentialité « Public ».

La fonction de publication assure à tout moment l'intégrité des informations qu'elles publient.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées du Prestataire et aux personnes dûment autorisées après authentification par un moyen d'authentification forte.

2.3. Relations avec les parties externes (utilisateurs, parties de confiance, autorités de supervision)

Pour chaque Service de Confiance référençant cette DPG, le prestataire présentera dans la Politique ou dans la Déclaration de Pratique les relations avec les différentes parties prenantes, à savoir, entre autres :

- Utilisateurs
- Tiers de confiance,
- Autorités de Contrôle
- Autorités de Supervision

2.4. Responsabilités légales et contractuelles

Pour chaque Service de Confiance référençant cette DPG, le prestataire présentera dans la Politique ou dans la Déclaration de Pratique ses responsabilités légales et contractuelles.

2.4.1. Confidentialité des données professionnelles

Périmètre des informations confidentielles

La classification des informations se décompose en :

- Secret (niveau 4 de la Politique de Sécurité) ;
- Confidentiel (niveau 3 de la Politique de Sécurité) ;
- Interne (niveau 2 de la Politique de Sécurité).

Chaque déclaration de pratique définit ses informations et leur classification

Les informations considérées comme « confidentielles » sont au moins les suivantes :

- La DPC privée du service ;
- Les journaux d'événements des composantes ;

Informations hors du périmètre des informations confidentielles

Par défaut, en complément des informations déjà explicitement listées dans cette section, une information est considérée comme confidentielle.

Responsabilités en termes de protection des informations confidentielles

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire du grand-duché du Luxembourg. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des Porteurs à des tiers dans le cadre de procédures légales.

2.4.2. Protection des données à caractère personnel

Politique de protection des données à caractère personnel

Toute collecte et tout traitement de données à caractère personnel par le Prestataire sont réalisés dans le strict respect de la réglementation en vigueur, et en particulier le règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit « Règlement Général sur la Protection des Données [RGPD] ».

Informations à caractère personnel

Chaque service définit la liste complète des informations personnelles qu'il traite.

Elles sont traitées dans le strict respect de la réglementation en vigueur relative au [RGPD].

Responsabilité en termes de protection des données à caractère personnel

Le traitement des données à caractère personnel est sous la responsabilité du président de l'entité traitant les données. Pour la conformité au [RGPD], le Prestataire a mis en place une organisation centrée sur le Délégué à la Protection des Données DPO.

Notification et consentement d'utilisation des données à caractère personnel

Conformément à la législation et réglementation en vigueur sur le territoire du grand-duché du Luxembourg, les informations à caractère personnel remises par les Utilisateurs au Prestataire ne sont ni divulguées ni transférées

à un tiers, sauf dans les cas suivants : consentement préalable de la personne concernée, décision judiciaire ou autre autorisation légale.

Conditions de divulgation d'informations à caractère personnel aux autorités judiciaires ou administratives

Toute diffusion et communication des données à caractère personnel vers des tiers autorisés doivent être en conformité aux lois spécifiques y afférant.

Il n'y a pas d'autres circonstances de divulgation d'informations personnelles

2.4.3. Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par le Prestataire sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de non-respect. Par exemple, conformément au droit applicable les bases de données réalisées par les composantes des services sont protégées.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages web, bases de données, textes originaux, …) est sanctionnée conformément aux dispositions des lois Luxembourgeoises.

2.5. Tarifs et aspect financiers

Les informations suivantes sont fournies dans les différents documents contractuels établis entre les parties : (i.e. Prestataire, les Clients du service, et éventuellement les fournisseurs assurant en tout ou partie certaines fonctions du service) :

- Les conditions de facturation du Service proposé par le Prestataire ;
- Les responsabilités ;
- Les responsabilités financières ;
- Le montant des indemnités.

2.6. Dispositions concernant la résolution de conflits

Chaque service définit un point de contact (mail ou autres) afin de permettre toute demande d'information ou réclamation.

En cas de litige sur l'interprétation du contenu ou l'exécution de la présente DPC, une résolution amiable des conflits est privilégiée.

2.7. Juridictions compétentes

Le droit applicable à tout litige relatif à l'interprétation et l'exécution de la présente DPC est le droit du Luxembourg.

2.8. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 1.4. Le Prestataire se conforme à la législation et aux réglementations en vigueur et conserve les éléments de preuve de cette conformité. En particulier, chaque fois que cela est possible, le Prestataire :

- Met en place des moyens pour faciliter l'accès de ses services aux personnes en situation de handicap ;
- Traite les données personnelles en conformité avec la Réglementation en vigueur.

3. Politiques de certification

3.1. Références aux politiques de certification applicables

Ce document ne référence aucune politique, il rassemble les pratiques de certification communes à différents services du Prestataire.

Ce document peut être référencé dans les déclarations de pratiques de service de confiance du Prestataire. Ces déclarations de pratique référencent les politiques auxquelles elles sont rattachées.

3.2. Typologie de services couverts

Les services couverts peuvent être les suivants :

- Emission de certificats dans le cadre du règlement européen eIDAS
- Emission de contremarque de temps
- Fourniture d'un service de signature électronique à distance.

4. Gestion et exploitation du service

Le Prestataire met en œuvre une organisation fiable, disposant des structures, des ressources et des procédures nécessaires pour assurer la fourniture continue, sécurisée et conforme de ses services de confiance, conformément aux exigences de la Politique de Certification et aux référentiels applicables.

4.1. Organisation Interne

4.1.1. Non-discrimination et accessibilité

Les pratiques du Service de Confiance sont non-discriminatoires. Les services de confiance sont offerts à toute personne physique ou morale dont les activités entrent dans le champ d'application défini par la, dès lors que cette personne accepte les conditions générales et les obligations contractuelles associées.

Le Prestataire veille à ce que l'accès à ses services soit équitable et transparent, sans distinction fondée sur la nationalité, la taille de l'entreprise ou le secteur d'activité.

4.1.2. Ressources financières et stabilité

Le Prestataire dispose de ressources financières, techniques et humaines suffisantes pour assurer la continuité et la qualité de ses services de confiance.

