ORDRE DES EXPERTS-COMPTABLES

Conseil Supérieur

POLITIQUE DE CERTIFICATION « Cachet Serveur »
DE LA PROFESSION COMPTABLE

Version 1.3

du 7 septembre 2015

OID n° 1.2.250.1.165.1.8.1.1

Signature numérique de Jean Saphores

HISTORIQUE DES VERSIONS

Date	Évolutions	Édition / révision
05/01/12	Création du document	0.1
24/04/12	Mise à jour processus	0.2
23/05/12	Compléments	0.3
06/06/12	Détail des processus de délivrance et de révocation	0.4
07/12	Compléments	0.5
07/12	Version pour signature	1.0
12/12	Corrections mineures + Ajout région Corse	1.1
06/15	Mises à jour R.G.S. v2	1.2
08/15	Corrections suite audit externe	1.3

Contributeurs	Organisation
Stéphane GASCH	CSOEC
Thierry PIETTE-COUDOL	Avocat
Samuel LACAS	SEALWeb
Jean SAPHORES	CSOEC

TABLE DES MATIÈRES

I INTRODUCTION

I.1 Présentation générale

Le Conseil Supérieur de l'Ordre des Experts-Comptables a décrit dans sa *Politique Générale de Sécurité* (PGS-OEC) les diverses fonctions de sécurisation à mettre en œuvre lors des échanges électroniques avec les administrations comme avec ses autres partenaires professionnels. Parmi les fonctions et instruments de sécurisation figure la signature électronique dont conditions et modalités de d'organisation et fonctionnement sont décrites dans un document de type « PGS-OEC Politique de Certification ». Le présent document constitue cette politique.

Ce document constitue une Politique de Certification (P.C.) mise en œuvre par une Autorité de Certification de l'Ordre des Experts Comptables (OEC) pour les membres de l'Ordre. Elle réunit l'ensemble des obligations et engagements des différents acteurs relatifs à la délivrance et l'usage des certificats numériques pour des cabinets (sociétés) d'expertise comptable.

Dans le cadre de cette P.C., les certificats sont à destination de services applicatifs déployés sur des serveurs informatiques afin de signer (« cachet électronique », ou sceau) des données qu'ils transmettent.

Cette P.C. est conforme aux principes et recommandations de la *Politique Générale de Sécurité* (PGS) de l'OEC et met en œuvre un niveau de sécurité deux étoiles (ci-après « ** ») selon la typologie en vigueur dans le *Référentiel Général de Sécurité* (R.G.S.).

I.2 Identification du document

La présente P.C. est dénommée *PGS-OEC Politique de Certification – Cachet Serveur*. Elle est identifiée par le numéro d'identifiant d'objet (OID) suivant, ainsi que par le nom, numéro de version, et la date de mise à jour.

Le numéro d'OID de cette P.C. sera porté dans les certificats correspondants.

OID de la présente P.C. : 1.2.250.1.165.1.8.1.1

Le type de service R.G.S. correspondant est (P.C. Type Cachet, OID : 1.2.250.1.137.2.2.1.2.2.6) :

Service	**Niveau de sécurité**	**Type de certificat**
Cachet serveur	**	Entreprise

La P.C. est complétée par une *Déclaration des Pratiques de Certification* correspondante référencée par un numéro d'OID. La *Politique de Certification* et la *Déclaration des Pratiques de Certification* identifiées ci-dessus sont désignes dans la suite du document respectivement sous le nom de « P.C. » et de « D.P.C. ».

I.2.1 Transfert de compétence de la région PACAC

Le CROEC de Marseille Provence Alpes Côte-d'Azur Corse est remplacé par les CROEC de Corse et de Provence Alpes Côte-d'Azur à la date du 1er octobre 2012. Par décret ministériel, ce dernier est le successeur, « à compétence territoriale réduite », du Conseil Régional de Marseille Provence Alpes Côte-d'Azur Corse, et a été « investi de l'ensemble des droits et obligations » de celui-ci. Le SIREN est, par ailleurs, inchangé.

Afin d'assurer la continuité de service des A.C., la population des porteurs PACAC sera partitionnée pour rattachement aux A.C. PACA et Corse. Les A.E. de ces deux structures auront autorité pour renouveler les certificats PACAC correspondants.

I.3 Entités intervenant dans l'I.C.P. et responsabilités

I.3.1 Le Prestataire de services de certification électronique

Dans le cadre de cette P.C., ***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 seul 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.

En tant que PSCE, le CSOEC comporte plusieurs A.C., au minimum autant que de CROEC et que de CDOEC (voir ci-dessous pour l'ensemble des A.C. du CSOEC).

Le PSCE est identifié dans tout certificat dont il a la responsabilité au travers des A.C. ayant émis ce certificat et qui sont elles-mêmes directement identifiées dans le champ "*issuer*" (émetteur) du certificat.

I.3.2 Autorité de certification (A.C.)

L'A.C. 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.C.P.).

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

Dans le cadre de cette politique, ***l'A.C. est le CSOEC lui-même***. Elle est identifiée dans les certificats par le nom « OEC - CC ».

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.C.P. qui est retenue dans la présente P.C. est la suivante :

Fonction d'enregistrement (A.E.)	A.E. et A.E. technique
Fonction de génération des certificats	A.C. et OSC
Fonction de génération des éléments secrets du R.C. (responsable du certificat)	A.C. et OSC
Fonction de remise au R.C.	A.E.
Fonction de publication	A.C. (documents, certificats d'A.C.) et OSC (LCR)
Fonction de gestion des révocations	A.E. et 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'A.C. en tant que responsable de l'ensemble de l'I.C.P. 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 R.C. de cette entité.

- Rendre accessible l'ensemble des prestations déclarées dans sa P.C. aux promoteurs d'application d'échanges dématérialisés de l'administration, aux R.C., aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la P.C. et les procédures de la D.P.C. sont appliquées par chacune des composantes de l'I.C.P. et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa P.C., correspondant au minimum aux fonctions obligatoires de la présente P.C., notamment en matière de génération des certificats, de remise au R.C., 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'A.C. 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.C.P. et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre pour atteindre un niveau de sécurité (**). Elle élabore sa D.P.C. en fonction de cette analyse.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa P.C., et correspondant au minimum aux exigences de la présente P.C., 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'A.C. est rattachée à une A.C. hiérarchiquement supérieure. Diffuser ses certificats d'A.C. aux R.C. 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.3.3 Autorité d'enregistrement (A.E.)

L'A.E. a pour rôle de vérifier l'identité du futur R.C. Pour cela, l'A.E. assure les tâches suivantes :

- la prise en compte et la vérification des informations du futur R.C. et de son entité de rattachement ; constitution du dossier d'enregistrement correspondant ;
- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'I.C.P. 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 R.C. y compris lors des échanges de ces données avec les autres fonctions de l'I.C.P. (notamment, elle respecte la législation relative à la protection des données personnelles).

La fonction d'AE est exercée par le Conseil supérieur de l'Ordre (permanents du CSOEC).

Toutefois, une partie des procédures de gestion des certificats (délivrance, révocation, etc.) étant dématérialisée, les A.E. s'appuient sur une autorité d'enregistrement technique tierce, en charge du système d'information des A.E. ; se référer à la D.P.C. pour plus de détail.

I.3.4 Opérateur de certification (OC/OSC)

Se référer à la D.P.C.

I.3.5 Responsable de certificat de cachet (R.C.)

Le R.C. est la personne physique responsable du certificat de cachet, notamment de l'utilisation de ce certificat et de la biclé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat.

Dans le cadre de la présente P.C., un R.C. ne peut être qu'un expert-comptable personne physique (cf. I.6.2) disposant d'un certificat *Signexpert* valide.

