POLITIQUE DE CERTIFICATION

Autorité de certification

« CERTEUROPE ADVANCED CA V4 »
Authentification serveur

Identification (OID) :
Authentification Serveur SSL/TLS Niveau * : 1.2.250.1.105.18.1.1.0
Authentification Serveur SSL/TLS Niveau ** : 1.2.250.1.105.18.3.1.0
Authentification Serveur Client * : 1.2.250.1.105.18.4.1.0

Version : 1.0
Mise à jour : 01
Date de création : 03 décembre 2012
Dernière MAJ : 22 novembre 2013
Etat du document : Officiel
Rédigé par : CertEurope
Vérifié par : Comité PKI
Approuvé par : Comité PKI

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

MODIFICATIONS			
Date	Etat	Version	Commentaires
03/12/2012	Officiel	1.0	
22/11/2013	Officiel	1.0 Mise à jour 01	Mise à la nouvelle charte graphique Prise en compte niveau ** et ajout du profil Authentification serveur client niveau *

SOMMAIRE

1. Introduction

1.1. Présentation générale

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 v2.3 du Référentiel Général de Sécurité v1.0, pour un référencement pour les profil s « Authentification Serveur SSL/TLS », aux niveaux * et ** et le profil « Authentification Serveur Client », au niveau *.
Les exigences spécifiques à l'un ou à l'autre de ces types de serveurs, lorsqu'elles existent, sont clairement identifiées en faisant précéder le paragraphe concerné respectivement par [SERVEUR-SERVEUR] ou [SERVEUR-CLIENT].

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.

1.2. Identification du document

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

La présente PC est identifiée par les OID suivants :

- Authentification serveur SSL/TLS niveau * : 1.2.250.1.105.18.1.1.0
- Authentification serveur SSL/TLS niveau ** : 1.2.250.1.105.18.3.1.0
- Authentification serveur-client niveau * : 1.2.250.1.105.18.4.1.0

La Déclaration des Pratiques de Certification correspondante est référencée par l'OID 1.2.250.1.105.18.2.1.1

Les OID sont composés de la façon suivante :

- Iso (1)
  - member-body (2)
    - fr (250)
      - type-org (1)
        - CertEurope (105)

- CERTEUROPE ADVANCED CA V4 – Authentification Serveur (18)
  - Profils (1), (3), (4)
    - Version majeure (1)
      - Version mineure (0)

1.3. Entités intervenant dans l'IGC

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

1.3.1. Autorités de certification

L'autorité à laquelle les utilisateurs des services de certification accordent leur confiance pour la création et l'émission de certificats est appelée Autorité de Certification et notée dans le document AC.
Une AC est un Prestataire de Services de Certification Electronique (PSCE) qui délivre des certificats.

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 ledit certificat 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 générer le certificat d'authentification serveur suite à une vérification préalable.
  - **Autorité d'Enregistrement Déléguée (AED) :** fonction qui consiste à transmettre le certificat au responsable du certificat d'authentification serveur (RCAS) et le cas échéant à procéder à l'authentification du futur RCAS.
- **Service d'enregistrement** : vérifie les informations d'identification du RCAS 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 RCAS 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 des serveurs.
- **Service de fourniture de code d'activation au RCAS**
- Ce service remet au RCAS le code d'activation du certificat.
- **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 RCAS** : assiste les RCAS 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 Service de Certification Electronique C@rteurope.
- **Responsable du Certificat d'authentification serveur Serveur (RCAS)** - La personne physique responsable du certificat d'authentification serveur, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le 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 RCAS et des serveurs informatiques de cette entité (il assure notamment le face-à-face pour l'identification des RCAS 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 serveur auquel le certificat est rattaché, ou pour établir une clé de session.
- **Personne autorisée** - Il s'agit d'une personne autre que le RCAS 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 RCAS (demande de révocation, de renouvellement, …).Typiquement, dans une entreprise, il peut s'agir d'un responsable hiérarchique du RCAS 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.

1.3.2. Autorités d'enregistrement

L'Autorité d'Enregistrement (AE) est une composante du PSCE ayant en charge les services suivants tels que définis au §1.3.1 :

- service d'enregistrement,
- service de fourniture de dispositif au RCAS,
- 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 RCAS ou à son mandataire (cf. §1.3.1).

1.3.3. Responsables de Certificats d'authentification serveur

Dans le cadre de la présente PC, un RCAS est une personne physique qui est responsable de l'utilisation du certificat du serveur informatique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat. Le RCAS a un lien contractuel / hiérarchique / réglementaire avec cette entité.
Le RCAS respecte les conditions qui lui incombent définies dans la présente PC.
A noter que le certificat étant attaché au serveur informatique et non au RCAS, ce dernier peut être amené à changer en cours de validité du certificat : départ du RCAS de l'entité, changement d'affectation et de responsabilité au sein de l'entité, etc.
L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RCAS de ses fonctions et lui désigner un successeur. L'AC révoquera un certificat d'authentification serveur pour lequel il n'y a plus de RCAS explicitement identifié.

1.3.4. Les utilisateurs de certificat

L'utilisateur de certificat, également nommé tiers utilisateur, fait confiance aux certificats délivrés par l'AC et/ou à des signatures numériques vérifiées à l'aide de ce certificat. L'utilisateur peut être :

- Un agent (personne physique) destinataire de données signées par un serveur informatique et qui utilise un certificat et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat du serveur, afin d'établir une clé de session partagée entre son poste et le serveur. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- Un usager accédant à un serveur informatique d'une autorité administrative et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, afin d'établir une clé de session partagée entre son poste et le serveur.
- Un serveur informatique accédant à un autre serveur informatique et qui utilise un certificat et un applicatif de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, et afin d'établir une clé de session partagée entre les deux serveurs.

1.3.5. Autres participants

1.3.5.1. Composantes de l'IGC

Voir chapitre cf. §1.3.1.

1.3.5.2. Mandataire de certification

Voir chapitre cf. §1.3.1.

