Goodflag Cachetage

Politique et Pratiques du Service de Cachet Electronique Qualifié 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 Cachet Electronique Qualifié à Distance (SCEQAD) pour des Sujets de type personne morale.

La Clé Privée de cachet d'un Sujet est générée et stockée 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. Cette Clé Privée, ne quitte jamais ce dispositif, et est strictement utilisée sous le contrôle exclusif d'une personne physique nommée Responsable de la Clé Privée du Sujet (RCPS), dans le cadre de Transactions initiées par ce dernier.

Il est important de noter que le RCPS ne contacte jamais de sa propre initiative le SCEQAD : c'est un Module de Création de Cachet (MCC), édité par Lex Persona, qui appelle le SCEQAD de manière sécurisée et qui, à son tour, déclenche le cachet électronique des données. De même, le SCEQAD ne manipule jamais les documents à signer définis par la Transaction initiée par le RCPS, mais uniquement leur empreinte SHA 256, SHA384 ou SHA 512, préalablement calculée par le MCC. Le fonctionnement détaillé du MCC ainsi que ses 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 SCEQAD, et constitue la Politique de Service de Cachet Electronique Qualifié à Distance (PSCEQAD) et sa Déclaration des Pratiques de Service associée (DPSCEQAD).

1.2 Identification du SCEQAD

Le SCEQAD est identifié par l'identifiant d'objet (OID) 1.3.6.1.4.1.22542.100.3.2.

1.3 Identification du document

La présente PSCEQAD/DPSCEQAD est identifiée par l'OID 1.3.6.1.4.1.22542.100.3.2.1 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 PSCEQAD/DPSCEQAD 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 SCEQAD.

1.4 Déclaration de conformité

Le SCEQAD est un service de confiance de création de cachet électronique qualifié à distance, qui s'appuie notamment :

- Sur un service de délivrance de Certificat qualifié conforme à [ETSI_319_411-2] au niveau QCP-l-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 SCEQAD

Le SCEQAD met en jeu plusieurs entités ayant des rôles et responsabilités distincts, qui interviennent à différents niveaux du cycle de vie des cachets qualifiés. 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 SCEQAD, notamment en lien avec l'utilisation d'un QSCD distant, l'activation des cachets, et la relation entre les Sujets, les RCPS et les Clés Publiques.

Les principales entités intervenant dans le cadre de ce service 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 SCEQAD 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 SCEQAD sont les suivantes :

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

1.5.2 SCEQAD

Le SCEQAD est l'ensemble des composantes, procédures et dispositifs mis en œuvre par Lex Persona pour permettre la création de Cachets Electroniques Qualifiés à Distance (CEQAD) pour les

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

- Les interfaces applicatives permettant au RCPS de soumettre des demandes de cachet ;
- Le module d'activation de signature, appelé Signature Activation Module (SAM) dans la suite du présent document ;
- Les données d'activation de la Clé Privée qui sont communiquées au RCPS ;
- 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 SCEQAD s'appuie sur une Autorité de Certification (AC) qualifiée, opérée dans l'Infrastructure de Gestion de Clés (IGC) de Lex Persona, qui délivre des Certificats qualifiés associés aux cachets générés à distance.

1.5.3 Fournisseur du SCEQAD (FSCEQAD)

Le FSCEQAD est responsable de la fourniture du SCEQAD 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 FSCEQAD est Lex Persona.

1.5.4 Autorité d'Enregistrement (AE)

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

Pour les personnes morales, l'AE gère et contrôle les formulaires de demande de Certificat, signés électroniquement à l'aide d'une signature électronique qualifiée au sens du règlement [eIDAS], par le Représentant Légal (RL) du Sujet et par le RCPS, ce qui permet de garantir leur identité respective. L'AE est gérée et opérée par Lex Persona, laquelle peut déléguer contractuellement certaines opérations à des entités tierces conformément à la [PGSC]. Lex Persona reste, dans tous les cas, responsable des obligations qui lui incombent vis-à-vis des Clients et des Sujets.

1.5.5 Client

Le Client est une Entité Légale qui a contractualisé avec Lex Persona pour l'utilisation du SCEQAD.

Le Client est responsable, notamment, de la configuration fonctionnelle du SCEQAD, de la prise en compte, pour chaque demande de Certificat relative à un Sujet, des Conditions Générales d'Utilisation (CGU) relatives aux Certificats et au(x) MCC, par le RCPS et les Utilisateurs, ainsi que de la conformité de ses propres traitements de données aux exigences légales applicables.

Dans le cadre de l'utilisation du SCEQAD, le Client peut également être la personne morale pour laquelle un ou plusieurs Certificats sont émis et aux noms desquels les documents sont cachetés.

Dans le cas où Lex Persona met en œuvre le SCEQAD pour ses propres besoins (signature simple, fichier de preuve, certificat de preuve, etc.), et dans son propre réseau interne, Lex Persona est alors

considérée comme une Entité Légale qui crée des cachets électroniques qualifiés pour elle-même, en local et non à distance.

1.5.6 Utilisateur

L'Utilisateur est une personne physique habilitée par le Client à mettre en œuvre le SCEQAD par le biais d'un MCC 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 création de CEQAD de documents par un RCPS. Cet Utilisateur peut être à l'initiative de l'exécution d'un programme batch (MCC) qui met en œuvre le Certificat d'authentification et des données d'activation de la Clé Privée du Certificat de cachet détenus par le RCPS.

