CRITERE DE DIFFUSION : PUBLIC

POLITIQUE DE CERTIFICATION

Autorité de certification

« CERTEUROPE ADVANCED CA V3 »

Identification (OID)	1.2.250.1.105.9.1.1.2	Version	1.2
Date de création	01/07/2010	Date de mise à jour	30/12/2010

Ce document contient 75 pages

Etat du document	Officiel
Rédigé par	CertEurope
Vérifié par	Comité PKI
Approuvé par	Comité PKI

MODIFICATIONS

Date	Etat	Version	Commentaires
20/08/2010	Officiel	1.0	
12/10/2010	Officiel	1.1	Modification suite à l'audit interne de conformité et suite à l'audit LSTI
30/12/2010	Officiel	1.2	Modification de la méthode de résolution des problèmes d'homonymie. Corrections §VI.2.1.2 et §III.3.2. Correction §III.3.2.3.2 Correction §IV.3.2 et §IV.4.1 Ajout du face-à-face lors du dépôt du dossier. §III.2.3.1 §III.2.3.2 §III.2.3.3 §IV.3.2 §VI.1.2

DOCUMENTS REFERENCES

SOMMAIRE

I. INTRODUCTION

I.1. PRESENTATION GENERALE

Ce document constitue la Politique de Certification de l'Autorité de Certification CERTEUROPE et a été établi sur la base de la Politique de Certification type de l'Etat (RGS 2.3), en vue d'un référencement pour le profil « Authentification & Signature », au niveau **.

Le Référentiel Global de Sécurité (RGS) est un référentiel technique listant les règles que les prestataires de services de certification électronique (PSCE) délivrant des certificats électroniques doivent respecter.

Une Politique de Certification (PC) est identifiée par un nom unique (OID*). Elle est composée d'un ensemble de règles décrivant les conditions de recevabilité d'un Certificat pour des applications ayant des besoins de sécurité communs.

Une PC est définie indépendamment des modalités de mise en œuvre de l'Infrastructure à Clés Publiques (ICP) à laquelle elle s'applique. Elle décrit les exigences auxquelles l'ICP doit se conformer pour l'enregistrement et la validation des demandes de Certificats, et pour la gestion des Certificats. Les procédures de certification sont rassemblées dans un document appelé Déclaration des Pratiques de Certification (DPC), distinct de la PC, qui décrit comment ces exigences sont atteintes en pratique.

Cette PC est donc associée à la DPC relative à l'AC CERTEUROPE. Contrairement à la PC, la consultation de la DPC doit faire l'objet d'une demande argumentée auprès du Prestataire de Service de Certification Electronique (PSCE).

La gestion des Certificats couvre toutes les opérations relatives à la vie d'un Certificat, depuis son émission jusqu'à la fin de vie de ce Certificat (expiration ou révocation).

L'AC CERTEUROPE est une Autorité de Certification mutualisée. Cette mutualisation permet à l'AC de gérer plusieurs clients qui délivreront des certificats électroniques à leur population.

I.2. IDENTIFICATION DU DOCUMENT

La présente PC est identifiée par l'OID 1.2.250.1.105.9.1.1.2.

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 ADVANCED CA V3 (9)
            - PC CERTEUROPE ADVANCED CA V3 (1)
              - Version majeure (1)
                - Version mineure (2)

I.3. ENTITES INTERVENANT DANS L'IGC

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

I.3.1. AUTORITES 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.

L'AC est entièrement responsable de la fourniture des services de certification décrits ci-dessous :

- **Autorité d'Enregistrement (AE) :** Fonction remplie par une personne désignée par l'Autorité de Certification C@rteurope qui consiste à vérifier l'identité et la qualité d'un demandeur de certificat et/ou à générer avant remise en main propre et/ou à révoquer ledit certificat. Au sein de la fonction d'Autorité d'Enregistrement, les rôles peuvent être subdivisés en :
  - **Autorité d'Enregistrement Administrative (AEA) :** fonction qui consiste à vérifier l'identité et la qualité d'un demandeur de certificat avant de pouvoir procéder à la remise du certificat.
  - **Autorité d'Enregistrement Technique (AET) :** fonction qui consiste à personnaliser (tirage du bi-clé et insertion du certificat) les clés des Porteurs suite à une vérification préalable.
  - **Autorité d'Enregistrement Déléguée (AED) :** fonction qui consiste à procéder à la remise en face-à -face contre récépissé du SSCD au Porteur.
- **Service d'enregistrement** : vérifie les informations d'identification du porteur d'un certificat lors de son enregistrement initial ou d'un renouvellement.
- **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 conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.
- **Service de fourniture de dispositif au porteur** : remet au porteur un dispositif d'authentification et de signature (SSCD) contenant la bi-clé et le certificat du porteur.
- **Service de fourniture de code d'activation au porteur**

  Ce service remet au porteur le code d'activation de son SSCD.
- **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. Une composante de ce service est en mesure de prendre en charge des révocations en urgence.
- **Service d'information sur l'état des certificats** : fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, valide, etc.).
- **Service d'assistance aux porteurs** : assiste les porteurs et utilisateurs de certificats émis par l'AC. Ce service est accessible par téléphone ou par messagerie électronique.

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

- **Demandeur** – personne physique ou morale qui souhaite souscrire au Service de Certification Electronique C@rteurope.
- **Abonné** : personne physique ou morale qui souscrit au **S**ervice de Certification Electronique C@rteurope.
- **Porteur / Sujet** - La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.
- **Mandataire de certification (MC)** - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des porteurs de cette entité (il assure notamment le face-à-face pour l'identification des porteurs lorsque celui-ci est requis).
- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur d'authentification provenant du porteur du certificat ou pour vérifier une signature électronique provenant du porteur du certificat.
- **Personne autorisée** - Il s'agit d'une personne autre que le porteur et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …).Typiquement, dans une entreprise, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, l'AC CERTEUROPE, en tant que responsable de l'ensemble de l'IGC, a mené une analyse de risques permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC. Les mesures de sécurité ad'hoc ont été mises en œuvre.

I.3.2. AUTORITES D'ENREGISTREMENT

L'Autorité d'Enregistrement (AE) est une composante du PSCE ayant en charge les services suivants tels que définis au §I.3.1 :

- service d'enregistrement,
- service de fourniture de dispositif au porteur,
- service de gestion des révocations.

L'Autorité d'Enregistrement peut éventuellement déléguer la vérification du dossier de demande de certificat et/ou la remise du dispositif au porteur ou à son mandataire (cf. §I.3.1).

I.3.3. PORTEURS DE CERTIFICATS

Dans le cadre de la présente PC, les certificats sont remis à des personnes physiques appartenant à une entité. Il faut donc dissocier le souscripteur qui passe un contrat avec l'AC et le porteur ou sujet à qui le certificat s'applique.

Le porteur utilise sa clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle il a un lien contractuel / hiérarchique / réglementaire.

Le porteur et le souscripteur respectent les conditions qui leur incombent définies dans la présente PC.

Le souscripteur est responsable en dernier ressort concernant l'utilisation de la clé privée associée au certificat à clé publique, mais le porteur est l'individu authentifié par sa clé privée.

I.3.4. 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 peuvent également être des plateformes de marchés publics ou toute application autorisée par l'AC.

I.3.5. AUTRES PARTICIPANTS

I.3.5.1. Composantes de l'IGC

Voir chapitre cf. §I.3.1.

I.3.5.2. Mandataire de certification

Voir chapitre cf. §I.3.1.

I.3.5.3. 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

I.4.1.1. Bi-clés et certificats des porteurs

La présente PC traite des bi-clés et des certificats à destination des catégories de porteurs identifiées au chapitre I.3.3 ci-dessus, afin que ces porteurs puissent s'authentifier et/ou signer électroniquement des données (documents, messages) dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées au chapitre I.3.4 ci-dessus.

Concernant la fonction **d'authentification**, il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique.

Concernant la fonction **signature**, celle-ci apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

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

I.4.1.2. Bi-clés et certificats d'AC et de composantes

L'AC dispose d'une seule bi-clé et le Certificat correspondant est rattaché à une AC de niveau supérieur (AC Racine de CertEurope).

les différentes clés internes à l'IGC sont décomposées suivant les catégories ci-dessous :

– la clé de signature de l'AC est utilisée pour signer les Certificats générés par l'AC ainsi que les informations sur l'état des Certificats (LCR et, éventuellement, réponses OCSP) ;
– les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC à des fins d'authentification, de signature des journaux d'événements, de chiffrement des données échangées ou stockées au sein de l'IGC, etc. ;
– les clés de contrôle, assignées au personnel de l'IGC afin de s'authentifier vis-à-vis des différents systèmes, de signer et/ou de chiffrer des messages ou des données échangés, etc. Par exemple, les clés du personnel de l'AE qui s'authentifie et signe les demandes de Certificat.

