Sunnystamp

Politique de certification

Autorité de certification
Coffreo Users AppSigning CA 2

1.3.6.1.4.1.41806.1.1.3.1

Version 1.0.0

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 – infos@lex-persona.com
SARL au capital de 30 000 Euros – R.C.S. Troyes 480 622 257 – Code NAF 6202A – TVA FR01480622257

Historique des versions

Version	Date	Nature de l'évolution
1.0.0	10/11/2015	Création du document

Table des matières

1. Introduction

1.1. Présentation générale

Le présent document est lié à l'Infrastructure de Gestion de Clés (IGC) de la plateforme Sunnystamp, développée et opérée par la société LEX PERSONA et constitue la Politique de Certification de l'AC « Coffreo Users AppSigning CA 2 ».

Il a été établi sur la base du document « Politique de Certification Type Signature » faisant partie du Référentiel Général de Sécurité de l'Etat (RGS 2.3). Ce référentiel technique liste les règles que les prestataires de service de certification électronique (PSCE) délivrant des certificats électroniques de type signature électronique doivent respecter.

1.2. Identification du document

La présente PC est identifiée par l'OID 1.3.6.1.4.1.41806.1.1.3.1

1.3. Entités intervenant dans l'IGC

1.3.1. Autorités de Certification

L'Autorité de Certification (AC) a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur l'IGC.

Les prestations de l'AC sont le résultat des fonctions suivantes qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

- Fonction d'enregistrement des Porteurs : cette fonction vérifie les informations d'identification du futur Porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. Cette fonction a également en charge, lorsque cela est nécessaire, la revérification des informations du Porteur lors du renouvellement du certificat de celui-ci.

- Fonction de génération des certificats : cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par la fonction d'enregistrement des Porteurs et de la clé publique du Porteur provenant de la fonction de génération des éléments secrets du Porteur.

- Fonction de génération des éléments secrets du Porteur : cette fonction génère le bi-clé du Porteur et un code secret de protection de la clé privée du Porteur. Ce code est par la suite appelé code de signature.

- Fonction de remise au Porteur : lorsqu'elle est utilisée, cette fonction remet au Porteur son certificat et le code secret de protection de sa clé privée.

- Fonction de publication : cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux Porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.

- Fonction de gestion des révocations : cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

- Fonction d'information sur l'état des certificats : cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et également selon un mode requête / réponse temps réel (OCSP).

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- Porteur : la personne physique identifiée dans le certificat contenant une clé publique à laquelle correspond une clé privée utilisée pour signer des documents au nom du Porteur. Les Porteurs de certificats délivrés par l'AC sont des personnes physiques représentants ou non une personne morale. Les Porteurs de certificats acceptent la présente politique de certification.

- Mandataire de certification (MC) : le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'Autorité d'Enregistrement. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des Porteurs de cette entité (il assure notamment le face-à-face pour l'identification des Porteurs lorsque celui-ci est requis).

- Utilisateur de certificat : l'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du Porteur du certificat.

  Personne autorisée : il s'agit d'une personne autre que le Porteur et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du Porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du Porteur ou d'un responsable des ressources humaines.

- L'Autorité d'Enregistrement (AE) définit et coordonne les actions d'identification des Porteurs de certificats et de vérification de leurs informations d'identification.

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats des Porteurs

Les usages sont la signature électronique de données par le Porteur du certificat (signataire).

Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

1.4.1.2 Bi-clés et certificats d'AC et de composantes

L'AC génère et signe les certificats des Porteurs ainsi que les LCR.
Pour signer ces objets, l'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (hiérarchie d'AC).

La bi-clé et le certificat de l'AC sont utilisés pour la signature de certificats et de LCR et ne sont utilisés qu'à cette fin.

1.4.2. Domaines d'utilisation interdits

Toute utilisation d'un certificat autre que celles prévues dans le cadre de la présente PC interdite. En cas de non-respect de cette interdiction, la responsabilité de LEX PERSONA ne saurait être engagée.

1.5. Gestion de la PC

1.5.1. Entité gérant la PC

La société COFFREO est responsable de cette PC.

1.5.2. Point de contact

Tout utilisateur de certificats émis par cette AC peut s'adresser à COFFREO :

- Par courrier : COFFREO - BP 201 - 91401 ORSAY CEDEX
- Par e-mail : certificat@coffreo.com
- Par téléphone : +33 (0)1 83 64 02 49

1.5.3. Entité déterminant la conformité d'une DPC avec cette PC

La détermination qu'une DPC répond ou non aux exigences de cette PC est prononcée par la Direction de COFFREO.

1.5.4. Procédures d'approbation de la conformité de la DPC

L'AC est garante de l'application de la DPC avec la Politique de Certification.
L'AC est responsable de la gestion (mise à jour, révisions) de la DPC.

1.6. Définitions et acronymes

1.6.1. Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Opérateur de Signature
PC	Politique de Certification
PE	Politique d'Enregistrement
PSCE	Prestataire de Service de Certification Electronique
RSA	Rivest Shamir Adelman
SMS	Short Message Service
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator

1.6.2. Définitions

Autorité de certification (AC)
Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification.

