Sunnystamp Legal Persons CA

Déclaration d'IGC

Version 1.1

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 Legal 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 « cachetage » dont l'OID de la PC/DPC est 1.3.6.1.4.1.22542.100.1.1.2.1 et conformes ETSI EN 319 411-1 NCP+, générés à partir d'une requête de certificat au format PKCS#10 ;
- Certificats de type « horodatage » dont l'OID de la PC/DPC est 1.3.6.1.4.1.22542.100.1.1.2.2 et conformes ETSI EN 319 411-1 NCP+, générés à partir d'une requête de certificat au format PKCS#10.

Dans le présent document, le terme "Sunnystamp" désigne 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

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

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.

Responsable de la Clé Privée du Sujet (RCPS)
Un RCPS est une personne physique agissant pour le compte du Souscripteur et qui est dûment mandatée par le Souscripteur et qui est responsable de la Clé Privée associée à la Clé Publique contenue dans le Certificat. Le RCPS doit générer la bi-clé dans un dispositif cryptographique certifié FIPS 140-2 level 3 ou équivalent, pour ensuite demander un Certificat à l'AE. Il peut procéder, le cas échéant à la demande de révocation d'un Certificat.

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 de type « cachetage » ou de type « horodatage », délivrés par une AC appartenant à l'IGC « Sunnystamp », le terme désignant également et indifféremment les services de confiance opérés par la société Lex Persona que l'IGC elle-même.

Cette AC est dénommée « Sunnystamp Legal Persons CA ». Elle délivre des Certificats d'une durée de validité de 3 années au maximum.

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 NCP+.

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

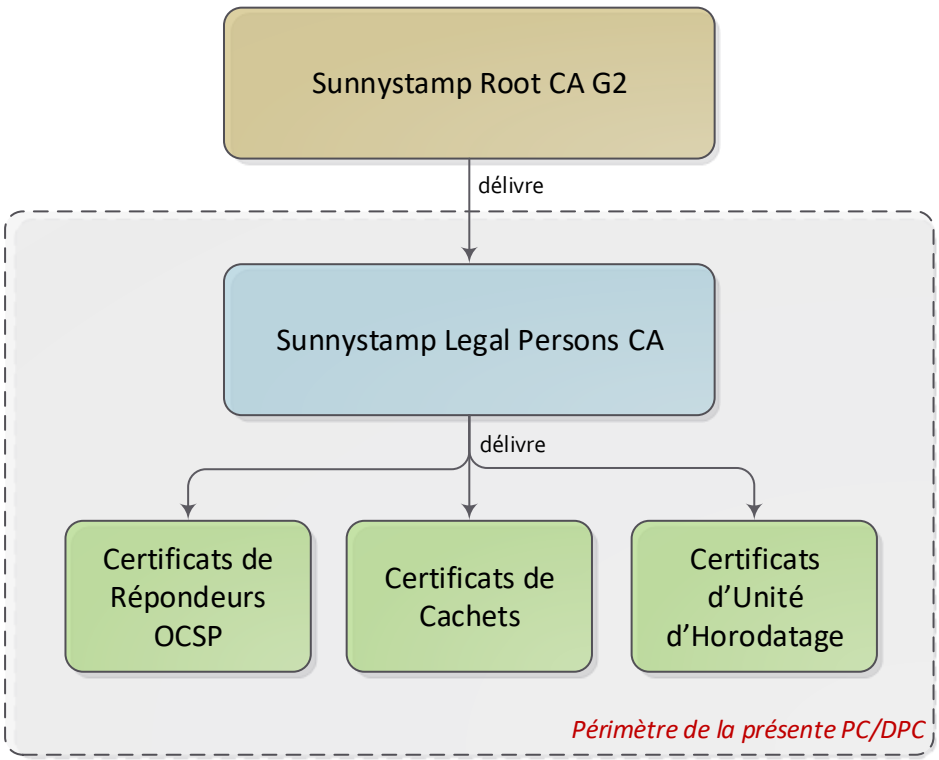

Figure 1 : hiérarchie des certificats de l'AC

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

Les OID des PC/DPC correspondants aux deux types de Certificats sont les suivants :

- Certificat de type « cachetage » : 1.3.6.1.4.1.22542.100.1.1.2.1 ;
- Certificat de type « horodatage » : 1.3.6.1.4.1.22542.100.1.1.2.2.

Plus généralement on parle de :

- « Certificat de cachetage », pour désigner un Certificat de type « cachetage » ;
- « Certificat d'horodatage », pour désigner un Certificat de type « horodatage ».

Les Certificats de cachetage sont utilisés pour effectuer des opérations de cachetage sur des données afin de garantir leur intégrité et leur authenticité.

Les Certificats d'horodatage sont utilisés pour effectuer des opérations d'horodatage sur des données afin de garantir leur intégrité et leur antériorité par rapport à une date et une heure de référence.

