ORDRE DES EXPERTS-COMPTABLES

Conseil Supérieur

jesignexpert.com

Déclaration des pratiques de certification – Signature avancée

Version 1.05

octobre 2018

OID nº 1.2.250.1.165.1.13.1.1

HISTORIQUE DES VERSIONS

Date	Évolutions	Edition / révision
Juillet 2018	Version préliminaire	0.1
Septembre 2018	Pour publication	1.0
Octobre 2018	Révision post-audit	1.05

Contributeurs	Organisation
Samuel LACAS	SEALWeb

TABLE DES MATIÈRES

I Introduction 5
I.1 Présentation générale 5
I.2 Identification du document 5
I.3 Entrée en vigueur du document 5
I.4 Entités intervenant dans l'I.G.C. et responsabilités 5
I.5 Usage des certificats 8
I.6 Gestion de la DPC 9
I.7 Définitions et abréviations 9
II Responsabilités concernant la mise à disposition des informations devant être publiées 13
II.1 Entités chargées de la mise à disposition des informations 13
II.2 Informations devant être publiées 13
II.3 Délais et fréquences de publication 13
II.4 Contrôle d'accès aux informations publiées 13
III Identification et authentification 14
III.1 Nommage 14
III.2 Validation initiale de l'identité de la structure professionnelle d'exercice du porteur 15
III.3 Identification et validation d'une demande de délivrance d'un certificat suite au changement de biclé 16
III.4 Identification et validation d'une demande de révocation 17
IV Exigences opérationnelles sur le cycle de vie des certificats 18
IV.1 Demande de certificat 18
IV.2 Traitement d'une demande de certificat 18
IV.3 Délivrance du certificat 19
IV.4 Acceptation du certificat 19
IV.5 Usages de la biclé et du certificat 19
IV.6 Renouvellement d'un certificat 19
IV.7 Modification du certificat 19
IV.8 Révocation et suspension des certificats 20
IV.9 Fonction d'information sur l'état des certificats 22
IV.10 Fin de la relation entre le porteur et l'AC 22
IV.11 Séquestre de clé et recouvrement 22
IV.12 Certificats de test 23
V Mesures de sécurité non techniques 24
V.1 Mesures de sécurité physique 24
V.2 Mesures de sécurité procédurales 25
V.3 Mesures de sécurité vis-à-vis du personnel 26
V.4 Procédures de constitution des données d'audit 26
V.5 Archivage des données 28
V.6 Changement de clé d'A.C. 30
V.7 Reprise suite à compromission et sinistre 30
V.8 Fin de vie de l'I.G.C. 30
VI Mesures de sécurité techniques 32
VI.1 Génération et installation de biclés 32
VI.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 32
VI.3 Données d'activation 34
VI.4 Mesures de sécurité des systèmes informatiques 35
VI.5 Mesures de sécurité liées au développement des systèmes 35
VI.6 Mesures de sécurité réseau 35
VI.7 Horodatage / Système de datation 35

VII Profils des certificats, OCSP et des LCR 36
VII.1 Certificats de porteurs 36
VII.2 Certificat d'A.C. 37
VII.3 Liste de Certificats Révoqués 37
VII.4 Certificat des réponses OCSP 38
VIII Audit de conformité et autres évaluations 39
VIII.1 Fréquences et / ou circonstances des évaluations 39
VIII.2 Identités / qualifications des évaluateurs 39
VIII.3 Relations entre évaluateurs et entités évaluées 39
VIII.4 Sujets couverts par les évaluations 39
VIII.5 Actions prises suite aux conclusions des évaluations 39
VIII.6 Communication des résultats 39
IX Autres problématiques métiers et légales 40
IX.1 Tarifs 40
IX.2 Responsabilité financière 40
IX.3 Confidentialité des données professionnelles 40
IX.4 Protection des données personnelles 41
IX.5 Droits sur la propriété intellectuelle et industrielle 41
IX.6 Interprétations contractuelles et garanties 41
IX.7 Limite de garantie 41
IX.8 Limite de responsabilité 41
IX.9 Indemnités 41
IX.10 Durée et fin anticipée de validité de la DPC 41
IX.11 Notifications individuelles et communications entre les participants 42
IX.12 Amendements à la DPC 42
IX.13 Dispositions concernant la résolution de conflits 42
IX.14 Juridictions compétentes 42
IX.15 Conformité aux législations et réglementations 42
IX.16 Transfert d'activités 42
X Annexe 1 : Documents cités en référence 43
X.1 Législation et réglementation 43
X.2 Documents techniques 43
XI Annexe 2 : Exigences de sécurité du module cryptographique de l'A.C. 44
XII Annexe 3 : Exigences de sécurité du dispositif de création de signature 45
XII.1 Exigences sur les objectifs de sécurité 45
XII.2 Exigences sur la qualification 45

I INTRODUCTION

I.1 Présentation générale

Le présent document constitue la politique et les pratiques de certification (DPC) mises en œuvre par l'autorité de certification de l'Ordre des Experts-Comptables (OEC) pour les membres de l'Ordre, en conformité avec la politique de certification identifiée par l'OID *1.3.6.1.4.1.15819.5.1.3.3*. Elle réunit l'ensemble des obligations et engagements des différents acteurs relatifs à la délivrance et l'usage des certificats numériques de personnes physiques dans le cadre de leur activité réglementée d'Experts-Comptables ou de collaborateurs de ces Experts-Comptables.

Cette DPC est conforme aux principes et recommandations définies dans la norme *ETSI EN 319411-1*.

Cette politique de certification vise à permettre la délivrance de certificats permettant de réaliser une signature avancée au sens du *Règlement (UE) N° 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur* (dit « Règlement eIDAS »). Ces certificats seront utilisés pour des signatures électroniques ayant des effets juridiques effectifs sur des écrits électroniques et, par conséquent, recevables en justice.

I.2 Identification du document

Le présent document est dénommé *Déclaration des pratiques de certification – Signature avancée*. Il est identifié par son numéro d'identifiant d'objet (OID), ainsi que par le nom, numéro de version, et la date de mise à jour.

L'OID de la présente DPC est : 1.2.250.1.165.1.13.1.1

I.3 Entrée en vigueur du document

La présente DPC s'applique à partir du 10 octobre 2018.

I.4 Entités intervenant dans l'I.G.C. et responsabilités

I.4.1 Le Prestataire de services de certification électronique

Dans le cadre de cette DPC, ***le rôle de PSCE assuré au niveau national par le Conseil Supérieur de l'Ordre des Experts-Comptables (CSOEC).*** Au titre de l'Ordonnance n° 45-2138 du 19 septembre 1945 portant institution de l'ordre des experts-comptables et règlementant le titre et la profession d'expert-comptable, le CSOEC est l'organe de direction et de gestion des membres de l'Ordre des experts-comptables. Il a seule qualité pour représenter la profession et exercer, devant toutes les juridictions, tous les droits réservés à la partie civile. Il est composé des présidents des Conseils régionaux et de membres élus.

Le PSCE est identifié dans tout certificat dont il a la responsabilité au travers de l'AC ayant émis ce certificat et qui sont elles-mêmes directement identifiées dans le champ "*issuer*" du certificat.

I.4.2 Autorité de certification (AC)

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (I.G.C.).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des biclés et des certificats.

Dans le cadre de ce document, l'AC est le Conseil Supérieur de l'Ordre (CSOEC).

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine, la décomposition fonctionnelle d'une I.G.C. qui est retenue dans la présente DPC est la suivante :

Fonction d'enregistrement (AE)	Opérateur d'enregistrement (OE) OSC
Fonction de génération des certificats	AC et OSC
Fonction de génération des éléments secrets du porteur	OSC
Fonction de remise au porteur	Sans objet
Fonction de publication	AC (documents, certificats d'AC) et OSC (LCR)
Fonction de gestion des révocations	AE Nationale OSC
Fonction d'information sur l'état des certificats	OSC (OCSP, LCR)

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

- Être une entité juridique au sens de la loi française.
- Être en relation par voie 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 DPC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la DPC et les procédures de la DPC sont appliquées par chacune des composantes de l'I.G.C. et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa DPC, correspondant au minimum aux fonctions obligatoires de la présente DPC, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels, notamment l'AC doit mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'I.G.C. et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre pour atteindre le niveau de sécurité requis.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa DPC, et correspondant au minimum aux exigences de la présente DPC, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure.

- Générer, et renouveler lorsque nécessaire, ses biclés 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.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacités de traitement et de stockage.

