CRITERE DE DIFFUSION : PUBLIC

AC Certeurope Classe 1

POLITIQUE DE CERTIFICATION

AC CERTEUROPE CLASSE 1

Identification (OID)	1.2.250.105.5.1	Version	1.0
Date de création	28/05/2008	Date de mise à jour	17/08/2008

Ce document contient 46 pages

Etat du document	Projet
Rédigé par	Daniel MAMPIONONA
Vérifié par	Frédéric FOUYET
Approuvé par	

MODIFICATIONS

Date	Etat	Version	Commentaires
18/08/2008	Officiel	V1.0	

DOCUMENTS REFERENCES

Référence	Version	Titre des documents

SOMMAIRE

I. INTRODUCTION

I.1. PRESENTATION GENERALE

Ce document constitue la Politique de Certification de l'Autorité de Certification AC CERTEUROPE CLASSE 1, c'est-à-dire l'ensemble des obligations et engagements des différents acteurs et plus particulièrement de l'AC AC CERTEUROPE CLASSE 1, concernant la délivrance de certificats numériques.

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 CLASSE 1. Contrairement à la PC, la consultation de la DPC doit faire l'objet d'une demande argumentée auprès de l'AC.

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).

I.2. IDENTIFICATION DU DOCUMENT

La présente Politique de Certification est identifiée par l'OID 1.2.250.1.105.5.1. La Déclaration des Pratiques de Certification correspondante est référencée par l'OID 1.2.250.1.105.5.2.

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

I.3. ENTITES INTERVENANT DANS L'IGC

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

I.3.1. AUTORITES DE CERTIFICATION

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

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

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

– **Service de génération des certificats** : génère et signe les certificats à partir des informations transmises par le service d'enregistrement.

- **Service de publication et diffusion** : met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.
- **Service de gestion des révocations** : traite les révocations 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.).

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

- **Porteur / Sujet** - La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.
- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur d'authentification provenant du porteur du certificat ou pour vérifier une signature électronique provenant du porteur du certificat.

I.3.2. AUTORITES D'ENREGISTREMENT

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

- service d'enregistrement,
- service de gestion des révocations.

I.3.3. OPERATEUR DE CERTIFICATION

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

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

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

I.3.4. PORTEURS DE CERTIFICATS

Dans le cadre de la présente PC, les certificats sont remis à des personnes physiques appartenant ou non à une entité (entreprise, administration, …).

Le porteur respecte les conditions qui l'incombent définies dans la présente PC.

Le porteur est responsable concernant l'utilisation de la clé privée associée au certificat à clé publique.

I.3.5. LES UTILISATEURS DE CERTIFICAT

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

I.3.6. AUTRES PARTICIPANTS

I.3.6.1. Composantes de l'IGC

La décomposition en services de l'AC est présentée ci-dessus. Les composantes de l'IGC mettant en œuvre ces services seront présentés dans la Déclaration des Pratiques de Certification (DPC) de l'AC.

I.3.6.2. Mandataire de certification

Sans d'objet.

I.4. USAGE DES CERTIFICATS

I.4.1. DOMAINE D'UTILISATION APPLICABLES

I.4.1.1. Bi-clés et certificats des porteurs

L'Autorité de Certification Certeurope Classe 1 distribue des Certificats qui peuvent être utilisés dans le cadre :

- d'applications internes à l'AC Certeurope Classe 1 ou ses composantes (AE),
- d'autres applications ayant signé un accord avec l'AC Certeurope Classe 1 ou ses composantes (AE),
- d'échange de documents signés entre diverses parties.

Cette utilisation implique en particulier l'acceptation par les gestionnaires de l'application ou les utilisateurs de l'intégralité des chapitres contenus dans cette PC.

La présente PC traite des bi-clés et des certificats à destination des catégories de porteurs identifiées au chapitre I.3.4 ci-dessus, afin que les porteurs puissent s'authentifier et signer électroniquement les documents dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées au chapitre I.3.5 ci-dessus.

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

L'AC dispose d'une seule bi-clé et le certificat correspondant est un certificat délégué (certificat signé par une AC de niveau supérieur).

Conformément au [CWA14167-1], 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'évènements, 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.

I.4.2. DOMAINE D'UTILISATION INTERDITS

La présente PC est strictement limitée aux plateformes dédiées à l'utilisation des certificat issus de l'AC CERTEUROPE CLASSE 1.

L'Autorité de Certification « AC CERTEUROPE CLASSE 1 » décline toute responsabilité dans l'usage que ferait un Porteur de ses certificats dans le cadre d'une application différente de celles visées au précédent paragraphe. En particulier, l'Autorité de Certification « AC CERTEUROPE CLASSE 1 » n'acceptera aucune plainte d'aucune sorte d'usagers ou d'utilisateurs, liés à des litiges sans rapport avec le ou les applications autorisées au précédent alinéa.

I.5. GESTION DE LA PC

I.5.1. ENTITE GERANT LA PC

L'AC AC CERTEUROPE CLASSE 1 est responsable de la validation et de la gestion de la PC.

I.5.2. POINT DE CONTACT

Organisme responsable :
La société CERTEUROPE est responsable de cette PC.
CERTEUROPE S.A.
34-36, rue de la Folie Regnault
75011 Paris
FRANCE

Contact technique :
Direction Technique
Monsieur Frédéric Fouyet
34-36, rue de la Folie Regnault
75011 Paris
FRANCE

Contact juridique :
Direction Générale
Monsieur Stéphane Drai
34-36, rue de la Folie Regnault
75011 Paris
FRANCE

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

CERTEUROPE détermine la conformité de la DPC à la PC soit directement, soit par l'intermédiaire d'experts indépendants spécialisés dans le domaine des Infrastructures à Clé Publique.

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

CERTEUROPE, par le biais de son Autorité de Politique, détermine la conformité de la DPC à la PC soit directement, soit par l'intermédiaire d'experts indépendants spécialisés dans le domaine des Infrastructures à Clé Publique.

I.6. DEFINITIONS ET ACRONYMES

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AP	Autorité de Politique
C	Country (Pays)
CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	Common Name
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DDS	Dossier de Souscription
DGME/SDAE	Direction Générale de la Modernisation de l'Etat/ Service du Développement de l'Administration Electronique
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification, ou EPC
DSA	Digital Signature Algorithm
EAR	Entité d'Audit et de Référencement
EPC	Enoncé des Pratiques de Certification, ou DPC
ETSI	European Telecommunications Standards Institute
ICP	Infrastructure à Clés Publiques
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
LDAP	Light Directory Access Protocol
MC	Mandataire de Certification
MD5	Message Digest n°5
MINEFI	Ministère de l'Économie, des Finances et de l'Industrie
O	Organisation

OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisation Unit
PC	Politique de Certification
PDS	Déclaration de divulgation d'IGC (PKI Disclosure Statement)
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adelman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSCD	Dispositif Sécurisé de Création de Signature
SHA-1	Secure Hash Algorithm One
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

I.6.1. TERMES COMMUNS A LA PRIS

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

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

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.