I.4.2. DOMAINE D'UTILISATION INTERDITS

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre IV.5 ci-dessous. L'AC doit respecter ces restrictions et imposer leur respect par ses porteurs et ses utilisateurs de certificats. L'Autorité de Certification CERTEUROPE décline toute responsabilité quant à l'usage que ferait un Abonné de son Certificat dans le cadre d'une application ne relevant pas de celles citées au chapitre XIII.

I.5. GESTION DE LA PC

I.5.1. ENTITE GERANT LA PC

I.5.1.1. Organisme responsable

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

CERTEUROPE
34-36, rue de la Folie Regnault 75011 Paris
FRANCE

I.5.1.2. Personne physique responsable

Monsieur Stéphane Drai
Président du Directoire
34-36, rue de la Folie Regnault - 75011 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 C@rteurope – 34-36, rue de la Folie Regnault – 75011 PARIS
– Par e-mail à l'adresse :
info@certeurope.fr
– Par téléphone au numéro : 01.45.26.72.00

I.5.3. ENTITE DETERMINANT LA CONFORMITE DE LA DPC A LA PC

CertEurope via son Comité PKI détermine la conformité de la DPC à la PC.

I.5.4. PROCEDURES D'APPROBATION DE LA CONFORMITE DE LA DPC

La conformité de la DPC avec la PC est approuvée par le Comité Qualité (CQUAL) de CertEurope

I.6. DEFINITIONS ET ACRONYMES

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AEA	Autorité d'Enregistrement Administrative
AET	Autorité d'Enregistrement Technique
AED	Autorité d'Enregistrement Déléguée
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
DGME/SDAE	Direction Générale de la Modernisation de l'Etat/ Service du Développement de l'Administration Electronique
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)
PIN	Personal Identification Number
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RGS	Référentiel Global de Sécurité
RSA	Rivest Shamir Adelman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SN	Serial Number
SSCD	Dispositif Sécurisé de Création de Signature
SHA-1	Secure Hash Algorithm One
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

I.6.1. TERMES COMMUNS AU RGS

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat.

Autorités administratives - Ce terme générique désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage type du RGS).

Infrastructure de gestion de clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en oeuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée

(lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Promoteur d'application - Un responsable d'un service de la sphère publique accessible par voie électronique.

Qualification des produits de sécurité - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS]. La procédure de qualification des produits de sécurité est décrite dans le [DécretRGS]. Le [RGS] précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

I.6.2. TERMES SPECIFIQUES OU COMPLETES / ADAPTES POUR LA PRESENTE PC

Autorité de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre I et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC.

Autorité d'enregistrement - Cf. chapitre I.3.2

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

Code PIN : code adressé par courrier postal au Porteur après avoir été généré automatiquement et aléatoirement par l'AC. Il permet d'activer le SSCD du porteur. Le Porteur assume en toutes circonstances le caractère secret du Code PIN, aussi l'utilisation de celui-ci fera présumer de manière irréfragable que le Porteur est bien l'initiateur de l'action opérée (non-répudiation).

Code de révocation d'un Certificat : code connu uniquement par le Porteur et utilisé pour faire une demande de révocation.

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction ou service de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Common Name (CN) : identité réelle ou pseudonyme du Porteur* (exemple CN = Jean Dupont).

Communauté : ensemble de personnes liées entre elles soit par des contrats (exemples : une entreprise et ses fournisseurs, des employés d'une entreprise..) soit par leur qualité (membres d'un ordre….)

Compromission : une clé est dite compromise lorsqu'elle est connue par d'autres personnes que celles habilitées à la mettre en œuvre.

Dossier de Souscription (DDS) : ensemble des pièces justificatives à fournir à l'AE afin de lui permettre de vérifier les informations demandées par l'AC pour l'émission d'un Certificat. Ces pièces justificatives sont décrites dans la présente PC.

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

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

Mandataire de certification - Cf. chapitre I.3.1

Personne autorisée - Cf. chapitre I.3.1

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Porteur - Cf. chapitre I.3.1

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

Référencement - Opération qui consiste, pour l'Administration, à tenir à jour la liste des offres de certification électronique des PSCE qui répondent à des exigences spécifiées dans le RGS. Seuls les certificats d'offres référencées peuvent être utilisées dans le cadre des échanges dématérialisés de l'Administration. Une offre référencée par rapport à un service donné et un niveau de sécurité donné du

RGS peut être utilisée dans toutes les applications d'échanges dématérialisés requérant ce service et ce niveau de sécurité ou un niveau inférieur. Pour les usagers, le référencement permet de connaître quelles offres de certificats électroniques ils peuvent utiliser pour quels échanges dématérialisés.

Service d'enregistrement : Cf. chapitre I.3.1
Service de génération des certificats Cf. chapitre I.3.1
Service de publication et diffusion : Cf. chapitre I.3.1
Service de fourniture de dispositif au porteur : Cf. chapitre I.3.1
Service de fourniture de code d'activation au porteur - Cf. chapitre I.3.1
Service de gestion des révocations : Cf. chapitre I.3.1
Service d'information sur l'état des certificats : Cf. chapitre I.3.1
Service d'assistance aux porteurs : Cf. chapitre I.3.1

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale dans ses relations avec une administration.
Nota - Un agent d'une autorité administrative qui est en relation avec une autre autorité administrative est, pour cette dernière, un usager.

Utilisateur de certificat - Cf. chapitre I.3.1

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

II.1. ENTITES CHARGEES 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 ADVANCED CA V3, OU=0002 434202180, O=Certeurope, C=FR?certificateRevocationList ;

copie 2 : ldap://lcr2. certeurope.fr/CN=CERTEUROPE ADVANCED CA V3, OU=0002 434202180, O= Certeurope, C=FR?certificateRevocationList ;

copie 3 : http://www.certeurope.fr/reference/certeurope_v3.crl ;

II.2. INFORMATIONS DEVANT ETRE PUBLIEES

L'OC pour le compte de l'AC CERTEUROPE 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_certeurope_v3_v1.2.pdf
– la Liste de Certificats Révoqués (LCR).
– le certificat de l'AC Certeurope Root CA 2, en cours de validité, auquel la clé de l'AC CERTEUROPE est subordonnée. Ce certificat est disponible sur le site Web de CertEurope à l'URL http://www.certeurope.fr/chaine-confiance-numerique.php. L'empreinte numérique du certificat est également disponible pour une garantie d'intégrité.
– le Certificat de l'AC CERTEUROPE en cours de validité et son empreinte numérique.
– les informations permettant aux utilisateurs de certificats de s'assurer de l'origine du certificat de l'AC et son état,
– les conditions générales d'utilisation.
– les conditions générales de vente et les conditions particulières et générales d'utilisation des certificats.
– le formulaire de demande de certificat.
– le formulaire de demande de révocation de certificat.
– les empreintes numériques des données publiées (exemple hash des fichiers pour la PC).

Le format recommandé pour la publication des documents est le PDF pour faciliter la lecture par les utilisateurs.

Tous les documents sont disponibles sur le site à l'adresse : http://www.certeurope.fr/certeurope_advanced_ca_v3/doc/dossier_auth-sign_v3.zip à savoir :

- le Certificat de l'AC CERTEUROPE en cours de validité et son empreinte numérique (certeurope_advanced_ca_v3.crt)
- Les conditions générales d'utilisation.
- Les conditions particulières et générales d'utilisation des certificats.
- Formulaire de demande de certificat.
- Formulaire de demande de révocation.

L'AC CERTEUROPE n'étant en certification croisée avec aucune autre AC, la publication de la liste des AC avec lesquelles elle est en certification croisée est sans objet.

II.3. DELAIS ET FREQUENCES DE PUBLICATION

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

– Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.
– Pour les certificats d'AC, ils doivent être diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants.
– Pour les informations d'état des certificats, cf. §IV.9 et §IV.10.

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 assurent une disponibilité les Jours ouvrés
– 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. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

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 (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. NECESSITE D'UTILISATION DE NOMS EXPLICITES

Les noms choisis pour désigner les porteurs de certificats doivent être explicites.

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 tel que figurant au K-Bis ou dans l'avis SIRENE ;
– dans le champ « **OrganizationUnitName** » :
  Ce champ contient le numéro de SIREN de l'Entreprise, tel que figurant au K-Bis ou dans l'avis SIRENE ; 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 premier prénom de l'état civil du porteur (si la pièce d'identité présentée pour l'enregistrement comporte d'autres prénoms, il n'y a pas d'obligation à mentionner ces autres prénoms dans le certificat, mais s'ils le sont, ils doivent l'être dans le même ordre que sur la pièce d'identité et séparés par une virgule sans espace ni avant ni après la virgule), suivi d'un espace, suivi au choix du porteur du nom de l'état civil ou du nom d'usage figurant sur la pièce d'identité. A la suite du nom d'état civil, et en fonction des besoins de l'AC, d'autres informations peuvent être mentionnées dans cet attribut (séparées par des espaces), notamment des informations permettant de traiter les cas d'homonymie au sein du domaine de l'AC. Cependant, si l'attribut serialNumber est présent dans les certificats, c'est celui-ci qui doit être utilisé pour traiter les cas d'homonymie (cf. [RFC3739]).
– dans le champ « **SerialNumber** » :
  Ce champ permet de garantir l'unicité du DN par l'utilisation d'un HASH (SHA-1) calculé à partir des informations personnelles du porteur contenues dans la pièce d'identité (carte d'identité nationale ou passeport ou carte de séjour). Il permet de résoudre les cas d'homonymie (cf. [RFC3739]).