I.4.3 Opérateur d'enrôlement (OE)

L'OE (I.7.2) a en charge :

- La vérification d'identité en face-à-face du demandeur
- Le contrôle de son habilitation à demander un certificat
- La vérification de l'identité apparaissant dans le certificat

Pour les porteurs EC, l'OE est l'Ordre des experts-comptables et ses conseils régionaux et départementaux devant lesquels les EC prêtent serment.

Pour les porteurs collaborateurs, l'OE un expert-comptable du cabinet dans lequel le collaborateur officie.

I.4.4 Autorité d'enregistrement (AE)

L'AE a pour rôle de vérifier l'identité du futur porteur de certificat. Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations du futur porteur et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'I.G.C. suivant l'organisation de cette dernière et les prestations offertes ;
- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur y compris lors des échanges de ces données avec les autres fonctions de l'I.G.C. (notamment, elle respecte la législation relative à la protection des données personnelles).

La fonction d'AE est partagée entre l'opérateur d'enregistrement (CSOEC) et l'OSC ; voir I.4.2 pour la façon dont les responsabilités sont réparties.

En effet, une majorité des procédures de gestion des certificats (délivrance, révocation, etc.) est dématérialisée et s'appuie sur une autorité d'enregistrement technique chez l'OSC.

I.4.5 Opérateur de certification (OC/OSC)

L'OSC est en charge :

- Du contrôle de la pièce d'identité du demandeur
- De la mise à disposition des éléments secrets du porteur
- De la création et du stockage des certificats

L'opérateur de certification est la société *Cryptolog International*, enregistrée au RCS sous le numéro 439129164.

I.4.6 Porteurs de certificats

Dans le cadre de la présente DPC, un porteur de certificat appartient aux deux catégories de population suivantes :

- Un ou une expert-comptable personne physique (cf. I.7.2)
- Un collaborateur ou une collaboratrice d'un expert-comptable ayant reçu délégation pour signer en son nom propre

Cette personne 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 réglementaire.

Le porteur respecte les conditions qui lui incombent telles que définies dans la présente DPC.

I.4.7 Utilisateurs de certificat

La présente DPC traitant de certificats de signature, un utilisateur de certificat peut être notamment :

- Un service de l'administration accessible par voie électronique aux porteurs (application, serveur internet, base de données, etc.), sous la responsabilité d'une personne physique ou morale, qui utilise un certificat et un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat. L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable d'application.
- Un agent (personne physique) de l'administration destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- Un usager destinataire d'un message ou de données provenant d'un porteur et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données transmises par le porteur du certificat.

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document fournis par l'AC. En particulier, l'AC respecte ses responsabilités envers les utilisateurs qui ont « raisonnablement » confiance dans un certificat, selon les dispositions de l'article 33 de la *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

I.5 Usage des certificats

I.5.1 Domaines d'utilisation applicables

Dans le cadre de la présente DPC, il s'agit de produire une signature électronique avancée de document, conformément aux dispositions du règlement eIDAS.

I.5.1.1 Biclés et certificats des porteurs

La présente DPC traite des biclés et des certificats à destination des catégories de porteurs identifiées au chapitre 0 ci-dessus, afin que ces porteurs puissent signer électroniquement des données (documents ou messages) dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées au chapitre I.4.7 ci-dessus. Une telle signature électronique apporte, outre l'authentification du signataire et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu juridique de ces données.

Les certificats de signature objets de la présente DPC sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité afin de pouvoir signer indûment des données sont forts.

Enfin, certaines applications d'échanges dématérialisés de la sphère publique peuvent nécessiter des certificats à des fins de tests ou de recette, différents des certificats de production fournis et gérés par l'AC.

I.5.1.2 Biclés et certificats d'AC et de composantes de l'I.G.C.

La chaîne de certification de l'AC est la suivante :

I.5.1.2.1 Certificats d'AC

Pour tous ces certificats, une unique biclé est utilisée pour la signature des certificats porteurs et de la L.C.R. sous la responsabilité de l'AC.

I.5.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des biclés et des certificats sont définies au chapitre IV.5 ci-dessous. L'AC respecte ces restrictions et impose leur respect par ses porteurs et ses utilisateurs de certificats.

À cette fin, elle communique à tous les porteurs et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

I.6 Gestion de la DPC

I.6.1 Entité gérant la DPC

La DPC est gérée par le CSOEC.

I.6.2 Point de contact

La rédaction, la modification et la diffusion de la DPC est confiée à la Direction des Études Informatiques (DEI) du CSOEC.

Direction des études informatiques
Conseil supérieur de l'Ordre des experts-comptables
19 rue Cognacq Jay
75341 Paris Cedex 07

I.7 Définitions et abréviations

I.7.1 Abréviations

Les abréviations utilisées dans la présente DPC sont les suivantes :

A.C.	Autorité de Certification
A.E.	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CDOEC	Conseil départemental de l'Ordre des experts-comptables

CEN	Comité Européen de Normalisation
CRL	Liste des Certificats Révoqués *(Certificate revocation list)*
CRLDP	*Point de Distribution de la Liste des Certificats Révoqués (Distribution Point of the Certificate revocation list)*
CSOEC	Conseil Supérieur de l'Ordre des Experts-Comptables
CROEC	Conseil Régional de l'Ordre des Experts-Comptables
DCS	Dispositif de Création de Signature
DN	*Distinguished Name* (nom distinctif)
D.P.C.	Documentation des Pratiques de Certification
EC	Expert-Comptable
ETSI	*European Telecommunications Standards Institute*
I.G.C.	Infrastructure de Gestion de Clés
LCR	Liste des Certificats Révoqués
OSC	Opérateur de Service de Certification
OC	Opérateur de Certification
OCSP	*Online Certificate Status Protocol*
OE	Opérateur d'enregistrement
OID	*Object Identifier* (identifiant d'objet)
P.C.	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
URL	*Uniform Resource Locator* (adresse universelle)

I.7.2 Définitions

Les termes utilisés dans la présente DPC sont les suivants :

Agent - Personne physique agissant pour le compte d'une autorité administrative.

Autorité d'Enregistrement (AE) : Fonction ou entité chargée de la vérification que les demandeurs ou les porteurs de certificat sont identifiés, que leur identité est authentique et que les contraintes liées à l'usage d'un certificat sont remplies conformément à la politique de certification.

Différentes AE se répartissent les tâches incombant à cette fonction :

- L'AE technique (portail Jesignexpert) contrôle :
  - Pour les experts-comptables, l'inscription professionnelle du demandeur sur le tableau régional géré par le CROEC/CDOEC auquel il appartient
  - Pour les collaborateurs, la délégation délivrée par l'expert-comptable
  - Pour tous les demandeurs, la conformité de la copie de la pièce d'identité fournie avec les éléments de la demande.

- L'AE nationale gère les demandes de révocation

Autorité de Certification (AC) : L'AC assure les fonctions suivantes :

- Rédaction des documents de spécifications de l'I.G.C., notamment la/les DPC,
- Mise en application de la DPC ;
- Gestion des certificats (de leur cycle de vie) ;
- Choix des dispositifs cryptographiques et gestion des données d'activation ;
- Publication des certificats valides et des listes de certificats révoqués ;
- Conseil, information ou formation des acteurs de l'I.G.C. ;
- Maintenance et évolution de la DPC et de l'I.G.C. ;
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'I.G.C., à son niveau ;

Autorité de Certification Racine (ou **AC Racine**) **:** désigne l'entité de plus haut niveau dans l'infrastructure à Clé publiques et qui certifie les autorités de certification filles.

Autorités administratives - Ce terme générique, défini à l'article 1 de l'Ordonnance n° 2005-1516 du 8 décembre 2005, désigne les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif, notamment l'Ordre des Experts-Comptables.

Certificat électronique - Fichier électronique attestant qu'une biclé 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 le biclé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

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 de l'I.G.C. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

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

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

Expert-comptable (EC) : personne inscrite au tableau de l'Ordre ou à sa suite, salarié autorisé à exercer la profession d'expert-comptable.

Identificateur d'objet (OID) - identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifique. Dans le cadre de l'I.G.C., les identificateurs OID servent notamment à identifier chacune des politiques, ainsi que les algorithmes de chiffrement acceptés.

Infrastructure à Gestion de Clés (**I.G.C.**) : désigne un ensemble de moyens organisationnels, techniques (matériels et logiciels), humains, documentaires et contractuels pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques. L'I.G.C. génère, distribue, gère et archive les Certificats. Chacune des composantes de l'I.G.C. est

décrite dans la Politique de certification définissant le niveau de confiance confié à chacune d'entre elles.

