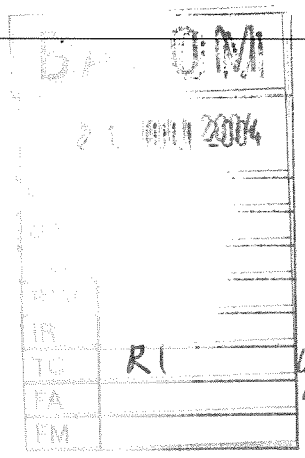
République
et canton
de Genève

LE CHANCELIER D'ETAT



Chancellerie d'Etat
Rue de l'Hôtel-de-Ville 2
Case postale 3964
1211 Genève 3

N/réf. : RH/DW

Monsieur Peter FISCHER
Directeur suppléant
Office fédéral de la communication
Rue de l'Avenir 44
Case Postale 1003
2501 Bienne

Genève, le 16 juillet 2004

Concerne : Ordonnance sur les services de certification dans le domaine de la signature électronique et prescriptions techniques et administratives

Monsieur le Directeur suppléant,

En date du 1er juin 2004 vous avez consulté la Chancellerie d'Etat de la République et canton de Genève sur une ordonnance relative aux services de certification dans le domaine de la signature électronique et prescriptions techniques et administratives et nous vous en remercions.

Je vous prie de bien vouloir trouver ci-dessous la position de notre République et canton, laquelle a inscrit, dans sa stratégie, la mise en place, étape par étape, d'un concept de cyberadministration. Ce déploiement s'appuie sur une décision politique forte et sur une participation de tous les secteurs de l'administration.

Un ensemble de projets Pilotes, comme le vote par Internet, renforce la démarche pragmatique que notre Canton entend mener pour mettre en place, dans le cadre de la cyberadministration, de nouvelles prestations pour le citoyen.

Cette nouvelle approche nous amène naturellement à intégrer le concept de "Nomadisation" avec les nouvelles techniques de certification électronique pour répondre aux relations que ce nouveau mode de fonctionnement induit vis-à-vis du citoyen, des autres administrations, des communautés d'intérêt et de l'environnement en général.

Au cœur de celle-ci, nous trouvons le principe de l'identification qui selon les demandes, peut être forte, non-duplifiable ou permettant juste l'accès libre à certaines informations.

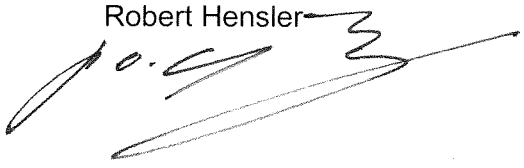
Cette identification doit être accompagnée des concepts d'authentification et d'identification, en tenant compte de la protection des données, de la sécurité et de l'éthique.

Pour ces différentes raisons, nous sommes solidaires de la démarche permettant d'utiliser la signature électronique, qui bien sûr, doit définir les moyens juridiques et technologiques nécessaires pour obtenir un déploiement efficace.

Vous trouverez en annexe les commentaires relatifs au texte même de l'ordonnance sur les services de certification dans le domaine de la signature électronique et prescriptions techniques et administratives.

Veuillez agréer, Monsieur le Directeur suppléant, l'expression de ma considération distinguée.

Robert Hensler



Annexe: Commentaires relatifs à l'Ordonnance sur la signature électronique (OSCSE)

Copie: Monsieur Jean-Marie LECLERC, Directeur général du CTI

A/ Ordonnance sur la signature électronique (OSCSE)

De manière générale, aucune considération commerciale n'est mentionnée ; il n'est par exemple pas précisé quelles seraient les prestations de base offertes, ou quelles seraient les prestations complémentaires qui seraient proposées moyennant supplément financier. Il nous semble utile de préciser cet aspect.

Considérants : Il aurait également dû être fait référence à l'article 19, al. 1 et 2 SCSE.

Article 1 al. 2 : Conformément à ce que préconisent les explications jointes au projet d'ordonnance, il faudra effectivement prévoir de confier la tâche de reconnaissance des fournisseurs de services d'accréditation à une autre entité que le SAS; l'OFCOM par exemple, en cas d'absence d'organisme de reconnaissance accrédité.