Certificat électronique
Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC, le terme "certificat électronique" désigne uniquement un certificat délivré à une personne physique et portant sur une bi-clé de signature, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

Code de signature
Code généré automatiquement et aléatoirement par l'AC. Il permet d'utiliser la clé privée du Porteur pour signer des documents. Lorsque ce code est fourni au Porteur, celui-ci en assume en toutes circonstances le caractère secret, et fera présumer de manière irréfragable que le Porteur est bien l'initiateur de la signature à réaliser avec sa clé privée (non-répudiation). Dans la présente PC le code de signature n'est pas fourni au Porteur mais retourné à l'AE qui pourra le communiquer aux programmes en charge de la signature des documents par le Porteur.

Déclaration des pratiques de certification (DPC)
Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Dispositif de création de signature
Il s'agit du dispositif matériel et/ou logiciel utilisé pour stocker et mettre en œuvre la clé privée de signature du Porteur.

Entité
Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

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.

Politique de certification (PC)
Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC 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 peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Porteurs et les utilisateurs de certificats.

Opérateur de signature (OS)
Personne morale en charge de gérer la clé privée du Porteur et d'effectuer des signatures pour le compte de ce dernier. Dans la présente PC, l'Opérateur de Signature est également la société COFFREO.

Porteur

Personne physique possédant un certificat dont il en est le sujet. Le Porteur est le bénéficiaire de son propre certificat.

Prestataire de services de certification électronique (PSCE)
Personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des Porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

2. Responsabilités concernant la mise à disposition des informations devant être publiées

2.1. Entités chargées de la mise à disposition des informations

La fonction de publication de l'AC met à disposition l'information sur l'état des certificats délivrés par l'AC « Coffreo Users AppSigning CA 2» par le biais d'un fichier LCR.

La LCR est accessible en HTTP à l'adresse suivante :
http://pki.sunnystamp.com/crls/coffreo-users-appsigning-ca-2.crl

2.2. Informations devant être publiées

Les informations suivantes sont diffusées via le site Sunnystamp :

- la présente PC ;
- les LCR ;
- les certificats d'AC.

2.3. Délais et fréquences de publication

Les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats de Porteurs et/ou de LCR correspondants et les systèmes les publiant assurent une disponibilité les jours ouvrés.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres 4.9 et 4.10.

A noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une non disponibilité de cette information et que les exigences ci-dessus s'appliquent également à la disponibilité des informations publiées sur ces systèmes.

2.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

En revanche, l'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC.

3. Identification et authentification

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500. Dans chaque certificat conforme à la norme X.509v3, l'AC émettrice (issuer) et le Porteur (subject) sont identifiés par un "Distinguished Name" (DN) de type [X.501].

Le DN du Porteur contient les informations suivantes :

Elément	Obligatoire	Commentaire
CN (Common Name)	Oui	Prénom(s) et nom du Porteur
O (Organization)	Oui	Société à laquelle est rattaché le Porteur
OU (Organization Unit)	Oui	N° de SIREN de la société à laquelle est rattaché le Porteur
C (Country)	Oui	Code ISO3166 du pays du Porteur
UID (Unique Identifier)	Non	Identifiant interne du Porteur
SerialNumber	Non	Numéro de série du certificat
Phone	Non	Numéro de téléphone portable du Porteur
T (Title)	Non	Titre du Porteur (ex : Mr, Monsieur, Mme, etc.)
ST (State or Province)	Non	Région du Porteur
L (Locality)	Non	Ville du Porteur

3.1.2. Nécessité d'utilisation de noms explicites

Les noms utilisés dans les champs « issuer » et « subject » d'un certificat de Porteur sont explicites dans le domaine de certification de l'AC.

3.1.3. Pseudonymisation des Porteurs

Les pseudonymes ne sont pas autorisés.

3.1.4. Règles d'interprétation des différentes formes de nom

Voir tableau 3.1.1.

3.1.5. Unicité des noms

Dans chaque certificat produit, le DN du champ « issuer » (AC émettrice) et du champ « subject » (AC ou Porteur) est unique sur le domaine de certification de l'AC.

3.1.6. Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L. 711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n°92-957 du 1 er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

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

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

Sans objet. C'est l'AC qui génère la clé privée du Porteur.

3.2.2. Validation de l'identité d'un organisme

Cf. chapitre 3.2.3.

3.2.3. Validation de l'identité d'un individu

L'AE est gérée par COFFREO. L'enregistrement d'un Porteur se fait par l'intermédiaire de l'AE. Cet enregistrement pourra être délégué à une entité tierce sous contrat avec l'AE.

3.2.4. Informations non vérifiées du Porteur

Les informations non vérifiées du Porteur dépendent du niveau de validation de son identité par l'AE ou l'entité tierce sous contrat avec l'AE.

3.2.5. Validation de l'autorité du demandeur

La validation de l'autorité du demandeur dépend des contrôles effectués par l'AE ou l'entité tierce sous contrat avec l'AE.

3.2.6. Certification croisée d'AC

Sans objet.

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

Le renouvellement de la bi-clé d'un certificat entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni au bénéficiaire sans renouvellement de la bi-clé correspondante.

3.3.1. Identification et validation pour un renouvellement courant

Toute demande de renouvellement fait l'objet d'une authentification du demandeur.

