Goodflag Signature

Politique et Pratiques du Service de Signature Electronique Qualifiée à Distance

Version 1.0

Date d'entrée en vigueur : 17/04/2026

9 Av Maréchal Leclerc – 10120 ST ANDRE LES VERGERS – FRANCE
Tél. : +33 (0)3 25 43 90 78 – www.goodflag.com
SAS au capital de 26 739 euros – R.C.S. Troyes 480 622 257 – Code APE 5829C – TVA FR01480622257

Table des matières

1 Introduction

1.1 Présentation générale

La société Lex Persona a adopté la marque commerciale Goodflag au début de l'année 2025. Néanmoins, dans le contexte de ce document, le nom Lex Persona est utilisé par souci de compatibilité avec les informations préalablement communiquées à l'organisme français de supervision des services de confiance au titre du règlement [eIDAS].

Dans le cadre de son offre de services de confiance, Lex Persona fournit un Service de Signature Electronique Qualifiée à Distance pour les personnes physiques (SSEQAD).

La Clé Privée de signature du Signataire personne physique est générée et utilisée dans un dispositif qualifié de création de signature (QSCD), opéré par Lex Persona dans un environnement contrôlé et sécurisé, conformément au règlement [eIDAS] et aux standards ETSI et EN applicables, sans jamais quitter ce dispositif, dans le cadre d'une Transaction initiée par un Utilisateur.

Il est important de noter que le Signataire ne contacte jamais de sa propre initiative le SSEQAD : c'est un Module de Création de Signature (MCS), édité par Lex Persona, qui appelle le SSEQAD de manière sécurisée et qui, à son tour, déclenche son composant d'interaction avec le Signataire, appelé Parcours de Consentement, à l'aide d'un protocole également sécurisé. De même, le SSEQAD ne manipule jamais les documents à signer définis par la Transaction initiée par un Utilisateur, mais uniquement leur empreinte SHA 256, préalablement calculée par le MCS. Le fonctionnement détaillé du Parcours de Consentement et du MCS ainsi que leurs Conditions Générales d'Utilisation sont en dehors du périmètre du présent document.

Le présent document décrit les règles, exigences et pratiques mises en œuvre par Lex Persona pour la fourniture du SSEQAD pour les personnes physiques, et constitue la Politique de Service de Signature Electronique Qualifiée à Distance (PSSEQAD) et sa Déclaration des Pratiques de Service associée (DPSSEQAD).

1.2 Identification du SSEQAD

Le SSEQAD est identifié par l'identifiant d'objet (OID) 1.3.6.1.4.1.22542.100.3.1.

1.3 Identification du document

La présente PSSEQAD/DPSSEQAD est identifiée par l'OID 1.3.6.1.4.1.22542.100.3.1.1 qui permet de la référencer de manière unique dans les environnements techniques et documentaires concernés.

Les valeurs d'OID peuvent être amenées à évoluer ou à être complétées dans le cadre de l'évolution de l'offre de services, sous le contrôle du Lex Persona Trust Service Provider Board (LPTSP Board). Toute modification majeure de la PSSEQAD/DPSSEQAD fait l'objet d'une mise à jour du présent document, du dernier indice de son OID et d'une publication dans le dépôt d'informations officielles de Lex Persona.

L'OID de la présente politique permet aux Clients, aux auditeurs, aux autorités de supervision et aux parties tierces de se référer précisément au corpus de règles qui encadre le SSEQAD.

1.4 Déclaration de conformité

Le SSEQAD est un service de confiance de création de signature électronique qualifiée à distance, qui s'appuie notamment :

- Sur un service de délivrance de Certificat qualifié conforme à [ETSI_319_411-2] au niveau QCP-n-qscd, et dont la Clé Privée associée à la Clé Publique figurant dans le Certificat est stockée dans un QSCD qualifié à distance, lui-même s'appuyant ;
- Sur un service de gestion de QSCD à distance conforme à [ETSI_119_431-1] au niveau NSP + EUSPv2 et dont la politique fait l'objet du présent document.

1.5 Entités intervenant dans le SSEQAD

Le SSEQAD met en jeu plusieurs entités ayant des rôles et responsabilités distincts, qui interviennent à différents niveaux du cycle de vie des signatures qualifiées. Certaines de ces entités sont communes aux autres services de confiance opérés par Lex Persona et sont décrites de manière globale dans la Politique Générale des Services de Confiance [PGSC]. D'autres sont spécifiques au SSEQAD, notamment en lien avec l'utilisation d'un QSCD distant, l'activation des signatures, et la relation entre les Signataires et les Clés Publiques.

Les principales entités intervenant dans le cadre du SSEQAD sont décrites dans les sous-sections suivantes. Les responsabilités détaillées des entités transverses, telles que définies dans la [PGSC], restent applicables et sont complétées, le cas échéant, par les dispositions particulières du présent document.

1.5.1 LPTSP Board

Le SSEQAD est placé sous la responsabilité du LPTSP Board. Le LPTSP Board est représenté par Lex Persona. Il est composé des membres suivants :

- Le responsable du LPTSP Board, qui est un représentant légal de Lex Persona ;
- Des intervenants spécialisés dans le Management de la Sécurité des Systèmes d'Information, nommés par le responsable du LPTSP Board.

Les missions principales du LPTSP Board dans le cadre du SSEQAD sont les suivantes :

- Rédiger et approuver la PSSEQAD/DPSSEQAD ;
- Approuver le corpus documentaire associé au SSEQAD ;
- Définir le processus d'examen et de mise à jour de la PSSEQAD/DPSSEQAD ;
- Définir et attribuer les rôles de confiance au sein du SSEQAD ;
- Approuver le rapport annuel d'audit interne des composantes du SSEQAD et, plus largement ;
- S'assurer que le SSEQAD demeure conforme aux exigences légales, réglementaires, normatives et contractuelles applicables.

1.5.2 SSEQAD

Le SSEQAD est l'ensemble des composants, procédures et dispositifs mis en œuvre par Lex Persona pour permettre la création de Signature Electronique Qualifiée à Distance (SEQAD) pour les

personnes physiques, à partir de Clés Privées de type RSA 3072 bits stockées dans un QSCD distant. Le SSEQAD inclut, notamment, les éléments suivants :

- Les interfaces applicatives permettant aux Utilisateurs de soumettre des demandes de signature aux Signataires ;
- Le module d'activation de signature, appelé Signature Activation Module (SAM), dans la suite du présent document ;
- Les composants assurant le lien avec les Moyens d'Identification Electronique (MIE) notifiés ;
- Les dispositifs cryptographiques qualifiés de type Hardware Security Module (HSM) assurant la génération et la protection des Clés Privées ;
- Ainsi que les fonctions de journalisation, de preuve et d'archivage.

Le SSEQAD s'appuie sur une Autorité de Certification (AC) délivrant des Certificats qualifiés, opérée dans l'Infrastructure de Gestion de Clés (IGC) de Lex Persona, pour l'émission des Certificats qualifiés associés aux signatures générées à distance.

1.5.3 Fournisseur du SSEQAD (FSSEQAD)

Le FSSEQAD est responsable de la fourniture du SSEQAD durant l'ensemble de son cycle de vie, en mettant en œuvre les composants techniques, les services associés et les mesures organisationnelles nécessaires. Dans ce document le FSSEQAD est Lex Persona.

1.5.4 Autorité d'Enregistrement (AE)

Les missions principales de l'AE dans le cadre du SSEQAD consistent à collecter et vérifier les informations d'identité nécessaires pour permettre l'émission de Certificats qualifiés ou la création de SEQAD.

Pour les personnes physiques, l'AE exploite notamment les données issues d'un MIE notifié de niveau élevé ou équivalent, ainsi que les informations fournies par l'Utilisateur dans la demande de signature.

1.5.5 Client

Le Client est une entité légale qui a contractualisé avec Lex Persona pour l'utilisation du SSEQAD par des Utilisateurs pour mettre en œuvre des parcours de SEQAD pour des Signataires personnes physiques.

Le Client est responsable, notamment, de la configuration fonctionnelle du SSEQAD, des CGU proposées aux Utilisateurs des MCS, et aux Signataires, lorsqu'il est en charge de la relation avec ces derniers, ainsi que de la conformité de ses propres traitements de données aux exigences légales applicables.

Dans le cas où Lex Persona met en œuvre le SSEQAD pour ses propres besoins (besoins de signature internes et externes, Goodflag Community, etc.), Lex Persona endosse alors les responsabilités d'un Client.

1.5.6 Utilisateur

L'Utilisateur est une personne physique habilitée par le Client à mettre en œuvre le SSEQAD par le biais d'un MCS pour des usages exclusivement définis par le Client, conformément au contrat conclu entre le Client et Lex Persona. Dans le contexte du présent document, l'Utilisateur doit être compris dans le sens de celui qui déclenche une demande de signature de documents par un ou plusieurs Signataire(s).

La mise en œuvre du SSEQAD par l'Utilisateur peut s'effectuer soit à l'aide d'applications interactives, soit par le biais d'API. Ces applications et API et leurs Conditions Générales d'Utilisation respectives sont en dehors du périmètre du présent document.

1.5.7 Signataire

Un Signataire est une personne physique identifiée qui utilise le SSEQAD pour signer des documents électroniques. Le Signataire peut être rattaché ou non à une entité légale. Dans le cadre de la SEQAD, la Bi-Clé de signature du Signataire est générée de manière éphémère dans le QSCD distant, et est utilisée pour signer les documents d'une Transaction déterminée, puis détruite immédiatement à l'issue de cette Transaction.

Le Signataire est identifié au moyen d'un MIE notifié au niveau élevé ou équivalent, et doit donner un consentement explicite pour chaque opération de signature.

