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

Rapport explicatif

1 Introduction

Les prescriptions techniques et administratives (PTA) concernant les services de certification électronique ont été élaborées en 2001. Entre-temps, de nouveaux standards internationaux décrivant plus précisément les politiques, les pratiques et l'organisation des fournisseurs de services de certification ont été publiés, notamment par l'ANSI (American National Standards Institute), l'ISO (International Organization for Standardization) et l'EESSI (European Electronic Signature Standardization Initiative).

Par la suite, les PTA de 2001 ont été comparées aux récentes publications internationales. Cette comparaison a mis en évidence d'essentielles différences qui ont été analysées et évaluées dans le cadre imposé par la nouvelle loi fédérale sur les services de certification dans le domaine de la signature électronique (SCSE) mais aussi en ayant pour objectif de favoriser le développement d'un marché sain, l'interopérabilité et l'harmonisation internationale.

Dans ce contexte, il a aussi été nécessaire de vérifier dans quelle mesure les anciennes PTA pouvaient être adaptées et où la référence à des standards reconnus était judicieuse.

2 Processus mis en œuvre pour l'élaboration des prescriptions techniques et administratives

2.1 Organismes de standardisation et leurs publications dans le domaine de la signature électronique

L'analyse des travaux réalisés par les organismes de standardisation a permis d'une part de dresser l'inventaire des publications, d'autre part d'évaluer leur reconnaissance au sein de l'économie et enfin de comprendre le processus d'élaboration et de mise à jour des standards.

2.1.1 ANSI X9.79 - PKI policy and practices framework

Pour le domaine des services financiers, l'ANSI (American National Standards Institute) a développé un cadre relatif aux politiques et pratiques des infrastructures à clé publique (PKI). Le standard ANSI X9.79*: Public Key Infrastructure (PKI) Practices and Policy Framework* comprend dans son annexe 2 des exigences spécifiques qui s'adressent aux exploitants de PKI. Ceux-ci ne sont pas tenus d'adopter des exigences particulières. Ils ont la liberté de choisir parmi les exigences relatives aux politiques, celles qui correspondent aux objectifs de leur propre politique.

Bien qu'il soit destiné aux exigences spécifiques de la communauté financière, il a cependant été très largement adopté dans le marché pour la reconnaissance des PKI. Il est recommandé par le PKI Forum, un groupe international de fournisseurs et d'utilisateurs de PKI. Le standard ANSI X9.79 a par ailleurs été adopté par l'AICPA/CICA (American and Canadian institutes for accountants) dans le cadre de son programme WebTrust qui consiste à évaluer l'adéquation et l'efficacité des contrôles utilisés par les autorités de certification.

2.1.2 ISO CD 21188-1 - PKI policy and practices framework

Fin 2001, les membres du comité TC68 de l'ISO (International Organization for Standardization) ont adopté une proposition de l'ANSI (American National Standards Institute) prévoyant l'élaboration d'un standard relatif aux pratiques et politiques des infrastructures à clé publique dans les services financiers, en se basant sur l'ANSI X9.79.

La majorité des membres européens de l'ISO ont approuvé ce projet à condition que les travaux tiennent compte de la directive européenne et de la spécification ETSI TS 101 456 *Policy requirements for certification authorities issuing qualified certificates*.

La première phase des travaux a permis la publication d'une première ébauche (Committee Draft ISO CD 21188-1) en octobre 2002.

L' European Telecommunication Standardization Institute (ETSI) a délivré de nombreuses suggestions destinées à faciliter l'alignement avec ses propres spécifications. Les commentaires issus de cette première consultation ont été intégrés au processus rédactionnel qui devrait livrer une seconde ébauche en 2004 et une publication définitive en 2005.

Contrairement au standard ANSI X9.79 utilisé comme document de référence lors de l'élaboration, l'ISO 21188-1 ne constitue pas un cadre général susceptible d'être appliqué dans bon nombre de secteurs mais s'adresse essentiellement au secteur financier.

