ORDRE DES EXPERTS-COMPTABLES

ECM Association

POLITIQUE DE CERTIFICATION « Cachet Serveur » DE LA PROFESSION COMPTABLE

Version 2.2

Du **27 février 2019**

OID n° 1.2.250.1.165.1.11.1.1

HISTORIQUE DES VERSIONS

Date	Évolutions	Édition / révision
Avril 2016	Création du document	2.0-alpha
Mai 2017	Mise à jours diverses : eIDAS, point de contact, mise en page	2.1
Février 2019	Mise à jour des URL	2.2

Contributeurs	Organisation
Mathieu JORRY	ECMA
Samuel LACAS	SEALWeb

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 politique de certification vise à permettre la délivrance de certificats de cachets qualifiés au sens de l'article 38 du *Règlement (UE) N° 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur* (dit « Règlement eIDAS »). Ces certificats seront utilisés pour des cachets électroniques bénéficiant d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié.

Cette PC vise la conformité aux exigences de l'ETSI EN 319401 et de l'ETSI EN 319411-2.

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. : 1.2.250.1.165.1.11.1.1

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 désignés dans la suite du document respectivement sous le nom de « P.C. » et de « D.P.C. ».

I.3 Entrée en vigueur du document

La présente P.C. s'applique à partir du 1er Juillet 2016

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

I.4.1 Le Prestataire de services de certification électronique

Se référer au document [PC_SA].

I.4.2 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 « Cachet - Ordre des Experts-Comptables ».

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.4.3 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.4.4 Opérateur de certification (OC/OSC)

Se référer à la D.P.C.

I.4.5 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.7.2) 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.4.6 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 nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

I.5 Usage des certificats

I.5.1 Domaines d'utilisation applicables

I.5.1.1 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 sceller des données, afin que les catégories d'utilisateurs de certificats identifiées au chapitre I.4.6 ci-dessus puissent en vérifier 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 cachet objets de la présente P.C. sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité afin de pouvoir signer indûment des données sont forts.

Enfin, certaines applications d'échanges dématérialisés de la sphère publique peuvent nécessiter des certificats à des fins de tests ou de recette, différents des certificats « de production » fournis et gérés par l'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.5.1.2 Biclés et certificats d'A.C. et de composantes de l'I.C.P.

Se référer au document [PC_SA].

I.5.1.2.1 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.5.1.2.2 Certificats de composante

Se référer à la D.P.C.

I.5.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des biclés et des certificats sont définies au chapitre IV.5 ci-dessous. L'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.6 Gestion de la P.C.

Se référer au document [PC_SA].

I.7 Définitions et abréviations

I.7.1 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.7.2 Définitions

Se référer au document [PC_SA].

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

Se référer au document [PC_SA].

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

C	FR
O	Ordre des Experts-comptables
OU	0002 775670003
CN	Cachet - Ordre des Experts-Comptables

Conformément au R.G.S. et à la norme *ETSI EN 319 412*, le *DN* de ces AC est construit comme suit :

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

III.1.2.2 Identité des services de création de cachet

Le *DN* des certificats de création de cachet est construit comme suit :

C	FR
O	*[Nom du cabinet]*
OU	0002 *[SIREN du cabinet]*
OI	NTRFR-*[SIREN du cabinet]*
T	*[voir ci-dessous pour les valeurs possibles]*
SERIALNUMBER	*[identifiant saisi par le demandeur]*
CN	*[Nom du service]*

- Le champ `C=FR` désigne la France ;
- Le champ `O` désigne l'organisme de rattachement du porteur, à savoir son cabinet d'exercice professionnel, tel qu'inscrit au registre du commerce ;

- Le champ `OU` est contient le SIREN de ce même organisme, précédé de la chaîne « 0002 » ;
- Le champ `OI` est contient le SIREN de ce même organisme, précédé du code « NTRFR » désignant le registre du commerce des sociétés françaises ;
- 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 `CN` contient le nom du service, tel que déclaré par le RCC.

