ORDRE DES EXPERTS-COMPTABLES

Conseil Supérieur

PGS-OEC POLITIQUE DE CERTIFICATION

ÉLUS DE L'ORDRE DES EXPERTS-COMPTABLES

Version 1.1

mai 2016

OID n° 1.2.250.1.165.1.10.11.1

Signature numérique de Jean Saphores

HISTORIQUE DES VERSIONS

Date	Évolutions	Edition / révision
Avril 2016	Version préliminaire	1.1-gamma

Contributeurs	Organisation
Stéphane GASCH	CSOEC
Samuel LACAS	SEALWeb
Jean SAPHORES	CSOEC

TABLE DES MATIÈRES

I INTRODUCTION

I.1 Présentation générale

Ce document constitue une Politique de Certification (P.C.) mise en œuvre par une Autorité de Certification de l'Ordre des Experts Comptables (OEC), à destination des élus de la profession. Elle réunit l'ensemble des obligations et engagements des différents acteurs relatifs à la délivrance et l'usage des certificats numériques de personnes physiques dans le cadre de leur qualité d'élus de l'Ordre.

Elle réunit l'ensemble des obligations et engagements des différents acteurs relatifs à la délivrance et l'usage des certificats numériques de personnes physiques dans le cadre de leur activité réglementé d'Experts-Comptables.

Cette PC est conforme aux principes et recommandations définies dans la norme *ETSI TS 101 456* et, dans une version ultérieure, *ETSI EN 319411-2*.

Cette politique de certification vise à permettre la délivrance de certificats qualifiés au sens du *Règlement (UE) N° 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur* (dit « Règlement eIDAS »). Ces certificats seront utilisés pour des signatures électroniques ayant des effets juridiques identiques sur des écrits électroniques à ceux procurés par la signature manuscrite sur les documents papier et qui sont par conséquent recevables en justice. Ces certificats qualifiés sont distribués à des utilisateurs finaux pour sécuriser des applications à l'aide d'un dispositif sécurisé de création de signature (DSCS).

I.2 Identification du document

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

L'OID de la présente PC est : 1.2.250.1.165.1.10.11.1

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 désignes 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 juin 2016

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

I.4.1 Le Prestataire de services de certification électronique

Se référer au document [PC_SA].

I.4.2 Autorité de certification (AC)

Se référer au document [PC_SA].

I.4.3 Autorité d'enregistrement (AE)

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

- la prise en compte et la vérification des informations du futur porteur et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'ICP suivant l'organisation de cette dernière et les prestations offertes ;

- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur y compris lors des échanges de ces données avec les autres fonctions de l'ICP (notamment, elle respecte la législation relative à la protection des données personnelles).

La fonction d'AE est exercée par le secrétaire général de l'Ordre de chaque région, ou bien l'AE nationale (permanent du CSOEC).

Les salariés des CROEC/CDOEC peuvent recevoir délégation du rôle d'AE.

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

I.4.4 Opérateur de certification (OC/OSC)

Se référer au document [PC_SA].

I.4.5 Porteurs de certificats

Se référer au document [PC_SA].

I.4.6 Utilisateurs de certificat

Se référer au document [PC_SA].

I.4.7 Mandataire de certification

La fonction de mandataire de certification n'est pas utilisée dans l'I.G.C. de l'OEC.

I.5 Usage des certificats

Se référer au document [PC_SA].

I.6 Gestion de la PC

Se référer au document [PC_SA].

II RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES

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'AC émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un "*Distinguished Name*" (DN) de type X.501.

III.1.2 Nécessité d'utilisation de noms explicites

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

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

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

III.1.2.1 Identité de l'A.C émettrice

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

C	FR
O	Ordre des Experts-comptables
OU	0002 775670003
OI	NTRFR-775670003
CN	Signature et Authentification - 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 SIREN de l'organisme, précédé du code « 0002 » (contrainte R.G.S.) ;
- le champ `OI` contient le SIREN de l'organisme, précédé du code « NTRFR- » (contrainte ETSI) ;
- le champ `CN` contient le nom de l'A.C.