Il garantit sa stabilité financière et sa capacité à respecter ses obligations légales et contractuelles, notamment au titre de la responsabilité liée à la fourniture du Service de Confiance.

Le Prestataire maintient une assurance de responsabilité civile professionnelle couvrant les dommages pouvant résulter de ses activités, conformément aux dispositions du règlement (UE) n°910/2014 (eIDAS) et à la législation luxembourgeoise en vigueur.

4.1.3. Gouvernance et surveillance interne

La fiabilité organisationnelle repose sur une gouvernance structurée, assurée par l'Autorité de Gouvernance, responsable de la conformité et du pilotage des activités de certification.

L'Autorité de Gouvernance approuve les politiques et déclarations de pratiques mises en place dans son périmètre de responsabilité.

Le Prestataire met en œuvre un dispositif d'audit interne et de contrôle permanent visant à vérifier le respect des politiques, des procédures et des exigences réglementaires.

Les audits périodiques permettent d'identifier les écarts potentiels, de définir les mesures correctives nécessaires et de maintenir un niveau de sécurité conforme aux référentiels ETSI et à la Politique de Certification.

4.1.4. Gestion des plaintes et des litiges

Le Prestataire a établi des procédures formalisées de gestion des plaintes et des litiges.

Toute réclamation émanant d'un client, d'un porteur de certificat ou d'une partie utilisatrice est enregistrée, analysée et traitée selon une procédure interne documentée. Les plaintes peuvent être adressées au Prestataire via les canaux officiels indiqués dans les conditions générales de service.

Le Prestataire favorise la résolution amiable des litiges ; à défaut, ceux-ci sont soumis à la juridiction compétente du Grand-Duché de Luxembourg.

4.2. Ségrégation des rôles

4.2.1. Séparation des fonctions et des responsabilités

Le Prestataire applique le principe de séparation des fonctions et de répartition claire des responsabilités afin de réduire les risques de modification non autorisée, d'erreur ou d'utilisation abusive des actifs, systèmes et informations de l'Infrastructure.

Cette mesure vise à éviter les conflits d'intérêts et à garantir qu'aucune personne n'exerce simultanément des fonctions incompatibles susceptibles de compromettre la sécurité, l'intégrité ou la traçabilité des opérations liées aux services de confiance.

4.2.2. Rôles et responsabilités

Les rôles de confiance définis ci-dessous sont ceux requis pour les composantes d'un Service de Confiance, chaque Service de Confiance peut définir des rôles complémentaires si nécessaires.

- Officier de Sécurité : est chargé de la mise en œuvre de la politique de sécurité . Il gère les contrôles d'accès physiques aux équipements des systèmes de l'entité. Il est habilité à prendre connaissance des documents conservés, et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- Directeur de sécurité des services de confiance : est chargé de la mise en œuvre des différentes politiques et Déclaration de Pratiques. Sa responsabilité couvre l'ensemble des fonctions rendues par les applications et des performances correspondantes.
- Ingénieur système est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de l'entité. Il assure l'administration technique des systèmes et des réseaux de l'entité. Il est également chargé des opérations de restauration.

- Opérateur : réalise, dans le cadre de ses attributions, l'exploitation des applications pour les services délivrés.
- Contrôleur : est une personne désignée qui a pour rôle de procéder à l'analyse des journaux et des incidents. Le contrôleur est indépendant des autres rôles de confiance.
- Opérateur d'enregistrement est une personne responsable pour vérifier les informations nécessaires à la délivrance d'un certificat et approuver les demandes de certificat.
- Opérateur de révocation est une personne responsable pour toutes les opérations de changement d'un statut de certificat.

Chaque rôle dispose de droits et privilèges limités à ses missions spécifiques, selon le principe du moindre privilège.

Les responsabilités sont formalisées dans des fiches de fonction et des procédures internes validées par l'Autorité de Gouvernance.

4.2.3. Séparation opérationnelle et contrôle croisé

La conception et l'exploitation des systèmes reposent sur une séparation stricte entre les fonctions d'administration, d'exploitation, de développement et de supervision.

Les actions critiques (ex. génération de clés, émission de certificats, modification de configurations sensibles) nécessitent la présence ou la validation de plusieurs personnes habilitées (principe du double contrôle).

Les accès techniques sont segmentés par profils (opérateurs, administrateurs, auditeurs), et chaque intervention est tracée et journalisée dans les systèmes de supervision et d'audit.

4.2.4. Vérification et supervision

Les affectations de rôles et de droits d'accès sont revues régulièrement afin de s'assurer que la séparation des fonctions demeure effective, notamment lors de changements organisationnels ou de mobilité du personnel.

Les vérifications périodiques sont menées par la fonction Sécurité, et leurs résultats sont communiqués à l'Autorité de Gouvernance.

4.3. Ressources humaines

4.3.1. Qualifications, compétences et habilitations requises

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité, l'engageant à ne pas diffuser les documents sensibles du service à des personnes non habilitées à les recevoir.

Le directeur de la sécurité des Services de Confiance doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de l'IGC, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein des Services de confiance ainsi que des mesures de protection des données personnelles.

Le prestataire informe toute personne intervenant dans des rôles de confiance :

- De ses responsabilités relatives aux services de confiance ;
- Des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

Cette nomination est réalisée de façon formelle et est acceptée par écrit par la personne nommée dans un rôle de confiance.

Les qualifications, compétences et habilitations requises pour la cérémonie des clés sont définies dans une procédure spécifique.

Les responsabilités des personnels dans les rôles de confiance sont attribuées de façon à séparer les rôles et responsabilité, éviter les conflits d'intérêt et réduire les opportunités de modification ou de mauvaise utilisation, volontaire ou involontaire, des systèmes de l'IGC.

Les accès et habilitation sont attribués et configurés suivant la politique du moindre privilège.

4.3.2. Procédures de vérification des antécédents

Les personnels amenés à travailler au sein d'un service de confiance, et en fonction du contexte applicable, sont amenés à remettre une attestation sur l'honneur de non-condamnation, un extrait de casier judiciaire, ou un engagement de confidentialité.

Les personnes disposant d'un rôle de confiance ne doivent pas souffrir de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches.