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

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

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

politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre I et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC.

Autorité d'enregistrement - Cf. chapitre I.3.2

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

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

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

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

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

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

Porteur - Cf. chapitre I.3.1

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

Service d'enregistrement : Cf. chapitre I.3.1
Service de génération des certificats Cf. chapitre I.3.1
Service de publication et diffusion : Cf. chapitre I.3.1
Service de gestion des révocations : Cf. chapitre I.3.1
Service d'information sur l'état des certificats : Cf. chapitre I.3.1

Utilisateur de certificat - Cf. chapitre I.3.1

II. DISPOSITIONS GENERALES

II.1. OBLIGATIONS

II.1.1. OBLIGATIONS DE L'AC

L'AC AC CERTEUROPE CLASSE 1 garantit le respect des exigences définies dans la présente PC ainsi que dans la DPC associée. Quels que soient les recours à des entités extérieures pour la mise en œuvre de son activité de certification, l'AC garantit le respect de ces exigences par chacune de ces entités.

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

– Etre une entité légale au sens de la loi française.
– Etre en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des porteurs de cette entité. Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats,… qui mettent en oeuvre ses certificats.
– S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
– Mettre en oeuvre les différentes fonctions identifiées dans sa PC notamment en matière de génération des certificats, remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
– Mettre en oeuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité.
– Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats.

II.1.2. OBLIGATIONS DE L'AE

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

– déclencher la génération du bi-clé du Porteur
– 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 selon les exigences décrites au chapitre III.3

II.1.3. OBLIGATIONS COMMUNES A TOUTES LES COMPOSANTES DE L'ICP

Les composantes de l'ICP s'engagent à :

- protéger et garantir l'intégrité et la confidentialité de leurs clés privées ;
- n'utiliser leurs clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification ;
- respecter et appliquer la PC et DPC associée au moins pour les parties leur incombant;

- se soumettre aux contrôles de conformité effectués par CERTEUROPE ou par toute autre organisme mandaté par CERTEUROPE, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- respecter les accords ou contrats qui les lient entre elles ainsi qu'aux Entreprises et Porteurs de Certificats ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent, dans des conditions garantissant qualité et sécurité.

II.1.4. OBLIGATIONS RELATIVES A LA GESTION DES CERTIFICATS

L'AC CertEurope Classe 1 s'engage à :
- tenir à disposition des Porteurs et des Utilisateurs, la liste des certificats ayant fait l'objet d'une révocation; cette liste est publiée sous la forme d'une LCR conformément au chapitre II.1.6 ;
- garantir la cohérence entre la PC et la DPC associée ;
- s'assurer que ses Porteurs soient en mesure de connaître 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.

II.1.5. OBLIGATIONS RELATIVES A L'IDENTIFICATION

Sans objet.

II.1.6. OBLIGATIONS RELATIVES A LA PUBLICATION

II.1.6.1. Entités chargées de la mise a disposition des informations

L'OC est représenté par la société CERTEUROPE.

L'OC est en charge des services de publication :
– service de publication et diffusion,
– service d'information sur l'état des certificats.

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

Les canaux utilisés sont :
– le site Web de la société CERTEUROPE : www.certeurope.fr
– Deux annuaires LDAP sur deux sites différents pour garantir une haute disponibilité

II.1.6.2. Informations devant être publiées

L'AC CertEurope Classe 1 s'engage à diffuser publiquement :
– la Politique de Certification de l'AC CERTEUROPE CLASSE 1 en cours de validité (PC);
– la Liste de Certificats Révoqués (LCR) ;
– les certificats de l'AC en cours de validité,
– les informations permettant aux utilisateurs de certificats de s'assurer de l'origine du certificat de l'AC et leur état,

– les formulaires d'enregistrement,
– les conditions générales d'utilisation,
– 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.

II.1.6.3. 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, etc.), l'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.
– Pour les certificats d'AC, ils doivent être diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants sous délai 24h.
– Pour les informations d'état des certificats, voir chapitre IV.8.

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, etc.), les systèmes doivent avoir une disponibilité de Jours ouvrés avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 8h (jours ouvrés) et une durée totale maximale d'indisponibilité par mois de 32h (jour ouvrés), ceci hors cas de force majeure.
– Pour les certificats d'AC, les systèmes doivent avoir une disponibilité de 24h/24 7j/7 avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h et une durée totale maximale d'indisponibilité par mois de 8h, ceci hors cas de force majeure.
– Pour les informations d'état des certificats, voir chapitre IV.10.

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

II.1.6.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats doit être 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) doit être strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

L'accès en modification aux systèmes de publication des autres informations doit être strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion stricte des mots de passe.

II.1.7. OBLIGATIONS RELATIVES A LA JOURNALISATION

Pour le compte de l'AC CertEurope Classe 1, l'OC enregistre tout événement relatif à son activité de certification. Ces enregistrements concernent :

- L'accès physiques aux machines de la plateforme ;
- L'accès logique aux systèmes ;
- L'accès aux applications ;
- Les opérations effectuées sur ces applications.

Certains de ces journaux font l'objet de renseignements manuels, certains sont entièrement automatisés; tous concourent à assurer l'imputabilité de toute action sur la plate-forme de certification.

II.1.8. OBLIGATIONS RELATIVES A L'ARCHIVAGE

L'AC CertEurope Classe 1 s'engage à faire archiver les journaux d'événements. L'OC met en œuvre les moyens techniques permettant de réaliser l'archivage des journaux.

Bien entendu ces archives sont disponibles en cas de nécessité (litige ou autre).

II.1.9. OBLIGATIONS RELATIVES AU SEQUESTRE

L'AC CertEurope Classe 1 ne réalise pas de fonction de séquestre.

II.1.10. OBLIGATIONS DU MANDATAIRE DE CERTIFICATION.

Sans objet.

II.1.11. OBLIGATIONS DU PORTEUR

Le Porteur a l'obligation de :

- protéger sa clé privée par des moyens appropriés à l'environnement dans lequel se trouve cette clé, contre la perte, la divulgation, la compromission, la modification ou l'usage non autorisé ;

respecter les conditions d'utilisation de sa clé privée et du Certificat correspondant ;

- informer sans délai l'AC CertEurope Classe 1 en cas de compromission ou de soupçon de compromission de sa clé privée.

II.1.12. OBLIGATIONS DES APPLICATIONS UTILISATRICES ET DES UTILISATEURS DE CERTIFICATS

Les applications utilisatrices et utilisateurs de Certificats doivent :

– respecter l'usage pour lequel un Certificat a été émis ;
– vérifier la signature numérique de l'AC CertEurope Classe 1 émettrice du Certificat ainsi que celle de l'AC Certeurope Root CA 2 ;
– contrôler la validité des Certificats (date de validité et statut de révocation).

II.2. RESPONSABILITES

II.2.1. RESPONSABILITE DE L'AC

L'AC CertEurope Classe 1 s'engage à respecter la conformité de son dispositif de gestion des Certificats et de ses procédures avec les exigences décrites dans cette PC.