2.1.3 European Electronic Signature Standardisation Initiative (EESSI).

2.1.3.1 Contexte

La « Directive 1999/93/CE du 13 décembre 1999, du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques » définit une forme particulière de signature électronique basée sur un certificat qualifié, comme condition de la reconnaissance légale de cette signature. Dans ses annexes, la directive identifie les exigences minimales auxquelles doivent se conformer les prestataires de services de certification qui délivrent des certificats qualifiés, les mesures de sécurité à respecter durant les phases d'élaboration et de vérification de la signature ainsi que la structure des données à adopter.

Pour faciliter sa mise en œuvre dans les diverses législations nationales et pour établir l'interopérabilité, elle prévoit la référence à des standards reconnus dans le domaine des signatures électroniques.

2.1.3.2 Travaux de standardisation

À cette fin, l'European ICT Standards Board a lancé, en 1999, l'«European Electronic Signature Standardization Initiative» (EESSI) avec le soutien de la Commission européenne et la participation active des milieux industriels, des autorités publiques, des experts du domaine et autres acteurs du marché.

Au préalable, les besoins en matière de standardisation correspondant aux exigences de la directive ont été déterminés. L'évaluation des standards disponibles et autres initiatives en cours dans un contexte global a ensuite mis en évidence le manque de consistance, de cohérence, mais également certaines lacunes qui ont justifié la nécessité d'entreprendre des activités supplémentaires de standardisation.

Les tâches d'élaboration des standards ont été confiées au Comité Européen de Normalisation (CEN) et à l'ETSI qui poursuivent, aujourd'hui encore, leurs activités. Celles-ci sont par ailleurs supervisées par un « steering group » dans lequel sont représentés les différents acteurs du marché.

Les travaux de ces organismes de standardisation sont ouverts à toute partie intéressée, ce qui permet la production de spécifications de qualité dans un esprit consensuel. Par ailleurs,

l'ETSI et le CEN collaborent étroitement entres eux mais aussi avec tout autre instance reconnue dans le domaine, de façon à assurer l'interopérabilité et l'harmonisation internationale des développements.

Des contacts sont ainsi maintenus avec

- l'APEC-TEL eStg (Asia-Pacific Economic Community, Telecommunication and information Working Group, eSecurity Task Group)
- l'IETF – PKIX (Internet Engineering Task Force)
- le gouvernement américain dans le cadre du programme US Federal PKI
- l'ISO (International Organization for Standardization)
- l'Asia PKI Forum
- le Japan PKI Forum
- le China PKI Forum

Outre l'échange d'informations, cette collaboration permet notamment d'analyser la correspondance entre les standards des différentes organisations et contribue à la qualité des nouvelles publications et des mises à jour.

À ce jour, le CEN et l'ETSI ont publié un bon nombre de spécifications techniques reconnues au-delà des frontières européennes pour faciliter la mise en œuvre d'infrastructures et de services. Le chapitre suivant dresse l'inventaire des principaux documents relatifs aux services de certification.

L'expérience acquise au cours des premières réalisations techniques a permis d'évaluer la qualité des spécifications et de mettre en évidence leurs points faibles. Ces informations ont ensuite été exploitées lors des travaux de révision des standards.

L'ETSI a notamment publié le document intitulé ETSI TS 101 456 *Policy requirements for certification authorities issuing qualified certificates.* Accompagnant la Directive Européenne sur la signature électronique, ce document décrit les exigences de sécurité applicables aux autorités de certification souhaitant générer des certificats qualifiés. Cette spécification technique a déjà été révisée en avril 2002 et des travaux supplémentaires de révision sont en cours depuis 2003. Ils devraient être finalisés par l'ETSI avant la fin 2004.

Pour faciliter le processus de reconnaissance des fournisseurs de services de certification, le gouvernement hollandais a mis sur pied un projet qui a entraîné la publication de lignes directrices relatives à la spécification ETSI TS 101 456 (*TTP.NL Guidance on ETSI TS 101 456*). Ce document auquel plusieurs sociétés privées ont participé à l'instar de KPN, KPMG ou PricewaterhouseCoopers, complète la publication de l'ETSI et prévient tout problème d'interprétation.

Conscient de l'utilité d'un tel document, l'ETSI a entrepris l'élaboration d'un guide qui reprend le contenu du document *TTP.NL Guidance on ETSI TS 101 456* hollandais pour faciliter l'évaluation de la conformité.

