POLITIQUE DE CERTIFICATION

Autorité de certification

« Certeurope Root CA 3»

Identification (OID) : 1.2.250.1.105.8.1.1.0

Version : 1.0
Mise à jour : 01
Date de création : 19 juillet 2010
Dernière MAJ : 9 avril 2015
Etat du document : Officiel
Rédigé par : CertEurope
Vérifié par : Comité PKI
Approuvé par : Comité PKI

CertEurope, une société du groupe Oodrive
www.certeurope.fr
26, rue du Faubourg Poissonnière, 75010 Paris – France
Tel : +33 (0)1 45 26 72 00 / Fax : +33 (0)1 45 26 72 01

MODIFICATIONS			
Date	Etat	Version	Commentaires
19/07/2010	Officiel	1.0	
09/04/2015	Officiel	1.0 Mise à jour 01	Mise à la nouvelle charte graphique. Corrections de forme et précision sur le délai de publication des LAR

SOMMAIRE

I. Introduction

I.1. Présentation générale

CertEurope offre la possibilité de certifier les clés de signature des Autorités de Certification par son Autorité de Certification Racine CERTEUROPE ROOT CA 3. Cette possibilité offre :

- d'une part, la mutualisation d'une seule Autorité de Certification Racine entre les différentes AC,
- d'autre part, un vecteur de reconnaissance mutuelle de certificats d'abonné émis par les différentes Autorités subordonnées.

La Politique de Certification définie dans le présent document décrit les obligations des parties prenantes dans le cadre du service de certification des clés de signature d'Autorités subordonnées.

En vertu de la présente politique, les certificats ne seront délivrés qu'à des Autorités de Certification. La délivrance de certificat pour le compte d'un abonné personne physique est exclue.

L'AC Racine CERTEUROPE ROOT CA 3 sera assujettie aux lois et règlements en vigueur sur le territoire de la République française, ainsi qu'aux normes européennes en vigueur et aux conventions internationales ratifiées par la France, et qui touchent à l'application, l'élaboration, l'interprétation et la validité des politiques de certification mentionnées dans le présent document.

L'AC Racine CERTEUROPE ROOT CA 3 se réserve le droit de conclure des accords de certification croisée avec une ou des autorités de certification tierces.

La présente Politique de Certification s'applique à la délivrance et l'utilisation de certificats de type Autorité de Certification.

Cette politique a été conçue pour être utilisée dans certaines situations, et indique les rôles et responsabilités spécifiques

- de l'AC Racine,
- de l'autorité d'enregistrement,
- des AC subordonnées,

Ce document a été établi sur la base de la Politique de Certification type de l'Etat (RGS).

I.2. Identification du document

La présente PC est identifiée par l'OID 1.2.250.1.105.8.1.1.0.

Les Politique de Certification et Déclaration des Pratiques de Certification sont ci-après désignées sous le nom de "PC" et de "DPC".

- Iso(1)
  - member-body(2)
    - fr(250)
      - type-org(1)
        - CertEurope (105)
          - Certeurope Root CA 3 (8)
            - PC Certeurope Root CA 3(1)
              - Version majeure (1)
                - Version mineure (0)

I.3. Entités intervenant dans l'IGC

L'Infrastructure de Gestion des Clés (IGC) est composée de plusieurs entités, lesquelles sont décrites ci-après.

I.3.1. Autorités de certification

L'autorité à laquelle les utilisateurs des services de certification accordent leur confiance pour la création et l'émission de certificats est appelée Autorité de Certification et notée dans le document AC.

Une AC est un Prestataire de Services de Certification Electronique (PSCE) qui délivre des certificats.

Cette entité est responsable des certificats signés en son nom et de la fourniture des services de certification ci-dessous :

- **Service d'enregistrement** : vérifie les informations d'identification et l'habilitation de la personne physique, le mandataire.
- **Service de génération des certificats** : génère et signe les certificats à partir des informations transmises par le service d'enregistrement.
- **Service de publication et diffusion** : met à disposition des différentes parties concernées, les politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux mandataires, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides des AC Subordonnées.
- **Service de gestion des révocations** : traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via le service d'information sur l'état des certificats.
- **Service d'information sur l'état des certificats** : fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, valide, etc.).

L'Autorité de Certification Racine est responsable vis-à-vis de ses clients, mais aussi de toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification, et donc de la validité des certificats qu'elle émet. A ce titre, elle édicte la Politique de Certification et valide les Déclarations de Pratique de Certification qui doivent identifier les obligations de toutes les entités participant aux services de l'AC.

La garantie apportée par l'Autorité de Certification vient de la qualité de la technologie mise en œuvre, mais aussi du cadre réglementaire et contractuel qu'elle définit et s'engage à respecter.

En vertu de cette politique, L'AC Racine CERTEUROPE ROOT CA 3 est chargée:

- de créer et de signer des certificats liant les Autorités subordonnées et leurs bi-clés
- de faire connaître l'état des certificats par l'intermédiaire des LCR
- de faire respecter la PC et la DPC par les différentes composantes de l'AC Racine, et les Autorités subordonnées

La fonction d'enregistrement des certificats fait partie des fonctions indispensables d'une ICP, elle est assurée par l'Autorité d'Enregistrement.

I.3.2. Autorités d'enregistrement

L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification racine et l'Autorité subordonnée. En vertu de cette Politique de Certification, une AE est responsable de toutes les tâches qui lui sont assignées par l'AC.

L'AE applique des procédures d'identification des personnes physiques et morales responsables de la composante Autorité subordonnée à certifier, conformément aux règles définies par l'Autorité de Certification. Son but est :

- d'établir l'identité du demandeur,
- de distribuer le certificat au responsable de l'Autorité subordonnée,

- de maintenir, administrer, exploiter et protéger les machines et logiciels utilisés pour remplir ces fonctions.

L'AE a également pour tâche de réceptionner les demandes de révocation de certificats et doit les traiter.

L'AE archive les dossiers de demande de certificat ou de révocation.

Les fonctions de l'AE sont exécutées par des personnels désignés et agréés par le responsable de l'AC racine ; ces personnels ont connaissance et respectent les règles, principes et procédures énoncées dans la PC et la DPC.

I.3.3. Mandataire de Certification

Le Mandataire de Certification est une personne physique dûment identifiée et désignée par le demandeur afin de le représenter pour effectuer une demande de création de certificat d'Autorité de Certification subordonnée.

I.3.4. Porteurs de certificats

Les seuls porteurs de certificats émis par l'AC CERTEUROPE ROOT CA 3 sont les entités à qui se rattachent les certificats des AC subordonnées. Ces entités sont représentées par leur mandataire de certification ou leur représentant légal.

En vertu de cette Politique de Certification, une Autorité subordonnée est une personne morale qui obtient un certificat d'AC des services de l'AC Racine CERTEUROPE ROOT CA 3.

L'Autorité subordonnée est responsable :

- de l'authenticité, de l'exactitude, et de la complétude des données d'identification fournies à l'AE lors de l'enregistrement,
- d'établir et de faire respecter la politique de sécurité sur le ou les systèmes informatiques utilisés pour mettre en oeuvre le ou les certificats générés par l'AC Racine ainsi que la ou les clés privées associées.
- de la protection, de l'intégrité et de la confidentialité de la clé privée de l'Autorité subordonnée, et des éventuelles données d'activations,
- de la sécurité de ses équipements matériels, logiciels et de ses réseaux impliqués dans l'utilisation de ses certificats, de l'utilisation de sa clé privée et de son certificat, qui doit être conforme à la présente Politique de Certification.

L'Autorité subordonnée doit communiquer à l'AC Racine, par les canaux qu'elle aura désignés, définis dans la DPC, toute information ayant pour conséquence la révocation de son certificat.

I.3.5. Les utilisateurs de certificat

Les utilisateurs de certificat, également nommés tiers utilisateurs, font confiance aux certificats délivrés par l'AC et/ou à des signatures numériques vérifiées à l'aide de ce certificat.

Les utilisateurs de certificats de l'AC subordonnée, sont définis dans la PC de l'AC subordonnée.

I.3.6. Autres participants

I.3.6.1. Opérateur de Certification

L'Opérateur de Certification (OC) est une composante du PSCE ayant en charge les services suivants tels que définis au §I.3.1 :

- service de génération de certificats,
- service de publication et diffusion,
- service de fourniture de code d'activation au porteur,
- service de gestion des révocations d'urgence,

- service d'information sur l'état des certificats,
- service d'assistance aux porteurs.

L'OC doit respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

I.4. Usage des certificats

I.4.1. Domaine d'utilisation applicables

Les différents usages possibles des clés publiques sont définis et contraints par l'utilisation d'une extension de certificat X.509 v3 (champ « keyUsage »).
Le champ « keyUsage » est marqué comme "critique".