III.1.2.2 Identité des porteurs

Le DN des certificats porteurs est construit comme suit :

C	FR
O	*[CSOEC, CROEC ou CDOEC concerné]*
OU	0002 *[SIREN de l'organisation concernée]*
OI	NTRFR-*[SIREN de l'organisation concernée]*

T	*[soit* « Élu conseiller régional »*, soit* « Élu conseiller national »*]*
SERIALNUMBER	*[sha256 du supra du porteur]*
givenName	*[prénom du porteur]*
surName	*[nom du porteur]*
CN	*[« M » ou « Mme »] [Prénom Nom]*

- Le champ `C=FR` désigne la France ;
- Le champ `O` désigne le CSOEC ou le conseil régional (ou départemental) de l'Ordre d'élection du porteur ;
- 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 la chaîne « Élu régional » ou « Élu CSOEC », en fonction de la qualité du porteur ;
- Le champ `CN` contient le prénom et le nom du porteur (dans cet ordre) tels qu'ils apparaissent dans le tableau de l'Ordre, précédé du « M » ou d'un « Mme », en fonction du genre du porteur ;
- Le champ `surName` contient le nom du porteur tel qu'il apparaît dans le tableau de l'Ordre ;
- Le champ `givenName` contient le prénom du porteur tel qu'il apparaît dans le tableau de l'Ordre ;
- Le champ `serialNumber` contient un numéro unique d'identification, propre au porteur. Ce champ est calculé à partir du numéro SUPRA du porteur et est utilisé par les applications du métier pour identifier le porteur.

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

III.1.3 Pseudonymisation des porteurs

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

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

Voir III.1.2 ci-dessus.

III.1.5 Unicité des noms

Se référer au document [PC_SA].

III.1.6 Identification, authentification et rôle des marques déposées

Se référer au document [PC_SA].

III.2 Validation initiale de l'identité

La demande initiale s'appuie sur une copie d'une pièce d'identité officielle du demandeur. L'inscription du demandeur au tableau de l'Ordre est alors vérifiée par l'A.E, ainsi que sa qualité d'élu (vérification du mandat électif, via un P.-V. de séance, une publication des résultats, etc.).

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-dessus.

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

L'identité du porteur est vérifiée lors d'un face à face physique avec l'AE.

Le dossier d'enregistrement, déposé directement auprès de l'AE, comprend au moins :

- Une pièce d'identité officielle en cours de validité (carte nationale d'identité ou passeport).
- Une copie du formulaire de demande de certificat, signée par le porteur.

  La demande peut être établie sur papier (signature manuscrite) ou au format électronique, sous réserve que le formulaire soit signé par le futur porteur à l'aide d'une signature électronique qualifiée, et que la signature soit vérifiée et valide au moment de l'enregistrement.

Remarque : de part son statut d'expert-comptable, le demandeur possède *a priori* un certificat électronique de signature émis par le CROEC/CDOEC auquel il est rattaché ; ce certificat peut être utilisé pour établir une demande au format électronique. La possession d'un tel certificat n'est toutefois pas requise.

- Tout document attestant de la qualité d'élu du signataire (P.-V. de séance, de publication des résultats).

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

- une copie de la pièce d'identité présentée et des autres pièces mentionnées ci-dessus
- la copie du formulaire de demande de certificat, signée par le porteur.
- l'attestation d'acceptation du certificat signée par le porteur lors de la remise de la carte à puce (support du certificat et des clés)

La signature de l'attestation d'acceptation du certificat par le porteur est considérée comme la preuve de la possession du support de la clé privée. La possession de la clé privée sera démontrée par la signature en ligne au moyen du certificat du bordereau d'activation. Cette signature est possible à tout moment mais sera conseillée au moment du retrait.

III.2.4 Informations non vérifiées du porteur

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.

III.2.6 Certification croisée d'A.C.

Se référer au document [PC_SA].

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

Sans objet.

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

Se référer au document [PC_SA].

De plus, lorsque le CSOEC, en tant qu'AC, est informé de la perte du mandat électif du porteur, il procède à la révocation du certificat et en informe le porteur.