À plusieurs reprises, la spécification technique ETSI TS 101 456 et le guide *TTP.NL Guidance on ETSI TS 101 456* font référence au standard ISO 17799 *Information technology – Code of pratice for Information security management* afin de préciser les exigences auxquelles les fournisseurs de services de certification devraient se soumettre.

2.1.3.3 Publications de l'EESSI

Pour favoriser la mise en œuvre de la directive, l'ETSI et le CEN ont notamment publié la série de documents suivants :

- TS 101 456 *Policy Requirements for CAs issuing Qualified Certificates*
- TS 101 733 *Electronic Signature Formats*

- TS 101 903 *XML Advanced Electronic Signatures (XAdES)*
- TS 101 861 *Time Stamping Profile*
- TS 101 862 *Qualified Certificate Profile*
- CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures*
- CWA 14167-2 *Cryptographic Module for CSP Signing Operations -Protection*
- *Profile (MCSO-PP)*
- CWA 14169 *Secure Signature-Creation Devices Version EAL4+*

2.2 Comparaison et identification des différences

Après cet inventaire des acteurs du domaine de la standardisation et des publications, ces dernières ont été comparées aux PTA de 2001. Les conclusions de cette comparaison ont contribuées à l'élaboration des nouvelles PTA en permettant de déterminer quelles exigences sont nécessaires.

2.3 La référence à des standards

Afin de favoriser l'interopérabilité et l'harmonisation internationale, il a été nécessaire de vérifier dans quelle mesure les nouvelles PTA pourraient référencer des standards reconnus et utilisés.

Le bien-fondé de la référence à des standards est confirmé par les constatations d'une étude mandatée par la Commission européenne (*The Legal and Market Aspects of Electronic Signatures* de l' « Interdisciplinary Centre for Law & Information Technology » et l'université de Leuven, Belgique) qui mentionne :

> *(page 6)*
> *Qualified electronic signatures need to be in compliance with the requirements as stated by the first three annexes of the Directive. It is, therefore, important that the annexes are correctly transposed into national legislation. … The only risk is related to interoperability problems which might occur if technical implementations of annex I diverge by, for example, not using TS 101862, or other common format for encoding the requirements of annex I. The Commission should therefore promote the use of interoperability standards for the technical implementations of annex I.*
>
> *(pages 6 et 7)*
> *For the implementation of annex II, implementation levels are sometimes quite varying, meaning that the establishment and running of a CSP will differ considerably. Any organization wishing to establish a CSP business in several countries must therefore adapt itself to different requirements and procedures. Product vendors will also have difficulties building products for this very fragmented market. In addition, several countries put additional detailed and unnecessary requirements on the CSP, thus creating barriers for the establishment of a CSP.*
>
> *(page 10)*
> *Since EESSI already has published a number of valuable documents in this area it is recommended that supervisory authorities be encourage to make use of these specifications.*
>
> *(page 13)*
> *The Commission and Member States must ensure that all member States*

correctly implement presumption of conformity with standards referenced in the Official Journal.

(page 119)
In order to achieve interoperability, standards are required.

Ce point de vue est par ailleurs partagé par l' « International Chamber of Commerce » qui mentionne dans « *ICC comments on the 2003 review of the E-Signatures Directive (1999/93/EC*) » du 26.9.2003 :

To remedy the existing divergence in Member States' transpositions of the Directive and to increase the uptake in use of electronic signatures in the EU, ICC recommends that the Commission:
[…]
Press Member States to refrain from imposing additional requirements on ordinary electronic signatures beyond the Directive's definition of electronic signature;
[…]

Le souhait de référencer des standards reconnus et plus particulièrement des standards européens a du reste été évoqué lors des différentes consultations.

2.4 Pourquoi référencer les spécifications de l'EESSI ?

Tout comme la loi (art. 1, SCSE) et l'ordonnance sur les services de certification dans le domaine de la signature électronique, les dispositions d'exécution visent à assurer la disponibilité et l'utilisation d'une large offre en matière de services de certification ainsi qu'à encourager la reconnaissance des fournisseurs de services étrangers et de leurs prestations. Pour atteindre ces objectifs, l'harmonisation internationale et l'interopérabilité constituent des critères importants lors de l'élaboration des prescriptions techniques et administratives. Dès lors, il ne fait aucun doute que le recours à des standards reconnus et utilisés dans le cadre de législations similaires permet de réaliser ces critères.