Le Signataire s'engage à utiliser le SSEQAD uniquement dans le respect des lois et réglementations applicables, ainsi que des CGU mises à sa disposition.

1.5.8 Utilisateur de Signature (US)

Un US est une personne physique qui s'appuie sur les SEQAD produites par le SSEQAD pour vérifier l'intégrité de documents signés à l'aide du SSEQAD et l'identité du Signataire.

Les US peuvent être des destinataires de documents signés, des systèmes applicatifs tiers ou des autorités administratives ou judiciaires. Ils sont amenés à se fier au statut des Certificats qualifiés correspondants, à la validité des chaînes de certification, ainsi qu'aux informations publiées par les AC concernées.

Les US doivent vérifier les signatures conformément aux bonnes pratiques de validation, en s'appuyant sur des logiciels de validation de signature électronique conformes aux spécifications techniques pertinentes et, le cas échéant, aux recommandations publiées par les autorités compétentes.

1.6 Usage du SSEQAD

Le SSEQAD permet de produire, conformément au règlement [eIDAS], des SEQAD pour des personnes physiques.

L'usage du SSEQAD pour les personnes physiques concerne principalement la signature de documents électroniques dans le cadre de parcours de signature initiés par des Utilisateurs, par exemple des procédures contractuelles, des approbations internes ou des démarches réglementaires.

La Bi-Clé du Signataire est alors générée dans le QSCD pour une Transaction déterminée, utilisée pour signer les documents de cette Transaction, puis détruite.

Les SEQAD générées ne doivent être utilisées que dans le respect du périmètre fonctionnel défini par la présente PSSEQAD/DPSSEQAD, les documents contractuels applicables et le cadre réglementaire en vigueur.

1.7 Gestion de la PSSEQAD/DPSSEQAD

1.7.1 Entité gérant la PSSEQAD/DPSSEQAD

Lex Persona est l'entité responsable de la gestion de la Politique de Service de Signature Electronique Qualifiée à Distance (PSSEQAD) et de la Déclaration des Pratiques de Service associée (DPSSEQAD). Ses coordonnées sont les suivantes :

LEX PERSONA

9 AVENUE MARECHAL LECLERC

10120 ST-ANDRE-LES-VERGERS

FRANCE

Courriel : pki@sunnystamp.com

Téléphone : +33 (0)3 25 43 90 78

Lex Persona s'assure que la PSSEQAD/DPSSEQAD demeurent adaptées au fonctionnement réel du SSEQAD, qu'elles prennent en compte l'évolution des exigences réglementaires, normatives et contractuelles applicables, et qu'elles sont alignées avec la [PGSC].

1.7.2 Entité déterminant la conformité de la PSSEQAD/DPSSEQAD

Le LPTSP Board détermine la conformité de la PSSEQAD/DPSSEQAD en réalisant des audits et des contrôles de conformité. Il s'appuie, pour ce faire, sur les résultats des audits internes, des audits externes de certification ou de qualification, ainsi que sur les rapports de contrôles opérationnels menés par les équipes de Lex Persona.

Le LPTSP Board veille à ce que les exigences définies dans la présente politique soient effectivement appliquées par les équipes opérationnelles et techniques, et que les éventuels écarts identifiés fassent l'objet de plans de remédiation documentés et suivis. Il décide, le cas échéant, des modifications à apporter à la PSSEQAD/DPSSEQAD pour maintenir un niveau de conformité satisfaisant.

1.7.3 Procédure d'approbation de la conformité de la PSSEQAD/DPSSEQAD

Le LPTSP Board approuve la PSSEQAD/DPSSEQAD après avoir déterminé leur conformité, au regard des exigences internes, réglementaires et normatives applicables.

Toute version nouvelle ou révisée de la politique fait l'objet d'un processus formalisé comprenant la rédaction ou la mise à jour du texte, la revue par les parties prenantes internes concernées, la validation par la direction et l'approbation finale par le LPTSP Board.

Une fois approuvée, la nouvelle version de la PSSEQAD/DPSSEQAD est publiée sur le site Web de Goodflag, et, le cas échéant, aux autorités de supervision compétentes.

Les versions antérieures sont archivées afin de permettre, si nécessaire, des analyses historiques ou des vérifications dans le cadre d'audits.

1.8 Définitions et Acronymes

1.8.1 Définitions

Les définitions suivantes sont utilisées dans le cadre de la présente PSSEQAD. Lorsque ces définitions recoupent des termes définis dans la [PGSC], cette dernière fait foi pour les aspects généraux, et la présente politique précise les éléments spécifiques au SSEQAD.

Application Programming Interface (API)

Interface logicielle permettant de « connecter » un logiciel ou un produit à un autre logiciel ou produit afin d'échanger des données et des fonctionnalités.

Autorité de Certification (AC)

Entité qui, au sein d'un Prestataire de Services de Confiance, a en charge, au nom et sous la responsabilité de ce prestataire, l'application d'au moins une PC/DPC et est identifiée comme telle dans les Certificats qu'elle émet. Dans le présent document, l'AC sans épithète désigne l'AC « Sunnystamp Natural Persons CA », qui délivre des Certificats qualifiés générés à la volée et éphémère sur la base d'une authentification réalisée à l'aide d'un MIE de niveau élevé ou équivalent.

Autorité d'Enregistrement (AE)

Entité chargée de l'identification des Signataires, ainsi que de la gestion des demandes de Certificats.

Bi-Clé

Combinaison d'une Clé Privée et d'une Clé Publique utilisée pour effectuer des opérations cryptographiques.

Certificat

Ensemble d'informations garantissant l'association entre l'identité d'une personne physique ou morale et une Clé Publique, grâce à une signature électronique de ces données effectuée à l'aide de la Clé Privée de l'AC qui délivre le Certificat. Un Certificat contient des informations telles que : la Clé Publique et l'identité de son propriétaire, ses usages autorisés, la durée de vie du Certificat, la Signature électronique du Certificat par l'AC et son identité, etc. Le format standard de Certificat est défini dans la recommandation X.509 v3 et dans la RFC 5280. Dans le cadre de la présente PSSEQAD/DPSSEQAD, un Certificat désignera généralement celui utilisé par le Signataire pour signer et qui lui est délivré « à la volée » par l'AC « Sunnystamp Natural Persons CA » gérée par Lex Persona et dédié à une Transaction.

Clé Privée

Clé d'une Bi-Clé d'une entité devant être utilisée exclusivement par cette entité.

Clé Publique

Clé d'une Bi-Clé d'une entité pouvant être rendue publique.

Client

Voir 1.5.5.

Déclaration des Pratiques de Service de Signature Electronique Qualifiée A Distance (DPSSEQAD)

Ce document décrit les pratiques opérationnelles mises en œuvre pour respecter la PSSEQAD.

Fournisseur d'Identité

Entité chargée d'identifier et d'authentifier les Signataires. Le Fournisseur d'Identité, après avoir vérifié l'identité du Signataire, produit un Jeton d'Identité attestant de cette identité qui est ensuite vérifié par le SSEQAD.

Jeton d'Identité

Données numériques signées, produite par un Fournisseur d'Identité et attestant de l'identité d'un Signataire.

Module de Création de Signature (MCS)

Le MCS est un module édité par Lex Persona, qui fonctionne à l'initiative d'un Utilisateur, en vue de faire signer un ou plusieurs document(s) par un ou plusieurs Signataire(s). En particulier, il calcule l'empreinte SHA 256 des documents qui sont ensuite intégrées à une Transaction de signature destinée a un Signataire concerné. Une fois la Transaction effectuée avec succès, le MCS intègre la/les signature(s) électronique(s) produite(s) par le SSEQAD au(x) document(s) concerné(s). Lex Persona propose différents MCS (mono-signataire, multi-signataires), en fonction des besoins métiers des Clients.

Parcours de Consentement

Ensemble d'interactions entre le SSEQAD et le Signataire, déclenché lors de l'exécution d'une Transaction, au cours duquel le Signataire va visualiser le(s) document(s) à signer, accepter les CGU de la Transaction, s'authentifier et confirmer sa volonté de signer le(s) document(s) de la Transaction. Voir description détaillée au paragraphe 5.4.

Politique de Service de Signature Electronique Qualifiée à Distance (PSSEQAD)

Désigne le présent document.

Service de Signature Electronique Qualifiée à Distance (SSEQAD)

Désigne le service décrit dans ce document pour la création de SEQAD.

Signataire

Voir 1.5.7.

Signature Activation Data (SAD) : Données d'activation permettant au Signataire d'autoriser l'opération de signature.

Signature Activation Module (SAM)

Composante qui met en œuvre les données d'activation de signature et assure que l'utilisation de la Clé Privée se fait sous le contrôle exclusif du signataire. Le SAM est chargé d'interpréter la demande de signature, de collecter la SAD et d'autoriser l'opération au QSCD distant.

Transaction : Opération déclenchée à l'initiative d'un Utilisateur qui fait signer un ou plusieurs document(s) par un Signataire.

Utilisateur

Voir 1.5.6.

Utilisateur de Signature (US)

Voir 1.5.8.