4.3.3. Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, au sein de la composante de l'IGC dans laquelle il opère.

Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

4.3.4. Exigences et fréquence en matière de formation continue

Le prestataire s'assure que le personnel en charge des services dispose des compétences nécessaires à la réalisation de ses tâches. Des formations de sensibilisations sont menées régulièrement sur les principaux sujets des services de confiance :

- Sensibilisation au traitement des données personnelles,
- Sensibilisation aux risques cyber.

Un plan de formation est élaboré chaque année afin de maintenir et développer les compétences des collaborateurs. Les collaborateurs peuvent également exprimer leur besoin de formation lors des entretiens individuels semestriels qui permette de remettre à jour les plannings de formation individuels.

4.3.5. Fréquence et séquence de rotation entre différentes attributions

La rotation entre les attributions est effectuée à l'occasion d'un changement de poste ou de fonction de l'une des personnes disposant d'un rôle opérationnel ou d'un rôle de confiance pour l'AC.

La validité des attributions, en fonction des postes réellement occupés par les personnes cibles est revue à l'occasion de chaque audit interne.

4.3.6. Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans le règlement intérieur ou contrat de travail.

4.3.7. Exigences vis-à-vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées notamment celles encadrant le respect des niveaux de confidentialités des documents qui sont délivrés aux prestataires externes.

Les clauses suivantes pourront être ajoutées le cas échéant aux contrats liant le Prestataire aux prestataires externes :

- Le prestataire externe s'oblige à affecter en permanence à l'exécution du présent contrat un personnel qualifié et compétent ou le cas échéant, un personnel ayant le niveau de qualification déterminé ;
- Le prestataire externe s'engage à actualiser son savoir-faire, à se tenir informé des meilleures pratiques du marché en la matière et à réaliser des sessions de formation permanente de son Personnel à ce savoir-faire évolutif ;
- Le prestataire externe s'engage à prendre les mesures nécessaires, notamment vis-à-vis de son Personnel, pour que soient maintenues confidentielles les informations de toute nature qui lui sont communiquées par le Prestataire.

4.3.8. Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de leur prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans l'infrastructure de gestion de clés disposent des procédures correspondantes.

4.4. Gestion des actifs

4.4.1. Mesure de protection des actifs

Le Prestataire met en œuvre une politique de gestion et de protection des actifs visant à garantir la disponibilité, l'intégrité et la confidentialité des informations et équipements utilisés dans le cadre de la fourniture des services de confiance.

Un inventaire des actifs critiques (matériels, logiciels, clés cryptographiques, informations et supports de sauvegarde) est établi et maintenu à jour (voir 4.4.2)

Les actifs sont classés selon leur niveau de sensibilité et protégés par des mesures physiques, logiques et organisationnelles appropriées, conformément à la Politique de Sécurité du Prestataire.

Les équipements et supports contenant des données sensibles sont conservés dans des zones à accès restreint et protégés contre la perte, le vol, la destruction ou la compromission. Leur utilisation et leur destruction sont encadrées par des procédures formalisées et auditées.

Les fournisseurs et sous-traitants doivent démontrer la conformité de leurs produits ou services aux exigences de sécurité définies dans les contrats et procédures d'acquisition (voir 4.15)

Des mécanismes de traçabilité, d'intégrité et de conformité sont mis en œuvre pour garantir que ces actifs ne sont ni modifiés ni compromis avant leur mise en service.

4.4.2. Gestion de l'inventaire

Le prestataire dispose d'un inventaire ou l'ensemble des actifs sont répertoriés. Pour chacun, les informations suivantes (quand cela est applicable) sont répertoriées :

- Identifiant unique,
- Une courte description,
- Une personne ou une entité propriétaire,

- Sa localisation,
- Son type,
- Une classification du type d'information traitée par l'actif,
- Une classification de l'actif,
- La version de l'actif et la date de dernière mise à jour,
- La date de fin de support de l'actif
- Sa date de fin de vie envisagée.

La définition du propriétaire (ou responsable) d'un actif doit permettre d'identifier rapidement un membre de l'organisation en charge de l'actif. Cela signifie que la taille d'une entité doit être raisonnable ; il ne peut que rarement s'agir d'une entité plus large qu'une équipe.

La classification des actifs revue après chaque analyse de risque.

4.4.3. Gestion des stockages

Le Prestataire a défini et applique des procédures de gestion des supports de stockage couvrant l'ensemble de leur cycle de vie : acquisition, utilisation, transport, conservation et élimination. Ces procédures sont conformes au schéma de classification de la sécurité de l'information défini par le Prestataire et garantissent un niveau de protection adapté à la sensibilité des données contenues.

Tous les supports de stockage utilisés dans le cadre des services de confiance sont :

- identifiés, enregistrés et tracés dans un inventaire des actifs ;
- protégés contre les dommages physiques, la perte, le vol et l'accès non autorisé ;
- stockés dans des zones sécurisées, protégées contre les risques d'incendie, d'humidité, d'inondation et de surchauffe ;
- manipulés uniquement par des personnes habilitées, conformément aux procédures internes de sécurité.

Le Prestataire veille à prévenir l'obsolescence et la détérioration des supports en assurant un contrôle régulier de leur état et en effectuant la migration des données lorsque cela est nécessaire pour garantir la lisibilité et la disponibilité des enregistrements pendant toute la période de conservation réglementaire.

En fin de vie, les supports sont effacés ou détruits de manière sécurisée selon leur niveau de classification :

- les supports électroniques sont réinitialisés, chiffrés ou physiquement détruits ;
- les supports papier ou optiques sont broyés avant élimination.

Toutes les opérations de destruction sont documentées et consignées dans les registres internes, conformément à la Politique de Certification du Prestataire.

Les sauvegardes sont effectuées sur des supports dédiés, conservés dans des emplacements distincts et testées régulièrement pour en vérifier la fiabilité et la possibilité de restauration.

4.5. Contrôle d'accès

L'accès au système du service de confiance est limité aux personnes autorisées.

4.5.1. Comptes privilégiés, principe du moindre privilège

L'ensemble des administrateurs intervenant sur le système serveur de l'IGC se connecte sur ces équipements par authentification forte.

