SunPKI

Sunnystamp Natural Persons CA

Déclaration d'IGC

Version 1.8

Date d'entrée en vigueur : 07/04/2023

Table des matières

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

1. Objet du document

Ce document est la Déclaration d'Infrastructure de Gestion de Clés de l'Autorité de Certification intermédiaire « Sunnystamp Natural Persons CA », ci-après dénommée AC dans le reste du document.

Ce document a pour objectif de présenter et résumer les points principaux décrits par la Politique de Certification et la Déclaration des Pratiques de Certification (PC/DPC) de l'AC disponible à l'adresse : https://pki2.sunnystamp.com/repository.

Il est à destination des titulaires de Certificats (appelés Signataires), des demandeurs de Certificats (appelés Clients) et des Utilisateurs de Certificats (UC).

2. Définitions et acronymes

Autorité de Certification (AC)
Au sein d'un Prestataire de Service de Certification Electronique (PSCE), ici la société Lex Persona, une AC a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une PC/DPC, et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du Certificat).

Autorité d'Enregistrement (AE)
Les missions principales de l'AE consistent à vérifier l'identité des Signataires, authentifier et transmettre à l'AC les demandes de création et de révocation de Certificats et d'archiver les données relatives à l'identification des Signataires. L'AE est gérée et opérée par Lex Persona. L'AE peut déléguer une partie de ses missions à une entité tierce sous contrat avec Lex Persona mais reste toujours responsable des obligations qui lui incombent vis-à-vis des Clients, des UC et des Signataires.

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'un Signataire 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 :

- L'identité du Signataire ;
- La Clé Publique du Signataire ;
- Le(s) usage(s) autorisé(s) de la Clé Publique ;
- La durée de vie du Certificat ;
- L'identité de l'AC ;

- La signature de l'AC.

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
Personne physique ou morale qui demande un Certificat pour un Signataire.

Déclaration des Pratiques de Certification (DPC)
Ensemble de pratiques qu'une Autorité de Certification met en œuvre pour émettre, gérer, révoquer et renouveler les Certificats qu'elle émet dans le cadre d'une Politique de Certification.

Entité Légale
Terme utilisé dans ce document pour désigner exclusivement la personne morale à laquelle le Signataire est rattaché et au nom de laquelle ce dernier utilise son Certificat.

Infrastructure de Gestion de Clés (IGC)
Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs Certificats utilisés par des services de confiance. Une IGC peut être composée d'une Autorité de Certification, d'un Opérateur de Certification, d'une Autorité d'Enregistrement centralisée et/ou locale, de Mandataires de Certification, d'une entité d'archivage, d'une entité de publication, etc.

Liste des Certificats Révoqués (LCR) : liste signée, publiée par l'AC et contenant à un instant donné la liste des Certificats révoqués par l'AC.

Object Identifier (OID)
Identifiant universel, représenté sous la forme d'une suite d'entiers. Les OID sont organisés sous une forme hiérarchique avec des nœuds visant à faciliter l'interopérabilité entre différents logiciels.

Politique de Certification (PC)
Ensemble de règles, identifié par un OID), définissant les exigences auxquelles une Autorité de Certification se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC/DPC peut également, si nécessaire, identifier les obligations et les exigences portant sur les autres intervenants, notamment les Signataires et les UC.

Service de signature

Service mis à disposition par la plateforme de signature de LEX PERSONA et permettant à des Signataires de créer des signatures électroniques en mode « serveur » avec un Certificat de signature délivré par l'AC.

Signataire
Personne physique titulaire d'un Certificat obtenu suite à la demande d'un Client.

Transaction de signature
Opération de courte durée, gérée par le Service de signature, durant laquelle un Signataire doit s'authentifier auprès de l'AE pour obtenir un Certificat et pouvoir signer électroniquement les documents de cette transaction avec sa Clé Privée opérée par le Service de signature.

Utilisateur de Certificats (UC)
Toute personne physique ou morale qui utilise un Certificat délivré par l'AC, pour ses propres besoins, et qui doit pour cela le vérifier préalablement.