Article 3 al. 1 : Cette disposition repose sur des notions juridiques indéterminées ("clef de longueur suffisante", "algorithme capable de résister à des attaques cryptographiques") appliquées à une durée de vie du certificat qualifié ("durant toute la durée de vie du certificat"), alors qu'il n'est pas fixé de durée de vie maximum pour de tels documents. Cela aboutit à une solution peu crédible sur le plan technique, nul n'étant capable de certifier qu'une clef tiendra indéfiniment contre des attaques, le marché de la sécurité évoluant constamment et restant tributaire de la puissance des machines, elle-même en constante évolution.

C'est l'occasion de souligner que personne ne semble à l'heure actuelle en mesure de garantir que les clés pourront effectivement résister à des attaques cryptographiques (voir remarques ad art. 7 al. 1 let. e SCSE).

Il faudrait par conséquent limiter la durée de vie des certificats à trois an au plus, ou renoncer à exiger des clefs attribuées qu'elles résistent à des attaques, ce qui présenterait d'autres dangers, en matière de responsabilité notamment. Le plus simple reste donc de conférer une durée de validité limitée à ces certificats.

Une autre solution pourrait également consister à établir une tabelle de référence sécurité de type « Best Practice » mettant en relation la longueur de clé, l'algorithme choisi et la durée de validité du certificat.

Article 8 al. 2 : Bien que le texte actuel reprenne à la lettre la formulation de l'ancien article 13 OSCert, il conviendrait de profiter de l'élaboration du nouveau texte pour décomposer explicitement le délai de 11 ans qui s'y trouve mentionné, le document actuel ne permettant pas de comprendre qu'il repose sur la prescription décennale de l'article 127 CO ou sur le délai minimum de conservation des livres stipulé par l'article 962 CO joint à la précision apportée par l'article 962 al. 3 CO. Il conviendrait de le décomposer expressément.

Article 9 : Voir remarques ci-dessus à propos de l'article 8 al. 2.

Article 12 al. 1 : Un code à quatre positions alphanumériques semble insuffisant, vu l'importance des dommages possibles en cas de violation et considérant le fait qu'il n'est pas fait référence à un nombre limité de tentatives avant blocage.

Un code à huit positions serait préférable. Il est rappelé que la protection des transactions bancaires par cartes de crédit au moyen d'un code reste couplé à une limitation des sommes qu'il est possible de retirer par jour sur le compte ou de l'importance des transactions qu'il est possible d'effectuer par mois, ce qui limite considérablement la portée des dommages encourus. Tel n'est pas le cas en matière de signature électronique, laquelle peut être apposée sur un contrat vital pour une société.

Article 12 al. 2 : Le code ne doit pas davantage se référer à des entrées connues comme celles du dictionnaire.

Article 12 al. 5 : Si la notion de "lieu sûr" au sens de l'article 11 n'a pas besoin d'être définie de manière trop précise afin de maintenir une certaine souplesse, il convient de préciser ce que l'on entend par "lieux séparés". Il doit s'agir de deux lieux dont les accès sont garantis par des protections différentes (deux pièces fermées à clef par exemple, les serrures étant commandées par des clefs différentes).

Article 13 : De manière générale, le projet n'indique pas qui supporte la responsabilité des dommages subis entre la perte effective de la clef et la demande de son annulation par le titulaire, voire entre la perte de la clef et son annulation effective. Il conviendrait de le préciser.

Article 13 al. 1 : La disposition ne précise pas par quel biais le titulaire peut demander l'annulation de son certificat. Un simple courriel suffit-il ?

Article 13 al. 3 : La formulation reste ambiguë, en raison du terme "prolongé". Il serait préférable de prévoir que le délai ne commence à courir qu'à partir du moment où cette impossibilité prend fin.

