ORDRE DES EXPERTS-COMPTABLES

ECM Association

POLITIQUE DE CERTIFICATION « OCSP AC Unique »

Version 1.2

Du 04 Mai 2017

OID nº 1.2.250.1.165.1.10.7.1 et 1.2.250.1.165.1.11.7.1

ORDRE DES EXPERTS-COMPTABLES

M DOMINIQUE JOURDE
2017.06.08 17:34:57 +0200

HISTORIQUE DES VERSIONS

Date	Nom	Évolutions	Édition / révision
Avril 2016	Samuel LACAS	Création du document	1.1-alpha
Mai 2017	Mathieu JORRY	Modifications diverses : point de contact, eIDAS, mise en page	1.2

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 OCSP ». Le présent document constitue cette politique.

Ce document constitue une Politique de Certification (P.C.) mise en œuvre par les Autorités de Certification de l'Ordre des Experts Comptables (OEC) pour les membres de l'Ordre.

Dans le cadre de cette P.C., les certificats sont destinés au service de vérification en ligne (OCSP) des certificats Signexpert des A.C. de l'Ordre. Ces certificats sont utilisés pour signer (sceller) les réponses de ce service.

En pratique, chaque A.C. de l'Ordre émettant des certificats finaux fournit un service de vérification en ligne, et produit donc des certificats de scellement. Le présent document décrit les modalités de production de ces certificats, communes à toutes les A.C.

À la date de rédaction du présent document, deux A.C. sont concernées (cf. ci-dessous).

I.2 Identification du document

Le présent document est dénommé *PGS-OEC Politique de Certification – OCSP AC Unique*. Il est identifié par le nom, numéro de version, et la date de mise à jour.

Ce document décrit la politique commune à deux familles de certificats identifiés par les OID suivants :

AC Émettrice	OID (de la PC) de l'AC Émettrice	OID de la famille OCSP
Signature et Authentification - Ordre des Experts-Comptables	1.2.250.1.165.1.10.1.1	1.2.250.1.165.1.10.7.1
Cachet - Ordre des Experts-Comptables	1.2.250.1.165.1.11.1.1	1.2.250.1.165.1.11.7.1

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

I.3.1 Le Prestataire de services de certification électronique

Se référer au document [PC_SA] ou [PC_CC].

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

Se référer au document [PC_SA] ou [PC_CC].

I.3.3 Autorité d'enregistrement (A.E.)

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

- la prise en compte et la vérification des informations du futur R.C.O. 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.O. 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).

I.3.4 Opérateur de certification (OC/OSC)

Se référer au document [PC_SA] ou [PC_CC].

I.3.5 Responsable de certificat OCSP (R.C.O.)

Le R.C.O. est la personne physique responsable du certificat OCSP, 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., le R.C.O. est désigné par l'A.E. (CSOEC).

Le R.C.O. 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.O., ce dernier peut être amené à changer en cours de validité du certificat : départ du R.C.O. 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.O. 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.O. explicitement identifié.

I.3.6 Utilisateurs de certificat

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

- Un agent (personne physique) destinataire de données signées par un serveur informatique et qui utilise un certificat Signexpert et un module de vérification de certificat.
- Un serveur informatique destinataire de données provenant d'un autre serveur informatique et qui utilise un certificat Signexpert et un module de vérification de certificat afin de s'assurer de la validité du certificat Signexpert.

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

I.4 Usage des certificats

I.4.1 Domaines d'utilisation applicables

I.4.1.1 Biclés et certificats

La présente P.C. traite des biclés et des certificats utilisés pour signer (authentifier) des réponses OCSP relatives aux certificats Signexpert.

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

Se référer au document [PC_SA] ou [PC_CC].

I.4.1.2.1 Certificats d'A.C.

Se référer au document [PC_SA] ou [PC_CC].

I.4.1.2.2 Certificats de composante

Se référer au document [PC_SA] ou [PC_CC].

I.4.2 Domaines d'utilisation interdits

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

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

I.5 Gestion de la P.C.

Se référer au document [PC_SA] ou [PC_CC]. La présente PC est gérée de façon identique.

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

Se référer au document [PC_SA] ou [PC_CC].

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.O. (*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

Se référer au document [PC_SA] ou [PC_CC].

III.1.2.2 Identité des services OCSP

Le DN des certificats est décrit dans la PC de l'A.C. ([PC_SA] ou [PC_CC]).

III.1.2.3 Certificats de test

L'A.C. est susceptible d'émettre des certificats de test. Ceux-ci ne se distinguent en aucune manière des certificats utilisés en production.

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 {plate-forme OCSP; entité de rattachement} au sein du domaine de l'A.C.

Dans chaque certificat X509v3, 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 `CN` du DN (y compris pour les certificats de test).