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.4.3), 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 s'adresse au service Client ou à l'AE nationale pour 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 signer électroniquement le formulaire de demande.

L'expert-comptable confirme l'exactitude de ces informations et les signe électroniquement à l'aide de son certificat *Signexpert*. Il transmet ensuite par courrier postal à l'A.E. nationale les CGU signées, le paiement et les éléments du dossier qui n'ont pas été transmis électroniquement.

Après le paiement des frais relatifs à l'acquisition du certificat et la vérification de la complétude du dossier (pièces électroniques et papier), 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. De plus, le contenu du certificat est validé par le demandeur avant son émission (signature d'un formulaire d'acceptation).

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.5.1.1). 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 : https://kregistration-user.certificat2.com/OEC/ACUNIQUE/CACHET2016:

Commenté [SL1]:

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

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

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

```
http://seec.experts-comptables.fr/OEC/CRL_cachet.crl
http://www.signexpert.fr/OEC/CRL_cachet.crl
http://trustcenter-crl.certificat2.com/CRL/CRL_cachet.crl
```

L'A.C. émettrice est aussi en charge de la production des certificats de signature des réponses (le document [PC-OCSP] décrit la politique s'appliquant à ces certificats).

IV.10.1 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.*) 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

Se référer au document [PC_SA].

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. 4096 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.5.1).

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.

Se référer au document [PC_SA].

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

Se référer au document [PC_SA].

VI.7 Horodatage / Système de datation

Se référer au document [PC_SA].

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	Voir III.1.2.1
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (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	1.2.250.1.165.1.11.1.1
policyQualifier-cps	http://www.signexpert.fr/PC/PC_Cachet.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/OEC/CRL_cachet.crl http://www.signexpert.fr/OEC/CRL_cachet.crl http://trustcenter-crl.certificat2.com/CRL/CRL_cachet.crl
Authority Information Access	
Ocsp	http://ocsp.experts-comptables.fr/OEC-ACCACHET
caIssuer	http://seec.expert-comptables.fr/cert/cert_cachet.p7b
QCStatements	
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	Set

Champ	Description
id-etsi-qcs-QcPDS (0.4.0.1862.1.5)	URL= https://www.signexpert.fr/CPS/CPS_Signature_et_Authentification_Ordre_des_Experts-Comptables.pdf language="EN"

VII.2 Liste de Certificats Révoqués

VII.3 Certificat de l'A.C. émettrice

Champ	Valeur
Version	3 (0x2)
Serial Number	11:20:ab:ae:4d:00:2f:9a:3c:b6:57:7b:a2:e0:de:c3:b3:bf
Signature Algorithm	sha512WithRSAEncryption
Issuer	C=FR, O=Ordre des Experts-Comptables, OU=0002 775670003, CN=Ordre des Experts-Comptables
Not Before	Feb 18 00:00:00 2016 GMT
Not After	May 9 00:00:00 2031 GMT
Subject	C=FR O=Ordre des Experts-Comptables OU=0002 775670003 OI=NTRFR-775670003 CN=Cachet - Ordre des Experts-Comptables
Public Key Algorithm	rsaEncryption
RSA Public Key	(4096 bit)