3.3.2. Identification et validation pour un renouvellement après révocation

Toute demande de renouvellement après révocation fait l'objet d'une authentification du demandeur.

3.4. Identification et validation d'une demande de révocation

Toute demande de révocation fait l'objet d'une authentification du demandeur.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Un certificat ne peut être demandé que par l'AE.

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

Les informations suivantes font partie de la demande de certificat :

- le nom du Porteur à utiliser dans le certificat ;
- les données personnelles d'identification du Porteur ;
- les données d'identification de l'entité (dans le cas où le Porteur est attaché à une entité).

Le dossier de demande est établi par l'AE.

4.2. Traitement d'une demande de certificat

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

L'identité des futurs Porteurs est vérifiée conformément aux exigences du chapitre 3.2.

L'AE ou l'entité tierce sous contrat avec l'AE effectue les opérations suivantes :

- valider l'identité du futur Porteur ;
- vérifier la cohérence des justificatifs présentés, le cas échéant ;
- s'assurer que le futur Porteur a pris connaissance des modalités applicables pour l'utilisation du certificat.

4.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le Porteur.

4.2.3. Durée d'établissement du certificat

Une fois la demande de certificat validée, le certificat est émis dans les meilleurs délais.

4.3. Délivrance du certificat

4.3.1. Actions de l'AC concernant la délivrance du certificat

Suite à la vérification de l'intégrité et de l'authenticité de la demande provenant de l'AE, l'AC déclenche le processus de génération de la bi-clé et du certificat du Porteur en suivant les étapes suivantes :

1. L'AC génère la bi-clé et le certificat en reprenant notamment les informations contenues dans la demande provenant de l'AE ;
2. L'AC génère de manière aléatoire le Code de signature ;
3. L'AC insère la clé privée et le certificat du Porteur dans un fichier au format PKCS#12 protégé (en confidentialité) par le Code de signature ;
4. L'AC retourne le fichier PKCS#12 et le Code de signature à l'OS ;
5. L'AC notifie l'AE de la bonne génération du certificat.

4.3.2. Notification par l'AC de la délivrance du certificat au Porteur

Le certificat est conservé par l'OS et n'est pas délivré au Porteur. Le Porteur est en revanche notifié explicitement ou implicitement par l'AE, ou l'entité tierce sous contrat avec l'AE, que son certificat vient d'être généré et qu'il peut l'utiliser pour signer.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

Le certificat fait l'objet d'une acceptation implicite par le Porteur suite à sa génération.

4.4.2. Publication du certificat

Le certificat ne fait pas l'objet d'une publication.

4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

L'AC informe l'AE de la délivrance du certificat.

4.5. Usages de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat par le Porteur

La clé privée du Porteur est sous la responsabilité de l'OS puisque c'est ce dernier qui détient le Code de signature et le fichier PKCS#12 permettant de l'utiliser.

Le certificat du Porteur contient la valeur « nonRepudiation » dans l'extension « KeyUsage » du certificat et ne peut être utilisé que dans le contexte de la signature électronique de documents.

L'utilisation d'une clé privée n'est autorisée que pendant la période de validité du certificat associé et vaut, pour l'AC, l'acceptation des conditions d'usage par le Porteur dont l'AE se sera préalablement assuré.

4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Cf. chapitre précédent et chapitre 1.4. Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6. Renouvellement d'un certificat

Conformément au [RFC3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du Porteur).

Dans la cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante.

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 au Porteur 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'AC aux autres entités de la délivrance du nouveau certificat

Sans objet.

4.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

4.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des bénéficiaires, et les certificats correspondants, seront renouvelés au minimum tous les cinq ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat (cf. chapitre Révocation et suspension des certificats, notamment le chapitre Certificats de Porteurs pour les différentes causes possibles de révocation).

4.7.2. Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat du Porteur peut être automatique ou bien à l'initiative du Porteur.

4.7.3. Procédure de traitement d'une demande d'un nouveau certificat

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3.
Pour les actions de l'AC, cf. chapitre 4.3.1.

4.7.4. Notification au Porteur de l'établissement du nouveau certificat

Sans objet.

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.7.6. Publication du nouveau certificat

Cf. chapitre 4.4.2.

4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre 4.4.3

4.8. Modification du certificat

La modification d'un certificat entraîne obligatoirement le renouvellement du certificat et de la bi-clé correspondante.
Une modification sans renouvellement est interdite.

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 au Porteur 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'AC aux autres entités de la délivrance du certificat modifié

Sans objet.

4.9. Révocation et suspension des certificats

Il n'y a pas de suspension possible de certificat. Seule la révocation définitive des certificats peut être réalisée.

4.9.1. Causes possibles d'une révocation

4.9.1.1 Certificats de Porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un Porteur :

- les informations du Porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple le changement d'entité du Porteur), ceci avant l'expiration normale du certificat ;
- le Porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le Porteur n'a pas respecté les obligations découlant de la PC de l'AC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du Porteur ;
- la clé privée du Porteur est suspectée de compromission, est compromise, est volée ;
- le Porteur ou une entité autorisée (représentant légal de l'entité par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du Porteur et/ou de son support) ;
- le décès du Porteur ou la cessation d'activité de l'entité du Porteur (dans le cas où le Porteur est attaché à une entité).