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

Une seule identité est considérée dans le cadre de cette P.C. : le service OCSP *Signexpert*.

Le R.C.O. et le nom de la plate-forme devant apparaître dans le certificat sont établis par l'A.C., en accord avec l'opérateur du service.

Un R.C.O. peut être amené à changer en cours de validité du certificat OCSP (voir chapitre I.3.3), dans ce cas, tout nouveau R.C.O. 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.O.

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

- Une copie de la carte d'identité du R.C.O.
- Un e-mail et un numéro de téléphone du R.C.O.

III.2.3.2 Enregistrement d'un Mandataire de Certification

Sans objet.

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

Sans objet

III.2.4 Informations non vérifiées du R.C.O.

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.O.).

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 douze mois. Le renouvellement de la biclé d'un serveur entraîne automatiquement la génération et la fourniture d'un nouveau certificat dans les conditions et suivant les modalités décrites dans la présente section.

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

La procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial. Si le R.C.O. ne change pas, l'A.C. génère et transmet les nouvelles clés et le certificat automatiquement à celui-ci.

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

Le R.C.O. peut demander la révocation de son certificat auprès du CSOEC en le contactant par tout moyen : sur place, par téléphone, par e-mail (signexpert@cs.experts-comptables.org).

IV EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

IV.1 Demande de certificat

IV.1.1 Origine d'une demande de certificat

L'opérateur technique du service OCSP établit la demande de certificat (génération de la biclé, création de la C.S.R.) et la soumet à l'A.C. (CSOEC) pour validation.

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

L'opérateur technique du service OCSP est responsable de la génération de la biclé et de la création de la C.S.R.

IV.2 Traitement d'une demande de certificat

À la réception de la demande, l'A.C. transmet celle-ci au R.C.O. (si celui-ci n'en est pas déjà destinataire). Le R.C.O. valide les aspects techniques de la demande et informe l'A.C. En cas de problème ou d'erreur dans la demande, celle-ci est annulée et une nouvelle demande est établie en collaboration avec l'opérateur technique.

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

IV.2.1 Acceptation ou rejet de la demande

Voir ci-dessus.

IV.2.2 Durée d'établissement du certificat

La durée d'établissement du certificat est d'au plus 5 jours.

IV.3 Délivrance du certificat

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

Après établissement de la demande, l'A.C. déclenche les processus de génération et de préparation des différents éléments destinés au R.C.O. auprès de l'OSC.

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

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

La remise du certificat se fait par e-mail. L'adresse utilisée est l'adresse du R.C.O. saisie lors du processus de désignation du R.C.O.

Le certificat complet et exact est mis à la disposition du R.C.O., lequel le transmet à l'opérateur technique pour intégration au service OCSP après vérification.

IV.4 Acceptation du certificat

Voir ci-dessus.

IV.4.1 Démarche d'acceptation du certificat

L'acceptation du certificat est tacite dès lors que le R.C.O. le transmet au service OCSP pour intégration.

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.

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.O.

L'utilisation de la clé privée du R.C.O. et du certificat associé est strictement limitée à la signature des réponses OCSP (*cf.* chapitre I.4.1.1). Cette contrainte est portée à la connaissance des R.C.O. et de l'opérateur technique du serviec par l'A.C., notamment dans l'accord contractuel qui les lie.

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 le certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat
- le R.C.O. ou l'opérateur technique n'a pas respecté les modalités applicables d'utilisation du certificat
- le R.C.O. 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.O. 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.O. de rattachement du serveur
- le décès du R.C.O.

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

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 OCSP

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.O.
- le représentant légal de l'organisme identifié dans le certificat
- le CSOEC, par l'intermédiaire de l'A.C.

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.O.

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

- 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 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.O. pour formuler la demande de révocation

Dès que le R.C.O. (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.O.

Toute demande de révocation est traitée en urgence.

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

Il s'écoule au maximum 72 heures entre la demande de révocation par le R.C.O. 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. de l'A.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.O. 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

Se référer au document [PC_SA] ou [PC_CC].

IV.9.7 Délai maximum de publication d'une LCR

Se référer au document [PC_SA] ou [PC_CC].

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

Sans objet.

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

Sans objet pour un certificat OCSP.

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

IV.9.12 Suspension de certificats

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

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

IV.10.1 Caractéristiques opérationnelles

Se référer au document [PC_SA] ou [PC_CC].

IV.10.2 Disponibilité de la fonction

Se référer au document [PC_SA] ou [PC_CC].

IV.11 Fin de la relation entre le R.C.O. et l'A.C.

Se référer au document [PC_SA] ou [PC_CC].