Champ	Valeur
Modulus (4096 bit)	00:bc:e9:24:df:16:34:8e:78:21:9a:e7:81:ce:bb: d1:8f:a8:c9:0d:78:a5:b0:14:11:c9:71:f4:1c:1d: c4:de:c5:15:9d:fb:80:4c:07:18:54:8f:39:99:fe: 00:bf:bc:4a:4b:7b:ca:a8:1b:c4:a6:9e:56:73:c5: 52:b0:74:f0:57:eb:08:46:40:26:f1:9b:a5:88:e0: b3:fa:54:1b:98:e2:94:47:bd:26:63:bf:f8:f0:9a: 8c:d7:0b:9f:4e:a5:32:51:70:2c:3b:39:93:80:32: eb:47:3d:75:26:ac:33:27:3b:1c:59:7f:9d:8a:f2: a9:4d:ac:94:3d:a3:5f:ff:a8:5a:a8:98:bd:7f:e5: c0:20:af:7d:26:6f:be:dd:c7:0c:d5:cd:70:81:a1: 63:26:c1:78:73:e1:b8:d3:41:a3:7c:05:e8:f9:4b: ce:a9:1c:bc:20:3c:d3:c3:9a:1f:48:b0:3d:7e:66: ee:1d:7d:1b:03:51:a7:ed:81:2a:16:21:b5:bd:3f: 8a:1f:74:37:7d:bc:3c:ce:20:d5:8f:ac:1b:f8:f9: ab:7e:e8:0d:d0:d4:34:4c:88:38:56:76:67:43:82: 57:9a:00:25:5e:2c:59:97:4f:60:42:7c:e3:21:38: 9a:15:b1:b9:b2:75:2e:71:c6:77:70:0b:1d:48:1d: a6:39:d5:67:b0:73:f3:d1:15:ee:b7:db:77:89:9c: 8a:9d:8a:83:cf:50:1c:74:d4:5b:61:47:db:d0:75: 9a:e7:b3:23:bd:05:1c:f6:c2:d8:e5:8c:32:8e:72: 7b:74:a2:30:86:3d:46:88:bd:6a:87:8f:5c:ed:3e: e2:3e:4e:fa:37:e6:a3:4f:f3:d2:c0:fb:22:1e:ba: 96:12:51:2b:9a:b4:04:3e:58:06:1f:6c:90:dd:bc: bb:24:40:12:30:f2:8e:56:ee:31:e1:c3:ea:fa:d7: b4:11:3c:07:53:de:12:9a:f5:5c:43:f5:b9:aa:c2: e0:18:fe:78:94:38:9c:aa:06:b8:35:ea:1c:87:53: 4d:28:ab:ba:e9:50:8e:a3:59:06:52:78:b8:aa:0d: 68:2f:cd:a4:79:1e:90:e2:6d:d9:85:1e:7a:e0:63: 99:dc:7d:48:c4:92:2b:e7:8e:3d:a1:5f:6c:d7:60: d4:28:7c:06:b2:3a:2e:9f:a5:9f:e5:6b:1b:04:80: 6b:64:74:8e:e6:99:2f:4f:4f:68:d3:b0:0d:42:a5: f2:f3:fe:59:fa:80:67:26:a9:b4:0a:48:f9:ce:67: 76:14:bc:5f:ae:2e:79:78:1d:f7:09:20:fc:ad:dc: af:f5:f3:3a:65:78:c4:3b:08:8a:38:f4:dc:0c:26: d0:2e:fd
Exponent	65537 (0x10001)
X509v3 Key Usage (critical)	Certificate Sign, CRL Sign
X509v3 Certificate Policies	
Policy	1.2.250.1.165.1.1.1.2
CPS	http://www.signexpert.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf
X509v3 Basic Constraints (critical)	CA:TRUE, pathlen:0
X509v3 CRL Distribution Points	URI:http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl
X509v3 Subject Key Identifier	81:8B:08:CD:27:FF:FD:6A:23:FE:AE:99:62:F3:FD:8E:53:8E:9B:DD
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	sha512WithRSAEncryption 62:02:ef:55:11:8c:06:a1:28:55:04:97:f2:3b:de:6b:c4:c5: 8a:ee:60:e8:4c:89:f1:3f:1c:80:52:e0:d8:33:25:f6:f6:27: 6e:3c:dc:e9:18:9f:78:37:53:c9:a1:4e:44:6e:b5:24:d6:2b: 77:07:b5:03:af:d5:b6:cc:0d:f2:d0:8c:cb:22:e5:b7:32:a8: ee:23:55:3f:2c:2d:a9:a9:87:13:70:92:08:06:36:92:e7:a3: b4:1f:b5:d5:29:de:97:90:33:77:8b:c8:fb:2e:73:44:17:41: aa:fd:51:c1:e9:38:58:7b:90:7d:dd:77:d2:5e:24:8b:a2:c4: 71:d1:39:e9:a0:05:ac:8f:25:98:1c:a9:39:c3:e7:0f:57:6e: 32:f9:56:f6:78:a8:5a:7d:8e:c3:0d:a5:6e:35:02:67:b2:12: 