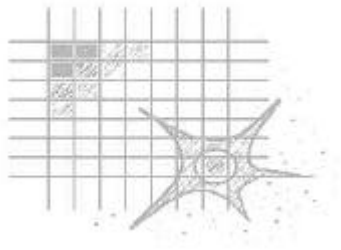
Avis n° 2 de la Commission Télématique

"Normes en matière de Télématique au service du Secteur des Soins de Santé"

Groupe de travail 'Sécurité'

Approuvé lors de l'assemblée plénière du 10/10/2000



Signature Digitale et Certificats Electroniques dans le secteur des Soins de Santé

Les objectifs généraux du groupe de travail sont les suivants : p
romouvoir des standards pour des mesures techniques destinées à protéger et à accroître la confidentialité, l'intégrité et la disponibilité des informations relatives à la santé ; promouvoir la responsabilité des utilisateurs dans ce domaine et donner des lignes de conduite pour la politique de sécurité dans l'ensemble des soins de santé.
Le premier thème abordé par le groupe de travail est l'utilisation de la signature digitale (ou numérique) et des certificats électroniques dans le domaine des soins de santé.

Ce document a pour objectif de résumer les conclusions principales formulées par le groupe de travail, qui s'est réuni les 21.01.2000, 18.02.2000, 21.03.2000, 21.04.2000, 17.05.2000, 23.06.2000 et 29.09.2000.

Les membres du groupe de travail sont G. De Moor (président), L. Corbeel (vice-président), F. De Meyer (membre externe, secrétaire), M. Bangels, M. Bossens, B. Macq, P. Piette, Y. Poullet, F. Robben, F. Roger-France, R. Van de Velde, B. Van den Bosch, E. Van Hove, L. Baert (membre externe), J.-J. Quisquater, (membre externe), D. Simon (membre externe) et S. Waterbley (membre externe).

Les invités du groupe de travail étaient F. Allaert, (invité le 21.01.2000), J.-P. Dercq (invité le 21.03.2000 et le 17.05.2000), J.-M. Dinant (invité le 21.03.2000), S. Jacobs (invitée le 21.03.2000), L. Baert (invité le 17.05.2000 >nouveau membre), S. Lacroix (invitée le 23.06.2000) et S. Waterbley (invitée le 23.06.2000 > nouveau membre).

Recommandations relatives à la signature digitale et aux certificats électroniques dans le secteur des soins de santé

Le groupe de travail souhaite éviter de formuler des recommandations qui limitent les choix techniques ou qui contraignent l'implémentation.

1.1. Signature Digitale et Certificats Electroniques

1.1.1. Les techniques et les procédures de la signature digitale[1] offrent plus de garantie et d'avantages *(p.ex. en termes d'intégrité et d'authentification)* que les signatures manuscrites. C'est pourquoi les signatures digitales méritent d'être reconnues comme des signatures valides et leur usage - lorsqu'il est approprié - devrait être encouragé dans le secteur des soins de santé.

1.1.2. Il est essentiel de pouvoir disposer de services fiables d'enregistrement et de certification[2] si l'on veut atteindre dans le domaine de la communication électronique les niveaux élevés de confiance, de sécurité et de qualité exigés par le secteur des soins de santé.

1.1.3. Afin d'obtenir la "meilleure pratique" (best practice), il est recommandé de se conformer aux lois internationales, aux normes reconnues de standardisation et aux accords applicables à de tels services *(cf. la Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, publiée au Journal Officiel des Communautés européennes, 19.01.2000)*. Une liaison sera également établie avec la Commission Nationale mixte "relative aux obstacles à la Société de l'information".

1.1.4. Il convient d'établir une distinction entre les certificats d'identité et les certificats d'attributs. La vérification de l'identité et des attributs peut être effectuée par plusieurs autorités chargées de l'enregistrement. Plusieurs certificats peuvent être associés à une paire de clés. Le titulaire de certificats devrait être capable d'utiliser chaque certificat séparément[3].

---

[1] Le groupe de travail Sécurité a établi une distinction entre les signatures électronique et digitale. Le terme "signature électronique" est utilisé dans le contexte de "validité légale ou force de preuve" quelle que soit la technique utilisée pour réaliser une signature électronique (p.ex. un crayon électronique). Par "signature digitale (ou numérique)", le groupe de travail désigne l'utilisation de la technique de "hashing" et de chiffrement asymétrique.