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

4.9.1.2 Certificats 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 (y compris un certificat d'AC pour la génération de certificats et/ou de LCR) :

- suspicion de compromission, compromission, perte ou vol de la 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 DPC (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 Certificats de Porteurs

Les personnes / entités qui peuvent demander la révocation d'un certificat de Porteur sont les suivantes :
- le Porteur au nom duquel le certificat a été émis ;
- l'AC émettrice du certificat ;
- l'AE à l'origine de la création du certificat.

Nota : Le Porteur doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat.

4.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité responsable de l'AC.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat de Porteur

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre 3.4.

La demande de révocation doit comporter au minimum :
- l'identité du Porteur ;
- le prénom et nom du demandeur de la révocation ;
- le DN du Porteur ou toute autre information (par exemple : le numéro de série du certificat) permettant d'identifier de façon certaine le certificat devant être révoqué ;
- la cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

L'information de révocation est alors diffusée via une nouvelle LCR signée par l'AC indiquera désormais que le certificat est révoqué.

L'opération est enregistrée dans les journaux d'évènements avec notamment les informations sur les causes initiales ayant entraîné la révocation du certificat.

4.9.3.2 Révocation d'un certificat d'une composante de l'IGC

Les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC sont précisés dans la DPC associée à cette PC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des Porteurs concernés que leurs certificats ne sont plus valides.

4.9.4. Délai accordé au Porteur pour formuler la demande de révocation

Dès que le Porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

4.9.5. Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Révocation d'un certificat de Porteur

Par nature une demande de révocation est traitée en urgence.

La fonction de gestion des révocations est disponible 24h/24 7j/7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 1h et une durée maximale totale d'indisponibilité par mois de 4h.

Toute demande de révocation d'un certificat est traitée dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

4.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (signature de certificats et/ou de LCR / LAR) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de Porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

4.9.7. Fréquence d'établissement des LCR

La fréquence de publication des LCR est de 7 jours.

4.9.8. Délai maximum de publication d'une LCR

La LCR est publiée dans un délai maximum de 30 minutes après sa 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 de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre 4.9.6 ci-dessus.

4.9.11. Autres moyens disponibles d'information sur les révocations

Aucun autre moyen n'est disponible.

4.9.12. Exigences spécifiques en cas de compromission de la clé privée

Il n'y a pas de mesures particulières, concernant les clés privées des Porteurs, autres que la révocation des certificats correspondants.

4.9.13. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée.

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

L'AC fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine).
Les LCR sont des LCR au format V2 et sont publiées sur un serveur Web accessible librement par l'intermédiaire du protocole HTTP.

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats par l'intermédiaire de la LCR est disponible 24h/24 7j/7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4h et une durée maximale totale d'indisponibilité par mois de 32h.

4.10.3. Dispositifs optionnels

Sans objet.

4.11. Fin de la relation entre le Porteur et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et le Porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier est révoqué.

4.12. Séquestre de clé et recouvrement

Les clés privées d'AC ne sont pas séquestrées.

Les clés privées des Porteurs ne sont pas séquestrées au sens conventionnel du terme puisqu'elles sont stockées par l'OS sous son contrôle exclusif.

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

Ce chapitre présente un ensemble de mesures non techniques concernant la sécurité de l'IGC.

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

La construction des sites respecte les règlements et les normes en vigueur. La localisation géographique des sites n'est pas dans des zones à risques (explosion, tremblement de terre, inondation).

5.1.2. Accès physique

Un système de contrôle d'accès nominatif est mis en place. Il est strictement limité aux seules personnes autorisées. Il garantit aussi la traçabilité des accès.

5.1.3. Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les exigences des conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.
Elles permettent également de respecter les exigences de la présente PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestions des révocations et d'information sur l'état des certificats.

5.1.4. Vulnérabilité aux dégâts des eaux

L'IGC respecte les exigences de protection contre les dégâts des eaux. Elles permettent de respecter les exigences de la présente PC 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 en matière de disponibilité de ses fonctions.

5.1.6. Conservation des supports

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.
Des procédures de gestion ont été rédigées afin de protéger les supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC est engagée à conserver ces informations.

5.1.7. Mise hors service des supports

En fin de vie, les supports sont détruits de manière sécurisée.

5.1.8. Sauvegardes hors site

Aucune sauvegarde hors site n'est actuellement effectuée.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiances

L'IGC comprend les rôles suivants :

- Responsable de sécurité : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.

- Responsable d'application : Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

- Ingénieur système : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.

- Opération : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.

- Contrôleur : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

5.2.2. Nombre de personnes requises par tâches

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

5.2.3. Indentification et authentification pour chaque rôle

Toute personne intervenant dans le fonctionnement de l'IGC doit avoir préalablement reçu le rôle correspondant.
L'affectation des rôles est tracée.
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 sont interdits :

- Responsable de sécurité et ingénieur système.

5.3. Mesures de sécurité vis-à-vis du personnel

5.3.1. Qualifications, compétences et habilitations requises

Le personnel travaillant pour l'une des composantes de l'IGC est soumis à une clause de confidentialité vis-à-vis de l'employeur.
Les fonctions demandées à chaque membre du personnel doivent être compatibles avec ses compétences. Notamment, le personnel d'encadrement doit avoir l'expertise nécessaire et être familier des procédures de sécurité.