1.5.7 RCPS

Le RCPS est une personne physique désignée et autorisée par le RL à initier des opérations de cachet relatives à un Certificat de cachet via le SCEQAD.

Le RCPS est authentifié par le SCEQAD au moyen d'un Certificat d'authentification délivré par l'AC et de données d'activation relatives à la Clé Privée du Sujet fournies par l'AC. De plus le RCPS doit disposer du Certificat du Sujet ainsi que de l'adresse du SCEQAD, ces 4 éléments étant nécessaires et suffisants pour permettre au RCPS d'utiliser la Clé Privée du Sujet dans le QSCD et ainsi de déclencher les opérations de cachet des documents.

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

Dans le cadre du SCEQAD, le Sujet est une personne morale au nom de laquelle un Certificat qualifié de cachet est émis. La Clé Privée de cachet associée à ce Certificat est générée et stockée dans le QSCD, et utilisée pour produire des CEQAD.

La relation entre le RCPS, le Sujet, la Clé Privée du Certificat est gérée par l'AE selon des procédures formalisées, et fait l'objet de contrôles documentés et d'une traçabilité complète.

1.5.8 Utilisateur de Cachet (UC)

Un UC est une personne morale qui s'appuie sur les CEQAD produits par le SCEQAD pour vérifier l'intégrité de documents et l'identité du Sujet.

Les UC peuvent être des destinataires de documents cachetés, 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 l'AC concernée.

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

1.6 Usage du SCEQAD

Le SCEQAD permet de produire, conformément au règlement [eIDAS] des CEQAD pour des personnes morales.

L'usage du SCEQAD pour les personnes morales concerne la production de cachets qualifiés sur des documents sous le contrôle de l'entité légale, la Clé Privée de cachet étant stockée de manière persistante dans le QSCD et utilisée sous le contrôle du RCPS.

Les cachets générés ne doivent être utilisés que dans le respect du périmètre fonctionnel et des conditions d'utilisation définis par la présente politique, les documents contractuels applicables et le cadre réglementaire en vigueur.

1.7 Gestion de la PSCEQAD/DPSCEQAD

1.7.1 Entité gérant la PSCEQAD/DPSCEQAD

Lex Persona est l'entité responsable de la gestion de la PSCEQAD et de la DPSCEQAD associée. 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 PSCEQAD/DPSCEQAD demeurent adaptées au fonctionnement réel du SCEQAD, 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 PSCEQAD/DPSCEQAD

Le LPTSP Board détermine la conformité de la PSCEQAD / DPSSCEQAD associée 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 PSCEQAD ou à la DPSCEQAD pour maintenir un niveau de conformité satisfaisant.

1.7.3 Procédure d'approbation de la conformité de la PSCEQAD/DPSCEQAD

Le LPTSP Board approuve la PSCEQAD et la DPSCEQAD 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 PSCEQAD et de la DPSCEQAD est publiée dans le dépôt d'informations officiel de Lex Persona, et les changements sont communiqués aux Clients 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 PSCEQAD. 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 SCEQAD.

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 Legal Persons CA 1 », qui délivre des Certificats qualifiés de personne morale persistants sur la base sur la base d'un processus d'enregistrement géré par l'AE.

Autorité d'Enregistrement (AE)

Entité chargée de l'identification des signataires et des sujets, ainsi que de la gestion des demandes de Certificats ou d'activation de services. Dans le cadre du présent document l'AE est Lex Persona.

Bi-Clé

Combinaison d'une Clé Privée et d'une Clé Publique.

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 PSCEQAD/DPSCEQAD, un Certificat désignera généralement celui utilisé par le RCPS de manière persistante pour cacheter des documents et qui lui est délivré par l'AC « Sunnystamp Legal Persons CA 1 » gérée par Lex Persona.

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 Cachet Electronique Qualifiée A Distance (DPSCEQAD)

Décrit les pratiques opérationnelles mises en œuvre pour respecter cette politique.

Module de Création de Cachet (MCC)

Le MCC est un module édité par Goodflag, qui fonctionne à l'initiative d'un Utilisateur, sous le contrôle du RCPS, en vue de faire cacheter un ou plusieurs document(s) par un Certificat de cachet. En particulier, il calcule l'empreinte SHA 256, SHA 384 ou SHA 512 des documents qui sont ensuite intégrées à une Transaction de cachet. Une fois la Transaction effectuée avec succès, le MCC intègre le(s) cachet(s) électronique(s) produit(s) par le SCEQAD au(x) document(s) concerné(s). Lex Persona propose différents MCC (mono-document, multi-documents), en fonction des besoins métiers des Clients.

Politique de Service de Cachet Electronique Qualifié à Distance (PSCEQAD)

Désigne le présent document.

Représentant Légal (RL)

Le RL est une personne physique disposant des pouvoirs de représenter le Sujet, de par la loi ou de par une délégation de pouvoir, et habilitée à procéder à des demandes d'émission et de révocation de Certificats au bénéfice des Sujets qu'elle aura expressément définis.

Responsable de la Clé Privée du Sujet (RCPS)

Personne physique désignée par le RL de la personne morale titulaire du Certificat de cachet, pour faire usage de la Clé Privée associée à la Clé Publique contenue dans le Certificat et de la conformité de cet usage.