I.4.1.1. Bi-clés et certificats de l'AC Racine et des AC subordonnées

Une clé publique de vérification doit être utilisée à des fins d'identification, d'authentification, d'intégrité et/ou de non - répudiation.
La clé publique de vérification de l'AC Racine est la seule clé utilisable pour vérifier la signature d'un certificat d'AC Subordonnée et des LCR.
Le champ « **keyUsage** » du certificat est utilisé conformément au profil des certificats et des LCR. Ce champ comporte les valeurs suivantes :
Pour les certificats de clés de signature AC Racine et AC subordonnée :

- **Signature de certificat**,
- **Signature de LCR**,

Aucun autre usage de la bi-clé n'est autorisé.

I.4.2. Domaine d'utilisation interdits

Les certificats d'AC subordonnées ne peuvent pas être utilisés en dehors de la signature des certificats et des CRL des AC subordonnées de l'AC CERTEUROPE ROOT CA 3.

I.5. Gestion de la PC

I.5.1. Entité gérant la PC

I.5.1.1. Organisme responsable

La société **CERTEUROPE** est responsable de cette PC.

CERTEUROPE
26 rue du Faubourg Poissonnière – 75010 Paris
FRANCE

I.5.1.2. Personne physique responsable

Monsieur Stanislas de Rémur
Président
26 rue du Faubourg Poissonnière – 75010 Paris
FRANCE

I.5.2. Point de contact

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

- Par courrier à l'adresse :

  CERTEUROPE – Autorité de Certification CERTEUROPE ROOT CA 3 26 rue du Faubourg Poissonnière – 75010 Paris
  FRANCE

  Par e-mail à l'adresse :
  info@certeurope.fr
- Par téléphone au numéro : 01.45.26.72.00

I.5.3. Entité déterminant la conformité de la DPC à la PC

La conformité de la DPC avec la PC est déterminée par la Direction de CertEurope.

I.5.4. Procédures d'approbation de la conformité de la DPC

La conformité de la DPC avec la PC est approuvée par le Comité PKI de CertEurope en suivant le processus d'approbation mis en place. Toute nouvelle version de la DPC est publiée sans délai.

I.6. Définitions et acronymes

AC	Autorité de Certification
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AP	Autorité de Politique
C	Country (Pays)
CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	Common Name
DDS	Dossier de Souscription
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification, ou EPC
DSA	Digital Signature Algorithm
EAR	Entité d'Audit et de Référencement
EPC	Enoncé des Pratiques de Certification, ou DPC
ETSI	European Telecommunications Standards Institute
ICP	Infrastructure à Clés Publiques
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
LDAP	Light Directory Access Protocol
MC	Mandataire de Certification

MD5	Message Digest n°5
MINEFI	Ministère de l'Économie, des Finances et de l'Industrie
O	Organisation
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisation Unit
PC	Politique de Certification
PDS	Déclaration de divulgation d'IGC (PKI Disclosure Statement)
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RGS	Référentiel Global de Sécurité
RSA	Rivest Shamir Adelman
SGMAP	Secrétariat général pour la modernisation de l'action publique
S/MIME	Secure/Multipurpose Internet Mail Extensions
SN	Serial Number
SSCD	Dispositif Sécurisé de Création de Signature
SHA-1	Secure Hash Algorithm One
SHA-256	Secure Hash Algorithm Two
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

II. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIEES

II.1. Entités chargées de la mise a disposition des informations

L'OC est en charge des services de publication :

- service de publication et diffusion,
- service d'information sur l'état des certificats.

L'OC utilise plusieurs canaux pour diffuser les informations en fonctions des exigences de disponibilité.

Les canaux utilisés sont :

copie 1 (original) : ldap://lcr1.certeurope.fr/CN= Certeurope Root CA 3, OU=0002 434202180, O=Certeurope, C=FR?certificateRevocationList ;

copie 2 : ldap://lcr2. certeurope.fr/CN= Certeurope Root CA 3, OU=0002 434202180, O= Certeurope, C=FR?certificateRevocationList ;

copie 3 : http://www.certeurope.fr/reference/root3.crl ;

II.2. Informations devant être publiées

L'OC pour le compte de l'AC CERTEUROPE ROOT CA 3 diffuse publiquement :

- la Politique de Certification CERTEUROPE en cours de validité (PC), celle-ci est accessible à l'URL suivante : http://www.certeurope.fr /reference/pc-root3.pdf
- la Liste de Certificats Révoqués (LCR).
- le certificat de l'AC CERTEUROPE ROOT CA 3 en cours de validité. Ce certificat est disponible sur le site Web de CertEurope à l'URL http://www.certeurope.fr/?subject=180&language=1. L'empreinte numérique du certificat est également disponible pour une garantie d'intégrité.

II.3. Délais et fréquences de publication

Les délais et les fréquences de publication dépendent des informations concernées :

- La PC est publiée dès sa validation. Elle est revue à chaque fois que nécessaire.
- Le certificat d'AC CERTEUROPE ROOT CA 3 est diffusé préalablement à toute diffusion de certificats d'AC subordonnées et/ou de LCR sous délai de 24h.
- Pour les informations d'état des certificats, cf. §IV.9 et §0.

Les exigences de disponibilité des systèmes publiant ces informations dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), les systèmes doivent avoir une disponibilité de Jours ouvrés avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 8h (jours ouvrés) et une durée totale maximale d'indisponibilité par mois de 32h (jour ouvrés), ceci hors cas de force majeure.
- Pour les certificats d'AC, les systèmes doivent avoir une disponibilité de 24h/24 7j/7 avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h et une durée totale maximale d'indisponibilité par mois de 8h, ceci hors cas de force majeure.
- Pour les informations d'état des certificats.

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.

II.4. Contrôle d'accès aux informations publiées

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

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (certificat et mot de passe).

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort **(**par certificat et mot de passe).

III. Identification et authentification

III.1. Nommage

III.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat X509v3, l'AC CERTEUROPE ROOT CA 3 (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" DN de type X.501 conforme aux exigences définies dans le document [PROFILS].

III.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats sont explicites.

Tous les caractères sont au format *printableString ou en UTF8String* i.e. sans accents ni caractères spécifiques à la langue française et de manière conforme au standard X.501 ;

Les informations portées dans le champ "Subject" du Certificat sont décrites ci-dessous de manière explicite selon les différents champs X509v3 :

- dans le champ « **CountryName** » : les caractères FR ;
- dans le champ « **OrganizationalName** » :
  Le nom officiel complet de l'entité responsable de l'AC subordonnée ;
- dans le champ « **OrganizationUnitName** » :
  Ce champ contient le numéro de SIREN de l'entité responsable de l'AC subordonnée ; ce numéro sera précédé de la chaîne de caractères « 0002 » et d'un espace.
  Si d'autres instances de l'attribut organizationalUnitName sont présentes, elles ne doivent pas commencer par 4 chiffres.
- dans le champ « **CommonName** » :
  Ce champ contient le nom de l'AC subordonnée.

III.1.3. pseudonymisation des porteurs

Sans objet.

III.1.4. Règles d'interprétation des différentes formes de nom

Sans objet.

III.1.5. Unicité des noms

L'unicité d'un certificat d'AC subordonnée est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC Racine. Cependant, les noms distinctifs doivent être uniques au sein de l'AC CERTEUROPE ROOT CA 3. L'unicité des noms est obtenue suivant les règles décrites au §III.1.2 de ce chapitre.

L'AE garantit l'unicité des noms utilisés pour les certificats des AC subordonnées.

III.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 1er 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'AE limite ses vérifications concernant le droit d'utiliser un nom à la vérification des informations contenues dans les pièces d'identité, les mandats éventuels, le K-BIS ou l'avis SIRENE.

CertEurope dégage toute responsabilité en cas d'utilisation illicite par les clients et Abonnés des marques déposées, des marques notoires et des signes distinctifs, ainsi que les noms de domaine.

III.2. Validation initiale de l'identité

III.2.1. Méthode pour prouver la possession de la clé privée

La génération des bi clés des AC subordonnées est effectuée sous le contrôle de l'OC.

III.2.2. Validation de l'identité d'un organisme

Cf. §III.2.3.

III.2.3. Validation de l'identité d'un porteur AC subordonnée

L'AE vérifie l'identification de l'organisation, de son représentant légal et de toutes personnes désignées par ce dernier, directement ou indirectement, pour le représenter vis-à-vis de l'AC CERTEUROPE ROOT CA 3 ou de l'AE.

La validation de l'identité de la personne à l'origine de la demande de certificat d'AC est effectuée par l'AE, lors d'un face à face avec le mandataire de certification.

L'AC ou l'AE doit archiver toutes les informations pertinentes relatives à l'enregistrement.

III.2.4. Informations non vérifiées du porteur

Sans objet.