– dans le champ « **1.2.250.1.105.20.1** » :
  Ce champ contient l'identifiant de l'Autorité d'enregistrement qui a délivré ce certificat. L'AC CERTEUROPE est une autorité de certification mutualisée.

Exemple : DN = {C=FR, O=Société AAA, OU= 0002 243111589, CN=Jean-Claude DUPONT, Numéro de série = c36f37bc6fc9315651ad5426bb437f77d841c888, 1.2.250.1.105.20.1=Identifiant AE , Email=jean-claude.dupont@societeaaa.fr}

III.1.3. PSEUDONYMISATION DES PORTEURS

Les pseudonymes ne sont pas autorisés.

III.1.4. REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOMS

Aucune interprétation particulière n'est à faire des informations portées dans le champ "Subject" des Certificats.

Ces informations sont établies par l'AE et reposent essentiellement sur les règles suivantes :

– 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 prénoms et noms composés sont séparés par des tirets " - ".

III.1.5. UNICITE DES NOMS

L'unicité du DN est garantie par l'unicité des informations permettant de construire ce dernier. Il s'agit du numéro SIREN pour différencier deux Entreprises, du nom et du prénom du Porteur et du HASH créé à partir d'informations personnelles contenues dans la pièce d'identité du Porteur.

III.1.6. IDENTIFICATION, AUTHENTIFICATION ET ROLE DES MARQUES DEPOSEES

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 se dégage de 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'IDENTITE

L'enregistrement d'un Porteur peut se faire soit directement auprès de l'AE, soit via un Mandataire de Certification. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

La validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants :

– Enregistrement d'un porteur sans MC : validation par l'AE de l'identité "personne morale" de l'entité de rattachement du porteur et de l'identité "personne physique" du futur porteur.

– Enregistrement d'un MC : validation de l'identité "personne morale" de l'entité pour lequel le MC interviendra et de l'identité "personne physique" du futur MC.
– Enregistrement d'un porteur via un MC préalablement enregistré: validation par le MC de l'identité "personne physique" du futur porteur.

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre III.2.3.

III.2.1. METHODE POUR PROUVER LA POSSESSION DE LA CLE PRIVEE

Sans objet. Le porteur ne génère pas sa clé privée.

III.2.2. VALIDATION DE L'IDENTITE D'UN ORGANISME

Cf. §III.2.3.

III.2.3. VALIDATION DE L'IDENTITE D'UN INDIVIDU

III.2.3.1. Enregistrement d'un porteur sans MC

La distribution des certificats par l'AE nécessite impérativement un face-à-face au dépôt du dossier auprès de l'AE ou lors de la remise de la clé. Ce face-à-face se fait directement entre le Porteur et l'AE (ou l'AED) auquel cas l'AE vérifie un original d'une pièce d'identité officielle du Porteur comportant sa photo et sa signature et en prend une copie.

Le dossier d'enregistrement déposé directement auprès de l'AE, doit au moins comprendre :
– Une demande de certificat
  - Une demande écrite, sur papier à entête portant le numéro SIREN de l'entreprise, signée par le représentant légal et datant de mois de 3 mois. ;
  - une déclaration du Porteur, portant l'acceptation des engagements du Porteur ;
  - une adresse postale du Porteur ;
  - le prénom et le nom du Porteur à utiliser dans le certificat ;
  - l'adresse de courrier électronique du Porteur ;

– Les pièces justificatives de l'identité du Porteur
  - une photocopie d'un justificatif d'identité du Porteur muni d'une photo (carte d'identité nationale, passeport ou carte de séjour). La pièce doit indiquer la date et le lieu de naissance du Porteur ;

– Les pièces justificatives de l'entité (Entreprise)
  - une photocopie d'un justificatif d'identité du représentant légal muni d'une photo (carte d'identité nationale, passeport ou carte de séjour). La pièce doit indiquer la date et le lieu de naissance du représentant légal ;
  - une pièce valide au moment de l'enregistrement portant le numéro d'identification de l'entreprise (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou répertoire des métiers) ;

Nota : Le Porteur est informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation.

Des procédures d'enregistrement spécifiques respectant les exigences du RGS peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

III.2.3.2. Enregistrement d'un Mandataire de Certification

La distribution des certificats par l'AE nécessite impérativement un face-à-face au dépôt du dossier auprès de l'AE ou lors de la remise de la clé. Ce face-à-face se fait directement entre le MC et l'AE (ou l'AED) auquel cas l'AE vérifie un original d'une pièce d'identité officielle du MC comportant sa photo et sa signature et en prend une copie.

Une AE (ou AEA) est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification (MC) pour répondre aux besoins suivants :

– Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les porteurs présentés par le MC.
– Eventuellement, fourniture d'un certificat au MC pour qu'il puisse signer les dossiers d'enregistrement de porteurs d'entité qu'il représente sous forme électronique.

Le dossier d'enregistrement, déposé auprès d'un MC, comprend :

– un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le MC. Ce mandat doit être signé par le MC pour acceptation,
– un engagement signé avec entête ou cachet de l'entreprise, et daté de moins de 3 mois, du MC, de respecter et de faire respecter l'ensemble des dispositions contractuelles et des procédures conformément au contrat d'abonnement au service signature électronique,
– un engagement signé, et daté de moins de 3 mois, du MC à signaler à l'AE son départ de l'entité,
– une pièce, valide au moment de l'enregistrement, portant le numéro SIREN de l'entreprise (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou répertoire des métiers) ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat,
– un document officiel d'identité en cours de validité du MC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,

Nota : Le porteur est informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation.

Nota : Un face-à-face entre le MC et l'AE doit avoir lieu

A l'issue de cet enregistrement, le mandataire de certification reçoit, par email, un code de révocation d'urgence lui permettant de s'identifier auprès de l'AE pour demander la révocation de porteurs de son organisation.

S'il s'agit de la première demande d'enregistrement pour un mandataire de certification de cette société (nouveau client de l'AC), le représentant légal recevra également, par courrier, un code de révocation d'urgence lui permettant de s'identifier auprès de l'AE pour demander la révocation des mandataires de sa structure, ou de porteurs de son organisation.

III.2.3.3. Enregistrement d'un porteur via un MC préalablement enregistré.

La distribution des certificats par l'AE nécessite impérativement un face-à-face au dépôt du dossier auprès de l'AE ou lors de la remise de la clé. Ce face-à-face se fait directement entre le Porteur et le MC auquel cas le MC vérifie un original d'une pièce d'identité officielle du Porteur comportant sa photo et sa signature et en prend une copie.

Le dossier d'enregistrement, déposé auprès de l'AE via un MC, comprend :

– Une demande de certificat
  - Une demande écrite sur papier à entête ou doit contenir le cachet de l'entreprise portant le numéro SIREN de l'entreprise, co-signée par le MC et le porteur, et datant de mois de 3 mois. Un modèle est proposé sur l'URL suivante : http://www.certeurope.fr/certeurope_advanced_ca_v3/doc/dossier_auth-sign_v3.zip
  - une déclaration du Porteur, portant l'acceptation des engagements du Porteur ;
  - une adresse postale professionnelle du Porteur ;
  - le prénom et le nom du Porteur à utiliser dans le certificat ;
  - l'adresse de courrier électronique du Porteur ;

– Les pièces justificatives de l'identité du Porteur
  - une photocopie d'un justificatif d'identité du Porteur muni d'une photo (carte nationale d'identité, passeport ou carte de séjour). La pièce doit indiquer la date et le lieu de naissance du Porteur ;

– Le dossier d'enregistrement du MC si celui-ci n'est pas déjà enregistré (cf. III.2.3.2).
  Nota : Le MC doit être mandaté par le représentant légal de l'entité du Porteur.

– Les pièces justificatives de l'entité (Entreprise) si différente de celle du MC
  - une photocopie d'un justificatif d'identité du représentant légal muni d'une photo (carte d'identité nationale, passeport ou carte de séjour). La pièce doit indiquer la date et le lieu de naissance du représentant légal ;
  - une pièce, valide au moment de l'enregistrement, portant le numéro SIREN de l'entreprise (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou répertoire des métiers) ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;

Nota : Le Porteur est informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation.