Service de Cachet Electronique Qualifié à Distance (SCEQAD)

Désigne le service décrit dans ce document pour la création de CEQAD à partir de Clés Privées stockées dans un QSCD distant.

Signature Activation Module (SAM)

Composant 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 RCPS. Le SAM est chargé d'interpréter la demande de cachet et d'autoriser l'opération au QSCD distant.

Transaction de cachet

Opération par laquelle un RCPS déclenche des opérations de cachet sur des documents via un MCC.

1.8.2 Acronymes

AC – Autorité de Certification

AE – Autorité d'Enregistrement

CEQAD – Cachet Electronique Qualifié à Distance

CGU – Conditions Générales d'Utilisation

DPC – Déclaration des Pratiques de Certification

DPSCEQAD – Déclaration des Pratiques du Service de Cachet Electronique Qualifié à Distance

HSM – Hardware Security Module

MCC – Module de Création de Cachet

MIE – Moyen d'Identification Electronique

PGSC – Politique Générale des Services de Confiance

PSCEQAD – Politique du Service de Cachet Electronique Qualifié à Distance

RL – Représentant Légal

QSCD – Qualified Signature/Seal Creation Device

SAM – Signature Activation Module

SCEQAD – Service de Cachet Electronique Qualifié à Distance

UC – Utilisateur de Certificat

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 SCEQAD. 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 PSCEQAD/DPSCEQAD, 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_SLP1]

Politique de Certification de l'Autorité de Certification « Sunnystamp Legal Persons CA 1 ». *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 SCEQAD et sont complétées par les exigences spécifiques de la présente PSCEQAD et de la DPSCEQAD associée.

1.9.3 Autres politiques et référentiels internes

Le SCEQAD s'appuie sur une AC qualifiée pour l'émission des Certificats utilisés dans le cadre des CEQAD.

La PC/DPC de l'AC [PC_SLP1], ainsi que celle de l'AC racine « Sunnystamp Root CA G2 » [PC_RG2] et les autres PC/DPC d'autres AC intermédiaires ou finales concernées, 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 PSCEQAD/DPSCEQAD 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 SCEQAD 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 SCEQAD figure dans [EU_QSCD], et sa configuration est conforme au certificat 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 SCEQAD, 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 SCEQAD.

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

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

- La PSCEQAD/DPSCEQAD ;
- La [PGSC] ;
- Les documents techniques publiés relevant du périmètre du SCEQAD ;
- Les informations nécessaires pour vérifier la validité des cachets réalisés via le SCEQAD ;
- 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 SCEQAD sont définies dans la présente PSCEQAD, dans la [PGSC] et dans les politiques de certification des AC concernées. Il s'agit notamment des documents suivants, sans que cette liste soit exhaustive :

- La version en vigueur de la PSCEQAD/DPSCEQAD ;
- 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 cachets ;
- Les conditions générales d'utilisation destinées aux signataires et aux RCPS 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.

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 SCEQAD ;
- Modification organisationnelle impactant le SCEQAD,
- Mise à jour du périmètre documentaire.

Les informations liées au SCEQAD 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 PSCEQAD/DPSCEQAD est publiée immédiatement 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 SCEQAD repose sur un ensemble cohérent de mécanismes permettant d'assurer que les Clés Privées utilisées pour la création de CEQAD 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 morales, l'identification repose sur des documents justificatifs et sur la vérification de la capacité du RL à engager l'Entité Légale, complétée par l'identification et l'habilitation du RCPS.

Le lien entre l'identité et la Bi-Clé de cachet est matérialisé par un Certificat qualifié, émis par une AC qualifiée, et par des éléments de preuve conservés par le SCEQAD.

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 ou entité légitime peut faire usage de la Clé Privée qui lui est associée.

Dans le cadre du SCEQAD, les fonctions de contrôle de l'activation du cachet 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 qualifié de création de cachet et n'est pas certifié en tant que tel. Il est toutefois implémenté et exploité dans un environnement de sécurité résistant aux altérations, conforme 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 cachet, 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 morales et RCPS

Pour les personnes morales, l'identification et l'enrôlement dans le cadre du SCEQAD reposent sur un processus documentaire et contractuel formalisé.

1. Pour les Certificats de cachet, l'identification repose sur un formulaire de demande de Certificat, signé par :

    a. Un RL de la personne morale, ou une personne disposant d'un pouvoir lui permettant de représenter la personne morale, au moyen d'une signature qualifiée conforme au règlement [eIDAS] ;

    b. Le RCPS, également au moyen d'une signature électronique qualifiée conforme au règlement [eIDAS] ;

    c. L'Opérateur d'Enregistrement au moyen d'une signature électronique qualifiée conforme au règlement [eIDAS] .

Le formulaire s'appuie notamment sur :

- Les documents attestant du nom et du numéro d'identification de la personne morale ;

- Les documents attestant de la capacité du Représentant Légal à représenter la personne morale.

2. Lors de cet enrôlement, le RCPS génère dans son environnement une Bi-Clé d'authentification, produit une CSR associée et la transmet à l'AE.

3. L'ensemble du dossier d'enrôlement, comprenant les signatures qualifiées, les documents justificatifs et la CSR du Certificat d'authentification, est revu par l'AE. En particulier l'Opérateur d'Enregistrement vérifie les signatures qualifiées via l'outil officiel de validation mis à disposition par la Commission européenne et hébergé par Lex Persona.

