Sunnystamp PKI

Sunnystamp Root CA G2

Politique de Certification / Déclaration des Pratiques de Certification

Version 1.2

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 – Code NAF 6202A – TVA FR01480622257

Sunnystamp PKI

Sunnystamp Root CA G2

Politique de Certification /

Déclaration des Pratiques de Certification

Version 1.2

Table des matières

1 Introduction

1.1 Présentation générale

Dans le cadre de son offre de services de confiance Sunnystamp, LEX PERSONA se positionne en tant que Prestataire de Service de Certification Electronique (PSCE) et fournit une Autorité de Certification racine appartenant à l'Infrastructure de Gestion de Clés (IGC) Sunnystamp.

Cette Autorité de Certification est dénommée « Sunnystamp Root CA G2 » et sera nommée ACR dans le reste du document.

Le présent document constitue la Politique de Certification et la Déclaration des Pratiques de Certification (PC/DPC) de l'ACR. Il décrit les exigences de toutes les phases du cycle de vie des Certificats délivrés par l'ACR et fixe les règles et engagements que doivent respecter LEX PERSONA et toutes les parties concernées.

Cette PC/DPC est conforme à la norme [EN 319 411-1] niveau NCP+.

L'ACR est une Autorité de Certification racine auto-signée qui délivre des Certificats à des Autorités de Certification intermédiaires qui seront nommées ACI dans le reste du document.

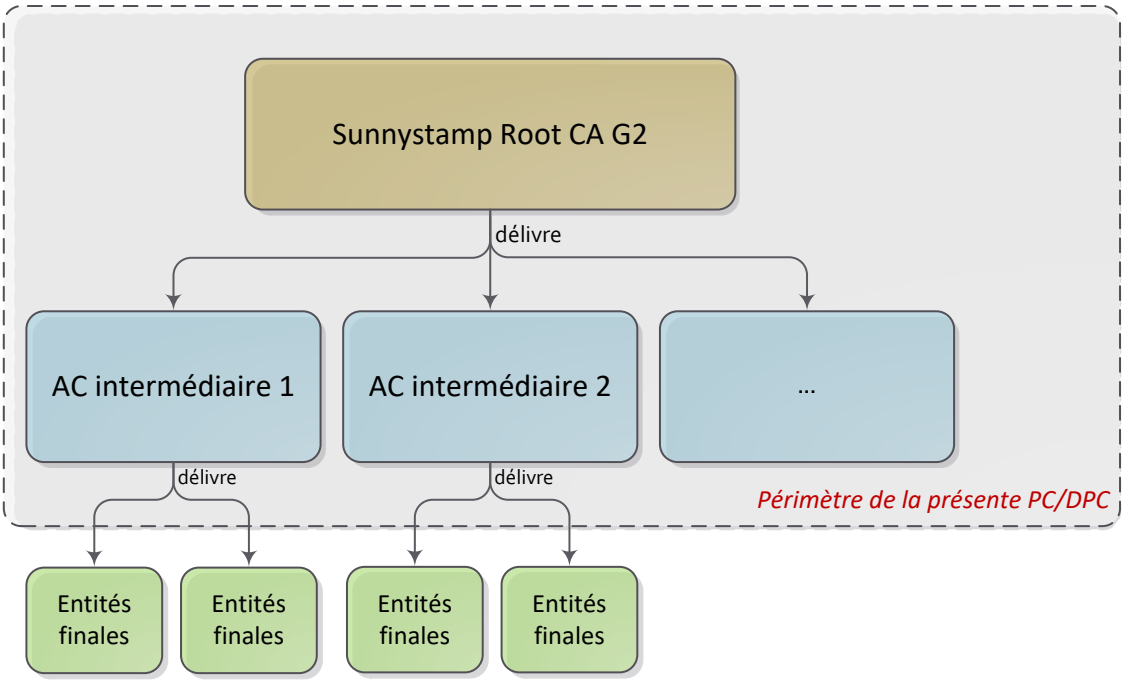

Figure 1 : hiérarchie des certificats de l'AC

Chacune des ACI doit fournir sa propre PC/DPC en conformité la présente PC/DPC.

1.2 Identification du document

Ce document est identifié par l'Object Identifier (OID) suivant : 1.3.6.1.4.1.22542.100.1.1.0.1.

1.3 Entités intervenant dans l'IGC

1.3.1 LEX PERSONA Certification Service Provider Board (LPCSP Board)

L'ACR est sous la responsabilité du LPCSP Board. Le LPCSP Board est représenté par LEX PERSONA. Il est composé des membres suivants :

- Le responsable du LPCSP Board qui est un représentant légal de LEX PERSONA ;
- Des intervenants spécialisés dans le management de la sécurité des systèmes d'information et nommés par le responsable du LPCSP Board.

Les missions principales du LPCSP Board dans le cadre de l'ACR sont les suivantes :

- Rédiger et approuver la PC/DPC ;
- Approuver le corpus documentaire de l'ACR ;
- Définir le processus d'examen et de mise à jour de la PC/DPC ;
- Définir et attribuer les rôles de confiance au sein de l'ACR ;
- Approuver le rapport annuel d'audit interne des composantes de l'IGC.

1.3.2 Autorité de Certification Racine (ACR)

L'ACR est responsable de la fourniture des prestations de gestion des Certificats durant leur cycle de vie (génération, délivrance, révocation, diffusion, etc.) en mettant en œuvre différents services dans une Infrastructure de Gestion de Clés (IGC) opérée par LEX PERSONA.

1.3.3 Autorité d'Enregistrement (AE)

Les missions principales de l'AE consistent à :

- Vérifier l'identité des Responsables d'ACI qui demande un Certificat à l'ACR ;
- Authentifier et transmettre à l'ACR les demandes de création et de révocation de Certificats ;
- Archiver les données relatives à l'identification des Responsables d'ACI.

L'AE est gérée et opérée par LEX PERSONA.

1.3.4 Autorité de Certification Intermédiaire (ACI)

Une ACI est identifiée dans le champ `subject` du Certificat délivré par l'ACR.

Une ACI est gérée et opérée par LEX PERSONA.

1.3.5 Responsable d'ACI

Personne physique responsable de la Clé Privée d'une ACI et du cycle de vie de son Certificat (demande de certificat, révocation, etc.).

Le Responsable d'une ACI est rattaché LEX PERSONA. Il est nommé par le LPCSP Board.

1.3.6 Utilisateur de Certificat (UC)

Un UC désigne une personne physique ou morale qui utilise le Certificat d'une ACI et qui doit, pour pouvoir s'y fier, vérifier la validité dudit Certificat en contrôlant notamment son statut de révocation.

1.4 Usage des Certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Certificat d'ACR

La Clé Privée associée à la Clé Publique du certificat de l'ACR est utilisée pour signer :

- Les Certificats des ACI ;
- Les LAR.

1.4.1.2 Certificat d'ACI

La Clé Privée associée à la Clé Publique du Certificat de l'ACI est utilisée pour signer :

- Des certificats ;
- Des LCR.

1.4.2 Domaines d'utilisation interdits

Les usages autres que ceux listés dans la section 1.4.1 sont interdits.
De plus, les Certificats doivent être utilisés dans la limite des lois et réglementations en vigueur.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

LEX PERSONA
2 RUE GUSTAVE EIFFEL
CS 90601
10901 TROYES CEDEX 9
FRANCE
E-mail : pki@sunnystamp.com
Téléphone : 0033 325 439 078

1.5.2 Entité déterminant la conformité de la PC/DPC

Le LPCSP Board détermine la conformité de la PC/DPC en réalisant des audits et des contrôles de conformité.

1.5.3 Procédure d'approbation de la conformité de la PC/DPC

Le LPCSP Board approuve la PC/DPC après avoir notamment déterminé la conformité de la PC/DPC.

1.6 Définitions et Acronymes

1.6.1 Définitions

Autorité de Certification
Au sein d'un Prestataire de Service de Certification Electronique (PSCE), une Autorité de Certification 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), dans les Certificats émis au titre de cette PC/DPC.