L'AC informe toute personne intervenant dans les rôles de confiance de l'IGC :

- De ses responsabilités relatives aux services de l'IGC,
- 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'IGC est soumis à une procédure de vérification de ses antécédents lors de leur prise de fonction.

Pour les rôles de confiance, des vérifications sont menées en plus tous les 3 ans.

Les vérifications portent sur les points suivant :

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

Les membres du personnel devront fournir le bulletin n°3 de leur casier judiciaire.

5.3.3. Exigences en matière de formation initiale

Le personnel travaillant pour l'une des composantes de l'IGC sera formé. Cette formation lui permettra de prendre conscience des enjeux de sécurité.

5.3.4. Exigences et fréquence en matière de formation continue

Le personnel concerné recevra une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation en fonction de la nature de ces évolutions.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Aucune exigence particulière.

5.3.6. Sanctions en cas d'actions non autorisées

Les sanctions sont communiquées au personnel avant la prise de fonction.

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

Les exigences du paragraphe 5.3 sont applicables aux prestataires externes.

5.3.8. Documentation fournie au personnel

Le personnel doit prendre connaissance des procédures concernant les fonctions de chacun.

5.4. Procédures de constitution des données d'audit

5.4.1. Type d'événement 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 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.

De plus, les événements ci-dessous doivent être recueillis par des moyens automatiques ou manuels :

- Réception d'une demande de certificat,
- Validation / Rejet d'une demande de certificat,
- Evénement liés aux clés de signature et aux certificats d'AC (génération, sauvegarde / récupération, révocation, renouvellement, destruction…)
- Génération des éléments secrets du serveur,
- Transmission des certificats aux RCC et, selon les cas, acceptations / rejets explicites par les RCC,
- Remise du dispositif de création de cachet du serveur au RCC,
- Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.),
- Réception d'une demande de révocation,
- Validation / rejet d'une demande de révocation,
- Génération puis publication des CRL,
- Les requêtes et réponses OCSP,

Chaque enregistrement est composé comme ceci :

- Type de l'évènement,
- Nom de l'exécutant ou référence du système déclenchant l'événement,
- Date et heure de l'événement,
- Résultat de l'événement.

En fonction de l'événement, l'enregistrement devra également contenir les champs suivants :

- Destinataire de l'opération,
- Nom du demandeur de l'opération ou référence du système effectuant la demande,
- Nom des personnes présentes,
- Cause de l'événement,
- Toute information caractérisant l'événement.

5.4.2. Fréquence de traitement des journaux d'événements

Cf. chapitre 5.4.8 ci-dessous.

5.4.3. Période de conservation des journaux d'événements

Les journaux sont conservés sur site pendant 1 mois.
Ils sont archivés au plus tard 1 mois après leur génération.

5.4.4. Protection des journaux d'événement

Le mode de conservation des journaux d'événements protège leur intégrité et leur disponibilité.
Le niveau de confidentialité de chaque type d'événements a été classé. Les moyens de protection de la confidentialité des journaux sont adaptés à cette classification.
Le système de datation des événements respecte les exigences du paragraphe 6.8.

5.4.5. Procédures de sauvegarde des journaux d'événements

Les événements sont sauvegardés, puis exporter sur un support de sauvegarde.

5.4.6. Système de collecte des journaux d'événements

Sans objet.

5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement

Sans objet.

5.4.8. Evaluation des vulnérabilités

Les journaux d'événements sont contrôlés une fois par jour ouvré afin de détecter toutes anomalies liées à des tentatives en échec.
Les journaux sont également analysés dans leur totalité une fois toutes les 2 semaines.

5.5. Archivage des données

5.5.1. Types de données à archiver

En plus des journaux, les pièces suivantes sont également archivées :

- Les logiciels,
- Les PC,
- Les DPC,
- Les accords contractuels avec d'autres AC,
- Les certificats et CRL tels qu'émis ou publiés,
- Les récépissés,
- Les engagements signés des MC,
- Les justificatifs d'identité des RCC,
- Les justificatifs de possession des serveurs ainsi que leurs noms,
- Les journaux d'événements des différentes entités de l'IGC.

5.5.2. Période de conservation des archives

Les archives sont conservées pendant minimum 5 ans. Le RCC ainsi que les MC sont informés de ces données lors de la prise d'engagement.

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes sont :

- Protégées en intégrité,
- Accessibles aux personnes autorisées,
- Relues et exploitées.

5.5.4. Procédure de sauvegarde des archives

Une procédure de sauvegarde des archives est définie. Elle est détaillée dans la DPC.

5.5.5. Exigence d'horodatage des données

Les journaux d'événement sont datés (cf. chapitre 5.4.4).
Le paragraphe 6.8 précise les exigences relatives au système de datation des événements.

5.5.6. Systèmes de collecte des archives

Sans objet.

5.5.7. Procédures de récupération et de vérification des archives

Seule l'AC peut accéder à l'ensemble des archives. Les composantes de l'IGC ne peuvent accéder qu'aux archives de la composante.