1.8.2 Acronymes

AC : Autorité de Certification

AE : Autorité d'Enregistrement

API : Application Programming Interface

CGU : Conditions Générales d'Utilisation

CSR : Certificate Signing Request

DPC : Déclaration des Pratiques de Certification

DPSSEQAD : Déclaration des Pratiques du Service de Signature Electronique Qualifiée à Distance

FSSEQAD : Fournisseur de Service de Signature Electronique Qualifiée à Distance

HSM : Hardware Security Module

MCS : Module de Création de Signature

MIE : Moyen d'Identification Electronique

OIDC : OpenID Connect

PC : Politique de Certification

PGSC : Politique Générale des Services de Confiance

PKCS : Public Key Cryptographic Standard

PSSEQAD : Politique du Service de Signature Electronique Qualifiée à Distance

QSCD : Qualified Signature Creation Device

SAM : Signature Activation Module

SEQAD : Signature Electronique Qualifiée à Distance

SNP : Sunnystamp Natural Persons CA

SSCD : Secure Signature Creation Device

SSEQAD : Service de Signature Electronique Qualifiée à Distance

UC : Utilisateur de Certificat

US : Utilisateur de Signature

1.9 Documents associés

1.9.1 Documents normatifs

Les documents normatifs suivants sont utilisés comme références pour la conception, la mise en œuvre et l'évaluation du SSEQAD. Ils peuvent être mis à jour ou complétés en fonction de l'évolution du cadre réglementaire ou normatif. Parmi ces documents figurent notamment :

[eIDAS]

Il s'agit du *Règlement (UE) N° 910/2014 du Parlement Européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*, abrogeant la *Directive 1999/93/CE*, modifié par la *Directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022*, modifié par le *Règlement (UE) 2024/1183 du Parlement Européen et du Conseil du 11 avril 2024*, rectifié par le *Rectificatif paru au JO L 90317 du 9.4.2025, p. 1 (2024/1183)*. Dans le contexte de la présente PSSEQAD/DPSSEQAD, il s'entend également complété du *règlement d'exécution concernant la gestion des dispositifs de création de signature électronique qualifiés à distance et des dispositifs de création de cachets électroniques qualifiés à distance*.

[ETSI_119_431-1]

ETSI TS 119 431-1 V1.3.1 (2024-12). Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev.
https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.03.01_60/ts_11943101v010301p.pdf.

[ETSI_319_411-1]

ETSI EN 319 411-1 V1.3.1 (2021-05). Policy and security requirements for Trust Service Providers issuing certificates. Part 1: General requirements.

https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.03.01_60/en_31941101v010301p.pdf.

[ETSI_319_411-2]

ETSI EN 319 411-2 V2.4.1 (2021-11). Policy and security requirements for Trust Service Providers issuing certificates. Part 2: Requirements for trust service providers issuing EU qualified certificates. *https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.03.01_60/en_31941102v020301p.pdf*.

[ETSI_319_412-1]

ETSI EN 319 412-1 V1.4.4 (2021-05). Certificate Profiles. Part 1: Overview and common data structures.
https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.04.04_60/en_31941201v010404p.pdf.

[ETSI_319_412-2]

ETSI EN 319 412-2 V2.2.1 (2020-07). Certificate Profiles. Part 2: Certificate profile for certificates issued to natural persons.

https://www.etsi.org/deliver/etsi_en/319400_319499/31941202/02.02.01_60/en_31941202v020201p.pdf.

[EN_419_241-1]

NF EN 419241-1 juillet 2018. Systèmes fiables de serveur de signature électronique — Partie 1 : Exigences de sécurité générales du système. *https://www.boutique.afnor.org/fr-fr/norme/nf-en-4192411/systemes-fiables-de-serveur-de-signature-electronique-partie-1-exigences-de/fa188045/81349*.

[EU_QSCD]

Liste des dispositifs qualifiés de création de signature et de création de cachet et des dispositifs sécurisés de création de signature. *https://eidas.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD*.

[Linux_Config_ANSSI]

Recommandations de configuration d'un système GNU/Linux.
https://messervices.cyber.gouv.fr/documents-guides/linux_configuration-en-v2.pdf.

[PC_RG2]

Politique de Certification de l'Autorité de Certification « Sunnystamp Root CA G2 ». *https://pki2.sunnystamp.com/repository*.

[PC_SNP]

Politique de Certification de l'Autorité de Certification « Sunnystamp Natural Persons CA ». *https://pki2.sunnystamp.com/repository*.

[PKCS#11]

PKCS #11 Cryptographic Token Interface Base Specification Version 3.0. Committee Specification 01. 19 December 2019. *https://docs.oasis-open.org/pkcs11/pkcs11-base/v3.0/cs01/pkcs11-base-v3.0-cs01.html*.

1.9.2 [PGSC]

La [PGSC] de Lex Persona décrit les exigences communes à l'ensemble des services de confiance opérés par Lex Persona, notamment les aspects de gouvernance, de sécurité générale, de gestion des risques, de gestion des ressources humaines, de gestion des fournisseurs, de journalisation et d'audit.

La [PGSC] est publiée sur le dépôt officiel de Lex Persona à l'adresse suivante :

https://pki2.sunnystamp.com/repository.

Sauf mention contraire, les dispositions de la [PGSC] s'appliquent au SSEQAD et sont complétées par les exigences spécifiques de la présente PSSEQAD/DPSSEQAD.

1.9.3 Autres politiques et référentiels internes

Le SSEQAD s'appuie sur une AC nommée « Sunnystamp Natural Persons CA » (SNP) pour l'émission des Certificats qualifiés utilisés dans le cadre des SEQAD.

La PC/DPC de cette AC [PC_SNP], ainsi que la PC/DPC celle de l'AC racine qui l'a délivrée « Sunnystamp Root CA G2 » [PC_RG2] sont publiées dans le dépôt de Lex Persona. Ces documents décrivent les exigences spécifiques relatives aux Certificats émis, aux profils utilisés, aux conditions de délivrance, de suspension et de révocation, ainsi qu'aux obligations des différentes parties prenantes.

La présente PSSEQAD/DPSSEQAD s'inscrit dans la continuité de ces politiques et en respecte les contraintes.

1.9.4 Référentiels externes complémentaires

Le choix et la qualification des dispositifs utilisés comme QSCD pour le SSEQAD s'appuient sur la liste européenne des dispositifs qualifiés de création de signature et de cachet [EU_QSCD]. [EU_QSCD] recense les dispositifs certifiés conformément au règlement [eIDAS] et reconnus comme QSCD ou SSCD à l'échelle de l'Union européenne.

Le module HSM utilisé dans le cadre du SSEQAD figure dans [EU_QSCD], et sa configuration est conforme au certificat de QSCD qui lui est associé. Les références exactes du dispositif et de son certificat de qualification sont tenues à disposition dans le corpus documentaire technique de Lex Persona et peuvent être communiquées aux auditeurs ou autorités compétentes sur demande.

Le module SAM développé et opéré par Lex Persona et utilisé dans le cadre du SSEQAD, est le seul module applicatif exécuté par un serveur Linux dédié et durci au niveau « Enhanced » selon [Linux_Config_ANSSI].

2 Publication et responsabilités de repository

2.1 Entité chargée de la publication

Lex Persona est responsable de la mise à disposition des informations devant être publiées dans le cadre de ses services de confiance, y compris le SSEQAD.

Lex Persona est responsable de la publication et de la mise à disposition des documents relatifs au SSEQAD.

À ce titre, Lex Persona gère un dépôt documentaire (repository) permettant d'accéder aux documents suivants :

- La PSSEQAD/DPSSEQAD (le présent document ;
- Les CGU du Parcours de Consentement du SSEQAD ;
- La [PGSC] ;
- Les documents techniques publiés relevant du périmètre du SSEQAD ;
- Les informations nécessaires pour vérifier la validité des signatures réalisées via le SSEQAD ;
- Toute mise à jour de ces documents.

Le repository officiel de Lex Persona est accessible à l'adresse suivante :

https://pki2.sunnystamp.com/repository

2.2 Informations devant être publiées

Les informations devant être publiées dans le cadre du SSEQAD sont définies dans la présente PSSEQAD/DPSSEQAD, dans la [PGSC] et dans les PC/DPC des AC concernées. Il s'agit notamment des documents suivants, sans que cette liste soit exhaustive :

- La version en vigueur de la PSSEQAD/DPSSEQAD ;
- Les versions obsolètes archivées lorsque leur consultation est nécessaire pour vérifier des opérations passées ;
- La [PGSC] ;
- Les PC/DPC des AC utilisées ;
- Les informations nécessaires à la vérification des Certificats et des signatures ;
- Les CGU destinées aux signataires lorsque celles-ci sont mises à disposition par Lex Persona.

Lex Persona peut également publier d'autres documents jugés pertinents pour les Clients, Signataires ou Utilisateurs de Signature.

2.3 Délais et fréquences de publication

Lex Persona met à jour et publie les documents du repository dès qu'une nouvelle version entre en vigueur.

Les mises à jour peuvent notamment intervenir dans les cas suivants :

- Evolution réglementaire ou normative ;
- Evolution technique du SSEQAD ;
- Modification organisationnelle impactant le SSEQAD ;
- Mise à jour du périmètre documentaire.

Les informations liées au SSEQAD sont publiées dès que nécessaire afin d'assurer à tout moment la cohérence entre les informations délivrées et les engagements de Lex Persona.

Lex Persona garantit la disponibilité et l'intégrité des informations publiées.

Toute nouvelle version de la PSSEQAD/DPSSEQAD est publiée dès sa mise en service, après son approbation par le LPTSP Board.

2.4 Contrôles d'accès aux informations publiées

Sauf indication contraire, les documents publiés par Lex Persona dans le repository sont publics et librement accessibles.

Certains documents internes ou sensibles ne sont pas publiés. Leur diffusion est restreinte au personnel autorisé ou aux auditeurs mandatés, conformément aux règles définies dans la [PGSC].

L'accès en modification au système de publication des informations est strictement limité aux fonctions internes habilitées de Lex Persona.

Cet accès en modification requiert une authentification forte.

3 Identification et authentification

3.1 Principes généraux

Le SSEQAD repose sur un ensemble cohérent de mécanismes permettant d'assurer que les Clés Privées utilisées pour la création de SEQAD sont liées à des identités préalablement vérifiées, dans le respect des exigences du règlement [eIDAS] et des standards ETSI et EN applicables.

