Sunnystamp Natural Persons CA

Déclaration d'IGC

Version 1.2

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 « multi-transactions », générés à la demande par la plate-forme de signature en ligne [Sunnystamp], dont l'OID de la PC/DPC est 1.3.6.1.4.1.22542.100.1.1.1.1 ;
- 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.

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.

Représentant Légal (RL)
Le RL est une personne physique disposant des pouvoirs de représenter le Sujet de par la loi. Elle dispose de la faculté de procéder à des demandes d'émission et de révocation de Certificat au bénéfice des Sujets qu'elle aura expressément défini.

Souscripteur
Le Souscripteur est une personne qui demande un Certificat pour un Sujet et qui est soit une personne physique ou morale habilitée à représenter le Sujet (un représentant légal (RL) du Sujet ou une personne physique ou morale qui détient le Sujet) ou un RL qui demande un Certificat pour une filiale, une unité, un département ou un service du Sujet.

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 un Souscripteur pour une personne physique qui sera le Sujet du Certificat délivré.

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

L'AC délivre 2 types de Certificats à la demande :

- Des certificats de type « mono-transaction » qui ont une durée de validité maximale de 12 heures et qui peuvent être utilisés pour signer exclusivement les documents de la transaction de signature pour laquelle ils ont été spécialement créés ;
- Des certificats de type « multi-transactions » qui ont une durée de validité maximale de 3 ans et qui peuvent être utilisé pour signer les documents de différentes transactions de signature.

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.

Cette PC/DPC est conforme à la norme [EN 319 411-1] niveau LCP pour l'émission de certificats de type « mono-transaction » délivrés à des personnes physiques pouvant être rattachées ou non à une Entité Légale.

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

Les OID correspondants aux deux types de Certificats sont les suivants :

- Certificat de type « multi-transactions » : 1.3.6.1.4.1.22542.100.1.1.1.1 ;
- Certificat de type « mono-transaction » : 1.3.6.1.4.1.22542.100.1.1.1.2.

Plus généralement on parle de :

- « Certificat multi-transactions », pour désigner un Certificat de type « multi-transactions » ;
- « Certificat mono-transaction », pour désigner un Certificat de type « mono-transaction ».

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 6202A – TVA FR01480622257

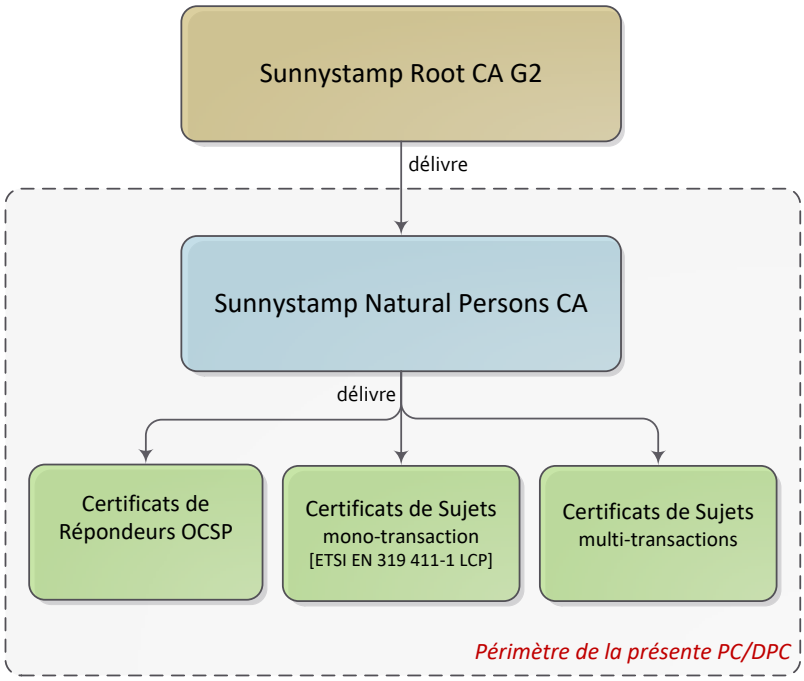

Figure 1 : hiérarchie des certificats de l'AC

Le champ `subject` du Certificat mono-transaction ou multi-transactions 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 dans le cas d'un certificat mono-transaction.	Non
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

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 6202A – TVA FR01480622257

4. Demande d'un Certificat

a. Certificat mono-transaction

Un Certificat mono-transaction peut être généré à tout moment par un appel à Sunnystamp REST API.

