Politique de Certification (PC) et Déclaration des Pratiques de Certification (DPC)

Autorité de Certification pour la délivrance de certificats aux personnes physiques selon le référentiel ETSI EN 319 411-1 LCP

« CertEurope eID User Signature »

Version : 1.1
Mise à jour : 00
Date de création : 2 décembre 2021
Dernière mise à jour : 28 février 2022
Etat du document : Officiel
Rédigé par : CertEurope
Vérifié par : Comité PKI
Approuvé par : Comité PKI

CertEurope, une société du groupe InfoCert

www.certeurope.fr

41, rue de l'échiquier, 75010 Paris – France

Tel : +33 (0)1 45 26 72 00 / Fax : +33 (0)1 45 26 72 01

Modifications

Date	Etat	Version	Commentaires
02/12/2021	Draft	0.1	
09/02/2022	Public	1.0	Validation en COSSI
28/02/2022	Public	1.1	Corrections mineures suite à l'audit

Table des matières

1 Introduction

1.1 Présentation générale

Ce document constitue la « Politique de Certification » (PC) et la « Déclaration des Pratiques de Certification » (DPC) de l'Autorité de Certification AC CertEurope eID User vise la conformité aux

- Exigences du référentiel ETSI 319 411-1 pour le profil LCP

Les engagements définis dans ce document proviennent de diverses sources :

- L'ETSI EN 319 411-1
- La RFC5280 de l'IETF [RFC5280]
- La PSSI de CertEurope (Politique de Sécurité).

Les autres PC et DPC de CertEurope.

Une PC/DPC est identifiée par un numéro 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/DPC 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 ainsi que les procédures de certification publiques.

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 eID User 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

Le tableau suivant décrit les usages possibles pour les profils de certificats :

Acronyme	Description	Champs X509
SIGN	Signature	(Bit 1) : nonRepudiation

La norme X.509[1] a renommé le bit nonRepudiation en "contentCommitment". La RFC 5280 a gardé le nom d'origine « nonRepudiation » pour des raisons de compatibilité ascendante. Ces bits sont équivalents en fonction et en signification indépendamment de leurs noms différents.

La présente Politique de Certification est identifiée par les OID suivants :

OID	Usages	Profil de certification
	SIGN	
1.2.250.1.105.**23.411.1.6**.1.*1.0*	X	ETSI EN 319 411-1 **LCP**

.

[1] Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

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 Certeurope qui consiste à vérifier l'identité et la qualité d'un demandeur de certificat et/ou à générer ledit certificat. A ce titre, ce sont les Client Certeurope qui en agissant en tant qu'AE assure : - la prise en compte et la vérification des informations, notamment de données à caractère personnel, présentées par l'Utilisateur, futur Porteur de certificat et la constitution de son dossier d'enregistrement.
- **Service d'enregistrement :** vérifie les informations d'identification du porteur d'un certificat lors de son enregistrement initial ou d'un renouvellement.
- **Service de génération des certificats :** génère et signe les certificats à partir des informations transmises par le service d'enregistrement.
- **Service de publication et diffusion :** met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.
- **Service de fourniture de code d'activation au porteur :** Ce service remet au porteur le code d'activation de son dispositif.
- **Service de gestion des révocations :** traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via le service d'information sur l'état des certificats. Une composante de ce service est en mesure de prendre en charge des révocations en urgence.
- **Service d'information sur l'état des certificats :** fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, valide, etc.).
- **Service d'assistance aux porteurs :** assiste les porteurs et utilisateurs de certificats émis par l'AC. Ce service est accessible par téléphone ou par messagerie électronique.

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

- **Demandeur** - personne physique ou morale qui souhaite souscrire au Service de Certification Electronique C@rteurope.
- **Abonné** : personne physique ou morale qui souscrit au Service de Certification Electronique C@rteurope.
- **Porteur / Sujet** - La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.

- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur d'authentification provenant du porteur du certificat ou pour vérifier une signature électronique provenant du porteur du certificat.
- **Personne autorisée** - Il s'agit d'une personne autre que le porteur et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, l'AC CertEurope eID User, 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 :

- L'enregistrement et la vérification d'identité du porteur,
- Dans le cas des certificats à usage professionnel, la vérification du lien contractuel entre le porteur et l'entité qu'il représente

1.3.3 Les porteurs de certificat

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

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

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

Dans le cas d'un usage « particulier », le souscripteur et le porteur désigne la même personne.

1.3.4 Les utilisateurs de certificat

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

Les utilisateurs de certificats peuvent également être des plateformes de marchés publics ou toute application autorisée par l'AC.

1.3.5 Autres participants

1.3.5.1 Composantes de l'IGC

Cf. §1.3.1.

1.3.5.2 Mandataire de certification

Cf. §1.3.1.

1.3.5.3 Opérateur de certification

L'Opérateur de Certification (OC) est une composante du PSCE ayant en charge d'opérer 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 porteur,
- service de gestion des révocations d'urgence,
- service d'information sur l'état des certificats,

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

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats des porteurs

La présente PC/DPC traite des bi-clés et des certificats à destination des catégories de porteurs identifiées au § 1.3.3 ci-dessus, afin que ces porteurs puissent signer électroniquement des données (documents, messages) dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées au § 1.3.4 ci-dessus.

La fonction « Signature », celle-ci apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

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

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 (L'AC racine CertEurope eID Root).

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

La bi-clé n'est jamais transmise au porteur et elle est systématiquement détruite à l'issue de la transaction de signature, ce qui empêche tout autre usage que la signature.

1.5 Gestion de la PC/DPC

1.5.1 Entité gérant la PC/DPC

1.5.1.1 Organisme responsable

La société CertEurope est responsable de cette PC/DPC.

Gouvernance IGC CertEurope

41 rue de l'échiquier, 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 CertEurope – 41 rue de l'échiquier – 75010 Paris
- Par e-mail à l'adresse : info@certeurope.fr
- Par téléphone au numéro : +33 (0)1 46 22 07 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. Il s'agit en l'occurrence du même document validé par le Comité PKI 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 PC/DPC est publiée sans délai, conformément aux exigences du paragraphe 1.2.