L'inventaire des standards globalement reconnus met en évidence les documents de l'EESSI. Leur reprise dans le droit national en application de l'art. 20 SCSE paraît également offerte. La reconnaissance de ces documents est du reste confirmée puisque les Pays-Bas et le Luxembourg les utilisent d'ores et déjà pour la reconnaissance des fournisseurs de services de certification. Par ailleurs, en reprenant la terminologie (art. 2, SCSE) voire certains passages (art. 6 SCSE), la SCSE souligne la volonté du législateur de se rapprocher du contexte législatif européen.

La compétence des experts impliqués lors des travaux d'élaboration, l'étroite collaboration entretenue avec d'autres organismes de standardisation et les processus sérieux mis en œuvre pour l'élaboration et la révision des publications sont autant d'atouts qui illustrent la qualité de ces dernières.

D'autre part, le fait que les travaux l'EESSI aient aboutis à un recueil étoffé de documents fort utiles à la reconnaissance des fournisseurs de services de certification constitue un avantage supplémentaire plaidant en faveur de la référence aux standards de l'EESSI.

2.5 Définition du contenu

En conséquence, la nouvelle version des prescriptions techniques et administratives se réfère largement aux spécifications édictées au niveau européen (EESSI).

La comparaison des standards met en évidence qu'un nombre conséquent d'exigences qui figurent dans les PTA de 2001 n'apparaissent pas dans les différents standards internationaux.

Au cours de l'élaboration des nouvelles PTA, il a été nécessaire de qualifier l'utilité de ces exigences supplémentaires en gardant à l'esprit que des écarts trop importants entre les diverses dispositions nationales risquent de porter préjudice à l'interopérabilité et à l'harmonisation internationale.

2.6 Participants à l'élaboration

L'expérience et les compétences des différents acteurs du marché ont été prises en considération pour assurer la qualité dans l'élaboration des prescriptions techniques et administratives. Les principaux fournisseurs de services de certification (Keyon, SwissCert, Swisssign, Wisekey), l'organisme de reconnaissance (KPMG), l'organisme d'accréditation (SAS) ainsi que l'OFIT en tant qu'exploitant d'une infrastructure à clé publique conséquente ont effet collaborer à cette élaboration.

L'OFCOM a également requis l'assistance d'un expert reconnu au niveau international et ayant participé depuis l'origine aux travaux de l'EESSI. Très proche du marché et de la pratique puisqu'il est employé par la société Bull en tant que consultant en matière de sécurité, Monsieur Denis Pinkas a participé directement à la rédaction de plusieurs documents de l'EESSI et de l'IETF (Internet Engineering Task Force). Sa compétence est également utilisée dans le cadre de certains travaux à l'ISO de même que pour les travaux de révision de la législation française dans le domaine des services de certification.

Le processus d'élaboration prévoit en outre une consultation dite « publique » au cours de laquelle divers milieux directement ou potentiellement concernés ont la possibilité de se prononcer sur les travaux effectués avant la publication de la version finale.

3 Explications relatives à l'élaboration des nouvelles prescriptions techniques et administratives

Pour faciliter la comparaison, la structure des nouvelles PTA correspond à celle des standards internationaux du point de vue de l'organisation des chapitres.

La structure actuelle du document doit faciliter la recherche d'exigences particulières, les comparaisons, les mises à jour et l'inscription de nouvelles exigences. Elle pourra être remaniée en fonction des propositions qui seront émises au cours des diverses consultations.

3.1 Chapitre 2, Principe de la reconnaissance des CSP

Le service d'accréditation suisse (SAS) gère et publie sur sont site Internet la liste des organismes de reconnaissance accrédités.

Le SAS est également responsable de la tenue et de la publication des informations relatives à la liste des fournisseurs de services de certification reconnus. Il indique à cet effet sur son site Internet l'emplacement et le format électronique utilisé pour ces données afin de permettre leur consultation par des logiciels.

3.2 Chapitre 1.1, Champs d'application

Les prescriptions techniques et administratives se fondent sur la loi fédérale et l'ordonnance du conseil fédéral sur les services de certification dans le domaine de la signature électronique. Elles ne sont, en conséquence, que valables pour le type de certificat prévu par la loi.