4. Une fois validé, l'AE transmet le dossier à l'AC qui procède alors à sa vérification.

5. Un membre du personnel rattaché à l'AC et disposant du rôle de confiance approprié génère la Bi-Clé du Certificat de cachet dans le QSCD et produit le Certificat de cachet. Il produit également, à partir de la CSR incorporée dans le formulaire, un Certificat d'authentification destiné au RCPS et qui lui fournira ainsi un moyen d'authentification auprès du SCEQAD. Les données d'activation du Certificat de cachet sont quant à elles chiffrées à l'aide de la Clé Publique du Certificat d'authentification du RCPS.

6. L'ensemble des informations nécessaires au RCPS pour créer des CEQAD via le SCEQAD sont alors transmises par l'AC à l'AE qui les transmet au RCPS : le Certificat de cachet et ses données d'activation chiffrées, le Certificat d'authentification ainsi que l'adresse Internet du SCC du SCEQAD.

Ce processus permet notamment de s'assurer que la personne morale est correctement identifiée, que son représentant légal est légitime, que le RCPS est clairement désigné et que les Certificats émis reposent sur des preuves documentaires suffisantes. Il permet également de s'assurer du contrôle exclusif de la Clé Privée du Certificat de cachet par le RCPS.

Lors d'une opération de cachet, l'authentification du RCPS est réalisée comme suit :

1. Le RCPS présente son Certificat d'authentification (authentification mutuelle TLS) ;

2. Le RCPS fournit des données d'activation associées à la Clé Privée du Sujet.

Ces deux éléments sont vérifiés côté serveur, qui établit :

- L'identité du RCPS ;
- Son habilitation à utiliser la Clé Privée du Sujet.

Une fois cette vérification effectuée, l'application serveur s'authentifie auprès du SAM via un mécanisme d'authentification mutuelle TLS.

3.3 Lien identité – données d'activation de la Clé Privée

A travers la configuration du SCC vis-à-vis du Certificat d'authentification et des données d'activation de la Clé Privée, le SCEQAD conserve les preuves nécessaires pour démontrer que l'identité de la personne morale associée à la Clé Privée utilisée pour cacheter a été vérifiée selon un niveau de garantie compatible avec les exigences du règlement [eIDAS].

3.4 Lien identité – Clé Publique de cachet

Le lien entre l'identité et la Clé Publique de cachet 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 morales, la Bi-Clé de cachet est générée dans le QSCD par un membre du personnel rattaché à l'AC et disposant du rôle de confiance approprié, puis une CSR est produite avec la Clé Publique et les informations d'identité du Sujet. Cette CSR est également signée par la Clé Privée de cachet, afin de prouver la possession de cette Clé Privée. L'AC vérifie alors la CSR, émet le Certificat de cachet et transmet le Certificat ainsi généré à l'AE.

Dans tous les cas, les Certificats émis sont cohérents avec [PC_SLP1], et les paramètres cryptographiques utilisés par le SCEQAD sont alignés sur ceux déclarés dans [PC_SLP1].

3.5 Lien Certificat – Bi-Clés de cachet

Pour les Certificats de cachet :

- La Clé Privée du Sujet est non exportable et non extractible ;
- Les objets « Clé Privée », « Clé Publique » et « Certificat » du HSM partagent le même identifiant interne ;
- La CSR signée par la Clé Privée garantit la preuve de possession ;
- L'AC vérifie la CSR et émet le Certificat.

3.6 Contrôles et traçabilité

Le SCEQAD 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-Clés, de création de CSR, d'émission de Certificat, d'activation de cachet 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 – Bi-Clé – Certificat] est correctement géré et que les cachets générés peuvent faire l'objet d'une analyse a posteriori fiable.

4 Génération des Bi-Clés

4.1 Dispositif de génération et initialisation

La génération des Bi-Clés de cachet utilisées dans le cadre du SCEQAD repose sur l'utilisation d'un dispositif cryptographique certifié, configuré en tant que QSCD 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 dans [EU_QSCD].

Ce module assure :

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

L'initialisation du module est réalisée par deux personnes distinctes disposant des rôles de confiance appropriés, 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 SCEQAD sont isolées et protégées.

4.2 Génération des Bi-Clés de Certificat de cachet

Pour les personnes morales, les Bi-Clés de cachet sont générées sous forme de Bi-Clés persistantes, stockées dans le QSCD et utilisées pour produire des cachets qualifiés sur des documents émanant du Sujet.

A la suite de la réception et de la vérification du formulaire de demande de Certificat de cachet, signé par le RL et le RCPS, et après la validation des documents justificatifs par l'AE, une personne disposant du rôle de confiance approprié procède à la génération d'une Bi-Clé RSA 3072 bits dans la partition QSCD dédiée.

Une CSR est ensuite créée, contenant :

- La Clé Publique ;
- Les informations d'identité de la personne morale Sujet.

La CSR est signée par la Clé Privée de cachet afin d'attester de la possession de cette Clé Privée.

Cette CSR est déposée dans le système de gestion des demandes, où une personne rattachée à l'AE et disposant du rôle de confiance approprié vérifie la conformité de la demande, des signatures qualifiées et des informations d'identité avant de transmettre la CSR à l'AC.