Autorité d'Enregistrement (AE)
Cf. section 1.3.3.

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'une entité 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 de l'entité ;
- La Clé Publique de l'entité ;
- 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.

Le format standard de certificat est défini dans la recommandation X.509 v3 et dans la [RFC 5280].

Dans le cadre de la présente PC/DPC, le terme Certificat sans épithète sera utilisé pour désigner le Certificat d'une ACI.

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.

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.

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, d'une entité d'archivage, d'une entité de publication, etc.

Politique de Certification (PC)
Ensemble de règles, identifié par un nom (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 ACI et les UC.

1.6.2 Acronymes

Les acronymes utilisés dans la présente PC/DPC sont les suivants :

ACI	Autorité de Certification intermédiaire délivrée par l'ACR
ACR	Autorité de Certification « Sunnystamp Root CA G2 »
AdES	Advanced Electronic Signature
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CGU	Conditions Générales d'Utilisation
DN	Distinguished Name
DPC	Déclarations des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
LAR	Liste des Autorités de certification Révoquées
LCR	Liste de Certificats Révoqués
LPCSP Board	LEX PERSONA Certification Service Provider Board
OID	Object Identifier
PC	Politique de Certification
PCA	Plan de Continuité d'Activité

PRA	Plan de Reprise d'Activité
PSCE	Prestataire de Service de Certification Electronique
UC	Utilisateurs de Certificat

2 Responsabilité concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

LEX PERSONA est chargée de la mise en place et de la mise à disposition, aux Utilisateurs de Certificats, des informations devant être publiées.

Ces informations, énumérées dans la section suivante, sont publiées sur le site de publication suivant : https://pki2.sunnystamp.com/repository.

2.2 Informations devant être publiées

L'ACR publie en ligne les informations suivantes :

- La présente PC/DPC ;
- L'accord d'utilisation des Certificats ;
- Le certificat X.509 de l'ACR ainsi que son empreinte de hachage ;
- La LAR consultable aux adresses suivantes :
  - http://pki2.sunnystamp.com/crls/sunnystamp-root-ca-g2.crl ;
  - http://pki3.sunnystamp.com/crls/sunnystamp-root-ca-g2.crl ;

2.3 Délais et fréquences de publication

La PC/DPC est publiée en conformité avec la section 9.12.

L'accord d'utilisation des Certificats est publié après chaque mise à jour.

Le certificat X.509 de l'ACR et son empreinte de hachage sont publiés avant leur utilisation effective.

Les LAR sont publiées comme spécifié à la section 4.9 de la présente PC.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées sont librement accessible en lecture. En revanche, l'accès en modification aux données publiées est strictement limité aux personnes habilitées de l'IGC.

3 Identification et authentification

3.1 Nommage

3.1.1 Types des noms

Les Certificats et les noms qu'ils contiennent sont conformes à la norme [RFC 5280].
L'ACR est identifiée dans le champ `issuer` du Certificat et l'ACI est identifié dans le champ `subject`.

Le champ `subject` du Certificat émis par l'ACR comporte les attributs suivants :

Attribut	Description	Obligatoire ?
CN	Nom commun de l'ACI.	Oui
O	Nom de l'entité légale de l'ACI.	Oui
OI	Identifiant unique de l'entité légale de l'ACI (structuré conformément à la section 5.1.4 de la norme [EN 319 412-1]).	Oui
OU	Identifiant unique de l'entité légale de l'ACI (structuré conformément à l'ISO 6523).	Oui
C	Code pays dans lequel l'ACI est établie.	Oui

Chaque `subject` émis par l'ACR doit être unique.

Les informations contenues dans les attributs énumérés ci-dessus sont tous vérifiées par l'AE. Concernant l'attribut CN, l'AE vérifie qu'il s'agit d'un nom explicite tel que décrit dans la section suivante.

3.1.2 Nécessité d'utilisation de noms explicites

L'ACR s'assure que le champ `subject` et notamment l'attribut CN est un nom explicite qui permet d'identifier l'ACI.

3.1.3 Anonymisation et pseudonymisation

Ces pratiques sont interdites par cette PC/DPC.

3.1.4 Règles d'interprétation des différentes formes de nom

Les éléments contenus dans les sections 3.1.1, 3.1.2 et 3.1.3 fournissent les explications permettant d'interpréter correctement les différentes formes de nom.

3.1.5 Unicité des noms

L'ACR s'assure que le champ `subject` des Certificats qu'elle émet est unique. Ainsi 2 ACIs différentes n'auront jamais le même champ `subject`.

3.1.6 Identification, authentification et rôle des marques déposées

L'ACR ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par des Souscripteurs de marques déposées, de marques notoires et de signes distinctifs, ainsi que de noms de domaine.

Si un tel cas se produit, l'AE pourra refuser de délivrer le Certificat à l'ACI et l'ACR pourra prendre la décision de révoquer le Certificat.

3.2 Validation initiale de l'identité

3.2.1 Méthodes pour prouver la possession de la Clé Privée

L'ACI prouve à l'ACR qu'elle possède bien la Clé Privée correspondant à la Clé Publique à certifier en transmettant à l'AE la requête de certificat au format [PKCS#10] qu'elle signe à l'aide de sa Clé Privée.

3.2.2 Validation de l'identité d'une entité légale

La validation de l'entité légale opérant l'ACI est réalisée lors de la phase de validation de l'identité du Responsable de l'ACI.

3.2.3 Validation de l'identité du Responsable de l'ACI

Pour demander un Certificat à l'ACR, le Responsable de l'ACI doit envoyer un formulaire de demande de certificat daté et signé à l'AE qui contient son adresse mail professionnelle et son numéro de téléphone.

L'AE s'assure que le Responsable de l'ACI est bien un employé de LEX PERSONA.

L'AE peut accepter ou refuser sa demande si elle juge que cette personne ne peut pas être le Responsable de l'ACI.

La validation de l'identité de la personne physique du Responsable de l'ACI est réalisée lors d'un face à face physique avec l'AE durant lequel elle demandera au Responsable de l'ACI de lui présenter sa pièce d'identité afin qu'elle en vérifie l'authenticité et la validité puis qu'elle l'authentifie par rapport à la photographie contenue dans sa pièce d'identité.

Une copie de la pièce d'identité et le formulaire de demande de certificat sont archivés par l'AE.

3.2.4 Informations non vérifiées de l'ACI

Toutes les informations contenues dans le champ `subject` du Certificat sont vérifiées par l'AE.

3.2.5 Validation de l'autorité du demandeur

L'AE s'assure que le demandeur est LEX PERSONA.

3.2.6 Critères d'interopérabilité

Sans objet.

3.3 Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé et du Certificat d'une ACI n'est pas autorisé par cette PC/DPC.

3.3.1 Identification et validation d'un renouvellement courant

Sans objet.

3.3.2 Identification et validation pour un renouvellement après révocation

Sans objet.

3.4 Identification et validation d'une demande de révocation

Pour demander la révocation d'un Certificat, le demandeur doit envoyer par mail à l'AE le formulaire de demande de révocation dûment rempli et signé. Ce formulaire contient les informations suivantes :

- Les nom, prénom(s), adresse mail, numéro de téléphone et fonction du demandeur ;
- La valeur de l'attribut CN du champ `subject` du Certificat ;
- Le n° de série du Certificat ;
- Optionnellement, une description sur la raison de la révocation du Certificat (qui n'apparaîtra dans l'ARL).

L'AE authentifie le demandeur en vérifiant la signature du formulaire de révocation et si besoin, contacte directement le demandeur pour l'authentifier.

4 Exigences opérationnelles sur le cycle de vie des Certificats

4.1 Demande de Certificat

4.1.1 Origine d'une demande de Certificat

L'origine d'une demande de Certificat provient du Responsable de l'ACI.