Tout fournisseur de service de certification qui propose d'autres types de certificat a la liberté de se faire reconnaître conformément à une norme internationale de son choix sans toutefois pouvoir prétendre à la reconnaissance de sa signature électronique dans les relations de droit privé.

3.3 Chapitre 1.2, Références

La référence à des normes internationales est statique. Cela signifie que seules les versions de documents mentionnées au chapitre 1.2 sont à prendre en considération.

La publication d'une version ultérieure implique une analyse de l'OFCOM et le cas échéant, une réadaptation des prescriptions techniques et administratives. Cette dernière pourrait toutefois intervenir dans un court délai puisqu'elle est de la seule responsabilité de l'OFCOM.

Une autre question est de savoir dans quelle mesure la prise en compte d'une nouvelle version ou d'une nouvelle norme touche les fournisseurs de service de certification reconnus sur la base de l'ancienne référence. Il incombe dans ce cas à l'OFCOM de régler cette modification dans des dispositions transitoires et de prévoir un délai d'adaptation.

3.4 Chapitre 3.1, Principe

Le chapitre 3 fait largement référence à la spécification ETSI TS 101 456. Ce document est actuellement en cours de révision et devrait être finalisé au cours de cette année. Toutefois, l'incertitude quant à l'ampleur des modifications et à la date de la publication de la nouvelle version ne permet pas encore de référencer ces changements pour l'entrée en vigueur des prescriptions techniques et administratives.

Le document *TTP.NL Guidance on ETSI TS 101 456* cité au chapitre 3.1 des PTA est censé fournir des informations complémentaires au lecteur de la spécification ETSI TS 101 456 dans le but de supprimer tout problème d'interprétation. Au cours des travaux de révision de la spécification ETSI TS 101 456, il est également prévu d'élaborer une version ETSI de ce document. L'adaptation de cette référence dans les PTA dépend donc, dans ce cas également, de l'évolution des travaux de l'ETSI.

3.5 Chapitre 3.4.1, Format des certificats

Afin d'assurer l'interopérabilité et plus particulièrement de permettre l'analyse du certificat par les logiciels, ce chapitre reprend le contenu de la spécification ETSI 101 862 à l'exception des particularités imposées par la SCSE. Celle-ci exige en effet que le certificat contienne la signature électronique qualifiée du fournisseur de services de certification alors qu'une signature électronique avancée est jugée suffisante dans le contexte européen. Elle se distingue également en imposant la mention du caractère reconnu ou non du fournisseur et, s'il est reconnu, le nom de l'organisme de reconnaissance

Ce chapitre fait référence aux nouvelles versions des normes RFC dont certaines ont été révisées au début de l'année 2004.

La première colonne du tableau figurant au chapitre 3.4.3.1 des PTA reprend les exigences de l'art. 7 SCSE. Les deux autres colonnes décrivent les moyens à mettre en œuvre pour définir le contenu du certificat conformément aux exigences imposées par la loi.

La mention du caractère reconnu ou non du fournisseur et, s'il est reconnu, le nom de l'organisme de reconnaissance sont des informations qui sont communiquées en faisant figurer les noms du SAS, de l'organisme de reconnaissance et du fournisseur de services de certification dans l'extension « issuerAltName » du certificat. La présence de ces informations ne constitue malheureusement pas une garantie de la reconnaissance du fournisseur de services de certification. Pour confirmation, il convient de consulter le site Internet du SAS sur lequel figure la liste des fournisseurs reconnus.

La mention qu'il s'agit d'un certificat qualifié et l'indication relative à la valeur des transactions sont des informations fournies sous la forme d'une déclaration. Le certificat contient en réalité un identifiant de déclaration (Object identifier-OID) défini dans le document ETSI TS 101 862 Qualified Certificate Profile.

Les déclarations mentionnées sont basées délibérément sur la Directive 1999/93/EC du Parlement Européen et du Conseil sur un cadre communautaire pour les signatures électroniques alors que cette dernière n'est pas contraignante pour la Suisse. La définition de nouveaux OID pour des déclarations nationales aurait certes été possible. En pratique, de telles informations génériques risqueraient cependant de ne pas être interprétées par les logiciels.

OFCOM/1.6.04