Pour les personnes physiques, l'identification et l'authentification des Signataires s'appuient sur des Moyens d'Identification Electronique notifiés de niveau élevé ou équivalent.

Le lien entre l'identité et la Clé de Publique est matérialisé par un Certificat qualifié, émis par l'AC SNP, et par des éléments de preuve conservés par le SSEQAD.

Les mécanismes d'enrôlement, de création de Bi-Clé, de génération de CSR, d'émission de Certificat et de collecte du consentement sont conçus pour garantir que seule la personne peut faire usage de la Clé Privée qui lui est associée.

Dans le cadre du SSEQAD, les fonctions de contrôle de l'activation de la signature sont assurées par un SAM. Ce composant intervient de manière transversale pour appliquer les décisions issues des mécanismes d'identification et d'authentification décrits dans le présent chapitre.

Le SAM ne constitue pas un dispositif de création de signature qualifié et n'est pas certifié en tant que tel. Il est toutefois implémenté et exploité dans un environnement de sécurité résistant aux altérations, conformément aux hypothèses de sécurité et aux exigences décrites dans les standards [ETSI_119_431-1] et [EN_419_241-1]. Notamment, le SAM est le seul module applicatif hébergé sur un serveur exécutant un système d'exploitation durci au niveau « Enhanced » selon [Linux_Config_ANSSI] et non connecté au réseau Internet, et qui met en œuvre des mesures techniques et organisationnelles destinées à prévenir toute modification non autorisée, tout contournement des contrôles d'authentification et d'autorisation, ou toute activation frauduleuse de la Clé Privée. Cette architecture a été définie conforme aux recommandations d'une analyse de risque disponible en accès restreint aux organismes d'évaluation de la conformité et aux autorités de supervision.

Le SAM ne permet en aucun cas l'accès direct aux Clés Privées et n'effectue aucune opération cryptographique de signature, ces opérations étant réalisées exclusivement au sein du QSCD. Son rôle est strictement limité au contrôle logique de l'activation, à la vérification des conditions d'autorisation et à l'orchestration sécurisée des appels vers le QSCD, garantissant ainsi que l'utilisation de la Clé Privée reste sous le contrôle exclusif des entités autorisées.

3.2 Identification et authentification des personnes physiques

Pour les personnes physiques, l'identification et l'authentification dans le cadre du SSEQAD s'appuient sur l'utilisation d'un MIE notifié de niveau élevé ou équivalent, conformément aux exigences applicables aux signatures qualifiées.

Ce MIE notifié est opéré par un Fournisseur d'Identité approuvé :

- France Identité (niveau élevé) ;
- Identité Numérique La Poste (niveau substantiel jusqu'au 21/05/2026 et selon décision de l'ANSSI pour une extension au-delà de cette date au titre de l'article 24-1-c du règlement [eIDAS]).

L'Utilisateur, via une application ou une API habilitée, initie une Transaction en fournissant les informations d'identité de la personne physique devant signer :

- Le nom ;
- Le prénom ;
- Le pays de naissance.

Le Signataire est ensuite redirigé vers le fournisseur de MIE, où il s'authentifie selon les modalités propres à ce moyen d'identification.

À l'issue de cette authentification, un jeton OpenID Connect (OIDC) est fourni au SSEQAD, contenant les attributs d'identité attestés par le MIE. Le SSEQAD compare ces attributs aux informations d'identité initialement fournies par l'Utilisateur, en intégrant une tolérance contrôlée pour les accents et caractères spéciaux.

Si les informations concordent, la Transaction se poursuit et la génération de la Bi-Clé éphémère est autorisée. Dans le cas contraire, le processus est interrompu. Ce mécanisme assure que

l'identité du Signataire correspond bien à celle attendue par l'Utilisateur et que la signature produite est liée à cette identité identifiée de manière fiable.

3.3 Lien identité – MIE

Le lien entre l'identité du Signataire personne physique et le MIE utilisé est un élément déterminant de la sécurité du SSEQAD.

Le MIE notifié fournit une preuve d'authentification forte, et le jeton OIDC retourné contient les attributs d'identité du Signataire, tels qu'enregistrés par le fournisseur de MIE.

Le SSEQAD met en œuvre un rapprochement entre ces attributs et les informations d'identité présentes dans la demande de signature, afin de s'assurer de la cohérence de l'ensemble. Lorsque ce lien est établi, les informations d'identité issues du jeton OIDC sont utilisées pour constituer le contenu des Certificats éphémères générés pour la Transaction.

Le SSEQAD conserve les preuves nécessaires pour démontrer que l'identité associée à la Clé Privée utilisée pour signer a été vérifiée selon un niveau de garantie compatible avec les exigences du règlement [eIDAS].

3.4 Lien identité – Clé Publique de signature

Le lien entre l'identité et la Clé Publique de signature est réalisé par l'intermédiaire d'une CSR signée par la Clé Privée générée dans le QSCD et d'un Certificat qualifié émis sur la base de cette CSR.

Pour les personnes physiques, la Bi-Clé éphémère est générée dans le QSCD une fois l'identification et l'authentification du Signataire validées. Une CSR au format ASN.1 est produite, contenant les informations d'identité du Signataire issues du jeton OIDC et la Clé Publique de la Bi-Clé de signature. Cette CSR est signée avec la Clé Privée éphémère, ce qui fournit une preuve de possession de la Clé Privée et garantit l'intégrité de la demande. La CSR est ensuite transmise au service de certification, qui vérifie la signature de la CSR et émet un Certificat qualifié d'une durée d'une heure.

A noter qu'indépendamment de la durée de vie du Certificat qualifié, la Bi-Clé éphémère est automatiquement détruite à l'issue de la Transaction de Signature.

Dans tous les cas, les Certificats émis sont cohérents avec [PC_SNP], et les paramètres cryptographiques utilisés par le SSEQAD sont alignés sur ceux déclarés dans [PC_SNP].

3.5 Lien Certificat – Bi-Clé de signature

Pour les Certificats de signature :

- La CSR est signée par la Clé Privée générée dans le QSCD ;
- L'AC vérifie la signature de la CSR ;
- Le secret dérivé ECDH assure que la CSR correspond bien à la Transaction active ;
- Le Certificat contient la Clé Publique correspondant à la Clé Privée non exportable du QSCD.

Le secret dérivé n'est pas utilisé après l'émission :

- Il sert uniquement à vérifier que la Clé-Publique utilisée dans la CSR appartient à la Transaction authentifiée du Signataire.

3.6 Contrôles et traçabilité

Le SSEQAD met en œuvre des mécanismes de contrôle et de traçabilité visant à assurer que l'ensemble des opérations d'identification, d'authentification, de génération de Bi-Clé, de création de CSR, d'émission de Certificat, d'activation de signature et de collecte de consentement laisse des traces exploitables.

Ces journaux d'événements sont collectés dans un système de gestion des logs et de corrélation (SIEM), permettant d'assurer le suivi des opérations sensibles, de détecter les anomalies et de disposer des éléments nécessaires en cas d'audit, de contrôle réglementaire ou de gestion d'incident de sécurité.

Les informations journalisées incluent notamment :

- Les identifiants techniques des Transactions ;
- Les horodatages ;
- Les identités impliquées ;
- Les références de Certificats ;
- Et les résultats des vérifications effectuées.

La conservation de ces journaux est assurée pendant une durée compatible avec les exigences réglementaires et contractuelles applicables, et des mesures de protection de l'intégrité et de la confidentialité des logs sont mises en place. Ces éléments permettent de démontrer que le lien [identité - Clé Publique - Certificat] est correctement géré et que les signatures générées peuvent faire l'objet d'une analyse a posteriori fiable.

4 Génération des Bi-Clés de signature

La génération des Bi-Clés de signature personne physique est réalisée exclusivement dans un QSCD certifié et selon une procédure maîtrisée, garantissant l'intégrité des Clés Privées, leur non-exportation, leur traçabilité et leur usage contrôlé.

Les algorithmes et tailles des Bi-Clés sont définis et validés par le LPTSP Board.

4.1 Dispositif de génération et initialisation

La génération des Bi-Clés de signature utilisées dans le cadre du SSEQAD repose sur l'utilisation d'un dispositif cryptographique certifié, configuré en tant que QSCD à distance conformément au règlement [eIDAS].

Le module utilisé est un module HSM de type Thales Luna SA 7, certifié au niveau EAL4+ et qualifié comme QSCD à distance dans [EU_QSCD].

Ce module assure :

- La génération de Bi-Clé RSA 3072 bits dans un environnement sécurisé ;
- La protection des Clés Privées ;
- La mise en œuvre des opérations de signature sans que les Clés Privées ne quittent le périmètre du QSCD.

L'initialisation du module est réalisée par deux Administrateurs distincts, selon une procédure documentée qui prévoit :

- La configuration des partitions ;
- L'activation des mécanismes de sécurité matériels ;
- La mise en place d'un canal sécurisé de type Secure Trusted Channel ;
- La production d'un procès-verbal signé décrivant les opérations réalisées.

Cette initialisation garantit que le dispositif est conforme à son certificat QSCD et que les partitions utilisées pour le SSEQAD sont isolées et protégées.

4.2 Génération des Bi-Clés de signature pour une personne physique

Pour les personnes physiques, la Bi-Clé de signature est générée sous forme de Bi-Clé éphémère, créée à la volée dans le QSCD pour une Transaction donnée et détruite à l'issue de cette Transaction ou à l'expiration du Certificat associé.

Après l'identification et l'authentification réussies du Signataire via un MIE notifié de niveau élevé ou équivalent, et la collecte de son consentement explicite, le SSEQAD déclenche la génération d'une Bi-Clé RSA 3072 bits dans le QSCD.