1.3.5.3. Opérateur de Certification

L'Opérateur de Certification (OC) est une composante du PSCE ayant en charge les services suivants tels que définis au §1.3.1 :

- service de génération de certificats,
- service de publication et diffusion,
- service de fourniture de code d'activation au RCAS,
- service de gestion des révocations d'urgence,
- service d'information sur l'état des certificats,
- service d'assistance aux RCAS.

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

1.4. Usage des certificats

1.4.1. Domaine d'utilisation applicables

1.4.1.1. Bi-clés et certificats du serveur

La présente PC traite des bi-clés et des certificats à destination de serveurs informatiques, afin que ces serveurs puissent être authentifiés dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS, avec les catégories d'utilisateurs de certificats identifiées au chapitre 1.3.4 ci-dessus et établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

L'établissement de la clé de session se fait par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique par la clé publique du serveur).
Les usages des certificats d'authentification serveur sont donc :

- établissement d'une session sécurisée entre un serveur d'une autorité administrative et un usager,
- établissement d'une session sécurisée entre un serveur et un agent,
- établissement d'une session sécurisée entre deux serveurs.

1.4.1.2. 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.

1.4.2. Domaine d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5 ci-dessous. L'AC doit respecter ces restrictions et imposer leur respect par ses RCAS 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 4.

1.5. Gestion de la PC

1.5.1. Entité gérant la PC

1.5.1.1. Organisme responsable

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

CERTEUROPE
26, rue du Faubourg Poissonnière, 75010 Paris
FRANCE

1.5.1.2. Personne physique responsable

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

1.5.2. 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 – 26, rue du Faubourg Poissonnière – 75010 Paris
- Par e-mail à l'adresse : info@certeurope.fr
- Par téléphone au numéro : 01.45.26.72.00

1.5.3. Entité déterminant la conformité de la DPC à la PC

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

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

La conformité de la DPC avec la PC est approuvée par le Comité PKI de CertEurope en suivant le processus d'approbation mis en place. Toute nouvelle version de la DPC est publiée sans délai, conformément aux exigences du paragraphe 1.2. de la présente PC.

1.6. Définitions et acronymes

1.6.1. 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
C	Country (Pays)
CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	Common Name
CSR	Certificate Signing Request
DDS	Dossier de Souscription
DSIC/SGMAP	Direction des systèmes d'information et de communication/Secrétariat général pour la modernisation de l'action publique
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 et des Finances
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
SHA256	Secure Hash Algorithm 256
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

1.6.2. Définitions

1.6.2.1. 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 serveur.

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.

1.6.2.2. Termes spécifiques ou complétés / adaptés pour la présente PC

Applicatif de vérification d'authentification - Il s'agit de l'application mise en œuvre par l'utilisateur ou le serveur pour vérifier l'authentification d'un autre serveur et établir une session sécurisée avec ce serveur, notamment générer la clé symétrique de session et la chiffrer avec la clé publique du serveur contenue dans le certificat correspondant.

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 1 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 1.3.2

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 Type, le terme "certificat électronique" désigne uniquement un certificat délivré à un serveur informatique sous la responsabilité d'un RCAS et portant sur une bi-clé d'authentification et d'échange de clés symétriques de session, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

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.

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.

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

Dispositif de protection des clés privées - Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en oeuvre sa clé privée.

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.

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 1.3.1

Personne autorisée - Cf. chapitre 1.3.1

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 RCAS et les utilisateurs de certificats.

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 RCAS 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 utilisés 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.

Responsable du Certificat d'Authentification Serveur : cf chapitre 1.3.1

Serveur informatique - Il s'agit d'un service applicatif (disposant d'un certificat fourni par l'AC) rattaché à l'entité, (identifiée dans le certificat) détenant le nom de domaine correspondant au service ou en charge de ce service.

Service d'enregistrement : Cf. chapitre 1.3.1
Service de génération des certificats Cf. chapitre 1.3.1
Service de publication et diffusion : Cf. chapitre 1.3.1
Service de fourniture de dispositif au RCAS : Cf. chapitre 1.3.1
Service de fourniture de code d'activation au RCAS - Cf. chapitre 1.3.1
Service de gestion des révocations : Cf. chapitre 1.3.1
Service d'information sur l'état des certificats : Cf. chapitre 1.3.1
Service d'assistance aux RCAS : Cf. chapitre 1.3.1

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 1.3.1

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

2.1. Entités chargées de la mise à 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 pour la publication de la liste des certificats révoqués sont :

- copie 1 (original) : ldap://lcr1.certeurope.fr/CN=CERTEUROPE ADVANCED CA V4, OU=0002 434202180, O=Certeurope, C=FR?certificateRevocationList ;
- copie 2 : ldap://lcr2. certeurope.fr/CN=CERTEUROPE ADVANCED CA V4, OU=0002 434202180, O= Certeurope, C=FR?certificateRevocationList ;
- copie 3 : http://www.certeurope.fr/reference/certeurope_v4.crl ;

2.2. Informations devant être publiées

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_v4_auth-serveur_v1.0.pdf
- la Liste de Certificats Révoqués (LCR).
- le certificat de l'AC Certeurope Root CA 3, 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_v4/doc/dossier_auth-serveur_v4.zip à savoir :

- le Certificat de l'AC CERTEUROPE en cours de validité et son empreinte numérique (certeurope_advanced_ca_v4.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.

La DPC correspondant à cette PC ainsi que toute autre documentation pertinente pour rendre possible l'évaluation de la conformité avec sa politique de certification est disponible aux RCAS et utilisateurs de certificats sur demande.

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.

2.3. Délais et fréquences 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 serveurs et/ou de LCR correspondants.
- Pour les informations d'état des certificats, cf. § 4.9 et § 4.10.

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.

2.4. Contrôle d'accès aux informations publiées

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

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).

3. Identification et authentification

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.
Dans chaque certificat X509v3, l'AC CERTEUROPE (issuer) et le serveur informatique (subject) sont identifiés par un "Distinguished Name" DN de type X.501 conforme aux exigences définies dans le document [PROFILS].