Le champ `subject` du Certificat de cachetage ou d'horodatage émis par l'AC comporte les attributs suivants :

Attribut	Description	Obligatoire ?
CN	Nom courant utilisé par le Sujet pour se représenter : Une unité, un département, un service ou une filiale du Sujet	Oui
C	Code du pays dans lequel le Sujet est établi	Oui
O	Nom légal du Sujet	Oui
OI	Identifiant unique du Sujet (structuré conformément à la section 5.1.4 de la norme [EN 319 412-1]).	Oui
serialNumber	Identifiant interne unique du Certificat du Sujet généré par l'AC	Oui
OU	Attribut utilisé pour préciser le Sujet : Une unité, un département, un service ou une filiale du Sujet	Non
L	Attribut utilisé pour désigner la ville dans laquelle le Sujet est enregistré	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

Un Certificat est demandé par un RCPS désigné par un RL de l'entité légale pour laquelle est demandé le Certificat.

Le RCPS et le RL peuvent être une seule et même personne.

La demande d'un Certificat est formulée par le biais d'un formulaire PDF interactif, qui permet au RCPS de remplir les informations nécessaires à la délivrance du Certificat.

Ces informations sont les suivantes :

- La requête de certificat conforme au standard PKCS#10 PEM contenant la clé publique issue de la génération par le RCPS de la bi-clé sur un support cryptographique de niveau FIPS 140-2 Level 2 minimum ; la requête est signée avec la clé privée afin de prouver à l'AE la possession par le RCPS de la clé privée associée à la clé publique contenue dans cette requête de certificat.
- Le type du Certificat : cachetage ou horodatage.
- Les caractéristiques du Certificat, constitués des attributs CN, O, OI, C, OU, L, qui seront vérifiées par l'AE et intégrées par l'AC dans le champ « subject » du Certificat.
- Les informations de contact relatives au RCPS.
- Les informations de contact relatives au RL.
- Les pièces justificatives nécessaires à la demande de Certificat incorporées dans des champs du formulaire prévus à cet effet (pièce d'identité en cours de validité du RCPS, Kbis récent de l'entité légale).
- Les informations de facturation du Certificat quand elles existent.

Le formulaire contient également les conditions générales d'utilisation du Certificat. Il est certifié par Lex Persona pour en garantir l'intégrité et l'authenticité.

Le formulaire constitue l'accord de souscription et doit être signé successivement par le RCPS et le RL après avoir été validé par l'AE. Ce processus de validation et de signature du formulaire est mis en œuvre par le RCPS à l'aide de la plate-forme de signature électronique en ligne Sunnystamp disponible à l'adresse : https://www.sunnystamp.com.

Une fois le formulaire correctement validé et signé, le RCPS l'envoie par e-mail à l'AE qui vérifie la demande, procède le cas échéant à la vérification en face-à-face de l'identité du RCPS, puis créé le Certificat avant de le remettre au RCPS par le biais d'un circuit de validation organisé sur la plate-forme Sunnystamp. Consécutivement à la remise du Certificat, un e-mail est envoyé par l'AE au RCPS et le cas échéant au RL contenant le code de révocation du Certificat.

5. Révocation d'un Certificat

Les seules personnes habilitées à demander la révocation d'un Certificat en dehors de l'AC sont le RCPS et le RL.

Le RCPS ou le RL doit remplir le formulaire de demande de révocation et l'envoyer par e-mail à l'AE à l'adresse ae-slp@sunnystamp.com en renseignant en particulier le code de révocation du Certificat.

Le formulaire de demande de révocation est téléchargeable en accès libre depuis l'adresse https://pki2.sunnystamp.com/repository.

Comme le stipule la PC/DPC, les demandes de révocation reçues par e-mail sont traitées par l'AE en moins de 24h.

La procédure de révocation par e-mail se déroule de la façon suivante :

1. L'OR réceptionne l'e-mail et ouvre le formulaire PDF en pièce jointe.
2. L'OR s'assure que les champs suivants du formulaire sont correctement remplis :
   - Le nom, prénom, fonction, adresse e-mail et numéro de téléphone du demandeur ;
   - Le numéro de série du Certificat à révoquer.
3. L'OR s'assure que cette demande de révocation n'est pas déjà en cours de traitement, ou n'a pas déjà été traitée, par un autre OR. Si c'est le cas il arrête le traitement de cette demande.
4. Si le Certificat n'existe pas, a expiré ou a déjà été révoqué alors l'OR rejette la demande.
5. L'OR authentifie le demandeur de la façon suivante :
   a) Avec le code de révocation ;
   b) Si le code de révocation a été perdu ou oublié, l'OR contacte le demandeur au numéro spécifié dans le formulaire, afin de l'authentifier par le biais d'un jeu de questions.
6. L'OR révoque le Certificat.
7. L'OR envoie un e-mail de notification au RCPS et au RL pour leur indiquer que le Certificat vient d'être révoqué avec succès.

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

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 Legal 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-legal-persons-ca.crl ;
- http://pki3.sunnystamp.com/crls/sunnystamp-legal-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-legal-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
Types de Certificats émis	L'AC délivre des Certificats de cachetage et d'horodatage 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 personnes morales.
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 sont exclusivement utilisés par les Sujets pour réaliser des cachetages et des horodatages. Un Certificat délivré par l'AC est utilisé par un UC pour valider les cachetages et horodatages créés par une personne morale qui est le propriétaire du Certificat.
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.

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

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.
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