Des procédures d'enregistrement spécifiques respectant les exigences du RGS peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

III.2.4. INFORMATIONS NON VERIFIEES DU PORTEUR

Les champs : Title, Locality, Email, Description, sont purement informatifs et n'ont donné lieu à aucune vérification avancée.

III.2.5. VALIDATION DE L'AUTORITE DU DEMANDEUR

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AE ou par le MC).

III.2.6. CERTIFICATION CROISEE D'AC

Sans objet. L'AC CERTEUROPE n'a aucun accord de reconnaissance avec une autre AC.

III.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

III.3.1. IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

Le porteur est averti de l'arrivée à expiration de son certificat 3 mois et 1 mois avant l'expiration. Le renouvellement de certificat nécessite la constitution d'un dossier identique à la demande initiale. Le premier renouvellement ne nécessite pas obligatoirement de face-à-face pour la remise de la clé. Cette remise est effectuée par un moyen permettant de garantir l'identité du destinataire.

Des procédures d'enregistrement spécifiques respectant les exigences du RGS peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

III.3.2. IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION

Suite à la révocation d'un certificat pour les causes suivantes, celui-ci peut être renouvelé :

- Détérioration du SSCD ;
- blocage du SSCD ;
- perte du SSCD ;
- vol du SSCD ;
- compromission de la clé privée ;

Ce renouvellement est effectué par l'intermédiaire d'un formulaire signé et daté par le Porteur et l'AE.

L'AE vérifie la validité du dossier déjà enregistré et archivé lors de la demande initiale (cf. §III.2). Le nouveau certificat est généré à l'identique du précédent et remis en face-à-face.

III.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

Une demande de révocation peut être faite :

– par courrier ou par télécopie. Elle doit alors être signée par le demandeur et le Service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au Certificat à révoquer.

– Par téléphone ou par internet. Le demandeur est formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au Certificat à révoquer. L'identité du demandeur est réalisée par une série de 3 questions sur des informations propres au demandeur, dont un code de révocation connu uniquement du demandeur.

Des procédures de révocation spécifiques respectant les exigences du RGS peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

IV. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

IV.1. DEMANDE DE CERTIFICAT

IV.1.1. ORIGINE DE LA DEMANDE

Un certificat CERTEUROPE ne peut être demandé que par le futur porteur, le représentant légal de l'entité ou le MC dûment mandaté pour cette entité. Dans tous les cas, le consentement préalable du futur porteur est obligatoire.

IV.1.2. PROCESSUS ET RESPONSABILITES POUR L'ETABLISSEMENT D'UNE DEMANDE DE CERTIFICAT

La demande de certificat comporte (cf. chapitre III.2 ci-dessus) :

– le nom du porteur à utiliser dans le certificat (nom réel) ;
– les données personnelles d'identification du porteur ;
– les données d'identification de l'entité (sauf si l'enregistrement est effectué par l'intermédiaire d'un MC).

Le dossier de demande est établi soit directement par le futur porteur à partir des éléments fournis par son entité, soit par son entité et signé par le futur porteur. Si l'entreprise n'a pas mis en place de MC, le dossier est transmis directement à l'AE. Si l'entreprise a mis en place un MC, le dossier lui est remis.

IV.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

IV.2.1. EXECUTION DES PROCESSUS D'IDENTIFICATION ET DE VALIDATION DE LA DEMANDE

Une demande de certificat peut être déposée ou expédiée par courrier au service d'enregistrement de l'AE.

A la réception du dossier d'enregistrement, l'AE effectue les opérations suivantes :

– valider l'identité du futur porteur ;
– vérifier la cohérence des justificatifs présentés ;
– s'assurer de l'existence et de la validité des pouvoirs du demandeur ;
– s'assurer que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat.

  Nota : Si le dossier n'est pas complet, le demandeur est contacté pour compléter son dossier. Quelque soit la suite donnée à la demande le demandeur en est informé.

Dans le cas d'une demande via un MC, celui-ci retransmet le dossier à l'AE après avoir effectué les opérations ci-dessus. L'AE s'assure que la demande correspond bien au mandat du MC.

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat vers la fonction adéquate de l'IGC (cf. chapitre I.3.1).

L'AE conserve les pièces énumérées dans la procédure d'archivage; en particulier elle conserve un exemplaire original de la demande signée par le futur porteur et par l'AE, ou par le MC le cas échéant ainsi qu'une photocopie de la pièce d'identité présentée avec la demande.

IV.2.2. ACCEPTATION OU REJET DE LA DEMANDE

En cas de rejet de la demande, l'AE en informe le porteur ou, le MC le cas échéant, par courrier en justifiant le rejet.

IV.2.3. DUREE D'ETABLISSEMENT DU CERTIFICAT

Le délai de génération d'un certificat est de deux jours ouvrés à compter de la réception d'un dossier complet, sans préjuger des délais d'acheminement des clés par voie postale.

IV.3. DELIVRANCE DU CERTIFICAT

IV.3.1. ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT

Lorsqu'une demande de certificat a été validée par le service d'enregistrement de l'AE, l'AE procède à la demande de certificat au service de génération de l'AC. Lors de la demande, les clés du Porteur sont générées sur le SCCD.

Suite à l'authentification de l'origine de la demande et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC génère le certificat.

Une fois le certificat généré, le service de fourniture de code d'activation de l'AC (OSC) envoie le code PIN au porteur qui est ainsi prévenu officiellement de la mise à disposition de son certificat

Nota : Le service de fourniture de code d'activation du SSCD du Porteur est nécessairement indépendant de l'AE. Cette indépendance garantit que seul le Porteur est en mesure d'utiliser son SSCD.

Le délai de génération d'un certificat est de 2 jours ouvrés à compter de la remise du dossier complet. NB : il s'agit là du délai de génération (temps nécessaire à l'AE pour générer la clé) et pas du délai de délivrance du certificat

IV.3.2. NOTIFICATION PAR L'AC DE LA DELIVRANCE DU CERTIFICAT AU PORTEUR

Le porteur est notifié immédiatement par email dès la génération de son certificat.

Le service de fourniture de dispositif au porteur de l'AE remet en face-à-face le SSCD au porteur ou au MC. Lors de ce face-à-face, l'AE vérifie l'identité du porteur ou du MC en s'assurant que les pièces justificatives transmises lors de la demande correspondent bien aux originaux présentés.

Lors de ce face-à-face une copie de la pièce d'identité du porteur est récupérée par l'AE. Celle-ci est signée au dos et accompagnée de la mention « certifiée conforme à l'original ».

Dans le cas où le MC effectue le face-à-face avec l'AE, celui-ci s'engage à remonter auprès de l'AE une copie de la pièce d'identité du porteur cosignée par le porteur lui-même et le MC au dos et accompagnée de la mention « certifiée conforme à l'original ».

Dans le cas où le face-à-face a eu lieu au dépôt du dossier, le SSCD est envoyé directement au Porteur par courrier recommandé avec accusé de réception.

Des procédures d'enregistrement spécifiques respectant les exigences du RGS peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

IV.4. ACCEPTATION DU CERTIFICAT

IV.4.1. DEMARCHE D'ACCEPTATION DU CERTIFICAT

Le retrait du SSCD auprès de l'AE vaut acceptation du certificat. Le Porteur doit informer l'AE, dans les 8 jours après réception de son certificat, d'une éventuelle erreur. Passé ce délai, le certificat sera considéré comme accepté par le Porteur.

Lors du face-à-face de remise le porteur ou le MC signe un reçu attestant de l'acceptation de son certificat. Ce reçu est cosigné par l'AE et ajouté au dossier du porteur conservé par l'AE.

Lors du face-à-face une copie de la pièce d'identité du porteur est récupérée par l'AE. Celle-ci est cosignée par le porteur et l'AE au dos et accompagnée de la mention « certifiée conforme à l'original ».

Dans le cas où le MC effectue le face-à-face avec l'AE, celui-ci s'engage à remonter auprès de l'AE une copie de la pièce d'identité du porteur cosignée par le porteur lui-même et le MC au dos et accompagnée de la mention « certifiée conforme à l'original ».

Le porteur est soumis à une acceptation tacite sous seize (16) jours. Passé ce délai, le certificat sera considéré comme accepté.

Dans le cas où le MC effectue le face-à-face avec l'AE, celui-ci doit remettre le certificat au porteur en face-à-face sous huit (8) jours.

IV.4.2. PUBLICATION DU CERTIFICAT

Les certificats des porteurs ne sont pas publiés par l'AC.

IV.4.3. NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT

Lors de la génération d'un nouveau Certificat :

- l'AE est nécessairement avertie puisque c'est elle qui initie le processus et qui s'assure que le certificat demandé est bien présent dans le SSCD du Porteur ;
- L'OC est au courant de la demande de l'AE puisque cette organisation est en charge de la partie technique de l'AC et en particulier la signature du certificat. De plus, toutes les demandes sont tracées ;
- L'AC en tant qu'entité de gestion de l'ensemble de l'IGC dispose d'un outil de suivi qui lui permet de contrôler les générations de certificats ;
- Le Porteur est averti dès la génération de son certificat par e-mail ;
- Le demandeur est contacté par l'AE pour venir récupérer le ou les certificats.