Le délai de récupération d'une archive est inférieure à 2 jours ouvrés.

5.6. Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.

Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC 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.

5.7. Reprise suite à compromission et sinistre

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

Les procédures de remontée et de traitement sont mises en place par le personnel de l'AC. La DPC détaille le fonctionnement de ces procédures.
Dans le cadre d'un incident majeur, le responsable de l'AC en est informé dans le plus bref délai. Les incidents majeurs sont traités en première urgence. Cela peut donner lieu à la révocation d'un certificat d'AC (voir paragraphes 4.9.3.2 et 4.9.5.2).

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

Le plan de reprise d'activité définit les modalités de reprise en cas de corruption des ressources informatiques. La DPC donne plus d'informations sur ces modalités.
Le plan de continuité est testé une fois tous les deux ans.

5.7.3. Procédures de reprise en cas de corruption de la clé privée de la composante

Dans le cas d'une compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué.

En outre, l'AC doit au minimum respecter les engagements suivants :

- informer les entités suivantes de la compromission : tous les Porteurs, MC et les autres entités avec lesquelles l'AC a passé des accords ou à d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information doit être mise à disposition des autres tiers utilisateurs ;
- indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

5.7.4. Capacités de continuité d'activité suite à un sinistre

La capacité de continuité d'activité suite à un sinistre est traitée dans le cadre du plan de continuité.

5.8. Fin de vie de l'ICG

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC a pris les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC a pris les dispositions suivantes :

- Mise en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage.
- Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des CRL), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.

Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement).
La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des CRL conformément aux engagements pris dans sa PC.

L'AC doit stipuler dans ses pratiques les dispositions prises en cas de cessation de service. Elles doivent inclure :

- Les notifications 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'AC doit :

1- S'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats,
2- Prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante,
3- Révoquer son certificat,
4- Révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité,
5- Informer tous les Porteurs des certificats révoqués ou à révoquer.

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'AC

Les clés de signature d'AC sont générées et mises en œuvre dans un module logiciel sécurisé de l'IGC.

6.1.1.2 Clés Porteurs générées par l'AC

La génération des clés privées des Porteurs est effectuée par l'AC dans un environnement sécurisé conformément au chapitre 5.

Les clés privées des Porteurs sont stockées par l'OS

6.1.1.2.1 Clés Porteurs générées par le Porteur

Les Porteurs ne peuvent pas générer leur clé.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée n'est pas transmise à son propriétaire.

6.1.3. Transmission de la clé publique à l'AC

Sans objet. La bi-clé n'est pas générée par le Porteur.

6.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

La clé publique de vérification de l'AC est diffusée sous la forme d'un certificat numérique au format X.509v3 qui est téléchargeable sur le site Web de l'AC.

6.1.5. Tailles des clés

Les clés des Porteurs utilisent l'algorithme RSA et ont une taille de 2048 bits.

La clé de l'AC utilise l'algorithme RSA et a une taille de 2048 bits.

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats et de LCR / LAR (cf. chapitre 1.4.1.2).

L'utilisation de la clé privée du Porteur et du certificat associé est définie dans la Politique de Services de l'OS.

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

Sans objet.

6.2.2. Contrôle de la clé privée par plusieurs personnes

Sans objet.

6.2.3. Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des certificats émis ne sont en aucun cas séquestrées.

6.2.4. Copie de secours de la clé privée

Sans objet.

6.2.5. Archivage de la clé privée

Les clés privées de l'AC et les clés privées des Porteurs ne font en aucun cas l'objet d'archivage.

6.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Sans objet.

6.2.7. Stockage de la clé privée dans un module cryptographique

Sans objet.

6.2.8. Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

La méthode d'activation est précisée au niveau de la DPC.

6.2.8.2 Clés privées des Porteurs

Sans objet.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

Sans objet.

6.2.9.2 Clés privées des Porteurs

Sans objet.

6.2.10. Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

Sans objet.

6.2.10.2 Clés privées des Porteurs

La destruction de la clé privée du Porteur consiste pour l'OS à effacer de manière sécurisée la clé privée.

6.2.11. Niveau de qualification du module cryptographique et des dispositifs de création de signature

Sans objet.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des Porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des Porteurs couverts par la présente PC ont une durée de vie d'un an non renouvelables.

La bi-clé et le certificat de l'AC a une durée de vie de 10 ans.

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

6.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation correspondant à la clé privée de l'AC sont décrites dans la DPC.

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du Porteur

Lors de la génération de la clé privée d'un Porteur, l'AC génère aléatoirement un code de signature de 4 caractères minimum et le transmet à l'OS.

L'AC ne conserve pas ce code de signature.

6.4.2. Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

La protection des données d'activation correspondant à la clé privée de l'AC est décrite dans la DPC.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des Porteurs

A aucun moment l'AC ne conserve le code de signature permettant de protéger la clé privée d'un Porteur.

6.4.3. Autres aspects liés aux données d'activation

La présente PC ne formule pas d'exigence spécifique sur le sujet.