L'AC vérifie alors la CSR, émet le Certificat et renvoi les informations à l'AE selon une procédure décrite au chapitre 5. L'AE communique ensuite ces informations au RCPS.

La Clé Privée demeure dans le QSCD pendant toute la durée de validité du Certificat et n'est jamais exportée en clair, les opérations de cachet étant déclenchées par le RCPS au travers du mécanisme d'authentification et des données d'activation décrits dans le chapitre 5.

4.3 Paramètres cryptographiques et cohérence avec les PC/DPC

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

Pour les cachets qualifiés, 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 EN 319 412, et les usages des Bi-Clés sont limités aux fonctions de cachets qualifiés, selon l'OID concerné [PC_SLP1].

Le SCEQAD veille à ce que les paramètres de génération de Bi-Clé dans le QSCD soient strictement alignés avec ceux déclarés dans [PC_SLP1] pour l'émission des Certificats correspondants.

Cette cohérence garantit que :

- La chaîne de confiance cryptographique est homogène ;
- Les cachets peuvent être vérifiés 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 SCEQAD ne doivent en aucun cas être exportées en clair hors du QSCD.

Les partitions du module HSM utilisées pour le SCEQAD 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 cachet persistantes, certaines opérations de sauvegarde chiffrée peuvent être autorisées dans le strict cadre des procédures décrites dans [PC_SLP1], mais ces sauvegardes restent confinées à des HSM dédiés et ne permettent jamais d'obtenir la Clé Privée en clair.

Le SCEQAD 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 SCEQAD 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 SCEQAD 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 cachet

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

Le cycle de vie des Bi-Clés utilisées dans le cadre du SCEQAD 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-Clés persistantes 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 Prestataire.

Ces mécanismes assurent que seule la personne ou l'entité légitime 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 morale

L'accès à cette Bi-Clé nécessite que le Responsable de la Clé Privée du Sujet (RCPS) s'authentifie au moyen de son Certificat d'authentification, généré lors de son enrôlement initial, combiné à des données d'activation spécifique autorisant l'usage de la Clé Privée du Sujet.

Ce processus à deux facteurs assure que seule la personne moralement et contractuellement responsable puisse utiliser la Clé Privée du Sujet.

Lorsque le RCPS initie une opération de cachet, l'application serveur vérifie d'abord l'authenticité du Certificat présenté et la validité des données d'activation fournies, établissant ainsi la légitimité de la demande.

Ensuite, après authentification du RCPS, l'application serveur s'authentifie à son tour auprès du QSCD en utilisant le code PIN de partition qui est connu uniquement du serveur et jamais des RCPS.

L'utilisation de la Clé Privée est strictement contrôlée par le SCEQAD, les autorisations applicatives internes et les journaux d'audit.

Ce mécanisme garantit que chaque utilisation de la Clé Privée est volontaire, authentifiée, autorisée et allouée à une seule identité organisationnelle clairement définie.

5.3 Gestion des sessions de cachet pour une personne morale

Pour les personnes morales, la gestion des sessions implique plusieurs niveaux, en raison du caractère persistant des Clés Privées et de l'existence d'un logiciel serveur intermédiaire entre le RCPS et le QSCD.

La première session, dite applicative, est établie entre le RCPS et l'application cliente, lorsque celui-ci déverrouille son Certificat d'authentification et initie une opération de cachet. Cette session peut être courte ou plus longue, notamment dans le cas de traitements par lots.

La seconde session, dite serveur-HSM, correspond à la connexion établie entre l'application serveur et la partition QSCD contenant la Clé Privée du Sujet. Cette session est authentifiée via le code PIN de partition et permet d'exécuter les opérations cryptographiques sans exposer la Clé Privée.

Les sessions sont surveillées, horodatées et retracées via le SIEM de l'organisation, ce qui garantit une visibilité complète sur les opérations réalisées.

A la fin de chaque opération, ou lorsque le serveur estime qu'aucune autre requête légitime n'est en attente, la session HSM est fermée de manière sécurisée. Ce mécanisme permet d'éviter les dérives, les utilisations prolongées et les accès non autorisés tout en maintenant un niveau élevé de performance opérationnelle.

5.4 Consentement de la personne morale

Le consentement initial du RCPS est obtenu lors de son enrôlement, lorsqu'il signe les conditions générales d'utilisation (CGU) et reçoit son Certificat d'authentification.

En acceptant ces CGU, le RCPS reconnaît être responsable des opérations de cachet qu'il initiera.

Lors de chaque opération, le consentement se manifeste à travers l'action volontaire du RCPS d'utiliser l'application cliente pour transmettre les documents à cacheter.

Le système journalise l'intention du RCPS et les actions entreprises, ce qui permet de démontrer que chaque utilisation de la Clé Privée résulte d'un acte volontaire et autorisé.

Les preuves associées à ces opérations sont conservées conformément aux politiques de conservation du Prestataire, garantissant qu'en cas d'audit ou de litige, la traçabilité du consentement est clairement démontrable et juridiquement opposable.

5.5 Vérification du Certificat avant usage

Pour les personnes morales, les Certificats de cachet ont une durée de validité plus longue et sont soumis aux obligations habituelles de vérification.