Cette personne utilise la clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle elle a un lien réglementaire. Dans le cadre de cette P.C., le RCC est forcément :

- Mandataire social de cette entité
- Salarié de cette entité
- Représentant ordinal de l'entité
- ou exerce son activité d'expert-comptable dans l'entité.

Le R.C. respecte les conditions qui lui incombent telles que définies dans la présente P.C.

Il est rappelé que le certificat étant attaché au serveur informatique et non au R.C., ce dernier peut être amené à changer en cours de validité du certificat : départ du R.C. de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.

L'entité doit signaler à l'A.C. préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un R.C. de ses fonctions et lui désigner un successeur. L'A.C. révoque un certificat de cachet pour lequel il n'y a plus de R.C. explicitement identifié.

I.3.6 Utilisateurs de certificat

La présente P.C. traitant de certificats de signature, un utilisateur de certificat peut être notamment :

- Un agent (personne physique) destinataire de données signées par un serveur informatique et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- Un usager destinataire de données provenant d'un serveur informatique d'une autorité administrative et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat.
- Un serveur informatique destinataire de données provenant d'un autre serveur informatique et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat.

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document fournis par l'A.C. En particulier, l'A.C. 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.4 Usage des certificats

I.4.1 Domaines d'utilisation applicables

I.4.1.1 Biclés et certificats serveurs

La présente P.C. traite des biclés et des certificats utilisés par des services applicatifs déployés sur des serveurs informatiques dont la fonction est de signer des données, afin que les catégories d'utilisateurs de certificats identifiées au chapitre I.3.6 ci-dessus puissent en vérifier la signature (le cachet). Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par

un usager à un serveur informatique, une réponse automatique d'un serveur informatique à une demande formulée par un usager ou la signature d'un jeton d'horodatage.

Ceci correspond notamment aux relations suivantes :

- apposition d'un cachet sur des données par un serveur informatique et vérification de ce cachet par la personne destinataire des données,
- apposition d'un cachet sur des données par un serveur informatique et vérification de ce cachet par un autre serveur informatique.

Les certificats de signature objets de la présente P.C. sont utilisés au niveau (**) 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'A.C. Dans certains cas, une A.C. spécifique « de test » pourra être mise en place ; des certificats de test pourront aussi être émis.

I.4.1.2 Biclés et certificats d'A.C. et de composantes de l'I.C.P.

La hiérarchie d'A.C. du CSOEC est la suivante :

L'A.C. de l'Ordre des Experts-Comptables est la racine de la hiérarchie. En-dessous, se trouvent trois types d'A.C. subalternes :

- L'A.C. des élus de l'OEC (bleu)
- Des A.C. techniques (orange), parmi lesquelles se trouve l'A.C. « OEC - CC », objet de la présente politique.
- Des A.C. régionales et départementales (violet)

Pour des détails à propos des A.C. régionales « Marseille PACA/PACAC » et Corse, voir I.2.1.

I.4.1.2.1 Certificats d'A.C.

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

I.4.1.2.2 Certificats de composante

Se référer à la D.P.C.

I.4.2 Domaines d'utilisation interdits

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

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

I.5 Gestion de la P.C.

I.5.1 Entité gérant la P.C.

La P.C. est gérée par le CSOEC. Cette fonction est dévolue au CSOEC par le Règlement Intérieur de l'Ordre des Experts-Comptables.

I.5.2 Point de contact

La rédaction, la modification et la diffusion de la P.C. 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.5.3 Entité déterminant la conformité d'une D.P.C. avec cette P.C.

Le CSOEC agissant comme PSCE confie à la DEI le soin et la responsabilité finale pour déterminer la conformité de la D.P.C. avec la P.C.

I.5.4 Procédures d'approbation de la conformité de la D.P.C.

La D.P.C. sera déclarée conforme à la P.C. à l'issue d'un processus d'approbation élaboré par le CSOEC.

Toute mise à jour de la D.P.C. suivra le processus d'approbation mis en place et sera publiée, conformément aux exigences du paragraphe II sans délai.

I.6 Définitions et abréviations

I.6.1 Abréviations

Les abréviations utilisées dans la présente P.C. 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)*
CROEC	Conseil Régional de l'Ordre des Experts-Comptables
CSOEC	Conseil Supérieur de l'Ordre des Experts-Comptables
DCS	Dispositif de Création de Signature
DN	*Distinguished Name* (nom distinctif)

D.P.C.	Déclaration des Pratiques de Certification
EC	Expert-Comptable
ETSI	*European Telecommunications Standards Institute*
I.C.P.	Infrastructure à Clés Publiques
LCR	Liste des Certificats Révoqués
OSC	Opérateur de Service de Certification
OC	Opérateur de Certification
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier* (identifiant d'objet)
P.C.	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique
SGMAP	Secrétariat Général pour la Modernisation de l'Action Publique
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
URL	*Uniform Resource Locator* (adresse universelle)

I.6.2 Définitions

Les termes utilisés dans la présente P.C. sont les suivants :

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

Autorité d'Enregistrement (A.E.) : Fonction ou entité chargée de la vérification que les demandeurs ou les R.C. 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.

Ici, l'A.E. contrôle de la validité du certificat *Signexpert* du R.C., assurant indirectement l'inscription professionnelle du demandeur sur le tableau régional géré par le CROEC/CDOEC auquel appartient l'A.E.

Autorité de Certification (A.C.) : L'A.C. assure les fonctions suivantes :

- rédaction des documents de spécifications de l'I.C.P., notamment la PS et les P.C.,
- mise en application de la P.C. ;
- 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.C.P. ;
- maintenance et évolution de la P.C. et de l'I.C.P. ;
- journalisation et archivage des événements et informations relatives au fonctionnement de l'I.C.P., à son niveau.

Autorité de Certification Racine (ou **A.C. Racine**) **:** désigne l'entité de plus haut niveau dans l'infrastructure à Clé publiques et qui certifie les autorités de certification filles. Dans le cadre des présentes, l'A.C. Racine est celle de l'Ordre des Experts-Comptables. À ce titre, les A.C. des CROEC/CDOEC peuvent être qualifiées d'A.C. « filles » ou « subalternes ».

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'A.C. valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la biclé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Certificat Signexpert - Sans plus de précision, ce terme désigne l'un des deux certificats émis par les A.C. des CROEC ou CDOEC aux experts-comptables de la profession. Ces certificats sont des certificats de signature de niveau R.G.S. (***) [PC_S] ou signature-authentification R.G.S. (**) [PC_AS].

On parle aussi, pour désigner ces certificats, de « certificats Signexpert d'expert-comptable », pour les différencier, par exemple, des certificats émis par le CSOEC pour ses élus.

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

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

Dispositif de création de signature électronique (DCS) : un matériel ou un logiciel destiné à générer un biclé cryptographique et à mettre en œuvre la clé privée pour générer la signature électronique. Le DCS est dit "sécurisé" (DSCS) lorsqu'il satisfait aux exigences définies au I de l'article 3 du décret n° 2001-272 du 30 mars 2001.

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 alphanumérique 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.C.P., les identificateurs OID servent notamment à identifier chacune des politiques, ainsi que les algorithmes de chiffrement acceptés.

Infrastructure à Clés Publiques (**I.C.P.**) : 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.C.P. génère, distribue, gère et archive les Certificats. Chacune des composantes de l'I.C.P. est décrite dans la Politique de certification définissant le niveau de confiance confié à chacune d'entre elles.

Opérateur de Service de Certification (OSC) : composante de l'I.C.P. 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.C.P. par lequel un certificat est validé (non révocation) en ligne. Le protocole fait l'objet de la norme RFC 2560.

Politique de certification (P.C.) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une A.C. se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière ou à une classe d'applications avec des exigences de sécurité communes. Une P.C. peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les R.C. 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 et (iv) télécharge le Progiciel de signature sur son poste informatique.