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
DDS	Dossier de Souscription
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification, ou EPC
EAR	Entité d'Audit et de Référencement
EPC	Enoncé des Pratiques de Certification, ou DPC
EIDAS	electronic IDentification, Authentication and trust Services
ETSI	European Telecommunications Standards Institute
ICP	Infrastructure à Clés Publiques

IGC	Infrastructure de Gestion de Clés
LCR	Liste des Certificats Révoqués
LDAP	Light Directory Access Protocol
MC	Mandataire de Certification
O	Organisation
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OI	Organisation Identifier
OID	Object Identifier
OU	Organisation Unit
PC	Politique de Certification
PIN	Personal Identification Number
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adelman
SN	Serial Number
SCD	Dispositif 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

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

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage.

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 œuvre 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.

1.6.3 Termes spécifiques ou complétés / adaptés pour la présente PC/DPC

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/DPC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du § 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/DPC.

Autorité d'enregistrement - Cf. § 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/DPC, 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).

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

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

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

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/Organisme - 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. § 1.3.1

Personne autorisée - Cf. § 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 porteurs et les utilisateurs de certificats.

Porteur - Cf. chapitre 1.3.1

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

Référencement - Opération qui consiste, pour l'Administration, à tenir à jour la liste des offres de certification électronique des PSCE qui répondent à des exigences spécifiées dans le référentiel ETSI EN 319 411-1. Seuls les certificats d'offres référencées peuvent être utilisés dans le cadre des échanges dématérialisés de l'Administration.

Service d'enregistrement : Cf. § 1.3.1

Service de génération des certificats Cf. § 1.3.1

Service de publication et diffusion : Cf. § 1.3.1

Service de fourniture de dispositif au porteur : Cf. § 1.3.1

Service de fourniture de code à usage unique (OTP) au porteur - Cf. § 1.3.1

Service de gestion des révocations : Cf. § 1.3.1

Service d'information sur l'état des certificats : Cf. § 1.3.1

Service d'assistance aux porteurs : Cf. § 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. § 1.3.1

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

2.1 Entités chargées de la mise à disposition des informations

L'AC est en charge des services de publication :

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

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

Les canaux utilisés sont :

- copie 1 (original) : http://www.certeurope.fr/reference/certeurope_eid_user.crl
- copie 2 : ldap://lcr1.certeurope.fr/cn=CertEurope%20eID%20User,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList
- copie 3 : ldap://lcr2.certeurope.fr/cn=CertEurope%20eID%20User,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

2.2 Informations devant être publiées

Sur son site web (https://www.certeurope.fr/chaine-de-confiance), l'AC diffuse publiquement les informations suivantes:

- la Politique de Certification ainsi que la Déclaration des Pratiques de Certification CertEurope en cours de validité (PC/DPC).
- la Liste de Certificats Révoqués (LCR).
- le certificat de l'AC CertEurope eID Root, en cours de validité, auquel la clé de l'AC CertEurope eID User est subordonnée. L'empreinte numérique du certificat est également disponible pour une garantie d'intégrité.
- le Certificat de l'AC CertEurope eID User 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 particulières et générales d'utilisation des certificats.
- les empreintes numériques des données publiées.

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 Web de CertEurope : https://www.certeurope.fr

L'AC CertEurope eID User 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/DPC, formulaires, etc.), l'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.

- Pour les certificats d'AC, ils doivent être diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants.
- Pour les informations d'état des certificats, cf. §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/DPC, formulaires, etc.), les systèmes assurent une disponibilité 24h/24 7j/7.
- 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 : 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 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).

L'accès est autorisé aux personnes habilitées conformément au document « [5] CERTEUROPE – Rôles et habilitations ».

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 eID User (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" (DN) de type X.501 conforme aux exigences définies dans les documents [RFC3739] et [AFNOR_QCP] ainsi qu'au chapitre § 7.

3.1.2 Nécessité d'utilisation de noms explicites

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

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

- dans le champ **« CountryName »** (C) :

Pays de domiciliation de la structure juridique dans le cas d'un certificat pour un usage professionnel, ou du signataire dans le cas d'un particulier.;

- dans le **champ « givenName »** (G) : Le premier prénom, ou les prénoms de l'état civil du porteur. Dans le cas de prénoms composés, ceux-ci doivent être séparés par un tiret (« - »).
- dans le **champ « surname »** : (SN) : Nom de l'état civil ou le nom d'usage du porteur présent sur le justificatif d'identité du porteur utilisée pour l'enregistrement et la vérification d'identité du porteur,
- dans le **champ « CommonName »** (CN) : Ce champ contient le givenName et le surName du porteur séparé par un espace.
- dans le champ **« SerialNumber »** : est un identifiant unique de la transaction de signature.

Exemple : DN = {C=FR, CN=Jean DUPONT, SN=Jean, G=DUPONT, serialNumber = c36f37bc6fc9315651ad5426bb437f77d841c888}

3.1.3 Pseudonymisation des porteurs

Les pseudonymes ne sont pas autorisés.

3.1.4 Règles d'interprétation des différentes formes de noms

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

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

- tous les caractères sont au format printableString ou en UTF8String i.e. sans accents ni caractères spécifiques à la langue française et de manière conforme au standard X.501 ;
- les prénoms et noms composés sont séparés par des tirets " - ".

3.1.5 Unicité des noms

L'unicité du DN est garantie par l'unicité des informations permettant de construire ce dernier : nom et prénom du Porteur et l'identifiant unique de la transaction de signature présent dans le champ « serialNumber ».

3.1.6 Identification, authentification et rôle des marques déposées

L'AE limite ses vérifications concernant le droit d'utiliser un nom à la vérification des informations contenues dans les pièces d'identité.

3.2 Validation initiale de l'identité

L'enregistrement d'un Porteur se fait directement auprès de l'AE. Le porteur doit pouvoir présenter un justificatif d'identité qui sera analysé par l'AE ou un sous-traitant prestataire de vérification d'identité en contrat avec l'AE.