4.1.2 Processus et responsabilités pour l'établissement d'une demande de Certificat

Le processus d'enregistrement pour une demande de Certificat se déroule de la façon suivante :

- Le Responsable d'ACI doit fournir à l'AE les différentes informations requises dans la section 3.2.3 en garantissant leur exactitude ;
- L'AE doit valider la demande en conformité avec la présente PC/DPC et notifier le Responsable d'ACI de la prise en compte de sa demande ;
- Le Responsable d'ACI doit générer la bi-clé de l'ACI, lors d'une cérémonie des clés, dans un dispositif cryptographique satisfaisant aux exigences de la section 6.2.11 ;

- Le Responsable d'ACI doit fournir à l'ACR une preuve de la possession de la Clé Privée de l'ACI conformément à la section 3.2.1.

4.2 Traitement d'une demande de Certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

L'AE valide les informations fournies par les ACI conformément à la section 3.2.

4.2.2 Acceptation ou rejet de la demande

La demande est acceptée dès lors que l'AE a validé avec succès la demande de certificat.

L'AE peut rejeter une demande si elle est incomplète, invalide ou pour toute autre raison.

Dans tous les cas, le Responsable d'ACI qui a fait la demande de certificat est notifié par l'AE de l'acceptation ou du rejet de sa demande.

Si sa demande est acceptée, le Responsable d'ACI doit créer la bi-clé de l'ACI et générer une requête de certificat qu'il remettra à l'AE en présence physique de l'opérateur d'AE.

4.2.3 Durée d'établissement du Certificat

La demande de certificat reste active tant qu'elle n'est pas rejetée.

4.3 Délivrance du Certificat

4.3.1 Actions de l'ACR concernant la délivrance du Certificat

Les actions de l'ACR concernant la délivrance du Certificat sont les suivantes :

- L'ACR vérifie la signature de la requête de certificat [PKCS#10] de l'ACI en utilisant la Clé Publique qu'elle contient ;
- L'ACR crée le Certificat, en conformité avec le profil du Certificat défini dans la section 7.2, en certifiant avec sa Clé Privée, l'association de la Clé Publique de l'ACI avec les informations d'identification de l'ACI contenues dans la demande.

Le Certificat est créé lors d'une cérémonie de délivrance d'un certificat d'ACI, dans les locaux sécurisés hébergeant le HSM contenant la bi-clé de l'ACR, sous le contrôle d'au moins 2 personnes ayant les rôles de confiance adéquats pour activer le HSM et la Clé Privée de l'ACR.

4.3.2 Notification par l'ACR de la délivrance du Certificat à l'ACI

Une fois généré, le Responsable d'ACI est notifié de la délivrance du Certificat qui lui est transmis de manière appropriée.

4.4 Acceptation du Certificat

4.4.1 Démarche d'acceptation du Certificat

L'acceptation d'un Certificat est tacite dès la notification par l'ACR de la délivrance du Certificat au Responsable d'ACI.

4.4.2 Publication du Certificat

L'ACR ne publie pas le Certificat de l'ACI.

4.4.3 Notification par l'ACR aux autres entités de la délivrance du Certificat

Sans objet.

4.5 Usages de la bi-clé et du Certificat

4.5.1 Utilisation de la Clé Privée et du Certificat par l'ACI

L'utilisation par l'ACI, de sa Clé Privée et de son Certificat associé, doit respecter les exigences définies dans cette PC/DPC, en particulier les usages définis dans la section 1.4 ainsi que ceux spécifiés dans l'extension `KeyUsage` du Certificat.

4.5.2 Utilisation de la Clé Publique et du Certificat par l'UC

Voir section 9.6.6.

4.6 Renouvellement d'un Certificat

Aucun renouvellement de Certificat n'est autorisé par l'ACR.

4.6.1 Causes possibles de renouvellement d'un Certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification à l'ACI de l'établissement du nouveau Certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau Certificat

Sans objet.

4.6.6 Publication du nouveau Certificat

Sans objet.

4.6.7 Notification par l'ACR aux autres entités de la délivrance du nouveau Certificat

Sans objet.

4.7 Délivrance d'un nouveau Certificat suite au changement de la bi-clé

Aucune délivrance d'un nouveau Certificat suite au changement de la bi-clé n'est autorisée par l'ACR.

4.7.1 Causes possibles de changement d'une bi-clé

Sans objet.

4.7.2 Origine d'une demande d'un nouveau Certificat

Sans objet.

4.7.3 Procédure de traitement d'une demande d'un nouveau Certificat

Sans objet.

4.7.4 Notification de l'ACI de l'établissement du nouveau Certificat

Sans objet.

4.7.5 Démarche d'acceptation du nouveau Certificat

Sans objet.

4.7.6 Publication du nouveau Certificat

Sans objet.

4.7.7 Notification par l'ACR aux autres entités de la délivrance du nouveau Certificat

Sans objet.

4.8 Modification du Certificat

Pour modifier un Certificat en cours de validité, il est nécessaire de le révoquer puis de demander la délivrance d'un nouveau Certificat.

4.8.1 Causes possibles de modification d'un Certificat

Sans objet.

4.8.2 Origine d'une demande de modification d'un Certificat

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification d'un Certificat

Sans objet.

4.8.4 Notification de l'ACI de l'établissement du Certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du Certificat modifié

Sans objet.

4.8.6 Publication du Certificat modifié

Sans objet.

4.8.7 Notification par l'ACR aux autres entités de la délivrance du Certificat modifié

Sans objet.

4.9 Révocation et suspension des Certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat d'ACI

Les circonstances suivantes peuvent être à l'origine de la révocation du Certificat d'une ACI :

- L'ACI n'a pas respecté, ou ne respecte plus, les obligations découlant de la présente PC/DPC ;
- Une erreur a été détectée dans la procédure d'enregistrement de l'ACI ;
- Les informations contenues dans le Certificat ne sont plus exactes ;
- L'ACI demande la révocation de son Certificat ;
- La Clé Privée de l'ACI est compromise ou suspectée de l'être ;
- Les données d'activation permettant à l'ACI d'activer sa Clé Privée sont perdues ou volées ;
- L'ACR est révoquée.

4.9.1.2 Certificat d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un Certificat d'une composante de l'IGC :

- Suspicion de compromission, compromission, perte ou vol de Clé Privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la présente PC/DPC ou dans les procédures internes (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat d'ACI

Les personnes autorisées à demander la révocation d'un Certificat d'ACI sont les suivantes :

- Le Responsable de l'ACI ;
- Le Responsable de l'ACR ;
- Le LPCSP Board, en cas d'urgence et d'absence du responsable de l'ACR.

4.9.2.2 Certificats d'une composante de l'IGC et de l'ACR

La révocation d'un Certificat d'une composante de l'IGC peut être demandée par un membre de l'ACR.

Les entités autorisées à demander la révocation du certificat de l'ACR sont les suivantes :

- Le LPCSP Board ;
- Une autorité judiciaire suite à une décision de justice.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat d'ACI

Une demande de révocation peut être transmise à l'AE selon l'une des manières décrites dans la section 3.4.

Le traitement d'une demande de révocation se déroule de la façon suivante :

- L'AE authentifie le demandeur comme indiqué dans la section 3.4 ;
- L'AE vérifie que la demande est complète ;
- L'AE demande à l'ACR de procéder à la révocation du Certificat ;
- L'ACR révoque le Certificat de manière définitive ;
- L'AE notifie le demandeur de la révocation effective du Certificat et le cas échéant le Responsable d'ACR, si ce n'est pas lui qui a fait la demande.

4.9.3.2 Certificat d'ACR

En cas de révocation du certificat de l'ACR, cette dernière doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) :

- L'ANSSI à travers le point de contact identifié sur le site https://www.ssi.gouv.fr/agence/contacts ;
- L'ensemble des ACI concernées, en leur précisant que leur Certificat va être révoqué et qu'elles ne doivent plus utiliser la Clé Privée correspondante ;
- L'ensemble des entités avec lesquelles l'ACR est sous contrat.