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 R.C. et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes ou des niveaux de sécurité différents. Un PSCE comporte au moins une A.C. mais peut en comporter plusieurs en fonction de son organisation. Les différentes A.C. d'un PSCE peuvent être indépendantes les unes des autres ou liées par des liens hiérarchiques ou autres (A.C. Racines / A.C. Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son A.C. 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 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 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 P.C. pour un niveau de sécurité donné et correspondant au service visé par les certificats.

Qualification d'un produit de sécurité - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le RGS. La procédure de qualification des produits de sécurité est décrite dans le Décret du 8 décembre 2005 précité. Le RGS précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Support : désigne un support physique contenant la clé privée et le ou les certificats électroniques (d'authentification et de signature), protégés à l'aide d'un code PIN, et permettant des opérations cryptographiques.

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. Rappelons aussi qu'une personne physique peut détenir plusieurs certificats, avec un même SUPRA, mais dans ce cas, les SIRET seront différents.

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

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

L'A.C. met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats sur les informations devant être publiées à destination des R.C. et des utilisateurs de certificats (*cf.* chapitre I.3.1 ci-dessus).

Les méthodes de mise à disposition et les adresses universelles correspondantes (annuaire accessible par le protocole LDAP ou HTTP, serveur OCSP, etc.) sont précisées ci-après.

II.2 Informations devant être publiées

L'A.C. a pour obligation de publier au minimum les informations suivantes à destination des R.C. 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'A.C., en cours de validité
- le certificat de l'A.C. Racine et son empreinte cryptographique (SHA-256)
- la P.C. de l'A.C.

L'A.C. a également pour obligation de publier sur un modèle établi par le PSCE, à destination des R.C., 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.10), est libre et précisé plus loin dans la P.C. 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.C.P. (nouvelle version de la P.C., 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'A.C. En particulier, toute nouvelle version sera communiquée au R.C. lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent avoir une disponibilité de 24 h sur 24.

Les certificats d'A.C. sont diffusés préalablement à toute diffusion de certificats de R.C. ou de LCR correspondants et les systèmes les publiant doivent avoir la même disponibilité.

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.9 et IV.10.

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.C.P., 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'A.C. émettrice (*issuer*) et le R.C. (*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 services de création de cachet sont explicites.

Le DN du certificat est construit à partir des éléments fournis par le demandeur et vérifiés par l'A.E.

III.1.2.1 Identité des A.C émettrices

L'A.C. émettrice est identifiable par son DN, comme suit.

DN de l'A.C.	Entité
CN = Ordre des Experts-Comptables - CC **OU = 0002 775670003** **O = Conseil Supérieur de l'Ordre des Experts-Comptables** **C = FR**	Conseil Supérieur de l'Ordre des Experts-Comptables

Conformément au R.G.S., le DN de cette A.C. est construit comme suit :

- le champ `C` désigne le pays de l'A.C.
- le champ `O` contient le nom officiel de l'organisme en charge de l'A.C.
- le champ `OU` contient le SIREN de cet organisme
- le champ `CN` identifie l'A.C. au sein de cet organisme

III.1.2.2 Identité des services de création de cachet

Le DN des certificats est construit comme suit :

- Le champ `C=FR` désigne la France.
- Le champ `O` désigne le nom officiel de l'organisme de rattachement du service (tel qu'inscrit au registre du commerce, le cas échéant).
- Le champ `OU` contient soit le SIREN de ce même organisme (9 caractères), soit le SIRET d'un établissement de cet organisme (14 caractères), précédé de la chaîne « 0002 » et séparé de celle-ci par une espace.
- Le champ `CN` contient le nom du service tel que déclaré par le RCC.
- Le champ `Title` contient l'une des valeurs suivantes :
    - `Cabinet d'expertise comptable`
    - `Société d'expertise comptable`
    - `Association de gestion comptable`
    - `Institut régional de formation`
    - `Conseil régional de l'Ordre des experts-comptables`
    - `Conseil supérieur de l'Ordre des experts-comptables`
    - `Association au service des membres de l'Ordre des experts-comptables`
    - `Expert-comptable`

- Le champ `serialNumber` contient un identifiant propre au certificat ; ce champ est déterminé par le RCC et contrôlé par l'A.C. (*cf.* III.1.5).
- Le champ optionnel `Subject Alternative Name` contient une adresse courriel relative au service applicatif (attribut `rfc822Name`)

III.1.2.3 Certificats de test

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

CES CERTIFICATS NE SONT PAS ATTRIBUES A DES CABINETS D'EXPERTISE COMPTABLES ET NE DOIVENT EN AUCUN CAS ETRE CONSIDERES COMME TELS.

III.1.3 Anonymisation ou pseudonymisation des services de création de cachet

Sans objet.

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

Sans objet.

III.1.5 Unicité des noms

Le DN du champ "*subject*" de chaque certificat permet d'identifier de façon unique le couple {nom du service de création d'un cachet ; entité de rattachement} au sein du domaine de l'A.C.

Dans chaque certificat X.509v3, l'A.C. émettrice (*issuer*) et le service de création de cachet (*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 `serialNumber` du DN (y compris pour les certificats de test) : bien que déterminé par le demandeur, l'A.C. vérifie l'unicité du DN au moment de la demande et la rejette si un certificat ayant le même DN a déjà été émis.

L'anonymat ou le pseudonyme des services de cachet ne sont pas supportés par la présente P.C.

III.1.6 Identification, authentification et rôle des marques déposées

L'A.C. est responsable de l'unicité des noms et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

III.2 Validation initiale de l'identité

L'enregistrement d'un service de création de cachet d'une entité auquel un certificat doit être délivré se fait via l'enregistrement du R.C. correspondant.

La demande initiale est saisie sur une application en liaison avec les tableaux régionaux de l'Ordre. L'identité du demandeur est issue du certificat *Signexpert* (certificat de signature) présenté lors de la demande.

Un R.C. peut être amené à changer en cours de validité du certificat de cachet correspondant (voir chapitre I.3.3), dans ce cas, tout nouveau R.C. doit également faire l'objet d'une procédure d'enregistrement.

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 R.C.

L'enregistrement du futur R.C. (personne physique) représentant une entité nécessite, l'identification de cette entité et l'identification de la personne physique. S'agissant d'un certificat de cachet, le R.C. doit de plus être habilité en tant que R.C. pour le service de création de cachet considéré.

Le dossier d'enregistrement, déposé directement auprès de l'A.E., doit au moins comprendre :

- une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du service de création de cachet concerné par cette demande,
- Le SIREN de l'entité responsable du service de création de cachet
- une copie de la carte d'identité du représentant légal, si celui-ci ne dispose pas d'un certificat électronique recevable (voir IV.2.1 ci-après)
- Un courriel et un numéro de téléphone du représentant légal
- un mandat, daté de moins de 3 mois, désignant le futur R.C. comme étant habilité à être R.C. pour le service de création de cachet pour lequel le certificat de cachet doit être délivré.

  Le mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur R.C.
- les conditions générales d'utilisation signées

L'authentification du R.C. par l'A.E. est réalisée à travers :

1. la signature de la demande par le R.C. en utilisant l'un de ses certificats *Signexpert*
2. la vérification par l'A.E. de cette signature au moment de l'enregistrement de la demande

Ces éléments permettent par ailleurs à l'A.E. de s'assurer de :

i. l'existence de l'entreprise qui figurera dans le certificat et du numéro SIREN de celle-ci.
ii. la qualité du signataire de la demande de certificat
iii. l'identité du R.C., via une pièce officielle comportant une photographie d'identité

En effet, les points (ii) et (iii) ont été préalablement vérifiés lors de la délivrance du certificat *Signexpert* au R.C., et le point (i) est vérifié à partir des référentiels de l'Ordre.

III.2.3.2 Enregistrement d'un Mandataire de Certification

Sans objet.