B/ Prescriptions techniques et administratives (PTA)

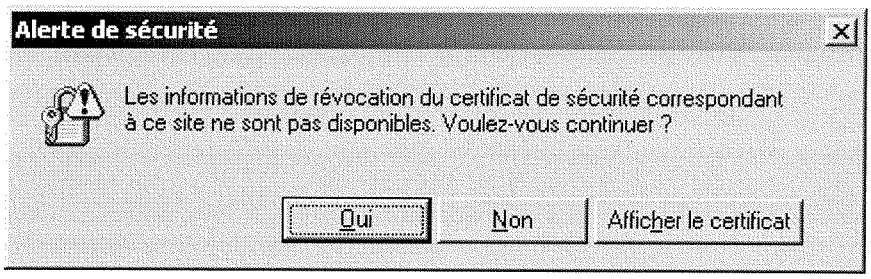
De manière générale, il n'est pas aisé d'étudier les PTA avec des références à des documents techniques complémentaires non fournis, voire parfois payants sur Internet. Une compilation des chapitres cités ou des liens précis seraient les bienvenus.

3.4.7 Publication de l'état des certificats et des listes de certificats révoqués

Seules les CRL sont citées, aux dépends d'une autre technologie très pratique comme l'OCSP (Online Certificate Status Protocol), qui présente l'avantage de contrôler la validité du seul certificat objet de la recherche, évitant ainsi de devoir télécharger la liste de tous les certificats révoqués avant d'avoir à contrôler dans un second temps s'il se trouve dans cette dernière. Les précédentes PTA du 15.8.01 de l'OSCert permettaient en leur point 2.12.6 ("Exigence 7") d'utiliser ce protocole (voir RFC 2560).

Cet avantage est indéniable pour les personnes privées et peut être illustré au travers de l'exemple suivant portant sur un certificat SSL :

Lorsqu'un citoyen accède depuis son domicile à un site dit sécurisé (commençant par https) avec les paramètres sécurité correspondants activés (contrôle de la validité et des révocations des certificats), il risque fort d'obtenir le message d'erreur suivant :



Cette alerte se déclenche du fait que le navigateur n'arrive pas à charger les CRL vérifiant la chaîne de validation du certificat du site sécurisé auquel il tente de se connecter, avant le "timeout". Les CRL peuvent atteindre une taille de plus de 750k, et leur transfert peut dépasser les tolérances de temps de chargement, même avec une ligne ADSL 600k !

En conclusion, il serait préférable de maintenir cette possibilité technique. Dans ce cas, le point 3.4.3.1 "Champs des certificats ", devra être modifié en conséquence.

3.4.5 Annulation du certificat, point a)

La suspension provisoire du certificat pour une durée maximale de 3 jours, admise par l'ordonnance actuelle, ne semble malheureusement plus possible en application de la loi.

Il pourrait s'ensuivre une incohérence, la loi excluant cette possibilité alors que les PTA se réfèrent à des spécifications techniques (à savoir "ETSI TS 101 456 [6] "), qui, elles, au chapitre 7.3.6, intitulé "Certificate revocation and suspension", traitent la suspension comme une annulation, mais provisoire.

Si la suspension n'est effectivement plus offerte, il serait plus clair de le rappeler dans les PTA sans se référer au message du Conseil fédéral.

C/ Loi sur la signature électronique (SCSE)

Article 6 : Des notions juridiques indéterminées ("élevé", "pratiquement", "suffisant", "sûre"), sont sujettes à caution et à de futurs débats d'experts, voir de futures jurisprudences

Article 7 al. 1 let. e : La lettre "e" ne mentionne pas de durée limite de validité du certificat. Or la technologie évolue et rien ne nous garantit qu'à l'avenir le nouvel état de la science ne nous permette pas de casser les clés actuelles.

Article 10 : Annulation des certificats qualifiés : le terme « immédiatement » est utilisé deux fois sans être réellement défini. Doit-on suivre la recommandation et appliquer le délai de un jour entre la prise en compte et la diffusion ? Il conviendrait alors de remplacer "immédiatement" par "dans les 24 heures ". Dans tous les cas, le responsable des éventuels préjudices survenus entre l'annonce de la perte et sa publication n'est pas précisé (voir remarques ad article 13 OSCSE).

Le fournisseur devrait de plus expliciter en termes simples et clairs la procédure applicable, les horaires de réception des avis de perte et les éventuels coûts d'annonce.

Article 12 : Système d'horodatage. Cet article qui permettra de légaliser toute transaction effectuée par Internet semble peu développé par rapport aux perspectives envisageables à terme.

* * *