3.1.2. Nécessité d'utilisation de noms explicites

Le contenu des champs de nom Subject et Issuer doit avoir un lien explicite avec l'entité authentifiée

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 d'identification de l'entreprise, tel que figurant sur le justificatif. Ce numéro sera précédé d'un numéro ICD de 4 caractères conformes à la norme ISO 6523, par exemple « 0002 » suivi d'un espace pour les entités de nationalité françaises. Si aucun numéro ICD conforme à la norme ISO 6523 n'est disponible, le numéro d'identification de l'entreprise ne doit pas être précédé de 4 chiffres.
  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 FQDN (« Fully Qualified Domain Name » ou nom de domaine totalement qualifié) du serveur.

Exemple de DN : C=FR, O= Société ABC, OU= 0002 123456789, OU= Site de Toulouse, CN=www.abc.fr

3.1.3. Anonymisation ou pseudonymisation des serveurs

S'agissant de certificats délivrés à des machines, les notions d'anonymisation ou de pseudonymisation sont sans objet.

3.1.4. Règles d'interprétation des différentes formes de nom

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 ;

3.1.5. Unicité 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 et du nom du service applicatif.

3.1.6. Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L.711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n°92-957 du 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.

3.2. Validation initiale de l'identité

L'enregistrement d'un serveur auquel un certificat doit être délivré se fait via l'enregistrement du RCAS correspondant.
Un RCAS peut être amené à changer en cours de validité du certificat d'authentification serveur correspondant, dans ce cas, tout nouveau RCAS doit également faire l'objet d'une procédure d'enregistrement.

L'enregistrement d'un RCAS, et du serveur informatique correspondant, peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité. 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 RCAS sans MC pour un certificat d'authentification serveur à émettre : validation par l'AE de l'identité "personne morale" de l'entité de rattachement du RCAS, de l'identité "personne physique" du futur RCAS, de son habilitation à être RCAS pour le serveur informatique considéré et pour l'entité considérée.
- [SERVEUR-SERVEUR] Validation par l'AE de de l'appartenance du nom de domaine du serveur à l'entité représentée par le RCAS.
- Enregistrement d'un nouveau RCAS sans MC pour un certificat d'authentification serveur déjà émis : validation par l'AE de l'identité "personne physique" du futur RCAS et de son habilitation à être RCAS pour le serveur informatique considéré et pour l'entité considérée.
- 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 RCAS via un MC pour un certificat d'authentification serveur à émettre ou d'un nouveau RCAS pour un certificat d'authentification serveur déjà émis : validation par le MC de l'identité "personne physique" du futur RCAS, de son habilitation à être RCAS pour le serveur informatique considéré et pour l'entité considérée, ainsi que du nom de domaine du serveur.

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre 3.2.3.

3.2.1. Méthode pour prouver la possession de la clé privée

La clé privée peut être générée par l'AC.
Dans le cas où la bi-clé n'a pas été générée par l'AC, le RCAS fournit à l'AC une CSR en vue de la génération du certificat. Cette CSR sert de preuve de la possession de la clé privée par le RCAS.

3.2.2. Validation de l'identité d'un organisme

Cf. §3.2.3.

3.2.3. Validation de l'identité d'un individu

3.2.3.1. Enregistrement d'un RCAS sans MC

L'enregistrement du futur RCAS (personne physique) représentant une entité nécessite l'identification de cette entité et l'identification de la personne physique. S'agissant d'un certificat d'authentification serveur, le RCAS doit de plus être habilité en tant que RCAS pour le serveur informatique considéré et justifier que ce serveur appartient bien à cette entité.
Le dossier d'enregistrement, déposé directement auprès de l'AE, doit comprendre :

- Une demande de certificat :
  - [SERVEUR-SERVEUR] une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le FQDN du serveur concerné par cette demande,

- [SERVEUR-CLIENT] une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du serveur concerné par cette demande,
- un mandat, daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être RCAS pour la ou les machines sur lesquelles sera déployé le certificat d'authentification serveur devant être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCAS,
- [SERVEUR-SERVEUR] une preuve de possession par l'entité du nom de domaine correspondant au FQDN du serveur,
- les conditions générales d'utilisation signées par le RCAS

- Les pièces justificatives de l'identité du RCAS :
  - Une photocopie d'un justificatif d'identité du RCAS 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 RCAS.
- 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).
  - 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 Établissements ou répertoire des métiers) ;

Pour le niveau *, l'authentification du RCAS se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. La photocopie des pièces d'identité doit être certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").

Pour le niveau **, l'authentification du RCAS par l'AE se fait lors d'un face-à-face physique.

Nota - Le RCAS est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

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.

3.2.3.2. Enregistrement d'un nouveau RCAS sans MC pour un certificat d'authentification serveur déjà émis

Dans le cas de changement d'un RCAS en cours de validité d'un certificat d'authentification serveur, le nouveau RCAS doit être enregistré en tant que tel par l'AC en remplacement de l'ancien RCAS. L'enregistrement du nouveau RCAS (personne physique) représentant une entité nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le serveur est rattaché et en tant que RCAS pour le serveur considéré.
Le dossier d'enregistrement, déposé directement auprès de l'AE, doit comprendre :

- Une demande d'enregistrement :
  - un mandat, daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être RCAS pour la ou les machines sur lesquelles sera déployé le certificat d'authentification serveur devant être délivré, en remplacement du RCAS précédent. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCAS,
  - les conditions générales d'utilisation signées par le futur RCAS.
- Les pièces justificatives de l'identité du RCAS :

- une photocopie d'un justificatif d'identité du RCAS 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 RCAS.

- 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.
  - Tout document attestant de la qualité du signataire du mandat ;

Pour le niveau *, l'authentification du RCAS se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. La photocopie des pièces d'identité doit être certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").

Pour le niveau **, l'authentification du RCAS par l'AE se fait lors d'un face-à-face physique.

Nota - Le RCAS est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

3.2.3.3. Enregistrement d'un Mandataire de Certification

Une AE est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification de façon à utiliser le dossier du MC comme référence pour les données d'identification de l'entité de tous les bénéficiaires présentés par le MC.
Le dossier d'enregistrement d'un MC, déposé directement auprès de l'AE, doit comprendre :

- un mandat, daté de moins de 3 mois, désignant le Mandataire de Certification. Ce mandat doit être signé par le représentant légal et le MC.
- un engagement signé, et daté de moins de 3 mois, du MC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs.
- un engagement signé, et daté de moins de 3 mois, du MC à signaler à l'AE son départ de l'entité.
- Les pièces justificatives de l'identité du MC :
  - la photocopie d'un justificatif d'identité du MC 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 RCAS.
- 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.
  - Tout document attestant de la qualité du signataire du mandat ;

Pour le niveau *, l'authentification du MC se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. La photocopie des d'identité doit être certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").