III.2.3.3 Enregistrement d'un R.C. via un MC

Sans objet

III.2.4 Informations non vérifiées du R.C.

La présente P.C. 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 (R.C.).

III.2.6 Certification croisée d'A.C.

Pas d'exigences en l'état actuel de la P.C.

III.3 Identification et validation d'une demande de renouvellement des clés

Les biclés des serveurs et les certificats correspondants sont renouvelés tous les trois ans. Le renouvellement de la biclé d'un serveur entraîne automatiquement la génération et la fourniture d'un

nouveau certificat dans des conditions et suivant des modalités identiques à la procédure d'enregistrement initial.

Dans tous les cas, un nouveau certificat de cachet ne peut pas être fourni au R.C. sans renouvellement de la biclé correspondante (*cf.* chapitre IV.6).

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

Le R.C. peut demander la révocation de son certificat par différents moyens :

- Sur le Portail Client ou celui de l'OSC : le R.C. s'identifie à l'aide du code de révocation choisi lors de sa demande de certificat.
- Depuis son espace personnel *Signexpert* : le R.C. est authentifié sur sa page personnelle à travers son certificat *Signexpert*.
- En envoyant par courriel au CSOEC (signexpert@cs.experts-comptables.org) un formulaire de demande de révocation électronique signé avec son certificat de signature *Signexpert*.
- Auprès de son CSOEC : le R.C. peut se présenter directement muni d'une pièce d'identité.

Enfin, le représentant légal de l'entité responsable du service de cachet peut demander la révocation du certificat auprès du CSOEC en saisissant le code de révocation à partir de son espace, tous deux définis lors de la demande (voir IV.1.2 ci-après).

Dans tous les cas, le R.C. est informé de la demande (IV.9.3).

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 disposant d'un certificat *Signexpert* d'expert-comptable en cours de validité.

L'A.E. assure la validation de la demande de certificat en s'appuyant sur la vérification du certificat, des signatures électroniques et sur les documents présentés.

Une demande de certificat n'oblige en rien l'A.C. à émettre un certificat. Un refus doit cependant être motivé.

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

IV.1.2.1 Demande en ligne

L'expert-comptable se connecte au site Portail internet client et s'authentifie en utilisant sa clé *Signexpert*. Il peut alors choisir de demander un certificat pour un service de création de cachet d'un cabinet d'expertise comptable reconnu par l'Ordre.

Les informations suivantes font partie de la demande de certificat :

- le nom du service de création de cachet à utiliser dans le certificat
- les données personnelles d'identification du R.C. ([1])
- le CROEC/CDOEC d'inscription du demandeur ([1])
- le SIREN du cabinet d'expertise comptable responsable du service de création de cachet
- le mandat, daté de moins de 3 mois, désignant le R.C. comme étant habilité à être R.C. pour le service de création de cachet pour lequel le certificat de cachet doit être délivré.
    - Si le R.C. est le représentant légal du cabinet, ce mandat est signé électroniquement par le R.C. dans le cadre de la signature de sa demande.
    - Si le R.C. n'est pas le représentant légal du cabinet, le mandat est soit signé électroniquement par un représentant légal du cabinet et co-signé par le R.C. dans le cadre de la signature de sa demande, soit transmis à l'A.E. par voie postale.

      La signature électronique du représentant légal, le cas échéant, doit être faite en utilisant un certificat de signature qui porte la qualité de représentant légal du cabinet.
- Un numéro de série pour le certificat
- Un courriel et un numéro de téléphone du représentant légal
- Une copie de la carte d'identité (ou du passeport) du représentant légal

([1]) Ces éléments proviennent du certificat *Signexpert* utilisé par le R.C. pour se connecter au portail.

L'expert-comptable confirme l'exactitude de ces informations et les signe électroniquement à l'aide de son certificat *Signexpert*. Toujours sur le portail Web, il procède ensuite à la saisie…

- des questions de révocation
- de l'adresse de facturation

Après le paiement en ligne des frais relatifs à l'acquisition du certificat, la demande est traitée par l'A.E.

IV.1.2.2 Demande en face-à-face

Le R.C. dépose un dossier auprès de l'A.E. au cours d'un face-à-face. Les éléments de la demande sont identiques à ceux d'une demande en ligne.

IV.2 Traitement d'une demande de certificat

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

Le contrôle d'enregistrement effectue les opérations suivantes avant de demander la production d'une biclé et d'un certificat (*cf. IV.4*) :

- Valider l'identité du futur R.C. : cette opération est réalisée à travers la vérification de la signature électronique et du certificat R.G.S. (**) utilisé par le R.C.
- Vérifier l'existence et la nature de l'entité de rattachement du service : l'A.E. s'appuie pour cela sur le SIREN présenté dans la demande et sur les référentiels de l'Ordre contenant notamment, les éléments d'identification (SIREN/SIRET, nom officiel, etc.) des cabinets d'expertise comptable en activité.
- Vérifier la qualité du représentant légal : les référentiels de l'Ordre incluent la liste des mandataires sociaux des cabinets d'expertise comptable en activité. Cette qualité peut aussi être établie sur la base du certificat de signature utilisé par le représentant légal pour signer le mandat joint à la demande, le cas échéant.
- Vérifier la présence du mandat et l'identité du représentant légal l'ayant signé :
    - Si le mandat est sous forme électronique, les signatures électroniques apposées sont vérifiées par l'A.E. De plus, le certificat du représentant légal doit porter la qualité de mandataire social de celui-ci vis-à-vis de l'entité de rattachement du service (la liste des certificats/A.C. acceptées est définie dans la D.P.C.).
    - Si le mandat est sous forme papier, l'A.E. vérifie l'identité et la signature manuscrite du représentant légal par rapport à la copie de la pièce d'identité fournie avec la demande.
- Vérifier le numéro de téléphone du représentant légal : le numéro de téléphone est directement vérifié par le personnel de l'A.E.
- Vérifier le courriel du représentant légal :
    - Si la demande est déposée en ligne (IV.1.2.1), un courriel contenant un lien d'enregistrement (adresse) est envoyé à l'adresse de la boîte électronique fournie dans la demande. Pour que celle-ci soit acceptée, la personne doit se connecter à cette adresse et y définir des identifiants, un mot de passe, un nom, un prénom et un code de révocation (spécifique au représentant légal).

      L'A.E. vérifie que cette étape a été effectuée avant de valider la demande.
    - Si la demande est déposée en face-à-face (IV.1.2.2), l'A.E. s'assure directement de la validité du courriel fourni auprès du représentant légal contacté par téléphone. À cette occasion, le représentant légal convient avec l'A.E. de son code de révocation.
- Vérifier l'unicité du DN du certificat à produire
- Vérifier la cohérence des justificatifs présentés

Le processus assure que le futur R.C. a pris connaissance des modalités applicables pour l'utilisation du certificat (conditions générales d'utilisation).

La demande acceptée, une demande de génération du certificat et de la biclé est générée par l'A.C. vers la fonction adéquate de l'I.C.P. (*cf.* chapitre I.3.1).

Il est conservé une trace des justificatifs présentés : l'A.E. numérise les pièces « papier » et archive l'ensemble au format électronique sous une forme ayant valeur légale.

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 R.C. en en justifiant le rejet.

IV.2.3 Durée d'établissement du certificat

La durée d'établissement du certificat est d'au plus 35 jours.

IV.3 Délivrance du certificat

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

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

Chez l'OSC, le processus de génération du certificat est lié de manière sécurisée au processus de génération de la biclé : l'ordonnancement des opérations est assuré ainsi que l'intégrité et l'authentification des échanges entres les composantes. La clé privée est protégée en intégrité et en confidentialité tout au long de son cycle de vie : le support est envoyé par courrier postal avec accusé de réception au R.C. ; les données d'activation lui sont transmises par un canal distinct (voir ci-dessous).