Les accès et habilitation sont attribués et configurés suivant la politique du moindre privilège.

Les administrateurs ont la charge de la gestion des comptes. Ils effectuent les modifications et/ou suppressions des accès sans délais.

4.5.2. Authentification forte

Tous les membres du personnel de confiance disposent d'un moyen d'authentification fort (soit carte à puce et code PIN, soit vpn) pour accéder aux composantes de l'IGC. L'authentification forte est requise avant tout actions sur les composantes de l'IGC.

4.5.3. Revue des droits d'accès et révocation en cas de départ ou changement

Le Prestataire de Services de Confiance réalise une vérification périodique des droits d'accès aux comptes privilégiés et administrateurs.

Ces droits d'accès doivent être modifiés en fonction des changements organisationnels.

Le résultat de cette vérification est documenté et conservé.

4.5.4. Séparation des rôles et contrôle des utilitaires système

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des services offerts.

Les attributions associées à chaque rôle sont conformes à la Politique de Sécurité.

Pour les différents rôles de confiance, il est recommandé qu'une même personne ne détienne pas plusieurs rôles.

Les cumuls suivants sont interdits :

- Contrôleur et tout rôle d'enregistrement ;
- Administrateur système/réseau et officier de sécurité.

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques du service de confiance est défini dans la déclaration de pratique. Il répond en particulier aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par le service de confiance, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;

- Fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- Eventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle est cohérente avec la Politique de Sécurité.

Pour atteindre ces objectifs de sécurité, le Prestataire utilise des systèmes et des produits fiables permettant de mettre en œuvre de façon sécurisé les différents processus du Service de Confiance. Les systèmes et produits sont choisis et/ou développés en prenant en compte les exigences de sécurité.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système sont mis en place. Ces dispositifs permettent :

- De détecter, enregistrer et réagir dans les meilleurs délais à un accès ou une tentative d'accès non autorisée aux ressources du Service de Confiance ;
- De surveiller l'usage du service et les requêtes ;
- De déclencher des alarmes en cas de détection de potentielles violations des mesures de sécurité ;
- De surveiller l'activation ou la désactivation des fonctions de génération de traces ;
- De surveiller la disponibilité et le trafic réseau.

Les dispositifs de surveillance prennent en compte la sensitivité de l'information collectée et analysée. Le suivi des alertes sur les événements critiques de sécurité est assuré par des personnels en rôle de confiance. Ces derniers s'assurent que les incidents sont analysés et sont traités suivant les procédures en places.

4.5.5. Identification, responsabilité

Chaque entité opérant une composante du service de confiance fait vérifier l'identité et les autorisations de tout membre de son personnel avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant les systèmes concernés par le rôle,
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes,
- qu'un compte soit ouvert à son nom dans ces systèmes,
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Ces contrôles sont conformes à la Politique de Sécurité.

Les rôles d'opérateurs, d'administrateurs et de contrôleurs sont directement gérés par le Prestataire ou ses sous-traitant selon le même niveau de contrainte. Les administrateurs ont la charge de la gestion des comptes. Ils effectuent les modifications et/ou suppressions des accès sans délais.

Les opérations réalisées par les personnels en rôle de confiance sont tracées.

4.5.6. Protection contre la réutilisation de supports ou objets de stockage

En fin de vie, les supports seront, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes. Les procédures et moyens de destruction et de réinitialisation sont conformes à la Politique de Sécurité du Prestataire.

Les supports (papier, disque dur, disquette, CD, etc.) utilisés au sein du service de confiance sont traités et conservés conformément aux besoins de sécurité pour les actifs sensibles (en confidentialité, intégrité et disponibilité).

En particulier, les supports font l'objet de mesures contre les dommages, le vol, les accès non autorisés et l'obsolescence. Ces mesures s'appliquent durant toute la période de rétention du contenu de ces supports.

4.6. Contrôle cryptographique

4.6.1. Gestion des clés, des algorithmes et des dispositifs cryptographiques

Le Prestataire applique une politique centralisée de gestion du cycle de vie des clés, couvrant la génération, la distribution, l'utilisation, la sauvegarde, la révocation et la destruction des clés cryptographiques utilisées dans les services de confiance. Cette politique s'appuie sur les exigences des normes ETSI EN 319 401, ETSI EN 319 411-1/2 et FIPS 140-2 niveau 3 ou CC EAL4+.

Les fonctions cryptographiques sont réalisées exclusivement au sein de modules matériels de sécurité (HSM) certifiés et approuvés par l'Autorité de Gouvernance.

Les HSM sont configurés en cluster redondant et répartis sur deux sites géographiques distincts afin d'assurer la continuité des opérations et la résilience du service.

Les algorithmes, tailles de clé et durées de vie sont conformes aux recommandations de SOG-IS et aux publications de l'ENISA.

Un registre des clés et des certificats d'infrastructure est tenu à jour, documentant pour chaque clé :

- l'usage prévu (signature d'AC, chiffrement, authentification, horodatage, etc.) ;
- la date de génération et d'expiration ;
- le HSM et le site de stockage associés ;
- les porteurs de secrets ou custodians désignés.

4.6.2. Génération et installation des clés

Les clés d'infrastructure sont générées dans les HSM lors de cérémonies de clés formalisées.

Chaque cérémonie fait l'objet d'un dossier complet comprenant :

- le plan de cérémonie (participants, étapes, objectifs) ;
- les identités des participants et leurs rôles ;
- les logs HSM et journaux d'événements ;
- les procès-verbaux signés et archivés.

La génération est supervisée par au moins deux personnes habilitées (principe du double contrôle) : un officier de sécurité et un opérateur cryptographique.

Les clés sont créées directement dans le HSM et ne sont jamais exportées en clair.

Les certificats racine et d'autorité intermédiaire sont signés selon des procédures validées par l'Autorité de Gouvernance. Ces opérations sont effectuées dans des environnements isolés (air-gapped) dédiés aux cérémonies de clés.

4.6.3. Protection, stockage et utilisation

Les clés privées sont stockées uniquement dans les HSM.

L'accès aux fonctions sensibles (import/export, backup, destruction) est limité aux personnels désignés comme custodians, chacun possédant une donnée d'activation personnelle (Smartcard + PIN).

