ORDRE DES EXPERTS-COMPTABLES

ECM Association

Signexpert – Plan de fin de vie

ECMA

Version 1.1

Du 02 Mai 2017

M DOMINIQUE JOURDE
2017.06.08 17:35:40 +0200

HISTORIQUE DES VERSIONS

N°. vers.	Date	Auteur	Modifications
1.0	6 mars 2017	Samuel Lacas	Création du document
1.1	2 Mai 2017	Mathieu JORRY	Modifications diverses et mise en page

Contributeurs	Organisation
Sylvie PICON	ECMA
Samuel LACAS	SealWeb
Mathieu JORRY	ECMA
Fabrice FAIVRE	ECMA

DESTINATAIRES DU DOCUMENT

ENTITÉ / Interne	NOM
CSOEC/ECMA	Président de l'Ordre
	Secrétaire Général de l'Ordre
	Membres COMEX & CODIR
	Johanne KAUFLING
	Mathieu JORRY
	Sylvie PICON
	Fabrice FAIVRE

ENTITÉ / Externe	NOM
IDnomic	Amira OULED-BARKA
	Céline GROULT
SEALWEB	Samuel LACAS

SOMMAIRE

1. OBJET DU DOCUMENT

Le présent document décrit les procédures de fin de vie des AC et, en particulier, les procédures de :

- Renouvellement
- Fin de vie

Dans tous les cas, le CSOEC, agissant en tant que prestataire de service de confiance, prendra toutes les mesures nécessaires pour minimiser l'impact de ces procédures sur les porteurs et tiers.

Ces procédures respectent, le cas échéant, les exigences 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 et abrogeant la directive 1999/93/CE*, dit « Règlement eIDAS ».

2. DEFINITIONS

2.1 ULTIME LCR

Il s'agit de la dernière LCR produite par une AC. Celle-ci comprend au moins l'intégralité des certificats révoqués par l'AC et en cours de validité à la date de production de cette LCR.

Si l'AC en question produisait des certificats qualifiés au sens du *Règlement (UE) N° 910/2014* (règlement eIDAS), cette LCR doit de plus :

- avoir une fin de validité positionnée à la date de fin de vie de l'AC ou, à défaut, au 31 décembre 9999, 23h59m59s (« 99991231235959Z »)
- contenir l'intégralité des certificats révoqués par l'AC (tout au long de sa période d'activité)

2.2 ULTIME REPONSE OCSP

Il s'agit du dernier ensemble de jetons OCSP produits par une AC. Cet ensemble comprend au moins l'intégralité des certificats produits par l'AC et en cours de validité à la date de production de cet ensemble.

L'ultime réponse OCSP est signée à l'aide du certificat d'AC : cela permet, le cas échéant, de révoquer les certificats de répondeur OCSP de l'AC.

Remarque : conformément à la *RFC 6960*, un jeton OCSP peut contenir des informations sur le statut de plusieurs certificats. L'ultime réponse OCSP peut donc être produite sous la forme d'un unique jeton OCSP contenant lui-même le statut de l'ensemble des certificats concernés.

Si l'AC en question produisait des certificats qualifiés au sens du *Règlement (UE) N° 910/2014* (règlement eIDAS) :

- cet ensemble doit de plus contenir l'intégralité des certificats produits par l'AC (tout au long de sa période d'activité)
- tous les jetons doivent avoir une fin de validité positionnée à la date de fin de vie de l'AC ou, à défaut, au 31 décembre 9999, 23h59m59s (« 99991231235959Z »)
- (rappel) les jetons devraient comporter l'extension « *archive cutoff* », comme prévu par la *RFC 6960*, avec une date identique à la date de début de validité du certificat de l'AC.

3. RENOUVELLEMENT

3.1 PERIODE DE RENOUVELLEMENT

La durée de validité des AC du CSOEC est de 10 ans (pour les AC RGS), et de 15 (quinze) ans pour les autres. En conformité avec les politiques de certification, ces AC ne sauraient produire des certificats ayant une date d'expiration postérieure à celle de l'AC elle-même. Le renouvellement d'une AC se fera donc au plus tard 3 ans avant la date de fin de validité de son certificat.

Dans le cas où l'AC ne serait pas renouvelée, celle-ci cessera de produire des certificats à cette date.

3.2 GENERATION D'UN NOUVEAU CERTIFICAT D'AC

Cette génération sera effectuée dans le cadre d'une cérémonie de clés. Se référer à la PC de l'AC.

Une fois le nouveau certificat en production, l'ancien certificat, ni la clé privée associée, ne seront plus utilisés par l'AC pour l'émission de certificats de porteurs.

3.2.1 Procédure de publication du certificat

Concernant la publication sur le site du CSOEC, se référer à la PC de l'AC.