IV.5. USAGES DE LA BI-CLE ET DU CERTIFICAT

IV.5.1. UTILISATION DE LA CLE PRIVEE ET DU CERTIFICAT PAR LE PORTEUR

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service d'authentification et de signature. Les porteurs 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 du porteur 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 CLE 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 d'un certificat est de trois ans et l'Autorité de Certification CERTEUROPE ne permet pas le renouvellement de ses certificats.
Le porteur est prévenu par courrier ou par e-mail au moins un mois avant la date de fin de validité de son certificat.

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. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE RENOUVELLEMENT

Sans objet.

IV.6.4. NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Sans objet.

IV.6.5. DEMARCHE 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 ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT

Sans objet.

IV.7. DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

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-CLE

Les bi-clés seront renouvelées au minimum tous les trois ans.
Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du porteur (cf. chapitre IV.9, notamment le chapitre IV.9.1.1 pour les différentes causes possibles de révocation).

Nota - Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat".

IV.7.2. ORIGINE D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Le porteur est prévenu par courrier ou par e-mail au moins un mois avant la date de fin de validité de son certificat.
L'origine d'une demande d'un nouveau certificat est identique à celle d'une demande initiale.

IV.7.3. PROCEDURE 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'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Cf. chapitre IV.3.2.

IV.7.5. DEMARCHE 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 ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT

Cf. chapitre IV.4.3.

IV.8. MODIFICATION DU CERTIFICAT

Nota - Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre IV.7) et autres que uniquement la modification des dates de validité (cf. chapitre IV.6).

La modification de Certificat CERTEUROPE 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. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT

Sans objet.

IV.8.4. NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU CERTIFICAT MODIFIE

Sans objet.

IV.8.5. DEMARCHE D'ACCEPTATION DU CERTIFICAT MODIFIE

Sans objet.

IV.8.6. PUBLICATION DU CERTIFICAT MODIFIE

Sans objet.

IV.8.7. NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT MODIFIE

Sans objet.

IV.9. REVOCATION 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 REVOCATION

IV.9.1.1. Certificats de porteurs

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

- les informations du Porteur figurant dans son Certificat ne sont pas ou plus exactes, ceci avant l'expiration normale du Certificat ;
- les informations figurant dans le Dossier de Souscription ne sont plus exactes ou s'avèrent frauduleuses
- le Porteur n'a pas respecté des règles d'utilisation du Certificat ;
- la clé privée du Porteur est suspectée de compromission, est compromise ou perdue ;
- la résiliation ou le non-paiement du contrat d'abonnement ;
- le Porteur, le MC le représentant légal de l'Entreprise en fait la demande ;
- le départ, la mutation à un autre poste ou le décès du Porteur, ainsi que la cessation d'activité de son Entreprise.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a eu connaissance, le Certificat concerné est révoqué et placé dans la Liste de Certificats Révoqués (LCR).

Des procédures de révocation spécifiques respectant les exigences du RGS peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures spécifiques dument validées par CertEurope qui prévaudront.

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

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats, de LCR) :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

Des procédures de révocation spécifiques respectant les exigences du RGS peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures spécifiques dument validées par CertEurope qui prévaudront.

IV.9.2. ORIGINE D'UNE DEMANDE DE REVOCATION D'UN CERTIFICAT PORTEUR

IV.9.2.1. Certificats de porteurs

La révocation d'un Certificat Porteur peut émaner :

- du Porteur au nom duquel le Certificat a été émis ;
- du représentant légal de l'Entreprise ;
- du Mandataire de Certification ;
- de l'AC CERTEUROPE émettrice du Certificat ou de l'AE.

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

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

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

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

IV.9.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

IV.9.3.1. Révocation d'un certificat de porteur

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre III.4.

La demande de révocation doit comporter au minimum :

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

Les demandes de révocation par les Porteurs et les représentants légaux d'entreprises peuvent être réalisées auprès de l'AE en face-à-face (pendant ses heures d'ouverture), par l'envoi d'une demande signée, ou encore par téléphone (pour les Porteurs et Représentant Légal) en possession de son code de révocation.

Les procédures de révocation sont détaillées dans la DPC.

A la réception d'une demande de révocation, l'authenticité du demandeur est vérifiée. Cette vérification est réalisée par l'AE lors d'un face à face, par téléphone ou par échange de documents signés électroniquement.

Si la demande est recevable, l'AE demande la révocation du certificat en demandant à l'AC d'introduire le numéro de série du Certificat et la date de révocation du Certificat dans la Liste des Certificats Révoqués.

Si la demande n'est pas recevable, l'AE en informe le demandeur.
Le Porteur est notifié de la publication de la révocation. Les causes de révocation ne sont pas publiées.
L'opération est enregistrée dans les journaux d'événements de l'AC CERTEUROPE.

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

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

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

Le certificat de l'AC étant signé par une racine, le simple fait de révoquer le certificat par l'AC racine invalide l'ensemble des certificats de porteur.

Le contact identifié sur le site http://www.references.modernisation.gouv.fr/) est immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

IV.9.4. DELAI ACCORDE AU PORTEUR POUR FORMULER LA DEMANDE DE REVOCATION

Dès que le porteur (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. DELAI DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCATION

IV.9.5.1. Révocation d'un certificat de porteur

Par nature une demande de révocation doit être traitée en urgence.

La fonction de gestion des révocations est disponible 24h/24 7j/7.
Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme à 1h et une durée maximale totale d'indisponibilité par mois conforme à 4h.
Toute demande de révocation d'un certificat porteur est traitée dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.
Le délai de publication de la révocation d'un Certificat n'excède jamais 24 heures à partir de la réception de la demande de révocation.

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

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.
La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

IV.9.6. EXIGENCES DE VERIFICATION DE LA REVOCATION PAR LES UTILISATEURS DE CERTIFICATS

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

IV.9.7. FREQUENCE D'ETABLISSEMENT DES LCR

La fréquence de publication des LCR est de 24h.

IV.9.8. DELAI MAXIMUM DE PUBLICATION D'UNE LCR

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

IV.9.9. DISPONIBILITE D'UN SYSTEME DE VERIFICATION EN LIGNE DE LA REVOCATION ET DE L'ETAT DES CERTIFICATS

Il n'y a pas de serveur OCSP.

IV.9.10. EXIGENCES DE VERIFICATION EN LIGNE DE LA REVOCATION DES CERTIFICATS PAR LES UTILISATEURS DE CERTIFICATS

Cf. chapitre IV.9.6 ci-dessus.

IV.9.11. AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS.

Le porteur peut se connecter sur le site https://services.certeurope.fr/ muni de son certificat pour vérifier le statut de son certificat.
Ce service s'appuie sur les points de distribution des LCR de la chaîne de confiance.

IV.9.12. EXIGENCES SPECIFIQUES EN CAS DE REVOCATION POUR COMPROMISSION DE CLE

Pour les certificats des porteurs, aucune exigence spécifique en cas de compromission de la clé privée d'un porteur hormis la révocation du certificat.

En cas de compromission de la clé privée de l'AC, l'information de la révocation du certificat est diffusée sur le site de CertEurope http://www.certeurope.fr.
Par conséquent, l'accès au portail de demande de certificat en ligne devient indisponible.
Voir chapitre IV.9.3.2.

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. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE SUSPENSION

Sans objet**.**

IV.9.16. LIMITES DE LA PERIODE DE SUSPENSION D'UN CERTIFICAT

Sans objet**.**

IV.10. FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

IV.10.1. CARACTERISTIQUES OPERATIONNELLES

L'accès à la Liste de Certificats Révoqués est possible via deux annuaires LDAP V3 et d'un serveur Web. Les LCR sont au format dénommé "LCR V2".

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

IV.10.2. DISPONIBILITE 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 et le porteur avant la fin de validité du certificat, ce dernier est révoqué.

IV.12. SEQUESTRE DE CLE ET RECOUVREMENT

L'AC interdit le séquestre des clés des porteurs.

IV.12.1. POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR SEQUESTRE DES CLES

Sans objet.

IV.12.2. POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR ENCAPSULATION DES CLES DE SESSION

Sans objet.

V. MESURES DE SECURITE 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.

V.1. MESURES DE SECURITE PHYSIQUE

Une analyse de risque a été menée par Certeurope. Les exigences de sécurité sont décrites dans la Politique de Sécurité de l'OSC [CERT_PS].