III.2.5. Validation de l'autorité du demandeur

Pour toute demande de certificat d'AC subordonnée faite au titre de l'appartenance à une organisation, il faut que ladite demande soit confirmée par écrit par le représentant légal de cette même organisation.
Dans le cas d'un mandataire de certification, l'AE s'assure des pouvoirs de ce dernier.
Le contenu du demande de certificat d'AC subordonnée est décrit dans le chapitre §IV.1.2.

III.2.6. Certification croisée d'AC

Sans objet.

III.3. Indentification et validation d'une demande de renouvellement des clés

III.3.1. Identification et validation pour un renouvellement courant

Sans objet.

III.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, un certificat d'AC subordonnée ne peut faire l'objet d'un renouvellement.

III.4. Identification et validation d'une demande de révocation

Une demande de révocation ne peut être présentée que par une entité habilitée et est authentifiée par l'AE ou l'AC CERTEUROPE ROOT CA 3.

Dans le cas où un certificat AC subordonnée se doit d'être révoqué, le responsable de l'AC subordonnée doit informer au plus vite l'AC CERTEUROPE ROOT CA 3.

IV.Exigences opérationnelles sur le cycle de vie des certificats

IV.1. Demande de Certificat

Une demande de certificat d'AC subordonnée se matérialise par un contrat conclut entre l'organisation demandeuse et CERTEUROPE.

CERTEUROPE peut également être à l'origine d'une demande de certificat d'AC subordonnée. Dans ce cas, cette demande est formalisée par l'établissement d'un procès-verbal lors de la cérémonie des clés nécessaire à la création de l'AC subordonnée et de la bi-clé correspondante.

IV.1.1. Origine de la demande

Un certificat d'AC subordonnée est demandé par le représentant légal de l'organisation demandeuse ou par une personne mandatée de cette organisation.

IV.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

La demande de certificat comporte, si elle ne provient pas de CERTEUROPE :

- une demande écrite signée par le représentant légal ou le mandataire de certification,
- une déclaration du demandeur, portant l'acceptation de ses engagements,
- une adresse postale de l'organisation responsable de l'AC subordonnée,
- le nom du responsable du Certificat d'AC subordonnée,
- la clé publique de l'AC subordonnée à certifier,
- les données d'identification de l'organisation (DN X509),
- Le type de certificats émis par la nouvelle AC subordonnée (certificat personne physique, certificat serveur, certificat d'AC, …),
- Les usages des certificats délivrés par la nouvelle AC subordonnée (signature, authentification, chiffrement, …).

IV.2. Traitement d'une demande de certificat

IV.2.1. Exécution des processus d'identification et de validation de la demande

L'AE vérifie l'identité ainsi que les pouvoirs du mandataire de certification.

IV.2.2. Acceptation ou rejet de la demande

La demande est acceptée ou rejetée avant la cérémonie des clés. Le face-à-face du demandeur avec l'AE vaut acceptation du certificat et des obligations qui le lient à l'AC CERTEUROPE ROOT CA 3.

IV.2.3. Durée d'établissement du certificat

Le certificat d'une AC subordonnée est généré lors de la cérémonie des clés.

IV.3. Délivrance du certificat

IV.3.1. Actions de l'AC concernant la délivrance du certificat

La génération du bi clé et du certificat d'une AC subordonnée est consignée lors de la cérémonie des clés.

IV.3.2. Notification par l'AC de la délivrance du certificat au porteur

Un représentant (ex : mandataire de certification) de l'entité responsable de l'AC subordonnée est présent lors de la cérémonie des clés. Par conséquent, le demandeur est systématiquement notifié de la génération du certificat.

IV.4. Acceptation du Certificat

IV.4.1. Démarche d'acceptation du certificat

A l'issue de la cérémonie des clés, l'acceptation du certificat est considérée comme acquise.

IV.4.2. Publication du certificat

Les certificats des AC subordonnées sont publiés par l'AC CERTEUROPE ROOT CA 3 sur le site http://www.certeurope.fr/.

IV.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

IV.5. Usages de la bi-clé et du certificat

IV.5.1. Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée d'une AC subordonnée et du certificat associé est strictement limitée :

- à la signature des certificats EndUser ;
- à la signature de CRL ;

Les AC subordonnées respectent strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité sera engagée.
L'usage autorisé de la bi-clé de l'AC subordonnée et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

IV.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Cf. chapitre précédent et chapitre I.4. Les utilisateurs de certificats respectent strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité sera engagée.

IV.6. Renouvellement d'un Certificat

La durée de vie du certificat de l'Autorité de Certification CERTEUROPE ROOT CA 3 est de trente ans. Ll'Autorité de Certification CERTEUROPE ROOT CA 3 ne permet pas le renouvellement de ses certificats.

IV.6.1. Causes possibles de renouvellement d'un certificat

Sans objet.

IV.6.2. Origine d'une demande de renouvellement

Sans objet.

IV.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet.

IV.6.4. Notification au porteur de l'établissement du nouveau certificat

Sans objet.

IV.6.5. Démarche d'acceptation du nouveau certificat

Sans objet.

IV.6.6. Publication du nouveau certificat

Sans objet.

IV.6.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Sans objet.

IV.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

Nota - Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au porteur liée à la génération d'une nouvelle bi-clé.

IV.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés générées pour les AC subordonnées ont une durée de vie de 10 ans.
Par ailleurs, une bi-clé et un certificat peuvent être renouvelés :

- par anticipation, afin de garantir une continuité de service ;
- suite à la révocation du certificat de l'AC subordonnée (cf. chapitre IV.9, notamment le chapitre IV.9.1.1 pour les différentes causes possibles de révocation).

IV.7.2. Origine d'une demande d'un nouveau certificat

L'origine d'une demande d'un nouveau certificat est identique à celle d'une demande initiale.

IV.7.3. Procédure de traitement d'une demande d'un nouveau certificat

La procédure de traitement d'une demande d'un nouveau certificat est identique à celle d'une demande initiale (Cf. chapitre IV.3.1)

IV.7.4. Notification au porteur de l'établissement du nouveau certificat

Cf. chapitre IV.3.2.

IV.7.5. Démarche d'acceptation d'un nouveau certificat

Cf. chapitre IV.4.1.

IV.7.6. Publication du nouveau certificat

Cf. chapitre IV.4.2.

IV.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre IV.4.3.

IV.8. Modification du certificat

La modification de Certificat CERTEUROPE ROOT CA 3 n'est pas autorisée.

IV.8.1. Causes possibles de modification d'un certificat

Sans objet.

IV.8.2. Origine d'une demande de modification d'un certificat

Sans objet.

IV.8.3. Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

IV.8.4. Notification au porteur de l'établissement du certificat modifié

Sans objet.

IV.8.5. Démarche d'acceptation du certificat modifié

Sans objet.

IV.8.6. Publication du certificat modifié

Sans objet.

IV.8.7. Notification par l'AC aux autres entités de la délivrance du certificat modifié

Sans objet.

IV.9. Révocation et suspension et de Certificat

Un Certificat CERTEUROPE ne peut être que dans l'un des trois états suivants : valide, expiré ou révoqué.

IV.9.1. Causes possibles d'une révocation

IV.9.1.1. Certificats de porteurs

Les cas de figures suivants peuvent être à l'origine de la révocation d'un Certificat d'AC subordonnée, et notamment :

- la clé privée de l'AC subordonnée est suspectée de compromission, est compromise ou perdue ;
- la clé privée de l'AC CERTEUROPE ROOT CA 3 est suspectée de compromission, est compromise ou perdue ;
- modification d'une information contenue dans le certificat,
- décision de changement de composante de l'AC Racine ou de l'AE suite à non-conformité des procédures de la DPC ;
- cessation de l'activité de l'AC subordonnée ;
- l'AC CERTEUROPE ROOT CA 3 doit être révoquée ;

Outre les cas de révocation de certificats mentionnés plus haut, l'AC CERTEUROPE ROOT CA 3 révoque un certificat d'AC subordonnée dès lors qu'elle est en possession d'informations de nature à indiquer une perte de confiance dans un certificat d'AC subordonnée.

Plus généralement, l'AC CERTEUROPE ROOT CA 3 peut révoquer le certificat AC subordonnée d'une entité identifiée lorsqu'elle ne respecte pas les obligations énoncées dans la présente PC et dans tous documents contractuels ainsi que dans toute loi et règlement applicable.

IV.9.1.2. Certificats d'une composante de l'IGC

Sans objet.

IV.9.2. Origine d'une demande de révocation d'un Certificat Porteur

IV.9.2.1. Certificats de porteurs

La demande de révocation d'un Certificat d'AC subordonnée peut émaner :

- d'un mandataire de certification ;
- d'un représentant légal de l'entité responsable de l'AC subordonnée ;
- de l'AC CERTEUROPE ROOT CA 3 ;

IV.9.2.2. Certificats d'une composante de l'IGC

Sans objet.