IV EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

IV.1 Demande de certificat

IV.1.1 Origine d'une demande de certificat

Les personnes habilitées à déposer une demande de certificat sont les experts-comptables inscrits au tableau de l'Ordre lorsqu'ils deviennent élus de la profession.

L'A.E. assure la validation de la demande de certificat en s'appuyant sur le tableau de l'Ordre 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

Les informations suivantes font partie de la demande de certificat :

- Les nom et prénoms du porteur à utiliser dans le certificat
- Le CROEC de rattachement
- La qualité d'élu (élu conseiller régional ou conseiller supérieur) et, éventuellement, le CROEC afférent
- L'adresse postale du porteur
- La ou les adresses courriel du porteur
- Le code de révocation

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 :

1. Valider l'identité du futur porteur et son inscription au tableau de l'Ordre ; dans le cas des changements de nom de famille (nom de jeune fille, mariages…), l'AE s'assurera par tout autre moyen de l'identité d'usage du demandeur à l'aide de pièces complémentaires.
2. S'assurer de la qualité d'élu du porteur ;
3. Vérifier la cohérence des justificatifs présentés ;
4. S'assurer que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation) ;
5. Dans le cas où la demande a été déposée au format numérique, vérifier la signature électronique de celle-ci.

Une fois ces opérations effectuées, une demande de génération du certificat et du biclé est générée par l'A.C. vers la fonction adéquate de l'ICP.

IV.2.2 Acceptation ou rejet de la demande

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

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'A.C. déclenche les processus de génération et de préparation des différents éléments destinés au porteur 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 remis en mains propres au porteur, tandis que 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 aux chapitres V et VI, notamment la séparation des rôles de confiance.

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

La remise du certificat se fait en mains propres (face-à-face).

Le certificat complet et exact est mis à la disposition de son porteur.

IV.4 Acceptation du certificat

IV.4.1 Processus préalable à la délivrance

En parallèle au tirage de la biclé par l'A.C. et à la confection du certificat, l'E.-C. demandeur recevra à en courrier simple le code PIN de son support (clé USB). L'adresse utilisée est l'adresse professionnelle d'inscription au tableau de l'Ordre.

La carte est envoyée au CROEC/CDOEC dont dépend l'expert-comptable, ou au CSOEC (dans le cas d'un élu national).

L'expert comptable demandeur se rend alors au siège du CROEC/CDOEC dont il dépend, ou au CSOEC.

IV.4.1.1 Cas particulier d'une remise collective

La remise des supports et des certificats en mains propres pourra se dérouler pour chaque élu soit individuellement (ci-dessus), soit collectivement à l'occasion d'un événement officiel de l'Ordre, notamment lors de la réunion des assemblées collégiales. Dans ce cas, le support n'est pas envoyé au CROEC/CDOEC dont dépend le porteur, mais à l'A.C., dont un représentant sera présent à cet événement.

Le cas échéant, en fonction des modalités d'organisation des remises en masse, le code PIN d'activation des cartes pourra être transmis aux porteurs par un autre moyen que le courrier postal. Dans tous les cas, les codes d'activation seront transmis de manière séparée, dans le temps et dans l'espace, des supports, et par un canal assurant l'identité du destinataire.

IV.4.2 Démarche d'acceptation du certificat

Au cours d'un face à face, le demandeur doit présenter une pièce d'identité en cours de validité. Si elle correspond à la demande de certificat et aux informations enregistrées dans l'annuaire de la profession, alors le certificat peut être délivré.

Dans le cas où une discordance est notée, le certificat est immédiatement révoqué par l'A.E. et la carte détruite.

Sinon, la carte contenant les clés et le certificat est remise au porteur. Il visualise alors le contenu du certificat avec l'A.E. et signe le document d'acceptation du certificat et le bordereau de remise de la ou des cartes physiques.

IV.4.2.1 Cas particulier d'une remise collective

Les demandes font l'objet d'une vérification dans la demi-journée précédant la remise physique, et non lors de la remise (vérification de l'inscription du porteur dans l'annuaire de la profession et de la détention d'un mandat électif).

L'A.E. peut être une personne dûment habilitée pour l'occasion : la liste des A.E. présentes est validée par le CSOEC.