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 R.C.

La remise du certificat se fait par courrier postal avec accusé de réception. L'adresse utilisée est l'adresse du R.C. saisie lors du processus de demande.

Le certificat complet et exact est mis à la disposition du R.C.

IV.4 Acceptation du certificat

En parallèle au tirage de la biclé par l'A.C. et à la confection du certificat, le R.C. recevra à son domicile sous correspondance sécurisée en courrier simple le code PIN d'activation de sa ou ses supports.

L'adresse utilisée est l'adresse du R.C. saisie lors du processus de demande.

IV.4.1 Démarche d'acceptation du certificat

L'acceptation du certificat est tacite à la première utilisation de celui-ci.

IV.4.2 Publication du certificat

Le certificat fait l'objet d'une publication dans les annuaires techniques du système d'information de l'Ordre.

La publication ne peut avoir lieu qu'après acceptation du contenu du certificat par celui-ci. Son acceptation de publication est dans les Conditions Générales d'Utilisation, elle est cosubstancielle à la demande.

IV.4.3 Notification par l'A.C. aux autres entités de la délivrance du certificat

L'A.C. informe les autres entités de l'I.C.P. 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 R.C.

L'utilisation de la clé privée du R.C. et du certificat associé est strictement limitée au service de cachet (*cf.* chapitre I.4.1.1). Cette contrainte est portée à la connaissance des R.C. par l'A.C., notamment dans l'accord contractuel qui les lie. Il y est rappelé que :

- Les R.C. 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 R.C. 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 ou le contrat R.C. faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du R.C. par l'A.C. avant d'entrer en relation contractuelle.

Toute autre utilisation de la clé privée et du certificat est interdite.

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

Dans la cadre de la présente P.C., il n'y a pas de renouvellement de certificat.

IV.7 Délivrance d'un nouveau certificat suite à changement de la biclé

Dans la cadre de la présente P.C., la délivrance d'un nouveau certificat s'effectue dans les mêmes conditions et selon les mêmes modalités que la demande initiale.

IV.8 Modification du certificat

La modification du certificat n'est pas admise.

IV.9 Révocation et suspension des certificats

IV.9.1 Causes possibles d'une révocation

IV.9.1.1 Certificats de cachet

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat de cachet :

- les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du nom du serveur), ceci avant l'expiration normale du certificat
- le R.C. n'a pas respecté les modalités applicables d'utilisation du certificat
- le R.C. 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
- le R.C. ou une entité autorisée (représentant légal de l'entité, par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur ou de son support)
- l'arrêt définitif du serveur ou la cessation d'activité de l'entité du R.C. de rattachement du serveur
- le décès du R.C.

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 R.C. ne respecte pas les obligations énoncées dans la présente politique de certification.

En particulier, lorsqu'une des circonstances ci-dessous 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), l'A.C. révoquera le certificat si un nouveau R.C. répondant aux obligations de la présente P.C. n'est pas identifié dans un délai de 2 jours calendaires.

- le R.C. n'est plus membre de l'Ordre

IV.9.1.2 Certificats d'une composante de l'I.C.P.

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

IV.9.2 Origine d'une demande de révocation

IV.9.2.1 Certificats de R.C.

Les personnes et entités qui peuvent demander la révocation d'un certificat émis au titre de la présente politique sont les suivantes :

- le R.C.
- le représentant légal de l'organisme identifié dans le certificat
- l'A.C. émettrice du certificat ou l'une de ses composantes (A.E.)
- le CSOEC, par l'intermédiaire de l'A.C.

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

IV.9.2.2 Certificats d'une composante de l'I.C.P.

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

IV.9.3 Procédure de traitement d'une demande de révocation

IV.9.3.1 Révocation d'un certificat de R.C.

Une demande de révocation peut être demandée sur le Portail internet client et sur celui de l'OSC, 24h/24 et 7j/7.

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- Le nom du service contenu dans le certificat ;
- le nom du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (numéro de série,…) ;
- éventuellement, la cause de révocation.

Une fois la demande déposée, le demandeur reçoit un courriel de confirmation contenant une adresse (lien http) sur lequel il faut se connecter pour confirmer la demande de révocation.

De plus, si le R.C. n'est pas le demandeur, il est également être informé de la révocation effective de son certificat. L'entité professionnelle est informée de la révocation de tout certificat des R.C. qui lui sont rattachés.

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.

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.9.3.2 Révocation d'un certificat d'une composante de l'I.C.P.

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

IV.9.3.3 Délai accordé au R.C. pour formuler la demande de révocation

Dès que le R.C. (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.9.4 Délai de traitement par l'A.C. d'une demande de révocation

IV.9.4.1 Révocation d'un certificat de R.C.

Toute demande de révocation est traitée en urgence.

Les demandes de révocation sont immédiatement traitées par l'A.E. saisie par le R.C. ou par le représentant légal sur le site de la profession.

Il s'écoule au maximum 12 heures entre la demande de révocation par le R.C. et la publication de la nouvelle LCR prenant en compte cette demande. Dans ce cas, la publication est biquotidienne;

La durée maximale d'indisponibilité par interruption de service (panne ou maintenance) ainsi que la durée maximale totale d'indisponibilité par mois est fixée dans le contrat PSCE-OSC et les modalités en sont précisées dans la D.P.C.

IV.9.4.2 Révocation d'un certificat d'une composante de l'I.C.P.

Sans objet, ici.

IV.9.5 Exigences de vérification de la révocation par les utilisateurs de certificats

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

IV.9.6 Fréquence d'établissement des LCR

La LCR est mise à jour biquotidiennement et publiée via HTTP et LDAP. Une LCR est valable au maximum 72 heures.

IV.9.7 Délai maximum de publication d'une LCR

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

IV.9.8 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

L'A.C. se réserve la possibilité d'ouvrir un service OCSP accessible à l'adresse indiquée dans les certificats. Dans le cas de l'ouverture du service, l'A.C. s'engage à respecter les exigences d'intégrité, de disponibilité et de délai de publication décrites dans la présente P.C.

IV.9.9 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

L'utilisateur d'un certificat de R.C. est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. *Cf.* chapitre IV.9.6 ci-dessus.

IV.9.10 Autres moyens disponibles d'information sur les révocations

Sans objet.

IV.9.11 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de R.C., 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.9.3.2 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 R.C., l'A.C. impose par voie contractuelle qu'en cas de compromission de sa clé privée du R.C. ou de connaissance de la compromission de la clé privée de l'A.C. ayant émis son certificat, le R.C. s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

IV.9.12 Suspension de certificats

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

IV.10 Fonction d'information sur l'état des certificats

IV.10.1 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 dans un annuaire accessible en protocole LDAP V3 dont l'adresse suit la convention suivante :

```
ldap://ldapseec.experts-comptables.fr/CN = Ordre des Experts-Comptables – CC,OU = 0002 775670003,O = Conseil Supérieur de l'Ordre des Experts-Comptables,C = FR?certificaterevocationlist;binary?base?objectclass=pkiCA
```

Le tableau ci-dessous résume les adresses HTTP des LCR de chacune des A.C.

Autorité de certification	Adresse
CSOEC	http://seec.experts-comptables.fr/CRL/CRL_CACHET.crl http://www.signexpert.fr/CRL/CRL_CACHET.crl

Le cas échéant, une A.C. dédiée est en charge de la production des certificats de signature des réponses OCSP. Le tableau ci-dessous explicite les moyens d'identifier cette A.C.

Champ	**Valeur**
Serial Number	11:20:52:57:8a:7a:42:86:a0:95:70:aa:3f:95:3b:e0:48:13
Subject	C=FR, O=Conseil Supérieur de l'Ordre des Experts-Comptables, OU=0002 775670003, CN=Ordre des Experts-Comptables – OCSP
X509v3 Subject Key Identifier	CC:05:0D:2F:CF:AA:B5:CC:DA:B6:71:36:87:FA:77:F2:EC:A.C.:41:2C

IV.10.2 Disponibilité de la fonction

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 2 heures et une durée maximale totale d'indisponibilité par mois de 8 heures.