V.1.1. SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES

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

V.1.2. ACCES PHYSIQUE

Les zones hébergeant les systèmes informatiques de l'AC CERTEUROPE 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 ELECTRIQUE ET CLIMATISATION

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

V.1.4. VULNERABILITE AUX DEGATS DES EAUX

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

V.1.5. PREVENTION ET PROTECTION INCENDIE

Les locaux d'hébergement des systèmes informatiques de l'AC CERTEUROPE 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 sont 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 sont 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 sont 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 SECURITE PROCEDURALES

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

V.2.1. ROLES 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 ;

Auditeur / 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 TACHES

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 ROLE

Chaque composante de l'AC 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 ;
- qu'une clé cryptographique et un certificat lui soient délivrés pour accomplir le rôle qui lui est affecté dans l'IGC.

V.2.4. ROLES EXIGEANT UNE SEPARATION 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 SECURITE VIS-A-VIS DU PERSONNEL

V.3.1. QUALIFICATIONS, COMPETENCES 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. PROCEDURES DE VERIFICATION DES ANTECEDENTS

Chaque entité opérant une composante de l'IGC met en oeuvre 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.
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).

V.3.3. EXIGENCES EN MATIERE 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 FREQUENCE EN MATIERE 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. FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS

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

V.3.6. SANCTIONS EN CAS D' ACTIONS NON-AUTORISEES

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-A-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. PROCEDURES DE CONSTITUTION DES DONNEES 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.

Des dispositions et procédures dérogatoires à cette journalisation peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures spécifiques dûment validées par CertEurope qui prévaudront.

V.4.1. TYPE D'EVENEMENTS A 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 oeuvre 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 ;
- remise de son dispositif de signature (SSCD) au porteur ;
- 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 clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- génération des éléments secrets du porteur (codes d'activation,…) ;
- génération des certificats des porteurs ;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, 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. FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS

Cf. chapitre V.4.8.

V.4.3. PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS

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'EVENEMENTS

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 VI.8.

V.4.5. PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS

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. SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS

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 EVENEMENT AU RESPONSABLE DE L'EVENEMENT

Sans objet.

V.4.8. EVALUATION DES VULNERABILITES

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 DONNEES

V.5.1. TYPES DE DONNEES A 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. PERIODE DE CONSERVATION DES ARCHIVES

Dossiers de demande de certificat

Chaque dossier de demande de Certificat et des pièces justificatives est archivé par l'AC pendant une durée de dix ans à compter de la date de génération du certificat.

Le Porteur, toute Personne autorisée, toute autorité judiciaire dûment habilitée peut y accéder pendant cette période d'archivage.

Le dossier de demande de Certificat et des pièces justificatives est détruit au terme de la période d'archivage par une broyeuse à papier.

Des procédures d'archivage spécifiques respectant les exigences du RGS peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'archivage spécifiques dument validées par CertEurope qui prévaudront.

Certificats et LCR émis par l'AC

Les Certificats de clés de signature, ainsi que les LCR produites par l'AC 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 oeuvre 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 :
- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- protégées en intégrité ;
- accessibles aux personnes autorisées ;
- lisibles et exploitables sur l'ensemble de leur cycle de vie ;

V.5.4. PROCEDURE DE SAUVEGARDE DES ARCHIVES

Sans objet.

V.5.5. EXIGENCES D'HORODATAGE DES DONNEES

Cf. chapitre V.4.4 pour la datation des journaux d'évènements.
Le chapitre VI.8 précise les exigences en matière de datation / horodatage.

V.5.6. SYSTEME DE COLLECTE DES ARCHIVES

Sans objet.

V.5.7. PROCEDURES DE RECUPERATION ET DE VERIFICATION 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 CLE D'AC

La période de validité de la clé de l'AC est de 10 ans.

La durée de vie des certificats Porteur étant de 3 ans, le renouvellement de cette clé devra intervenir au plus tard trois (3) ans 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 Porteurs émis ainsi que la LCR.

Le certificat précédent restera utilisable pour la validation de certificats 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 A COMPROMISSION ET SINISTRE

V.7.1. PROCEDURES DE REMONTEE ET DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSIONS

Chaque entité opérant une composante de l'IGC met en oeuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements.

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'événement 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 …).

V.7.2. PROCEDURES DE REPRISE EN CAS DE CORRUPTION DES RESSOURCES INFORMATIQUES (MATERIELS, LOGICIELS ET / OU DONNEES)

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.

Les postes des AE utilisés pour la révocation des certificats sont répartis sur les infrastructures de l'AE et de l'OC afin d'assurer une disponibilité optimale de la fonction révocation.

V.7.3. PROCEDURES DE REPRISE EN CAS DE COMPROMISSION DE LA CLE PRIVEE D'UNE COMPOSANTE

Les clés d'infrastructure ou de contrôle sont réparties dans les composantes AC, AE et OC.

Composante AE

L'AE dispose de clés pour son personnel habilité à générer et révoquer des certificats.

En cas de compromission d'une de ses clés, l'AE en informe l'AC laquelle fait une demande à l'OC afin de révoquer le certificat de l'AE et le cas échéant en générer un nouveau.

Composante AC

L'AC dispose de clés pour son personnel habilité : suivi de la production et révocation des certificats.

En cas de compromission d'une de ses clés, l'AC fait une demande à l'OC afin de révoquer le certificat de l'AC et le cas échéant en générer un nouveau.

Composante OC

L'OC dispose de clés pour son personnel habilité à administrer les ressources informatiques ainsi qu'à procéder aux révocations d'urgence.

En cas de compromission d'un de ces clés, l'OC en informe l'AC et procède à la révocation et cas échéant en générer un nouveau.

V.7.4. CAPACITES DE CONTINUITE D'ACTIVITE SUITE A 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 (cf. chapitre V.7.2).

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 AE
Lorsqu'une AE cesse son activité, l'AE en informe l'AC suffisamment tôt pour que les activités et fonctions remplies par l'AE puissent être transférées à une autre AE sans incidence sur les certificats émis par l'AE.

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'AE : dossier de demande de certificats, courriers divers,…
  - transfert des fonctions assurées par l'AE : révocation, génération, …
  - la communication vers les porteurs et autres composantes de l'IGC,
  - la communication vers les utilisateurs de certificats,
  - la révocation des certificats du personnel habilité.
- Communiquer le plan d'actions au contact identifié sur le site http://www.references.modernisation.gouv.fr, à la DGME et l'ANSSI et de tout changement pendant le déroulement du transfert.

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 assurer 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 porteurs et utilisateurs de certificats,

- Communiquer le plan d'actions au contact identifié sur le site http://www.references.modernisation.gouv.fr, à la DGME et l'ANSSI 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 et/ou porteurs 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 SECURITE TECHNIQUES

VI.1. GENERATION ET INSTALLATION DE BI-CLES

VI.1.1. GENERATION DES BI-CLES

VI.1.1.1. Clés d'AC

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

Les clés de signature d'AC CERTEUROPE 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 sont générées dans le module cryptographique de l'AC Certeurope Qualifiée 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 le SCCD par l'AE. La protection du bi-clé dépend à partir de ce moment des dispositifs de protection du SCCD. Le SCCD répond aux exigences du chapitre XII.

VI.1.1.3. Clés porteurs générées par le porteur

Sans objet.

VI.1.2. TRANSMISSION DE LA CLE PRIVEE A SON PROPRIETAIRE

La clé privée est transmise à son propriétaire lors de la remise en face-à-face du SSCD lequel contient de façon protégé la clé privée du porteur.
Si le face-à-face a eu lieu au dépôt du dossier, le SSCD est transmis au Porteur par courrier recommandé avec accusé de réception.

VI.1.3. TRANSMISSION DE LA CLE PUBLIQUE A L'AC

Sans objet. Le bi-clé n'est pas généré par le porteur.

VI.1.4. TRANSMISSION DE LA CLE 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.
La DPC précise les modalités de l'accès au certificat de l'AC.

VI.1.5. TAILLES DES CLES

Les clés RSA des Porteurs 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 est de 2048 bits.

VI.1.6. VERIFICATION DE LA GENERATION DES PARAMETRES DES BI-CLES ET DE LEUR QUALITE

Les SSCD des Porteurs utilisent des paramètres standards ou normalisés pour garantir l'aspect aléatoire de la génération des bi-clés.

Les SSCD des Porteurs vérifient la qualité des bi-clés qu'ils génèrent.

Le bi-clé de l'AC (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 CLE

L'utilisation de la clé privée de l'AC CERTEUROPE et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (cf. chapitre I.4.1.2 et document [PROFILS]).
L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée aux services d'authentification et de signature (cf. chapitres I.4.1.1, IV.5 et le document [PROFILS]).

VI.2. MESURE DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LE MODULES CRYPTOGRAPHIQUES

VI.2.1. STANDARDS ET MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

VI.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en oeuvre des ses clés de signature sont des modules cryptographiques 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. Dispositifs d'authentification et de signature des porteurs (SSCD)

L'AC CERTEUROPE fournit le SSCD au porteur qui est responsable de la confidentialité de ses données d'activation.
Les SSCD des porteurs, pour la mise en œuvre de leurs clés privées d'authentification et de signature, sont qualifiés au minimum au niveau standard (Cf. chapitre XII).