IV.4.3 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 sans l'accord du porteur du certificat et qu'après acceptation du contenu du certificat par celui-ci.

IV.4.4 Notification par l'A.C. aux autres entités de la délivrance du certificat

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

IV.5 Usages de la biclé et du certificat

IV.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature et d'authentification (*cf.* chapitre I.4.1.1). Les porteurs doivent respecter strictement les usages autorisés des biclés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'utilisation des clés privées est limitée à :

La signature électronique de documents (en rapport avec le mandat électif)

Cet usage est indiqué explicitement dans explicité dans les conditions générales d'utilisation et le contrat porteur. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du porteur par l'AC avant d'entrer en relation contractuelle.

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

Voir chapitre précédent et chapitre I.4.

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

IV.6 Renouvellement d'un certificat

Se référer au document [PC_SA].

IV.7 Modification du certificat

La modification de certificat n'est pas autorisée dans la présente P.C.

IV.8 Révocation et suspension des certificats

IV.8.1 Causes possibles d'une révocation

IV.8.1.1 Certificats de porteurs

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

- les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité personnelle ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat

- la révocation du certificat d'expert-comptable du fait de la perte de cette qualité professionnelle
- le porteur n'a pas respecté les modalités applicables d'utilisation du certificat
- le porteur n'a pas respecté leurs obligations découlant de la P.C. de l'A.C.
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur
- la clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées)
- le porteur ou une entité autorisée (représentant légal de l'entité) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur ou de son support)
- le décès du porteur
- la perte de la qualité d'élu du porteur pour quelle que cause que ce soit (démission, inéligibilité ou incompatibilité, sanction disciplinaire ou pénale, etc.)

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.

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

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'I.G.C. (y compris un certificat d'A.C. pour la génération de certificats, de L.C.R. ou de réponses O.C.S.P.) :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante
- décision de changement de composante de l'I.G.C. suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la D.P.C. (par exemple, suite à un audit de qualification ou de conformité négatif)
- cessation d'activité de l'entité opérant la composante

IV.8.2 Origine d'une demande de révocation

IV.8.2.1 Certificats de porteurs

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

- le porteur au nom duquel le certificat a été émis
- l'assemblée collégiale de l'Ordre à laquelle le porteur a été élu
- l'A.C. émettrice du certificat ou l'une de ses composantes (A.E.)
- l'A.C. du CROEC d'appartenance, émettrice du certificat personnel d'EC, du fait de la perte de la qualité d'EC
- le CSOEC par l'intermédiaire de l'AC

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

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

La révocation d'un certificat d'A.C. ne peut être décidée que par l'entité responsable de l'A.C., ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'A.C. sans délai.

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

IV.8.3.1 Certificats de porteurs

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre III.4.

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

a) En contactant l'AE nationale (CSOEC) par téléphone ou par e-mail

b) Depuis le portail web client de l'OSC, 24h/24 et 7j/7. Selon les cas, le porteur est authentifié soit à l'aide de questions/réponses (s'il les a configurées), soit à l'aide d'un code de révocation.

c) Auprès du CSOEC : le porteur peut se présenter directement muni d'une pièce d'identité.

d) Une demande de révocation peut également être faite par courrier ou par télécopie auprès du CSOEC

Les informations suivantes figurent dans la demande de révocation de certificat :

- l'identité du porteur du certificat utilisée dans le certificat (nom, prénom, …)
- le nom du demandeur de la révocation
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (numéro de série, etc.)
- la cause de révocation, notamment si elle concerne le mandat électif du porteur.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée au minimum via une L.C.R. signée par une entité désignée par l'A.C. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'A.C. (voir chapitre IV.8.12).

Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le porteur du certificat n'est pas le demandeur, il est également informé de la révocation effective de son certificat.

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

IV.8.3.2 Certificats d'une composante de l'I.G.C.

Se référer au document [PC_SA].

IV.8.4 Délai accordé au porteur pour formuler la demande de révocation

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

IV.8.5 Délai de traitement par l'A.C. d'une demande de révocation

Se référer au document [PC_SA].