L'AC CertEurope Classe 1 fait son affaire personnelle de toute conséquence dommageable résultant du non-respect du présent document par elle-même ou l'une de ses composantes.

L'AC CertEurope Classe 1 est responsable en cas de faute intentionnelle des préjudices causés à une personne physique ou morale.

Le détail des engagements pris envers les Porteurs est détaillé dans la présente PC et dans les Conditions Générales.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes.

II.2.2. RESPONSABILITE DE L'AE

Seule l'AC CertEurope Classe 1 peut mettre en cause la responsabilité de l'AE, ce qui exclut explicitement tout engagement de l'AE envers les Porteurs et les utilisateurs finaux.

II.3. RESPONSABILITE FINANCIERE

Sans objet.

II.4. PUBLICATION ET REFERENTIEL

Voir chapitre II.1.6

II.5. AUDIT DE CONFORMITE

Sans objet.

II.6. POLITIQUE DE CONFIDENTIALITE

II.6.1. TYPES D'INFORMATIONS CONSIDEREES COMME CONFIDENTIELLES

Les informations suivantes sont considérées comme confidentielles :

- les clés privées associées aux Certificats ;
- les données d'identification ou autres informations personnelles du Porteur contenues dans son certificat, sauf
  - si le Porteur a donné explicitement son consentement préalablement à la publication du Certificat ;
  - si leur publication a été demandée sur décision judiciaire ou administrative ;
- les causes de révocations des Certificats ;
- les journaux d'événements des composantes de l'ICP CERTEUROPE ;
- 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 dans les conditions fixées par dans la loi n° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

II.6.2. DIVULGATION DES CAUSES DE REVOCATION

La cause de la révocation n'est pas publiée dans la LCR.

II.6.3. REMISE SUR DEMANDE DU PROPRIETAIRE

CERTEUROPE ne remettra aucune donnée sur demande du propriétaire hormis bien entendu les informations protégées par la loi n°7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

II.6.4. DELIVRANCE AUX AUTORITES HABILITEES

L'activité de l'AC CertEurope Classe 1 s'exerce dans le cadre de la législation française, aussi sur requête d'une autorité habilitée, l'AC CertEurope Classe 1 peut être amenée à fournir certaines informations confidentielles selon la loi L90-1170.

II.7. DROITS DE PROPRIETE INTELLECTUELLE

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.

III. IDENTIFICATION ET AUTHENTIFICATION

III.1. ENREGISTREMENT INITIAL D'UN PORTEUR

III.1.1. CONVENTIONS DE NOMS

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

Dans chaque certificat X509v3 le porteur (subject) est identifié par un "Distinguished Name" DN de type X.501 est conforme aux exigences définies dans les documents [PROFILS], [RFC3739] et [ETSI_CERT].

III.1.2. NECESSITE D'UTILISATION DE NOMS EXPLICITES

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

Les pseudonymes ne sont pas autorisés.

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 « **CommonName** » :
  Ce champ contient le prénom et nom du porteur. Le Porteur est libre de donner un autre nom tel que celui présent dans son état civil.
– Dans le champ « **Organization** » la raison sociale de l'entreprise (optionnel) ;
– dans le champ « **Title** » : la qualité du Porteur (optionnel);
– dans le champ « **Email** » : l'adresse email du Porteur ;

Tous ces champs sont purement à titre informatif et ne donnent lieu à aucune vérification avancée.

Exemple : DN = {C=FR, T=Gérant, O= SOCIETE X, CN=Jean-Claude DUPONT, Email=jean-claude.dupont@societex.fr}

III.1.3. UNICITE DES NOMS

L'unicité d'un Certificat est établie par l'unicité de son numéro de série.

III.1.4. PROCEDURE DE RESOLUTION DE LITIGE SUR DECLARATION DE NOM

L'AC s'engage quant à l'unicité des noms de ses Porteurs, conformément au chapitre III.1.33 et proposera des procédures de résolution amiables des litiges.

III.1.5. VALIDATION INITIALE DE L'IDENTITE

L'enregistrement d'un porteur se fait directement auprès de l'AE.

L'AE délivre le certificat après réception des informations d'identification :

- déclarées par le futur porteur, personne physique (par exemple lors d'un processus d'enregistrement en ligne),

- déclarées par le porteur et vérifiées par l'AE,
- extraites d'une base de données maîtrisée par l'AE.

III.1.6. ENREGISTREMENT D'UN PORTEUR

L'AE délivre le certificat après réception des informations d'identification du porteur et suivant une procédure qui lui est propre.

III.2. ENREGISTREMENT D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

III.2.1. RENOUVELLEMENT DES CLES HORS REVOCATION

Sans objet.

III.2.2. RENOUVELLEMENT DES CLES APRES REVOCATION

Sans objet.

III.2.3. RENOUVELLEMENT DES CLES AVANT EXPIRATION

Sans objet.

III.3. ENREGISTREMENT D'UNE DEMANDE DE REVOCATION

Une demande de révocation peut être faite par le service de gestion des révocations.

IV. BESOINS OPERATIONNELS

IV.1. DEMANDE DE CERTIFICAT

IV.1.1. ORIGINE DE LA DEMANDE

Une demande de certificat ne peut être demandée que par le futur Porteur.

IV.1.2. ENREGISTREMENT D'UNE DEMANDE

Les informations suivantes font partie de la demande de certificat :

- le nom du porteur
- le prénom du porteur
- l'entreprise du porteur (optionnel)
- l'adresse de courrier électronique du porteur
- le cas échéant, sa qualité

IV.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

Les identités « personne physique » sont vérifiées conformément aux exigences du chapitre III.1.5.

IV.2.2. DUREE D'ETABLISSEMENT DU CERTIFICAT

La durée d'établissement d'un certificat varie suivant l'AE de 1 an à 3 ans.

IV.3. DELIVRANCE DU CERTIFICAT

IV.3.1. DELIVRANCE EN LIGNE

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

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 déclenche le processus de génération du certificat.

IV.3.2. DELIVRANCE DU CERTIFICAT PAR L'AE

L'AE a la possibilité de générer les certificats et les clés privées du porteur sous forme PKCS12 et de les remettre au porteur.

IV.4. ACCEPTATION DU CERTIFICAT

L'acceptation du certificat est tacite à compter de la date d'envoi du certificat au porteur suite à la réception des informations d'identification déclarées par le futur porteur.

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

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

L'utilisation de la clé privée du Porteur et du certificat associé est limitée au service de signature et à l'authentification. Les Porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

IV.5.2. UTILISATION DE LA CLE PUBLIQUE ET DU CERTIFICAT PAR LE PORTEUR

Les bi-clés associés aux certificats de signature générés par l'AC CertEurope Classe 1 ne sont utilisables que pour la signature et la non répudiation. Ces usages sont précisés dans le champ « Utilisation de la clé » des certificats CERTEUROPE CLASSE 1 ; ce champ a donc les valeurs « **Signature** » et « **non Répudiation »**.