Opérateur d'enregistrement (OE) : personne physique chargée de réaliser le face-à-face avec le demandeur d'un certificat (lorsqu'il est requis) et d'effectuer une première vérification des pièces justificatives. Ces pièces seront transmises *in fine* à l'AE pour validation.

Opérateur de Service de Certification (OSC) : composante de l'I.G.C. disposant d'une plate-forme lui permettant de générer et émettre des certificats auxquels une communauté d'utilisateurs fait confiance.

Online Certificate Status Protocol **(OSCP)** : protocole de l'I.G.C. par lequel un certificat est validé (non révocation) en ligne. Le protocole fait l'objet de la norme RFC 2560.

Politique de certification (DPC) - 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 DPC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Portail web client : désigne un site web sous la responsabilité du CSOEC sur lequel chaque Porteur (i) effectue ses demandes d'émission, de renouvellement et de révocation de Certificats, (ii) suit en ligne l'état de ses demandes, (iii) recueille la documentation relative à l'utilisation de ses Certificats.

Ce site peut être assuré par le CSOEC lui-même ou être confié par lui à une des organisations spécialisées de l'Ordre des Experts-Comptables.

Prestataire de services de certification électronique (PSCE) - Un PSCE se définit comme 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.

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.

Qualification d'un prestataire de services de certification électronique - Le *Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005* décrit la procédure de qualification d'un PSCE. Il s'agit d'un acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une DPC pour un niveau de sécurité donné et correspondant au service visé par les certificats.

Désigne aussi le processus selon lequel un prestataire de services de certification électronique est certifié conforme aux exigences de l'article 24 du règlement eIDAS.

SUPRA : Ce numéro identifie de façon unique chaque Expert-Comptable inscrit au Tableau de l'Ordre. Ce numéro est délivré à la première inscription de la personne physique à l'Ordre et n'est plus modifié par la suite, même en cas de pluri-adhésion.

II RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

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

L'AC met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats à destination des porteurs et des utilisateurs de certificats (*cf.* chapitre I.3.1 ci-dessus).

Les méthodes de mise à disposition et les adresses correspondantes sont précisées ci-après.

II.2 Informations devant être publiées

L'AC a pour obligation de publier au minimum les informations suivantes à destination des porteurs et utilisateurs de certificats :

- La politique de certification, établie par le PSCE et couvrant l'ensemble des rubriques du RFC3647
- La liste des certificats révoqués
- Les certificats de l'AC, en cours de validité
- Le certificat de l'AC Racine et son empreinte cryptographique (SHA-256)

L'AC a également pour obligation de publier sur un modèle établi par le PSCE, à destination des porteurs de certificats, les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.). Ces conditions générales font notamment partie intégrante du dossier d'enregistrement.

Le moyen utilisé pour la publication de ces informations, sauf pour les LCR / LAR (cf. chapitre IV.9), est libre et précisé plus loin dans la DPC. Il garantit l'intégrité, la lisibilité, la compréhensibilité et la clarté des informations publiées.

II.3 Délais et fréquences de publication

Les informations liées à l'I.G.C. (nouvelle version de la DPC, formulaires, etc.) sont publiées 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.

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats de porteurs ou de LCR.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres IV.8 et IV.9.

II.4 Contrôle d'accès aux informations publiées

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

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'I.G.C., au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

III IDENTIFICATION ET AUTHENTIFICATION

III.1 Nommage

III.1.1 Types de noms

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

Dans chaque certificat conforme à la norme X.509, l'AC émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un "*Distinguished Name*" (DN) de type X.501.

III.1.2 Nécessité d'utilisation de noms explicites

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

Le DN du porteur est construit à partir des nom et prénom de son état civil tels que contenus dans le tableau de l'Ordre.

Ces éléments sont vérifiés par l'AE à partir des documents d'identité joints au dossier. Les noms d'épouse ou d'usage sont acceptés dès lors qu'ils figurent sur ces documents d'identité.

III.1.2.1 Identité de l'A.C. émettrice

L'AC émettrice est identifiée par son *DN*, comme suit.

C	FR
O	Conseil Superieur de l'Ordre des Experts-comptables
OU	0002 775670003
OI	NTRFR-775670003
CN	Signature – Conseil Superieur de l'Ordre des Experts-Comptables – CA

Conformément à la norme *ETSI EN 319 412*, le *DN* de ces AC est construit comme suit :

- Le champ `C` désigne le pays de l'AC
- Le champ `O` désigne l'organisme (ici, l'Ordre des E.-C.)
- Le champ `OU` contient le SIREN de l'organisme, précédé du code « 0002 » (contrainte R.G.S.)
- Le champ `OI` contient le SIREN de l'organisme, précédé du code « NTRFR- » (contrainte ETSI)
- Le champ `CN` contient le nom de l'A.C.

III.1.2.2 Identité des porteurs experts-comptables

Le DN des certificats porteurs experts-comptables est construit comme suit :

C	FR
SERIALNUMBER	*[aléa propre au porteur]*
givenName	*[prénom du porteur]*
surName	*[nom du porteur]*

CN	*[Prénom Nom]*

- Le champ `C=FR` désigne la France ;
- Le champ `CN` contient le prénom et le nom du porteur (dans cet ordre) tels qu'ils apparaissent dans le tableau de l'Ordre ;
- Le champ `surName` contient le nom du porteur tel qu'il apparaît dans le tableau de l'Ordre ;
- Le champ `givenName` contient le prénom du porteur tel qu'il apparaît dans le tableau de l'Ordre ;
- Le champ `serialNumber` contient un numéro unique d'identification, propre au porteur. Sa valeur est déterminée aléatoirement par l'AC lors de la création du certificat.

  Ce numéro apparaît ainsi dans tous les certificats attribués au porteur par l'AC du CSOEC.

III.1.2.3 Identité des porteurs collaborateurs habilités

Le DN des certificats porteurs pour les collaborateurs habilités est identique à celui des experts-comptables. Les noms et prénoms du porteurs proviennent dans ce cas de la pièce d'identité du collaborateur.

III.1.2.4 Certificats de test

Les certificats de test sont identifiables par le fait que leur `CN` contient le mot « `TEST` », précédant un prénom et un nom fictifs. Tous les autres champs (à l'exception des informations d'AC, comme les champs `Issuer`, AIA, AKI, etc.) sont susceptibles de différer des profils des certificats porteurs décrits au chapitre VII.1.

III.1.3 Pseudonymisation des porteurs

La politique n'autorise pas l'utilisation de pseudonymes dans ses certificats.

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

Voir III.1.2 ci-dessus.

III.1.5 Unicité des noms

Le *DN* du champ "*subject*" de chaque certificat de porteur permet d'identifier de façon unique le porteur correspondant au sein du domaine de l'A.C.

Ce *DN* respecte les règles d'homonymie au sein du domaine de l'A.C.

Dans chaque certificat X509v3, l'A.C. émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un "*Distinguished Name*" (DN) de type X.501.

L'unicité des noms au sein de la présente A.C. est assurée par le champ `serialNumber` du *DN* (y compris pour les certificats de test).

L'anonymat ou le pseudonyme des porteurs ne sont pas supportés par la présente A.C.

III.1.6 Identification, authentification et rôle des marques déposées

Les litiges pouvant survenir dans les noms apparaissant dans les certificats ne peuvent porter que sur le cabinet de rattachement : cet aspect est déjà traité au niveau de l'inscription au Tableau de l'Ordre.

III.2 Validation initiale de l'identité de la structure professionnelle d'exercice du porteur

Sans objet.

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

Sans objet, car la biclé est tirée en central.

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

Voir ci-dessous.

III.2.3 Validation de l'identité d'un individu

III.2.3.1 Enregistrement d'un expert-comptable

La demande initiale est saisie sur une application Web en liaison avec les tableaux régionaux de l'Ordre. L'identité du demandeur est issue de ce référentiel, sans possibilité de changement, y compris pour l'adresse courriel professionnelle concernée par le certificat. En cas d'anomalie sur cette adresse, l'Expert-Comptable doit, préalablement à sa demande de certificat, faire procéder à la rectification des informations auprès de l'Ordre.

L'inscription au tableau de l'Ordre est nécessaire et suffisante pour la présente validation.