[2] L'autorité chargée de l'enregistrement vérifie l'identité du candidat qui demande un certificat. L'autorité de certification délivre les certificats. La certification peut être directe ('on line') ou en mode différé ('off line'). Des exemples des différents types de certificats sont : les certificats d'identité, les certificats de qualification, les certificats de "rôle au sein d'une organisation", les certificats de mandats (délégation) et pour les personnes morales : les certificats "de relations".

[3] Tout un chacun (les professionnels de la santé y compris) devrait, s'il le souhaite, avoir la possibilité de faire une sélection des certificats utilisés dans une circonstances particulière (sans devoir présenter les autres certificats de qualification inutiles ou inappropriés dans le contexte).

1.1.5. Selon la loi belge, l'Ordre des Médecins (par l'intermédiaire des Conseils provinciaux) et l'Ordre des Pharmaciens sont les autorités responsables de l'inscription et de la révocation des médecins et des pharmaciens. En Belgique, on devrait s'accorder sur le choix de la ou des organisation(s) qui tiendrai(en)t à jour un annuaire complet des données d'identification appropriées relatives aux professionnels des soins de santé[4], permettant, par exemple, de garantir leur identité et leurs qualifications professionnelles[5]. Le ministère des Affaires sociales et de la Santé publique pourrait lancer une telle initiative en partenariat avec les autres organismes appropriés (p.ex. l'Ordre des Médecins et son Conseil National, le Conseil de Pharmaciens, …) et en coopération avec l'INAMI. Une telle plateforme pourrait faire office d'autorité nationale d'enregistrement des qualifications professionnelles et d'interface avec les prestataires de services de certification *(p.ex. des compagnies privées agissant comme "organisme tiers de confiance" : OTC – "trusted third party" : TTP)*.

1.1.6. Un cadre devrait définir les rôles, les droits, les responsabilités et les obligations des différents acteurs impliqués dans l'implémentation de services de signatures digitales.

1.1.7. Dans les domaines d'utilisation de la signature digitale, les flux d'informations et les scenarios de communication relatifs aux soins de santé (identifiant les types et les finalités des messages, les types d'expéditeurs et de destinataires[6], les besoins de certification d'identité et les besoins de certification d'attribut) devraient être identifiés.

1.1.8. Une paire de clés utilisée pour une signature digitale ne devrait jamais être employée à d'autres fins (par exemple pour encrypter).

1.1.9. Les pièces de preuve d'identité devraient être conservées aussi près que possible de la personne en tant que telle. Les clés privées utilisées pour des signatures digitales peuvent être stockées sur des cartes à puce, considérées comme sûres.

1.1.10. Les droits d'accès aux ressources devraient être conservés à proximité du système correspondant et gérés par l'organisation responsable de la décision et/ou de l'implémentation de l'accès.

1.1.11. Il faudrait promouvoir la multifonctionnalité des certificats ; p.ex. il devrait être possible d'avoir plusieurs certificats d'attributs liés à un seul certificat d'identité.

---

[4] Par professionnels des soins de santé, il faut entendre non seulement les médecins (généralistes ou spécialistes) mais également tous les autres acteurs des soins de santé tels que le personnel infirmier, les pharmaciens, les dentistes, les logopèdes, les diététiciens, … et le personnel administratif des soins de santé.

[5] Une personne physique peut avoir plusieurs qualifications (correspondant à des certificats d'attributs) octroyées par différentes organisations ou institutions (certificats délivrés par les autorités de certification correspondantes).

[6] Les partenaires de communication peuvent être soit des personnes physiques, soit des personnes morales de droit privé ou public voire même des machines (p.ex. des serveurs).

1.1.12. Si les différentes qualifications d'une personne pouvaient entraîner un conflit d'intérêt[7]-[8], c'est à cette dernière qu'il revient d'utiliser le(s) certificat(s) d'attribut(s) adéquat(s) (l'inclusion d'un certificat devrait être un acte "conscient" : il ne s'agit pas, en l'occurrence, d'un problème technique). En corollaire, les applications devraient suivre des procédures de dialogue avec l'utilisateur pour, lorsque cela est nécessaire, attirer son attention sur le contexte de signature et lui demander de sélectionner les certificats adéquats.