Les opérations sont enregistrées dans des journaux signés et horodatés, conservés pendant 7 ans.

Les clés ne sont utilisées que pour les fonctions pour lesquelles elles ont été créées.

4.6.4. Sauvegarde et redondance

Les clés critiques sont sauvegardées dans les HSM secondaires du cluster, selon un processus de duplication sécurisée nécessitant la présence simultanée de plusieurs porteurs de secrets.

Les HSM redondants sont hébergés sur deux sites distincts et synchronisés périodiquement.

Aucune clé privée d'infrastructure n'est exportée ni stockée en dehors du périmètre HSM.

Aucun séquestre de clé n'est autorisé.

4.6.5. Données d'activation et porteurs de secrets

Les données d'activation (PIN, smartcards, codes de déverrouillage) sont générées et distribuées pendant la cérémonie de clés.

Elles sont confiées à des porteurs désignés par l'Autorité de Gouvernance, selon le principe de segmentation des secrets (M sur N). Les porteurs signent un registre de remise et s'engagent à conserver ces éléments sous scellés, dans des coffres distincts.

Toute perte ou compromission déclenche immédiatement une procédure de révocation.

4.6.6. Algorithmes et durées de vie

Les algorithmes suivants sont utilisés par défaut, sauf exigence contraire d'une DPC spécifique :

- RSA ≥ 3072 bits pour les clés de signature ;
- ECDSA (P-256 ou P-384) pour les signatures de certificats ou tokens légers ;
- SHA-256 / SHA-384 pour les empreintes et signatures ;
- AES-256 pour le chiffrement des données stockées.

Les durées de vie des clés sont alignées sur le niveau de risque et la criticité du service :

- clés racine : 10 à 30 ans ;
- clés d'autorité intermédiaire : 5 ans ;
- clés de service : 1 à 3 ans selon usage.

4.6.7. Désactivation et destruction

À l'expiration, la révocation ou en cas de compromission, les clés sont désactivées dans le HSM, puis détruites de manière irréversible à l'aide des fonctions sécurisées intégrées au module.

Un procès-verbal de destruction est établi, signé par deux porteurs de rôle de confiance et archivé.

4.6.8. Contrôle et supervision

La gestion du cycle de vie des clés est supervisée par le Directeur de la Sécurité et le Responsable de l'Autorité de Certification, sous le contrôle de l'Autorité de Gouvernance.

Des revues périodiques des clés et certificats d'infrastructure sont effectuées pour vérifier :

- la conformité aux politiques et durées de vie ;
- la bonne tenue du registre des clés ;
- l'absence d'usage non autorisé.

Les journaux des opérations cryptographiques sont horodatés et stockés dans un environnement d'archivage sécurisé.

4.7. Sécurité physique et environnementale

Le Prestataire met en œuvre un ensemble de mesures physiques et environnementales destinées à assurer la protection des composants critiques du Service de Confiance et à prévenir toute compromission, dégradation ou indisponibilité résultant d'un incident physique ou environnemental.

Ces mesures répondent aux exigences ETSI EN 319 401 et s'appliquent à l'ensemble des sites hébergeant des fonctions sensibles du Prestataire.

4.7.1. Contrôle des accès physiques

Les composants critiques (serveurs, HSM, systèmes d'administration, salles techniques) sont installés dans des zones à accès restreint, situées dans des locaux à sécurité renforcée et surveillés en permanence.

L'accès à ces zones est strictement réservé aux personnes autorisées et identifiées dans la liste des personnels habilités. Tout accès est soumis à une authentification forte, reposant sur des mécanismes tels que badge nominatif, code personnel, biométrie, selon le niveau de sensibilité de la zone concernée.

Aucune personne non habilitée ne peut accéder seule à une zone sécurisée : les visiteurs ou intervenants externes sont systématiquement accompagnés.

Les accès sont enregistrés et tracés ; ils font l'objet d'un suivi et d'un contrôle périodique par les responsables de la sécurité.

4.7.2. Périmètre de sécurité physique

Les sites hébergeant des composants critiques sont protégés par un périmètre de sécurité physique intégrant :

- des systèmes de contrôle d'accès électroniques ;
- une détection d'intrusion reliée à un centre de surveillance 24h/24 et 7j/7 ;
- un dispositif de vidéosurveillance couvrant les points d'accès ;
- une alarme automatique en cas d'ouverture non autorisée ou de mouvement détecté hors plage d'exploitation.

Les salles techniques bénéficient de protections contre les risques d'incendie, d'inondation, de surtension ou de coupure électrique, conformément aux exigences du niveau de sécurité défini dans la Politique de Certification.

Les alimentations électriques sont redondées et secourues (onduleurs, groupes électrogènes), et la température ambiante est régulée par un système de climatisation contrôlé et supervisé.

4.7.3. Protection des actifs et supports

Les équipements, supports d'information et dispositifs de sauvegarde sont protégés contre la perte, le vol, les dégradations et la compromission.

Les sauvegardes sont stockées dans des environnements sécurisés distincts du site principal, assurant la continuité des opérations en cas d'incident majeur.

Les supports de stockage contenant des données sensibles sont inventoriés, tracés et détruits de manière sécurisée lorsqu'ils arrivent en fin de vie, conformément aux procédures internes du Prestataire.

4.7.4. Surveillance et continuité

Les installations sont surveillées en continu par un système d'alarme et des dispositifs automatiques de détection et de remontée d'incidents.

Les contrôles physiques et environnementaux (accès, températures, alimentation, climatisation, sécurité incendie) font l'objet de tests et de vérifications périodiques documentées.

En cas d'incident affectant la disponibilité ou l'intégrité d'un site, des procédures de bascule et de reprise sont prévues, garantissant la continuité des activités critiques.

4.8. Sécurité des opérations

Le Prestataire met en œuvre des mesures de sécurité opérationnelle destinées à garantir la fiabilité, l'intégrité et la disponibilité des systèmes supports des services de confiance.

Ces mesures visent à assurer que les composants critiques du Service de Confiance sont exploités dans des conditions maîtrisées, selon des procédures documentées, en limitant tout risque de modification non autorisée ou de dysfonctionnement.