VI.2.2. CONTROLE DE LA CLE PRIVEE 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. SEQUESTRE DE LA CLE PRIVEE.

L'AC CERTEUROPE n'autorise pas le séquestre ni des clés privées de l'AC ni des clés privées des porteurs.

VI.2.4. COPIE DE SECOURS DE LA CLE PRIVEE

Les clés privées des porteurs ne font l'objet d'aucune copie de secours par l'AC.

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.
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 CLE PRIVEE

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

Les clés privées des porteurs ne sont pas archivées ni par l'AC ni par aucune des composantes de l'IGC.

VI.2.6. TRANSFERT DE LA CLE PRIVEE VERS / DEPUIS LE MODULE CRYPTOGRAPHIQUE

Les privées des porteurs ne sont jamais transférées, elles sont générées dans le SSCD sans pouvoir être exportées.

Pour les clés privées d'AC, tout transfert se fera sous forme chiffrée, conformément aux exigences du chapitre VI.2.4.

VI.2.7. STOCKAGE DE LA CLE PRIVEE DANS UN MODULE CRYPTOGRAPHIQUE

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

VI.2.8. METHODE D'ACTIVATION DE LA CLE PRIVEE

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'un porteur nécessite la saisie du code PIN du SSCD, sous le contrôle exclusif du porteur.et permet de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.9. METHODE DE DESACTIVATION DE LA CLE PRIVEE

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 de la clé privée d'un porteur nécessite la saisie du code PIN du SSCD, sous le contrôle exclusif du porteur.

VI.2.10. METHODE DE DESTRUCTION DES CLES PRIVEES

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

En fin de vie de la clé privée d'un porteur, la destruction de cette clé privée ne peut être effectuée qu'à partir du SSCD.

VI.2.11. NIVEAU D'EVALUATION SECURITE DU MODULE CRYPTOGRAPHIQUE

Les modules cryptographiques de l'AC sont évalués au niveau EAL4+ correspondant à l'usage visé, tel que précisé au chapitre XI ci-dessous.
Les SSCD des porteurs sont évalués au niveau EAL4+ correspondant à l'usage visé, tel que précisé au chapitre XII ci-dessous.

VI.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES

VI.3.1. ARCHIVAGE DES CLES PUBLIQUES

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

VI.3.2. DUREE DE VIE DES BI-CLES ET DES CERTIFICATS

La durée de vie des bi-clés et des certificats porteurs fournis dans le cadre de l'AC CERTEUROPE est de 3 ans non renouvelables.

La durée de vie de la bi-clé et du certificat de l'AC CERTEUROPE est de 10 ans.

VI.4. DONNEES D'ACTIVATION

VI.4.1. GENERATION ET INSTALLATION DES DONNEES 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'IGC 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

Les SSCD sont fournis aux porteurs et sont protégés par un code d'activation (code PIN). Le code PIN est défini par l'AC de façon aléatoire. La longueur du code est de 6 chiffres. Ce code PIN est transmis directement au porteur le lendemain de la génération.

VI.4.2. PROTECTION DES DONNEES 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

Les données d'activation des SSCD des porteurs générées par l'AC sont protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs.

Les données d'activation sauvegardées par l'AC, doivent être protégées en intégrité et en confidentialité.

VI.4.3. AUTRES ASPECTS LIES AUX DONNEES D'ACTIVATION

L'AC ne conserve pas les codes d'activation des Porteurs au delà de un mois après leur envoi par courrier.

VI.5. MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

VI.5.1. EXIGENCES DE SECURITE TECHNIQUE SPECIFIQUES AUX SYSTEMES INFORMATIQUES

Les postes de travail des composantes de l'ICP nécessitent un niveau de sécurité optimal, ce niveau est défini dans la DPC 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'EVALUATION SECURITE DES SYSTEMES INFORMATIQUES

Sans objet.

VI.6. MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

VI.6.1. MESURES DE SECURITES LIEES AU DEVELOPPEMENT DES SYSTEMES

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 LIEES A LA GESTION DE LA SECURITE.

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'EVALUATION SECURITE DU CYCLE DE VIE DES SYSTEMES

Sans objet.

VI.7. MESURES DE SECURITE RESEAU

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 / SYSTEME 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 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	Sha1RSA = 1.3.14.3.2.29		Identifiant de l'algorithme de signature de l'AC
Emetteur	/C=FR /O=Certeurope /OU=0002 434202180 /CN=CERTEUROPE ADVANCED CA V3		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 CERTEUROPE)		Dates et heures d'activation et d'expiration du Certificat
Valide jusqu'au	Valide jusqu'au x+ 3 ans (au plus tard à la date de fin de vie de l'AC CERTEUROPE)		
Objet	E = jean-claude.dupont@societeaaa.fr 1.2.250.1.105.20.1 = Identifiant AE Numéro de série = c36f37bc6fc9315651ad5426bb437f77d841c888 CN = Jean-Claude DUPONT OU = 0002 243111589 O = Société AAA C = FR		Nom distinctif de l'entité identifiée
Clé publique	RSA(2048 Bits)		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=End Entity Path Length Constraint=None		
Autre Nom de l'objet	Nom RFC822= jean-claude.dupont@societeaaa.fr		
Point de distribution de la LCR	CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://lcr1.certeurope.fr/CN=CERTEUROPE ADVANCED CA V3, OU=0002 434202180, O=Certeurope, C=FR?CertificateRevocationList URL=ldap://lcr2.certeurope.fr/CN=CERTEUROPE ADVANCED CA V3, OU=0002 434202180, O=Certeurope, C=FR?CertificateRevocationList URL= http://www.certeurope.fr/reference/certeurope_v3.crl		
Certificate Policies	Certificate Policy: PolicyIdentifier=1.2.250.1.105.9.1.1.2 Policy Qualifier Info: Policy Qualifier Id= Qualifier=	OBJECT IDENTIFIER ' OBJECT IDENTIFIER cps http://www.certeurope.fr/reference/pc_certeurope_v3_v1.2.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		Champ d'octets caractérisant le Certificat de l'AC ayant signé le Certificat

VII.2. PROFIL DE LCR

VII.2.1. CHAMPS DES LCR

Les LCR de l'AC CERTEUROPE contiennent les champs suivants :

- Version : la version de la LCR. 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 ;
- ThisUpdate : date de génération de la LCR ;
- NextUpdate : prochaine date à laquelle cette LCR 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 LCR.

VII.2.2. EXTENSIONS DES LCR

Les LCR de l'AC CERTEUROPE comportent deux extensions :

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

VIII. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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. FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

L'AC CERTEUROPE a fait procéder à un audit de conformité du fonctionnement de son IGC par LSTI, agréé COFRAC. Elle fera procéder tous les deux ans à des audits de conformité par un organisme extérieur accrédité par le COFRAC. Par ailleurs, l'AC procèdera à un contrôle de conformité des autorités d'enregistrement déléguées.

VIII.2. IDENTITES / QUALIFICATIONS DES EVALUATEURS

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 EVALUATEURS ET ENTITES EVALUEES

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 EVALUATIONS

Les contrôles périodiques effectués par un organisme extérieur accrédité par le COFRAC 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 oeuvre, etc.).

VIII.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

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 RESULTATS

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 PROBLEMATIQUES METIERS ET LEGALES

IX.1. TARIFS

IX.1.1. TARIFS POUR LA FOURNITURE ET LE RENOUVELLEMENT DE CERTIFICATS

Voir les conditions particulières du contrat d'abonnement.

IX.1.2. TARIFS POUR ACCEDER AUX CERTIFICATS

Sans objet

IX.1.3. TARIFS POUR ACCEDER AUX INFORMATIONS D'ETAT ET DE REVOCATION DES CERTIFICATS

Sans objet.

IX.1.4. TARIFS POUR D'AUTRES SERVICES

Sans objet.

IX.1.5. POLITIQUE DE REMBOURSEMENT

Sans objet.

IX.2. RESPONSABILITE FINANCIERE

IX.2.1. COUVERTURE PAR LES ASSURANCES

L'AC CERTEUROPE 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 GENERALI France sous le numéro de police 56478516.

IX.2.2. AUTRES RESSOURCES

Sans objet.

IX.2.3. COUVERTURE ET GARANTIE CONCERNANT LES ENTITES UTILISATRICES

Sans objet.

IX.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

IX.3.1. PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Les informations suivantes sont considérées comme confidentielles :

– les clés privées associées aux Certificats ;

– les Codes PIN pour les Porteurs ;
– les données d'identification ou autres informations personnelles du Porteur contenues dans son certificat, sauf
  • si le Porteur a donné explicitement son consentement préalablement à la publication du Certificat ;
  • si leur publication a été demandée sur décision judiciaire ou administrative ;
– les causes de révocations des Certificats ;
– les journaux d'événements des composantes de l'ICP CERTEUROPE ;
– le dossier de demande de certificat du Porteur, et notamment les données personnelles (à l'exception des informations à caractère personnel contenues dans les Certificats) ;
– 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 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 spécifiques, liées à la politique de confidentialité, respectant les exigences du RGS 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 PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Sans objet.