7f:23:83:67:c3:6e:e9:bc:16:5a:8e:2e:c6:57:a2:97:fa:5b: 07:2f:75:bc:cb:17:26:7f:b9:f8:ed:e1:6a:18:73:87:fa:64: bf:39:d0:95:e3:be:9c:c3:f5:89:98:4c:0a:73:c3:85:64:a0: d5:b6:df:46:0f:5b:7f:7f:b5:77:a8:51:15:c5:70:d3:ba:71: 4a:bf:c8:b7:ce:4b:f2:a2:11:43:61:7d:ac:c3:44:1b:08:b2: 46:ed:0a:5f:82:d5:a3:54:3a:55:51:25:04:e1:48:5d:62:30: 5c:4c:d7:d6:dd:f1:00:6a:88:cb:b1:1f:db:86:46:07:3b:ce: 9b:f2:3d:26:8d:74:8b:8c:5f:6b:4a:77:5d:ab:e4:48:a6:ee: 42:4d:56:3d:24:9f:ba:8d:47:b3:11:f3:58:21:fd:ea:e2:5c: 70:63:53:90:41:1f:f9:76:b1:f4:4e:bc:17:9a:af:f0:6c:f3: ef:95:0e:1b:d8:a2:f6:cd:a2:38:eb:51:75:16:c5:d1:be:f0: 32:af:af:16:43:6d:5c:16:ee:2c:74:7c:85:55:10:8e:1f:49: a0:d0:0c:a3:99:c6:b9:7c:ab:9b:57:8e:e0:2f:1b:e4:d8:67: c0:a7:c7:2e:dd:16:3c:a3:57:50:cf:6b:2a:75:87:be:ec:66: f2:bb:8a:a2:60:72:b6:f8:ed:27:e7:6d:ec:79:24:bf:62:7c: e8:ea:da:be:60:e8:d3:3d:4a:fa:77:c3:12:66:c1:21:34:b9: 21:28:e2:04:7c:da:c6:4d:f9:65:0e:bd:86:de:2c:4c:bc:7b: 73:50:39:cf:a9:37:4e:43:0c:50:ad:69:22:22:16:ec:55:74: 8e:d3:67:a1:c1:03:8e:0b:3f:3b:88:fc:5f:c8:a0:a2:06:47: 43:52:79:59:bf:85:bf:90

VII.4 Certificat des réponses OCSP

Le profil des certificats OCSP est décrit dans le document [PC-OCSP].

VIII AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Se référer au document [PC_SA].

IX AUTRES PROBLEMATIQUES METIERS ET LEGALES

Hormis sur les points suivants, se référer au document [PC_SA].

IX.1.1 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.1.2 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.2 Limite de responsabilité

IX.2.1 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

X ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

X.1 Législation et réglementation

Se référer au document [PC_SA].

X.2 Documents techniques

Se référer au document [PC_SA].

X.3 Autres documents

[PC_SA] *PGS-OEC Politique de Certification - Signature & Authentification*, Version 1.1, OID nº 1.2.250.1.165.1.2.10.1.1

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

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

Se référer au document [PC_SA].

XII ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF DE CREATION DE CACHET ELECTRONIQUE

XII.1 Exigences sur les objectifs de sécurité

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

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

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

XII.2 Exigences sur la qualification

Dans le cas où la présente politique viserait à produire des certificats de cachet qualifiés, le dispositif de création de signature utilisé par le porteur devra être certifié conformément aux dispositions prévues à l'article 39 du règlement eIDAS.