3.2.1 Méthode pour prouver la possession de la clé privée

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

3.2.2 Validation de l'identité d'un organisme

Sans objet

3.2.3 Validation de l'identité d'un individu

Dans le cadre de la présente Politique de Certification, on entend par justificatif d'identité, un document délivré par une autorité administrative comportant la photographie, le(s) nom(s), le(s)

prénom(s), la date et le lieu de naissance du titulaire, ainsi qu'un numéro unique et une date de délivrance. Sont notamment acceptés : la carte nationale d'identité française, le passeport et la carte de séjour délivrée par les autorités françaises, sous réserve que ces documents soient en cours de validité.

La pièce d'identité est analysée automatiquement par l'AE, ou par son sous-traitant prestataire de vérification d'identité, pour extraire les informations requises :

- Nom et prénom du demandeur
- Type de pièce d'identité
- Numéro de pièce d'identité
- Pays de délivrance

Ces informations serviront à enregistrer la demande de certificat qui doit être accompagnée :

- du rapport de vérification de l'AE. Ce dernier reprend les éléments ci-dessus ainsi que le rapport de vérification de la pièce d'identité
- les CGUs signées du service

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

3.2.4 Informations non vérifiées du porteur

sans objet.

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.

3.2.6 Certification croisée d'AC

Sans objet. L'AC CertEurope eID User n'a aucun accord de reconnaissance avec une autre AC.

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

Sans objet.

3.4 Identification et validation d'une demande de révocation

Sans objet. La durée de vie du certificat est inférieure au délai de traitement d'une demande de révocation. Le porteur lorsqu'il ne valide pas les informations présentées lors du parcours de signature, annule la transaction, il n'y a donc pas de 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 une AE au nom d'un Utilisateur dans le cadre d'un service ou processus métier de signature électronique qu'il propose à ses Utilisateurs.

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

L'établissement de la demande de Certificat est effectué par l'AE via son Service d'enregistrement en ligne, ou celui de son sous-traitant, lequel transmet automatiquement la demande, si elle est correcte, à la fonction adéquate de l'AC pour la génération du certificat.

La connexion établie entre le système d'information de l'AE (ou de son prestataire sous-traitant) et celui de l'AC est sécurisée grâce à un système d'authentification mutuelle, basée sur l'utilisation de Certificats électroniques, qui permet d'identifier les parties, de chiffrer le canal de communication, et de faire des vérifications d'intégrité des flux échangés.

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

- le nom, prénom du porteur à utiliser dans le certificat ;
- Les données personnelles d'identification du porteur : adresse email, numéro de téléphone mobile

Une référence unique et associée à la transaction de signature par l'AC si la demande de certificat est conforme.
Pour les certificats « usage entreprise » :

- Numéro d'immatriculation de la structure juridique de rattachement du porteur (numéro de TVA communautaire, ou numéro SIREN en France),
- La raison sociale de la structure juridique.

4.2 Traitement d'une demande de certificat

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

L'AE effectue les opérations suivantes :

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

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat vers la fonction adéquate de l'IGC (cf. § 1.3.1).

L'AE transmet à l'AC les pièces énumérées dans la procédure d'archivage; en particulier l'AC conserve un exemplaire des CGUs signée par le futur porteur ainsi que le dossier de preuve avec la validation de la pièce d'identité du porteur.

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le porteur par email en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

Le délai de génération d'un certificat une fois la demande validée est immédiate.

4.3 Délivrance de certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Lorsqu'une demande de certificat a été validée par le service d'enregistrement de l'AE, l'AE procède à la demande de certificat au service de génération de l'AC.

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. Un code OTP est envoyé au porteur par SMS sur le numéro renseigné lors de la commande.

Le Certificat est destiné à un usage unique (durée de vie limitée au maximum à 1 heure).

Le Bi-clé est généré dans le SCD (Signature Création Device). La section 6.2.1 « Standards et mesures de sécurité pour le SCD et précise les caractéristiques des modules utilisés pour générer et stocker la Bi-clé de signature.

Les informations sur le certificat (nom et prénom), sont présentés à l'Utilisateur lors de la validation de la transaction de signature. Il les accepte en cochant la case des CGUs et en validant le code OTP envoyé par SMS.

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

Le certificat public est délivré au Porteur par téléchargement dans son navigateur du document signé. Le bi-clé est détruit immédiatement après l'opération de signature.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'acceptation du Certificat par l'Utilisateur est explicite : les informations du Certificat lui sont présentées en ligne après consultation des documents ou informations à signer et acceptation des Conditions générales d'utilisation du Service :

- En cas d'acceptation, le Certificat et le Bi-clé de signature de l'Utilisateur sont utilisés pour signer les documents présentés par le Client ;
- En cas de refus, la Transaction de signature est annulée. Le certificat n'ayant pas été encore généré, nul besoin de le révoquer.

4.4.2 Publication du certificat

Les certificats des porteurs 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, le document signé est délivré au Porteur par téléchargement dans son navigateur, après authentification.

L'AE est avertie par API de l'aboutissement de la demande de signature.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de « Signature ».

La clé privée est détruite à l'issue de la transaction de signature, ainsi aucun autre usage n'est possible.

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

Cf. section précédente.

4.6 Renouvellement d'un certificat

Sans objet.

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

Sans objet.

4.7.1 Causes possibles de changement d'une bi-clé

Sans objet.

4.7.2 Origine d'une demande d'un nouveau certificat

Sans objet.

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

Sans objet.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.7.5 Démarche d'acceptation d'un nouveau certificat

Sans objet.

4.7.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

4.8 Modification du certificat

La modification de Certificat de l'AC CertEurope eID User 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 porteur de l'établissement du certificat modifie

Sans objet.

4.8.5 Démarche d'acceptation du certificat modifie

Sans objet.

4.8.6 Publication du certificat modifie

Sans objet.

4.8.7 Notification par l'AC aux autres entités de la délivrance du certificat modifie

Sans objet.