Le cas échéant, le 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.11 Fin de la relation entre le R.C. et l'A.C.

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

IV.12 Séquestre de clé et recouvrement

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

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

IV.13 Certificats de test

Les certificats de test (*cf.* III.1.2.3) 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 supports détruits, 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.C.P. C'est pourquoi elles sont précisées dans la D.P.C., notamment sur les points suivants :

- Situation géographique et construction des sites
- Accès physique
- Alimentation électrique et climatisation
- Vulnérabilité aux dégâts des eaux
- Conservation des supports
- Mise hors service des supports
- Sauvegardes hors site

V.2 Mesures de sécurité procédurales

V.2.1 Rôles de confiance

L'A.C. 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.C.P. 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.C.P. 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.C.P. 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.C.P. 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 D.P.C.

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 D.P.C.

V.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'I.C.P. 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 ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'I.C.P.

Ces contrôles sont décrits dans la D.P.C. de l'A.C. et sont conformes à la politique de sécurité de la composante.

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.C.P. C'est pourquoi elles sont précisées dans la D.P.C., 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

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.C.P. C'est pourquoi elles sont précisées dans la D.P.C. en ce qui concerne la journalisation d'événements.

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 révocations
- 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.C.P., 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 R.C., 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 R.C.

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 D.P.C.

V.4.8 Copies de sauvegarde des journaux d'événement

Des sauvegardes mensuelles sur supports non réinscriptibles sont effectuées. Des précisions sont fournies dans la D.P.C. 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.C.P.
- Sécurité partielle de l'I.C.P. (analyse des composantes).
- Non-respect de la P.C.

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.C.P.

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 :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques
- la P.C.
- la D.P.C.
- les certificats et LCR tels qu'émis ou publiés
- les récépissés ou notifications (à titre informatif)
- les justificatifs d'identité des R.C. et, le cas échéant, de leur entité de rattachement
- les journaux d'événements des différentes entités de l'I.C.P.

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 R.C. 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 R.C. et d'A.C., ainsi que les LCR produites, sont archivés pendant au moins dix 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 dix 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 D.P.C. 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 D.P.C.

V.5.5 Exigences d'horodatage des données

Le chapitre VI.7 précise les exigences en matière de datation / horodatage.

V.5.6 Système de collecte des archives

La D.P.C. 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 inférieur à 72 h 00 sachant que seule l'A.C. peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'I.C.P. 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 D.P.C.

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

- informer tous les R.C. 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.C.P.

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

L'AC 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'IGC

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

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

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 la présente politique.

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'AC les en avise aussitôt que nécessaire et, au moins, 1 (un) mois auparavant.
2) L'AC communique au point de contact identifié sur le site :

   http://www.modernisation.gouv.fr/

   les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité.
   Elle y présente notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue.
   L'AC communiquera au SGMAP et à l'ANSSI, selon les différentes composantes de l'IGC 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 informées le SGMAP et 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'IGC 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'AC, 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'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans la présente politique. L'AC 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'A.C. doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'I.C.P., notamment par des dispositions spécifiques de la D.P.C.

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.C.P.

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

La génération des clés des serveurs est effectuée dans un environnement sécurisé (*cf.* chapitre V). Les biclés des serveurs sont générées dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré, puis transférées de manière sécurisée dans le dispositif de création de signature destiné au serveur sans que l'A.C. n'en garde aucune copie.

VI.1.1.3 Clés serveurs générées au niveau du serveur

Sans objet

VI.1.2 Transmission de la clé privée à son propriétaire

La clé privée générée par l'A.C. est transmise au serveur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Cette transmission se fait directement dans le dispositif de création de cachet destiné au serveur.

Une fois remise, la clé privée est maintenue sous le seul contrôle du R.C.

L'A.C. ne conserve ni ne duplique cette clé privée.

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 et des A.C. CROEC/CDOEC sont téléchargeables sur le site internet du CSOEC (http://www.experts-comptables.fr/)

VI.1.5 Tailles des clés

La taille des biclés des A.C. 2048 bits.

La taille des biclés des R.C. 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'A.C. et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR ou de réponses OCSP (voir chapitre I.4.1).

L'utilisation de la clé privée du R.C. et du certificat associé est strictement limitée au service de cachet.

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.

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

VI.2.1.2 Dispositifs de création de cachet des serveurs

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

L'A.C. s'assure que :

- la préparation des dispositifs de création de signature est contrôlée de façon sécurisée par le prestataire de service
- les dispositifs de création de signature sont stockés et distribués de façon sécurisée
- 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

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

VI.2.3 Séquestre de la clé privée

Les clés privées des serveurs ne doivent en aucun cas être séquestrées.

VI.2.4 Copie de secours de la clé privée

Les clés privées des serveurs ne doivent faire l'objet d'aucune copie de secours par l'A.C.

VI.2.5 Archivage de la clé privée

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

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

Le transfert de la clé privée du serveur vers le support cryptographique se fait conformément aux exigences du chapitre VI.1.1.2 ci-dessus.

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.C.P.

VI.2.8.2 Clés privées des serveurs

L'activation de la clé privée du serveur 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.C.P.

VI.2.9.2 Clés privées des serveurs

Les conditions de désactivation de la clé privée d'un serveur 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.C.P.

VI.2.10.2 Clés privées des serveurs

Les clés privées des serveurs 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 serveur, 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 serveurs 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 serveurs couverts par la présente P.C. doivent avoir une durée de vie au maximum de trois ans.

La fin de validité d'un certificat d'A.C. est postérieure à la fin de vie des certificats serveurs 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.C.P.

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

Comme l'A.C. génère la clé privée du serveur, elle a l'obligation de transmettre au R.C. les données d'activation correspondantes par le biais d'un chemin garantissant la protection en intégrité et en confidentialité des données. Notamment, la remise de la donnée d'activation est séparée dans le temps ou dans l'espace de la remise de la clé privée.

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.C.P.

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

Comme les données d'activation des dispositifs de création de cachet des serveurs sont générées par l'A.C., elles sont protégées en intégrité et en confidentialité jusqu'à la remise au R.C.

VI.4 Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques prises par l'A.C. sont décrites dans la D.P.C.

VI.5 Mesures de sécurité liées au développement des systèmes

Les mesures de sécurité liées au développement des systèmes prises par l'A.C. sont décrites dans la D.P.C.

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.C.P.

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.C.P. 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

Plusieurs exigences de la présente P.C. nécessitent la datation par les différentes composantes de l'I.C.P. d'événements liés aux activités de l'I.C.P. (*cf.* chapitre V.4). Les modalités d'application sont définies dans la D.P.C.

