Sunnystamp Natural Persons CA

Déclaration d'IGC

Version 1.4

Date d'entrée en vigueur : 15/07/2019

Table des matières

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 porteurs de Certificats, des Souscripteurs et des Utilisateurs de Certificats (UC).

Ce document ne représente en aucun cas un contrat entre Lex Persona et un quelconque individu ou une quelconque organisation.

Ce document s'applique aux Certificats suivants :

- Certificats de type « mono-transaction » générés à la demande par la plate-forme de signature en ligne [Sunnystamp] dont l'OID de la PC/DPC est 1.3.6.1.4.1.22542.100.1.1.1.2 et conformes à la norme ETSI EN 319 411-1 LCP ;
- Certificats de type « mono-transaction » générés à la demande par la plate-forme de signature en ligne [Sunnystamp] dont l'OID de la PC/DPC est 1.3.6.1.4.1.22542.100.1.1.1.3.

Dans le présent document, le terme "Sunnystamp" désigne aussi bien la plate-forme de signature en ligne Sunnystamp que la société Lex Persona, enregistrée au RCS de Troyes sous le numéro 480 622 257.

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 Sujets, 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 Sujets. 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 Souscripteurs et des Sujets.

Certificat
Ensemble d'informations garantissant l'association entre l'identité d'un Sujet 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 Sujet du Certificat ;
- La Clé Publique du Sujet du Certificat ;
- 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.

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 Sujet 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 une AC et contenant à un instant donné la liste des Certificats révoqués par l'AC.

Lex Persona Certification Services Provider Board (LPCSP Board)
Organe responsable de la gouvernance des services de confiance de l'IGC Sunnystamp.

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 Sujets et les UC.

Service de signature
Service mis à disposition par la plateforme Sunnystamp de LEX PERSONA et permettant à des Sujets de créer des signatures électroniques en mode « serveur » avec un Certificat délivré par une Autorité de Certification Sunnystamp. La Clé Privée associée au Certificat est générée et conservée de manière sécurisée par le Service de signature, qui impose au Sujet à qui elle appartient, de s'authentifier tout d'abord auprès de l'AE pour obtenir un jeton d'identité qui lui permettra ensuite de s'authentifier sur le Serveur de signature pour signer des documents.

Souscripteur
Le Souscripteur est une personne morale qui demande un Certificat pour un Sujet.

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

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

3. Usage des certificats

Dans le cadre de son offre de services de confiance Sunnystamp, Lex Persona fournit un service de génération de Certificats à la demande de type « personne physique », délivrés par une Autorité de Certification appartenant à l'Infrastructure de Gestion de Clés (IGC) Sunnystamp.

Une demande de génération de Certificat est effectuée par le Sujet dans le cadre de la signature des documents d'une Transaction de signature.

Cette Autorité de Certification est dénommée « Sunnystamp Natural Persons CA » et sera nommée « AC » dans le reste du document.

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 de 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 3 types de Certificats :

- Les certificats utilisés par ses répondeurs OCSP pour signer les réponses OCSP ;

- Les Certificats conformes à la norme [EN 319 411-1] pour le niveau LCP ;
- Les Certificats 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 Sujets.

La PC/DPC de l'AC, accessible à l'adresse https://pki2.sunnystamp.com/repository, décrit les exigences de toutes les phases du cycle de vie des Certificats délivrés par l'AC et fixe les règles et engagements que doivent respecter Lex Persona et toutes les parties concernées. Les procédures internes propres à la Déclaration des Pratiques de Certification (DPC) sont confidentielles et ne sont pas exposées dans ce document.

L'AC est délivrée par l'Autorité de Certification racine « Sunnystamp Root CA G2 ».

Plus généralement on parle de :

- « Certificat ETSI LCP », pour désigner un Certificat, délivré par l'AC selon l'OID 1.3.6.1.4.1.22542.100.1.1.1.2, de niveau LCP de la norme [EN 319 411-1] ;
- « Certificat OPEN REG », pour désigner un Certificat, délivré par l'AC selon l'OID 1.3.6.1.4.1.22542.100.1.1.1.3 pour lequel la présente PC/DPC laisse l'Autorité d'Enregistrement libre de définir le processus d'enregistrement mis en œuvre pour authentifier et vérifier l'identité des Sujets.