IV.9.3. Procédure de traitement d'une demande de révocation

IV.9.3.1. Révocation d'un certificat de porteur

Les exigences d'identification et de validation d'une demande de révocation sont décrites au chapitre III.4. La demande de révocation est effectuée par l'AE.

Le responsable de l'AC subordonnée est notifié de la publication de la révocation. Les causes de révocation ne sont pas publiées.

IV.9.3.2. Révocation d'un certificat d'une composante de l'IGC

Sans objet.

IV.9.4. Délai accordé au porteur pour formuler la demande de révocation

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

IV.9.5. Délai de traitement par l'AC d'une demande de révocation

IV.9.5.1. Révocation d'un certificat de porteur

L'AC CERTEUROPE ROOT CA 3 met tout en œuvre pour que le délai maximum de traitement soit le plus court possible, dès lors que la demande de révocation a été authentifiée et validée.

IV.9.5.2. Révocation d'un certificat d'une composante de l'IGC

Sans objet.

IV.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat délivré par l'AC CERTEUROPE ROOT CA 3 est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

IV.9.7. Fréquence d'établissement des LAR

La fréquence de publication des LCR est de 24h.

IV.9.8. Délai maximum de publication d'une LAR

La LAR est publiée dans un délai maximum conforme à 30 min suivant sa génération.

IV.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Il n'y a pas de serveur OCSP.

IV.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre IV.9.6 ci-dessus.

IV.9.11. Autres moyens disponibles d'information sur les révocations.

Sans objet.

IV.9.12. Exigences spécifiques en cas de révocation pour compromission de clé

Sans objet.

IV.9.13. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée.

IV.9.14. Origine d'une demande de suspension

Sans objet.

IV.9.15. Procédure de traitement d'une demande de suspension

Sans objet.

IV.9.16. Limites de la période de suspension d'un certificat

Sans objet.

IV.10. Fonction d'information sur l'état des certificats

IV.10.1. Caractéristiques opérationnelles

L'accès à la Liste des certificats d'AC subordonnées révoqués (en l'occurrence la LCR de la l'AC CERTEUROPE ROOT CA 3) est possible via deux annuaires LDAP V3 et d'un serveur Web. Les LCR sont au format dénommé "LCR V2".

IV.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h et une durée maximale totale d'indisponibilité par mois de 8h.

IV.10.3. Dispositifs optionnels

Sans objet.

IV.11. Fin de la relation avec le porteur

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC CERTEUROPE ROOT CA 3 et l'AC subordonnée avant la fin de validité du certificat, ce dernier est révoqué.

IV.12. Séquestre de clé et recouvrement

IV.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

V. Mesures de sécurité non techniques

Les différents contrôles décrits ici visent, par une gestion des risques adéquate, à assurer un niveau de confiance fort dans le fonctionnement de l'AC CERTEUROPE ROOT CA 3.

V.1. Mesures de sécurité physique

V.1.1. Situation géographique et construction des sites

La situation géographique des sites de productions est conforme aux exigences du document [CERT_PS].

V.1.2. Accès physique

Les zones hébergeant les systèmes informatiques de l'AC CERTEUROPE ROOT CA 3 sont physiquement protégées contre un accès extérieur non autorisé.
La liste des personnels autorisés à y accéder existe et est limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés est contrôlé par un moyen physique et enregistré.

V.1.3. Alimentation électrique et climatisation

Les installations électriques et de conditionnement d'air sont suffisantes pour le bon fonctionnement des systèmes informatiques de l'AC CERTEUROPE ROOT CA 3.

V.1.4. Vulnérabilité aux dégâts des eaux

Les systèmes informatiques de l'AC CERTEUROPE ROOT CA 3 ne sont pas situés en zone inondable, ni du fait d'intempéries, ni du fait de tuyauteries défaillantes.

V.1.5. Prévention et protection incendie

Les locaux d'hébergement des systèmes informatiques de l'AC CERTEUROPE ROOT CA 3 sont protégés contre les incendies (détection et extinction automatiques). La distribution des machines permet par ailleurs d'assurer une disponibilité maximale des services.

V.1.6. Conservation des supports

Les supports contenant des données sauvegardées ou archivées doivent être conservés avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.
Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

V.1.7. Mise hors service des supports

La destruction ou la réinitialisation des supports seront assurées avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.
Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

V.1.8. Sauvegarde hors site

L'organisation des sauvegardes des informations sera adaptée de façon à assurer une reprise après désastre la plus rapide possible, en particulier pour les services impliqués dans la révocation de certificats.

Les informations sauvegardées hors site doivent respecter les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

V.2. Mesures de sécurité procédurales

Des contrôles des procédures sont mis en place par l'AC CERTEUROPE ROOT CA 3 et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

V.2.1. Rôles de confiance

Chaque composante de l'IGC doit distinguer au moins les rôles fonctionnels de confiance suivants :

Responsable sécurité : Le responsable de sécurité est chargé de la mise en oeuvre 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. ;

Responsable d'exploitation / d'application : Le responsable d'exploitation est chargé, au sein de la composante à laquelle il est rattaché, de la mise en oeuvre 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;

Opérateur : 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 oeuvre par la composante. ;

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 ;

Controleur : 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 oeuvre 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.

Porteur de part de secret : Personne ayant la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts de secrets qui leur sont confiés.

Les attributions nominatives de chaque rôle sont décrites dans la DPC.

V.2.2. Nombre de personnes requises par tâches

Selon la tâche à effectuer, une ou plusieurs personnes devront être présentes lors de l'exécution de la tâche.
La DPC précisera, conformément à l'analyse de risques, pour chacune des tâches liées à la gestion des certificats le nombre et le rôle de personnes nécessaires.

V.2.3. Identification et authentification pour chaque rôle

Chaque composante de l'AC CERTEUROPE ROOT CA 3 doit vérifier l'identité et les autorisations de son personnel devant intervenir, avant :

- que son nom soit ajouté aux listes des personnes ayant accès physiquement aux systèmes informatiques de l'AC. ;
- qu'un compte lui soit ouvert dans les systèmes informatiques de l'AC CERTEUROPE ROOT CA 3 ;

V.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 oeuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur
- auditeur/contrôleur et tout autre rôle
- ingénieur système et opérateur

Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC et sont conformes à la politique de sécurité de la composante concernée.

V.3. Mesures de sécurité vis-à-vis du personnel

V.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis de leur employeur.

Chaque entité opérant une composante de l'IGC s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

L'AC s'assure que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une AC:

- sont nommés à leur poste par écrit ;
- sont tenus par contrat ou par la loi de respecter les obligations, notamment de confidentialité, du poste qu'ils occupent ;
- n'ont pas de tâches ou d'intérêts susceptibles d'entrer en conflit avec les obligations qui leur incombent à l'égard de l'AC.

V.3.2. Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC met en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante.

Ces personnels n'ont pas de condamnation de justice en contradiction avec leurs attributions. Ils devront remettre à leur employeur une copie du bulletin n°3 de leur casier judiciaire avant l'attribution du rôle de confiance puis à tout moment sur simple demande.
Les personnes ayant un rôle de confiance ne souffrent d'aucun conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans), sauf pour le bulletin de casier judiciaire.

V.3.3. Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures de fonctionnement et de sécurité de la composante au sein de laquelle il opère.
L'AC s'assure que tous les membres du personnel qui accomplissent des tâches touchant la gestion de l'AC ont reçu une formation adaptée concernant les principes de fonctionnement et des mécanismes de sécurité de l'AC, et sont familiarisés aux règles de sécurité en vigueur.

V.3.4. Exigences et fréquence en matière de formation continue

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

V.3.5. Fréquence et séquence de rotation entre différentes attributions

L'AC n'impose pas la rotation de son personnel habilité.

V.3.6. Sanctions en cas d'actions non-autorisées

Sur faute avérée ou soupçonnée d'un membre de l'AC dans l'accomplissement de ses tâches, l'AC lui interdit l'accès aux systèmes et, le cas échéant, prend toutes sanctions disciplinaires adéquates.

V.3.7. Exigences vis-à-vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées.

V.3.8. Documentation fournie au personnel.

L'AC s'assure que son personnel dispose de l'accès à toute loi, ou tout contrat qui s'applique aux postes occupés.
Les documents dont dispose le personnel sont notamment les suivants :

- la PC supportée par la composante à laquelle il appartient ;
- la DPC propre au domaine de certification ;
- les procédures internes de fonctionnement ;
- les documents constructeurs des matériels et logiciels utilisés.

V.4. Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.
Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

V.4.1. Type d'évènements à enregistrer

Chaque entité opérant une composante de l'IGC journalise au minimum les évènements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'IGC :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements 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.