4.9.4 Délai accordé à une ACI pour formuler la demande de révocation

La demande de révocation doit être transmise au plus tôt à l'AE.

4.9.5 Délai de traitement par l'ACR d'une demande de révocation

4.9.5.1 Certificat d'ACI

Une demande de révocation d'un Certificat est traitée dans un délai inférieur à 24 heures après l'authentification effective du demandeur de la révocation.

4.9.5.2 Certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection de l'évènement décrit dans les causes de révocation. En particulier, la révocation d'un certificat d'ACR

doit être effectuée immédiatement, notamment en cas de compromission de la Clé Privée associée.

4.9.6 Exigences de vérification de la révocation par les UC

L'UC est tenu de vérifier, avant son utilisation, l'état des certificats de la chaîne de certification en utilisant la dernière ARL publiée par l'ACR.

4.9.7 Fréquence d'établissement des ARL

Les ARL sont émises au plus tard tous les ans.

4.9.8 Délai maximum de publication d'une ARL

Les ARL sont publiées au maximum 30 minutes après leur génération.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des Certificats

Sans objet.

4.9.10 Exigences de vérification en ligne du statut de révocation des Certificats par les UC

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la Clé Privée

Pour un Certificat d'ACI, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la Clé Privée.

Pour un certificat d'ACR, la révocation suite à une compromission de la Clé Privée fait l'objet d'une information clairement diffusée par l'ACR. En cas de révocation de l'ACR, tous les Certificats délivrés par cette ACR et qui sont encore en cours de validité sont révoqués.

4.9.13 Causes possibles d'une suspension

La suspension de Certificat n'est pas autorisée dans la présente PC/DPC.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un Certificat

Sans objet.

4.10 Fonction d'information sur l'état des Certificats

4.10.1 Caractéristiques opérationnelles

La dernière ARL est accessible via les URL de publications décrites dans la section 2.2.

Les ARL contiennent les informations sur les Certificats révoqués, au moins jusqu'à ce qu'ils arrivent à expiration.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des Certificats est disponible en fonctionnement normal 24h/24 et 7j/7.

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre l'ACI et l'ACR

Cette relation cesse naturellement au terme de la durée de validité du Certificat ou suite à sa révocation.

4.12 Séquestre de clé et recouvrement

Les Clés Privées de l'ACR et des ACI ne sont pas séquestrées.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

L'ensemble des ressources matérielles de l'IGC sont hébergées dans deux Datacenters hautement sécurisés qui respectent les règlements et normes en vigueur et qui fournissent une protection robuste contre les accès non autorisés.

Ces deux Datacenters sont localisés sur le territoire français et sont séparés l'un de l'autre par une distance en ligne droite supérieure à 200 km.

5.1.2 Accès physique

L'accès au site d'hébergement de l'IGC est contrôlé et est strictement limité aux seules personnes autorisées à pénétrer dans les locaux. Les personnes non autorisées doivent toujours être accompagnées par des personnes autorisées.

5.1.3 Alimentation électrique et climatisation

LEX PERSONA assure que les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les exigences de la présente PC/DPC en matière de disponibilité de ses fonctions.

La baie dédiée à l'infrastructure de LEX PERSONA dispose d'une alimentation électrique redondante.

5.1.4 Vulnérabilité aux dégâts des eaux

LEX PERSONA respecte les exigences de protection contre les dégâts des eaux, elles permettent de respecter les exigences de la présente PC/DPC en matière de disponibilité de ses fonctions.

5.1.5 Prévention et protection incendie

Les risques d'incendie ont été pris en compte pour l'installation de l'IGC. Les règles de sécurité incendie permettent de respecter les exigences de la présente PC/DPC en matière de disponibilité de ses fonctions, notamment, les fonctions de gestion des révocations et d'information sur l'état des Certificats.

5.1.6 Conservation des supports

Les différents supports utilisés par l'IGC sont stockées de manière sécurisée.

L'ACR assure que les différentes informations nécessaires intervenant dans l'activité de l'IGC sont listées, et les besoins en sécurité sont définis. Les supports correspondant à ces informations sont gérés en fonction de leur besoin en sécurité.

L'ACR met en œuvre les moyens nécessaires pour que les supports soient protégés contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'ACR est engagée à conserver ces informations.

Les documents papiers sont conservés par l'ACR dans des locaux fermés à clés et sont stockés dans un coffre-fort fermé à clé, que seul le responsable de l'ACR ou les personnes autorisées pourront ouvrir.

5.1.7 Mise hors service des supports

En fin de vie, les supports sont détruits de manière sécurisée ou réinitialisés en vue d'une réutilisation.

5.1.8 Sauvegardes hors site

Des sauvegardes hors site sont mises en œuvre par l'IGC vers un site de secours afin d'assurer une reprise des fonctions de l'IGC le plus rapidement possible après incident, conformément aux

exigences de la présente PC/DPC et aux engagements de l'ACR en matière de disponibilité et plus particulièrement en ce qui concerne la fonction d'information de l'état de révocation des Certificats.

Le site de secours offre un niveau de sécurité au moins équivalent au site principal et garantit notamment que les informations sauvegardées hors site respecteront les mêmes exigences de la présente PC/DPC en matière de confidentialité et d'intégrité.

La procédure de sauvegarde hors site est détaillée dans la procédure de sauvegarde.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les rôles de confiance sont définis de telle sorte qu'il n'y ait aucun conflit d'intérêt possible entre ces rôles.

Les rôles de confiance suivants sont définis :

- **Security Officer** : cette personne est chargée de la mise en œuvre et du contrôle de la politique de sécurité des composantes de l'IGC. Elle gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Elle est habilitée à prendre connaissance des archives et des journaux d'évènements. Elle est responsable des opérations de génération et de révocation des certificats.
- **System Administrator** : cette personne est chargée de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Elle assure l'administration technique des systèmes et des réseaux des composantes de l'IGC.
- **HSM Administrator** : cette personne est chargée de l'administration des HSM de l'ACR.
- **System Operator** : cette personne est responsable de l'exploitation des applications pour les fonctions mises en œuvre par les composantes de l'IGC.
- **System Auditor** : cette personne est autorisée à accéder à l'IGC et est en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Registration Officer** : cette personne est chargée de vérifier les informations requises pour la délivrance d'un certificat et d'approuver les demandes de Certificats envoyés à l'AE.
- **Revocation Officer** : cette personne est chargée d'approuver les demandes de révocation de Certificats envoyées à l'AE.
- **Key Holder** : cette personne assure la confidentialité, l'intégrité et la disponibilité des parts de secrets qui lui sont confiées et qui sont liées aux clés d'ACR.

5.2.2 Nombre de personnes requises par tâche

En fonction des opérations réalisées, une ou plusieurs personnes avec des rôles différents sont requises.

5.2.3 Identification et authentification pour chaque rôle

Toute personne intervenant dans le fonctionnement de l'ACR doit avoir préalablement reçu le rôle correspondant.

L'accès physique est autorisé aux seules personnes qualifiées. L'accès logiciel est protégé par des politiques de sécurité fortes.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Les cumuls des rôles suivants par une même personne physique sont interdits :

- Security Officer et System Administrator ;
- System Administrator et System Operator.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tout le personnel de l'ACR est soumis à une clause de confidentialité et a notamment signé la charte de sécurité de l'ACR.

Les fonctions demandées à chaque membre du personnel de l'ACR sont compatibles avec ses compétences. Le personnel d'encadrement dispose de l'expertise nécessaire et est familier des procédures de sécurité.

Le LPCSP Board informe toute personne intervenant dans les rôles de confiances de l'ACR :

- Des responsabilités relatives aux services de l'IGC qui lui incombent ;
- Des procédures liées à la sécurité du système et au contrôle du personnel qu'elle doit respecter.

5.3.2 Procédures de vérification des antécédents

Le personnel travaillant pour l'une des composantes de l'ACR est soumis à une procédure de vérification des antécédents lors de leur prise de fonction.