Le dossier d'enregistrement, déposé directement auprès de l'A.E. en ligne sur le portail Jesignexpert, comprend au moins :

- Une copie de pièce d'identité officielle du futur porteur en cours de validité (carte nationale d'identité ou passeport) ;
- Un numéro de téléphone mobile personnel ;
- Le formulaire de demande de certificat constitué sur la base des informations provenant du tableau de l'Ordre.

L'A.E. garde une copie de la pièce d'identité présentée. Elle archive l'ensemble des documents constituants la demande de certificat, à savoir :

- Une copie de la pièce d'identité présentée
- Les données saisies dans le formulaire de demande de certificat

III.2.3.2 Enregistrement d'un collaborateur habilité

L'identité du collaborateur et son adresse courriel sont vérifiées lors d'un face à face physique avec l'expert-comptable faisant office d'opérateur d'enregistrement (OE).

Postérieurement à ce face-à-face, l'habilitation d'un collaborateur à signer est déclarée par l'expert-comptable sur le portail Web de l'A.C., ce qui l'autorise à déposer une demande auprès de l'A.E. ; le dossier d'enregistrement déposé est identique à celui d'un expert-comptable.

III.2.4 Informations non vérifiées du porteur

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

III.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 : pour les experts-comptables, cette validation provient du tableau de l'Ordre ; pour les collaborateurs, elle provient de l'habilitation déclarée par l'expert-comptable sur le portail Web de l'A.C.

III.2.6 Certification croisée d'A.C.

Aucune certification croisée n'est autorisée dans le cadre de la politique.

III.3 Identification et validation d'une demande de délivrance d'un certificat suite au changement de biclé

Sans objet.

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

Le porteur peut demander la révocation de son certificat par différents moyens :

a) En contactant l'AE nationale (CSOEC) par téléphone ou par courriel ;
b) Depuis le portail web client de l'O.S.C. : le porteur s'identifie à l'aide du numéro de téléphone mobile ou de l'adresse courriel utilisée lors de la création de son certificat.

Dans tous les cas, le demandeur est formellement authentifié par la vérification de son identité et de son autorité par rapport au certificat à révoquer.

IV EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

IV.1 Demande de certificat

IV.1.1 Origine d'une demande de certificat

Les personnes habilitées à déposer une demande de certificat sont :

- Les experts-comptables inscrits au tableau de l'Ordre
- Les collaborateurs dûment habilités par un ou une expert-comptable inscrit au tableau de l'Ordre

L'AE assure la validation de la demande de certificat en s'appuyant (indirectement) sur le tableau de l'Ordre, les habilitations déclarées, et (directement) sur les documents présentés.

Une demande de certificat n'oblige en rien l'AC à émettre un certificat ; tout refus est motivé.

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

Le demandeur se connecte au site Portail Web Client et peut y demander un certificat s'il n'en possède pas déjà un.

Les informations suivantes font partie de la demande de certificat :

- Les nom et prénom du porteur à utiliser dans le certificat ;
- Les données personnelles d'identification du porteur ;
- L'adresse courriel professionnelle ;
- Le numéro de téléphone

Concernant les experts-comptables, ces données proviennent du tableau de l'Ordre, à l'exception du numéro de téléphone.

Le demandeur procède ensuite à l'acceptation des conditions générales d'utilisation du service.

IV.2 Traitement d'une demande de certificat

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

Le portail Web assure la vérification de l'autorité du demandeur : son inscription au tableau de l'Ordre (expert-comptable) ou son habilitation (collaborateur). Dans les deux cas, cette vérification assure qu'un face-à-face préalable a été réalisé avec le demandeur.

La demande validée est transmise par le portail Web à l'AE, qui assure les opérations suivantes :

1. Validation de l'identité du futur porteur sur la base des justificatifs présentés ;
2. Vérification de la cohérence des justificatifs présentés, notamment par rapport au contenu de la demande ;
3. Collecte du consentement du futur porteur aux modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

Il est conservé une trace des justificatifs d'identité présentés.

IV.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, la composante chargée de l'enregistrement en informe le porteur en en justifiant le rejet.

IV.2.3 Durée d'établissement du certificat

La demande de génération du certificat et de la biclé est générée par l'AC vers la fonction adéquate de l'I.G.C. est produite dans les secondes suivant la validation de la demande.

IV.3 Délivrance du certificat

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

À la réception d'une demande en provenance du portail, l'A.C. déclenche les processus de génération et de préparation des différents éléments destinés au porteur auprès de l'OSC.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées ci-après.

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

Le porteur est notifié en ligne du succès de son enrôlement à la fin du processus de demande.

IV.4 Acceptation du certificat

L'utilisation du certificat par le porteur vaut acceptation de celui-là par celui-ci.

IV.4.1 Publication du certificat

Les certificats ne sont pas publiés.

IV.4.2 Notification par l'A.C. aux autres entités de la délivrance du certificat

L'A.C. informe les autres entités de l'I.G.C. de la délivrance du certificat si nécessaire.

IV.5 Usages de la biclé et du certificat

IV.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 (cf. chapitre I.5.1.1). Cette contrainte est portée à la connaissance des porteurs par l'A.C., notamment dans l'accord contractuel qui les lie. Il y est rappelé que :

- Les porteurs doivent respecter strictement les usages autorisés des biclés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.
- Ils s'engagent également à ne plus utiliser leur biclé ou leur certificat dès la perte ou la suspension de la qualité d'expert-comptable ou après révocation ou expiration du certificat.

L'usage autorisé de la biclé du porteur et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des clés. Cet usage est explicité dans les conditions générales d'utilisation et/ou le contrat porteur. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du porteur par l'A.C. avant d'entrer en relation contractuelle.

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

Les utilisateurs de certificats seront informés par l'A.C. qu'ils doivent respecter strictement les usages autorisés des certificats et que dans le cas contraire, leur responsabilité pourrait être engagée.

IV.6 Renouvellement d'un certificat

Le renouvellement d'un certificat suit la procédure d'enrôlement initiale, avec génération d'un nouveau biclé.

IV.7 Modification du certificat

La modification du certificat n'est pas admise.

IV.8 Révocation et suspension des certificats

IV.8.1 Causes possibles d'une révocation

IV.8.1.1 Certificats de porteurs

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

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat
- Le porteur n'a pas respecté les modalités applicables d'utilisation du certificat
- Le porteur ou l'entité n'ont pas respecté leurs obligations découlant de la P.C. de l'A.C.
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur
- La clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées)
- Le porteur ou une entité autorisée (représentant légal de l'entité) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur ou de son support)
- Le décès du porteur ou la cessation d'activité de l'entité du porteur
- (Uniquement pour les certificats d'expert-comptable) le porteur n'est plus membre de l'Ordre dans les conditions d'émission du certificat
- (Uniquement pour les certificats de collaborateurs) le porteur n'est plus habilité à signer

Lorsqu'une des circonstances ci-dessus se réalise et que l'A.C. en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné est révoqué.

L'A.C. peut, à sa discrétion, révoquer un certificat lorsqu'un porteur ne respecte pas les obligations énoncées dans la politique de certification.

IV.8.1.2 Certificats d'une composante de l'I.G.C.

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'I.G.C. (y compris un certificat d'A.C. 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'I.G.C. suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif)
- Cessation d'activité de l'entité opérant la composante.

IV.8.2 Origine d'une demande de révocation

IV.8.2.1 Certificats de porteurs

Les personnes ou entités qui peuvent demander la révocation d'un certificat de porteur sont les suivantes :

- Le porteur au nom duquel le certificat a été émis
- L'A.C. émettrice du certificat
- Le CSOEC

Le porteur est informé des personnes et entités susceptibles d'effectuer une demande de révocation pour son certificat.

IV.8.2.2 Certificats d'une composante de l'I.G.C.

Les demandes de révocation des certificats de composantes sont émises par le CSOEC ou par la composante concernée.

IV.8.3 Procédure de traitement d'une demande de révocation

IV.8.3.1 Révocation d'un certificat de porteur

Une demande de révocation peut être déposée en utilisant l'un des moyens suivants :

a) En contactant l'A.E. nationale (CSOEC) par téléphone ou par courriel
b) En se connectant sur le Portail Web de l'O.S.C. (https://app.universign.com/fr/revocation/) Le porteur s'identifie via l'une des méthodes mentionnées en III.4.

Une fois la demande authentifiée et contrôlée, l'A.C. révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la publication sur l'état des certificats. L'information de révocation est diffusée au minimum via une LCR signée par l'A.C. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'A.C.

Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat.

L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

IV.8.3.2 Révocation d'un certificat d'une composante de l'I.G.C.

Les demandes de révocation des certificats de composante sont traitées par l'A.C. concernée selon ses procédures.

IV.8.3.3 Délai accordé au porteur pour formuler la demande de révocation

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

IV.8.4 Délai de traitement par l'A.C. d'une demande de révocation

Toute demande de révocation est traitée en urgence.

Il s'écoule au maximum 12 heures entre la demande de révocation par le porteur et la publication de la nouvelle LCR prenant en compte cette demande.

La durée maximale d'indisponibilité par interruption de service (panne ou maintenance) est de 4 (quatre) heures durant les jours ouvrés.

IV.8.5 Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

IV.8.6 Fréquence d'établissement des LCR

La LCR est mise à jour toutes les heures (60 minutes). Une LCR est valable au maximum 7 jours.

IV.8.7 Délai maximum de publication d'une LCR

Une LCR est publiée dans un délai de 30 minutes suivant sa génération.

IV.8.8 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

L'A.C. propose un service OCSP accessible à l'adresse indiquée dans les certificats.

IV.8.9 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Cf. chapitre IV.8.5 ci-dessus.

IV.8.10 Autres moyens disponibles d'information sur les révocations

Sans objet.

IV.8.11 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'A.C., outre les exigences du chapitre IV.8.3.2 ci-dessus, la révocation suite à une compromission de la clé privée fera l'objet d'une information clairement diffusée au moins sur le site internet de l'A.C. et éventuellement relayée par d'autres moyens (autres sites internet institutionnels, journaux, etc.).

Quant au porteur, l'A.C. impose par voie contractuelle qu'en cas de compromission de sa clé privée du porteur ou de connaissance de la compromission de la clé privée de l'A.C. ayant émis son certificat, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

IV.8.12 Suspension de certificats

La suspension de certificats n'est pas autorisée dans la présente DPC.

IV.9 Fonction d'information sur l'état des certificats

IV.9.1 Caractéristiques opérationnelles

L'A.C. fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'A.C. Racine), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR et l'état du certificat de l'A.C. Racine.

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR. Ces LCR sont des LCR au format V2, publiées aux adresses suivantes :

`http://crl.jesignexpert.com/csoecadvanced.crl`

L'A.C. émettrice est aussi en charge de la production des certificats de signature des réponses.

IV.9.2 Disponibilité de la fonction

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 4 (quatre) heures durant les jours ouvrés et une durée maximale totale d'indisponibilité par mois de 32 heures.

Le cas échéant, temps de réponse du serveur de vérification en ligne du statut d'un certificat (OCSP) à la requête reçue est inférieur à 10 secondes.

IV.10 Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'A.C. et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier est révoqué.

IV.11 Séquestre de clé et recouvrement

Il n'est procédé à aucun séquestre ni recouvrement des clés privées des porteurs.

Il n'est procédé à aucun séquestre ni recouvrement des clés d'A.C.

IV.12 Certificats de test

Les certificats de test (cf. III.1.2.4) et leurs supports sont produits et gérés par l'OSC en accord avec l'A.C., dans le cadre de campagnes de test définies et formalisées. Les certificats de test sont révoqués et leurs clés privées détruites, dès lors que la campagne de test est terminée.

V MESURES DE SECURITE NON TECHNIQUES

V.1 Mesures de sécurité physique

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'A.C. doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'I.G.C.

V.1.1 Situation géographique et construction des sites

L'AC fait héberger ses services de certification dans des locaux sécurises. Ces sites et locaux disposent de mécanismes de sécurité physique décrits dans ce chapitre (tels que des zones verrouillées, un service de gardiennage, des mécanismes de détection d'intrusion) permettant d'assurer une forte protection contre les accès non autorises.

V.1.2 Accès physique

Pour les systèmes critiques du service, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Des mesures sont mises en œuvre afin de prévenir la perte ou l'altération des biens nécessaires au bon fonctionnement du service, ou la perte ou le vol d'informations.

V.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les exigences et engagement des présentes pratiques en matière de disponibilité du service.

V.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences et engagement des présentes pratiques en matière de disponibilité du service.

V.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences et engagement des présentes pratiques en matière de disponibilité du service.

V.1.6 Conservation des supports

Les supports sont conservés de façon sécurisée. Les supports de sauvegarde sont stockés de manière sécurisée dans un site géographiquement éloigné du support original.

Les zones contenant les supports de données sont protégées contre les risques d'incendie, d'inondation et de détérioration.

V.1.7 Mise hors service des supports

En fin de vie, les supports sont détruits ou réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations qu'ils contiennent.

V.1.8 Sauvegardes hors site

Afin de permettre une reprise après incident conforme à ses engagements, l'AC met en place des sauvegardes hors site des informations et fonctions critiques.

L'AC garantit que les sauvegardes sont réalisées par des personnes ayant des rôles de confiance.

L'AC garantit que les sauvegardes sont exportées hors du site de production et bénéficient de mesures pour la protection de la confidentialité et de l'intégrité.

L'AC garantit que les sauvegardes sont testées de façon régulière pour s'assurer que les mesures du plan de continuité d'activité sont respectées.

V.2 Mesures de sécurité procédurales

V.2.1 Rôles de confiance

L'AC distingue au moins les cinq rôles fonctionnels de confiance suivants :

Responsable de sécurité : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.

Responsable d'application : Le responsable d'application 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'I.G.C. au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

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.

Opérateur : Un opérateur au sein d'une composante de l'I.G.C. réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.

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'I.G.C. et aux politiques de sécurité de la composante.

Un même rôle fonctionnel peut être tenu par différentes personnes.

De manière générale, des procédures sont établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification. Ces rôles sont décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'I.G.C. sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Lorsqu'appropriées, ces descriptions doivent différencier entre les fonctions générales et les fonctions spécifiques à l'A.C. L'A.C. doit implémenter techniquement ce principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre. Ces descriptions figurent dans la DPC.

V.2.2 Nombre de personnes requises par tâches

Le nombre de personnes requises par tâches selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, est précisé dans la DPC.

V.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'I.G.C. doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment que :

- Son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- Son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, un compte soit ouvert à son nom dans ces systèmes ;

– Éventuellement, des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'I.G.C.

V.2.4 Rôles exigeant une séparation des attributions

Les cumuls suivants sont interdits :

– Responsable de sécurité et ingénieur système / opérateur

– Contrôleur et tout autre rôle

– Ingénieur système et opérateur

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

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'A.C. doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'I.G.C. C'est pourquoi elles sont précisées dans la DPC, notamment sur les points suivants :

– Qualifications, compétences et habilitations requises

– Procédures de vérification des antécédents

– Exigences en matière de formation initiale

– Exigences et fréquence en matière de formation continue

– Fréquence et séquence de rotation entre différentes attributions

– Sanctions en cas d'actions non autorisées

– Exigences vis-à-vis du personnel des prestataires externes

– Documentation fournie au personnel

V.4 Procédures de constitution des données d'audit

V.4.1 Informations enregistrées pour chaque événement

Toutes les opérations effectuées par l'A.C. ou l'A.E. sont journalisées automatiquement avec les éléments d'authentification des opérateurs et horodatage local afin d'être en mesure de fournir une preuve de la certification en justice. Les éléments suivants sont mémorisés pour chaque événement :

– Type d'opération ;

– Destinataire de l'opération ;

– Nom du demandeur de l'opération ;

– Nom de l'opérateur ;

– Nom des personnes présentes (s'il y en a d'autres) ;

– Lieu de l'opération ;

– Date et heure de l'opération ;

– Cause de l'événement ;

– Résultat de l'événement (échec ou réussite) ;

– Date et heure de journalisation.

V.4.2 Imputabilité

L'imputabilité d'une action revient à la personne, à la composante, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure dans l'un des champs du journal d'événements.

V.4.3 Événements enregistrés par l'A.E.

L'A.E. enregistre et sauvegarde les événements suivants :

- Les dossiers de demandes de certificat
- Les dossiers de demandes de révocation
- Toutes les relations avec l'A.C.
- Tous les accès aux fonctions ayant trait aux opérations d'enregistrement

V.4.4 Événements enregistrés par l'A.C.