VII PROFILS DES CERTIFICATS, OCSP ET DES LCR

VII.1 Certificats de serveur

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

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	CN = Ordre des Experts-Comptables - CC OU = 0002 775670003 O = Conseil Supérieur de l'Ordre des Experts-Comptables C = FR
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (trois ans après la date d'émission du certificat)
Subject	voir III.1.2.2
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 ci-dessous)
keyIdentifier	issuerName+serialNumber
Subject Key Identifier	Identification de la clé publique du R.C.
Key Usage (critical)	digitalSignature
Certificate Policies (critical)	
policyIdentifier	1.2.250.1.165.1.8.1.1
policyQualifier-cps	http://seec.experts-comptables.fr/PC/PC_cachet-cabinet.pdf
policyQualifier-unotice	Certificat de scellement
Subject Alternative Name	
rfc822Name	Adresse courriel du R.C. ou du contact cabinet (champ optionnel)
dNSName	Adresse du serveur (champ optionnel)
Basic Constraint (critical)	CA:False
CRL Distribution Points	
distributionPoint	http://seec.experts-comptables.fr/CRL/CRL_CACHET.crl http://www.signexpert.fr/CRL/CRL_CACHET.crl
Authority Information Access	
Ocsp	http://ocsp.experts-comptables.fr/OEC/
caIssuer	http://seec.expert-comptables.fr/cert/cert_CACHET.p7b

VII.2 Liste de Certificats Révoqués

Champ	Valeur
Version	V2
Issuer DN	CN = Ordre des Experts-Comptables - CC OU = 0002 775670003 O = Conseil Supérieur de l'Ordre des Experts-Comptables C = FR
ThisUpdate	AAAA/MM/JJ HH:MM:SS Z (date d'émission de la CRL)
NextUpdate	AAAA/MM/JJ HH:MM:SS Z (3 jours après la date d'émission)
UpdateFrequency	12 heures
Signature (algorithm & OID)	SHA256WithRsaEncryption
CRL Extension	
CRLNumber	Numéro de la CRL
AKI	Identification de la clé publique de l'A.C.
CRL Entry Extension	
Revocation Reason	Défini lors de la révocation (champ optionnel)
Distribution point	
HTTP	http://seec.experts-comptables.fr/CRL/CRL_CACHET.crl http://www.signexpert.fr/CRL/CRL_CACHET.crl

VII.3 Certificat de l'A.C. émettrice

Champ	Valeur
Version	3 (0x2)
Serial Number	11:20:85:31:dd:41:da:d9:5f:8b:87:8b:6c:eb:2e:eb:6a:5b
Signature Algorithm	sha256WithRSAEncryption
Issuer	C=FR, O=Ordre des Experts-Comptables, OU=0002 775670003, CN=Ordre des Experts-Comptables
Validity	
Not Before	May 9 00:00:00 2011 GMT
Not After	Dec 31 01:00:00 2019 GMT
Subject	C=FR, O=Conseil Supérieur de l'Ordre des Experts-Comptables, OU=0002 775670003, CN=Ordre des Experts-Comptables - CC
Subject Public Key Info	
Public Key Algorithm	rsaEncryption
Public-Key	(2048 bit)

Champ	Valeur
Modulus	00:bc:bc:be:0a:7c:67:8a:f7:fe:68:f0:c0:1e:ed: 41:95:ea:e6:e1:5d:91:79:d5:8f:b8:bf:54:cf:f8: f3:65:b6:77:3b:61:3f:f7:3b:8a:10:00:0b:7b:6f: a2:0b:40:a0:4d:d8:5c:a5:54:c5:88:e1:2e:00:77: 89:4b:2f:93:a9:65:a5:aa:e6:ef:84:61:9e:07:81: 2f:90:62:b5:46:b3:4b:9a:7e:e7:cb:5f:73:7c:46: 9c:5d:be:92:25:ef:58:95:10:6c:82:04:15:b1:f9: 22:5a:30:ea:08:e8:4c:8f:38:c8:a1:c1:2e:db:5b: 00:a7:ca:3b:9f:bb:f7:e7:16:93:60:41:c6:63:d9: 12:fc:65:33:b6:22:0b:18:95:85:a3:d4:c0:2e:c4: bb:82:3c:e3:7f:15:ce:04:8a:8b:e0:56:3b:49:46: ce:38:86:2d:61:1d:39:37:e8:56:f1:69:4b:11:c4: 2a:96:29:99:fa:27:a0:23:1d:e9:b7:34:1d:d2:49: 82:c0:03:b1:3f:f4:ee:73:c0:4d:3b:db:ae:6a:3c: 06:60:fc:d8:5f:d3:8d:68:23:39:71:33:e0:bf:e5: ef:1e:a5:fb:73:1d:0e:c0:b1:92:10:bb:28:53:7f: f9:79:33:ac:19:90:fc:61:1d:73:24:dc:32:4a:43: 58:eb
Exponent	65537 (0x10001)
X509v3 extensions	
X509v3 Key Usage (critical)	Certificate Sign, CRL Sign
X509v3 Certificate Policies	
Policy	X509v3 Any Policy
CPS	http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf
X509v3 Basic Constraints (critical)	CA:TRUE, pathlen:0
X509v3 CRL Distribution Points	
Full Name	URI:http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl
X509v3 Subject Key Identifier	C4:C4:71:E6:15:B8:1A:0A:51:7A:77:4D:37:B1:D8:3A:72:C8:28:D6
X509v3 Authority Key Identifier	keyid:81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56

Champ	Valeur
Signature Algorithm	sha256WithRSAEncryption 32:56:9d:4c:07:25:05:12:b6:10:19:3f:17:30:51:f6:c0:eb: 96:45:c0:39:9e:d6:21:64:6c:70:37:f4:66:df:a7:a5:3a:54: e6:c5:81:df:39:71:c8:7d:af:08:61:0b:d3:10:e8:b8:b4:98: 52:ab:a0:82:3e:6d:b1:21:8f:b5:83:a3:1f:47:f7:73:32:8a: 13:d2:95:26:bf:9f:45:89:af:62:b1:d9:4f:c7:7a:a0:3e:46: 21:d2:e0:d5:71:fb:27:d5:4b:82:bd:a0:3b:0d:49:07:2e:68: e2:c7:95:ee:ab:b7:97:e6:47:c4:24:6b:03:82:83:32:39:1e: 19:27:30:b4:6f:85:47:a1:c7:f5:7c:68:2a:da:87:28:3c:68: c2:5b:e1:c5:fa:34:70:9e:bc:27:e1:8f:93:fb:7a:66:36:08: 8e:a3:59:7a:00:e2:82:05:e7:8d:3e:93:67:e9:b9:54:88:64: eb:09:f4:68:a7:08:71:b4:7e:fb:57:95:79:47:4a:e7:21:e9: 58:ab:e6:8a:b4:fd:1c:58:37:6e:52:12:a0:78:2d:19:33:08: 8c:1d:60:67:97:e6:02:22:bc:1c:73:27:ea:19:ee:81:df:a7: 51:d4:70:51:c6:65:af:3d:8f:94:29:f3:9c:c1:f4:88:16:e3: f4:b8:fa:51:1a:55:bb:1a:39:9f:e8:9d:72:a5:31:b3:43:3d: cc:49:cd:76:bb:5e:8d:4d:a3:1c:40:4e:ca:30:fb:85:ac:1d: d2:c7:ed:c3:89:85:8c:1c:05:79:8f:bd:91:d8:cd:10:ab:25: e3:b2:15:c5:31:ac:b2:11:4a:e4:d2:ab:39:e1:8c:67:7b:67: 3d:ea:63:eb:7d:93:b7:c7:51:00:c1:11:ef:2f:26:a7:6e:30: d3:81:78:63:b3:04:dc:e6:69:3d:82:80:e6:87:fa:3b:09:fe: 08:d7:d3:0d:4a:5b:2a:34:40:94:e1:cc:05:b3:02:ee:e2:f8: b7:02:02:a1:29:49:f3:33:1d:29:83:e9:9e:d0:f6:68:f5:ce: 4a:55:a1:17:ad:c2:13:1d:db:1d:11:33:10:46:05:4d:1f:df: ef:49:a1:31:a8:6b:6c:4e:a2:3e:b2:68:b4:40:3a:07:fc:66: 4d:ba:b8:7d:8f:43:ae:fc:50:e4:0c:c0:4a:82:8a:bc:25:ec: d1:ce:9a:c1:da:87:b6:ae:2a:64:f4:e6:8b:36:52:64:f8:15: 40:71:a4:6e:31:57:59:ba:2b:20:8d:25:9d:01:b9:d5:34:41: f2:80:4d:5e:ee:02:60:aa:0f:17:b6:c2:99:80:76:42:9d:74: 13:01:fd:9c:59:2f:22:93