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC sont journalisés, notamment :

V.4.1.1. Evénements enregistrés par l'AE

Les évènements enregistrés par l'AE sont :

- réception d'une demande de certificat ;
- validation / rejet d'une demande de certificat ;
- réception d'une demande de révocation ;
- validation / rejet d'une demande de révocation ;
- sollicitation et accusés de réception de l'AC.

V.4.1.2. Evénements enregistrés par l'AC

Les évènements enregistrés par l'AC sont :

- événements liés aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, etc.) ;
- génération puis publication des LCR.

V.4.1.3. Description d'un événement

Chaque enregistrement d'un évènement dans un journal contient au minimum les champs suivants :

- type de l'événement ;
- nom de l'exécutant ou référence du système déclenchant l'événement ;
- date et heure de l'événement ;
- résultat de l'événement (échec ou réussite).

V.4.1.4. Imputabilité

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'événements.
De plus, en fonction du type de l'évènement, chaque enregistrement contient également les champs suivants : destinataire de l'opération ;

- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'événement ;
- toute information caractérisant l'événement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation sont effectuées au cours du processus.
En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'événement.

V.4.1.5. Evénements divers

D'autres évènements sont aussi recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

V.4.2. Fréquence de traitement des journaux d'événements

Cf. chapitre V.4.8.

V.4.3. Période de conservation des journaux d'événements

Les journaux d'événements sont conservés sur site pendant au moins 1 mois.
Ils sont archivés au plus tard 1 mois après.

V.4.4. Protection des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non). Les journaux d'événements sont accessibles uniquement au personnel autorisé de l'AC.

Le système de datation des évènements respecte les exigences du chapitre 0.

V.4.5. Procédure de sauvegarde des journaux d'évènements

Les procédures de sauvegarde des journaux sont quotidiennes par delta avec la sauvegarde précédente, et globale de manière hebdomadaire. Ces journaux sont ensuite archivés par l'AC.
Chaque entité opérant une composante de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la Politique de Sécurité de CertEurope [CERT_PS] et en fonction des résultats de l'analyse de risque de l'AC.

V.4.6. Système de collecte des journaux d'évènements

Un système automatique de collecte des journaux d'événements est mis en place. Ce système permet de garantir l'intégrité, la confidentialité et la disponibilité de ces journaux d'évènements.

V.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

V.4.8. Evaluation des vulnérabilités

Les journaux d'évènements sont contrôlés quotidiennement afin de pouvoir d'anticiper toute vulnérabilité.

Les journaux d'évènements sont contrôlés suivant la fréquence 1 fois par 24h, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins à une fréquence 1 fois par semaine et dès la détection d'une anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fera apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué à une fréquence au moins égale à 1 fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

V.5. Archivage des données

V.5.1. Types de données à archiver

L'AC procède en propre à l'archivage des données ci-dessous, et se réserve le droit de déléguer tout ou partie de ces obligations à un tiers avec lequel elle contractera sur la base de ces obligations.

Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC. Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC et DPC ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis ou publiés ;

- les récépissés ou notifications (à titre informatif) ;
- les engagements signés des MC ;
- les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC.

V.5.2. Période de conservation des archives

Dossiers de demande de certificat

Les dossiers d'enregistrement (demandes de certificats d'AC subordonnée) sont archivés pendant 10 ans.

Certificats et LCR émis par l'AC

Les Certificats d'AC subordonnées, ainsi que les LCR produites par l'AC CERTEUROPE ROOT CA 3 sont archivés pendant une durée de dix ans à compter de la date de génération du certificat.

Journaux d'évènements

Les journaux d'évènements sont archivés pendant dix ans après leur génération.
Les moyens mis en œuvre par l'AC pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements est assurée tout au long de leur cycle de vie.

V.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 ;
- lisibles et exploitables sur l'ensemble de leur cycle de vie ;

V.5.4. Procédure de sauvegarde des archives

Sans objet.

V.5.5. Exigences d'horodatage des données

Cf. chapitre V.4.4 pour la datation des journaux d'évènements.
Le chapitre 0 précise les exigences en matière de datation / horodatage.

V.5.6. Système de collecte des archives

Sans objet.

V.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) sont récupérées dans un délai inférieur à
2 jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

V.6. Changement de clé d'AC

La période de validité de la clé de l'AC CERTEUROPE ROOT CA 3 est de 30 ans.

La durée de vie des certificats d'AC subordonnée étant de 10 ans, le renouvellement de cette clé devra intervenir au plus tard avant la fin de sa validité. L'AC se réserve la possibilité de la renouveler avant sa limite de validité. La décision de son renouvellement pourra être prise plus tôt en fonction de divers critères (évolution de la technique cryptographique, allongement de la longueur, …).

Le nouveau bi-clé généré servira à signer les nouveaux certificats d'AC subordonnée émis ainsi que la LCR.

Le certificat précédent restera utilisable pour la validation de certificats d'AC subordonnée émis avant le renouvellement et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

V.7. Reprise suite à compromission et sinistre

V.7.1. Procédures de remontée et de traitement des incidents et des compromissions

Des procédures (sensibilisation, formation des personnels) et des moyens de remontée et de traitement des incidents (analyse des différents journaux d'événements) sont mises en œuvre.
Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …). L'AC prévient directement et sans délai le contact identifié sur le site : www.ssi.gouv.fr.

V.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Conformément à l'analyse de risque réalisée par l'AC, l'OC qui est en charge de l'ensemble des ressources informatiques, dispose d'un plan de continuité dans lequel sont décrites les procédures de reprise.

V.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante

Les cas de compromission des éléments secrets des autres composantes sont traités dans le plan de continuité d'activité.

V.7.4. Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de cette PC.

V.8. Fin de vie de l'IGC

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

Le transfert d'activité ne comporte 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

Les composantes de l'AC pour lesquelles une cessation d'activité est envisageable sans remettre en cause l'IGC sont : les AE et l'OC.

Composante OC
Le contrat liant l'OC et l'AC dispose d'une clause de réversibilité permettant à l'AC de changer d'opérateur. En effet, en cas de cessation d'activité de l'OC, l'AC s'engage à transférer les fonctions assurées par l'OC sur un autre OC.

En particulier, L'AC s'assurera de :

- Réaliser un plan d'actions et le confronter à l'analyse de risques de l'AC : en particulier, le plan d'action devra traiter du :
  - transfert des archives sous la responsabilité de l'OC,
  - transfert des fonctions assurées par l'OC,
  - la continuité de services lors du transfert,
  - Transfert des clés de l'AC hébergées par l'OC,
  - suppression des habilitations de l'OC sur la révocation d'urgence,
  - modification du référentiel documentaire de l'AC : PC, DPC,
  - la formation du personnel habilité de l'AC,
  - la communication vers les autres composantes de l'IGC,
  - la communication vers les AC subordonnées et utilisateurs de certificats,

- Communiquer le plan d'actions au contact identifié sur le site www.ssi.gouv.fr, et de tout changement pendant le déroulement du transfert.

Cessation d'activité affectant l'AC

Dans le cas 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, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans cette PC.

Lors de l'arrêt du service, l'AC s'engage à :

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 MC des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3).

Dans le cas où la cessation d'activité est programmée, l'AC respectera un délai de 6 mois entre l'alerte administrative et la révocation de son certificat d'AC et s'engage à convenir d'accords particuliers avec d'autres autorités assurant un bon niveau d'assurance conformément aux exigences de réversibilité des archives.

VI.Mesures de sécurité techniques

VI.1. Génération et installation de bi-clés

VI.1.1. Génération des bi-clés

VI.1.1.1. Clés d'AC

La génération des clés de signature d'AC CERTEUROPE ROOT CA 3 est effectuée dans un environnement sécurisé (cf. chapitre V).

Les clés de signature d'AC CERTEUROPE ROOT CA 3 sont générées lors de la cérémonie des clés et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.
La cérémonie des clés de l'AC a lieu sous le contrôle d'un officier public ministériel, veillant à la bonne application des procédures et au respect des exigences de sécurité définies dans ce document et dans la DPC. Elle est effectuée par au moins deux personnes ayant des rôles de confiance (cf. chapitre V.2.1), dans le cadre de la "cérémonies de clés". Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

Les clés de l'AC CERTEUROPE ROOT CA 3 sont générées dans un module cryptographique dont les parts de secrets sont déjà existantes et distribuées à des porteurs identifiés et habilités à ce rôle de confiance.

VI.1.1.2. Clés porteurs générées par l'AC

Le bi-clé est généré directement dans un module cryptographique équivalent à celui de l'AC CERTEUROPE ROOT CA 3.

VI.1.1.3. Clés porteurs générées par le porteur

Sans objet.

VI.1.2. Transmission de la clé privée a son propriétaire

Sans objet.

VI.1.3. Transmission de la clé publique à l'AC

Sans objet.

VI.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

La clé publique de l'AC est téléchargeable sur le site Internet de l'AC.
L'empreinte du Certificat de la clé publique de l'AC permet d'en établir l'authenticité.