La fonction de journalisation de l'A.C. doit consister à enregistrer tous les événements et notamment :

- Tous les événements ayant trait à la sécurité des systèmes informatiques utilisés
- Démarrage et arrêt des systèmes informatiques
- Démarrage et arrêt des applications
- Opérations échouées ou réussies pour créer, extraire, établir des mots de passe ou modifier les privilèges système d'Utilisateurs privilégiés (Utilisateurs maîtres de l'I.G.C., responsables de sécurité, gestionnaires),
- Génération des clés de ses composantes
- Chargement, déchargement du dispositif contenant la clé de l'A.C., insertion et retrait de la carte cryptographique
- Création et révocation de certificats
- Opérations pour initialiser, extraire, valider et invalider des porteurs, et pour mettre à jour ou récupérer leurs clés
- Opérations d'écriture dans l'annuaire des certificats et des LCR
- Requêtes et réponses OCSP

V.4.5 Événements divers

L'environnement d'exploitation fait lui aussi l'objet d'une journalisation des événements :

- Accès physiques aux locaux et matériels protégés.
- Opérations de maintenance et de changements de la configuration des systèmes.
- Les changements de personnel.
- Le suivi des dossiers et supports physiques.
- Le suivi des opérations de sauvegarde et d'archivage.
- Les actions de destruction des supports contenant des clés, des données d'activation ou des renseignements personnels sur les porteurs.

V.4.6 Processus de journalisation

Le processus de journalisation est effectué en tâche de fond et permet un enregistrement en temps réel des opérations effectuées. Il est incontournable au sens de l'exploitation. Il n'est pas modifiable.

La journalisation des opérations d'origine manuelle porte mention des deux dates (exécution et saisie) qui sont proches (quelques heures).

V.4.7 Protection d'un journal d'événements

L'écriture dans les journaux d'événements est automatique, elle est une conséquence des contrôles des droits d'accès. Les enregistrements ne sont pas modifiables a posteriori et le système de signature séquentiel assure ce contrôle.

Les journaux d'événements sont protégés en intégrité et horodatés selon des modalités précisées dans la DPC.

V.4.8 Copies de sauvegarde des journaux d'événement

Des sauvegardes mensuelles sur sont effectuées. Des précisions sont fournies dans la DPC sur les modalités de sauvegarde.

V.4.9 Procédure de collecte des journaux (interne ou externe)

La collecte des journaux commence au démarrage des systèmes concernés par les événements à enregistrer et se termine aux arrêts de ces systèmes.

V.4.10 Anomalies et audit.

Les responsables des traitements de journalisation prennent toutes les mesures nécessaires, au regard de l'état de l'art, pour détecter toute tentative de violation de l'intégrité du système de gestion des certificats, y compris les équipements physiques, l'environnement d'exploitation et le personnel. Pour assurer ce contrôle les journaux d'événements journaliers sont contrôlés afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux de l'A.C. sont examinés périodiquement par un responsable qui en fait la revue à partir d'un résumé d'exploitation joint dans lequel les éléments importants sont analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées. L'A.C. est susceptible d'approfondir ou de faire approfondir toute période présentant des anomalies potentielles.

Des rapprochements ponctuels sont effectués de façon au plus hebdomadaire entre les journaux de l'A.E. et ceux de l'A.C. pour vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

Les anomalies détectées à l'occasion de ces contrôles réguliers ou ponctuels donnent lieu à la mise en œuvre des actions de recherche pour identifier les conséquences éventuelles des anomalies :

- Validité des certificats concernés par l'événement.
- Sécurité globale de l'I.G.C.
- Sécurité partielle de l'I.G.C. (analyse des composantes).
- Non-respect de la DPC.

V.5 Archivage des données

Les opérations d'archivage sont réalisées suivant *Les Recommandations pour l'archivage sécurisé*, en date du 12 juillet 2000, par le groupe de travail commun du Conseil Supérieur de l'Ordre des Experts-Comptables et de l'association IALTA France et (http://www.edificas.org).

V.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont prises par l'A.C. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'I.G.C.

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 au moins les suivantes :

- La DPC ;

- Les certificats, LCR tels qu'émis ou publiés ;
- Les récépissés ou notifications (à titre informatif) ;
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- Les traces et journaux d'événements liés au cycle de vie des biclés d'A.C. et des biclés produites ;
- Les journaux d'événements des différentes entités de l'I.G.C.

V.5.2 Période de conservation des archives

V.5.2.1 Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi française.

La durée de conservation des dossiers d'enregistrement pendant 10 ans est portée à la connaissance du porteur. Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat est tenu à disposition des autorités habilitées par l'A.C. Ce dossier, complété par les mentions consignées par l'A.E., permet de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'A.C.

V.5.2.2 Certificats et LCR émis par l'A.C.

Les certificats de clés de porteurs et d'A.C., ainsi que les LCR produites, sont archivés pendant au moins sept ans après leur expiration.

V.5.2.3 Journaux d'événements et autres

La durée d'archivage des journaux d'événements et autres est de sept ans.

V.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :

- Être protégées en intégrité ;
- Être accessibles aux personnes autorisées ;
- Pouvoir être relues et exploitées.

La DPC expose les moyens mis en œuvre pour archiver les pièces en toute sécurité.

V.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes, qui est équivalent au niveau de protection des archives, est précisé dans la DPC.

V.5.5 Exigences d'horodatage des données

Le chapitre VI.7 précise les exigences en matière de datation ou d'horodatage.

V.5.6 Système de collecte des archives

La DPC décrit le système de collecte des archives, interne ou externe, qui doit respecter les exigences de protection des archives concernées.

V.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai de 3 jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'I.G.C. qui ne peut récupérer et consulter que les archives de la composante considérée).

V.6 Changement de clé d'A.C.

L'A.C. ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'A.C. Pour cela la période de validité de ce certificat de l'A.C. est supérieure à celle des certificats qu'elle signe. Au regard de la date de fin de validité de ce certificat, son renouvellement est demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle biclé d'A.C. est générée, seule la nouvelle clé privée est utilisée pour signer des certificats. Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

V.7 Reprise suite à compromission et sinistre

Les procédures de remontée et de traitement des incidents et des compromissions ainsi que de reprise seront précisées dans la DPC.

En cas de compromission ou de sinistre, l'A.C. s'engage à informer :

- Tous les porteurs
- Les tiers utilisateurs de certificats avec lesquels l'A.C. a passé des accords
- Toute autre entité précisée dans la DPC

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'A.C. ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors l'A.C. s'engage à :

- Informer tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'A.C. a passé des accords ou a d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats.
- Révoquer tout certificat concerné.

V.8 Fin de vie de l'I.G.C.

Une ou plusieurs composantes de l'I.G.C. peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'A.C. prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où elle serait en faillite ou, pour d'autres raisons, serait incapable de couvrir ces coûts par elle-même, autant que possible et en fonction des contraintes de la législation applicable en matière de faillite.

V.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'I.G.C.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'I.G.C. ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'A.C. en collaboration avec la nouvelle entité.

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'A.C. :

1) Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats).
2) Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans les présentes pratiques.

En particulier :

1) Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'A.C. les en avise aussitôt que nécessaire et, au moins, 1 (un) mois auparavant.
2) L'AC communiquera à l'ANSSI, selon les différentes composantes de l'I.G.C. concernées, les modalités des changements survenus.
   L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats.
3) L'AC tient informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

V.8.2 Cessation d'activité affectant l'AC

La cessation d'activité est définie comme la fin d'activité d'une composante de l'I.G.C. comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'A.C., ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'A.C. 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, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans les présentes pratiques. L'A.C. stipule dans ses pratiques les dispositions prises en cas de cessation de service. Celles-ci incluent :

- La notification des entités affectées
- Le transfert de ses obligations à d'autres parties
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés

Lors de l'arrêt du service, l'A.C. :

1) S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats
2) Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante
3) Révoque son certificat
4) Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité
5) Informe (par exemple par récépissé) tous les porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3).

VI MESURES DE SECURITE TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'I.G.C., notamment par des dispositions spécifiques de la DPC.

VI.1 Génération et installation de biclés

VI.1.1 Génération des biclés

VI.1.1.1 Clés de l'A.C.

Ces questions sont traitées dans d'autres documents de spécifications de l'I.G.C.

VI.1.1.2 Clés porteurs générées par l'A.C.

La génération des clés des porteurs est effectuée dans un environnement sécurisé (cf. chapitre V). Les biclés des porteurs sont générées dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

VI.1.1.3 Clés porteurs générées par le porteur

Sans objet.

VI.1.2 Transmission de la clé privée à son propriétaire

Sans objet. L'AC conserve la clé privée du porteur.