4.8.1. Utilisation de systèmes fiables et sécurisés

Les composants techniques utilisés par le Prestataire sont sélectionnés parmi des produits fiables, certifiés et éprouvés, conformes aux exigences de sécurité spécifiées dans la Politique de Certification.

Ils sont protégés contre toute modification non autorisée et font l'objet de contrôles d'intégrité réguliers afin de garantir la stabilité et la fiabilité des processus de certification et de signature.

4.8.2. Intégration de la sécurité dans le cycle de vie des systèmes

Toute évolution ou projet de développement technique fait l'objet d'une analyse préalable des exigences de sécurité dès la phase de conception. Les spécifications fonctionnelles et techniques intègrent des critères de sécurité, de traçabilité et de résilience.

Les développements internes ou sous-traités sont réalisés conformément aux procédures de sécurité définies et aux bonnes pratiques du Prestataire.

4.8.3. Gestion et contrôle des changements

Les modifications apportées aux systèmes de production, aux composants logiciels, aux configurations ou aux politiques de sécurité sont formellement encadrées par une procédure de gestion du changement.

Cette procédure définit les cas suivants :

- Mises à jour planifiées
- Correctifs d'urgence

- Changements de configuration.

Chaque modification fait l'objet d'une documentation, incluant la description du changement, sa justification, les impacts potentiels et les validations nécessaires avant déploiement.

Les changements sont exécutés uniquement par des personnels autorisés, selon le principe du double contrôle lorsque requis.

4.8.4. Protection contre les logiciels malveillants et menaces logicielles

Les systèmes sont protégés contre les logiciels malveillants, non autorisés ou compromettants.

Des tests de vulnérabilité, contrôles d'intégrité et revues de sécurité sont réalisés périodiquement afin de détecter toute anomalie ou comportement suspect.

Les journaux d'événements sont surveillés et analysés pour identifier rapidement tout incident de sécurité.

4.8.5. Gestion des correctifs et mises à jour de sécurité

Les correctifs de sécurité et mises à jour logicielles sont appliqués dans un délai raisonnable suivant leur publication par les éditeurs.

Avant toute mise à jour, le Prestataire évalue les risques techniques et fonctionnels associés.

Les correctifs susceptibles d'introduire des vulnérabilités ou instabilités sont suspendus après analyse de risque ; les motifs de non-application sont documentés et approuvés par le Responsable de la Sécurité.

Les procédures de mise à jour sont supervisées et contrôlées par l'Autorité de Gouvernance.

4.8.6. Gestion et revue des configurations

Les configurations matérielles, logicielles et réseau sont définies, documentées, validées et surveillées de manière continue.

Tout changement de configuration doit être autorisé et enregistré conformément à la politique de sécurité.

Le Prestataire utilise des outils de supervision et de gestion de configuration permettant :

- la détection des modifications non autorisées,
- la surveillance de l'intégrité des fichiers et composants,
- la sauvegarde et la restauration sécurisée des environnements.

Les configurations et paramètres de sécurité font l'objet d'une revue régulière afin de vérifier leur conformité, d'évaluer la robustesse des mécanismes d'authentification (mots de passe, certificats) et de confirmer l'adéquation des niveaux de protection appliqués.

4.8.7. Surveillance et audit opérationnel

Le Prestataire dispose d'un système de supervision centralisée qui collecte, corrèle et archive les journaux des systèmes critiques.

Ces informations permettent la détection des anomalies, le suivi des incidents et la traçabilité complète des actions d'administration et d'exploitation.

Des audits techniques et organisationnels périodiques permettent de s'assurer de la bonne application des procédures et du maintien du niveau de sécurité attendu.

4.9. Sécurité du réseau

Pour des raisons de confidentialité, l'architecture réseau détaillée ainsi que les matrices de flux internes et externes à la plate-forme sont disponibles dans le document Dossier d'architecture technique de la PKI du Prestataire.

4.9.1. Segmentation en zone

Fondé sur les résultats de l'analyse de risque, le Prestataire a segmenté son réseau en zone séparées (fonctionnellement, logiquement ou physiquement). Des mesures de contrôle similaires sont mise en place pour l'ensemble des éléments d'une même zone. Chaque système de l'infrastructure est exploité dans une zone réseau sécurisée et est installé suivant des procédures et une configuration assurant une exploitation sécurisée.

Le Prestataire a également mis en place une séparation stricte entre les systèmes de production et les autres systèmes (test, qualification, …).

4.9.2. Interconnexions

L'interconnexion vers des réseaux publics ainsi que l'interconnexion entre chaque zone réseau est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'infrastructure.

Le prestataire garantit que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement et logiquement sécurisé.

De plus, les échanges entre composantes au sein de l'infrastructure du Prestataire font l'objet de la mise en place de canaux sécurisés logiquement distincts et permettant d'assurer l'authentification de la destination des données et d'assurer l'intégrité et la confidentialité des données échangées.

La matrice des flux est revue régulièrement et les firewalls sont contrôlés afin de s'assurer que seuls les ouvertures utiles et nécessaires sont présentes. La gestion des ouvertures est faite suivant le principe des moindres privilèges.

4.9.3. Connexions

Seuls les personnels en rôle de confiance ont accès aux zones réseaux sécurisées.

Toute connexion d'un compte permettant de créer directement un certificat n'est possible qu'après une authentification multi-facteur. Les réseaux permettant d'opérer et d'administré l'IGC sont séparés. Le réseau d'administration est dédié à cet usage.

Tous les systèmes sont configurés de façon à supprimer ou désactiver les comptes, applications, services et ports qui ne sont pas utilisés pour les opérations.

Les accès d'administrations sont réalisés au travers d'accès VPN dédiés et différents des opérations.

4.9.4. Disponibilité

Afin de répondre aux besoins de disponibilité de ses composantes, le Prestataire a mis en place des mesures de redondances locales permettant d'offrir une haute disponibilité des services critiques.

4.9.5. Test de pénétration

Des tests de pénétration sont réalisés chaque année ou à chaque modification importante de l'infrastructure. Ces scans sont réalisés par des équipes compétentes choisies par le Prestataire.

Des scans sont réalisés sur les services accessibles publiquement.