VI.1.5. Tailles des clés

Les clés RSA des AC subordonnées utilisées ont une taille de 2048 bits et seront mises à niveau au fur et à mesure de l'évolution de la technique et/ou de la législation.
La taille de la clé RSA de l'AC CERTEUROPE ROOT CA 3 est de 2048 bits.

VI.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

Le bi-clé d'une AC subordonnée (pour la signature de certificats et de CRLs) est généré et protégé par un module cryptographique matériel. Ce module répond aux exigences du chapitre XI.
La génération ou le renouvellement du bi-clé de l'AC par ce module nécessite la présence d'au moins 3 personnes.

VI.1.7. Objectifs d'usage de la clé

L'utilisation de la clé privée de l'AC CERTEUROPE ROOT CA 3 et du certificat associé est strictement limitée à la signature de certificats d'AC subordonnée et de LCR / LAR.
L'utilisation de la clé privée d'une AC subordonnée et du certificat associé est strictement limitée à la signature de certificats et de LCR.

VI.2. Mesure de securité pour la protection des clés privées et pour le modules cryptographiques

VI.2.1. Standards et mesures de sécurité pour les modules cryptographiques

VI.2.1.1. Modules cryptographiques de l'AC

Le module cryptographique, utilisés par l'AC, pour la génération et la mise en oeuvre des ses clés de signature est un module cryptographique répondant aux critères communs au niveau EAL4+ et par conséquent aux exigences du chapitre XI ci-dessous pour le niveau de sécurité **.

VI.2.1.2. Modules cryptographiques de l'AC subordonnée

Le module cryptographique, utilisés par une AC subordonnée, pour la génération et la mise en oeuvre des ses clés de signature est un module cryptographique répondant aux critères communs au niveau EAL4+ et par conséquent aux exigences du chapitre XI ci-dessous pour le niveau de sécurité **.

VI.2.2. Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où 3 exploitants parmi 5 doivent s'authentifier).

VI.2.3. Séquestre de la clé privée.

L'AC CERTEUROPE ROOT CA 3 n'autorise pas le séquestre ni des clés privées de l'AC ni des clés privées des AC subordonnées.

VI.2.4. Copie de secours de la clé privée

La clé privée de l'AC fait l'objet de copie de secours sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Ces copies de secours bénéficient du même niveau de sécurité que la clé privée originale.
La clé privée d'une AC subordonnée fait l'objet de copie de secours sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Ces copies de secours bénéficient du même niveau de sécurité que la clé privée originale.
Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique et nécessitent l'intervention de 3 porteurs de secrets.

VI.2.5. Archivage de la clé privée

Les clés privées de l'AC ne sont pas archivée.

Les clés privées des AC subordonnées ne sont par archivées ni par l'AC CERTEUROPE ROOT CA 3 ni par aucune des composantes de l'IGC.

VI.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Pour les clés privées de l'AC CERTEUROPE ROOT CA 3 et des AC subordonnées, tout transfert se fera sous forme chiffrée, conformément aux exigences du chapitre VI.2.4.

VI.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC CERTEUROPE ROOT CA 3 sont stockées dans un module cryptographique répondant aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.
Les clés privées des AC subordonnées sont stockées dans un module cryptographique répondant aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

VI.2.8. Méthode d'activation de la clé privée

VI.2.8.1. Clés privées d'AC

L'activation de la clé privée de l'AC nécessite la présence de trois porteurs de secrets et permet de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

VI.2.8.2. Clés privées des porteurs

L'activation de la clé privée d'une AC subordonnée nécessite la présence de trois porteurs de secrets et permet de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

VI.2.9. Méthode de désactivation de la clé privée

VI.2.9.1. Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

VI.2.9.2. Clés privées des porteurs

La désactivation des clés privées d'une AC subordonnée dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

Une clé privée d'une AC subordonnée peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

VI.2.10. Méthode de destruction des clés privées

VI.2.10.1. Clés privées d'AC

La destruction des clés privées d'AC ne peut être effectuée qu'à partir du module cryptographique.
En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

VI.2.10.2. Clés privées des porteurs

La destruction des clés privées d'une AC subordonnée ne peut être effectuée qu'à partir du module cryptographique.
En fin de vie d'une clé privée d'une AC subordonnée, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

VI.2.11. Niveau d'évaluation sécurité du module cryptographique

Le modules cryptographique de l'AC CERTEUROPE ROOT CA 3 est évalué au niveau EAL4+ correspondant à l'usage visé, tel que précisé au chapitre XI ci-dessous.
Le modules cryptographique des AC subordonnées sont évalués au niveau EAL4+ correspondant à l'usage visé, tel que précisé au chapitre XI ci-dessous.

VI.3. Autres aspects de la gestion des bi-clés

VI.3.1. Archivage des clés publiques

Les clés publiques de l'AC CERTEUROPE ROOT CA 3 et des AC subordonnées sont archivées dans le cadre de l'archivage des certificats correspondants.

VI.3.2. Durée de vie des Bi-clés et des Certificats

La durée de vie de la bi-clé et du certificat de l'AC CERTEUROPE ROOT CA 3 est de 30 ans.
La durée de vie de la bi-clé et du certificat d'une AC subordonnée est de 10 ans.

VI.4. Données d'activation

VI.4.1. Génération et installation des données d'activation

VI.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 du module cryptographique de l'AC CERTEUROPE ROOT CA 3 ont été effectuées lors de la phase d'initialisation et de personnalisation de ce module.

VI.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du porteur

La génération et l'installation des données d'activation du module cryptographique d'une AC subordonnée ont été effectuées lors de la phase d'initialisation et de personnalisation de ce module.

VI.4.2. Protection des données d'activation

VI.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC

Suite à la cérémonie de l'AC, les données d'activation de l'AC sont remises entre plusieurs porteurs qui ont la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

VI.4.2.2. Protection des données d'activation correspondant aux clés privées des porteurs

Suite à la cérémonie de l'AC subordonnée, les données d'activation de l'AC subordonnée sont remises entre plusieurs porteurs qui ont la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

VI.4.3. Autres aspects liés aux données d'activation

Sans objet.

VI.5. Mesures de sécurité des systèmes informatiques

VI.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les postes de travail des composantes de l'ICP nécessitent un niveau de sécurité optimal et permet de satisfaire les besoins suivants :

- identification et authentification des utilisateurs du poste
- 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,
- protection du réseau (confidentialité, intégrité…)
- fonctions d'audits,
- imputabilité.

Le niveau minimal d'assurance recherché doit au moins répondre à ces objectifs de sécurité. Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires, à prendre en compte dans la recherche du niveau minimal d'assurance offert par les postes de travail.

VI.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Sans objet.

VI.6. Mesures de sécurité des systèmes durant leur cycle de vie

VI.6.1. Mesures de sécurités liées au développement des systèmes

Les applications de l'AC ont été implémentées dans le strict respect de l'analyse de risque préalable et de la politique de sécurité qui en découle.
L'implémentation de l'AC et de la plate-forme qui l'héberge est documentée.
Toute modification de l'AC et de la plate-forme qui l'héberge est documentée

VI.6.2. Mesures liées a la gestion de la sécurité.

Toute évolution des systèmes est enregistrée sur le livre d'activité de l'AC et fait l'objet d'un rapport.

VI.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

VI.7. Mesures de sécurité réseau

L'AC est implantée sur un réseau protégée par au moins deux niveaux de passerelles de type « coupe-feu ». Ces passerelles sont configurées de façon à n'accepter que les flux strictement nécessaires.

VI.8. Horodatage / système de datation

Pour dater les évènements, les différentes composantes de l'IGC recourt à l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les évènements avec une précision suffisante. La synchronisation par rapport au temps UTC se réfère à un système comprenant au deux sources indépendantes de temps.