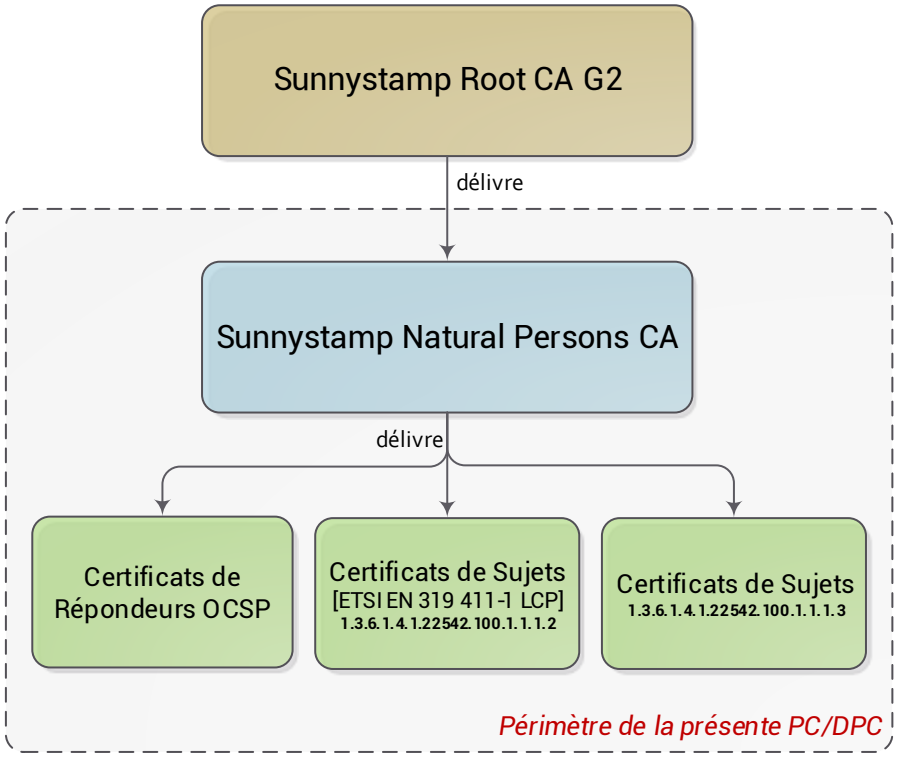

Figure 1 : hiérarchie des certificats de l'AC

Le champ `subject` des Certificats de Sujets émis par l'AC comporte les attributs suivants :

Attribut	Description	Obligatoire ?
CN	Prénom usuel suivi d'un espace et du nom de l'état civil ou, le cas échéant, du nom d'usage du Sujet	Oui
GN	Prénom usuel ou prénoms de l'état civil du Sujet	Oui
SN	Nom de l'état civil ou nom d'usage du Sujet	Oui
C	Code pays de la nationalité du Sujet	Oui
serialNumber	Identifiant interne unique du Certificat du Sujet	Oui
OU	Identifiant de la Transaction de signature	Oui
O	Nom de l'Entité Légale à laquelle le Sujet est rattaché	Non
OI	Identifiant unique de l'Entité Légale à laquelle le Sujet est rattaché (structuré conformément à la section 5.1.4 de la norme [EN 319 412-1]).	Non
T	Fonction du Sujet dans l'Entité Légale à laquelle il est rattaché	Non

4. Demande d'un Certificat

La demande de Certificat est transmise à l'AE lors de la Transaction de signature.

Certificat ETSI LCP :

Le processus de génération d'un Certificat ETSI LCP impose de s'assurer de disposer des informations nécessaires à la fabrication des certificats :

- Les attributs du Sujet doivent être renseignés ainsi que son adresse e-mail et son numéro de téléphone portable ;
- Une pièce d'identité en cours de validité doit être vérifiée.

Certificat OPEN REG :

L'AE doit décrire la manière dont elle procède pour vérifier l'identité du Sujet.

5. Acceptation d'un Certificat

L'acceptation par le Sujet est tacite dès la notification par l'AC de la délivrance du Certificat au Sujet, dès lors que le Sujet a utilisé la Clé Privée associée à la Clé Publique contenue dans le Certificat pour signer.