Des scans sont réalisés sur les IP privée à partir d'une connexion VPN autorisée.

4.9.6. Protection contre les virus

Le prestataire dispose d'un antivirus mis à jour régulièrement afin de protéger ses systèmes et réseaux contres les virus et programmes malicieux. Cette antivirus scanne les machines du services au moins quotidiennement.

4.9.7. Scan de vulnérabilité

Le Prestataire réalise régulièrement des scans de vulnérabilité sur ses adresses IP publiques et privées. Chaque scan est réalisé par une personne ou une entité qualifiée et indépendante.

Ces scans sont réalisés au moins une fois par trimestre.

Dès réception des résultats un plan d'action est mis en place afin de corriger les éventuelles vulnérabilités.

4.10. Gestion des vulnérabilités et des incidents

Chaque service définit les procédures spécifiques à ses composantes, ces procédures sont identifiées dans les déclarations de pratique spécifique.

4.10.1. Procédures de remontée et de traitement des incidents et des compromissions

Chaque composante des services met en œuvre des procédures et des moyens de remontée et de traitement des incidents conformément aux exigences de la Politique de Sécurité.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, l'événement déclencheur est la constatation de cet incident. L'AG du Prestataire en est immédiatement informée. Le cas de l'incident majeur est impérativement traité dès la détection.

En cas d'incident majeur de sécurité ou de perte d'intégrité ayant un impact important sur ses opérations de service de confiance ou sur les données personnelles, le Prestataire notifiera les parties concernées, en particulier l'organe de contrôle, l'organe de certification, la CNIL en France et le CNPD au Luxembourg (pour les données hébergés au Luxembourg), dans les 24 heures après l'identification de l'incident, conformément aux exigences du Règlement eIDAS et, le cas échéant, les clients impactés.

4.10.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)

Conformément à la Politique de Sécurité du Prestataire, chaque service dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité de ses fonctions sensibles, et découlant :

- De sa politique de certification spécifique ;
- Des engagements en termes de qualité de service des différentes composantes du service.

Ce plan est testé au minimum une fois tous les 1 an sur tout ou partie des scénarios.

4.10.3. Capacités de continuité d'activités à la suite d'un sinistre

Des mesures sont mises en œuvre par le Prestataire pour assurer la continuité et la reprise d'activité. Ces mesures incluent :

- La redondance et le basculement des services ;
- La sauvegarde et la restauration des services ;
- La notification et les communications vers les clients.

Le Prestataire dispose d'un plan de continuité d'activité à jour afin de réagir efficacement en cas de désastre et de restaurer le système dans les délais précisés dans ce plan.

4.11. Collecte des preuves

4.11.1. Types de données à archiver

Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'infrastructure. Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC ;
- Les DPC ;
- Les agréments contractuels avec d'autres services de confiance ou parties prenantes ;

Les déclarations de pratique des différents services peuvent compléter cette liste.

4.11.2. Période de conservation des archives

En l'état de la législation et de la réglementation en vigueur (dite « Informatique et Libertés »), toute information de type :

- Personnel,
- Trafic,
- Connexion,
- Facturation,

et issue d'un processus automatique de traitement de données, n'est pas archivée pendant plus d'un an.

Les documents suivants sont conservés pour la durée de vie du service concerné :

- PC,
- DPC,
- Documents organisationnels de cérémonies des clés.

Les journaux d'événements sont conservés pendant 7 ans après expiration de l'élément qu'ils journalisent.

Le Prestataire a mis en place les mesures nécessaires pour que ces archives soient conservées sur les durées mentionnées même en cas d'arrêt d'activité.

4.11.3. Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, sont :

- Protégés en intégrité ;
- Accessibles aux personnes autorisées ;

Les archives des AC sont protégées en intégrité et en confidentialité pendant toute la période de rétention.

4.11.4. Procédure de sauvegarde des archives

La solution de sauvegarde des archives consiste en une copie des archives sur un système similaire. Le niveau de protection des sauvegardes est équivalent au niveau de protection des archives, ceci inclut l'intégrité et la confidentialité.

4.11.5. Système de collecte des archives

Pour chaque Service de Confiance, La DPC précise les moyens mis en œuvre pour collecter les archives en toute sécurité.

4.11.6. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) sont récupérables dans un délai de 2 jour ouvré, étant noté que seul le Prestataire peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'infrastructure qui ne peut récupérer et consulter que les archives de la composante considérée).

4.12. Gestion de la continuité d'activité

Pour chacun de ses Services de Confiance, le Prestataire définit un plan de continuité qu'il pourra activer en cas de désastre. Le délai de réalisation du plan de continuité est défini dans chaque plan.

Afin d'être préparé à ce type d'incident, un test du plan de continuité est réalisé annuellement. Le test peut être annulé s'il a été activé au moins une fois lors de l'année écoulée.

4.13. Arrêt définitif du service

Cette déclaration de pratique ne précise pas les plans d'arrêt définitif des services. Ceux-ci doivent être définis dans les politiques et déclaration de pratique spécifique au service.

4.14. Conformité

Les pratiques du Prestataire sont non-discriminatoires. Dans la mesure du possible, le Prestataire mettra en œuvre toutes les dispositions nécessaires pour rendre accessible son service aux personnes en situation de handicap.

Toute déclaration de pratique se référant au présent document doit préciser les moyens mis en œuvre pour assurer le respect du cadre réglementaire et légal applicable à son activité. Ce cadre inclut a minima :

- le Règlement européen RGPD relatif à la protection des données personnelles ;
- le Règlement européen eIDAS relatif à l'identification électronique et aux services de confiance.
- la Directive NIS2, ainsi que ses mesures de transposition nationale applicables au Luxembourg.

4.15. Gestion des fournisseurs

Le Prestataire met en œuvre des processus et procédures formalisés afin d'assurer la maîtrise des risques de sécurité associés à la chaîne d'approvisionnement des produits et services utilisés pour le fonctionnement du Service de Confiance.

Ces processus visent à garantir que tous les produits, composants et services fournis ou exploités par des tiers respectent les exigences de sécurité définies par le Prestataire, et que leur intégrité, leur origine et leur configuration sont contrôlées tout au long de leur cycle de vie.