VI.1.3 Transmission de la clé publique à l'A.C.

Sans objet.

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

Le certificat de l'A.C. CSOEC est téléchargeable sur le site internet de l'A.C.

VI.1.5 Tailles des clés

La taille des biclés des AC 4096 bits.

La taille des biclés des porteurs est de 2048 bits.

VI.1.6 Vérification de la génération des paramètres des biclés et de leur qualité

L'équipement de génération de biclés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la biclé. Les paramètres et les algorithmes de signature sont documentés au chapitre VII.

VI.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats de porteurs (voir chapitre I.5.1), de LCR et des certificats des répondeurs OCSP de l'AC.

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

VI.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

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

VI.2.1.1 Modules cryptographiques de l'A.C.

Les modules cryptographiques utilisés par l'AC pour la génération et la mise en œuvre de ses clés de signature sont des boîtiers cryptographiques matériels certifiés répondant aux exigences d chapitre XI. L'AC s'assure de la sécurité des boîtiers utilisés tout au long de leur cycle de vie.

En particulier, l'AC met en place les procédures nécessaires pour :

- S'assurer de l'intégrité des boîtiers durant leur transport depuis le fournisseur ;
- S'assurer de leur intégrité durant leur stockage précédant la cérémonie des clés ;
- S'assurer que les opérations d'activation, de sauvegarde et de restauration des clés de signature sont réalisées sous le contrôle de deux personnels ayant des rôles de confiance ;
- S'assurer que le boîtier fonctionne correctement ;
- S'assurer que les clés contenues dans le boîtier sont bien détruites lorsque celui-ci est décommissionné.

VI.2.1.2 Dispositifs de création de signature des porteurs

Les dispositifs de création de signature des porteurs, pour la mise en œuvre de leurs clés privées de signature, doivent respecter les exigences du chapitre XII.

L'A.C. s'assure que :

- Les désactivations et réactivations des dispositifs de création de signature sont contrôlées de façon sécurisée.

VI.2.2 Contrôle de la clé privée de l'A.C. par plusieurs personnes

Les clés privées de l'AC sont contrôlées par plusieurs personnes à l'aide de données d'activation stockées sur des cartes à puce et remises à des porteurs de secrets lors de la cérémonie des clés.

Un partage de secret du boîtier est mis en œuvre par l'AC par une méthode de partage à seuil.

Les clés privées des porteurs sont contrôlées par des données d'activation sous leur contrôle exclusif.

VI.2.3 Séquestre de la clé privée

L'A.C. ne séquestre en aucun cas les clés privées des porteurs.

VI.2.4 Copie de secours de la clé privée

L'A.C. ne conserve aucune copie de secours des clés privées des porteurs.

VI.2.5 Archivage de la clé privée

Les clés privées des porteurs ne doivent en aucun cas être archivées ni par l'A.C. ni par aucune des composantes de l'I.G.C.

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

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

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

Voir ci-après.

VI.2.8 Méthode d'activation de la clé privée

VI.2.8.1 Clés privées d'A.C.

Ces questions sont traitées dans d'autres documents de spécifications de l'I.G.C.

VI.2.8.2 Clés privées des porteurs

L'activation de la clé privée du porteur est contrôlée via des données d'activation (cf. chapitre VI.3) et permet de répondre aux exigences définies dans le chapitre XII.

VI.2.9 Méthode de désactivation de la clé privée

VI.2.9.1 Clés privées d'A.C.

Ces questions sont traitées dans d'autres documents de spécifications de l'I.G.C.

VI.2.9.2 Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur doivent permettre de répondre aux exigences définies dans le chapitre XII.

VI.2.10 Méthode de destruction des clés privées

VI.2.10.1 Clés privées d'A.C.

Ces questions sont traitées dans d'autres documents de spécifications de l'I.G.C.

VI.2.10.2 Clés privées des porteurs

Les clés privées des porteurs étant générées par l'A.C. dans un module cryptographique hors du dispositif de création de signature, la méthode de destruction de ces clés privées après leur exportation hors du module cryptographique permet de répondre aux exigences définies dans le chapitre XII.

En fin de vie de la clé privée d'un porteur, la méthode de destruction de cette clé privée permet de répondre aux exigences définies dans le chapitre XII.

VI.2.10.3 Niveau de qualification du module cryptographique et des dispositifs de création de signature

Ces exigences sont précisées aux chapitres XI et XII.

VI.2.11 Autres aspects de la gestion des biclés

VI.2.11.1 Archivage des clés publiques

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

VI.2.11.2 Durées de vie des biclés et des certificats

Les biclés et les certificats des porteurs couverts par la présente DPC ont une durée de vie d'au maximum trois ans.

La fin de validité d'un certificat d'A.C. est postérieure à la fin de vie des certificats porteurs qu'elle émet.

VI.3 Données d'activation

VI.3.1 Génération et installation des données d'activation

VI.3.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'A.C.

Ces questions sont traitées dans d'autres documents de spécifications de l'I.G.C.

VI.3.1.2 Génération et installation des données d'activation correspondant à la clé privée du porteur

Les données d'activation sont déterminées par le porteur lui-même durant le processus d'enrôlement.

VI.3.2 Protection des données d'activation

VI.3.2.1 Protection des données d'activation correspondant à la clé privée de l'A.C.

Ces questions sont traitées dans d'autres documents de spécifications de l'I.G.C.

VI.3.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Les données d'activation sont sous la responsabilité des porteurs.

VI.4 Mesures de sécurité des systèmes informatiques

Toutes les composantes de l'IGC mettent en place, en fonction du système à protéger, des mécanismes de contrôle appropriés à la plate-forme à sécuriser afin de se protéger contre l'exécution de code non autorisé ou potentiellement dangereux sur son système.

Chaque composante met en place des mécanismes de contrôle d'accès et d'authentification pour toutes les rôles permettant la génération de nouveaux certificats.

Toutes les composantes de l'IGC appliquent les mesures décrites dans le *Guide d'hygiène informatique* de l'ANSSI (https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/).

VI.5 Mesures de sécurité liées au développement des systèmes

Tous les composants logiciels de l'IGC sont développés dans des conditions et suivant un processus de développement donnant des assurances sur leur sécurité. L'AC met en œuvre des processus qualité au cours du design et du développement de ses logiciels. L'AC s'assure, lors de la mise en production d'un élément logiciel, de son origine et de son intégrité et assure une traçabilité de l'ensemble des modifications apportées sur son SI.

Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles de l'IGC.

VI.6 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'I.G.C.

L'A.C. s'assure que les composants du réseau local sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'A.C.

De plus, les échanges entre composantes au sein de l'I.G.C. peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

VI.7 Horodatage / Système de datation

L'ensemble des serveurs de l'AC et de ses composantes sont quotidiennement synchronisés avec une source de temps UTC.

VII PROFILS DES CERTIFICATS, OCSP ET DES LCR

VII.1 Certificats de porteurs

Les certificats des porteurs sont émis suivant le profil ci-dessous. Dans ce profil, certains éléments dépendent de l'A.C. du porteur (voir sections suivantes).

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	Voir III.1.2.1
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (3 ans après la date d'émission du certificat)
Subject	C=FR Serialnumber=Code unique de l'expert-comptable (voir III.1.2.2) givenName=*[Prénom]* surName=*[Nom]* CN=*[Prénom Nom]*
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1
Key size	2048
Signature (algorithm & OID)	SHA256WithRsaEncryption
Authority Key Identifier	Identification de la clé publique de l'A.C. émettrice (voir VII.2)
keyIdentifier	issuerName+serialNumber
Subject Key Identifier	Identification de la clé publique du porteur
Key Usage (critical)	contentCommitment
Certificate Policies (critical)	
policyIdentifier	1.3.6.1.4.1.15819.5.1.3.3
policyQualifier-cps	http://docs.universign.eu
Explicit text	CPS : 1.2.250.1.165.1.13.1.1
X509v3	
Basic Constraint (critical)	CA:False
CRL Distribution Points	
distributionPoint	http://crl.jesignexpert.com/csoecadvanced.crl
Authority Information Access	
ocsp	http://ocsp.jesignexpert.com/advancedCA_ocsp
caIssuer	http://ca.jesignexpert.com/certificate/certificateCA-CSOEC.cer

VII.2 Certificat d'A.C.