Pour le niveau **, l'authentification du MC par l'AE se fait lors d'un face-à-face physique.

Nota - Le MC est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent

3.2.3.4. Enregistrement d'un RCAS via un MC pour un certificat d'authentification serveur à émettre

Le dossier d'enregistrement, déposé auprès du MC, doit comprendre :

Une demande de certificat :

- [SERVEUR-SERVEUR] une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le FQDN du serveur concerné par cette demande,
- [SERVEUR-CLIENT] une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du serveur concerné par cette demande,
- un mandat, daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être RCAS pour la ou les machines sur lesquelles sera déployé le certificat d'authentification serveur devant être délivré. Ce mandat doit être signé par le MC de l'entité et co-signé, pour acceptation, par le futur RCAS,
- [SERVEUR-SERVEUR] une preuve de possession par l'entité du nom de domaine correspondant au FQDN du serveur,
- les conditions générales d'utilisation signées par le RCAS
- Les pièces justificatives de l'identité du RCAS :
    - une photocopie d'un justificatif d'identité du RCAS 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 RCAS. La photocopie doit être certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original") et est présentée au MC qui en transmet un copie à l'AE pour conservation.
- Les pièces justificatives de l'entité (Entreprise)
    - 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 Établissements ou répertoire des métiers) ;

Pour le niveau *, l'authentification du RCAS se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. La photocopie des pièces d'identité doit être certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").

Pour le niveau **, l'authentification du RCAS par le MC se fait lors d'un face-à-face physique.

Nota - Le RCAS est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Lors de la transmission des dossiers de RCAS par le MC, celui-ci doit s'authentifier auprès de l'AE : en paraphant les différentes pages du dossier de demande, ainsi qu'en signant les principales pages.

3.2.3.5. Enregistrement d'un RCAS via un MC pour un certificat d'authentification serveur déjà émis

Dans le cas de changement d'un RCAS pour un certificat d'authentification serveur en cours de validité de ce certificat, le nouveau RCAS doit être enregistré en tant que tel par l'AC en remplacement de l'ancien RCAS.

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- Une demande d'enregistrement :
    - Un mandat, daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être RCAS pour la ou les machines sur lesquelles sera déployé le certificat d'authentification serveur devant être délivré, en remplacement du RCAS précédent. Ce mandat doit être signé par le MC de l'entité et co-signé, pour acceptation, par le futur RCAS,
    - les conditions générales d'utilisation signées par le futur RCAS.

- Les pièces justificatives de l'identité du RCAS :
  - une photocopie d'un justificatif d'identité du RCAS 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 RCAS.
- Les pièces justificatives de l'entité (Entreprise) :
  - 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 Établissements ou répertoire des métiers) ;

Pour le niveau *, l'authentification du RCAS se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. La photocopie des pièces d'identité doit être certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").

Pour le niveau **, l'authentification du RCAS par le MC se fait lors d'un face-à-face physique.

Nota - Le RCAS est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Lors de la transmission des dossiers de RCAS par le MC, celui-ci doit s'authentifier auprès de l'AE : en paraphant les différentes pages du dossier de demande, ainsi qu'en signant les principales pages.

3.2.4. Informations non vérifiées du RCAS

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

3.2.5. Validation de l'autorité 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).

3.2.6. Certification croisée d'AC

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

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

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

3.3.1. Identification et validation pour un renouvellement courant

Lors du premier renouvellement, la vérification de l'identité du RCAS et des informations du serveur informatique correspondant est optionnelle.

Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le RCAS et vérifiera les informations du serveur informatique selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

3.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial.

3.4. Identification et validation d'une demande de révocation

Une demande de révocation peut être faite par courrier ou par télécopie. Elle doit alors être signée par le demandeur. 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.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de Certificat

4.1.1. Origine de la demande

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

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

La demande de certificat comporte (cf. chapitre 3.2 ci-dessus) :

- [SERVEUR-SERVEUR] le FQDN du serveur à utiliser dans le certificat (nom du service applicatif) ;
- [SERVEUR-CLIENT] le nom du serveur à utiliser dans le certificat (nom du service applicatif) ;
- les données personnelles d'identification du RCAS ;
- 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 RCAS à partir des éléments fournis par son entité, soit par son entité et signé par le RCAS. 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.

4.2. Traitement d'une demande de certificat

4.2.1. Exécution 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 :

- [SERVEUR-SERVEUR] valider le FQDN du serveur informatique auquel le certificat doit être rattaché et vérifier que le FQDN du serveur est correctement formaté et ne contient pas le caractère NUL ;
- [SERVEUR-CLIENT] vérifier que le nom du serveur est correctement formaté ;
- valider l'identité du RCAS ;
- vérifier la cohérence des justificatifs présentés ;
- s'assurer de l'existence et de la validité des pouvoirs du demandeur ;
- s'assurer que le RCAS 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. Quel que 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 1.3.1).

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

4.2.2. Acceptation ou rejet de la demande

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

4.2.3. Durée d'établissement du certificat

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

4.3. Délivrance du certificat

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

La bi-clé peut être générée par le RCAS ou par l'AC. Lorsque la demande de certificat (CSR) a été validée par l'AE, celle-ci procède à la demande de génération du certificat au service de génération de l'AC.

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.

Le délai de génération d'un certificat est de 10 jours ouvrés à compter de la remise du dossier complet. NB : il s'agit là du délai de génération et pas du délai de délivrance du certificat.

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

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

Pour le niveau *, une fois le certificat généré, le service d'enregistrement envoie celui-ci au RCAS qui est ainsi prévenu officiellement de la mise à disposition de son certificat.

Pour le niveau **, le certificat est remis impérativement lors d'un face-à-face.