Les vérifications portent sur les points suivants :

- Les éventuelles condamnations en justice de la personne ne devront pas être contraires à ses fonctions ;
- Les rôles de confiance de la personne ne devront pas se trouver dans un conflit d'intérêt préjudiciable à l'impartialité de ses tâches.

5.3.3 Exigences en matière de formation initiale

Le recrutement du personnel de l'ACR permet de vérifier que chacun dispose de la formation initiale adéquate à la réalisation de ses fonctions.

Le personnel sera formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met œuvre et doit respecter.

Les exigences en matière de formation initiale s'appliquent également à l'AE.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel recevra une formation adaptée préalablement aux évolutions dans l'IGC (procédures, organisation, application, etc.) concernant la ou les composantes sur lesquelles il intervient.

D'autre part, le personnel de l'ACR participe régulièrement à des séances de formation sur la sécurité des systèmes d'information.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Si une personne a réellement fait ou est soupçonnée d'avoir fait une action non autorisée dans l'accomplissement de ses tâches en rapport avec l'exploitation de l'ACR, le LPCSP Board peut lui interdire l'accès aux composantes de l'IGC sur lesquelles elle intervenait.

En outre, si les faits sont avérés, le LPCSP Board pourra prendre à son encontre toutes sanctions disciplinaires adéquates.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les exigences de la section 5.3 sont applicables aux prestataires externes.

5.3.8 Documentation fournie au personnel

Tout le personnel de l'ACR a accès à des procédures et manuels complémentaires concernant leurs fonctions et leurs responsabilités.

5.4 Procédure de constitution des données d'audit

5.4.1 Type d'évènements à enregistrer

Les événements ci-dessous sont enregistrés de manière manuelle ou automatique :

- Création / modification / suppression de comptes utilisateur et des données d'authentification correspondantes ;
- Démarrage et arrêt des systèmes informatiques et des applications ;

- Evènement liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes ;
- Les accès physiques ;
- Les actions de maintenance et de changement de la configuration des systèmes ;
- Les changements apportés au personnel ;
- Les actions de destruction des supports.

Les types d'événements à enregistrer sont détaillés dans la procédure de sauvegarde.

5.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'événements sont systématiquement analysés en cas de remontée d'un événement anormal (cf. section 5.4.8).

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés pendant au moins un mois sur site avant d'être archivés pendant une période de conservation indiquée dans la procédure de sauvegarde.

5.4.4 Protection des journaux d'évènements

Le mode de conservation des journaux d'événements protège leur intégrité et leur disponibilité.
Ils ne sont accessibles qu'au personnel autorisé à les exploiter.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Les journaux d'évènement sont régulièrement sauvegardés et exportés sur le site de secours.

5.4.6 Système de collecte des journaux d'évènements

Sans objet.

5.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

5.4.8 Évaluation des vulnérabilités

Pour détecter les vulnérabilités et plus généralement les anomalies, l'ACR met en place les contrôles suivants :

- Analyse quotidienne des journaux d'événements de l'ACR ;
- Contrôle de l'accès aux ARL toutes les heures ;
- Vérification de la publication et de l'archivage des ARL ;
- Vérification de la disponibilité du site de publication toutes les heures ;

- Réalisation régulière de tests d'intrusion et de scans de vulnérabilités sur les équipements et serveurs de l'IGC.

5.5 Archivage des données

5.5.1 Types de données à archiver

Les données archivées sont les suivantes :

- Toutes les versions de la présente PC/DPC ;
- Les dossiers d'enregistrement qui sont composés des formulaires de demande de certificat et d'une copie des éléments ayant permis de vérifier l'identité physique des Responsables d'ACI ;
- Les Certificats d'ACR et les ARL ;
- Les journaux d'évènements des différentes composantes de l'IGC ;
- Les rapports d'audit.

Les différents types de données à archiver sont détaillés dans la procédure d'archivage.

5.5.2 Période de conservation des archives

Les journaux d'événements sont conservés au minimum 7 ans après l'expiration du dernier Certificat émis par l'ACR.

Les dossiers d'enregistrement sont conservés durant toute la durée de vie de l'ACR.

La période de conservation des archives est détaillée dans la procédure d'archivage.

5.5.3 Protection des archives

Les archives, qu'elles soient au format papier ou électronique, sont conservées de façon à garantir leur intégrité et leur confidentialité afin que seules les personnes autorisées puissent y accéder.

Les modalités de protection des archives sont décrites dans la procédure d'archivage.

5.5.4 Procédure de sauvegarde des archives

Les archives sont périodiquement sauvegardées sous forme électronique et sont exportées sur le site de secours de l'IGC en conservant le même niveau de sécurité en matière d'intégrité et de confidentialité.

Les détails sur la procédure de sauvegarde des archives sont décrits dans la procédure de sauvegarde.

5.5.5 Exigences d'horodatage des données

Voir 6.8.

5.5.6 Système de collecte des archives

Le système de collecte des archives est uniquement interne et est détaillé dans la procédure d'archivage.

5.5.7 Procédures de récupération et de vérification des archives

Les archives, qu'elles soient au format papier ou électronique, peuvent être récupérées dans un délai inférieur à 2 jours ouvrés suite à l'acceptation par l'ACR de la demande de récupération de l'archive.

Les détails sur les procédures de récupération et de vérification des archives sont décrits dans la procédure d'archivage.

5.6 Changement de clé d'ACR

L'ACR ne peut pas générer de Certificat dont la date de fin serait postérieure à la date d'expiration de son certificat. Pour cela la période de validité du certificat de l'ACR doit toujours être supérieure à celle des Certificats qu'elle délivre.

Dès qu'une nouvelle bi-clé d'ACR est générée, seule la nouvelle Clé Privée doit être utilisée pour signer des Certificats. Le Certificat précédent reste utilisable pour valider les Certificats émis sous cette clé et ce au moins jusqu'à ce que tous les Certificats signés avec la Clé Privée correspondante aient expiré.

D'autre part, le LPCSP Board se charge de changer la bi-clé de l'ACR et le Certificat correspondant dès que les algorithmes cryptographiques utilisés dans la bi-clé ou le Certificat cessent d'être conformes aux recommandations de sécurité cryptographique concernant la taille des clés ou les algorithmes de calculs d'empreintes.

5.7 Reprise suite à la compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

L'ACR met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements.

L'ACR a mis en place un Plan de Continuité d'Activité (PCA) qui décrit la procédure à exécuter en cas d'incident majeur impactant le bon fonctionnement de l'ACR et plus particulièrement ses mécanismes de publication de l'état de révocation des Certificats qu'elle délivre.

Un incident majeur tel que la perte, la suspicion de compromission, la compromission ou encore le vol de la Clé Privée de l'ACR, est immédiatement notifié au LPCSP Board qui peut alors décider, si cela est nécessaire, de demander la révocation du certificat de l'ACR. Dans ce cas il devra notifier dans les plus brefs délais, et au maximum dans les 24 heures, le point de contact identifié sur le site https://www.ssi.gouv.fr.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'ACR ou les ACI devient insuffisant pour son utilisation prévue restante, alors l'ACR doit publier l'information sur son site Web et révoquer tout Certificat concerné.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Le PCA définit notamment les procédures de reprise en cas de corruption des ressources informatiques ainsi que les procédures visant à assurer le maintien des services de révocation et de publication de l'état de révocation des certificats qu'elle délivre.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Si la Clé Privée de l'ACR est compromise, soupçonnée d'être compromise, perdue ou détruite :

- Le LPCSP Board, après enquête, demande la révocation du certificat de l'ACR ;
- La procédure de révocation de l'ACR est appliquée ;
- Les Responsables d'ACI ayant un Certificat en cours de validité et les autres entités avec lesquels l'ACR a passé des accords ou d'autres formes de relations établies sont notifiés dans les plus brefs délais de la révocation de l'ACR ;
- L'ACR indique sur son site de publication que les Certificats et les informations de statut de révocation délivrés en utilisant cette clé d'ACR peuvent ne plus être valables ;
- Après avoir corrigé les problèmes qui ont pu causer la révocation du certificat de l'ACR, l'ACR peut décider de générer une nouvelle bi-clé et un nouveau certificat d'ACR.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le Plan de Continuité d'Activité mis en œuvre par l'ACR permet d'assurer la continuité d'activité suite à un sinistre.