Avant chaque utilisation de la Clé Privée du Sujet, l'application serveur vérifie que le Certificat de cachet associé est en cours de validité, qu'il n'a pas été révoqué, et que l'AC émettrice est toujours de confiance.

Cette vérification est effectuée soit via le protocole OCSP, soit via la consultation des CRL publiées par l'AC.

Le système vérifie également que la Clé Privée associée est bien stockée dans le QSCD, que le Sujet est autorisé (via la configuration de l'application) à utiliser sa Clé Privée, et que le RCPS authentifié correspond bien à l'identité administrative habilitée à déclencher la demande.

Ces contrôles renforcent la sécurité et empêchent toute utilisation frauduleuse en cas de compromission ou d'expiration d'un Certificat, garantissant ainsi un fonctionnement conforme aux exigences de sécurité et de traçabilité du règlement [eIDAS].

5.6 Suppression et destruction des Clés Privées des Sujets

Pour les personnes morales, la destruction d'une Clé Privée de cachet peut intervenir dans plusieurs circonstances, notamment l'expiration du Certificat, la compromission suspectée ou avérée, ou la cessation de l'activité liée au Certificat.

Lorsque la destruction est nécessaire, un processus contrôlé est engagé, le système alerte les personnels habilités, puis membre du personnel rattaché à l'AC et disposant du rôle de confiance approprié procède à la suppression de la Bi-Clé à partir du QSCD.

Toutes les copies temporaires utilisées dans les processus de sauvegarde ou de transfert, par exemple celles présentes dans le HSM de backup, sont également détruites.

Un procès-verbal signé consigne l'opération, précisant la date, les identifiants de Bi-Clé et les opérateurs impliqués.

Lorsque la suppression découle de l'expiration d'un Certificat, celle-ci intervient généralement dès le lendemain de la date d'expiration.

Ce processus assure que les Bi-Clés obsolètes ou vulnérables ne subsistent jamais dans le système, maintenant un niveau de sécurité élevé et une conformité continue avec les politiques internes et les exigences de certification.

5.7 Sauvegarde des Bi-Clés des Sujets

Les Bi-Clés des Sujets ne sont pas sauvegardées.

5.8 Restauration des Bi-Clés des Sujets

Sans objet.

5.9 Copies et occurrences des Bi-Clés des Sujets

Pour les personnes morales, une même Clé Privée peut exister simultanément sur plusieurs partitions matérielles, tout en restant protégée au sein du périmètre QSCD.

Une Bi-Clé d'un Sujet existe généralement dans trois environnements :

- La partition active du QSCD de production ;
- La partition passive du même datacenter ;
- Et la partition QSCD du PRA dans un datacenter distant.

Lors d'un transfert sécurisé, une copie temporaire peut exister dans le HSM backup, mais cette copie est supprimée après la réplication vers le PRA, conformément aux procédures internes.

Ce modèle à redondance contrôlée assure une haute disponibilité, tout en préservant la sécurité et la non-exportabilité intrinsèque des Bi-Clés.

L'existence potentielle de copies supplémentaires dans le futur, par exemple en raison d'évolutions logicielles ou matérielles, devra être évaluée sous l'angle réglementaire et de sécurité avant d'être autorisée.

L'objectif est de maintenir un équilibre sain entre résilience opérationnelle, sécurité cryptographique et conformité au règlement [eIDAS].

6 Exigences opérationnelles sur les opérations de cachet

6.1 Principes généraux applicables aux opérations de cachet

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

Le SCEQAD est conçu pour garantir :

- Que l'utilisation de la Clé Privée intervient exclusivement dans un QSCD ;
- Que l'activation de la Clé Privée du Certificat de cachet est soumise à une authentification et à une autorisation explicites ;
- Que l'entité responsable conserve le contrôle de l'acte de cachet.

Les opérations suivent une séquence cohérente qui inclut :

- L'identification ;
- L'authentification ;
- L'autorisation de cachet ;
- La préparation des données à signer ;
- La création du cachet 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 PSCEQAD/DPSCEQAD 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'un CEQAD

Pour une personne morale, l'opération de création d'un CEQAD repose sur :

- Une Clé Privée persistante, générée et stockée dans le QSCD ;
- Un mécanisme d'authentification et d'autorisation du RCPS.

L'accès au SCEQAD est réalisé via une application cliente qui s'authentifie auprès de l'application serveur en utilisant une authentification mutuelle par Certificat. Ce Certificat d'authentification du RCPS est délivré à l'issue de son enrôlement, au cours duquel le RCPS génère sa Bi-Clé d'authentification dans son environnement, transmet une CSR, puis reçoit un Certificat d'authentification émis sur cette base.

Lors d'une opération de cachet, le RCPS présente ce Certificat et déclenche la demande. Des données d'activation distinctes, propres à l'autorisation d'usage de la Clé Privée du Sujet, sont fournies par le RCPS pour confirmer qu'il est bien autorisé à utiliser la Clé Privée du Sujet.

Ces données d'activation correspondent à un secret d'autorisation d'usage de la Clé Privée associée au Certificat de cachet et sont vérifiées côté serveur.

Une fois le RCPS authentifié et l'autorisation validée, l'application serveur s'authentifie auprès du QSCD via le code PIN de la partition, connu uniquement du serveur et des administrateurs habilités. Les opérations cryptographiques de cachet sont effectuées dans le QSCD.