4.4. Acceptation du Certificat

4.4.1. Démarche d'acceptation du certificat

Le RCAS vérifie les informations contenues dans le certificat dès sa réception et avertit l'AE en cas d'erreur. Il dispose d'un délai de seize (16) jours pour se manifester. Ce délai démarre à la remise ou à l'envoi du certificat par l'AE au RCAS ou au MC. La première utilisation du certificat vaut pour acceptation tacite de celui-ci.

4.4.2. Publication du certificat

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

4.4.3. Notification par l'AC aux autres entités de la délivrance 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 généré par l'AC ;
- 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 RCAS est averti dès la génération du certificat d'authentification serveur par e-mail ;

4.5. Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'authentification et d'établissement d'une session sécurisée : authentification du serveur, échange de la clé symétrique de session (cf. chapitre 1.4.1.1). Les RCAS doivent s'assurer du respect strict des usages autorisés des bi-clés et des certificats au niveau des serveurs. Dans le cas contraire, leur responsabilité pourrait être engagée.
L'usage autorisé de la bi-clé du serveur et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

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

Cf. chapitre précédent et chapitre 1.4. Les utilisateurs de certificats respectent strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité sera engagée.

4.6. 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 RCAS est prévenu par courrier ou par e-mail au moins un mois avant la date de fin de validité de son certificat.

4.6.1. Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2. Origine d'une demande de renouvellement

Sans objet.

4.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4. Notification au RCAS de l'établissement du nouveau certificat

Sans objet.

4.6.5. Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6. Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

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

Les bi-clés 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 serveur (cf. chapitre 4.9, notamment le chapitre 4.9.1.1 pour les différentes causes possibles de révocation).

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

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

Le RCAS 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.

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

La procédure de traitement d'une demande d'un nouveau certificat est identique à celle d'une demande initiale (Cf. chapitre 4.3.1)

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

Cf. chapitre 4.3.2.

4.7.5. Démarche d'acceptation d'un nouveau certificat
Cf. chapitre 4.4.1.

4.7.6. Publication du nouveau certificat
Cf. chapitre 4.4.2.

4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat
Cf. chapitre 4.4.3.

4.8. Modification du certificat
Nota - Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre 4.7) et autres que uniquement la modification des dates de validité (cf. chapitre 4.6).

La modification de Certificat CERTEUROPE n'est pas autorisée.

4.8.1. Causes possibles de modification d'un certificat
Sans objet.

4.8.2. Origine d'une demande de modification d'un certificat
Sans objet.

4.8.3. Procédure de traitement d'une demande de modification d'un certificat
Sans objet.

4.8.4. Notification au RCAS de l'établissement du certificat modifié
Sans objet.

4.8.5. Démarche d'acceptation du certificat modifié
Sans objet.

4.8.6. Publication du certificat modifié
Sans objet.

4.8.7. Notification par l'AC aux autres entités de la délivrance du certificat modifié
Sans objet.

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

4.9.1. Causes possibles d'une révocation
4.9.1.1. Certificats d'authentification serveur
Les cas de figures suivants peuvent être à l'origine de la révocation d'un certificat d'authentification serveur, et notamment :

- les informations du serveur figurant dans le 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 RCAS n'a pas respecté les règles d'utilisation du certificat ;
- la clé privée du serveur est suspectée de compromission, est compromise ou perdue ;
- la résiliation ou le non-paiement du contrat d'abonnement ;

- le RCAS, le MC le représentant légal de l'Entreprise en font la demande ;
- l'arrêt définitif du serveur 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.

4.9.1.2. Certificats d'une composante de l'IGC

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

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats serveurs

La révocation d'un certificat d'authentification serveur peut émaner :

- du RCAS du serveur considéré ;
- du représentant légal de l'Entreprise ;
- du Mandataire de Certification ;
- de l'AC CERTEUROPE émettrice du certificat ou de l'AE.

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

4.9.2.2. Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.
La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Révocation d'un certificat d'authentification serveur

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

La demande de révocation doit comporter au minimum :

- le prénom et nom du demandeur de la révocation ;
- [SERVEUR-SERVEUR] le FQDN du serveur utilisé dans le certificat ;
- [SERVEUR-CLIENT] le nom du serveur utilisé dans le certificat
- le DN du serveur 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 RCAS et les représentants légaux d'entreprises peuvent être réalisées auprès de l'AE CertEurope en face-à-face (pendant ses heures d'ouverture), par l'envoi d'une demande signée.

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 CertEurope par échange de documents signés.

Si la demande est recevable, l'AE CertEurope 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 RCAS 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.

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

Les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC sont 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 RCAS concernés que les certificats de leurs serveurs 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 d'authentification serveur.

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.

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

Dès que le RCAS (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.

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

4.9.5.1. Révocation d'un certificat d'authentification serveur

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

La fonction de gestion des révocations est disponible pendant les Heures ouvrées.
Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme à 2h (jours ouvrés) et une durée maximale totale d'indisponibilité par mois conforme à 16h (jours ouvrés).
Toute demande de révocation d'un certificat d'authentification serveur 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.

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

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

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

L'utilisateur d'un certificat d'authentification serveur 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.

4.9.7. Fréquence d'établissement des LCR

La fréquence de publication des LCR est de 24h.

4.9.8. Délai maximum de publication d'une LCR

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

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

Il n'y a pas de serveur OCSP.

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

Cf. chapitre 4.9.6 ci-dessus.

4.9.11. Autres moyens disponibles d'information sur les révocations.

Sans objet.

4.9.12. Exigences spécifiques en cas de révocation pour compromission de clé

Pour les certificats d'authentification serveur, aucune exigence spécifique en cas de compromission de la clé privée d'un serveur 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.
Voir chapitre 4.9.3.2.

4.9.13. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée.

4.9.14. Origine d'une demande de suspension

Sans objet.

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16. Limites de la période de suspension d'un certificat

Sans objet.

4.10. Fonction d'information sur l'état des certificats

4.10.1. Caractéristiques opérationnelles

L'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".

4.10.2. Disponibilité de la fonction

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

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4h (jours ouvrés) et une durée maximale totale d'indisponibilité par mois de 16h (jours ouvrés).

4.10.3. Dispositifs optionnels

Sans objet.