Une CSR est alors produite, contenant :

- La Clé Publique,
- Les informations d'identité du Signataire issues du jeton d'identification OIDC.

La CSR est signée par la Clé Privée éphémère afin de démontrer la possession de cette Clé Privée.

La CSR est transmise à l'AC SNP qui, après vérification, émet un Certificat qualifié d'une validité d'une heure.

La Clé Privée est utilisée uniquement pour signer les documents de la Transaction en cours, puis la Bi-Clé est automatiquement détruite à la fin de la Transaction ou en cas de défaillance.

Aucune sauvegarde ni export de la Clé Privée n'est possible, ce qui garantit un haut niveau de sécurité et de conformité aux standards ETSI et EN applicables.

4.3 Paramètres cryptographiques et cohérence avec les PC/DPC

Les paramètres cryptographiques utilisés dans le cadre du SSEQAD sont définis dans la présente politique et validés par le LPTSP Board, en cohérence avec les exigences des standards ETSI applicables et les PC/DPC des AC concernées.

Pour les signatures, les Bi-Clés sont générées avec :

- L'algorithme RSA ;
- Une taille minimale de 3072 bits.

Les Certificats émis par l'AC suivent les profils définis dans les standards [ETSI_319_412-1] et [ETSI_319_412-2], et l'usage des Clés Publiques est limité à la fonction de signature, selon l'OID concerné dans [PC_SNP].

Le SSEQAD veille à ce que les paramètres de génération de Bi-Clé dans le QSCD soient strictement alignés avec ceux déclarés dans [PC_SNP] pour l'émission des Certificats correspondants.

Cette cohérence garantit que :

- La chaîne de confiance cryptographique est homogène ;
- Les signatures peuvent être vérifiées sans ambiguïté ;
- Les exigences de sécurité et de conformité sont pleinement respectées.

4.4 Non exportation des Clés Privées

Les Clés Privées générées dans le cadre du SSEQAD ne doivent en aucun cas être exportées en clair hors du QSCD.

Les partitions du module HSM utilisées pour le SSEQAD sont configurées de manière à interdire l'extraction des Clés Privées, leur marquage comme non exportables et non extractibles étant systématique.

Pour les Bi-Clés de signature éphémères :

- Aucune opération d'export n'est mise en œuvre ;
- Aucune sauvegarde n'est réalisée ;
- Aucune duplication n'est autorisée.

Le SSEQAD met en place des contrôles techniques et organisationnels afin de s'assurer que ces politiques de non-exportation sont respectées en toutes circonstances.

4.5 Conformité au certificat QSCD et aux exigences ETSI et EN

La configuration et l'utilisation du module HSM en tant que QSCD pour le SSEQAD sont conformes au certificat de qualification délivré pour ce dispositif et aux exigences techniques décrites dans les standards ETSI et EN applicables, notamment [ETSI_119_431-1] et [EN_419_241-1].

Lors de l'initialisation du QSCD, les paramètres de sécurité, les mécanismes d'authentification, les politiques de gestion des partitions et les protections contre les attaques logiques ou physiques sont configurés conformément aux recommandations du fabricant et aux exigences du certificat QSCD.

Des audits et contrôles réguliers sont réalisés afin de vérifier que cette configuration reste conforme dans la durée, y compris en cas de mise à jour logicielle, de modification de l'architecture ou d'ajout de nouveaux services.

Le SSEQAD s'assure également que l'environnement global, dans lequel le QSCD est intégré, respecte les contraintes décrites dans les référentiels de qualification, de manière à garantir que la qualification s'applique bien à l'ensemble de la solution et pas seulement au composant matériel isolé.

5 Cycle de vie des Bi-Clés de signature

5.1 Principes généraux applicables au cycle de vie des Bi-Clés

Le cycle de vie des Bi-Clés utilisées dans le cadre du SSEQAD pour les personnes physiques repose sur un ensemble de processus contrôlés, couvrant l'activation, la gestion, l'utilisation, la protection, la suppression, la sauvegarde éventuelle et, le cas échéant, la restauration des Clés Privées.

L'objectif fondamental est de garantir que ces Bi-Clé, éphémères pour les SEQAD, ne puissent être générées, manipulées ou utilisées que conformément aux exigences du règlement [eIDAS], aux standards ETSI et EN applicables et aux procédures internes du FSSEQAD.

Ces mécanismes assurent que seul le Signataire peut activer la Clé Privée, que celle-ci demeure dans un QSCD à tout moment, que toute utilisation est tracée, et que la fin de vie des Bi-Clés est maîtrisée dans des conditions sécurisées.

5.2 Activation des Bi-Clés

Pour une personne physique, l'activation d'une Bi-Clé de signature éphémère repose entièrement sur un mécanisme d'authentification forte basé sur un MIE notifié de niveau élevé ou équivalent.

La procédure commence toujours par l'identification et l'authentification du Signataire via un Fournisseur d'Identité qualifié. Une fois la preuve d'identité reçue sous forme de jeton OIDC signé et vérifié, le SEQAD s'assure de la validité temporelle de la Bi-Clé en question, dont la durée de vie est intrinsèquement limitée à une heure en raison de la nature éphémère des Certificats délivrés.

Le Signataire exprime ensuite son consentement explicite au travers du SSEQAD, en consultant les documents, en acceptant les CGU du Parcours de Consentement du SSEQAD relatives à la Transaction et déclenchant volontairement la signature.

Lorsque toutes ces conditions d'accès sont validées, la Clé Privée est activée à l'intérieur du QSCD pour générer la signature. Cette Clé Privée n'est jamais accessible au Signataire, n'est jamais exportée, et n'est utilisable que pour la Transaction en cours.

Enfin, la Bi-Clé est détruite automatiquement dès la fin de la Transaction ou en cas d'erreur, garantissant que la signature ne puisse jamais être réutilisée de manière frauduleuse.

5.3 Gestion des Transactions

La gestion des Transactions est directement liée à la nature éphémère de la Clé Privée utilisée pour la signature.

Chaque Transaction correspond exclusivement à la durée de vie de la Bi-Clé générée à la volée. Cette Bi-Clé est créée pour une Transaction unique et ne subsiste que pour le temps strictement nécessaire à son exécution, en général quelques secondes à quelques minutes.

Cependant, une limite maximale d'une heure est fixée afin de garantir que la Bi-Clé et son Certificat associé ne puissent être utilisés au-delà de leur durée de validité.

Une Transaction peut être fermée volontairement, ou automatiquement après l'acte de signature, ou encore interrompue et détruite en cas d'erreur technique, de perte de connexion ou de défaut de validation du consentement.

Toutes les opérations réalisées durant la Transaction sont enregistrées et intégrées au fichier de preuve, qui permet d'attester de la conformité de la Transaction.

Ce fonctionnement garantit une utilisation minimale et strictement contrôlée des Bi-Clés, tout en empêchant toute réutilisation ou compromission ultérieure puisque la Clé Privée est détruite immédiatement après usage.

5.4 Parcours de Consentement du Signataire

Le consentement du Signataire est un élément central du processus de signature électronique qualifiée, puisqu'il garantit que la création de la signature découle d'une volonté explicite, libre et éclairée.

Pour les personnes physiques, le consentement est collecté via le Parcours de Consentement du SSEQAD, dans le cadre d'une Transaction de signature qui comporte les étapes suivantes :

- Le Signataire peut tout d'abord consulter les documents à signer et vérifier leur contenu ;
- Le Signataire confirme ensuite qu'il accepte les CGU de la Transaction ;
- Le Signataire s'authentifie avec un MIE de niveau élevé ou équivalent ;
- Le Signataire exprime son accord en cliquant manuellement sur le bouton "Signer".

Ce Parcours de Consentement constitue la confirmation explicite que le Signataire souhaite créer une SEQAD avec la Clé Privée générée spécifiquement pour sa Transaction.

Toutes les étapes du Parcours de Consentement, telles que l'affichage des documents, l'acceptation des CGU, la confirmation de la volonté de signer du Signataire, etc., sont conservées dans le fichier de preuve associé à la Transaction.

Cette conservation permet au FSSEQAD de démontrer, en cas de contestation ou d'audit, que la signature a été créée avec l'accord explicite du Signataire et dans des conditions conformes aux exigences du règlement [eIDAS].

5.5 Vérification du Certificat avant usage

Le Certificat qualifié utilisé pour les signatures de personnes physiques est éphémère, c'est-à-dire qu'il n'existe que pour la durée limitée de la Transaction et ne peut être révoqué en pratique, conformément aux exigences ETSI.

Avant toute utilisation, le Service de signature vérifie la validité temporelle du Certificat, s'assure que sa chaîne de certification est correcte, que le Certificat appartient bien au Signataire authentifié, et que sa période de validité n'est pas expirée.

La courte durée de vie du Certificat, qui ne peut dépasser une heure, élimine la nécessité de vérifier son état de révocation via OCSP ou CRL, puisque cela n'a pas de sens pour un tel Certificat éphémère ne survivant pas à l'opération.

Le système vérifie également l'intégrité du Certificat émis par l'AC et s'assure que celui-ci correspond bien à la Clé Privée stockée dans le QSCD.

Ces mécanismes garantissent que la signature générée repose sur une identité fraîchement vérifiée et sur un Certificat dont l'usage est strictement limité à la Transaction en cours.

5.6 Suppression et destruction des Bi-Clés

La suppression des Bi-Clés éphémères utilisées par les personnes physiques est un élément essentiel de la sécurité du SSEQAD, car elle garantit que personne ne peut réutiliser ou détourner une Clé Privée déjà employée dans une Transaction.