4.9 Révocation et suspension de certificat

Un Certificat de l'AC CertEurope eID User 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 de porteurs

S'agissant de certificat éphémère utilisés exclusivement lors de la transaction de signature, la durée de validité du certificat (1h) est inférieure au délai de traitement d'une demande de révocation (24h).

Le porteur n'a donc pas la possibilité de demander la révocation du certificat après avoir vérifié ses informations (nom et prénom) et validé la transaction de signature en renseignant le code OTP transmis par SMS.

Cependant, l'AC peut révoquer les certificats encore valides si elle détecte une attaque une anomalie ou une incohérence dans les demandes envoyées par l'AE.

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 PC/DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

4.9.2 Origine d'une demande de révocation d'un certificat porteur

4.9.2.1 Certificats de porteurs

Le Porteur ne peut demander la révocation du certificat car sa durée de validité est inférieure à la durée de traitement d'une demande de révocation.

L'AC peut néanmoins révoquer les certificats encore valides si elle détecte une attaque une anomalie ou une incohérence dans les demandes envoyées par l'AE.

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 de porteur

Le délai de traitement d'une demande de révocation est supérieur à la durée de validité du certificat. Par conséquent, il n'est pas possible pour le porteur de demander la révocation de son certificat de signature.

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 la PC/DPC (Cf. § 5.8)

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

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

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Sans objet.

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

4.9.5.1 Révocation d'un certificat de porteur

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

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

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

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

Le délai de publication de la révocation d'un Certificat n'excède jamais 24 heures à partir de la réception de la demande de révocation.

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

Le porteur déclenche une transaction de signature qui provoque la génération d'un certificat éphémère (short-term). Ce dernier est utilisé pour signer les documents présentés à l'utilisateur. Le processus de signature vérifie le statut de chaque certificat de la chaine de confiance, jusqu'à la racine. Il s'appuie alors sur les points de distributions de la CRL ou à défaut sur les serveurs OCSP.

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

Deux services OCSP sont décrits dans le gabarit des certificats. L'un sur le site principal et l'autre sur le secondaire. En cas d'indisponibilité des deux services, le client peut s'appuyer sur les points de distributions de la LCR.

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

Cf. § 4.9.6 ci-dessus.

4.9.11 Autres moyens disponibles d'information sur les révocations

L'utilisateur peut utiliser un outil de vérification des signatures qui pourra confirmer que le certificat qui a servi à signer est toujours valide.

4.9.12 Exigences spécifiques en cas de révocation pour compromission de clé

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

En cas de compromission de la clé privée de l'AC, l'information de la révocation du certificat est diffusée sur le site de CertEurope : https://www.certeurope.fr.

Par conséquent, l'accès au portail de demande de certificat en ligne devient indisponible.

Voir § 4.9.3.2.

4.9.13 Causes possibles d'une suspension

Sans objet.

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".

Deux services OCSP sont décrits dans le gabarit des certificats. L'un sur le site principal et l'autre sur le secondaire.

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 2h et une durée maximale totale d'indisponibilité par mois de 8h.

4.10.3 Dispositifs optionnels
Sans objet.

4.11 Fin de la relation avec le porteur
En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et le porteur avant la fin de validité du certificat, ce dernier est révoqué.

4.12 Séquestre de clé et recouvrement
L'AC interdit le séquestre des clés des porteurs.

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 eID User.

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 eID User 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 eID User.

5.1.4 Vulnérabilité aux dégâts des eaux

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

Des procédures spécifiques sont prévues pour la prévention du patrimoine notamment en matière de dégâts du feu sur le site de l'Hébergeur.

Les exigences sont contractuellement précisées dans les contrats d'infogérance « [3] CertEurope – Contrat Colt ».

Les AE s'engagent à archiver les documents dans un environnement offrant des garanties équivalentes

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 opérations effectuées par les AE sont automatiquement enregistrées dans le journal d'audit de la plate-forme CertEurope. Par conséquent, elles sont archivées par l'AC.

Les médias stockés par l'Hébergeur (bandes magnétiques) sont protégés contre tout excès de température, d'humidité et de rayonnement magnétique. Les mesures prises sont décrites dans le document « [7] CertEurope – Cycle de vie des supports de données ».

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.

Tous les supports servant au stockage des informations sensibles de l'AC sont effacés ou détruits avant leur mise au rebut. Voir les documents « [2] CertEurope – Procédures d'exploitation de l'ICP CertEurope » et « [7] CertEurope – Cycle de vie des supports de données ».

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. Conformément à son PRA, CertEurope sauvegarde les données de production sur ses deux sites.

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

Voir [2] CertEurope – Procédures d'exploitation de l'ICP CertEurope » rubrique « [8] CertEurope – Procédure de sauvegarde »

5.2 Mesures de sécurité procédurales

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 et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats.

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 des rôles sont détaillées dans les documents « [11] Contrat – AE ».

5.2.2 Nombre de personnes requises par tâches

Selon la tâche à effectuer, une ou plusieurs personnes doivent être présentes lors de l'exécution de la tâche.

Le tableau ci-dessous décrit le nombre de personnes requises par tâche :

Opération	Acteur de l'opération	Entité bénéficiaire de l'opération	Autorisations requises			
			Porteurs de secrets Certeurope	Porteurs de secrets OC	Nombre d'OP	Nombre d'ADM
Génération de bi-clé et certificat	AC RACINE	AC	0	0	0	2
	AC	AE	0	0	1	2
	AC	UF	0	0	1	0
Modification configuration des profils de l'AC	AC	AC,UF	0	0	0	2
Stockage et restauration de clé privée	AC	AC	2	1	0	0
Révocation de certificat	AC RACINE	AC	0	0	0	2
	AC	AE	0	0	1	2
	AC	UF	0	0	1	0
Contrôle des journaux d'événements	AC	*	0	0	0	1

5.2.3 Identification et authentification pour chaque rôle

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

Les procédures d'attributions des rôles sont détaillées dans le document « [1] CertEurope - Procédures de sécurité de l'ICP CertEurope ».