IV.6. RENOUVELLEMENT D'UN CERTIFICAT

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

L'AC CERTEUROPE CLASSE 1 ne gère pas le renouvellement de certificat.

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

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

IV.7.1. CAUSES POSSIBLES DE CHANGEMENT D'UNE BI-CLE

Sans objet.

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

Le déclenchement d'un nouveau certificat du Porteur est à l'initiative du Porteur.

IV.7.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Sans objet.

IV.7.4. NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Cf. chapitre IV.3

IV.7.5. DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

Cf. chapitre IV.4

IV.7.6. PUBLICATION DU NOUVEAU CERTIFICAT

Cf. chapitre IV.4

IV.7.7. NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT

Cf. chapitre IV.4

IV.8. SUSPENSION ET REVOCATION DE CERTIFICAT

IV.8.1. CAUSES POSSIBLES D'UNE REVOCATION

IV.8.1.1. Certificats de Porteurs

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

- l'AC ou l'AE détecte un risque qu'elle juge important. Dans ce cas, l'AC ou l'AE notifie par courrier électronique sa décision de procéder à la révocation du certificat au porteur.
- les personnes spécifiquement désignées par l'AE peuvent procéder à la révocation d'urgence d'un certificat. Dans ce cas, l'AE notifie par courrier électronique sa décision de procéder à la révocation d'urgence du certificat au porteur.

Seule l'AC ou l'AE sont autorisées à révoquer un certificat.

Lorsque l'une des circonstances ci-dessus se réalise, le ou les certificat(s) concerné(s) sont révoqués et placés dans la Liste de Certificats Révoqués (LCR).

IV.8.1.2. Certificats d'une composante de l'IGC

Dans les circonstances suivantes, l'AC pourra révoquer la clé d'une composante de l'ICP :
- Cessation d'activité de la composante ;
- Non conformité des procédures appliquées par la composante ;
- Compromission ou suspicion de compromission perte ou vol de la clé privée de la composante.

IV.8.2. ORIGINE D'UNE DEMANDE DE REVOCATION

IV.8.2.1. Certificats de Porteurs

La révocation d'un certificat Porteur peut émaner :
de l'AC CertEurope Classe 1 émettrice du certificat ou de l'AE.

IV.8.2.2. Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être 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 sui doit en informer l'AC sans délai.

IV.8.3. INFORMATIONS A FOURNIR

La demande de révocation doit comporter au minimum :
- le prénom et nom du demandeur de la révocation ;
- le DN du Porteur ou toute autre information permettant d'identifier de façon certaine le certificat devant être révoqué.

IV.8.4. PROCEDURE DE DEMANDE DE REVOCATION

IV.8.4.1. Révocation d'un certificat de Porteur

Les procédures de révocation sont détaillées dans la DPC.
L'AE demande la révocation du Certificat en demandant à l'AC d'introduire le numéro de série du Certificat et la date de révocation du Certificat dans la Liste des Certificats Révoqués.
Si la demande n'est pas recevable, l'AE en informe le demandeur.
L'opération est enregistrée dans les journaux d'événements de l'AC CertEurope Classe 1.
Révocation.

IV.8.4.2. Révocation d'un certificat d'une composante de l'IGC

La procédure de révocation d'un certificat d'une composante de l'ICP est définie dans la DPC.
Cette révocation doit avoir lieu en trois étapes :

IV.8.4.3. Etape 1 : Alerte administrative

Elle doit tout d'abord prévenir l'ensemble des applications utilisatrices de ces certificats de l'imminence de la révocation de son certificat et des certificats Porteurs.
Elle doit enfin signaler l'imminence de la révocation de son certificat à toute entité lui ayant attribué une quelconque accréditation.

IV.8.4.4. Etape 2 : Révocation des certificats Porteurs

L'AC doit révoquer l'ensemble des certificats qu'elle aura générés et en avertir les Porteurs.

IV.8.4.5. Etape 3 : Révocation du certificat de l'AC

L'AC CertEurope Classe 1 doit faire une demande de révocation de son certificat à l'AC Certeurope Root CA 2.
L'AC Certeurope Root CA 2 doit révoquer le certificat de signature de l'AC CertEurope Classe 1 et mettre à jour sa LCR.

IV.8.5. DELAI ACCORDE AU PORTEUR POUR FORMULER LA DEMANDE DE REVOCATION

Sans objet.

IV.8.6. DELAI DE TRAITEMENT D'UNE REVOCATION PAR L'AC

IV.8.6.1. Révocation d'un certificat de Porteur

Dans la mesure où seule l'AC et l'AE sont autorisées à révoquer un certificat, la révocation d'un certificat se fait sans délai.
Le délai de publication de la révocation d'un certificat n'excède jamais 24 heures ouvrées à partir de la révocation.

IV.8.6.2. Révocation d'un certificat d'une composante de l'IGC

La révocation des certificats des composantes de l'IGC doit avoir lieu dans les plus brefs délais.

IV.8.7. EXIGENCES DE VERIFICATION DE LA REVOCATION PAR LES UTILISATEURS DE CERTIFICATS

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

IV.8.8. FREQUENCE D'ETABLISSEMENT DES LCR

La LCR est mise à jour toutes les 24h et après chaque révocation.

IV.8.9. DELAI MAXIMUM DE PUBLICATION D'UNE LCR

Après traitement d'une demande de révocation, la LCR doit être publiée sans délai.

IV.8.10. DISPONIBILITE D'UN SYSTEME DE VERIFICATION EN LIGNE DE LA REVOCATION ET DE L'ETAT DES CERTIFICATS

Il est possible de vérifier en ligne si un Certificat émis par l'AC CertEurope Classe 1 est révoqué.
Il est de la responsabilité des applications utilisatrices des certificats et des utilisateurs de contrôler la validité d'un certificat avant toute utilisation.

IV.8.11. EXIGENCES DE VERIFICATION EN LIGNE DE LA REVOCATION PAR LES UTILISATEURS DE CERTIFICATS

Cf. chapitre IV.8.7.

IV.8.12. AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS

Sans objet.

IV.8.13. EXIGENCES EN CAS DE COMPROMISSION DE LA CLE PRIVEE

Aucune procédure spécifique n'est mise en place si la cause de révocation est la compromission de la clé privée de Porteur.

IV.8.14. SUSPENSION DE CERTIFICATS

Le service de suspension n'est pas proposé dans le cadre de cette PC.

IV.9. SUSPENSION DE CERTIFICATS

L'AC CertEurope Classe 1 ne gère pas la suspension des certificats

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

IV.10.1. CARACTERISTIQUES OPERATIONNELLES

Il est possible de vérifier en ligne si un Certificat émis par l'AC CertEurope Classe 1 est révoqué.

Il est de la responsabilité des applications utilisatrices des Certificats et des utilisateurs de contrôler la validité d'un Certificat avant toute utilisation.