Dès que l'opération de signature prend fin, et que le Certificat éphémère associé a accompli son rôle, la Bi-Clé est détruite automatiquement par le QSCD.

Cette destruction intervient également lorsque la Transaction échoue, est interrompue ou dépasse la limite temporelle d'une heure.

Aucune sauvegarde, exportation, duplication ou copie temporaire n'est réalisée pour ces Bi-Clé.

Le système journalise toutes les opérations liées à la création et à la destruction de la Bi-Clé, permettant de démontrer que les pratiques opérationnelles respectent strictement les exigences du règlement [eIDAS] et ETSI, ainsi que les règles de sécurité propres au FSSEQAD.

Ainsi, la Bi-Clé éphémère est utilisée strictement une seule fois et disparaît dès que son usage n'est plus légitime.

5.7 Sauvegarde des Bi-Clés

Aucune sauvegarde n'est effectuée pour les personnes physiques.

5.8 Restauration des Bi-Clés

Aucune restauration des Bi-Clés de personnes physiques n'est effectuée.

5.9 Copies et occurrences de la Bi-Clé

Aucune copie et occurrence de Bi-Clé de personnes physiques n’est possible.

6 Exigences opérationnelles sur les opérations de signature

6.1 Principes généraux applicables aux opérations de signature

Les opérations réalisées par le SSEQAD visent à produire des signatures électroniques qualifiées pour des personnes physiques dans des conditions permettant d'assurer la conformité au règlement [eIDAS], la maîtrise des risques et la traçabilité complète de chaque action sensible.

Le SSEQAD est conçu pour garantir :

- Que l'utilisation de la Clé Privée intervient exclusivement dans un QSCD ;
- Que l'activation de la signature est soumise à une authentification explicite ;
- Que le Signataire conserve le contrôle de l'acte de signature.

Les opérations suivent une séquence cohérente qui inclut :

- L'identification du Signataire ;
- L'authentification du Signataire ;
- L'expression du consentement ;
- La préparation des données à signer ;
- La création de la signature dans le QSCD ;
- La constitution des éléments de preuve.

Les contrôles de sécurité associés s'appuient sur des mesures techniques et organisationnelles décrites dans la présente politique et, pour les exigences communes, dans la [PGSC]. Toute anomalie détectée au cours d'une opération conduit à l'arrêt du processus, à la journalisation de l'événement et, lorsque nécessaire, à l'ouverture d'un traitement d'incident conformément aux procédures internes.

6.2 Déclenchement et déroulement d'une SEQAD pour une personne physique

Pour une personne physique, une opération de SEQAD est initiée par une application cliente qui connaît au préalable l'identité attendue du signataire, notamment le nom, le prénom et le pays de naissance.

Le SSEQAD vérifie ensuite cette identité par l'intermédiaire d'un Moyen d'Identification Electronique notifié au niveau élevé ou équivalent. Le signataire s'authentifie auprès du Fournisseur d'Identité, puis un jeton OIDC est retourné et contrôlé.

Les attributs d'identité contenus dans ce jeton OIDC sont comparés à ceux fournis dans la demande de signature, avec une tolérance contrôlée sur les accents et caractères spéciaux. Lorsque l'égalité est constatée, la Transaction se poursuit.

La Bi-Clé de signature est alors générée à la volée dans le QSCD. Une CSR au format ASN.1 est construite avec l'identité validée et la Clé Publique, puis signée avec la Clé Privée afin d'établir la preuve de possession et l'intégrité de bout en bout. Le Certificat qualifié éphémère est émis par l'AC et utilisé uniquement pour la Transaction.

Le consentement du signataire est collecté via la page de consentement gérée par le SSEQAD, avec acceptation explicite des CGU et action volontaire de déclenchement de la signature.

La Transaction est bornée par la durée de vie du Certificat et de la Bi-Clé, avec une limite maximale d'une heure. A la fin de la Transaction, la Clé Privée est détruite automatiquement, y compris en cas d'échec, afin d'empêcher toute réutilisation.

6.3 Données d'activation de signature et contrôle de l'acte de signature

Le SSEQAD met en œuvre des données d'activation de signature afin de s'assurer que la Clé Privée n'est utilisée que sous le contrôle du Signataire et uniquement dans le cadre prévu.

Pour les Signataires, les données d'activation s'inscrivent dans le Parcours de Consentement, avec :

- La visualisation par le Signataire des documents à signer ;
- L'acceptation par le Signataire des CGU du Parcours de Consentement ;
- L'authentification du Signataire par MIE notifié au niveau élevé ou équivalent ;
- Le consentement explicite du Signataire à la signature des documents à signer ;
- Les contrôles internes à la Transaction réalisés par le SSEQAD avant d'autoriser la génération de la Bi-Clé, la génération de la requête de Certificat, la génération du Certificat, la signature des documents à signer, la suppression de la Bi-Clé.

Les modalités détaillées de formatage, de collecte et de gestion des données d'activation pour le composant d'activation côté SSEQAD sont définies dans le dossier d'architecture et dans le corpus documentaire interne, et elles sont présentées aux auditeurs dans le cadre de la démarche de qualification.

Le code PIN de partition QSCD n'est pas exposé aux utilisateurs et il est réservé au fonctionnement du serveur. Chaque activation déclenche une journalisation complète et une association non ambiguë entre l'auteur de la demande, la Bi-Clé concernée et l'opération réalisée.

Dans le cadre du SSEQAD, les fonctions de contrôle de l'activation de la signature sont assurées par un composant applicatif jouant le rôle de module d'activation de signature (Signature Activation Module - SAM). Ce composant ne constitue pas un QSCD et n'est pas certifié en tant que tel. Il est toutefois implémenté et exploité dans un environnement de sécurité résistant aux attaques, conformément aux hypothèses et exigences décrites dans les standards [ETSI_119_431-1] et [EN_419 241-1].

Notamment, le SAM est un composant logiciel unique, non connecté à Internet et implémenté comme seul composant applicatif unique sur un serveur mis en œuvre à l'aide d'un OS durci au niveau renforcé tel que défini par le guide de l'ANSSI disponible à l'adresse *https://messervices.cyber.gouv.fr/documents-guides/linux_configuration-en-v2.pdf*. Il met en œuvre des mesures techniques et organisationnelles destinées à prévenir toute modification non autorisée, tout contournement des contrôles d'activation ou toute utilisation abusive des données d'activation.

Par ailleurs, le SAM ne permet en aucun cas l'accès direct aux Clés Privées et n'effectue aucune opération cryptographique de signature, celles-ci étant réalisées exclusivement au sein du QSCD.

6.4 Vérifications préalables, validations et conditions d'exécution

Avant de produire une signature, le SSEQAD applique des vérifications destinées à garantir que l'opération est légitime, cohérente et conforme au périmètre contractuel et normatif.

Pour les personnes physiques, les contrôles portent notamment sur :

- La concordance des données d'identité entre la demande et le Jeton d'Identité ;
- La validité temporelle de la Transaction ;
- La cohérence de la chaîne de certification et l'existence d'une ancre de confiance ;
- L'état d'activation interne de la Bi-Clé éphémère.

Compte tenu du caractère éphémère des Certificats, il n'est pas réalisé de contrôle de révocation pour ces Certificats, l'usage étant limité à la Transaction et la Bi-Clé étant détruite en fin de Transaction.

6.5 Constitution des preuves, journalisation et traçabilité des opérations

Chaque Transaction est associée à des preuves et à des journaux permettant d'assurer une traçabilité complète, exploitable en cas d'audit, de contrôle réglementaire ou de contestation.

Pour les personnes physiques, la preuve inclut notamment :

- Les éléments relatifs à l'identification et à l'authentification via le MIE ;
- Les contrôles de concordance d'identité ;
- L'expression du consentement du Signataire ;
- L'horodatage des étapes importantes ;
- Les informations de Transaction nécessaires à la reconstitution du parcours.

Les journaux sont centralisés dans un SIEM, avec collecte des logs systèmes, reverse proxies, composants applicatifs, PKI et Bastion. Les événements incluent les identifiants de Transaction ou d'opération, les horodatages, les empreintes de Certificats présentés, les résultats de contrôle et les erreurs éventuelles.

La disponibilité, l'intégrité et la conservation des journaux suivent les règles décrites dans le corpus de sécurité et, lorsque applicable, dans la [PGSC].

6.6 Gestion des erreurs, interruptions, refus et cas particuliers

Le SSEQAD est conçu pour refuser ou interrompre une opération dès qu'une condition de sécurité ou de conformité n'est pas satisfaite.

Pour les personnes physiques, le refus intervient notamment en cas :

- D'échec d'authentification auprès du MIE ;
- De non-concordance des attributs d'identité ;
- D'absence de consentement explicite ;
- De dépassement de la durée maximale de Transaction.

Toute tentative infructueuse est journalisée et peut déclencher des alertes selon les règles de supervision et de sécurité. En cas d'incident technique affectant la disponibilité du QSCD, de l'application serveur ou des composants de preuve, des procédures de continuité et de reprise d'activité sont appliquées conformément aux dispositions de la [PGSC] et aux procédures internes.

7 Mesures de sécurité non techniques

7.1 Sécurité physique

Les mesures de sécurité physique applicables au SSEQAD sont décrites dans la [PGSC].

Voir chapitre 4.1 de la [PGSC].

Ces mesures s'appliquent notamment aux infrastructures hébergeant les composants du SSEQAD, incluant les environnements applicatifs, les modules QSCD, les systèmes de preuve et les dispositifs de sauvegarde associés.

7.2 Sécurité procédurale

Les mesures de sécurité procédurales mises en œuvre par Lex Persona, incluant la définition des rôles de confiance, la séparation des tâches, les exigences de double contrôle et les mécanismes d'identification et d'authentification des personnels, sont décrites dans la [PGSC.