6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes informatiques supportant les fonctions de l'AC sont contraints aux règles de sécurité suivantes :

- identification et authentification forte des utilisateurs pour l'accès aux systèmes (authentification à deux facteurs, de nature physique et/ou logique),
- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôle multiples et de séparation des rôles),
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- 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 du réseau contre toute intrusion d'une personne non autorisée,
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- fonctions d'audits (non-répudiation et nature des actions effectuées),
- gestion des reprises sur erreur.

Des dispositifs de surveillance avec remontée automatique et des procédures d'audit sont mises en place au sein des systèmes d'informations.

6.5.2. Niveau de qualification des systèmes informatiques

Sans objet.

6.6. Mesures de sécurité liées au développement des systèmes

6.6.1. Mesures liées à la gestion de la sécurité

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC est documentée et respecte dans la mesure du possible des normes de modélisation et d'implémentation. La configuration du système, des composantes, ainsi que toute modification et mise à niveau, sont documentées et contrôlées.

6.6.2. Niveau d'évaluation sécurité du cycle de vie des systèmes

La présente PC ne formule pas d'exigence spécifique sur le sujet.

6.7. Mesures de sécurité réseau

L'architecture réseau des systèmes informatiques de l'IGC respecte les bonnes pratiques en matière de sécurité réseau : cloisonnement, séparation des environnements, règles de filtrage, antivirus, système anti-intrusion, doublement des équipements réseaux...

L'infrastructure réseau subit régulièrement des audits de sécurité de type boite noire et boite blanche.

6.8. Horodatage / Système de datation

L'AC horodate tous les journaux d'événement avant l'envoi à l'archivage.

Cet horodatage se base sur un serveur de temps interne synchronisé sur deux sources de temps en strate 1, celle de l'observatoire de Paris Meudon et l'Observatoire de Besançon.

La précision de temps est inférieure à 1 seconde.

7. Profils des certificats et des LCR

7.1. Profil des certificats

7.1.1. Champs de base

Champ	Valeur	Commentaire
Version	2	Correspond à la valeur 3 de X. 509
Algorithme de signature	1.2.840.113549.1.1.11	OID de l'algorithme de signature utilisé identifiant l'algorithme sha256WithRSAEncryption
Emetteur	CN = Coffreo Users AppSigning CA 2 OU = 0002 498277805 O = COFFREO L = ORSAY C = FR	Distinguished Name (DN) de l'AC
Numéro de série	Numéro de série du Porteur	Identifiant unique
Durée de validité	Un an à partir de la date de génération	
Sujet	CN = *Nom et prénom du Porteur* O = *société du Porteur* OU = *n° SIREN de la société du Porteur* T = *titre du porteur* UID = *Identifiant interne du Porteur* SerialNumber = *Numéro de série* Phone = *n° de téléphone portable du Porteur* ST = *région du porteur* L = *ville du Porteur* C = *pays du Porteur*	Distinguished Name (DN) du Porteur Les champs T, SerialNumber, UID, Phone, ST et L sont optionnels.

7.1.2. Extensions

Champ	Valeur	Commentaire
AuthorityKeyIdentifier	3d a7 8b ec 51 8f f6 03 b5 27 8f 7b 3c 28 0b ee e6 9a 6a a2	Identifiant de la clé publique de l'AC
BasicConstraints	cA=false	Certificat d'entité finale
CertificatePolicies	1.3.6.1.4.1.41806.1.1.3.1	OID de la PC que respecte le certificat.
CRLDistributionPoints	http://pki.sunnystamp.com/crls/coffreo-users-appsigning-ca-2.crl	URL où peut être téléchargée la LCR
KeyUsage	nonRepudiation	
SubjectAltName	Adresse email du Porteur	
SubjectKeyIdentifier	Empreinte SHA-1 de la clé publique du Porteur	

7.1.3. Longueur des clés

7.1.3.1 Clés d'AC

La bi-clé de l'AC est d'une complexité de 2048 bits pour l'algorithme RSA.

7.1.3.2 Clés des Porteurs

Les bi-clés des certificats des Porteurs émis sont d'une complexité de 2048 bits pour l'algorithme RSA.

7.2. Profil des LCR

7.2.1. Champs de base

Champ	Valeur	Commentaire
Version	1	Correspond à la version 2
Algorithme de signature	1.2.840.113549.1.1.11	OID de l'algorithme de signature utilisé identifiant l'algorithme sha256WithRSAEncryption
Emetteur	CN = Coffreo Users AppSigning CA 2 OU = 0002 498277805 O = COFFREO L = ORSAY C = FR	Distinguished Name (DN) de l'AC ayant délivré la LCR

7.2.2. Extensions de LCR

Champ	Valeur	Commentaire
AuthorityKeyIdentifier	3d a7 8b ec 51 8f f6 03 b5 27 8f 7b 3c 28 0b ee e6 9a 6a a2	Identifiant de la clé publique de l'AC ayant signé la LCR
CRLNumber	Numéro de la LCR	Ce numéro séquentiel est incrémenté de 1 lorsqu'une nouvelle LCR est publiée

7.2.3. Extensions d'entrée de LCR

Les extensions d'entrées de LCR sont conformes aux exigences de la RFC 5280.

7.3. Profil OCSP

Sans objet.

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'AC procède à un contrôle de conformité de cette composante.