5.8 Fin de vie de l'ACR

En cas de cessation définitive de l'activité de l'ACR, la procédure de fin de vie de l'ACR est appliquée.

L'ACR procède aux actions suivantes :

- La notification de l'ANSSI et des entités affectées ;
- Le transfert de ses obligations à d'autres parties ;
- La gestion du statut de révocation pour les Certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'ACR :

- Informe les ACI de la fin de vie de l'ACR ;
- Révoque tous les Certificats en cours de validité ;
- Publie une dernière ARL ;
- Prend toutes les mesures pour détruire sa Clé Privée et les éventuelles copies de secours ;
- Applique les dispositions qui ont été prises pour transférer ses obligations afin d'assurer les services suivants :
  - La publication de la dernière ARL générée ;
  - L'archivage des données (cf. section 5.5).

Ce plan est vérifié et maintenu à jour régulièrement.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'ACR

La génération de la bi-clé de l'ACR est effectuée dans le cadre d'une cérémonie des clés par au moins 2 personnes ayant des rôles de confiance et en présence d'un huissier de justice. La cérémonie se déroule dans les locaux sécurisés hébergeant l'IGC (cf. section 5.1).

La bi-clé de l'ACR est générée dans un HSM satisfaisant aux exigences de la section 6.2.11.

6.1.1.2 Clés d'ACI

La génération de la bi-clé d'une ACI est effectuée dans le cadre d'une cérémonie des clés par au moins 2 personnes ayant des rôles de confiance et en présence d'au moins un témoin de confiance (un huissier de justice par exemple). La cérémonie se déroule dans les locaux sécurisés hébergeant l'IGC (cf. section 5.1).

La bi-clé de l'ACI est générée dans un HSM satisfaisant aux exigences de la section 6.2.11.

6.1.2 Transmission de la clé privée à une ACI

Sans objet. Une ACI génère elle-même sa Clé Privée dans son propre HSM.

6.1.3 Transmission de la clé publique à l'ACR

La Clé Publique d'une ACI est transmise à l'ACR par l'AE dans une requête de certificat au format PKCS#10.

6.1.4 Transmission de la clé publique de l'ACR aux UC

La Clé Publique de l'ACR est publiée sur le site de publication de l'ACR (cf. section 2.1) dans un certificat au format X.509 v3.

L'ACR publie également l'empreinte de hachage de son certificat, afin que les UC puissent la comparer avec celle du certificat dont ils disposent.

6.1.5 Tailles des clés

Les bi-clés d'ACR et d'ACI sont des clés RSA d'une taille de 4096 bits ou supérieure.

L'ACI doit obligatoirement imposer dans sa PC/DPC à ce que les bi-clés associées aux certificats qu'elle délivre soient des clés RSA 2048 bits (ou supérieur) ou ECDSA P-256 (ou supérieur).

Les algorithmes de hachage utilisés par l'ACI pour signer les certificats qu'elle délivre doivent être d'un niveau supérieur ou égal à l'algorithme SHA-256.

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

Le LPCSP Board consulte fréquemment les normes et recommandations internationales qui concernent les algorithmes cryptographiques et les longueurs de clés afin de déterminer si les algorithmes utilisés pour les bi-clés et les Certificats sont adaptés.

Les bi-clés de l'ACR et des ACI sont générées dans des dispositifs cryptographiques certifiés avec un paramétrage respectant les normes de sécurité en la matière.

6.1.7 Objectifs d'usage de la clé

Voir l'extension « Key Usage » dans la section 7.

6.2 Mesures de sécurité pour la protection des clés privées et pour les dispositifs cryptographiques

6.2.1 Standards et mesures de sécurité pour les dispositifs cryptographiques

Les dispositifs cryptographiques utilisés pour la génération et la mise en œuvre des bi-clés de l'ACR sont des HSM certifiés satisfaisant aux exigences définies dans la section 6.2.11.

Les HSM de l'ACR sont hébergés dans les sites sécurisées de l'IGC et sont gérés exclusivement par les personnes ayant les rôles de confiance requis.

6.2.2 Contrôle de la Clé Privée

L'activation de la Clé Privée de l'ACR est réalisée par plusieurs porteurs de parts de secret qui ont nécessairement participé à la cérémonie des clés de l'ACR et au cours de laquelle leur part de secret leur avait été remise dans une carte à puce personnelle et protégée par un code PIN qu'ils avaient eux-mêmes choisis.

6.2.3 Séquestre de la Clé Privée

Les Clés Privées d'ACR et des ACI ne font pas l'objet de séquestre.

6.2.4 Copie de secours de la Clé Privée

La Clé Privée de l'ACR est sauvegardée dans le but d'avoir des copies de secours. Elle peut être sauvegardée :

- Soit hors d'un dispositif cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du dispositif cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé.
- Soit dans un dispositif cryptographique équivalent opéré dans des conditions de sécurité similaires ou supérieures.

Les sauvegardes sont réalisées sous le contrôle d'au moins deux personnes ayant les rôles de confiance adéquats dans l'ACR.

6.2.5 Archivage de la Clé Privée

Les Clés Privées ne sont pas archivées.

6.2.6 Transfert de la clé privée vers / depuis le dispositif cryptographique

La Clé Privée de l'ACR est transférée uniquement lors de la génération des copies de secours de la Clé Privée tel que décrit dans la section 6.2.4.

La création d'une copie de secours ou son import dans un HSM sont réalisés dans les locaux sécurisés de l'IGC par au moins deux personnes ayant les rôles de confiance adéquats dans l'ACR.

6.2.7 Stockage de la clé privée dans un dispositif cryptographique

Le stockage des Clés Privées des ACR et des ACI est réalisé dans un dispositif cryptographique satisfaisant aux exigences définies dans la section 6.2.11 ou en dehors d'un dispositif cryptographique moyennant le respect des exigences définies à la section 6.2.4.

6.2.8 Méthode d'activation de la clé privée

L'activation de la Clé Privée de l'ACR est réalisée dans le dispositif cryptographique de l'ACR par au moins deux personnes ayant les rôles de confiance adéquats.

6.2.9 Méthode de désactivation de la Clé Privée

La désactivation de la Clé Privée de l'ACR dans le dispositif cryptographique s'opère automatiquement lors de l'arrêt du dispositif cryptographique.

6.2.10 Méthode de destruction d'une Clé Privée

La destruction de la Clé Privée de l'ACR ne peut être effectuée qu'à partir du dispositif cryptographique. En cas de destruction, l'ACR s'assure que toutes les copies de secours de la Clé Privée de l'ACR sont également détruites.

6.2.11 Niveau de qualification des dispositifs cryptographiques

6.2.11.1 ACR

Le dispositif cryptographique de l'ACR est un HSM certifié FIPS 140-2 level 3 ou équivalent.

6.2.11.2 ACI

Le dispositif cryptographique des ACI doit être un HSM certifié FIPS 140-2 level 3 ou équivalent.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les Certificats contenant les Clés Publiques de l'ACR sont archivés conformément à la section 5.5.

6.3.2 Durées de vie des bi-clés et des Certificats

Les bi-clés et les Certificats de l'ACR ont une durée de vie maximale de 20 ans.

Les bi-clés et les Certificats d'ACI ont une durée de vie maximale de 10 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

La génération et l'installation des données d'activation de la Clé Privée de l'ACR sont réalisées lors de la cérémonie des clés, en présence d'un huissier de justice. Ces données d'activation sont stockées sur des cartes à puce associées au dispositif cryptographique de l'ACR et sont remises en main propre, durant la cérémonie, à chacune des personnes ayant le rôle de confiance de Key Holder. Ces personnes doivent prendre les mesures nécessaires pour se prémunir contre la perte, le vol et l'utilisation non autorisée de leurs cartes à puce et des données d'activation qu'elles contiennent.