Voir chapitre 4.2 de la [PGSC].

Ces mesures s'appliquent intégralement aux opérations liées au SSEQAD, notamment pour les activités d'administration des systèmes, de gestion des QSCD, de traitement des incidents et de supervision.

7.3 Sécurité du personnel

Les exigences relatives au personnel intervenant dans le cadre des services de confiance, incluant les conditions de recrutement, les vérifications d'antécédents, la formation initiale et continue, les obligations de confidentialité et les sanctions en cas d'actions non autorisées, sont définies dans la [PGSC].

Voir chapitre 4.3 de la [PGSC].

Ces exigences s'appliquent à l'ensemble des personnels impliqués dans la conception, l'exploitation, la supervision et l'audit du SSEQAD.

7.4 Données d'audit

Les principes et procédures relatifs à la constitution, à la protection, à l'analyse et à la conservation des données d'audit sont définis dans la [PGSC].

Voir chapitre 4.4 de la [PGSC].

Ces dispositions couvrent notamment la journalisation des accès physiques, des accès logiques, des opérations administratives, des opérations cryptographiques réalisées dans les QSCD, ainsi que des événements applicatifs liés au SSEQAD.

7.5 Archivage

Les principes généraux d'archivage applicables aux services de confiance sont définis dans la [PGSC].

Voir chapitre 4.5 de la [PGSC].

En complément, les données archivées spécifiques au SSEQAD comprennent notamment :

- Toutes les versions de la présente PSSEQAD/DPSSEQAD ;
- Les accords contractuels liant le Prestataire aux Clients du SSEQAD ;
- Pour les SEQAD :
    - Les éléments de preuve d'identification et d'authentification du Signataire, incluant les jetons OIDC retournés par les MIE notifiés et les résultats des contrôles de concordance,
    - Les preuves de consentement du Signataire, incluant l'acceptation des CGU, les actions de déclenchement de la signature et les horodatages associés
    - Les éléments techniques nécessaires à la reconstitution du parcours de signature,
- Les journaux d'événements des composants impliqués dans le SSEQAD (applications, systèmes, QSCD, interfaces PKCS#11, Bastion, reverse proxy, systèmes de preuve),
- Les rapports d'audit relatifs au SSEQAD.

Les durées de conservation des archives sont définies en cohérence avec les exigences réglementaires applicables au SSEQAD et, lorsque nécessaire, avec les obligations d'archivage définies dans [PC_SNP] correspondant aux Certificats utilisés par le SSEQAD.

Goodflag conserve les données d'audit liées au SSEQAD 10 ans.

7.6 Gestion des incidents et reprise

Les procédures de remontée, de traitement et de gestion des incidents de sécurité, ainsi que les mécanismes de reprise après sinistre, sont définies dans la [PGSC].

Voir chapitre 4.6 de la [PGSC].

Ces procédures s'appliquent aux incidents affectant les composants du SSEQAD, incluant notamment les QSCD, le SAM, les systèmes applicatifs, les systèmes de preuve et les infrastructures support.

7.7 Continuité du SSEQAD

Les capacités de continuité d'activité et de reprise après sinistre applicables aux services de confiance sont définies dans la [PGSC], au travers des PCA et PRA des services concernés.

Voir notamment les dispositions du chapitre 4.6 de la [PGSC].

Ces mécanismes garantissent le maintien ou la restauration du SSEQAD dans des délais compatibles avec les engagements de disponibilité.

7.8 Fin du SSEQAD

Les principes généraux applicables à la fin de vie d'un service de confiance sont définis dans la [PGSC].

Voir chapitre 4.7 de la [PGSC].

En cas de cessation définitive du SSEQAD, le PSSEQAD met en œuvre une procédure spécifique visant à :

- Notifier les autorités compétentes et les entités affectées, ainsi que les Clients du SSEQAD ;
- Informer publiquement de l'arrêt du SSEQAD et de son périmètre ;
- Arrêter de manière maîtrisée la production de nouvelles SEQAD ;
- Maintenir, pendant les durées requises, la disponibilité des éléments nécessaires à la vérification a posteriori des signatures produites ;
- Assurer la conservation et l'accessibilité des preuves, journaux et archives conformément aux dispositions du chapitre 7.5 ;
- Traiter les Bi-Clés et Certificats selon leur nature :
    - Pour les signatures de personnes physiques reposant sur des Bi-Clés éphémères, aucune révocation dédiée n'est requise, les Bi-Clés étant détruites à l'issue de chaque Transaction,
- Transférer, le cas échéant, certaines obligations de conservation ou de publication à une entité tierce, dans des conditions garantissant l'intégrité, la confidentialité et la disponibilité des données.

8 Mesures de sécurité techniques

8.1 Gestion et protection des Bi-Clés cryptographiques

Les Clés Privées utilisées dans le cadre du SSEQAD sont protégées de sorte qu'elles ne puissent être utilisées que conformément à la présente PSSEQAD/DPSSEQAD et aux exigences du règlement [eIDAS] et des standards ETSI et EN applicables. Cette protection vise en particulier à garantir le contrôle de la Clé Privée, l'impossibilité d'exportation en clair, la traçabilité des opérations sensibles, ainsi que la maîtrise de la fin de vie.

Pour les personnes physiques, les Bi-Clés de signature sont éphémères. Elles sont générées à la volée pour une Transaction donnée, utilisées uniquement pour signer les documents de cette Transaction, puis détruites automatiquement à la fin de la Transaction ou, à défaut, au plus tard à l'expiration du Certificat éphémère associé. Les Clés Privées des Signataires ne sont pas sauvegardées et ne font pas l'objet de séquestre.

Les paramètres cryptographiques (algorithmes, tailles des Bi-Clés, usages) sont définis et validés par le LPTSP Board. Ils sont cohérents avec [PC_SNP] pour les Certificats utilisés dans le cadre du SSEQAD, de sorte à assurer une chaîne de confiance homogène et vérifiable, ainsi qu'une applicabilité conforme aux profils ETSI pertinents.

8.2 Dispositifs cryptographiques du QSCD

La génération et l'utilisation des Clés Privées de signature (personnes physiques) sont réalisées exclusivement dans un dispositif qualifié de création de signature (QSCD) conforme au règlement [eIDAS].

Le QSCD utilisé est un module cryptographique certifié Common Criteria EAL4+, en l'occurrence un Thales Luna K7 Cryptographic Module version 7.7.2, qualifié comme QSCD, référencé dans [EU_QSCD] et dont le certificat peut être consulté *ici*. Les opérations cryptographiques sont exécutées de manière à garantir que les Clés Privées ne quittent jamais le périmètre du QSCD et qu'aucune extraction non autorisée ne soit possible.

L'exploitation des HSM et des partitions associées au SSEQAD est réalisée exclusivement par des personnels disposant des rôles de confiance requis. Les opérations sensibles réalisées sur le QSCD (initialisation, configuration, opérations nécessitant un contrôle multiple, actions de maintenance ayant un impact sur la sécurité, etc.) sont réalisées selon des procédures documentées et sous double contrôle lorsque nécessaire, avec production d'éléments de traçabilité exploitables.

Le QSCD est configuré et opéré conformément aux conditions prévues par sa certification et aux exigences applicables au SSEQAD. Les canaux de communication vers les HSM sont établis à travers des canaux sécurisés, logiquement distincts des autres canaux de communication, assurant une authentification de bout en bout, l'intégrité et la confidentialité des données transmises,

8.3 Contrôle des accès logiques

Le contrôle des accès logiques vise à garantir que seules les personnes et entités autorisées peuvent accéder aux systèmes, aux fonctions et aux composants nécessaires à la fourniture du SSEQAD, et que ces accès sont limités au strict nécessaire. Les objectifs de sécurité applicables incluent la gestion des droits des Utilisateurs, la gestion des comptes, l'identification et l'authentification fortes, la traçabilité des actions, la protection contre toute tentative non autorisée d'accès aux ressources, ainsi que la protection des informations sensibles contre la divulgation.

Voir chapitre 5.2 de la [PGSC].

Dans le cadre du SSEQAD, le contrôle d'accès logique s'applique notamment :

- Aux accès des personnels internes disposant de rôles de confiance ;

- Aux accès applicatifs et administratifs aux composants du SSEQAD (composants de preuve, services applicatifs, interfaces d'administration, bastion, supervision, SIEM, systèmes de publication, etc.) ;
- Aux accès nécessaires aux opérations de signature, lesquels sont conditionnés par les mécanismes d'identification, d'authentification, de consentement, et par les contrôles de cohérence décrits dans la présente politique.

Les droits et habilitations sont attribués et retirés selon des procédures alignées avec la gestion des ressources humaines, et les accès sensibles sont soumis à des mécanismes d'authentification forte. Toute action est tracée de sorte à pouvoir être imputable à la personne l'ayant effectuée. Les journaux d'accès et d'exécution des opérations sont collectés et analysés conformément aux dispositions d'audit, de supervision et de détection des anomalies.

8.4 Sécurité réseau

Voir chapitre 5.4 de la [PGSC].

Les principes suivants s'appliquent dans le cadre du SSEQAD :

- L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires ;
- Le système d'information est segmenté en réseaux ou zones en fonction de l'analyse de risques, et les communications entre zones sont limitées au strict nécessaire ;
- Les systèmes utilisés pour l'administration sont isolés sur un réseau d'administration dédié et cloisonné ;
- Les environnements de production sont séparés des environnements de développement et de test ;
- La communication vers les HSM n'est établie qu'à travers des canaux sécurisés, logiquement distincts, assurant l'authentification de bout en bout, l'intégrité et la confidentialité ;
- Des analyses de vulnérabilité régulières et des tests d'intrusion sont réalisés selon les modalités prévues.