1.1.13. Les certificats d'attributs peuvent –dans certaines circonstances- être utilisés sans certificat d'identité ou avec des pseudonymes.

1.1.14. Les certificats ne devraient jamais être délivrés à l'insu de la personne concernée. Les vérifications doivent être possibles. Cette personne devrait être informée.

1.2. Services de confiance

1.2.1 Le secteur des soins de santé nécessite absolument le recours aux services "d'organismes tiers de confiance" : OTC ("trusted third parties" : TTP). Le rôle de tels prestataires peut être très diversifié vu qu'ils peuvent offrir des services dans divers domaines ayant trait à la sécurité tels que le soutien à l'infrastructure de clé publique : ICP ("public key infrastructure" : PKI) (gestion des clés, personnalisation et distribution de la carte à puce, services d'annuaires, etc.), les services d'anonymisation et de pseudonymisation (techniques visant à garantir le respect de la vie privée, "privacy enhancing techniques" : PET) et les services de notarisation *(p.ex. l'apposition de une heure et d'une date, preuve de livraison)*.

1.2.2 Les priorités en matière "d'organismes tiers de confiance" : OTC ("trusted third parties" : TTP) dans le secteur des soins de santé sont les services d'infrastructure de clé publique ICP (PKI) (pour permettre l'implémentation des techniques de signature digitale) et les services d'anonymisation et de pseudonymisation (pour permettre la production de données anonymisées à des fins, par exemple, de recherche médicale et de gestion administrative).

1.2.3 Par conséquent, il faudrait élaborer des lignes de conduite pour le recours à des organismes tiers de confiance dans le secteur des soins de santé.

[7] P.ex. un conseiller clinicien et/ou médical d'une compagnie d'assurance et/ou un médecin et/ou un inspecteur du travail.

[8] Un membre du groupe de travail pense qu'en cas de conflit d'intérêts (qualifications antagonistes) et dans l'intérêt des patients, deux certificats d'identité offrent une meilleure garantie qu'un seul certificat d'identité avec deux ou plusieurs certificats d'attributs. Cette idée est en contradiction avec ce que pensent les autres membres du groupe de travail.

Références bibliographiques

1. Belgisch Staatsblad – 17.03.2000 – Moniteur belge. Ministerie van Ambtenarenzaken – N2000 – 688 [C-2000/02025]. 12 maart 2000 – Koninklijk Besluit tot oprichting van een Nationale Gemengde Commissie

2. F. De Meyer, F. Allaert, G. De Moor, T. Fiers. Arguments en faveur de la reconnaissance de la valeur juridique de la signature électronique. Informatique et Santé, 1996 (8) : 23-25 – Springer-Verlag France

3. G. De Moor, F. De Meyer. Beveiligingsaspecten met betrekking tot de elektronische medische gegevens. Tijdschrift voor geneeskunde – Volume 53 – Nummer 5 – 1 maart 1997

4. Y. Poullet, R.J. Barcelo. Working document based on the article 'Health telematics Network Reflections on Legislative and Contractual Models Providing Security Solutions'. Centre de Recherches Informatiques et Droit (CRID), University of Namur

5. P. Van Eecke. Bewijsrecht en digitale handtekeningen : nieuwe perspectieven. To be published in 'Belgische Vereniging van Bedrijfsjuristen', 1999

6. Digital Certificates. GlobalSign NV-Apr-99

7. Synthèse des décisions prises lors des réunions CARENET tenues les 1er, 15 juillet et 4 août 1999 concernant la certification des messages, en présence des représentants de l'INAMI, de la BCSS, du Ministère de la Santé publique et des organismes assureurs. Bruxelles, le 17 août 1999

8. Working Group '11-19' on Security Standards (www.11-19.org/security.html)

9. Projet de loi n°322 relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques. La Chambre. 27/01/2000.
   Wetsontwerp nr 322 betreffende de werking van de certificatiedienstverleners met het oog op het gebruik van elektronische handtekeningen. De Kamer. 27/01/2000.

Annexes

1. Electronic signatures and certificates in health care. F. De Meyer, 10.10.2000.

2. Electronic signature and certification models in health care. F. De Meyer, G.J.E. De Moor, 13.9.2000.

...