L'accès à la Liste de Certificats Révoqués est possible via un annuaire LDAP V3

Les LCR sont au format dénommé "LCR V2".

IV.10.2. DISPONIBILITE DE LA FONCTION

Cf. chapitre II.1.6.3

IV.11. RENOUVELLEMENT DE CLE D'UNE COMPOSANTE DE L'ICP

IV.11.1. CLE DE SIGNATURE DE L'AC

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

La durée de vie des certificats Porteur est variable selon le contexte de l'application utilisatrice et n'excèdera pas trois (3) ans.

Le renouvellement de cette clé devra intervenir au plus tard deux (2) jours avant la fin de sa validité. L'AC se réserve la possibilité de la renouveler avant sa limite de validité. La décision de son renouvellement pourra être prise plus tôt en fonction de divers critères (évolution de la technique cryptographique, allongement de la longueur, …).

Le nouveau bi-clé généré servira à signer les nouveaux certificats Porteurs émis ainsi que la LCR.

Le certificat précédent restera utilisable pour la validation de certificats émis avant le renouvellement.

IV.11.2. CLE DE SIGNATURE DES AUTRES COMPOSANTES DE L'ICP

L'CertEurope Classe 1 renouvellera les bi-clés des autres composantes de l'ICP 3 mois avant leur expiration.

IV.12. JOURNALISATION DES EVENEMENTS

La journalisation des événements concerne tous les événements ayant trait à la sécurité des systèmes informatiques utilisés.

Elle permet de garantir l'auditabilité, la traçabilité, l'imputabilité ainsi que de s'assurer que la séparation des fonctions est effective. Ce système permet également de collecter des preuves et de détecter des anomalies. La journalisation des événements est protégée, sauvegardée, intègre et fait l'objet de règles strictes d'exploitation.

Les actions de journalisation sont décrites précisément dans la DPC et abordent notamment les thèmes suivants :

- événements enregistrés par l'AC ;

- processus de journalisation des événements ;
- collecte des journaux d'événements (interne ou externe) ;
- conservation des journaux d'événements ;
- protection des journaux d'événements ;
- anomalies et audit ;
- imputabilité.

IV.12.1. INFORMATION ENREGISTREES

Ces enregistrements d'événements devront contenir au minimum les champs suivants, s'ils sont pertinents :
- type d'opération ;
- destinataire de l'opération ;
- nom du demandeur de l'opération ;
- nom de l'exécutant ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- date et heure de l'opération ;
- cause de l'évènement
- résultat de l'événement (échec ou réussite).

IV.12.2. IMPUTABILITE

L'objectif principal de la journalisation est de permettre d'imputer toute action à son auteur que ce soit une personne physique ou un système.

IV.12.3. EVENEMENTS ENREGISTRES PAR L'AE

L'AE doit consigner au moins les évènements suivants :
- demandes de certificats ;
- demandes de révocation ;
- sollicitation et accusés de réception de l'AC.

IV.12.4. EVENEMENTS ENREGISTRES PAR L'AC

Les évènements suivants seront enregistrés par l'AC, ce sont essentiellement des évènements générés par des systèmes informatiques :
- tous les événements ayant trait à la sécurité des systèmes informatiques impliqués dans l'ICP ;
- demandes de certificats ;
- demandes de révocation ;
- démarrage et arrêt des systèmes informatiques ;
- démarrage et arrêt des applications ;
- opérations échouées ou réussies pour créer, extraire, établir des mots de passe ou modifier les privilèges système d'exploitants privilégiés ;
- génération des clés de ses composantes ;
- la génération et la révocation de certificats ;
- changements des caractéristiques de l'AC et (ou) de ses composantes ;
- la publication de la LCR;
- événements relatifs aux supports cryptographiques (génération des données d'activation à enregistrer).

IV.12.5. EVENEMENTS DIVERS

D'autres évènements non issus de systèmes informatiques mais essentiels pour la sécurité de l'AC, doivent être enregistrés, ce sont en particulier :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration du système ;
- les changements apportés au personnel ;
- les actions de destruction : des supports contenant des clés, des données d'activation ou des renseignements personnels sur les Abonnés.

IV.12.6. PROCESSUS DE JOURNALISATION

Le processus de journalisation doit être effectué en tâche de fond et permettre un enregistrement en temps réel des opérations effectuées. Le processus de journalisation doit être conçu de façon à être incontournable.

En cas de saisie manuelle l'écriture doit se faire dans le même jour ouvré que l'événement.

IV.12.7. PROTECTION D'UN JOURNAL D'EVENEMENTS

L'écriture dans les journaux d'événements doit être conditionnée par des contrôles de droits d'accès. Les enregistrements et l'horloge des composantes de l'ICP doivent être protégés contre les tentatives non autorisées de modification et de destruction.

IV.12.8. COPIES DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS

Aucune exigence n'est stipulée.

IV.12.9. SYSTEME DE COLLECTE DES JOURNAUX (INTERNE OU EXTERNE)

L'enregistrement des événements doit commencer au démarrage des systèmes concernés par les événements à enregistrer et se terminer à l'arrêt de ces systèmes.

IV.12.10. ANOMALIES ET AUDIT

Les composantes de l'AC responsables de la fonction de journalisation doivent être en mesure de détecter toute tentative de violation de l'intégrité du système de gestion des certificats, y compris les équipements physiques, l'environnement d'exploitation et le personnel.

Les journaux d'événements journaliers doivent être contrôlés pour identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être revus avec une fréquence hebdomadaire. Cette révision donnera lieu à un résumé dans lequel les éléments importants sont analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

La DPC doit documenter les mesures à prendre à la suite de ces analyses.

IV.13. ARCHIVES

L'archivage est réalisé par l'AE et l'AC dans le but d'assurer la continuité de service, l'auditabilité et la non-répudiation des opérations.

Les mesures nécessaires sont mises en place par l'AE et l'AC afin que ces archives soient disponibles, exploitables, protégées en intégrité et qu'elles fassent l'objet de règles strictes d'exploitation et de protection contre la destruction.

L'AC décrit précisément dans ses procédures internes, et notamment dans la DPC, les points suivants :

IV.13.1. TYPES DE DONNEES A ARCHIVER

Doivent être archivées au minimum, les données suivantes :
- les logiciels et les fichiers de configuration des équipements informatiques de l'ICP ;
- la PC et la DPC ;
- les agréments contractuels ou les conventions avec d'autres AC ;
- les journaux d'événements ;
- les certificats tels qu'émis ;
- les LCR telles qu'émises ou publiées ;

IV.13.2. PROTECTION DES ARCHIVES

Les archives doivent être protégées durant leur conservation, cette protection concerne :
- leur intégrité ;
- leur confidentialité ;
- leur lisibilité.

Les moyens mis en œuvre pour atteindre ce triple objectif seront décrits dans la DPC.

IV.13.3. PERIODE DE RETENTION DES ARCHIVES

IV.13.3.1. Certificats et LCR

Les certificats de clés de signatureainsi que les LCR produites par l'AC doivent être archivés pendant au moins cinq ans après l'expiration des clés.
Les moyens mis en œuvre pour atteindre cet objectif seront décrits dans la DPC

IV.13.3.2. Dossier de demande de certificat

Sans objet.