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 conformes à la politique de sécurité de la composante concernée.

5.3 Mesure 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, avant leur prise de fonction et sur simple demande.

Les personnes ayant un rôle de confiance ne souffrent d'aucun conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

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.

Documents de référence : « [9] CertEurope – Charte Informatique » et « [10] CertEurope – Règlement Intérieur ».

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

5.4 Procédure 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 ;
- 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 éléments secrets du porteur (codes d'activation,…) ;
- génération des certificats des porteurs ;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- génération puis publication des LCR.

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

5.4.2 Fréquence de traitement des journaux d'évènements

Cf. § 5.4.8.

5.4.3 Période de conservation des journaux d'évènements

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'évènements

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 § 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.

Les journaux d'événements sont sauvegardés selon la procédure décrite dans le manuel « [1] CertEurope - Procédures de sécurité de l'ICP CertEurope ». Une copie de ces journaux est également envoyée à la société CertEurope, cet envoi est réalisé via le réseau Internet et utilise des méthodes de chiffrement robustes pour protéger la confidentialité des données.

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. Cf procédure de « [8] CertEurope – Procédure de sauvegarde ».

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/DPC ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les engagements signés des MC ;
- les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

Le détail de toutes les données à archiver et leur période de rétention est fourni dans le document « [6] CertEurope – Inventaire ICP ».

La plupart des données électroniques sont conservés pendant 7 ans (cf. « [6] CertEurope – Inventaire ICP »)
Toute version antérieure à la version courante de la PC/DPC est conservée selon la procédure d'archivage pour une durée de 7 ans ;

Dossiers de demande de certificat

Chaque dossier de demande de Certificat et ses pièces justificatives est archivé par l'AC pendant une durée de sept (7) ans à compter de la date d'expiration du certificat.

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

Le dossier de demande de Certificat et des pièces justificatives est détruit au terme de la période d'archivage.

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 sept (7) ans à compter de la date d'expiration du certificat.

Journaux d'évènements

Les journaux d'évènements sont archivés pendant sept (7) 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. § 5.4.4 pour la datation des journaux d'évènements.

Le § 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 20 ans.

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 Porteurs émis ainsi que la LCR.

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

5.7 Reprise suite a 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 porteurs 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.

La procédure est détaillée dans le document « [4] CertEurope – Plan de Continuité ».

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.

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 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.

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. § 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 porteurs et autres composantes de l'IGC,
  - la communication vers les utilisateurs de certificats,
  - la révocation des certificats du personnel habilité.
- Communiquer le plan d'actions et tout changement pendant le déroulement du transfert au contact identifié sur le site www.ssi.gouv.fr.

Composante OC

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

En particulier, L'AC s'assurera de :

- Réaliser un plan d'actions et le confronter à l'analyse de risques de l'AC : en particulier, le plan d'action devra traiter du :
  - transfert des archives sous la responsabilité de l'OC,
  - transfert des fonctions assurées par l'OC,
  - la continuité de services lors du transfert,
  - Transfert des clés de l'AC hébergées par l'OC,
  - suppression des habilitations de l'OC sur la révocation d'urgence,
  - modification du référentiel documentaire de l'AC : PC, DPC, ..
  - la formation du personnel habilité de l'AC,
  - la communication vers les autres composantes de l'IGC,
  - la communication vers les porteurs et utilisateurs de certificats,
- Communiquer le plan d'actions et tout changement pendant le déroulement du transfert au contact identifié sur le site www.ssi.gouv.fr.

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 porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. § 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.

La cessation d'activité est détaillée plus précisément dans le document « [4] CertEurope – Plan de Continuité ».

Après terminaison d'une de ses AC, CertEurope, en accord avec les exigences de la norme ETSI EN 319 411-1/2, publiera une dernière CRL en assignant la valeur "99991231235959Z" au champ "nextUpdate", sauf exigences complémentaires de l'organe de supervision national (ANSSI).

Les informations sur le statut de révocation (CRL et OCSP) seront disponibles au moins 5 ans après la terminaison de l'AC.

La fin de vie fait l'objet d'une information clairement diffusée au moins sur le site de CertEurope et éventuellement relayée par d'autres moyens (associations, clubs utilisateur, réseaux sociaux, etc.).

En plus des éventuelles recommandations de l'ANSSI, CertEurope doit :

Informer tous les Porteurs, Mandataires de Certification et les autres entités en lien avec l'AC (plateforme de marché, fournisseurs d'identités, etc.)

6 Mesure de sécurité technique

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 eID User est effectuée dans un environnement sécurisé (cf. § 5).

Les clés de signature d'AC CertEurope eID User sont générées lors de la cérémonie des clés et mises en œuvre dans un module cryptographique conforme aux exigences du l'Annexe 2 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. Elle est effectuée par au moins deux personnes ayant des rôles de confiance (cf. § 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 eID User sont générées dans le module cryptographique de l'AC CertEurope eID Root 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 porteurs générées par l'AC

Le bi-clé du Porteur est généré par l'AC dans un module cryptographique conforme aux exigences de l'Annexe 2 de la présente PC. La clé privée est supprimée du module cryptographique immédiatement après la signature du document.

6.1.1.3 Clés porteurs générées par le porteur

Sans objet.

6.1.2 Transmission de la clé privée a son propriétaire

La clé privée n'est jamais transmise.

6.1.3 Transmission de la clé publique a l'AC

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

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

La clé publique de 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.

Le certificat de l'AC est disponible sur le site https://www.certeurope.fr/chaine-de-confiance.

6.1.5 Tailles des clés

Les clés RSA des Porteurs 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 eID User est de 4096 bits.

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

La bi-clé du porteur est générée par un module cryptographique matériel. Ce module répond aux exigences de l'Annexe 2.

La bi-clé de l'AC (pour la signature de certificats et de CRLs) est générée et protégée par un module cryptographique matériel. Ce module répond aux exigences de l'Annexe 2.

La génération ou le renouvellement de la bi-clé de l'AC par ce module nécessite la présence d'au moins 2 personnes.