6.4.2 Protection des données d'activation

Les données d'activation correspondant à la Clé Privée de l'ACR sont générées durant la cérémonie des clés par le HSM de l'ACR et sont stockées sur des cartes à puce nominatives et personnelles remises en main propre aux personnes ayant le rôle de Key Holder. Chacune de ces personnes est responsable de sa carte à puce protégée par un code PIN qu'elle a spécifiée lors de la cérémonie des clés. Elle a de plus signé une attestation de remise de sa carte à puce.

6.4.3 Autres aspects liés aux données d'activation

La destruction des données d'activation est réalisée par la destruction physique de la carte à puce les contenant ou par leur effacement définitif et irréversible.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

LEX PERSONA définit les objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès aux systèmes ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'ACR, notamment pour implémenter les principes de moindres privilèges, de contrôle multiple et de séparation des rôles) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection contre toute tentative non autorisée et / ou irrégulière d'accès aux ressources (physique et / ou logique) ;

- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent.

6.5.2 Niveau de qualification des systèmes informatiques

Pas d'exigence.

6.6 Mesures de sécurité liées au développement des systèmes

6.6.1 Mesures de sécurité liées au développement des systèmes

Tous les développements réalisés par LEX PERSONA et impactant l'IGC sont documentés et réalisés via un processus de manière à en assurer la qualité.

La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau sont documentées et contrôlées.

LEX PERSONA opère un cloisonnement entre l'environnement de développement et les environnements de pré-production et de production.

6.6.2 Mesures liées à la gestion de la sécurité

Les configurations et les mises à jour des applications sont effectuées de manière sécurisée par le personnel compétent apparaissant dans les rôles de confiance de l'ACR.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC. De plus les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé.

6.8 Horodatage / Système de datation

Les différents serveurs utilisés par l'ACR sont synchronisés au moins une fois par jour à partir de serveurs Network Time Protocol (NTP).

7 Profils des certificats et des ARL

7.1 Certificat de l'ACR

Le certificat de l'ACR est un certificat au format X.509 v3 conforme aux exigences de la [RFC 5280] et qui respecte le profil [EN 319 412-1].

Champs de base :

Champ	Valeur
Version	2 (correspond à la v3 de X.509)
Numéro de série	Défini lors de la création
Emetteur	CN = Sunnystamp Root CA G2 OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Sujet	CN = Sunnystamp Root CA G2 OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Validité	20 ans maximum
Signature	RSAwithSHA512
Clé publique	RSA 4096 bits

Extensions :

Champ	Critique	Valeur
AuthorityKeyIdentifier	Non	
BasicConstraints	Oui	CA=true
CertificatePolicies	Non	OID=2.5.29.32.0
Key Usage	Oui	keyCertSign(5), cRLSign(6)
SubjectKeyIdentifier	Non	

7.2 Certificat d'ACI

Les Certificats des ACI sont des certificats au format X.509 v3 conforme aux exigences de la [RFC 5280] et qui respectent le profil [EN 319 412-1].

Champs de base :

Champ	Valeur
Version	2 (correspond à la v3 de X.509)
Numéro de série	Défini lors de la création
Emetteur	CN = Sunnystamp Root CA G2 OI = NTRFR-480622257

	OU = 0002 480622257 O = LEX PERSONA C = FR
Sujet	CN = {*Nom de l'ACI*} OI = NTRFR-480622257 OU = 0002 480622257 O = LEX PERSONA C = FR
Validité	10 ans maximum
Signature	RSAwithSHA512
Clé publique	RSA 4096 bits

Extensions :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-caIssuers= https://pki2.sunnystamp.com/certs/sunnystamp-root-ca-g2.cer
AuthorityKeyIdentifier	Non	
BasicConstraints	Oui	cA=true pathLenConstraint=0
CertificatePolicies	Non	anyPolicy (2.5.29.32.0)
CRLDistributionPoints	Non	http://pki2.sunnystamp.com/crls/sunnystamp-root-ca-g2.crl http://pki3.sunnystamp.com/crls/sunnystamp-root-ca-g2.crl
Key Usage	Oui	keyCertSign(5), cRLSign(6)
SubjectKeyIdentifier	Non	

7.3 Profil des ARL

Champs de base :

Champ	Valeur
Version	1
Emetteur	CN = Sunnystamp Root CA G2 OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Validité	1 an
Signature	RSAwithSHA512

Extensions :

Champ	Critique	Valeur
AuthorityKeyIdentifier	Non	
CRLNumber	Non	Défini par l'ACR

8 Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'ACR fait procéder à un audit de conformité de cette composante à la présente PC/DPC.

L'ACR réalise des audits internes au moins une fois chaque année et fait réaliser tous les 2 ans, par un organisme accrédité, un audit de certification [EN 319 411-1].

8.2 Identités / qualifications des évaluateurs

L'ACR s'engage à mandater des contrôleurs qui sont compétents en sécurité des systèmes d'information et en particulier dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

Pour les audits internes, l'auditeur sera nommé par le LPCSP Board et pourra appartenir à LEX PERSONA mais devra nécessairement être indépendant de l'ACR.

Pour l'audit de certification, l'auditeur ne devra pas appartenir à LEX PERSONA ou présenter un quelconque conflit d'intérêt.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la présente PC/DPC et dans les procédures internes associées.

8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'ACR, un avis parmi les suivants : « réussite », « échec », « à confirmer ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'ACR qui peuvent être :
  - La cessation (temporaire ou définitive) d'activité,

- La révocation du Certificat de la composante,
- La révocation de l'ensemble des Certificats émis depuis le dernier contrôle positif.

- Le choix de la mesure à appliquer est effectué par l'ACR et doit respecter ses politiques de sécurité internes.
- En cas de résultat « à confirmer », l'ACR remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées.
- Puis un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'ACR confirme à la composante contrôlée la conformité aux exigences de la présente PC/DPC et des procédures internes.

8.6 Communication des résultats

Les résultats de l'audit de l'ACR sont tenus à la disposition de l'organisme de certification en charge de l'ACR.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de Certificats

Les Certificats sont fournis aux ACI gratuitement par l'ACR.

9.1.2 Tarifs pour accéder aux Certificats

Les Certificats de l'ACR sont mis à disposition des UC gratuitement via le site de publication de l'ACR.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des Certificats

L'accès aux informations d'état de révocation des Certificats via les ARL publiées par l'ACR est gratuit.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

Sans objet.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

LEX PERSONA a souscrit une assurance en responsabilité civile professionnelle couvrant ses prestations de PSCE auprès d'une compagnie d'assurance.

9.2.2 Autres ressources

LEX PERSONA dispose des ressources financières suffisantes pour assurer sa mission conformément à cette PC/DPC.

9.2.3 Couvertures et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité intervenant dans l'IGC, et sous contrat avec l'ACR, du fait d'un manquement par l'ACR à ses obligations, l'ACR pourra être amenée à dédommager l'entité dans la limite de la responsabilité de l'ACR définie dans le contrat établi entre l'ACR et l'entité.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- Les procédures internes de l'ACR ;
- Les Clés Privées de l'ACR et des composantes de l'IGC ;
- Les données d'activation associées aux Clés Privées d'ACR ;
- Les dossiers d'enregistrement des ACI ;
- Les journaux d'événements des composantes de l'IGC ;
- Les rapports d'audit ;
- Tous les secrets de l'IGC.

D'autres informations peuvent être classées comme confidentielles.

9.3.2 Informations hors du périmètre des informations confidentielles

Toutes les informations publiées par l'ACR (cf. section 2.2) ne sont pas considérées comme confidentielles.