Par ailleurs, le CSOEC notifiera l'autorité de contrôle national (« *supervisory body* ») du renouvellement afin que celui-ci mette à jour la liste de confiance.

3.3 FIN DE VIE D'UN CERTIFICAT RENOUVELE

Lorsqu'un certificat d'AC est renouvelé, il reste néanmoins valide jusqu'à son expiration, et la clé privée associée peut continuer à être utilisée pour la signature de LCR, de jetons ou de certificats OCSP. S'il n'existe plus aucun certificat émis par cette AC en cours de validité, l'AC peut émettre une unique et ultime CRL avant de procéder à la destruction de cette clé privée.

3.3.1 Archivage

Le CSOEC s'engage à archiver :

- La liste des certificats émis par l'AC ;
- L'ultime LCR (cf. 2.1) produite par l'AC (si l'AC assurait la publication d'une LCR) ;
- L'ultime réponse OCSP (cf. 2.2) produite par l'AC (si celle-ci assurait un service de répondeur OCSP) ;
- Les journaux d'événement de l'AC (se référer à la PC de l'AC) ;
- Le P.-V. de destruction (voir ci-dessous).

Cet archivage est réalisé auprès d'IDNomic pour une durée de 10 ans.

3.3.2 Communication

Par ailleurs, le CSOEC notifiera l'autorité de contrôle national (« *supervisory body* »), l'ANSSI, au moins un mois à l'avance de la destruction prévue des clés privées de l'AC.

L'information sera aussi publiée sur le site Signexpert.

3.3.3 Destruction des clés privées

Le CSOEC procédera à la destruction de la clé privée de l'AC et de ses éventuelles copies. Dans le cas où il ne serait pas possible de détruire effectivement ces éléments, des mesures seront prises pour assurer qu'ils

seront rendus inexploitables (destruction des clés de chiffrement, des parts de secret ou des données d'activation).

Remarque : les clés privées du service de répondeur OCSP de l'AC doivent, le cas échéant, être inclus dans cette étape.

Un procès-verbal de la destruction témoignera du bon déroulement de cette étape.

4. FIN DE VIE D'UNE AC

Le CSOEC peut décider de mettre un terme à l'activité d'une AC, soit suite à l'expiration de son certificat, soit de façon anticipée, suite à un incident ou à la décision de l'AC.

4.1 CESSATION D'ACTIVITE SUIVANT L'EXPIRATION

La procédure est identique à celle du § 3.3, si ce n'est qu'il n'y a pas de renouvellement de certificat ni de maintien de la fonction de révocation. Dans ce cas, le CSOEC prendra toutes les mesures nécessaires pour assurer que l'archivage et la disponibilité des données concernées soient effectifs durant toute la durée légale de conservation.

Par ailleurs, le CSOEC mettra fin aux contrats avec ses sous-traitants et prestataires.

4.2 CESSATION D'ACTIVITE ANTICIPEE (DECISION DE L'AC)

La décision de mettre fin à l'activité de l'AC de façon anticipée est du ressort du CSOEC.

4.2.1 Communication

Le CSOEC notifiera au plus tôt l'ANSSI de la décision, ainsi que la date de fin de vie prévue pour l'AC.

L'information sera aussi publiée sur le site Signexpert.

4.2.2 Révocation

1. À la date prévue, l'AC procédera à la révocation de tous les certificats émis en cours de validité. Alternativement, cette révocation peut se faire progressivement sur une période donnée, l'essentiel étant que tous les certificats émis et en cours de validité à la date prévue soient révoqués.

   Exception : Si l'AC émet des certificats OCSP pour ses propres besoins, ceux-ci sont aussi révoqués à cette étape.
2. Si l'AC assurait un service de répondeur OCSP, l'AC produit son ultime réponse OCSP (cf. 2.2).
3. Si l'AC assurait la publication d'une LCR, l'AC produit son ultime LCR (cf. 2.1).
4. Puis, le certificat d'AC sera lui-même révoqué par l'AC de niveau supérieur.

4.2.3 Archivage

La procédure est identique à celle du § 3.3.1. De plus, les archives seront déposées pour conservation auprès d'un notaire désigné par le CSOEC.

4.2.4 Destruction

La procédure est identique à celle du § 3.3.3.

4.3 CESSATION D'ACTIVITE SUITE A UN INCIDENT

La procédure est identique à celle du § 4.2, mais celle-ci est effectuée en urgence dans le cadre d'une procédure de gestion de crise. Conformément aux obligations introduites par le règlement eIDAS, CSOEC avertira l'ANSSI de l'incident dans les 24 (vingt-quatre) heures suivant sa détection.

4.4 PROVISIONS

Le CSOEC a financièrement provisionné les mesures suivantes :

- Maintien du site de publication de ses AC
- Conservation des archives par un service tiers (ou dépôt notarial).