Champ	Valeur
Version	3 (0x2)
Serial Number	d3 ac 32 0e 90 ec 0b 5e 65 26 c0 eb 2d 92 78 6f
Signature Algorithm	sha256WithRSAEncryption
Issuer	C=FR O=Cryptolog International OU=002 43912916400026 CN=Universign Primary CA Hardware
Not Before	Oct 8 10:44:18 2018 GMT
Not After	Oct 8 10:44:18 2028 GMT
Subject	Voir III.1.2.1
Public Key Algorithm	(rsaEncryption) 1.2.840.113549.1.1.1
RSA Public Key	4096
Modulus (4096 bit)	…
Exponent	65537 (0x10001)
X509v3 Key Usage (critical)	Certificate Sign, CRL Sign
X509v3 Certificate Policies	
policyIdentifier	anyPolicy
PolicyQualifiers-CPS	http://docs.universign.eu
X509v3 Basic Constraints (critical)	CA:TRUE, pathlen:0
X509v3 CRL Distribution Points	http://crl.universign.eu/universign_primary_ca_hardware.crl
X509v3 Subject Key Identifier	BF CD E6 0F 93 F2 9C DA 4C 62 CD 97 D5 F4 68 58 8D 17 C6 F6
X509v3 Authority Key Identifier	4D D9 FC A8 2D C7 C8 5A A4 AD 5F 49 AE 68 A4 DC 9E 8A 12 22
Signature Algorithm	sha256WithRSAEncryption

VII.3 Liste de Certificats Révoqués

Champ	Valeur
Version	1 (=version 2)
Issuer DN	Voir III.1.2.1
ThisUpdate	AAAA/MM/JJ HH:MM:SS Z (date d'émission de la CRL)
NextUpdate	AAAA/MM/JJ HH:MM:SS Z (7 jours après date d'émission)
Signature (algorithm & OID)	SHA256WithRsaEncryption
CRL Extension	
CRLNumber	Numéro de la CRL
AKI	BF CD E6 0F 93 F2 9C DA 4C 62 CD 97 D5 F4 68 58 8D 17 C6 F6

VII.4 Certificat des réponses OCSP

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	DN de l'A.C. émettrice (voir VII.2)
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (2 ans après la date d'émission du certificat)
Subject	C=FR O=Conseil Superieur de l'Ordre des Experts-Comptables OU=0002 775670003 OI=NTRFR-775670003 CN=OCSP Jesignexpert.com [numéro de certificat]
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1
Key size	2048
Signature (algorithm & OID)	SHA256WithRsaEncryption
Authority Key Identifier	Identification de la clé publique de l'A.C. émettrice (voir VII.2)
keyIdentifier	issuerName+serialNumber
Subject Key Identifier	Identification de la clé publique du porteur
Key Usage (critical)	digitalSignature
X509v3	
Basic Constraint (critical)	CA:False
Extended Key Usage	OCSPSigning
OCSP No Check	null

VIII AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent,

- D'une part, ceux réalisés en vue de la certification à la norme ETSI EN 319 411-1 ;
- Et, d'autre part, ceux que doit réaliser, ou faire réaliser, le PSCE afin de s'assurer que l'ensemble de son I.G.C. est bien conforme à ses engagements affichés dans sa DPC et aux pratiques identifiées dans sa DPC.

La suite du présent chapitre ne concerne donc que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son I.G.C.

VIII.1 Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son I.G.C. ou suite à toute modification significative au sein d'une composante, le PSCE procède à un contrôle de conformité de cette composante. L'A.C. procède régulièrement à un contrôle de conformité de l'ensemble de son I.G.C., une fois par an.

VIII.2 Identités / qualifications des évaluateurs

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

VIII.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'I.G.C. contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

VIII.4 Sujets couverts par les évaluations

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

VIII.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend au PSCE, 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'A.C. et doit respecter ses politiques de sécurité internes.
- En cas de résultat « à confirmer », l'A.C. remet à la composante un avis précisant sous quel délai les non-conformités sont levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'A.C. confirme à la composante contrôlée la conformité aux exigences de la DPC et la DPC.

VIII.6 Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'autorité racine.

IX AUTRES PROBLEMATIQUES METIERS ET LEGALES

IX.1 Tarifs

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

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

IX.1.2 Tarifs pour accéder aux certificats

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

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

L'accès aux LCR, OCSP et, éventuellement, deltaLCR est en accès libre en lecture.

IX.1.4 Tarifs pour d'autres services

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

IX.1.5 Politique de remboursement

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

IX.2 Responsabilité financière

La responsabilité financière de l'AC pour l'émission de certificats est déterminée par la loi (*art 33 de la Loi n° 2004-801 du 6 août 2004 relative à la confiance dans l'économie numérique*).

IX.3 Confidentialité des données professionnelles

IX.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- La partie non-publique de la DPC de l'A.C.,
- Les clés privées de l'A.C., des composantes et des porteurs de certificats,
- Les données d'activation associées aux clés privées d'A.C. Et des porteurs,
- Tous les secrets de l'I.G.C.,
- Les journaux d'événements des composantes de l'I.G.C.,
- Les dossiers d'enregistrement des porteurs,
- Les causes de révocations, sauf accord explicite du porteur.

IX.3.2 Informations hors du périmètre des informations confidentielles

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

IX.3.3 Responsabilités en termes de protection des informations confidentielles

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations identifiées en IX.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'A.C. en garantit l'intégrité.

L'AC respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au porteur.

IX.4 Protection des données personnelles

IX.4.1 Politique de protection des données personnelles

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

IX.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- Le dossier d'enregistrement du porteur.

IX.4.3 Informations à caractère non personnel

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

IX.4.4 Responsabilité en termes de protection des données personnelles

Application de la législation et de la réglementation en vigueur sur le territoire français.

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

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'A.C. ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Se référer à la législation et réglementation en vigueur sur le territoire français.

IX.4.7 Autres circonstances de divulgation d'informations personnelles

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

IX.5 Droits sur la propriété intellectuelle et industrielle

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

IX.6 Interprétations contractuelles et garanties

Sans objet.

IX.7 Limite de garantie

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

IX.8 Limite de responsabilité

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

IX.9 Indemnités

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

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

IX.10.1 Durée de validité

La DPC de l'A.C. reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette DPC.

IX.10.2 Fin anticipée de validité

L'adoption d'actes d'exécution ou délégués du règlement eIDAS peut entraîner, en fonction des évolutions apportées, la nécessité pour l'A.C. de faire évoluer la présente DPC.

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

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

IX.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'I.G.C., l'A.C. devra :

- Au plus tard un mois avant le début de l'opération, faire 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, en informer l'organisme de qualification.

IX.12 Amendements à la DPC

Les amendements à la P.C. ne peuvent être apportés que par le PSCE.

L'OID de la DPC de l'A.C. étant inscrit dans les certificats qu'elle émet, toute évolution de cette DPC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) donnera lieu à une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

IX.13 Dispositions concernant la résolution de conflits

Le PSCE met en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles il fournit des services électroniques de confiance ou d'autres points qui y sont liés.

IX.14 Juridictions compétentes

Application de la législation et de la réglementation en vigueur sur le territoire français.

IX.15 Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente DPC sont, notamment, ceux indiqués au chapitre X ci-dessous.

IX.16 Transfert d'activités

Cf. chapitre V.8.

X ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

[DPC-OCSP] *PGS-OEC Politique de Certification – OCSP AC Unique*

X.1 Législation et réglementation

Ordonnance nº 45-2138 du 19 septembre 1945
Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi nº 2004-801 du 6 août 2004.
Règlement (UE) Nº 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dit « Règlement eIDAS »)

X.2 Documents techniques

Document
ETSI EN 319401, *General Policy Requirements for Trust Service Providers*, v. 2.1.1
ETSI EN 319411, *Policy & Security Requirements for TSPs Issuing Certificates*
ETSI EN 319412, *Certificate Profiles*
AFNOR AC Z74-400, *Exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés* (traduction de : ETSI TS 101 456 V1.4.3 (mai 2007) "*Policy Requirements for Certification Authorities issuing qualified certificates*").
RFC3647 - IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003

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

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

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

Il est recommandé que le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.

XII ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF DE CREATION DE SIGNATURE

XII.1 Exigences sur les objectifs de sécurité

Les dispositifs de création de signature électronique utilisés par les porteurs garantissent au moins, par des moyens techniques et des procédures appropriés, que :

a) La confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ;
b) Les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois ;
c) L'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ;
d) Les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

Les dispositifs de création de signature électronique utilisés par les porteurs ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.

XII.2 Exigences sur la qualification

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