3. Conditions générales d'utilisation

Contact de l'AC	LEX PERSONA 9 AVENUE MARECHAL LECLERC 10120 ST-ANDRE-LES-VERGERS FRANCE Adresse courriel : pki@sunnystamp.com Téléphone : +33 (0)3 25 43 90 78
Site de publication	Les informations, énumérées dans la section 2.2 de la PC/DPC, sont publiées sur le site de publication de l'AC : https://pki2.sunnystamp.com/repository. Le site de publication est disponible 24h/24 et 7j/7 en conditions normales de fonctionnement.
Types de Certificats émis	L'AC délivre des Certificats à des personnes physiques pouvant être rattachées ou non à une Entité Légale. Ces Certificats ont une durée de validité maximale d'une (1) heure et ne peuvent être utilisés que pour signer les documents de la Transaction de signature pour laquelle ils ont été spécialement créés. L'AC délivre cinq types de Certificats : 1. Les certificats utilisés par ses répondeurs OCSP pour signer les réponses OCSP ; 2. Les certificats « ETSI LCP avec possibilité de révocation » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.2, conformes à la norme [EN 319 411-1] pour le niveau LCP ; 3. Les certificats « OPEN REG » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.3, pour lesquels la présente PC/DPC laisse l'Autorité d'Enregistrement libre de définir le processus d'enregistrement appliqué pour authentifier et vérifier l'identité des Signataires ; 4. Les certificats « FranceConnect » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.4, délivrés à la suite d'une authentification du Signataire par un Fournisseur d'identité proposé par FranceConnect (https://franceconnect.gouv.fr) ; 5. Les certificats « MIE eIDAS » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.5, conformes à la norme [EN 319 411-2] pour le niveau QCP-n-qscd, délivrés à

	la suite d'une authentification du Signataire via un moyen d'identification électronique : - ayant fait l'objet d'une notification par l'un des États membres de l'Union européenne ; et - ayant un niveau de garantie substantiel ou élevé ; et - pour lesquels il est publié une documentation en langue anglaise ou française permettant d'établir, sans ambiguïté, que la présence de la personne physique ou un représentant autorisé de la personne morale est un prérequis à l'obtention de ce moyen d'identification électronique ; 6. Les certificats « ETSI LCP sans possibilité de révocation » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.6, conformes à la norme [EN 319 411-1] pour le niveau LCP. Les Certificats sont émis par l'AC « Sunnystamp Natural Persons CA », qui est elle-même émise par l'AC racine « Sunnystamp Root CA G2 ». Les certificats de ces AC sont disponibles à l'adresse suivante : https://pki2.sunnystamp.com/repository L'AC peut délivrer des certificats de test, lesquels sont identifiés par le préfixe « TEST- » dans les attributs SN et GN du sujet.
Objet des Certificats	Les Certificats émis par l'AC sont des certificats de signature à destination de personnes physiques, et qui, dans le cas des Certificats OPEN REG et MIE eIDAS, peuvent être rattachées à une Entité Légale.
Modalités d'obtention	La demande d'un Certificat provient du besoin par le Signataire de signer, au sein d'une Transaction de signature, les documents que lui a soumis le Client. **Validation de l'identité du Signataire :**

	Pour les Certificats ETSI LCP avec ou sans possibilité de révocation : Le Client doit fournir à l'AE les nom, prénom(s) et numéro de téléphone portable du Signataire devant signer les documents. Le Signataire doit ensuite saisir l'OTP SMS que lui a envoyé l'AE et transmettre à l'AE un document officiel d'identité (carte nationale d'identité, passeport ou carte de séjour) en cours de validité avec photographie comportant ses nom, prénom(s), date et lieu de naissance. Pour les Certificats OPEN REG : Le Client doit fournir au minima à l'AE les nom et prénom(s) du Signataire devant signer les documents. Le Client de l'AE doit décrire la manière dont elle procède pour vérifier l'identité du Signataire et l'authentifier. Pour les Certificats FranceConnect et MIE eIDAS : Le Client doit fournir au minimum à l'AE les nom et prénom(s) du Signataire devant signer les documents. L'AE délègue la validation de l'identité du Signataire à FranceConnect, ou bien respectivement à un organisme qui met en place un moyen d'identification électronique, et récupère auprès de celui-ci les informations d'identité suivantes du Signataire : • Nom de naissance ; • Prénom(s) ; • Date de naissance ; • Pays de naissance. **Utilisation de la clé privée et du Certificat par le Signataire pour signer :** La Clé Privée d'un Signataire est protégée par le Service de signature qui met en œuvre des moyens techniques et organisationnels pour garantir que seul le propriétaire de cette Clé Privée puisse l'utiliser pour signer.