IV.13.3.3. Journaux d'évènements

Les journaux de l'AC seront conservés 5 ans après son expiration. Bien entendu le triple objectif de confidentialité, intégrité, lisibilité est maintenu durant leur conservation.
Les moyens mis en œuvre pour atteindre cet objectif seront décrits dans la DPC.

IV.13.3.4. Autres journaux

Aucune exigence n'est stipulée.

IV.13.4. DUPLICATION DES ARCHIVES

Les précisions seront fournies dans la DPC.

IV.13.5. HORODATAGE DES ENREGISTREMENTS

Les enregistrements des certificats et des LCR sont horodatés conformément à la politique de sécurité de l'AC en matière d'horodatage des évènements.

IV.13.6. PROCEDURE DE COLLECTE DES ARCHIVES

Aucune exigence n'est stipulée.

IV.13.7. PROCEDURE DE RECUPERATION DES ARCHIVES

Une composante de l'ICP ne peut récupérer et consulter que ses propres archives.
Le processus de récupération doit faire l'objet d'une procédure et figurer dans la DPC.
Une archive doit être récupérée sous un délai inférieur à 2 jours ouvrés.
Les procédures sont décrites dans la DPC.

IV.14. CESSATION D'ACTIVITE DE L'AC

IV.14.1. TRANSFERT D'ACTIVITE

Si l'AC décide de transférer son activité de certification, elle doit tout d'abord en informer les applications utilisatrices et les Abonnés dans un délai de 4 mois avant le transfert effectif d'activité.
Elle doit également informer les applications utilisatrices et les utilisateurs des modifications liées à ce transfert d'activité.
Les archives de l'AC devront être reprises en charge par la société reprenant l'activité.

IV.14.2. CESSATION DEFINITIVE

En cas de cessation définitive d'activité, l'AC CertEurope Classe 1 procède comme indiqué au .IV.8.4.2 : révocation des certificats de signature de l'AC. L'AC CertEurope Classe 1 respectera un délai de 3 mois entre les étapes 1 et 2.

V. CONTROLE DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES, CONTROLE DU PERSONNEL

Les différents contrôles décrits ici visent, par une gestion des risques adéquate, à assurer un niveau de confiance fort dans le fonctionnement de l'CertEurope Classe 1.

V.1.1. SITUATION GEOGRAPHIQUE

Aucune exigence n'est stipulée.

V.1.2. ACCES PHYSIQUE

Les zones hébergeant les systèmes informatiques de l'CertEurope Classe 1 sont physiquement protégées contre un accès extérieur non autorisé.

La liste des personnels autorisés à y accéder existe et est limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés est contrôlé par un moyen physique et enregistré.

V.1.3. ENERGIE ET AIR CONDITIONNE

Les installations électriques et de conditionnement d'air sont suffisantes pour le bon fonctionnement des systèmes informatiques de l'CertEurope Classe 1.

V.1.4. EXPOSITION AUX LIQUIDES

Les systèmes informatiques de l'AC CertEurope Classe 1 ne sont pas situés en zone inondable, ni du fait d'intempéries, ni du fait de tuyauteries défaillantes.

V.1.5. SECURITE INCENDIE

Les locaux d'hébergement des systèmes informatiques de l'AC CertEurope Classe 1 sont protégés contre les incendies (détection et extinction automatiques). La distribution des machines permet par ailleurs d'assurer une disponibilité maximale aux services.

V.1.6. SITE DE SECOURS

Afin d'assurer l'accès aux services de certification/révocation même en cas de désastre sur le site de production des mesures doivent être prises. Ces mesures doivent permettre la reprise des activités de l'CertEurope Classe 1 dans les plus brefs délais.

Deux échelons de reprise d'activité peuvent être envisagés :

L'accès à la LCR ;

L'accès à l'ensemble des services (état nominal).

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

V.1.7. CONSERVATION DES MEDIAS

Les médias contenant des données sauvegardées ou archivées doivent être conservés avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.

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

V.1.8. DESTRUCTION DES SUPPORTS

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

V.1.9. 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 moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

V.2. CONTROLES DES PROCEDURES

Des contrôles des procédures sont mis en place par l'AC CertEurope Classe 1 et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

V.2.1. ROLES DE CONFIANCE

Pour le compte de l'CertEurope Classe 1, l'OC s'appuie sur du personnel réparti en 5 catégories (rôles) :
- ingénieur système : mise en place et maintenance des systèmes ;
- administrateur sécurité gestion de la sécurité des systèmes ;
- opérateur : exploitation basique du système ;
- responsable sécurité : Application de la politique de sécurité ;
- responsable qualité : assurance de la qualité des services rendus par l'AC CertEurope Classe 1.

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

V.2.2. NOMBRE DE PERSONNES NECESSAIRES A L'EXECUTION DE TACHES SENSIBLES

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

V.2.3. IDENTIFICATION ET AUTHENTIFICATION DES ROLES

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'CertEurope Classe 1.

V.3. CONTROLE DU PERSONNEL

V.3.1. PASSE PROFESSIONNEL, QUALIFICATIONS, EXPERIENCE, ET EXIGENCES D'HABILITATIONS

L'CertEurope Classe 1 vérifie le passé professionnel de la personne et son adéquation aux exigences de la gestion de l'CertEurope Classe 1.

L'AC CertEurope Classe 1 informera toute personne intervenant dans la Gestion de l'AC CertEurope Classe 1 de ses responsabilités relatives aux services de l'AC ainsi que des procédures liées à la sécurité.

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

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

V.3.2. PROCEDURES DE CONTROLE DU PASSE PROFESSIONNEL

Les précisions seront données dans la DPC.

V.3.3. EXIGENCES DE FORMATION

L'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches touchant la gestion de l'AC ont reçu une formation adaptée concernant les principes de fonctionnement et des mécanismes de sécurité de l'AC, et sont familiarisés aux règles de sécurité en vigueur.

V.3.4. FREQUENCE DES FORMATIONS

Les précisions seront données dans la DPC.

V.3.5. GESTION DES METIERS

Les précisions seront données dans la DPC.

V.3.6. SANCTIONS POUR DES ACTIONS NON-AUTORISEES

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

V.3.7. CONTROLE DES PERSONNELS CONTRACTANTS

Les précisions seront données dans la DPC.

Note : le périmètre de l'IGC est restreint au personnel de l'OC.

V.3.8. DOCUMENTATION FOURNIE AU PERSONNEL

L'AC doit s'assurer que son personnel dispose de l'accès à toute loi, ou tout contrat qui s'applique aux postes occupés.

Les documents dont doit disposer 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.

VI. CONTROLES TECHNIQUES DE SECURITE

VI.1. GENERATION ET INSTALLATION DE BI-CLES

VI.1.1. GENERATION D'UN BI-CLE DE PORTEUR

Les clés issues de l'CertEurope Classe 1 ont comme seuls usages au sens X509 du terme :
- La signature électronique ;
- La non répudiation.