Technopole de l'Aube en Champagne – CS 90601 – 10901 Troyes Cedex 9
Tél. : +33 (0)3 25 43 90 78 – Fax : +33 (0)9 81 40 30 08 – www.lex-persona.com
SARL au capital de 30 000 Euros – R.C.S. Troyes 480 622 257
SIRET 48062225700024 – Code NAF 5829C – TVA FR01480622257

L'acceptation d'un Certificat par le Sujet emporte le consentement par le Sujet à la publication par l'AC du Certificat.

6. Révocation d'un Certificat

Si le Sujet décide de refuser la Transaction de signature qui lui est proposée, son Certificat est immédiatement révoqué.

Si le Sujet ne refuse ni n'accepte la Transaction de signature qui lui est proposée, alors le Certificat reste valable jusqu'à la date de fin de validité du Certificat.

7. Utilisation d'un certificat

Avant toute utilisation d'un certificat émis par l'AC, vous devez lire la PC/DPC disponible à l'adresse https://pki2.sunnystamp.com/repository.

Pour vérifier la validité d'un certificat émis par l'AC vous pourrez avoir besoin de la chaine complète de certification que vous trouverez également à l'adresse https://pki2.sunnystamp.com/repository :

- Le certificat de l'AC « Sunnystamp Natural Persons CA » ;
- Le certificat de l'AC racine « Sunnystamp Root CA G2 ».

Si vous avez besoin de vérifier le statut de révocation d'un Certificat délivré par l'AC, vous pouvez télécharger les LCR aux adresses suivantes :

- http://pki2.sunnystamp.com/crls/sunnystamp-natural-persons-ca.crl ;
- http://pki3.sunnystamp.com/crls/sunnystamp-natural-persons-ca.crl ;

Le statut de révocation peut également être interrogé à travers un répondeur OCSP accessible à l'adresse suivante : http://ocsp2.sunnystamp.com/sunnystamp-natural-persons-ca.

8. Conditions générales d'utilisation

Contact de l'AC	Lex Persona 2 rue Gustave Eiffel CS 90601 10901 Troyes Cedex 9 France Adresse mail : 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 en conformité avec le chapitre 7 de la PC/DPC. Les Certificats de la chaine de certification à travers laquelle les Certificats sont émis, sont disponibles à l'adresse suivante : https://pki2.sunnystamp.com/repository.
Objet des Certificats	Les Certificats émis par l'AC sont des certificats à destination de Sujets de type personne physique, représentant elle-même ou rattaché à une Entité Légale.
Modalités d'obtention	Les modalités d'obtention d'un Certificat délivré par l'AC sont précisées dans les chapitres 4.1, 4.2 et 4.3 de la PC/DPC.
Modalités de renouvellement	Sans objet.
Modalités de révocation	Les modalités de révocation d'un Certificat délivré par l'AC sont précisées dans le chapitre 4.9 de la PC/DPC.
Limites d'usage	Les Certificats délivrés par l'AC ont une durée de validité maximale de 1 heure et sont utilisés par les Sujets 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 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 informations du dossier d'enregistrement ainsi que les traces des événements liés au cycle de vie des Certificats sont conservées pendant une durée maximale de 7 ans.

Technopole de l'Aube en Champagne – CS 90601 – 10901 Troyes Cedex 9
Tél. : +33 (0)3 25 43 90 78 – Fax : +33 (0)9 81 40 30 08 – www.lex-persona.com
SARL au capital de 30 000 Euros – R.C.S. Troyes 480 622 257
SIRET 48062225700024 – Code NAF 5829C – TVA FR01480622257

Obligations des Sujets	Le Sujet 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 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 du statut du Certificat.
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 Sujet.
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	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.
Gestion des données à caractère personnelles	L'AC prend toutes les mesures nécessaires pour que les données personnelles soient protégées et stockées de manière confidentielle 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	Les audits sont effectués en conformité avec l'ETSI EN 319 411-1. Voir le chapitre 8 de la PC/DPC.

9. Références

[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

[Sunnystamp]
Plate-forme de signature électronique en ligne Lex Persona.