IV.8.6 Exigences de vérification de la révocation par les utilisateurs de certificats

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

La méthode utilisée (L.C.R., O.C.S.P., etc.) est à l'appréciation de l'utilisateur selon sa disponibilité et les contraintes liées à son application.

IV.8.7 Fréquence d'établissement des L.C.R.

Se référer au document [PC_SA].

IV.8.8 Délai maximum de publication d'une L.C.R.

Se référer au document [PC_SA].

IV.8.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Se référer au document [PC_SA].

IV.8.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Se référer au document [PC_SA].

IV.8.11 Autres moyens disponibles d'information sur les révocations

Se référer au document [PC_SA].

IV.8.12 Exigences spécifiques en cas de compromission de la clé privée

Se référer au document [PC_SA].

IV.8.13 Suspension des certificats

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

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

Se référer au document [PC_SA].

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

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

IV.11 Séquestre de clé et recouvrement

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

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

IV.11.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

IV.11.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

V MESURES DE SÉCURITÉ NON TECHNIQUES

Se référer au document [PC_SA].

VI MESURES DE SÉCURITÉ TECHNIQUES

Se référer au document [PC_SA].

VII PROFILS DES CERTIFICATS, OCSP ET DES LCR

VII.1 Certificats de porteurs

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

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	Voir III.1.2.1
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (3 ans après la date d'émission du certificat)
Subject	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 VII.2)
keyIdentifier	issuerName+serialNumber
Subject Key Identifier	Identification de la clé publique du porteur
Key Usage (critical)	contentCommitment, digitalSignature
Certificate Policies (critical)	
policyIdentifier	1.2.250.1.165.1.10.11.1
policyQualifier-cps	https://www.signexpert.fr/PC/PC_ELUS.pdf
policyQualifier-unotice	Ce certificat de membre de l'Ordre des Experts-Comptables selon la politique ci-dessus
policyIdentifier (QCP-n-qscd)	0.4.0.194112.1.2
Subject Alternative Name	
rfc822Name	Adresse courriel 1 du porteur
rfc822Name	Adresse courriel 2 du porteur
Basic Constraint (critical)	CA:False
CRL Distribution Points	
distributionPoint	http://seec.experts-comptables.fr/CRL/CRL_signature_et_authentification.crl http://www.signexpert.fr/CRL/CRL_signature_et_authentification.crl http://trustcenter-crl.certificat2.com/CRL/CRL_signature_et_authentification.crl
Authority Information Access	
ocsp	http://ocsp2.experts-comptables.fr/OEC-ACUNIQUE
caIssuer	http://seec.experts-comptables.fr/cert/cert_signature_et_authentification.p7b

Champ	Description
QCStatements	
id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	Set
id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)	Set
id-etsi-qcs-QcType (0.4.0.1862.1.6)	id-etsi-qct-esign (1)
id-etsi-qcs-QcPDS (0.4.0.1862.1.5)	URL= https://www.signexpert.fr/PDS/PDS_Experts-Comptables_2016.pdf language="EN"

VII.2 Certificat d'A.C.

Se référer au document [PC_SA].

VII.3 Liste de Certificats Révoqués

Se référer au document [PC_SA].

VII.4 Certificat des réponses OCSP

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

VIII AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

Se référer au document [PC_SA].

IX AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

Se référer au document [PC_SA].

X ANNEXE 1 : DOCUMENTS CITÉS EN RÉFÉRENCE

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

[PC_SA] *PGS-OEC Politique de Certification - Signature & Authentification*, Version 1.1, OID n° 1.2.250.1.165.1.10.1.1

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.
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 »)

X.2 Documents techniques

Document
ETSI EN 319401, *General Policy Requirements for Trust Service Providers*, v. 2.1.1
ETSI EN 319411, *Policy & Security Requirements for TSPs Issuing Certificates*
ETSI EN 319412, *Certificate Profiles*
ETSI TS 101 456 V1.4.3 (mai 2007) "*Policy Requirements for Certification Authorities issuing qualified certificates*"
RFC3647 - IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003

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

Se référer au document [PC_SA].

XII ANNEXE 3 : EXIGENCES DE SÉCURITÉ DU DISPOSITIF DE CRÉATION DE SIGNATURE

Se référer au document [PC_SA].