Le bi-clé est généré directement sur le poste de l'utilisateur. La clé privée n'est donc jamais accessible par l'AC ni par l'AE.

VI.1.2. TRANSMISSION DE LA CLE PUBLIQUE DE SIGNATURE (DU PORTEUR) A L'AC

La clé publique du porteur est transmise à l'AC avec les informations nominatives que le certificat comportera via un protocole d'échange qui en assure l'intégrité. La DPC précise les modalités de cette transmission.

VI.1.3. FOURNITURE D'UN CERTIFICAT D'AC

La clé publique de l'AC est téléchargeable sur le site Internet de CERTEUROPE à l'adresse : http://www.certeurope.fr
L'empreinte du Certificat de la clé publique de l'AC permet d'en établir l'authenticité.
La DPC précise les modalités de l'accès au certificat de l'AC.

VI.1.4. TAILLES DES CLES

Les clés RSA des Porteurs utilisées ont une taille de 2048 bits et seront mises à niveau au fur et à mesure de l'évolution de la technique et/ou de la législation.
La taille de la clé RSA de l'CertEurope Classe 1 est de 2048 bits.

VI.1.5. PARAMETRES DE GENERATION DES CLES

Les clés sont générées dans les containers cryptographiques des navigateurs.

VI.1.6. CONTROLE DE LA QUALITE DES PARAMETRES DES CLES

Sans objet.

VI.1.7. MODE DE GENERATION DU BICLE DE L'AC

Le bi-clé de l'AC (pour la signature de certificats et de CRLs) est généré et protégé par un module cryptographique matériel.
Ce module doit répondre aux critères FIPS 140-2 niveau 3 ou équivalent.
La génération ou le renouvellement du bi-clé de l'AC par ce module nécessite la présence d'au moins 2 personnes.

VI.1.8. USAGE DE LA CLE PUBLIQUE DES PORTEURS

Les biclés délivrés par l'AC CertEurope Classe 1 ne sont utilisables que pour la signature et la non-répudiation.
Ces usages sont précisés dans le champ keyUsage des certificats CERTEUROPE CLASSE 1; ce champ a donc les valeurs **digitalSignature** et **nonRépudiation**.

VI.2. PROTECTION DE LA CLE PRIVEE

VI.2.1. DISPOSITIFS DE GESTION DES ELEMENTS SECRETS DU PORTEUR

Le bi-clé du Porteur est généré par et stocké sur son poste. L'ajout d'un code d'accès à la clé privée pendant la phase de génération du bi-clé est possible. Le Porteur est responsable de la confidentialité du code d'accès lié à sa clé privée.

VI.2.2. CONTROLE DE LA CLE PRIVEE DE SIGNATURE DE L'AC PAR PLUSIEURS PERSONNES

Le contrôle des clés privées de l'AC CertEurope Classe 1 (pour la signature de certificats et de CRL) nécessite la présence de plusieurs personnes.

VI.2.3. RECUPERATION DE CLE PRIVEE DE CONFIDENTIALITE* DU PORTEUR.

L'CertEurope Classe 1 n'offre pas de service de recouvrement de clé.

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

VI.3.1. ARCHIVAGE DES CLES PUBLIQUES DES PORTEURS

Les certificats des Porteurs, contenant la clé publique, sont archivés pendant 5 ans après leur expiration.

VI.3.2. DUREE DE VIE DES CERTIFICATS

La durée de vie des certificats fournis dans le cadre de l'AC CertEurope Classe 1 est variable et n'excèdera pas trois (3) ans. Ces certificats sont non renouvelables.

VI.4. CODE PIN DES PORTEURS

VI.4.1. GENERATION ET UTILISATION DES CODES PIN

Sans objet.

VI.4.2. PROTECTION DES CODES PIN

Sans objet.

VI.5. SECURITE DES POSTES DE TRAVAIL DES COMPOSANTES DE L'ICP

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…)
- imputabilité

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

VI.6. CONTROLES TECHNIQUES DU SYSTEME DURANT SON CYCLE DE VIE

VI.6.1. CONTROLES DES DEVELOPPEMENTS DES SYSTEMES

Les applications de l'AC ont été implémentées dans le strict respect de l'analyse de risque préalable et de la politique de sécurité qui en découle.

L'implémentation de l'AC et de la plate-forme qui l'héberge est documentée.

Toute modification de l'AC et de la plate-forme qui l'héberge est documentée

VI.6.2. CONTROLES DE LA GESTION DE LA SECURITE.

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

VI.7. CONTROLES DE LA SECURITE RESEAU

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

VI.8. CONTROLES DES MODULES CRYPTOGRAPHIQUES

Les modules cryptographiques utilisés par l'AC sont évalués selon les critères FIPS 140-1 au niveau 4.

VII. PROFILS DE CERTIFICATS ET DE LCR

VII.1. PROFIL DES CERTIFICATS

Les Certificats de l'AC CertEurope Classe 1 contiennent les champs primaires et les extensions suivantes :

Champ	Valeur	Détail valeur	Explications
Version	V3	2	Version du Certificat X.509
Numéro de série	1506 38D4 36F3 K231 C692 B849 E3F7 B943		Le numéro de série unique du Certificat attribué par le module cryptographique
Algorithme de signature	Sha1RSA = 1.3.14.3.2.29		Identifiant de l'algorithme de signature de l'AC
Emetteur	/C=FR /O=Certeurope /CN=AC Certeurope Classe 1		Le nom de l'AC émettrice est le Distinguished Name (X.500) de l'AC signant les Certificats
Valide à partir du	Date de début = x (au plus tôt le 04/01/2008 00 :00 :00)		Dates et heures d'activation et d'expiration du Certificat
Valide jusqu'au	Valide jusqu'au x+ y jours (au plus tard le 04/01/2018 00 :00 :00)		
Objet	E = jaen.dupond@certeurope.fr CN = Jean DUPOND O = SOCIETE X T = Gérant C = FR		Nom distinctif de l'entité identifiée
Clé publique	RSA(2048 Bits)	7C28 8902 8181 3963 8424 B08C CD71 9110 7E44 2B2E 8014 35F0 49CE B4D2 8CA9 3516 5FC7 9EB8 9A89 637C 20C4 DB30 97AF ECB3 37F2 A000 00E8 E350 BA90 2B20 EEE5 9D5B 4A87 E0D5 895A B6A4 05A6 B2C4 2715 555F 3081 0A68 95AD 00CF 6071 4C00 8431 7693 7EC0 20F9 8C31 EC2A 8585 9054 3478 4DD1 366B 9024 67B7 E8C8 C812 6EE9 E35B 5D04 700D 6699 2702 0301 0001	Identifiant de l'algorithme d'usage de la clé publique contenue dans le Certificat, et valeur de la clé publique
Contrainte de base	Subject Type=End Entity Path Length Constraint=None		
Point de distribution de la LCR	CRL Distribution Point Distribution Point Name: Full Name: URL=ldap ://lcr1.certeurope.fr/CN= AC Certeurope Classe 1, O=Certeurope, C=FR ?CertificateRevocationList URL=ldap ://lcr2.certeurope.fr/CN= AC Certeurope Classe 1, O=Certeurope, C=FR ?CertificateRevocationList URL=http ://www.certeurope.fr/reference/certeurope-1.crl		
Certificate Policies	Certificate Policy: PolicyIdentifier= 1.2.250.1.105.5.1 Policy Qualifier Info: Policy Qualifier Id= Qualifier=	OBJECT IDENTIFIER cps http://www.certeurope.fr/reference/pc-certeurope-1.pdf	Identifiant de la Politique de Certification
Algorithme d'empreinte numérique	Sha1 = 1.3.14.3.2.29		
Empreinte numérique	24 89 39 d0 af 41 47 66 de bc 39 67 08 94 16 e4 2f d3 4f 94	8C 62 E9 57 0B 94 DF EB 73 14 AE 15 0F A9 36 2B 22 84 81 28 0F 25 06 FF 1C D3 10 EC A5 BC 43 1C AB 02 1D CD 7E 9E D7 B9 A0 DA 13 59 22 26 DF 72 EB 6D B3 AA 4E 2C B0 B3 1B 38 A4 E5 C4 3A 4C 15 2F E2 B2 AD 1C 9D 8F 5A FE D6 05	Champ d'octets caractérisant le Certificat de l'AC ayant signé le Certificat