4.15.1. Acquisition de produits et services TIC

Avant tout achat ou intégration de produits ou services TIC, le Prestataire définit et applique des exigences de sécurité minimales adaptées à la sensibilité des systèmes concernés.

Ces exigences sont intégrées dans les cahiers des charges et contrats fournisseurs et couvrent notamment :

- la conformité aux standards de sécurité applicables (par ex. FIPS 140-2, EAL4+, ISO 27001) ;
- la garantie d'origine et d'intégrité des produits livrés ;
- les conditions d'exploitation sécurisée et de maintenance.

4.15.2. Propagation des exigences de sécurité dans la chaîne d'approvisionnement

Les fournisseurs de services TIC ont l'obligation contractuelle de propager les exigences de sécurité du Prestataire à tout sous-traitant intervenant dans la fourniture de leurs services.

De la même manière, les fournisseurs de produits TIC doivent s'assurer que leurs propres partenaires ou sous-traitants appliquent des pratiques de sécurité équivalentes pour les composants matériels et logiciels intégrés.

4.15.3. Information sur les composants et fonctions de sécurité

Le Prestataire demande à ses fournisseurs de produits TIC de fournir une description des composants logiciels intégrés, des versions et dépendances associées, ainsi qu'une documentation technique détaillant les mécanismes de sécurité implémentés et la configuration nécessaire pour une utilisation sécurisée.

Ces informations permettent au Prestataire d'évaluer la conformité des produits aux exigences internes et aux référentiels de certification applicables.

4.15.4. Validation et contrôle de conformité

Le Prestataire met en place un processus de validation et de surveillance continue des produits et services TIC acquis. Ce processus comprend :

- la vérification de la conformité des livrables aux spécifications de sécurité contractuelles ;
- des contrôles d'intégrité et de bon fonctionnement des composants critiques ;
- des tests de sécurité ou d'acceptation avant mise en production ;
- le suivi des vulnérabilités connues et l'application des mises à jour de sécurité publiées par les fournisseurs.

4.15.5. Identification et traçabilité des composants critiques

Les composants ou services considérés comme critiques pour le maintien de la disponibilité et de la fiabilité de l'IGC sont identifiés et documentés.

Le Prestataire exige que leur origine et leur chaîne de distribution soient traçables et vérifiables, afin d'obtenir l'assurance qu'ils sont authentiques et conformes à leurs spécifications d'origine.

Tout composant reçu fait l'objet d'un contrôle d'intégrité afin de garantir qu'il est non altéré.

4.15.6. Partage d'information et gestion des incidents fournisseurs

Le Prestataire établit des règles de partage d'information avec ses fournisseurs relatives aux vulnérabilités, incidents ou compromissions potentielles identifiées dans la chaîne d'approvisionnement.

Ces échanges se font selon des canaux sécurisés et dans le respect des obligations de confidentialité et de notification convenues contractuellement.

4.15.7. Gestion du cycle de vie et surveillance des fournisseurs

Le Prestataire suit le cycle de vie complet des composants et services TIC, depuis leur acquisition jusqu'à leur retrait ou remplacement.

Des revues régulières sont effectuées pour évaluer :

- la conformité continue des pratiques de sécurité des fournisseurs ;
- les changements affectant la qualité ou la sécurité du service fourni ;
- les mesures correctives à mettre en œuvre en cas de dérive ou d'incident.

Les résultats de ces revues sont consignés et présentés lors des audits internes et des comités de gouvernance sécurité.

4.15.8. Utilisation de services Cloud

Le prestataire n'utilise pas de services Cloud

5. Mesures de conformité et audit

5.1. Audits internes et externes (ETSI EN 319 403)

L'AG procède annuellement à un contrôle de conformité du Prestataire, en tout ou partie. Cet audit est mené par un auditeur externe. En préparation de cet audit, un audit interne est également mené avec la même fréquence.

Pour donner suite à toute modification significative d'une composante du service, l'AG procède à une analyse de sécurité et fait évoluer en conséquence, le cas échéant, les mesures techniques et organisationnelles permettant de maintenir ou d'améliorer le niveau de sécurité attendu.

5.2. Identités / Qualifications des évaluateurs

L'AG choisit et assigne une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité contrôlée.

L'équipe d'audit doit être indépendante et être dûment autorisée à pratiquer les contrôles visés.

L'organisme de supervision national est l'ILNAS.

5.3. Sujets couverts par les évaluations

Les audits de conformité portent sur tout ou partie de l'infrastructure et visent à vérifier le respect des engagements et pratiques définies dans la présente déclaration de pratique.

5.4. Actions correctives à la suite des conclusions des évaluations

A l'issue d'un audit, l'équipe d'audit rend à l'AG, un avis parmi les suivants : « réussite », « échec », « à confirmer ». Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AG qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du Certificat de la composante, la révocation de l'ensemble des Certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AG et doit respecter ses politiques de sécurité internes ;
- En cas de résultat « à confirmer », l'AG remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus ;
- En cas de réussite, l'AG confirme à la composante contrôlée la conformité aux exigences de la PC et de la DPC.

6. Gestion du document

6.1. Procédure de mise à jour et de contrôle de version

Tout projet de modification du présent document doit rester conforme aux exigences de la politique de sécurité du Prestataire, de la norme ETSI 319 401 [319401] et respecter les engagements existants. En cas de changement important, l'AG de l'IGC du Prestataire pourra faire appel à une expertise technique pour en contrôler l'impact.

Sauf en cas d'urgence, le délai d'information concernant les amendements (modifications) est d'un mois.

6.2. Publication et accessibilité (publique / restreinte)

Ce document de déclaration de pratique est un document public. Il est disponible sur le site de publication du Prestataire de service.

6.3. Périodicité des révisions

Le présent document devra faire l'objet d'une revue au moins une fois par an, pouvant entraîner ou non un amendement.

6.4. Responsables du maintien du document

Le Prestataire de service est responsable de ce document. Il s'assure périodiquement que le document est à jour, que son référentiel est correct. Il s'assure également de la cohérence entre ce document et la déclaration de pratique privée détaillant les procédures opérationnelles du service.