	Dans le cas d'un Certificat ETSI LCP avec ou sans possibilité de révocation, FranceConnect ou MIE eIDAS, la clé privée du Signataire est générée et stockée sur un HSM certifié *FIPS 140-2 level 3* et QSCD et figurant sur la liste [UE_QSig/SealCD].
Modalités de renouvellement	Il n'y a pas de processus de renouvellement.
Modalités de révocation	La révocation d'un Certificat est déclenchée automatiquement dès lors que le Signataire annule la Transaction de signature pour laquelle le Certificat a été spécialement créé. Cette annulation se produit dans les cas suivants : • Si le Signataire refuse de signer les documents de la Transaction de signature ; • Si le Signataire ne valide pas les informations contenues dans son Certificat qui lui sont présentées dans la page de signature à la suite de la génération de son Certificat.
Limites d'usage	Les Certificats délivrés par l'AC ont une durée de validité maximale de 1 heure et sont utilisés par les Signataires pour signer exclusivement les documents de la transaction de signature pour laquelle ils ont été spécialement créés. L'AC ne peut être tenue responsable de l'utilisation du Certificat d'une manière non conforme à la PC/DPC. Un Certificat délivré par l'AC est utilisé par un UC pour valider les signatures électroniques créées par une personne physique qui est le propriétaire du Certificat. Les certificats de test ne sont produits qu'à des fins de test technique ou de démonstration et n'engagent ni l'AC ni la personne qui les utilise. Les informations du dossier d'enregistrement ainsi que les traces des événements liés au cycle de vie des Certificats sont conservées par l'AC pendant une durée maximale de 7 ans.
Obligations des Signataires	Le Signataire à l'obligation de : • Respecter les modalités d'usages précisées dans le chapitre 4.5 de la PC ;

	• Fournir des informations correctes à l'AE lors de la phase d'enregistrement ; • Confirmer l'exactitude des informations contenues dans son Certificat ; • Informer l'AE de toute modification des informations contenues dans son Certificat.
Obligations des Clients	Le Client à l'obligation de : • Respecter les modalités d'usages précisées dans le chapitre 1.4 de la PC ; • Fournir des informations correctes à l'AE lors de la phase d'enregistrement ; • Informer l'AE de toute modification des informations contenues dans le Certificat.
Obligations de vérification des certificats par les UC	Les UC ont l'obligation de : • Vérifier et respecter l'usage pour lequel le Certificat a été émis ; • Utiliser le logiciel et le matériel adéquat pour la vérification de la validité du Certificat. Il est rappelé aux UC que les certificats de test ne sont produits qu'à des fins de test technique ou de démonstration et n'engagent ni l'AC ni la personne qui les utilise.
Limite de responsabilité	Lex Persona ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme des données d'authentification, des certificats, des LCR, ainsi que de tout autre équipement ou logiciel mis à disposition. Lex Persona décline sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le Signataire.
Références documentaires	La PC/DPC de l'AC est disponible à l'adresse suivante : https://pki2.sunnystamp.com/repository
Condition d'indemnisation	Sans objet.
Loi applicable et gestion des litiges	La présente PC/DPC est soumise au droit français. En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée au tribunal de commerce de Troyes.

	L'AC dispose d'une procédure de gestion des plaintes et réclamations qui consiste pour le demandeur à ouvrir un ticket sur le site de support de l'AC : https://support.lex-persona.com
Gestion des données à caractère personnelles	L'AC prend toutes les mesures nécessaires pour que les données personnelles soient protégées et stockées de manière à garantir leur intégrité et leur confidentialité conformément à la loi française N°78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés et modifications à venir ainsi que le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.
Audits et références applicables	L'AC est certifiée conforme : ▪ pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.2, à la norme [EN 319 411-1] pour le niveau LCP ; ▪ pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.6, à la norme [EN 319 411-1] pour le niveau LCP ; ▪ pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.5, à la norme [EN 319 411-2] pour le niveau QCP-n-qscd et au référentiel d'exigences [ANSSI_QCP]. Le certificat de conformité est valable 2 ans et est délivré à la suite d'un audit réalisé par un organisme accrédité selon la norme [EN 319 403].

4. Références

[EN 319 403]
ETSI EN 319 403 V2.2.2 (2015-08)
Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[EN 319 411-1]
ETSI EN 319 411-1 V1.2.2 (2018-04)
Policy and security requirements for Trust Service Providers issuing certificates
Part 1: General requirements

[EN 319 411-2]
ETSI EN 319 411-2 V2.3.1 (2021-05)
Policy and security requirements for Trust Service Providers issuing certificates
Part 2: Requirements for trust service providers issuing EU qualified certificates

[ANSSI_QCP]
Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site Internet, Critères d'évaluation de la conformité au règlement eIDAS
ANSSI, version 1.2 du 25 mars 2021

[UE_QSig/SealCD]
Liste des dispositifs qualifiés de création de signature et de création de cachet et des dispositifs sécurisés de création de signature