9.3.3 Responsabilités en termes de protection des informations confidentielles

LEX PERSONA s'engage à traiter les informations confidentielles dans le respect de la législation et de la réglementation en vigueur sur le territoire français.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

LEX PERSONA s'engage à collecter et utiliser les données personnelles en respectant la législation et la réglementation européenne en vigueur relative à la protection des données à caractère personnel.

9.4.2 Informations à caractère personnel

Les données d'enregistrement des ACI qui n'apparaissent pas dans les Certificats sont considérées comme confidentielles.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

LEX PERSONA respecte, pour le traitement et la protection des données à caractère personnel, la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 [CNIL].

9.4.5 Notification et consentement d'utilisation des données personnelles

Les données personnelles ne sont jamais utilisées, sans le consentement exprès et préalable de l'ACI, à d'autres fins que celles définies dans la présente PC/DPC.

9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Les données personnelles peuvent être mis à la disposition de la justice en cas de besoin pour servir de preuve dans le cadre d'une procédure judiciaire.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par l'ACR sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerces et de services, dessins et modèles, signes distinctifs et droits d'auteur est sanctionnée par le Code de la propriété intellectuelle.

L'ACR détient tous les droits de propriété intellectuelle et est propriétaire de la présente PC/DPC et des certificats émis par l'ACR. L'ACI détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans son Certificat et dont il est propriétaire.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC/DPC et les documents qui en découlent ;
- Respecter et appliquer les procédures internes ;
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'ACR (cf. section 8) et l'organisme de qualification ;
- Documenter leurs procédures internes de fonctionnement ;

- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 LPCSP Board

Les obligations du LPCSP Board sont les suivantes :

- L'approbation de la présente PC/DPC et de ses évolutions ;
- L'audit de l'ACR ;
- La gestion de la relation contractuelle avec les entités intervenant dans l'IGC.

9.6.2 ACR

L'ACR est LEX PERSONA.

Ses obligations consistent à :

- S'assurer du respect des exigences qui la concernent et qui sont décrites dans la présente PC/DPC ;
- Rédiger les procédures internes et les guides nécessaires aux personnels de confiance de l'ACR en vue de l'accomplissement de leur mission ;
- Mettre en œuvre les ressources techniques, humaines et organisationnelles pour effectuer les prestations qui lui incombent et qui sont décrites dans la présente PC/ DPC ;
- Vérifier le respect par les différentes composantes de l'IGC, des principes de sécurité et des contrôles afférents ;
- Assurer la conformité des Certificats qu'elle délivre vis-à-vis de la présente PC/DPC.

L'ACR est responsable vis-à-vis des ACI et des UC si l'ACR n'a pas procédé à la révocation d'un Certificat, consécutivement à une demande de révocation d'un Certificat, ou n'a pas publié cette information conformément aux engagements précisés dans la présente PC/DPC.

9.6.3 AE

L'AE est LEX PERSONA.

Les obligations de l'AE sont les suivantes :

- Mettre en œuvre les moyens décrits dans la présente PC/DPC relatifs à ses obligations ;
- Définir les procédures de traitement des demandes de Certificats et de demande de révocation ;
- Vérifier avec un soin raisonnable l'apparence de conformité et la cohérence des pièces justificatives ainsi que l'exactitude des mentions qui établissent l'identité de l'ACI;
- Vérifier l'origine et l'exactitude de toute demande de révocation et mettre en œuvre les moyens permettant de les traiter ;
- Avertir l'ACR en cas d'incident.

9.6.4 ACI

Les ACI doivent respect les exigences indiquées dans la présente PC/DPC qui les concernent.

9.6.5 UC

Les obligations des UC sont les suivantes :

- Respecter les obligations décrites dans l'accord d'utilisation des Certificats ;
- Vérifier que l'extension `KeyUsage` contenue dans le Certificat est conforme à l'utilisation du Certificat ;
- Vérifier la validité de la chaîne de certification (dates de validité, signature des certificats, statut de révocation) en remontant au moins jusqu'au certificat de l'ACR.

9.7 Limite de garantie

Les limites des garanties offertes par l'ACR sont décrites dans l'accord d'utilisation des Certificats pour les UC. Ces limites sont applicables dans la limite des lois et règlements en vigueur.

9.8 Limite de responsabilité

L'ACR ne pourra être tenue responsable d'une utilisation non autorisée ou non conforme à la présente PC/DPC des Clés Privées, Certificats associés, informations de révocation, ou de tout équipement ou logiciel mis à disposition dans le cadre de cette utilisation.

Egalement, l'ACR ne pourra être tenue responsable pour tout dommage consécutif à des erreurs, inexactitudes ou omissions entachant les informations contenues dans les certificats, dès lors que ces erreurs, inexactitudes ou omissions résultent du caractère erroné des informations communiquées par l'ACI.

Enfin, l'ACR ne pourra être tenue responsable, dans la limite de la loi française, de perte financière, de perte de données ou de dommage indirect lié à l'utilisation d'un Certificat ;

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la PC/DPC

9.10.1 Durée de validité

La présente PC/DPC reste en application au moins jusqu'à la fin de vie du dernier Certificat émis par l'ACR.

9.10.2 Fin anticipée de validité

La présente PC/DPC reste en application jusqu'à son remplacement par une nouvelle version.

9.10.3 Effets de la fin de validité et clauses restant applicables

En fin de validité de la présente PC/DPC, les intervenants dans l'IGC restent liés par la présente PC/DPC pour tous les certificats émis lorsqu'elle était encore valide, jusqu'à l'expiration du dernier certificat non révoqué.

9.11 Notification individuelles et communications entre les participants

Le LPCSP Board publie une nouvelle version de la présente PC/DPC sur le site de publication de l'ACR après l'avoir validé.

9.12 Amendements

9.12.1 Procédures d'amendements

Le LPCSP Board est responsable de la création, l'approbation, la maintenance et la modification de la présente PC/DPC.

Seuls les changements mineurs dans la présente PC/DPC tels que la correction de fautes d'orthographe ou d'erreurs ne remettant pas en cause le sens de la présente PC/DPC peuvent être réalisés par le LPCSP Board sans nécessiter de notification.

9.12.2 Mécanisme et période d'information sur les amendements

Lors de tout changement important impactant la présente PC/DPC, le LPCSP Board informera les acteurs au travers d'un communiqué distribué par voie électronique ou sur son site Internet. Si besoin, une communication par courrier postal pourra être réalisée.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Si le LPCSP Board juge qu'un changement important dans la présente PC/DPC est nécessaire et qu'il a un impact majeur sur les Certificats déjà émis, il devra publier une nouvelle version de la PC/DPC intégrant un nouvel OID.

9.13 Dispositions concernant la résolution de conflits

La présente PC/DPC est soumise au droit français.

9.14 Juridictions compétentes

L'ensemble des documents contractuels est soumis à la législation et à la réglementation en vigueur sur le territoire français.

9.15 Conformité aux législations et réglementations

La présente PC/DPC est conforme à la législation et à la réglementation en vigueur sur le territoire français et notamment à la règlementation [CNIL].

9.16 Dispositions diverses

9.16.1 Accord global

Sans objet.

9.16.2 Transfert d'activités

Sans objet.

9.16.3 Conséquences d'une clause non valide

Sans objet.

9.16.4 Application et renonciation

Sans objet.

9.16.5 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

9.17 Autres dispositions

LEX PERSONA s'assure que les activités qu'elle réalise dans le cadre de cette PC/DPC sont non discriminatoires.

10 Références

[CNIL]
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

[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

[EN 319 412-1]
ETSI EN 319 412-1 V1.1.1 (2016-02)
Certificate Profiles
Part 1: Overview and common data structures

[PKCS#10]
PKCS #10: Certification Request Syntax Specification Version 1.7
November 2000
https://tools.ietf.org/html/rfc2986

[RFC 3647]
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
November 2003
https://tools.ietf.org/html/rfc3647

[RFC 5280]
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
May 2008
https://tools.ietf.org/html/rfc5280