VII.4 Certificat des réponses OCSP

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	C=FR O=Conseil Supérieur de l'Ordre des Experts-Comptables OU=0002 775670003 CN=Ordre des Experts-Comptables - OCSP
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (3 mois après la date d'émission du certificat)
Subject	C=FR O=CSOEC OU=0002 775670003 OU=Opéré par Keynectis CN=YYYYMMDDHHMM Plate-forme
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1
Key size	2048
Signature (algorithm & OID)	SHA256WithRsaEncryption
Authority Key Identifier	CC:05:0D:2F:CF:AA:B5:CC:DA:B6:71:36:87:FA:77:F2:EC:A.C.:41:2C

Champ	Description
Subject Key Identifier	Identification de la clé publique de la plate-forme
Key Usage (critical)	digitalSignature
Certificate Policies (critical)	
policyIdentifier	1.2.250.1.165.1.2.9.1.6
policyQualifier-cps	http://seec.experts-comptables.fr/PC/PC_OCSP.pdf
policyQualifier-unotice	Ce certificat de l'Ordre des Experts-Comptables selon la politique ci-dessus
Subject Alternative Name	
Basic Constraint (critical)	CA:False
Extended Key Usage	OCSPSigning
CRL Distribution Points	
distributionPoint	http://seec.experts-comptables.fr/CRL/CRL_OCSP.crl
distributionPoint	ldap://ldapseec.experts-comptables.fr/C=FR,O=Conseil%20Supérieur%20de%20l'Ordre%20des%20Experts-Comptables,OU=0002%20775670003,CN=Ordre%20des%20Experts-Comptables%20-%20OCSP?certificaterevocationlist;binary?base?objectclass=pkiCA

VIII AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent…

- d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens de l'Ordonnance n° 2005-1516 du 8 décembre 2005 (schéma de qualification des prestataires de services de confiance conformément au Décret du 8 décembre 2005 précité)
- et, d'autre part, ceux que doit réaliser, ou faire réaliser, le PSCE afin de s'assurer que l'ensemble de son I.C.P. est bien conforme à ses engagements affichés dans sa P.C. et aux pratiques identifiées dans sa D.P.C.

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

VIII.1 Fréquences ou circonstances des évaluations

Avant la première mise en service d'une composante de son I.C.P. 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.C.P., 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.C.P. 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.C.P. (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'I.C.P. (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la P.C. de l'A.C. et dans la D.P.C. 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'A.C. 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 P.C. et la D.P.C.

VIII.6 Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de l'A.C.

IX AUTRES PROBLEMATIQUES METIERS ET LEGALES

IX.1 Tarifs

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

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

IX.1.2 Tarifs pour accéder aux certificats

La présente P.C. 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 et, éventuellement, deltaLCR est en accès libre en lecture.

IX.1.4 Tarifs pour d'autres services

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

IX.1.5 Politique de remboursement

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

IX.2 Responsabilité financière

La responsabilité financière de l'A.C. pour l'émission de certificats qualifiés 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*). Elle pourra être recherchée en cas de délivrance d'un certificat SEEC à une personne physique non membre de l'Ordre.

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 D.P.C. de l'A.C.,
- les clés privées de l'A.C., des composantes et des R.C.,
- les données d'activation associées aux clés privées d'A.C. et des serveurs,
- tous les secrets de l'I.C.P.,
- les journaux d'événements des composantes de l'I.C.P.,
- les dossiers d'enregistrement des R.C.,
- les causes de révocations, sauf accord explicite du R.C.

IX.3.2 Informations hors du périmètre des informations confidentielles

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

IX.3.3 Responsabilités en termes de protection des informations confidentielles

L'A.C. applique des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 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'A.C. 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 R.C. à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au R.C.

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, en particulier de la loi *Informatique et Libertés*.

IX.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des certificats des serveurs (qui sont considérées comme confidentielles sauf accord explicite du R.C.) ;
- le dossier d'enregistrement du R.C.

IX.4.3 Informations à caractère non personnel

La présente P.C. 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 R.C. à l'A.C. ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du R.C., décision judiciaire ou autre autorisation légale.

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

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

IX.4.7 Autres circonstances de divulgation d'informations personnelles

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

IX.5 Droits sur la propriété intellectuelle et industrielle

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

IX.6 Interprétations contractuelles et garanties

Sans objet.

IX.7 Limite de garantie

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

IX.8 Limite de responsabilité

IX.8.1 Obligations du R.C.

Le R.C. s'engage à…

- Communiquer des informations exactes lors de son enregistrement auprès de l'Autorité de Certification régionale, ainsi que toute modification de celles-ci, et les pièces justificatives correspondantes
- Protéger le code secret d'activation de toute perte et divulgation, ne jamais conserver ensemble la carte à puce cryptographique et le code d'activation
- Respecter les conditions d'utilisation des certificats
- Informer sans délai l'Autorité de Certification régionale en cas de compromission ou de suspicion de compromission de ses données de création de cachet

IX.9 Indemnités

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

IX.10 Durée et fin anticipée de validité de la P.C.

IX.10.1 Durée de validité

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

IX.10.2 Fin anticipée de validité

La publication d'une nouvelle version de la « P.C. Type » du R.G.S. peut entraîner, en fonction des évolutions apportées, la nécessité pour l'A.C. de faire évoluer sa P.C. correspondante.

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

La présente P.C. 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.C.P., 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'A.C. 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 P.C.

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

L'OID de la P.C. de l'A.C. étant inscrit dans les certificats qu'elle émet, toute évolution de cette P.C. ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des R.C., 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.

En particulier, l'OID de la présente P.C. évoluera dès lors qu'un changement majeur intervient dans les exigences de la P.C. Type applicable à la famille de certificats considérée.

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 P.C. 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

X.1 Législation et réglementation

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005
Décret n° 2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

X.2 Documents techniques

Document
Référentiel Général de Sécurité – Version 1.0
RGS - Fonction de sécurité « Signature électronique » - Version 2.3
RGS - Politiques de Certification Types - Variables de Temps - Version 2.3
RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3
Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - Version 1.20
CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). Ce PP a été certifié EAL4+.
CWA 14167-3 (2003-10) Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)
CWA 14167-4 (2003-10) Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP). Ce PP a été certifié EAL4+.
CWA 14169 (2002-04) Secure Signature Creation Devices (SSCD). Ce PP a été certifié EAL4+.
AFNOR A.C. 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".
ETSI TR 102 272 - ASN.1 format for signature policies V1.1.1 (décembre 2003) ETSI TR 102 038 - XML format for signature policies V1.1.1 (avril 2002)
Exigences de sécurité des sites de personnalisation, V1.0 (août 2007) http://www.references.modernisation.gouv.fr/sites/default/files/Exigences_sites_de_perso_V1_0.pdf
RFC3647 - IETF - internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003

X.3 Autres documents

[PC_AS] Politique de certification « Authentification forte » pour les A.C. de la profession comptable (A.C. CROEC), Version 6.0 du 1er juillet 2011, OID n° 1.2.250.1.165.1.2.x.7.6

[PC_S] Politique de certification « Signature » pour les A.C. de la profession comptable (A.C. CROEC), Version 6.0 du 31 août 2011, OID n° 1.2.250.1.165.1.2.x.1.6

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

XI.1 Exigences sur les objectifs de sécurité

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

XI.2 Exigences sur la qualification

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

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

XII.1 Exigences sur les objectifs de sécurité

Le dispositif de création de signature, utilisé par le R.C. pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa biclé, doit répondre aux exigences de sécurité suivantes :

- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une signature qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer la fonction de signature pour le R.C. légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

XII.2 Exigences sur la qualification

Le dispositif de création de cachet doit être qualifié au minimum au niveau standard, selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XII.1 ci-dessus.