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

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et l'entité de rattachement du serveur avant la fin de validité du certificat, ce dernier est révoqué.

4.12. Séquestre de clé et recouvrement

L'AC interdit le séquestre des clés privées des serveurs.

4.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5. Mesures de sécurité non techniques

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.

5.1. Mesures de sécurité 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_PSSI].

5.1.1. Situation géographique et construction des sites

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

5.1.2. Accès 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.

5.1.3. Alimentation électrique et climatisation

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

5.1.4. Vulnérabilité aux dégâts 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.

5.1.5. Prévention 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.

5.1.6. 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.

5.1.7. 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.

5.1.8. 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.

5.2. Mesures de sécurité procédurales

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 :

5.2.1. Rôles de confiance

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

- **Responsable sécurité** : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. ;
- **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 œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes;
- **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 œuvre 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 / Contrôleur** : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.
- **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.

5.2.2. Nombre de personnes requises par tâches

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

5.2.3. Identification et authentification pour chaque rôle

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.

5.2.4. Rôles exigeant une séparation des attributions

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

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

5.3.1. Qualifications, compétences et habilitations requises

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

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

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

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

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

5.3.2. Procédures de vérification des antécédents

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

Ces personnels n'ont pas de condamnation de justice en contradiction avec leurs attributions. Ils devront remettre à leur employeur une copie du bulletin n°3 de leur casier judiciaire.
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).

5.3.3. Exigences en matière de formation initiale

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

5.3.4. Exigences et fréquence en matière de formation continue

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

5.3.5. Fréquence et séquence de rotation entre différentes attributions

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

5.3.6. Sanctions en cas d'actions non-autorisées

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

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

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

5.3.8. 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.

5.4. Procédures de constitution des données d'audit

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

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.

5.4.1. Type d'évènements à enregistrer

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

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

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

5.4.1.1. Evénements enregistrés par l'AE

Les évènements enregistrés par l'AE sont :

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

5.4.1.2. 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 certificats d'authentification serveur ;
- transmission des certificats aux RCAS et, selon les cas, acceptations / rejets explicites par les RCAS
- 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.

5.4.1.3. 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).

5.4.1.4. 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.

5.4.1.5. 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 ;
- es actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les RCAS,...).

5.4.2. Fréquence de traitement des journaux d'événements

Cf. chapitre 5.4.8.

5.4.3. Période de conservation des journaux d'événements

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

5.4.4. Protection des journaux d'événements

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

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

Le système de datation des évènements respecte les exigences du chapitre 6.8.

5.4.5. Procédure de sauvegarde des journaux d'évènements

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

5.4.6. Système de collecte des journaux d'évènements

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

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

Sans objet.

5.4.8. Evaluation des vulnérabilités

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

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

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

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

5.5. Archivage des données

5.5.1. Types de données à archiver

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

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

Les données à archiver sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC et DPC ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les engagements signés des MC ;

- les justificatifs d'identité des RCAS et, le cas échéant, de leur entité de rattachement ;
- les justificatifs de possession des serveurs ainsi que leurs noms;
- [SERVEUR-SERVEUR] les justificatifs de possession des noms de domaine des FQDN des serveurs ;
- les journaux d'évènements des différentes entités de l'IGC.

5.5.2. Période 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 RCAS, 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 œuvre par l'AC pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements est assurée tout au long de leur cycle de vie.

5.5.3. 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 ;

5.5.4. Procédure de sauvegarde des archives

Sans objet.

5.5.5. Exigences d'horodatage des données

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.
Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6. Système de collecte des archives

Sans objet.

5.5.7. Procédures de récupération et de vérification des archives

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

5.6. Changement de clé d'AC

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

La durée de vie des certificats d'authentification serveur 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, …).

La nouvelle bi-clé générée servira à signer les nouveaux certificats d'authentification serveur 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.

5.7. Reprise suite à compromission et sinistre

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

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

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses serveurs devient insuffisant pour son utilisation prévue restante, alors l'AC doit :

- informer tous les RCAS et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- révoquer tout certificat concerné.

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

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

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.

5.7.3. Procédures de reprise en cas de compromission de la clé privée 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.
En outre, l'AC doit au minimum respecter les engagements suivants :

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

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.

5.7.4. Capacités de continuité d'activité suite à un sinistre
Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de cette PC (cf. chapitre 5.7.2).

5.8. 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 RCAS 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 RCAS 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 RCAS des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre 3.2.3).

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.

6. Mesures de sécurité techniques

6.1. Génération et installation de bi-clés

6.1.1. Génération des bi-clés

6.1.1.1. Clés d'AC

La génération des clés de signature d'AC CERTEUROPE est effectuée dans un environnement sécurisé (cf. chapitre 5).

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 11 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 5.2.1), 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.

6.1.1.2. Clés serveur générées par l'AC

La bi-clé peut être générée par le serveur lui-même ou par l'AC.

Si la bi-clé est générée l'AC, elle l'est dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré et sous contrôle exclusif du RCAS.

6.1.1.3. Clés serveur générées au niveau du serveur

Dans le cas où la bi-clé est générée au niveau du serveur, le RCAS s'engage contractuellement à effectuer cette génération dans un dispositif répondant aux exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré.

6.1.2. Transmission de la clé privée au serveur

Sans objet. La clé privée est générée au niveau du serveur ou dans un module cryptographique sous contrôle du RCAS et n'est pas transmise.

Pour le niveau **, un face-à-face physique avec le RCAS pour vérifier son identité.

6.1.3. Transmission de la clé publique à l'AC

Si la bi-clé et générée par le service de création de cachet, la clé publique est transmise à l'AC de manière sécurisée (CSR). Son origine est authentifiée.

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

La clé publique de l'AC est téléchargeable sur le site Internet de l'AC.
L'empreinte du Certificat de la clé publique de l'AC permet d'en établir l'authenticité.
La DPC précise les modalités de l'accès au certificat de l'AC.

6.1.5. Tailles des clés

Les clés RSA des serveurs 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.