		BC 6D 2E 81 D4 67 96 3D 74 BB F1 3F 37 7C 27 75 8C 9A 9A 9D 56 63 F1 BD 1E 76 89 09 ED 71 AA E1 F0 65 E1 A5 C8 0E DC AE 50 E1 C6 0D BF 76 6F A8 EC D0 D7 55 B9	

VII.2. PROFIL DE LCR

VII.2.1. CHAMPS DES LCR

Les LCR de l'CertEurope Classe 1 contiennent les champs suivants :
Version : la version de la LCR. Dans le cadre de la présente AC, il s'agit de la version 2;
Signature : l'identifiant de l'algorithme de signature de l'AC soit Sha1-RSA ;
Issuer : le nom de l'AC émettrice qui signe les Certificats soit l'CertEurope Classe 1;
ThisUpdate : date de génération de la LCR ;
NextUpdate : prochaine date à laquelle cette LCR sera mise à jour ;
RevokedCertificates : liste des numéros de série des Certificats révoqués ;
UserCertificate : numéro de série de Certificat révoqué ;
RevocationDate : date à laquelle un Certificat donné à été révoqué.
crlExtensions : liste des extensions de la LCR.

VII.2.2. EXTENSIONS DES LCR

Les LCR de l'CertEurope Classe 1 comportent deux extensions :
authorityKeyIdentifier : cette extension non critique identifie la clé publique à utiliser pour vérifier la validité de la LCR. Cet identifiant a la même valeur que le champ SubjectKeyIdentifier des certificats émis par l'AC CertEurope Classe 1 ;
CRLNumber : cette extension non critique contient le numéro de série de la LCR.

VIII. ADMINISTRATION DES SPECIFICATIONS REFERENTES A L'AC

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente Politique de Certification.

La PC de l'AC CERTEUROPE CLASSE 1 reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

VIII.1. PROCEDURES DE MODIFICATION DE LA PC

Le responsable de l'AC doit signaler aux Porteurs et aux applications utilisatrices toute modification de la présente politique selon les modalités prévues au VIII.1.2.

VIII.1.1. CAUSES DE MODIFICATION

Cette PC devra être revu en raison de projets de modifications suivants :

les certificats référencés ;

la composition de l'AC ;

à chaque modification des documents de référence de l'autorité de politique AP ainsi que chaque année pour assurer sa conformité aux normes de sécurité et à l'évolution des mises en œuvre du marché de la sécurité informatique.

VIII.1.2. DELAI DE PREAVIS

Le responsable de l'AC doit donner un préavis de trente (30) jours calendaires aux Porteurs et aux applications utilisatrices avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, a un impact majeur sur eux.

Le responsable de l'AC doit donner un préavis de quinze (15) jours calendaires aux Porteurs et aux applications utilisatrices avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact mineur sur eux.

Le responsable de l'AC doit donner un préavis aux Porteurs et aux applications utilisatrices dans les sept (7) jours calendaires d'un changement de la présente politique qui résulte d'une situation hors du contrôle du responsable de la politique, si ce changement ait un impact sur eux.

VIII.2. PROCEDURES DE PUBLICATION ET DE NOTIFICATION

La PC est disponible depuis la source suivante :

http://www.certeurope.fr/reference/pc-certeurope-1.pdf

VIII.3. PROCEDURES D'APPROBATION DE LA PC

L'approbation de la PC de l'AC est réalisée par l'AP qui notamment vérifie son adéquation aux documents de référence de l'AP.

La décision du Porteur de ne pas formuler de remarque écrite suite à la notification d'un changement proposé constitue l'acceptation du changement.

IX. AUTRES PROBLEMATIQUES METIERS ET LEGALES

IX.1. PROTECTION DES DONNEES PERSONNELLES

Toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier la CNIL.

IX.2. DROITS SUR LA PROPRIETE 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 AC CERTEUROPE CLASSE 1, il peut être échangé 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 AC CERTEUROPE CLASSE 1.

Du fait de son enregistrement, le Porteur n'acquiert sur ses données de création de signature et de chiffrement (bi-clés, données d'activation, certificats) qui lui sont remis par l'AE, qu'un droit d'usage limité aux seules opérations effectuées conformément à la présente Politique de Certification et aux conditions générales d'utilisation du service concerné.

En conséquence, le Porteur n'acquiert aucun droit de propriété, de quelque nature que ce soit, sur les certificats et les bi-clés, qu'il s'engage à restituer à l'AE et à cesser d'utiliser dans tous les cas prévus par la présente Politique de Certification ou par les conditions du générales d'utilisation.

IX.3. LIMITE DE RESPONSABILITE

L'AE décline toute responsabilité quant à l'exactitude des informations d'identification déclarée par le futur porteur.

IX.4. DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

La Loi française est applicable aux dispositions du présent document.

En cas de traduction, seule la version française du présent document fera foi.

En cas de difficultés survenant dans l'exécution ou l'interprétation de la présente PC, les parties s'engagent à rechercher une solution amiable avant toute action contentieuse.

En cas d'échec, tous les litiges concernant l'exécution ou l'interprétation du présent contrat seront portés devant les juridictions compétentes de Paris.

Si une disposition de la présente PC s'avère inapplicable ou incompatible avec une loi ou un règlement en vigueur, elle sera considérée comme nulle, cette nullité n'affectant en aucune manière la validité des autres dispositions de la présente PC.

IX.5. JURIDICTIONS COMPETENTES

Cf. chapitre IX.4.