IX.3.3. RESPONSABILITES 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 DONNEES PERSONNELLES

IX.4.1. POLITIQUE DE PROTECTION DES DONNEES 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 A CARACTERE PERSONNEL

Pour l'AC CERTEUROPE, les informations à caractère personnel sont les informations nominatives du porteur et 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 A CARACTERE NON PERSONNEL

Sans objet.

IX.4.4. RESPONSABILITE EN TERMES DE PROTECTION DES DONNEES PERSONNELLES

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

IX.4.5. NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES

Le porteur est averti de l'utilisation faite par l'AC de ces données personnelles, à l'occasion de la phase d'acceptation des conditions d'usage lors de l'enregistrement. Il signe personnellement ces conditions d'usage, valant acceptation et consentement.

IX.4.6. CONDITIONS DE DIVULGATION D'INFORMATIONS PERSONNELLES AUX AUTORITES 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 PROPRIETE 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. INTERPRETATIONS 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 Entreprises et Porteurs de Certificats ;
- 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. AUTORITES DE CERTIFICATION

L'AC CERTEUROPE 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 oeuvre 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 oeuvre. Elle élabore sa DPC en fonction de cette analyse.
– Mettre en oeuvre 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 oeuvre 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 et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats.

L'AC CERTEUROPE 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 ;
- s'assurer que ses Porteurs connaissent leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des Certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'ICP.

La relation entre un Porteur et l'AC CERTEUROPE est formalisée par un document précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

IX.6.2. SERVICE D'ENREGISTREMENT

Le service d'enregistrement est représenté par l'AE.

Lorsque l'AE est saisie d'une demande de Certificat, elle doit :

– vérifier avec un soin raisonnable l'apparence de conformité et la cohérence des pièces justificatives ainsi que l'exactitude des mentions qui établissent l'identité du Porteur et de l'Entreprise selon les procédures ;

  Note : L'AE peut s'appuyer sur un MC désigné et placé sous la responsabilité de l'entité cliente pour effectuer tout ou partie des opérations de vérification des informations (cf. chapitre I.3.5.2). Dans ce cas, l'AE doit s'assurer que les demandes sont complètes et exactes et effectuées par un MC dûment autorisé.

– déclencher la génération du bi-clé du Porteur sur un SSCD vierge.
– transmettre la demande de certificat au service de génération des certificats.
– transmettre les SSCD aux porteurs ;

  Note : L'AE ne peut pas utiliser le certificat du Porteur car le code d'activation du SSCD n'est pas connu de l'AE.

Lorsque l'AE est saisie d'une demande de révocation de Certificat, elle s'engage à :
vérifier avec un soin raisonnable l'apparence de conformité et la cohérence de l'origine de la demande,
mettre en œuvre les moyens permettant de traiter la demande de révocation,

L'AE doit archiver toutes les pièces du dossier d'enregistrement des porteurs et de demandes de révocation (sous forme électronique et/ou papier) suivant les modalités décrites dans cette PC et éventuellement conformément aux procédures mises en œuvre de manière dérogatoire.

Seule l'AC CERTEUROPE peut mettre en cause la responsabilité de l'AE, ce qui exclut explicitement tout engagement de l'AE envers les Entreprises clientes, les Porteurs et les utilisateurs finaux.

IX.6.3. PORTEURS DE CERTIFICATS

Le porteur a le devoir de :

- communiquer des informations exactes lors de la demande de certificat ;
- informer l'AC ou l'AE CERTEUROPE en cas de modifications de ces informations ;
- protéger sa clé privée par des moyens appropriés à l'environnement dans lequel se trouve cette clé, contre la perte, la divulgation, la compromission, la modification ou l'usage non autorisé ;

- définir son code de révocation. Ce code doit impérativement être défini dès réception du code PIN par le Porteur afin de permettre à celui-ci de demander une révocation d'urgence de son certificat. La procédure à suivre pour la définition est indiquée dans le courrier accompagnant le code PIN. Dans le cas où le Porteur ne définirait pas ce code de révocation, la révocation d'urgence ne sera pas possible.
- protéger son code PIN et son code de révocation d'urgence ;
- transmettre son code de révocation d'urgence à son MC lorsque celui-ci existe.
- respecter les conditions d'utilisation de sa clé privée et du Certificat correspondant ;
- informer sans délai son MC, l'AE ou l'AC CERTEUROPE en cas de compromission ou de soupçon de compromission de sa clé privée.

La relation entre le Porteur et l'AC CERTEUROPE est formalisée par un engagement contractuel du Porteur.

IX.6.4. 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 émettrice du Certificat ainsi que celle de l'AC Certeurope Root CA 2 ;
– 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.6.5. AUTRES PARTICIPANTS

Sans objet.

IX.7. LIMITE DE GARANTIE

Sans objet

IX.8. LIMITE DE RESPONSABILITE

Sans objet

IX.9. INDEMNITES

Sans objet

IX.10. DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

IX.10.1. DUREE DE VALIDITE

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

IX.10.2. FIN ANTICIPEE DE VALIDITE

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 VALIDITE 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 :

- au plus tard un mois avant le début de l'opération, 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.
- au plus tard un mois après la fin de l'opération, informera l'organisme de qualification.

IX.12. AMENDEMENTS A LA PC

IX.12.1. PROCEDURES D'AMENDEMENTS

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

IX.12.2. MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

Sans objet.

IX.12.3. CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) se traduit par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.
Un système de version permet d'évaluer le niveau d'évolution :majeure ou mineure (ex : I.2). Le premier chiffre change lorsqu'une évolution majeure a eu lieu et le deuxième pour une évolution mineure.

IX.13. DISPOSITIONS CONCERNANT LA RESOLUTION 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 COMPETENTES

Cf. les conditions générales d'abonnement.

IX.15. CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Cf. les conditions générales d'abonnement.

IX.16. DISPOSITIONS DIVERSES

IX.16.1. ACCORD GLOBAL

Sans objet.

IX.16.2. TRANSFERT D'ACTIVITES

Cf. chapitre V.8

IX.16.3. CONSEQUENCE 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 CITES EN REFERENCE

X.1. REGLEMENTATION

- 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 V2.3]		PC Type du référentiel RGS
[PROFILS]	V2.3	RGS – Politiques de Certification Types – Profils de Certificats, de LCR et OCSP et algorithmes cryptographiques
[ETSI_CERT].		
[RFC3647]		
[RFC3739]		
[LSTI_OSC]	8031 v1.0	Contrat de qualification selon le RGSd'un prestataire de service de confiance (N°8031)
[CERT_PS]		Certeurope – Politique de sécurité

XI. ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

XI.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE

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 :

- 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
- 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].

XII. ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF D'AUTHENTIFICATION ET DE SIGNATURE (SSCD)

XII.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le dispositif d'authentification et de signature, utilisé par le porteur pour stocker et mettre en oeuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- si la bi-clé d'authentification et de signature du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une authentification ou une signature qui ne peuvent être falsifiées sans la connaissance de la clé privée ;
- assurer la fonction d'authentification ou de signature pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- - permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Nota - Les dispositifs matériels sont susceptibles de respecter ces exigences. Notamment, Les spécifications techniques définies dans le socle commun [Socle_IAS] (Identification, Authentification, Signature) prennent en compte l'ensemble de ces exigences de sécurité. Une carte à puce respectant les exigences du socle commun, sous réserve de certification au niveau approprié (cf. chapitre suivant) répondra donc aux exigences de sécurité listées ci-dessus.

XII.2. EXIGENCES SUR LA CERTIFICATION

Le dispositif d'authentification et de signature utilisé par le porteur doit, dans les conditions prévues par le décret 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 XII.1 ci-dessus par le Premier ministre.
La certification doit permettre de démontrer une assurance moyenne que le dispositif d'authentification et de signature répond bien à ces exigences (équivalent à un niveau au minimum égal à EAL2+ des critères communs avec une résistance élevée des mécanismes) et déboucher sur une qualification de niveau standard [QUALIF_STD].

XIII. ANNEXE 4 : LISTES DES APPLICATIONS UTILISATRICES AUTORISEES

Les certificats CERTEUROPE sont utilisables :

- Pour l'authentification et la signature électronique dans le cadre des télé procédures de l'Administration, telles que les déclarations fiscales et sociales, référencées pour un niveau de risque inférieur ou égal au référentiel RGS**.
- Pour la sécurisation des messageries des porteurs : authentification et signature d'e-mail, entre les porteurs et leurs destinataires ;
- Pour la sécurisation des transactions entre la Banque et l'Entreprise sur Internet (authentification et signature).

  Les conditions d'accès à ces services font l'objet de la signature d'un abonnement ou contrat auprès de CertEurope.