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

Les bi-clés sont générées en utilisant des paramètres standards ou normalisés pour garantir l'aspect aléatoire de la génération des bi-clés.
L'AC vérifie la qualité des bi-clés générées par les serveurs.
La bi-clé de l'AC (pour la signature de certificats et de LCR) est générée et protégée par un module cryptographique matériel. Ce module répond aux exigences du chapitre 11.
La génération ou le renouvellement de la bi-clé de l'AC par ce module nécessite la présence d'au moins 3 personnes.

6.1.7. Objectifs d'usage de la clé

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 1.4.1.2 et document [PROFILS]).
L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'authentification et d'établissement d'une session sécurisée (cf. chapitres 1.4.1.1, 4.5 et le document [PROFILS]).

6.2. Mesure de sécurité pour la protection des clés privées et pour le modules cryptographiques

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature sont des modules cryptographiques répondant aux critères communs au niveau EAL4+ et qualifiés au niveau standard par l'ANSSI. Par conséquent ils répondent aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité **.

6.2.1.2. Dispositifs de protection de clés privées des serveurs

L'AC CERTEUROPE ne fournit pas ce dispositif au RCAS. Par conséquent, le RCAS s'engage contractuellement à utiliser un dispositif, pour la mise en œuvre de la clé privée du serveur dont il est rattaché, répondant aux exigences du RGS.

6.2.2. Contrôle de la clé privée par plusieurs personnes

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

6.2.3. Séquestre de la clé privée.

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

6.2.4. Copie de secours de la clé privée

Les clés privées des serveurs 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.

6.2.5. Archivage de la clé privée

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

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

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

Les clés privées des serveurs ne sont jamais transférées, elles sont générées dans le module cryptographique conforme aux exigences du chapitre 12 ci-dessous, sans pouvoir être exportées.

Pour les clés privées d'AC, tout transfert se fera sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC sont stockées dans un module cryptographique répondant aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. 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 11 pour le niveau de sécurité considéré.

6.2.8.2. Clés privées des serveurs

Les clés privées des serveurs sont protégées dans le module cryptographique par un mot de passe sous la responsabilité du RCAS.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. 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 11 pour le niveau de sécurité considéré.

6.2.9.2. Clés privées des serveurs

La désactivation de la clé privée d'un serveur est sous le contrôle exclusif du RCAS. Ce dernier s'engage à mettre en œuvre des conditions de désactivation de la clé privée du serveur dont il est rattaché conformément aux exigences du RGS.

6.2.10. Méthode de destruction des clés privées

6.2.10.1. 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.

6.2.10.2. Clés privées des serveurs

La destruction de la clé privée d'un serveur est sous le contrôle exclusif du RCAS. Ce dernier s'engage à mettre en œuvre des conditions de destruction de la clé privée du serveur dont il est rattaché conformément aux exigences du RGS.

6.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection de clés privées

Les modules cryptographiques de l'AC sont évalués au niveau EAL4+ et qualifiés au niveau standard. Par conséquent, ils répondent aux exigences du chapitre 11 ci-dessous pour les niveaux de sécurité * et **.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

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

6.3.2. Durée de vie des Bi-clés et des Certificats

La durée de vie des bi-clés et des certificats serveurs fournies 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.

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

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

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

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

Les données d'activation ne sont pas gérées du côté de l'AC.

6.4.2. Protection des données d'activation

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

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.

6.4.2.2. Protection des données d'activation correspondant aux clés privées des serveurs

Les clés privées des serveurs sont protégées dans le module cryptographique par un mot de passe sous la responsabilité du RCAS.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les postes de travail des composantes de l'ICP nécessitent un niveau de sécurité optimal, 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.

6.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Sans objet.

6.6. Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1. Mesures de sécurités liées au développement des systèmes

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

6.6.2. Mesures liées à la gestion de la sécurité.

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

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

Sans objet.

6.7. Mesures de sécurité réseau

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

6.8. Horodatage / système de datation

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

7. Profils de certificats et de LCR

Les profils complets sont détaillés dans le document [PROFILS_CERTEUROPE] disponible sur le site Web de CertEurope à l'URL : http://www.certeurope.fr/chaine-confiance-numerique.php

8. Audit de conformité et autres évaluations

Des audits annuels de surveillance sont organisés, conformément au schéma d'accréditation. Afin d'assurer la conformité de sa PC avec sa DPC, l'AC réalise des audits internes.
La suite du présent chapitre ne traite que le contrôle de conformité de l'IGC.

8.1. Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC procède à un contrôle de conformité de cette composante. Un contrôle de conformité de l'ensemble de son IGC est réalisé par l'AC suivant la fréquence d'une fois tous les deux ans pour le niveau ** et tous les trois ans pour le niveau *.

8.2. Identités / qualifications des évaluateurs

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

8.3. Relations entre évaluateurs et entités évaluées

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

8.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants :

- "réussite",
- "échec",
- "à confirmer".

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

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

Les éventuelles non conformités détectées lors de l'audit sont classifiées en « remarque », « non-conformité non prioritaire », « non-conformité prioritaire ».

Les « remarques » et les « non conformités non prioritaire » 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 prioritaires » 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.

8.6. Communication des résultats

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

9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture et le renouvellement de certificats

Voir les conditions particulières du contrat d'abonnement.

9.1.2. Tarifs pour accéder aux certificats

Sans objet

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

Sans objet.

9.1.4. Tarifs pour d'autres services

Sans objet.

9.1.5. Politique de remboursement

Sans objet.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

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 HISCOX sous le numéro de police HA RCP0081352.

9.2.2. Autres ressources

Sans objet.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles :

- les clés privées associées aux Certificats ;
- les causes de révocations des Certificats ;
- les journaux d'événements des composantes de l'ICP CERTEUROPE ;
- le dossier de demande de certificat d'authentification serveur, et notamment les données personnelles ;
- 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.

9.3.2. Informations hors du périmètre des informations confidentielles
Sans objet.

9.3.3. Responsabilités en terme de protection des informations confidentielles
L'AC est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

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

9.4.2. Informations à caractère personnel
Pour l'AC CERTEUROPE, les informations à caractère personnel sont les informations nominatives du RCAS et du mandataire de certification, enregistrées au sein du dossier d'enregistrement. Il s'agit des informations nom / prénom / adresse / téléphone / fonction / email, Ainsi que les causes de révocation des certificats d'authentification serveur.