Les sessions entre le serveur et le QSCD peuvent être persistantes pour des raisons opérationnelles, mais chaque opération de cachet est journalisée, associée à l'identité du RCPS et au Certificat du Sujet, et soumise aux contrôles applicatifs d'autorisation définis dans le SCEQAD.

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

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

Pour les personnes morales, les données d'activation reposent sur deux éléments complémentaires :

- L'authentification mutuelle par Certificat du RCPS ;
- Un mot de passe d'autorisation d'usage de la Clé Privée du Sujet.

Ce mot de passe est stocké côté serveur sous forme dérivée en PBKDF2 (Password-Based Key Derivation Function 2) et il est vérifié à chaque opération. Les secrets ou mots de passe transitent via des échanges protégés par TLS avec authentification mutuelle, et ils ne sont pas conservés en clair après usage.

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 Clé Privée concernée et l'opération réalisée.

Dans le cadre du SCEQAD, les fonctions de contrôle de l'activation du cachet 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 cachet, celles-ci étant réalisées exclusivement au sein du QSCD.

6.4 Vérifications préalables, validations et conditions d'exécution

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

Pour les personnes morales, les contrôles incluent :

- L'authentification du RCPS ;
- La validation du mot de passe d'autorisation d'usage de la Clé Privée ;
- La vérification applicative des droits associés ;
- La vérification du statut du Certificat de cachet avant usage, avec contrôle OCSP et ou CRL systématique.

Pour la génération et l'émission du Certificat de cachet, la CSR produite dans le QSCD est associée aux informations d'identité du Sujet, et une validation par un personnel de l'AC ayant un rôle de confiance approprié intervient avant l'émission du Certificat.

6.5 Constitution des preuves, journalisation et traçabilité des opérations

Chaque opération de cachet 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 morales, les preuves reposent sur :

- La journalisation des opérations de l'application serveur ;
- Les traces d'authentification du RCPS ;
- Les journaux liés aux autorisations applicatives ;

- Les traces d'accès et d'opérations PKCS#11 sur le HSM.

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

Pour les personnes morales, l'opération est refusée en cas :

- D'échec d'authentification mutuelle ;
- De Certificat RCPS invalide ;
- De mot de passe d'autorisation incorrect ;
- De droits insuffisants ;
- De statut non valide du Certificat de cachet.

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 SCEQAD sont décrites dans la [PGSC].

Voir chapitre 4.1 de la [PGSC].

Ces mesures s'appliquent notamment aux infrastructures hébergeant les composants du SCEQAD, 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 SCEQAD, 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 SCEQAD.

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 SCEQAD.

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 SCEQAD comprennent notamment :

- Toutes les versions de la présente PSCEQAD/DPSCEQAD ;
- Les accords contractuels liant le Prestataire aux Clients du SCEQAD ;
- Pour les cachets qualifiés de personnes morales :
    - Les dossiers d'enregistrement du Sujet, du RL et du RCPS, incluant les formulaires signés, les pièces justificatives et les preuves de vérification,
    - Les CSR des Clés Publiques des Certificats de cachet et des Certificats d'authentification RCPS,
    - Les journaux applicatifs relatifs aux opérations de cachet,

- Les journaux d'événements des composants impliqués dans le SCEQAD (applications, systèmes, QSCD, interfaces PKCS#11, Bastion, Reverse Proxy, systèmes de preuve) ;

- Les rapports d'audit relatifs au SCEQAD.

Les durées de conservation des archives sont définies en cohérence avec les exigences réglementaires applicables au SCEQAD et, lorsque nécessaire, avec les obligations d'archivage définies dans [PC_SLP1] correspondant aux Certificats utilisés par le SCEQAD.

Goodflag conserve les données d'audit liées au SCEQAD 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 définis dans la [PGSC].

Voir chapitre 4.6 de la [PGSC].

Ces procédures s'appliquent aux incidents affectant les composants du SCEQAD, incluant notamment les QSCD, les modules d'activation de signature, les systèmes applicatifs, les systèmes de preuve et les infrastructures support.

7.7 Continuité de service

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 SCEQAD dans des délais compatibles avec les engagements de disponibilité.

7.8 Fin de service

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 SCEQAD, le Prestataire met en œuvre une procédure spécifique visant à :

- Notifier les autorités compétentes et les entités affectées, ainsi que les Clients du SCEQAD ;
- Informer publiquement de l'arrêt du SCEQAD et de son périmètre ;
- Arrêter de manière maîtrisée la production de nouveaux cachets qualifiés ;
- Maintenir, pendant les durées requises, la disponibilité des éléments nécessaires à la vérification a posteriori des cachets produits ;
- Assurer la conservation et l'accessibilité des preuves, journaux et archives conformément aux dispositions du chapitre 7.5 ;

- Traiter les Bi-Clé et Certificats selon leur nature :
    - Pour les cachets de personnes morales reposant sur des Bi-Clés persistantes, les Certificats peuvent être révoqués et les Bi-Clés détruites dans les QSCD, en cohérence avec [PC_SLP1] ;
- 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

Les Clés Privées utilisées dans le cadre du SCEQAD sont protégées de sorte qu'elles ne puissent être utilisées que conformément à la présente PSCEQAD/DPSCEQAD et aux exigences du règlement [eIDAS] et aux 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 morales, les Bi-Clés de cachet sont persistantes et demeurent dans le QSCD pendant toute la durée de validité du Certificat de cachet associé. L'utilisation de la Clé Privée du Certificat cachet est conditionnée à l'authentification et à l'autorisation du RCPS, conformément aux dispositions décrites dans les chapitres relatifs à l'identification, à l'activation et aux opérations de cachet. Lorsque des mécanismes de sauvegarde chiffrée sont autorisés pour des Bi-Clés persistantes, ils sont mis en œuvre dans le strict respect des règles applicables au service concerné, en conservant un niveau de sécurité équivalent ou supérieur au stockage dans le dispositif cryptographique, et en assurant un contrôle multiple par des rôles de confiance.