8.2. Identités / qualifications des évaluateurs

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, LEX PERSONA procède à un contrôle de conformité de cette composante. LEX PERSONA procède également régulièrement à un contrôle de conformité de l'ensemble de son IGC, au moins une fois tous les trois ans.

8.3. Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

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 PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC un avis parmi les suivants : "réussite", "échec", "à confirmer". L'AC prend alors, et fait prendre, les mesures requises en fonction des conclusions du contrôle.

8.6. Communication des résultats

Les résultats des audits de conformité doivent être tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

9.1.2. Tarifs pour accéder aux certificats

Sans objet.

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

Sans objet.

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 justifie d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'elle pourrait devoir aux Utilisateurs d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle. LEX PERSONA déclare disposer d'une assurance professionnelle couvrant ses prestations de certification électronique souscrite auprès de la compagnie Allianz sous le numéro de police 41685247.

9.2.2. Autres ressources

Sans objet.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- la partie non-publique de la DPC de l'AC,
- les clés privées de l'AC, des composantes et des Porteurs de certificats,
- les données d'activation associées aux clés privées d'AC et des
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les dossiers d'enregistrement des Porteurs,
- les causes de révocations, sauf accord explicite du Porteur.

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

9.4.2. Informations à caractère personnel

Toutes les données d'enregistrement des Porteurs sont considérées comme personnelles.

9.4.3. Informations à caractère non personnel

Aucune exigence particulière.

9.4.4. Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français.

9.4.5. Notification et consentement d'utilisation des données personnelles

Conformément aux législations et réglementations en vigueur, en particulier sur le territoire français, les informations personnelles remises par les Porteurs à l'AC ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du Porteur, décision judiciaire ou autre autorisation légale.

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

Cf. législation et réglementation en vigueur sur le territoire français.

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 LEX PERSONA sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de leur non-respect. Par exemple, conformément à la loi n°98-536 du 1er juillet 1998 (Journal officiel du 2 juillet 1998, p.10075) et à la directive européenne 96/6/CE du 11 mars 1996, les bases de données réalisées par Lex Persona sont protégées. Le texte de la loi peut être consulté sur le site suivant : http://www.legifrance.gouv.fr (Interprétations contractuelles et garanties).

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 PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8) et l'organisme de qualification,

- respecter les accords ou contrats qui les lient entre elles ou aux Porteurs,
- 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. Autorités de Certification

L'AC garantit le respect des exigences définies dans la présente PC ainsi que dans la DPC associée. Quels que soient les recours à des entités extérieures pour la mise en œuvre de son activité de certification, l'AC garantit le respect de ces exigences par chacune de ces entités.

L'AC a pour obligation de :
- pouvoir démontrer aux applications utilisatrices de ses certificats, qu'elle a émis un certificat pour un Porteur donné et que ce Porteur a accepté le certificat, conformément au 4.4 ;
- tenir à disposition des Porteurs et des utilisateurs la LCR ;
- garantir la cohérence entre la PC et la DPC associée ;
- s'assurer que ses Porteurs connaissent leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

9.6.2. Service d'enregistrement

Lorsque l'AE est saisie d'une demande de certificat, elle doit :
- 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 du Porteur selon les procédures ;
- transmettre la demande de certificat au service de génération des certificats de l'AC ;

9.6.3. Porteurs de certificats

Le Porteur a le devoir de :
- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- informer l'AE de toute modification concernant les informations contenues dans son certificat ;

9.6.4. Utilisateurs de certificats

Les utilisateurs de la sphère publique utilisant les certificats doivent :
- vérifier et respecter l'usage pour lequel un certificat a été émis ;
- pour chaque certificat de la chaîne de certification, du certificat du Porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

9.6.5. Autres participants

Sans objet.

9.7. Limite de garantie

Sans objet.

9.8. Limite de responsabilité

Sans objet.

9.9. Indemnités

Sans objet.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

La PC de l'AC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2. Fin anticipée de validité

La publication d'une nouvelle version de la présente PC Type peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.

En fonction de la nature et de l'importance des évolutions apportées à la PC Type, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

9.10.3. Effets de la fin de validité et clauses restant applicables

Sans objet.

9.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC s'engage à :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes.
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

L'AC contrôlera que tout projet de modification de sa PC reste conforme aux exigences de la présente PC et des éventuels documents complémentaires. En cas de changement important, l'AC pourra faire appel à une expertise technique pour en contrôler l'impact.

9.12.2. Mécanisme et période d'information sur les amendements

Sans objet.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des Porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

9.13. Dispositions concernant la résolution de conflits

La présente PC est soumise au Droit français.

9.14. Juridictions compétentes

La présente politique de certification est expressément élaborée, régie, appliquée et interprétée selon les lois et règlements français, bien que les activités qui découlent de la présente Politique de Certification puissent avoir des effets juridiques en-dehors du territoire de la République française.

9.15. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 0 ci-dessous.

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

Sans objet.

10. Annexe 1 : Documents cités en référence

10.1. Réglementation

Renvoi	Document
[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.
[DIRSIG]	Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005.
[SIG]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

10.2. Documents techniques

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 1.0
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[RFC5280]	IETF - Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile – mai 2008
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complétée par les correctifs techniques n° 1 d'octobre 2001, n° 2 d'avril 2002 et n° 3 d'avril 2004)