Ces dispositions s'appliquent aux composants supportant la signature qualifiée à distance, y compris aux flux nécessaires aux échanges avec les composants de preuve, aux services d'identification, aux interfaces de gestion et aux dispositifs cryptographiques.

8.5 Sécurité des systèmes et durcissement

Voir chapitre 5.2 de la [PGSC].

Les objectifs de sécurité applicables incluent notamment :

- L'identification et l'authentification forte des utilisateurs pour l'accès aux systèmes ;
- La mise en œuvre du principe de moindre privilège, la séparation des rôles et le contrôle multiple ;

- La modification et la suppression rapide des droits d'accès ;
- La traçabilité des actions afin de permettre leur imputabilité ;
- La protection des informations sensibles contre la divulgation, y compris en cas de réutilisation de ressources ;
- La protection contre les tentatives non autorisées d'accès logique et, lorsque applicable, la cohérence avec les mesures de sécurité physiques.

Les configurations, durcissements, mises à jour et opérations d'exploitation sont réalisés par le personnel compétent et habilité, conformément aux rôles de confiance et aux procédures applicables. Les systèmes supportant la production des signatures, la journalisation, la collecte des preuves, les interfaces d'administration et les composants de supervision sont maintenus dans un état cohérent avec les objectifs de sécurité décrits dans la [PGSC] et les exigences spécifiques du SSEQAD.

8.6 Cycle de vie logiciel

Voir chapitre 5.3 de la [PGSC].

Les développements affectant le SSEQAD sont documentés et réalisés via un processus de manière à en assurer la qualité. La configuration des systèmes et des composantes, ainsi que toute modification et mise à niveau, est documentée et contrôlée. Un cloisonnement est opéré entre l'environnement de développement et les environnements de préproduction et de production.

Les configurations et les mises à jour des applications sont effectuées de manière sécurisée par le personnel compétent apparaissant dans les rôles de confiance. Les évolutions ayant un impact sur la sécurité, sur les mécanismes de signature, sur l'intégrité des preuves ou sur la disponibilité du SSEQAD font l'objet de contrôles appropriés et de validations conformes aux pratiques internes. Ces dispositions contribuent à prévenir l'introduction de vulnérabilités.

8.7 Gestion et protection des SAD

Les données d'activation de signature (SAD) sont gérées et protégées de manière à garantir que l'utilisation de la Clé Privée intervient uniquement sous le contrôle du signataire (personne physique), et uniquement dans le cadre prévu par le SSEQAD. Les SAD sont protégées contre la divulgation, la modification et l'utilisation non autorisée, et leur utilisation est tracée.

Pour les personnes physiques, les SAD s'inscrivent dans le parcours de signature et reposent sur :

- L'authentification via un MIE notifié de niveau élevé ou équivalent ;
- Le consentement explicite collecté via le composant de preuve ;
- Les contrôles de Transaction réalisés avant l'autorisation d'utiliser la Clé Privée éphémère.

Les modalités opérationnelles de gestion des SAD côté SSEQAD s'appuient sur un SAM non connecté à Internet et appelé uniquement par le SSEQAD. Le module SAM développé et opéré par Lex Persona et utilisé dans le cadre du SSEQAD, est le seul module applicatif exécuté par un serveur Linux dédié et durci au niveau « Enhanced » selon [Linux_Config_ANSSI] tel qu'attendu par [ETSI_119_431-1] et [EN_419_241-1]. Le SAM est utilisé de sorte à garantir que l'activation de la

signature n'est possible qu'après réalisation des contrôles requis et que la Clé Privée ne peut être utilisée en dehors du parcours prévu.

8.8 Continuité technique

La continuité technique vise à maintenir ou rétablir, dans des conditions maîtrisées, la capacité du SSEQAD à produire des SEQAD, ainsi qu'à préserver l'intégrité des journaux, des preuves et des éléments nécessaires à la vérification a posteriori. Les objectifs et mesures transverses (supervision, détection, segmentation, sauvegardes, reprise) sont définis par les politiques et procédures de Lex Persona et, lorsque applicable, par les dispositions de la [PGSC].

La continuité technique tient compte des dépendances critiques du service, notamment :

- La disponibilité des composants applicatifs supportant l'identification, le consentement et la constitution des preuves ;
- La disponibilité du QSCD et la capacité à établir des canaux sécurisés vers celui-ci ;
- La disponibilité des mécanismes d'authentification nécessaires au déclenchement des opérations de signature ;
- La disponibilité des systèmes de journalisation et du SIEM permettant d'assurer la traçabilité et la détection d'anomalies.

En cas d'incident affectant un composant critique, les dispositions de reprise s'appliquent afin de restaurer la capacité de service dans des délais cohérents avec les engagements applicables. Lorsque la continuité ne peut pas être assurée, le service est conçu pour refuser ou interrompre les opérations afin de préserver la sécurité, la conformité et l'intégrité des éléments probants. Les événements significatifs sont journalisés, et les procédures internes de gestion d'incident et de reprise sont appliquées conformément au corpus documentaire et aux exigences communes décrites dans la [PGSC].

9 Audit de conformité et autres évaluations

Voir chapitre 6 de la [PGSC].

10 Autres problématiques métiers et légales

10.1 Tarifs

Dans le cadre de son SSEQAD, le Prestataire peut appliquer un tarif concernant l'accès au service, l'utilisation des fonctionnalités de signature, ainsi que les prestations associées.

Les modalités tarifaires applicables aux Certificats qualifiés utilisés dans le cadre du service restent cohérentes avec celles définies dans [PC_SNP].

10.2 Responsabilité financière

10.2.1 Couverture par les assurances

Voir chapitre 7.2.1 de la [PGSC].

10.2.2 Autres ressources

10.2.3 Couvertures et garanties concernant les entités utilisatrices

Les conditions de couverture et de garantie applicables aux entités utilisatrices du SSEQAD sont définies dans la politique spécifique du service et dans les accords contractuels conclus avec les Clients.

10.3 Confidentialité

Les règles générales relatives à la confidentialité des données professionnelles sont définies au chapitre 7.3 de la [PGSC].

Dans le cadre du SSEQAD, sont notamment considérées comme confidentielles :

- Les procédures internes liées au service de signature ;
- Les Clés Privées mises en œuvre dans les QSCD ;
- Les données d'activation de signature ;
- Les journaux d'événements et éléments de preuve ;
- Les dossiers d'enrôlement et d'enregistrement spécifiques au SSEQAD.

Les informations rendues publiques, notamment celles figurant dans les Certificats ou sur les sites de publication, ne sont pas considérées comme confidentielles.

10.4 Protection des données personnelles

Les dispositions générales relatives à la protection des données à caractère personnel sont définies au chapitre 7.4 de la [PGSC].

Dans le cadre du SSEQAD , les données personnelles traitées incluent notamment :

- Les données d'identification des signataires personnes physiques ;
- Les éléments de preuve associés aux opérations de signature ;
- Les journaux et traces nécessaires à la conformité réglementaire et à la valeur probante des signatures.

Ces données sont traitées conformément au RGPD, aux lois nationales applicables et aux engagements contractuels du Prestataire.

10.5 Droits de propriété intellectuelle

Voir chapitre 7.5 de la [PGSC].

Les droits de propriété intellectuelle afférents aux composants logiciels, documentations, procédures et services mis en œuvre dans le cadre du SSEQAD demeurent la propriété de Lex Persona ou de ses ayants droit.

10.6 Interprétations contractuelles et garanties

Les principes généraux applicables aux interprétations contractuelles et aux garanties sont définis au chapitre 7.6 de la [PGSC].

Dans le cadre du SSEQAD :

- Lex Persona s'engage à mettre en œuvre les moyens techniques, humains et organisationnels nécessaires à la fourniture du service dans des conditions garantissant sécurité, disponibilité et conformité réglementaire ;
- Le LPTSP Board assure la gouvernance, l'approbation des politiques, la gestion des rôles de confiance et le suivi de la conformité du service ;
- Les obligations respectives du Prestataire, des Clients, des Signataires et des Utilisateurs finaux sont précisées dans la présente politique et dans les documents contractuels associés.

10.7 Notifications individuelles et communications entre les participants

Les modalités de notification et de communication entre les participants au service sont définies au chapitre 7.11 de la [PGSC].

Toute nouvelle version de la présente politique est publiée après validation par le LPTSP Board sur le site de publication du Prestataire.

10.8 Amendements de la Politique

Voir chapitre 7.12 de la [PGSC].

Les amendements mineurs peuvent être effectués sans notification préalable, tandis que toute modification substantielle donne lieu à une information des parties concernées et, le cas échéant, à l'attribution d'un nouvel OID.

10.9 Limite de responsabilité

Les limites de responsabilité applicables au SSEQAD sont définies dans les conditions contractuelles et dans la politique spécifique du service.

La responsabilité du Prestataire ne saurait être engagée en cas :

- D'utilisation non conforme du service ou des Certificats ;
- De fourniture d'informations erronées par le Client, le Signataire ;
- De dommages indirects, pertes financières ou pertes de données, dans les limites prévues par la législation applicable.

10.10 Gestion des litiges

Voir chapitre 7.13 de la [PGSC].

Une procédure de gestion des incidents et de résolution des différends est mise en place par le LPTSP Board et s'applique également au SSEQAD.

10.11 Loi applicable

Voir chapitre 7.14 de la [PGSC].

La présente politique est soumise au droit français.

10.12 Conformité aux législations et réglementations

Voir chapitre 7.15 de la [PGSC].

Le SSEQAD est conforme :

- Au règlement [eIDAS] ;
- Aux standards ETSI et EN applicables, notamment [ETSI_119_431-1] ;
- Aux législations nationales et européennes en vigueur.