Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement,
des transports, de l'énergie et de la communication DETEC

Office fédéral de la communication OFCOM
Division Services de télécommunication

20.06.2006

Révision des prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique

Rapport explicatif

L'expérience acquise au cours des premières procédures de reconnaissance démontre la nécessité d'adapter ou de préciser certains passages des prescriptions techniques et administratives (PTA) concernant les services de certification dans le domaine de la signature électronique.

Le présent document a pour but de présenter les adaptations majeures effectuées.

Chapitre 1.2 : Référence à la spécification ETSI TS 101 456
Il est dorénavant fait référence à la nouvelle version de la spécification ETSI 101 456 publiée en janvier 2006.
Cette adaptation n'a que peu d'influence sur les exigences imposées aux fournisseurs de services de certification (CSP) puisque seul le chapitre 7.2.5 a été adapté. Dans celui-ci, il est précisé que la clé du CSP utilisée pour générer les certificats qualifiés peut également être utilisée pour la signature d'autres types de certificats de même que pour la signature d'informations relatives à l'état révoqué des certificats (la liste des certificats annulés, par exemple).

Chapitre 1.2 : Référence à la spécification ETSI TS 101 861
En janvier 2006, une nouvelle version de la spécification ETSI TS 101 861 a également été publiée. Elle aussi présente des adaptations dont les effets sont négligeables pour les CSP.

Chapitre 3.2, lettres b et c : Principes opérationnels pour le système d'horodatage
Certains principes opérationnels relatifs au système d'horodatage sont ajoutés puisque la fourniture de contremarque de temps est imposée par l'art. 12 SCSE.

Chapitre 3.2, lettre c : Audits internes
Il est fait référence à la norme ISO/IEC 27001 pour préciser ce qui est entendu par « audits internes ».

Chapitre 3.2, lettre f : Examen d'équipements réparés
L'obligation d'examiner tout équipement avant sa remise en service est de toute évidence disproportionnée si l'on considère l'ensemble conséquent des équipements mis en œuvre par le CSP. Il est donc précisé que l'examen ne concerne que la remise en service d'équipements identifiés lors de l'analyse de risque comme éléments critiques du point de vue de la sécurité.
Afin d'assurer la sécurité des équipements, l'intervention de deux collaborateurs de confiance est non seulement exigée pour la remise en service mais également lors de la configuration de composants réparés.

Chapitre 3.2, lettre i : Tenir à jour les informations permettant le rétablissement des activités après un sinistre
Il est précisé que ce sont les informations actuelles qui doivent être sauvegardées afin de prendre en compte toute adaptation effectuée sur les systèmes qui pourrait avoir une incidence sur la sécurité.

Chapitre 3.3.3 : Dispositif de création de signature adapté à la génération en masse de signature
Il existe une réelle demande pour la génération en masse de signature afin d'assurer l'intégrité et l'authenticité de documents. L'ordonnance sur la Feuille officielle suisse du commerce (Ordonnance FOSC, RS 221.415), par exemple, prévoit à l'art. 8 al. 2, que la signature des données de la FOSC doit être fondée sur un certificat qualifié émis par un CSP reconnu au sens de la SCSE. On constate cependant que, dans le marché actuel, les certifications de produits selon ISO/IEC 15408 (*common criteria*) ou ITSEC qui sont exigées dans les PTA, ont plus généralement été obtenues pour des dispositifs sous forme de cartes à puce que pour des composants permettant la génération en masse de signatures (*Hardware Security Module HSM*). Ces derniers étant quant à eux disponibles sur le marché avec une certification FIPS 140-2.
Il convient donc d'adapter les PTA afin de ne pas empêcher la mise en œuvre de telles solutions. Pour assurer la sécurité physique, environnementale et opérationnelle ainsi que la sécurité relative au personnel lors de l'exploitation du dispositif de type *HSM*, il a été suggéré de référencer les chapitres

correspondant de la spécification ETSI TS 101 456. Il convient cependant de garder à l'esprit que cette spécification traite en particulier de la sécurité de l'infrastructure du CSP. Ces exigences ne paraissent donc pas adaptées aux HSM qui, dans le but visé par cette nouvelle disposition, sont exploités dans les infrastructures des titulaires de certificats. La référence à la norme ISO/IEC 27001 est donc préférée puisque cette dernière est neutre en ce qui concerne l'organisation considérée.
Le recours aux principes de l'ISO/IEC 27001 est certainement à l'avantage du titulaire de certificat dans le cas où ce dernier a d'ores déjà mis en œuvre un système de gestion de la sécurité basé sur la norme ISO/IEC 27001.
Les nouvelles exigences formulées dans les PTA laissent la liberté d'adopter des mesures de sécurité adaptées aux risques identifiés lors d'une analyse de risque ce qui est certainement sensé compte tenu de la diversité des mises en œuvre de tels dispositifs.
Ces nouvelles exigences imposent au CSP de s'assurer que le titulaire de certificat prend les mesures suffisantes en cas d'utilisation de tels dispositifs de création de signature à l'instar de ce qui est déjà imposé au chapitre 3.3.3 lettre a des PTA. Ceci est d'autant plus justifié que la solution de signature en masse sera très certainement réalisée par le CSP.

Chapitre 3.4.1, lettre b : Précision des informations à actualiser
Une précision relative aux informations à actualiser est apportée à la version allemande.

Chapitre 3.4.2, lettre c : Désignation de l'extension « qcStatements »
En pratique, il a été constaté que des applications courantes généraient des erreurs lors du traitement de l'extension « qcStatements » désignée comme critique dans le certificat.
Le choix de désigner cette extension comme extension critique ou non critique est donc laissé à la liberté du CSP afin d'éviter de telles erreurs. Ceci reste toutefois conforme au chapitre 3.2.6 du document RFC 3739 qui n'impose pas de désignation particulière.

Chapitre 3.5 : Contenu du certificat d'horodatage
Il a été suggéré que le contenu du certificat d'horodatage soit détaillé dans les PTA.
Ces dernières ne sauraient s'étendre au-delà du cadre légal et des exigences mentionnées dans les documents de référence. En conséquence, elles ne reprennent qu'une exigence du document RFC 3161. Celui-ci n'est en effet plus mentionné en tant que tel dans les PTA car il fait référence, dans le contexte du certificat d'horodatage, au document RFC 2459 qui a été remplacé par le document RFC 3280.