La durée de vie d'un Certificat mono-transaction ne peut pas excéder 12 heures. Une fois le Certificat généré, un code OTP (One Time Password) valable pendant une durée de vie paramétrable avec une valeur par défaut de 15 minutes est envoyé sur le téléphone portable du Sujet.

Dès lors que le Sujet utilise le code OTP pour signer une transaction de signature de document(s), la clé permettant de signer avec le Certificat est automatiquement et définitivement détruite.

Dès que la durée de vie du code OTP est écoulée, toute nouvelle demande de signature déclenchera l'envoi sur le téléphone portable du Sujet d'un nouveau code OTP.

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

- Les attributs du Sujet doivent être renseignés ;
- Une pièce d'identité en cours de validité doit être vérifiée ;
- Le numéro de téléphone portable du Sujet sur lequel sera envoyé le code OTP doit être renseigné.

b. Certificat multi-transactions

Le Certificat multi-transactions peut être généré à tout moment :

- Sur simple demande du Sujet en accédant à son compte sur la plate-forme [Sunnystamp] ;
- Par un appel à Sunnystamp REST API.

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

- Les attributs du Sujet doivent être renseignés ;
- Le numéro de téléphone portable du Sujet sur lequel sera envoyé le code OTP doit être renseigné.

La durée de validité du certificat multi-transactions est paramétrable et ne peut pas excéder 3 ans.

Dès la demande de Certificat effectuée, ce dernier est immédiatement généré et un code OTP valable pendant une durée de vie paramétrable avec une valeur par défaut de 15 minutes est envoyé sur le téléphone portable du Sujet.

Au cours de cette période le Sujet peut signer autant de fichiers que souhaité avec le même OTP. Dès que la durée de vie du code OTP est écoulée, toute nouvelle demande de signature déclenchera l'envoi sur le téléphone portable du Sujet d'un nouveau code OTP.

5. Révocation d'un Certificat

a. Certificat mono-transaction

Un Certificat mono-transaction est automatiquement et immédiatement révoqué par le biais d'un appel à Sunnystamp REST API dès lors que le Sujet décide de refuser la transaction de signature qui lui est proposée.

Si le Sujet ne refuse ni n'accepte la transaction de signature qui lui est proposée, alors le Certificat mono-transaction reste valable jusqu'à la date de fin de validité du Certificat qui ne peut excéder 12 heures.

b. Certificat multi-transactions

Un Certificat multi-transactions peut être révoqué à tout moment par le Sujet en accédant à son compte sur la plate-forme [Sunnystamp].

Accessoirement, un appel à Sunnystamp REST API permet également à une application métier de déclencher le processus de révocation d'un Certificat.

Dès la demande de révocation du Certificat effectuée, ce dernier est immédiatement révoqué.

6. 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.

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 6202A – TVA FR01480622257

7. 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 de Représentant Légal 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.

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 6202A – TVA FR01480622257

Limites d'usage	Les Certificats délivrés par l'AC sont exclusivement utilisés par les Sujets pour signer des documents, et sont des certificats de type « mono-transaction » qui ont une durée de validité maximale de 12 heures et qui peuvent être utilisés pour signer exclusivement les documents de la transaction de signature pour laquelle ils ont été spécialement créés, ou bien des certificats de type « multi-transactions » qui ont une durée de validité maximale de 3 ans et qui peuvent être utilisé pour signer les documents de différentes transactions de signature. 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 conservés pendant une durée maximale de 10 ans.
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 ; • 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.

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 6202A – TVA FR01480622257

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.
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.

8. Références

[EN 319 411-1]
ETSI EN 319 411-1 V1.1.1 (2016-02)
Policy and security requirements for Trust Service Providers issuing certificates
Part 1: General requirements

[Sunnystamp]
Plate-forme de signature électronique en ligne Lex Persona
https://www.sunnystamp.com