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée de l'AC CertEurope eID User et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (cf. § 7).

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de de signature comme précisé dans le document (cf. § 7).

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

6.2.1 Standards et mesures de sécurité pour les modules

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+. Par conséquent, ils répondent aux exigences de l'Annexe 2 du présent document.

6.2.1.2 Dispositifs d'authentification et de signature des porteurs

Sans objet.

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 2 exploitants parmi 5 doivent s'authentifier).

6.2.3 Séquestre de la clé privée

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

6.2.4 Copie de secours de la clé privée

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

La clé privée de l'AC fait l'objet de copie de secours sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Ces copies de secours bénéficient du même niveau de sécurité que la clé privée originale.

Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique et nécessitent l'intervention de 2 porteurs de secrets.

6.2.5 Archivage de la clé privée

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

Les clés privées des porteurs 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 porteurs sont générées dans le SSCD avant d'être exportées pour effectuer la transaction de signature. Elles sont supprimées immédiatement après l'opération de signature.

Pour les clés privées d'AC, tout transfert se fera sous forme chiffrée, conformément aux exigences du § 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 de l'Annexe 2 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 deux porteurs de secrets et permet de répondre aux exigences définies dans l'Annexe 2 pour le niveau de sécurité considéré.

6.2.8.2 Clés privées des porteurs

Les clés privées des porteurs sont utilisées pour signer des documents immédiatement après la validation de la commande et la saisie d'un code à usage unique. Ses clés sont systématiquement détruites.

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 l'Annexe 2 pour le niveau de sécurité considéré.

6.2.9.2 Clés privées des porteurs

L'Utilisateur ne pourra pas activer la clé privée s'il n'est pas capable de fournir le code d'activation qui l'autorise à déclencher la transaction de signature.

La désactivation de la clé a lieu à l'issue de la Transaction de signature (ou après écoulement du délai de signature) par le biais de la destruction du Bi-clé de signature. Cette destruction a lieu quel que soit l'état final de la transaction.

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 porteurs

Aucune exigence particulière car ces clés sont supprimées immédiatement après l'opération de signature, ou à échéance du délai autorisé pour la signature.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques de l'AC sont évalués au niveau EAL4+, correspondant à l'usage visé, tel que précisé au l'Annexe 2 ci-dessous.

Les modules cryptographiques (SCD) servant à générer les bi-clés des porteurs sont évalués au niveau EAL4+, correspondant à l'usage visé, tel que précisé l'Annexe 2 ci-dessous.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durée de vie des bi-clés et des certificats

La durée de vie des bi-clés et des certificats porteurs fournis dans le cadre de l'AC CERTEUROPE sont d'une heure.

La durée de vie de la bi-clé et du certificat de l'AC CertEurope eID User est de 20 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 porteur

Sans objet car une fois la bi-clé activée, les documents sont signés puis la bi-clé est détruite.

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 porteurs

Sans objet.

6.4.3 Autres aspects lies aux données d'activation

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

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

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

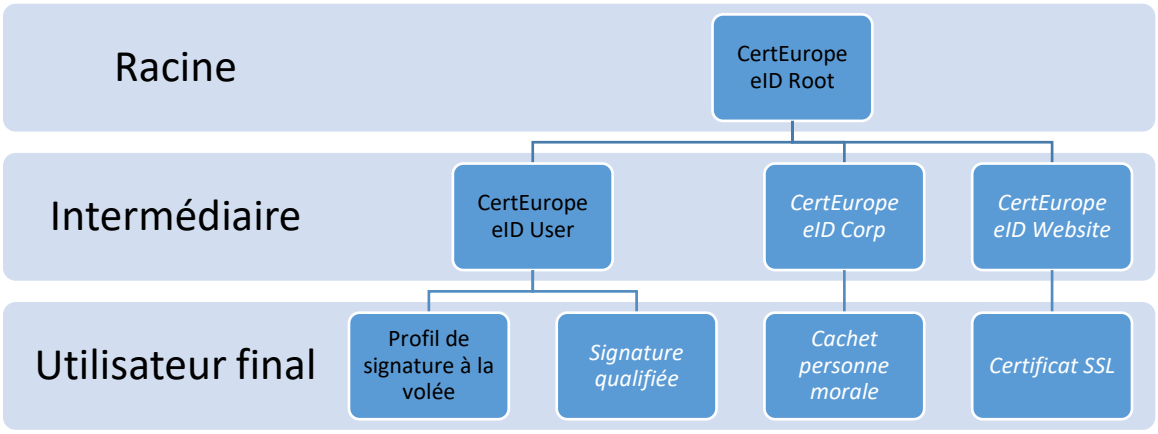
6.8 Horodatage / Système de datation

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

Ci-dessous un schéma qui décrit la hiérarchie complète des AC.



7.1 Profils des certificats des Autorités de Certifications

7.1.1 CertEurope eID Root

Certificat de l'AC racine dont découle les AC qualifiées EIDAS et certifiées (uniquement ETSI) pour les personnes physiques, les personnes morales et les serveurs web. Etant une racine auto-signée, la RFC 5280 n'impose pas la présence du champ *AuthorityKeyIdentifier* dont la valeur serait dupliquée avec le champ *SubjectKeyIdentifier.*

Le champ *Organizationidentifier (2.5.4.97)*, reprend la nomenclature de l'ANSSI (**SI:FR**) suivi du numéro de SIREN de CertEurope : **SI:FR-434202180**

Le champ *OrganizationUnitName*, reprend les exigences du RGSv2 en spécifiant l'identifiant ICD pour la France (0002) avant le SIREN de CertEurope : **0002 434202180**

La valeur de ces deux champs est la même pour l'AC Racine ainsi que les AC intermédiaires (User, Corp et Website).

La colonne « C » indique si le champ est critique (O) ou non (N).