IV.12 Séquestre de clé et recouvrement

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

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

IV.13 Certificats de test

Les certificats de test (*cf.* III.1.2.3) et leurs supports sont produits et gérés par l'OSC en accord avec l'A.C., dans le cadre de campagnes de test définies et formalisées. Les certificats de test sont révoqués dès lors que la campagne de test est terminée.

V MESURES DE SECURITE NON TECHNIQUES

Se référer au document [PC_SA] ou [PC_CC].

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

Se référer au document [PC_SA] ou [PC_CC].

VI.1.2 Transmission de la clé privée à son propriétaire

La clé privée est générée directement par l'opérateur technique du service sur le matériel de production du service OCSP.

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

La clé publique est transmise par e-mail à l'A.C. (voir IV.1).

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

Se référer au document [PC_SA] ou [PC_CC].

VI.1.5 Tailles des clés

Se référer au document [PC_SA] ou [PC_CC].

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

Se référer au document [PC_SA] ou [PC_CC].

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 (voir chapitre I.4.1).

L'utilisation de la clé privée du certificat OCSP est strictement limitée au service OCSP.

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

Se référer au document [PC_SA] ou [PC_CC].

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

Se référer au document [PC_SA] ou [PC_CC].

VI.2.3 Séquestre de la clé privée

Se référer au document [PC_SA] ou [PC_CC].

VI.2.4 Copie de secours de la clé privée

Se référer au document [PC_SA] ou [PC_CC].

VI.2.5 Archivage de la clé privée

Les clés privées du service OCSP ne doivent en aucun cas être archivées.

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

Sans objet ; la clé est générée dans le module.

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

Voir ci-dessus.

VI.2.8 Méthode d'activation de la clé privée

Se référer au document [PC_SA] ou [PC_CC].

VI.2.9 Méthode de désactivation de la clé privée

Se référer au document [PC_SA] ou [PC_CC].

VI.2.10 Méthode de destruction des clés privées

Se référer au document [PC_SA] ou [PC_CC].

VI.2.11 Autres aspects de la gestion des biclés

VI.2.11.1 Archivage des clés publiques

Les clés publiques du service OCSP 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 du service OCSP couverts par la présente P.C. doivent avoir une durée de vie au maximum de douze mois.

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

Ces questions sont traitées dans la politique de sécurité de l’opérateur du service OCSP.

VI.3.2 Protection des données d’activation

Ces questions sont traitées dans la politique de sécurité de l’opérateur du service OCSP.

VI.4 Mesures de sécurité des systèmes informatiques

Se référer au document [PC_SA] ou [PC_CC].

VI.5 Mesures de sécurité liées au développement des systèmes

Se référer au document [PC_SA] ou [PC_CC].

VI.6 Mesures de sécurité réseau

Se référer au document [PC_SA] ou [PC_CC].

VI.7 Horodatage / Système de datation

Se référer au document [PC_SA] ou [PC_CC].

VII PROFILS DES CERTIFICATS OCSP ET DES LCR

VII.1 Certificats OCSP

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	DN de l'A.C. émettrice (voir [PC_SA] ou [PC_CC])
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (12 mois après la date d'émission du certificat)
Subject	C=FR O=Ordre des Experts-Comptables OU=0002 775670003 OI=NTRFR-775670003 CN=OCSP Signature-OEC
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 [PC_SA] ou [PC_CC])
Subject Key Identifier	Identification de la clé publique de la plate-forme
Key Usage (critical)	digitalSignature
Certificate Policies (critical)	
policyIdentifier	1.2.250.1.165.1.10.7.1
policyQualifier-cps	http://www.signexpert.fr/PC/PC_OCSP_2016.pdf
policyQualifier-unotice	Ce certificat technique de l'Ordre des Experts-Comptables selon la politique ci-dessus
Others	
Basic Constraint (critical)	CA:False
Extended Key Usage	OCSPSigning
OCSP No Check	null

VII.2 Liste de Certificats Révoqués

Se référer au document [PC_SA] ou [PC_CC].

VII.3 Certificat de l'A.C. émettrice

Se référer au document [PC_SA] ou [PC_CC].

VIII AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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

IX AUTRES PROBLEMATIQUES METIERS ET LEGALES

Se référer au document [PC_SA] ou [PC_CC].

X ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

[PC_SA] *PGS-OEC Politique de Certification - Signature & Authentification,* Version 1.1, OID n° 1.2.250.1.165.1.2.10.1.1

[PC_CC] *PGS-OEC Politique de Certification – Cachet,* Version 1.1, OID n° 1.2.250.1.165.1.2.11.1.1

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

Se référer au document [PC_SA] ou [PC_CC].

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

XII.1 Exigences sur les objectifs de sécurité

Le dispositif de création de signature OCSP, utilisé par l'opérateur technique pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa biclé, doit répondre aux exigences de sécurité suivantes :

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

XII.2 Exigences sur la qualification

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