VII. Profils de certificats et de LCR

VII.1. Profil des Certificats

Les Certificats de l'AC CERTEUROPE ROOT CA 3 contiennent les champs primaires et les extensions suivantes :

Champ	Valeur	Détail valeur	Explications
Version	V3	2	Version du Certificat X.509
Numéro de série	1506 38D4 36F3 K231 C692 B849 E3F7 B943		Le numéro de série unique du Certificat attribué par le module cryptographique
Algorithme de signature	Sha256RSA = 1.2.840.113549.1.1.11		Identifiant de l'algorithme de signature de l'AC
Emetteur	/C=FR /O=Certeurope /OU=0002 434202180 /CN=Certeurope Root CA 3		Le nom de l'AC émettrice est le Distinguished Name (X.500) de l'AC signant les Certificats
Valide à partir du	Date de début = x (au plus tôt à la date de début de vie de l'AC Racine)		Dates et heures d'activation et d'expiration du Certificat
Valide jusqu'au	Valide jusqu'au x+ 10 ans (au plus tard à la date de fin de vie de l'AC Racine)		
Objet	CN = AC Certeurope Subordonée OU = 0002 434202180 O = CertEurope C = FR		Nom distinctif de l'entité identifiée
Clé publique	RSA(2048 Bits)	7C28 8902 8181 3963 8424 B08C CD71 9110 7E44 2B2E 8014 35F0 49CE B4D2 8CA9 3516 5FC7 9EB8 9A89 637C 20C4 DB30 97AF ECB3 37F2 A000 00E8 E350 BA90 2B20 EEE5 9D5B 4A87 E0D5 895A B6A4 05A6 B2C4 2715 555F 3081 0A68 95AD 00CF 6071 4C00 8431 7693 7EC0 20F9 8C31 EC2A 8585 9054 3478 4DD1 366B 9024 67B7 E8C8 C812 6EE9 E35B 5D04 700D 6699 2702 0301 0001	Identifiant de l'algorithme d'usage de la clé publique contenue dans le Certificat, et valeur de la clé publique
Contrainte de base	Subject Type=Certificate Authority Path Length Constraint=1		
Point de distribution de la LCR	CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://lcr1.certeurope.fr/CN=Certeurope Root CA 3, OU=0002 434202180, O=Certeurope, C=FR?CertificateRevocationList URL=ldap://lcr2.certeurope.fr/CN=Certeurope Root CA 3, OU=0002 434202180, O=Certeurope, C=FR?CertificateRevocationList URL=http://www.certeurope.fr/reference/root3.crl		
Certificate Policies	Certificate Policy: PolicyIdentifier=1.2.250.1.105.8.1.1.0 Policy Qualifier Info: Policy Qualifier Id= Qualifier=	OBJECT IDENTIFIER ' OBJECT IDENTIFIER cps http://www.certeurope.fr/reference/pc-root3.pdf	Identifiant de la Politique de Certification
Algorithme d'empreinte numérique	Sha1 = 1.3.14.3.2.29		
Empreinte numérique	07F2 AC3F 4E3A 30D5 277C 2A1A 6AD2 6BA4 F019 E130	8C 62 E9 57 0B 94 DF EB 73 14 AE 15 0F A9 36 2B 22 84 81 28 0F 25 06 FF 1C D3 10 EC A5 BC 43 1C AB 02 1D CD 7E 9E D7 B9 A0 DA 13 59 22 26 DF 72 EB 6D B3 AA 4E 2C B0 B3 1B 38 A4 E5 C4 3A 4C 15 2F E2 B2 AD 1C 9D 8F 5A FE D6 05 BC 6D 2E 81 D4 67 96 3D 74 BB F1 3F 37 7C 27 75 8C 9A 9A 9D 56 63 F1 BD 1E 76 89 09 ED 71 AA E1 F0 65 E1 A5 C8 0E DC AE 50 E1 C6 0D BF 76 6F A8 EC D0 D7 55 B9	Champ d'octets caractérisant le Certificat de l'AC ayant signé le Certificat

VII.2. Profil de LAR

VII.2.1. Champs des LAR

Les LAR de l'AC CERTEUROPE ROOT CA 3 contiennent les champs suivants :

- Version : la version de la LAR. Dans le cadre de la présente AC, il s'agit de la version 2;
- Signature : l'identifiant de l'algorithme de signature de l'AC soit Sha1-RSA ;
- Issuer : le nom de l'AC émettrice qui signe les Certificats soit l'AC CERTEUROPE ROOT CA 3 ;
- ThisUpdate : date de génération de la LAR ;
- NextUpdate : prochaine date à laquelle cette LAR sera mise à jour ;
- RevokedCertificates : liste des numéros de série des Certificats révoqués ;
- UserCertificate : numéro de série de Certificat révoqué ;
- RevocationDate : date à laquelle un Certificat donné à été révoqué.
- crlExtensions : liste des extensions de la LAR.

VII.2.2. Extensions des LAR

Les LAR de l'AC CERTEUROPE ROOT CA 3 comportent deux extensions :

- authorityKeyIdentifier : cette extension non critique identifie la clé publique à utiliser pour vérifier lavalidité de la LAR. Cet identifiant a la même valeur que le champ SubjectKeyIdentifier des certificats émis par l'AC CERTEUROPE ROOT CA 3 ;
- CRLNumber : cette extension non critique contient le numéro de série de la LAR.

VIII. Audit de conformité et autres évaluations

Des audits annuels de surveillance sont organisés, conformément au schéma d'accréditation. Afin d'assurer la conformité de sa PC avec sa DPC, l'AC réalise des audits internes.

La suite du présent chapitre ne traite que le contrôle de conformité de l'IGC.

VIII.1. Fréquences et / ou circonstances des évaluations

L'AC CERTEUROPE ROOT CA 3 procède à un audit de conformité de la PC au moins tous les deux ans.

VIII.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante est assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

VIII.3. Relations entre évaluateurs et entités évaluées

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

VIII.4. Sujets couverts par les évaluations

Les contrôles périodiques effectués par l'équipe d'audit porteront sur l'ensemble de l'architecture de l'IGC 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.).

VIII.5. Actions prises suite aux conclusions des évaluations

A l'issue des opérations de contrôles, les mesures correctives seront prises selon les schémas décrits ci-après :
A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'organisme contrôlé, un rapport d'audit. Les éventuelles non conformités détectées lors de l'audit sont classifiées en « remarque », « non-conformité mineure », « non-conformité majeure ».

Les « remarques » et les « non conformités mineures » seront corrigés selon les recommandations et les délais proposés par l'équipe d'audit. L'AC précisera comment et sous quels délais les non conformités seront levées.

Les « non-conformités majeures » devront être levées dans les plus brefs délais sous peine de cessation de l'activité provisoire ou définitive suivant la recommandation de l'équipe d'audit.

VIII.6. Communication des résultats

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

IX. Autres problématiques métiers et légales

IX.1. Tarifs

CertEurope se réserve le droit de facturer le service de création de certificat d'AC subordonnée.

IX.1.1. Tarifs pour la fourniture et le renouvellement de certificats

Sans objet.

IX.1.2. Tarifs pour accéder aux certificats

Sans objet

IX.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats

Sans objet.

IX.1.4. Tarifs pour d'autres services

Sans objet.

IX.1.5. Politique de remboursement

Sans objet.

IX.2. Responsabilité financière

IX.2.1. Couverture par les assurances

L'AC CERTEUROPE ROOT CA 3 justifie d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'il pourrait devoir aux Utilisateurs d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle. CertEurope déclare disposer d'une assurance professionnelle couvrant ses prestations de certification électronique souscrite auprès de la compagnie HISCOX sous le numéro de police HA RCP0081352.

IX.2.2. Autres ressources

Sans objet.

IX.2.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

IX.3. Confidentialité des données professionnelles

IX.3.1. Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles :

- les clés privées associées aux Certificats ;

- les causes de révocations des Certificats ;
- les journaux d'événements des composantes de l'ICP CERTEUROPE ROOT CA 3 ;
- la demande de certificat d'AC subordonnée ;
- les rapports d'audit ;
- la DPC.

Ces données ne seront utilisées et ne feront l'objet de communication extérieure que pour les seules nécessités de la gestion des opérations effectuées en exécution de la DPC associée à la présente PC, pour répondre aux exigences légales ou pour l'exécution de travaux ou de prestations de services confiés à des prestataires.

Les personnes sur lesquelles portent ces informations nominatives auront le droit d'en obtenir communication, auprès de l'AE, et d'en exiger le cas échéant, la rectification comme précisé dans la loi 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les personnes dont les données à caractère personnel sont collectées et traitées ont également le droit de s'opposer explicitement à l'utilisation de leurs données à des fins autres que celles stipulées dans la présente PC, par lettre adressée à l'adresse ci-dessus.

Toutes les données à caractère personnel collectées et détenues par l'IGC ou une composante sont considérées comme confidentielles et ne doivent pas être divulguées sans avoir obtenu le consentement préalable de la personne concernée.
Conformément à l'article 33 de la Loi Informatique, fichiers et Libertés modifiée, sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par l'AC CERTEUROPE ROOT CA 3 pour les besoins de la délivrance et de la conservation des Certificats doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies.
Des procédures dérogatoires à cette politique de confidentialité peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures spécifiques dûment validées par CertEurope qui prévaudront.

IX.3.2. Informations hors du périmètre des informations confidentielles

Sans objet.

IX.3.3. Responsabilités en terme de protection des informations confidentielles

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

IX.4. Protection des données personnelles

IX.4.1. Politique de protection des données personnelles

L'AC respecte la législation et la réglementation en vigueur sur le territoire Français et en particulier la loi [CNIL].
Le correspondant informatique et liberté de l'AC a inscrit ce traitement dans la liste des traitements effectué par l'AC.