Les paramètres cryptographiques (algorithmes, tailles des Bi-Clés, usages) sont définis et validés par le LPTSP Board. Ils sont cohérents avec [PC_SLP1] pour les Certificats utilisés dans le cadre du SCEQAD, 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 cachet sont réalisées exclusivement dans un QSCD conforme aux exigences du 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 QSCD et 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 en clair et qu'aucune extraction non autorisée ne soit possible.

L'exploitation des HSM et des partitions associées au SCEQAD 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 SCEQAD. 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 SCEQAD, 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 SCEQAD, 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 SCEQAD (composants de preuve, services applicatifs, interfaces d'administration, bastion, supervision, SIEM, systèmes de publication, etc.) ;
- Aux accès nécessaires aux opérations de cachet, lesquels sont conditionnés par les mécanismes d'identification, d'authentification, d'autorisation (personne morale), et par les contrôles de cohérence décrits dans la présente PSCEQAD/DPSCEQAD.

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 SCEQAD :

- 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 création de CEQAD, 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 cachets, 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 SCEQAD.

8.6 Cycle de vie logiciel

Voir chapitre 5.3 de la [PGSC].

Les développements affectant le SCEQAD 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 cachet, sur l'intégrité des preuves ou sur la disponibilité du

SCEQAD font l'objet de contrôles appropriés et de validations conformes aux pratiques internes. Ces dispositions contribuent à prévenir l'introduction de vulnérabilités et à

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 RCPS (personne morale), et uniquement dans le cadre prévu par le SCEQAD. Les SAD sont protégées contre la divulgation, la modification et l'utilisation non autorisée, et leur utilisation est tracée.

Pour les personnes morales, les SAD s'appuient sur :

- L'authentification mutuelle par Certificat du RCPS ;
- Un mot de passe distinct d'autorisation d'usage de la Clé Privée du Sujet, vérifié côté serveur ;
- L'authentification de l'application serveur auprès du QSCD via le code PIN de partition. Les secrets et mots de passe transitent via des échanges protégés et ne sont pas conservés en clair après usage. Les éléments permettant de démontrer le contrôle effectif de l'acte de cachet sont journalisés et conservés conformément aux règles de traçabilité et d'archivage applicables.

8.8 Continuité technique

La continuité technique vise à maintenir ou rétablir, dans des conditions maîtrisées, la capacité du SCEQAD à produire des CEQAD, 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 SCEQAD, 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 et d'autorisation nécessaires au déclenchement des opérations de cachet ;
- 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 SCEQAD 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 SCEQAD, le Prestataire peut appliquer un tarif concernant l'accès au SCEQAD, l'utilisation des fonctionnalités de cachet, ainsi que les prestations associées.

Les modalités tarifaires applicables aux Certificats qualifiés utilisés dans le cadre du SCEQAD restent cohérentes avec celles définies dans [PC_SLP1].

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 SCEQAD sont définies dans la politique spécifique du SCEQAD 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 SCEQAD, sont notamment considérées comme confidentielles :

- Les procédures internes liées au SCEQAD ;
- Les Clés Privées mises en œuvre dans les HSM ;
- Les données d'activation de la Clé Privée du Certificat de cachet ;
- Les journaux d'événements et éléments de preuve ;
- Les dossiers d'enrôlement et d'enregistrement spécifiques au SCEQAD.

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 SCEQAD, les données personnelles traitées incluent notamment :

- Les données relatives aux représentants légaux et aux RCPS pour les personnes morales ;
- Les éléments de preuve associés aux opérations de cachet ;
- Les journaux et traces nécessaires à la conformité réglementaire et à la valeur probatoire des cachets.

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 SCEQAD 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 SCEQAD :

- Lex Persona s'engage à mettre en œuvre les moyens techniques, humains et organisationnels nécessaires à la fourniture du SCEQAD 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 SCEQAD ;
- Les obligations respectives du Prestataire, des Clients, des Signataires, des RCPS et des Utilisateurs finaux sont précisées dans la présente PSSCEQAD / DPSCEQAD 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 PSSCEQAD / DPSCEQAD est publiée après validation par le LPTSP Board sur le site de publication du Prestataire.

10.8 Amendements de la PSSCEQAD / DPSCEQAD

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 SCEQAD sont définies dans les conditions contractuelles et dans la présente PSSCEQAD / DPSCEQAD.

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 ou le RCPS ;
- 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 SCEQAD.

10.11 Loi applicable

Voir chapitre 7.14 de la [PGSC].

La présente PSSCEQAD / DPSCEQAD est soumise au droit français.

10.12 Conformité aux législations et réglementations

Voir chapitre 7.15 de la [PGSC].

Le SCEQAD est conforme :

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