CertEurope eID Root		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 20 ans
SubjectPublicKeyInfo		La clé publique avec une longueur de 4096 bits (RSA)
Issuer		
CountryName		FR
CommonName		CertEurope eID Root
OrganisationName		CertEurope
OrganizationUnitName		0002 434202180

CertEurope eID Root		
OrganizationIdentifier		SI:FR-434202180
Subject		
CountryName		FR
CommonName		CertEurope eID Root
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Extensions		
KeyUsage	***O***	
keyCertSign		Set
crlSigning		Set
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		None

7.1.2 CertEurope eID User

Certificat intermédiaire pour l'AC des personnes physiques.

CertEurope eID User		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 20 ans
SubjectPublicKeyInfo		La clé publique avec une longueur de 4096 bits (RSA)
Issuer		
CountryName		FR
CommonName		CertEurope eID Root
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganisationIdentifier		SI:FR-434202180
Subject		
CountryName		FR
CommonName		CertEurope eID User
OrganisationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Extensions		
KeyUsage	***O***	
keyCertSign		Set
crlSigning		Set
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.22.1.1.0 (CertEurope eID Root)

CertEurope eID User		
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
CRL Distribution Point	***N***	URL(s) de distribution de la CRL de l'AC racine avec au moins une URL avec le protocole HTTP.
Authority Information Access	***N***	Renseignement de l'extension « Authority Information Access »: - accessMethod OID avec id-ad-caIssuers - accessLocation URL http de téléchargement du certificat de l'AC : http://www.certeurope.fr/reference/eid_root.crt Un répondeur OCSP est mis en œuvre pour respecter les bonnes pratiques décrites par le CA/B Forum : - accessMethod OID avec id-ad-ocsp - accessLocation URL d'accès au répondeur OCSP de l'AC : http://ocsp.certeurope.fr/root/
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice (eID Root)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		0 (Zéro)

7.2 Profils des certificats pour personnes physiques

7.2.1 Les champs communs aux certificats pour personnes physiques

Champ	C	Valeur
Subject		
countryName		Pays de résidence du demandeur
serialNumber		Elément complémentaire permettant de distinguer les homonymes. Il s'agit de l'identifiant unique de la transaction de signature.
givenName		Le premier prénom, le prénom d'usage, ou les prénoms de l'état civil du porteur
surname		Nom de l'état civil ou le nom d'usage du porteur
commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications. Il est composé du prénom d'usage du porteur, suivi d'un espace, suivi du nom de l'état civil ou du nom d'usage du porteur.
Extensions		
KeyUsage	***O***	Voir pour chaque profil décrit plus bas
CertificatePolicies	***N***	Voir pour chaque profil décrit plus bas
CRL Distribution Point	***N***	URL(s) de distribution de la CRL de l'AC CertEurope eID User
Authority Information Access	***N***	URL(s) du service OCSP de l'AC CertEurope eID User
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice (eID User)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		Faux

7.2.2 CertEurope eID User – Signature éphémère

Profils de certificats conformes à la norme ETSI EN 319 411-1 niveau LCP. La validation de l'identité se fait via la vérification automatique de la pièce d'identité du porteur par un prestataire qui respecte les exigences de l'AC. La durée de vie du certificat est assez courte et la bi-clé est détruite à la fin de la transaction de signature.

Champ	C	Signature
LCP		
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.23.411.1.**6**.1.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation
Extended Key Usage	***N***	NA

7.3 Profil des LCR

7.3.1 Champs des LCR

Champs de base	Valeur
Version	Version 2
Signature	Sha256WithRSAEncryption (2.16.840.1.101.3.4.2.1)
Hash	sha256
Issuer DN	Selon l'émetteur de chaque AC décrite plus haut
This Update	Au plus tôt à la date de début de vie de l'AC
Next Update	Prochaine date à laquelle la CRL sera mise à jour, soit 6 jours après la date de génération de la présente CRL.
Revoked Certificates	N° de série des certificats révoqués. Exemple : « 0C0062 »
Revocation Date	Date à laquelle un Certificat donné a été révoqué.

7.3.2 Extensions des LCR

Champ	O	C	Valeur
Authority Key Identifier	TRUE	FALSE	ID de la clé=voir la clé de chaque AC décrite plus haut
CRL Number	TRUE	FALSE	N° de série de la CRL Exemple : « 0115 »
ExpiredCertsOnCRL	FALSE	FALSE	Date à partir de laquelle les certificats expirés sont conservés dans la CRL. CertEurope conserve l'ensemble des certificats expirés dans la CRL. La date fixe correspond à une journée après la création des AC de la chaine eID, soit le 15 novembre 2016 (20161115000000Z)

7.4 Protocole de vérification de certificat en ligne (OCSP)

Bien que les exigences complémentaires n'imposent pas la mise en place d'un répondeur OCSP, la version 2 du RGS l'impose. C'est aussi une obligation du CA/B Forum.

Les réponses OCSP doivent se conformer à la RFC6960 et / ou RFC5019. Ainsi, il y a deux possibilités :

1. Être signé par l'AC qui a délivré les certificats dont le statut de révocation est vérifié, ou
1. Être signé par un répondeur OCSP dont le certificat est signé par l'AC qui a délivré le certificat dont l'état de révocation est vérifié.

Dans ce dernier cas, le certificat de signature OCSP doit contenir une extension de type id-pkix-ocsp-nocheckx.

L'AC intermédiaires eID User ne signe donc pas les réponses OCSP et par conséquent ne contiennent pas le keyUsage digitalSignature comme préconisé par le RGS qui reprend les préconisations du CAB Forum.

7.5 Les champs communs aux certificats de signature OCSP

Chaque AC intermédiaire possède son propre serveur OCSP. Les bi-clés pour chaque AC ont une durée maximum de validité d'un an.