IX.4.2. Informations à caractère personnel

Pour l'AC CERTEUROPE ROOT CA 3, les informations à caractère personnel sont les informations nominatives du mandataire de certification enregistrées au sein du dossier d'enregistrement. Il s'agit des informations nom / prénom / adresse / téléphone / fonction / email.

IX.4.3. Informations à caractère non personnel

Sans objet.

IX.4.4. Responsabilité en termes de protection des données personnelles

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

IX.4.5. Notification et consentement d'utilisation des données personnelles

Sans objet.

IX.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

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

IX.4.7. Autres circonstances de divulgation d'informations personnelles

Sans objet.

IX.5. Droits sur la propriété intellectuelle et industrielle

Lors de l'exécution des prestations de services définies dans le présent document et/ou de tout autre document contractuel relatif au Service de Certification, il peut être livré des éléments protégés par la législation sur les droits d'auteur.

Ces éléments, ainsi que les droits d'auteur qui y sont attachés, resteront la propriété du détenteur des droits correspondants. Le bénéficiaire de ces services aura le droit de reproduire ces éléments pour son usage interne. Mais il ne pourra, sans l'autorisation préalable du détenteur des droits d'auteur, mettre à la disposition de tiers, extraire ou réutiliser en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci, en particulier logiciels ou bases de données.

Sous réserve des dispositions du présent article, aucune licence, implicite ou explicite, n'est concédée par le détenteur des droits sur des inventions, brevets ou demandes de brevets lui appartenant et ayant été réalisés hors du présent document et/ou de tout autre document contractuel relatif au Service de Certification.

IX.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 privées ;
- n'utiliser leurs clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification ;
- respecter et appliquer la PC et DPC associée au moins pour les parties leur incombant;
- se soumettre aux contrôles de conformité effectués par CertEurope ou par toute autre organisme mandaté par CertEurope, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- respecter les accords ou contrats qui les lient entre elles ainsi qu'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.

IX.6.1. Autorités de certification

L'AC CERTEUROPE ROOT CA 3 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.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Etre une entité légale au sens de la loi française.
- Etre en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des porteurs de cette entité. L'AC peut aussi, le cas échéant, être en relation contractuelle / hiérarchique / réglementaire avec le ou les mandataires de certification choisis par l'entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats,… qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC notamment en matière de génération des certificats, remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR). Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats.

L'AC CERTEUROPE ROOT CA 3 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 § IV.4 ;
- tenir à disposition des Porteurs et des Utilisateurs, la liste des certificats ayant fait l'objet d'une révocation; cette liste est publiée sous la forme d'une LCR ;
- garantir la cohérence entre la PC et la DPC associée ;

IX.6.2. Service d'enregistrement

Cf. chapitre § IX.6.1.

IX.6.3. Mandataire de certification

Le mandataire de certification a le devoir de :

- Communiquer des informations exactes et à jour lors de sa demande ou du renouvellement du certificat,
- Informer l'AC de toute modification des informations contenues dans son certificat
- Faire sans délai une demande de révocation auprès de l'AC CERTEUROPE ROOT CA 3 en cas de perte, de compromission ou de suspicion de compromission d'une clé privée,
- Interrompre immédiatement et définitivement l'usage des clés privées en cas de compromission,

IX.6.4. Porteurs de certificats

Sans objet.

IX.6.5. Utilisateurs de certificats

Les Applications utilisatrices et Utilisateurs de Certificats doivent :

- respecter l'usage pour lequel un Certificat a été émis ;
- vérifier la signature numérique de l'AC CERTEUROPE ROOT CA 3 émettrice du Certificat ainsi que celle de l'AC CERTEUROPE ROOT CA 3 ;
- contrôler la validité des Certificats (date de validité et statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

IX.6.6. Autres participants

Sans objet.

IX.7. Limite de garantie

Sans objet

IX.8. Limite de responsabilité

Sans objet

IX.9. Indemnités

Sans objet

IX.10. Durée et fin anticipée de validité de la PC

IX.10.1. Durée de validité

Le présent document est applicable jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

IX.10.2. Fin anticipée de validité

Sauf événement exceptionnel lié à la sécurité, les évolutions du présent document n'imposent pas la révocation des certificats déjà émis.

IX.10.3. Effets de la fin de validité et clauses restant applicables

Sans objet.

IX.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC fera 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.

IX.12. Amendements à la PC

IX.12.1. Procédures d'amendements

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

IX.12.2. Mécanisme et période d'information sur les amendements

Sans objet.

IX.12.3. Circonstances selon lesquelles l'OID doit être changé

Les modifications de la présente PC entrainent un changement de numéro de version qui permet d'évaluer les évolutions sur 3 niveaux (exemple : version 1.0 Mise à jour 01) :

- Version majeure (1.) : correspond à une modification importante comme un changement des clés d'AC ou une refonte importante ou totale de la PC
- Version mineure (.0) : correspond à des modifications qui impactent sensiblement les Porteurs ou utilisateurs existants.
- Numéro de mise à jour (01) : correspond à des modifications qui n'ont pas d'impact sensible vis-à-vis des Porteurs ou utilisateurs existants et ne nécessite pas le changement de l'OID de la PC.

IX.13. Dispositions concernant la résolution de conflits

Cf. les conditions générales d'abonnement. La présente PC est soumise au Droit français.

Tous différends, découlant du présent Contrat, peuvent être réglés par voie d'arbitrage si les parties au litige sont d'accord sur ce mode de règlement du conflit. Si tel est le cas, le règlement d'arbitrage est celui de l'ATA (Centre de conciliation et d'arbitrage des techniques avancées, 57, avenue de Villiers, 75017 Paris - Tél : 01 56 21 10 00 - Fax : 01 56 21 10 10 – http://www.legalis.net/ata), auquel les parties déclarent expressément se référer.

Si tel n'est pas le cas, les parties ont recours à la juridiction de droit commun, sachant que CertEurope attribue compétence au Tribunal de Grande Instance de Paris, à raison de son siège.

Au besoin y compris par dérogation au règlement d'arbitrage de l'ATA, la sentence arbitrale sera susceptible d'appel devant les juridictions de droit commun.

IX.14. Juridictions compétentes

La présente Politique de Certification est soumise au droit français.
Tout litige relatif à la validité, l'interprétation, l'exécution de la présente Politique de Certification sera soumis aux tribunaux compétents de la cour d'appel de Paris.

IX.15. Conformité aux législations et règlementations

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

IX.16. Dispositions diverses

IX.16.1. Accord global

Sans objet.

IX.16.2. Transfert d'activités

Cf. chapitre V.8

IX.16.3. Conséquence d'une clause non valide

Sans objet.

IX.16.4. Application et renonciation

Sans objet.

IX.16.5. Force majeure

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

IX.17. Autres dispositions

Sans Objet.

X. Annexe 1 – Documents cités en référence

X.1. Réglementation

Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Directive européenne 95/46/EC relative à la protection des données personnelles

Directive européenne (1999/93/EC) relative à la signature électronique été adoptée le 13/12//1999

Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

Décret no 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.

Décret no 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie dispensées de toute formalité préalable.

Arrêté du 17 mars 1999 définissant la tome et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptographie.

Arrêté définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fournitures d'un moyen ou d'une prestation de cryptographie, no PRMX9802730A du 13 mars 1998

Arrêté définissant le modèle de notification préalable par le fournisseur des identités des intermédiaires utilisés pour la fourniture des moyens ou prestations de cryptographie soumis à autorisation, no PRMX9802732A du 13 mars 1998.

X.2. Documents techniques

Référence	Version	Titre des documents
[PC RGS]		PC Type du référentiel RGS
[PROFILS]		RGS – Politiques de Certification Types – Profils de Certificats, de LCR et OCSP et algorithmes cryptographiques
[ETSI_CERT].		
[RFC3647]		
[RFC3739]		
[CERT_PS]		Certeurope – Politique de sécurité
[PC RGS V2.3]		PC Type du référentiel RGS

XI. Annexe 2 : Exigences de sécurité du module cryptographique de l'AC

XI.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en oeuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des porteurs, doit répondre aux exigences de sécurité suivantes :

- si les bi-clés d'authentification et de signature des porteurs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- si les bi-clés d'authentification et de signature des porteurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des porteurs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif d'authentification et de signature du porteur et assurer leur destruction sûre après ce transfert ;
- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des clés privée de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

Le module cryptographique de l'AC doit détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

XI.2. Exigences sur la certification

Le module cryptographique utilisé par l'AC doit, dans les conditions prévues par le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, être certifié conforme aux exigences du chapitre XI.1 ci-dessus par le Premier ministre.
La certification doit permettre de démontrer une assurance moyenne que le module cryptographique répond bien à ces exigences (équivalent à un niveau EAL2+ des critères communs avec une résistance élevée des mécanismes) et déboucher sur une qualification de niveau standard [QUALIF_STD].