9.4.3. Informations à caractère non personnel
Sans objet.

9.4.4. Responsabilité en termes de protection des données personnelles
Cf. législation et réglementation en vigueur sur le territoire français.

9.4.5. Notification et consentement d'utilisation des données personnelles
Le RCAS 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.

9.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives
Cf. législation et réglementation en vigueur sur le territoire français.

9.4.7. Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5. Droits sur la propriété intellectuelle et industrielle

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.

9.6. Interprétations contractuelles et garanties

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

- protéger et garantir l'intégrité et la confidentialité de leurs clés 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 RCAS ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent, dans des conditions garantissant qualité et sécurité.

9.6.1. Autorités de certification

L'AC 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 d'authentification serveur 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 RCAS, aux utilisateurs de certificats,… qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC notamment en matière de génération des certificats, remise au RCAS, de gestion des révocations et d'information sur l'état des certificats.

- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR 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 RCAS 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 serveur donné et que le RCAS responsable du serveur a accepté le certificat, conformément au § 4.4 ;
- tenir à disposition des RCAS, 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 RCAS 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 RCAS et l'AC CERTEUROPE est formalisée par un document précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

9.6.2. 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 RCAS 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 1.3.5.2). Dans ce cas, l'AE doit s'assurer que les demandes sont complètes et exactes et effectuées par un MC dûment autorisé.
- transmettre la demande de certificat au service de génération des certificats.

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 RCAS 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 RCAS et les utilisateurs finaux.

9.6.3. RCAS

Le RCAS a le devoir de :

- communiquer des informations exactes lors de la demande ou du renouvellement du certificat ;
- informer l'AC ou l'AE CERTEUROPE en cas de modification des informations contenues dans le certificat d'authentification serveur ;
- protéger la clé privée du serveur dont il a la responsabilité 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 ;
- protéger les données d'activation de cette clé privée et, le cas échéant, les mettre en œuvre

- protéger l'accès à la base de certificats du serveur ;
- respecter les conditions d'utilisation de la clé privée du serveur 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 RCAS et l'AC CERTEUROPE est formalisée par un engagement contractuel du RCAS.

9.6.4. Utilisateurs de certificats

Les Applications utilisatrices et Utilisateurs de Certificats doivent :

- respecter l'usage pour lequel un certificat a été émis ;
- contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application
- vérifier la signature numérique de l'AC CERTEUROPE émettrice du certificat ainsi que celle de l'AC Certeurope Root CA 3 ;
- contrôler la validité des Certificats (date de validité et statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

9.6.5. Autres participants

Sans objet.

9.7. Limite de garantie

Sans objet

9.8. Limite de responsabilité

Sans objet

9.9. Indemnités

Sans objet

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

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

9.10.2. Fin anticipée de validité

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

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

Sans objet.

9.11. Notifications individuelles et communications entre les participants

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

- 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.

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

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

9.12.2. Mécanisme et période d'information sur les amendements

Sans objet.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

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

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

9.13. Dispositions concernant la résolution de conflits

Cf. les conditions générales d'abonnement. La présente PC est soumise au Droit français.
Tous différends, découlant du présent Contrat, peuvent être réglés par voie d'arbitrage si les parties au litige sont d'accord sur ce mode de règlement du conflit. Si tel est le cas, le règlement d'arbitrage est celui de l'ATA (7 rue de Madrid, 75008 PARIS - Tél : 01 44 90 17 10 - Fax : 01 44 70 01 64 – 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.

9.14. Juridictions compétentes

Cf. les conditions générales d'abonnement.

9.15. Conformité aux législations et règlementations

Cf. les conditions générales d'abonnement.

9.16. Dispositions diverses

9.16.1. Accord global

Sans objet.

9.16.2. Transfert d'activités

Cf. chapitre 5.8

9.16.3. Conséquence d'une clause non valide

Sans objet.

9.16.4. Application et renonciation

Sans objet.

9.16.5. Force majeure

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

9.17. Autres dispositions

Sans Objet.

10. Annexe 1 – Documents cités en référence

10.1. Réglementation

- Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Directive européenne 95/46/EC relative à la protection des données personnelles
- Directive européenne (1999/93/EC) relative à la signature électronique été adoptée le 13/12//1999
- Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
- Décret no 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.
- Décret no 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie dispensées de toute formalité préalable.
- Arrêté du 17 mars 1999 définissant la tome et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptographie.
- Arrêté définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fournitures d'un moyen ou d'une prestation de cryptographie, no PRMX9802730A du 13 mars 1998
- Arrêté définissant le modèle de notification préalable par le fournisseur des identités des intermédiaires utilisés pour la fourniture des moyens ou prestations de cryptographie soumis à autorisation, no PRMX9802732A du 13 mars 1998.

10.2. Documents techniques

DOCUMENTS REFERENCES		
Date	Version	Commentaires
[PC RGS V2.3]	2.3	PC Type V2.3 du référentiel RGS v1.0
[DécretRGS]		Décret n° 2010-112 du 2 février 2010
[PROFILS]	2.3	Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques
[PROFILS_CERTEUROPE]		Profils des certificats CertEurope
[ETSI_CERT]		
[RFC3647]	Novembre 2003	IETF – Internet X509 Public Key Infrastructure – Certificate Policy and Certification Practice Framework.
[CERT_PSSI]		CertEurope : Politique de Sécurité

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

11.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre 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 d'authentification serveur, 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 des serveurs 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 des serveurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des serveurs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif de protection des clés privées du serveur 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.

11.2. 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 11.1 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 élémentaire [QUALIF_STD].

12. Annexe 3 : Exigences de sécurité du dispositif de protection de clés privées

12.1. Exigences sur les objectifs de sécurité

Le dispositif de protection de clés privées, utilisé par le serveur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- si la bi-clé du serveur 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 qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, 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.

12.2. Exigences sur la certification

Le dispositif de protection des clés privées est qualifié au minimum au niveau élémentaire selon le processus décrit dans le [RGS] et être conforme aux exigences du chapitre 12.1 ci-dessus. '