CertEurope eID OCSP		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		2048 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		Maximum 1 an
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 1 an au maximum
SubjectPublicKeyInfo		La clé publique avec une longueur de 2048 bits (RSA)
Issuer		
CountryName		FR
CommonName		CertEurope eID Root
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Subject		
CountryName		FR
CommonName		Chaque AC intermédiaire possède son propre serveur/certificat OCSP : • CertEurope eID OCSP Root • CertEurope eID OCSP User
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
Extensions		
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC

7.6 Les profils des certificats OCSP

Champ	C	eID OCSP Root	eID OCSP User
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.22.6960.1.0	1.2.250.1.105.23.6960.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	digitalSignature	
Extended Key Usage	***N***	OCSP Signing with no-check	

La date définie dans le champ « ExpiredCertsOnCRL » est présente dans chaque réponse OCSP dans l'extension « ArchiveCutOff » (OID : 1.3.6.1.5.5.7.48.1.6) : le 15 novembre 2016, date de création de la chaine d'AC eID.

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 la PC/ 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.

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 à aucune autre 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/DPC de l'AC 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/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 eID User 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 données d'identification ou autres informations personnelles du Porteur contenues dans son certificat, sauf
  - si le Porteur a donné explicitement son consentement préalablement à la publication du Certificat ;
  - si leur publication a été demandée sur décision judiciaire ou administrative ;
- les causes de révocations des Certificats ;
- les journaux d'événements des composantes de l'ICP CERTEUROPE ;
- le dossier de demande de certificat du Porteur, et notamment les données personnelles (à l'exception des informations à caractère personnel contenues dans les Certificats) ;
- les rapports d'audit ;

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 PC/DPC, pour répondre aux exigences légales ou pour l'exécution de travaux ou de prestations de services confiés à des prestataires.

Les informations recueillies sont indispensables à CertEurope pour la mise en place et la gestion du Service. Le Porteur autorise expressément CertEurope à traiter en mémoire informatisée les données les concernant conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée, et à les communiquer à ses sous-traitants ou à ses partenaires dans le respect des Conditions Générales du contrat d'abonnement au Service C@rteurope et de sa finalité. Le Porteur peut, pour des motifs légitimes, s'opposer à ce que ces données fassent l'objet d'un traitement. Pour exercer leurs droits d'accès, de rectification ou d'opposition, le Porteur doivent s'adresser par écrit à : CertEurope, Correspondant Informatique et Libertés 41, rue de l'échiquier, 75010 Paris. Toute demande doit être accompagnée d'un justificatif d'identité en cours de validité.

La clé privée du Porteur est supprimée immédiatement après la signature des documents.

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 le règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit « Règlement Général sur la Protection des Données [RGPD]..

9.4.2 Informations à caractère personnel

Pour l'AC CertEurope eID User, les informations à caractère personnel sont les informations nominatives du porteur enregistrées au sein du dossier d'enregistrement. Il s'agit notamment des informations nom / prénom / adresse / téléphone / fonction / email.

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

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

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/DPC 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.

9.6.1 Autorités de certification

L'AC CertEurope eID User garantit le respect des exigences définies dans la présente PC/DPC. 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 œuvre ses certificats.
- S'assurer que les exigences et procédures de la PC/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.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC/DPC notamment en matière de génération des certificats, remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC/DPC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats.

L'AC CertEurope eID User a pour obligation de :

- pouvoir démontrer aux applications utilisatrices de ses certificats, qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément au § 4.4 ;
- tenir à disposition des Porteurs et des Utilisateurs, la liste des certificats ayant fait l'objet d'une révocation; cette liste est publiée sous la forme d'une LCR ;
- s'assurer que ses Porteurs connaissent leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des Certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'ICP.

La relation entre un Porteur et l'AC CertEurope eID User 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 Porteur;
- transmettre la demande de certificat au service de génération des certificats.

L'AE ne peut être saisie d'une demande de révocation dans le cas des certificats éphémère car la durée de celui-ci est inférieure au délai de traitement de la demande révocation.

L'AE doit transmettre à l'AC toutes les pièces du dossier d'enregistrement des porteurs suivant les modalités décrites dans cette PC/DPC et conformément aux procédures mises en œuvre de manière dérogatoire.

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

9.6.3 Porteurs de certificats

Le porteur a le devoir de :

- communiquer des informations exactes lors de la demande de certificat ;
- informer l'AC ou l'AE CERTEUROPE en cas de modifications de ces informations ;
- respecter les conditions d'utilisation de sa clé privée et du Certificat correspondant ;

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

9.6.4 Utilisateurs de certificats

Les Applications utilisatrices et Utilisateurs de Certificats doivent :

- respecter l'usage pour lequel un Certificat a été émis ;
- vérifier la signature numérique de l'AC CertEurope eID User émettrice du Certificat ainsi que celle de l'AC Certeurope eID Root ;
- 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. 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/DPC est soumise au Droit français.

Les parties s'efforceront de régler à l'amiable tout litige concernant l'interprétation ou l'exécution du contrat dans les meilleurs délais. 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.

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. § 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.

Annexe 1. Documents cités en référence

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 le 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.

Documents techniques

DOCUMENTS REFERENCES		
Date	Version	Commentaires
[ETSI_CERT]	1.3.1	ETSI EN 319 411-1
[CERT_PSSI]	1.0	CertEurope : Politique de Sécurité

Documents références

[1] CertEurope - Procédures de sécurité de l'ICP CertEurope

[2] CertEurope – Procédures d'exploitation de l'ICP CertEurope

[3] CertEurope – Contrat Colt

[4] CertEurope – Plan de Continuité

[5] CERTEUROPE – Rôles et habilitations

[6] CertEurope – Inventaire ICP

[7] CertEurope – Cycle de vie des supports de données

[8] CertEurope – Procédure de sauvegarde

[9] CertEurope – Charte Informatique

[10] CertEurope – Règlement Intérieur

[11] Contrat – AE

[12] Exigences techniques – AE

Annexe 2. Exigences de sécurité du dispositif de signature

Exigences sur les objectifs de sécurité

Sans objet

Exigences sur la certification

Le dispositif de signature utilisé doit être conforme aux exigences du référentiel ETSI EN 319 411-1.

Annexe 3. Listes des applications utilisatrices autorisées

Les certificats CERTEUROPE sont utilisables dans toutes les applications qui implémentent les normes de signature avancée (PAdES, XAdES, CAdES et ASiC).

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