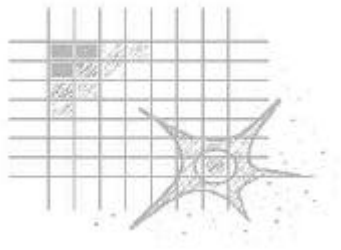
**Advies nr 2 van de Telematica Commissie**

"Standaarden inzake telematica ten behoeve van de sector van de gezondheidszorg"

**Werkgroep 'Veiligheid'**

Goedgekeurd tijdens de vergadering van de Plenaire Commissie dd. 10/10/2000



# Digitale Handtekening en Elektronische Certificaten in de Gezondheidszorg

De werkgroep heeft de volgende algemene doelstellingen : het bevorderen van standaarden voor technische maatregelen om de betrouwbaarheid, de integriteit en de beschikbaarheid van de gezondheidsinformatie en ook de aansprakelijkheid van gebruikers te beschermen en te verhogen, alsmede het geven van richtlijnen voor het veiligheidsbeleid in de gezondheidszorg. Het eerste onderwerp dat de werkgroep bestudeert, is het gebruik van digitale handtekening en elektronische certificaten in de gezondheidszorg.

Dit document beoogt een samenvatting te geven van de voornaamste conclusies van de werkgroep die op 21.1.2000, 28.2.2000, 21.3.2000, 21.4.2000, 17.5.2000, 23.6.2000 en 29.9.2000 is samengekomen.

De leden van de werkgroep zijn G. De Moor (voorzitter), L. Corbeel (ondervoorzitter), F. De Meyer (extern lid, secretaris), 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 (extern lid), J-J. Quisquater (extern lid), D. Simon (extern lid) en S. Waterbley (extern lid).

De genodigden van de werkgroep waren F. Allaert (uitgenodigd op 21.1.2000), J-P. Dercq (uitgenodigd op 21.3.2000 en 17.5.2000), J-M. Dinant (uitgenodigd op 21.3.2000), S. Jacobs (uitgenodigd op 21.3.2000), L. Baert (uitgenodigd op 17.5.200 > nieuw lid), S. Lacroix (uitgenodigd op 23.6.2000) en S. Waterbley (uitgenodigd op 23.6.2000 > nieuw lid)

## Aanbevelingen betreffende de digitale handtekening en de elektronische certificaten in de gezondheidszorg

### 1.1. Digitale handtekening en elektronische certificaten

1.1.1. De technieken en de procedures betreffende de digitale handtekening[1] bieden meer garanties en voordelen (bijvoorbeeld in termen van integriteit en authentificatie) dan handgeschreven handtekeningen. Digitale handtekeningen verdienen daarom als geldige handtekeningen erkend te zijn en het gebruik ervan zou - indien het aangewezen is- aangemoedigd moeten worden binnen de sector van de gezondheidszorg.

1.1.2. Het leveren van registratie-en certificatiediensten[2] is een essentiële vereiste om, op het vlak van elektronische communicatie, de door de gezondheidssector vereiste niveaus van vertrouwen, veiligheid en kwaliteit te bereiken.

1.1.3. Om te komen tot 'the best practice', is het aanbevolen zich te schikken naar internationale wetten, gestandaardiseerde regels en overeenkomsten die op dergelijke diensten van toepassing zijn (cf. Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, gepubliceerd in het Publicatieblad van de Europese Gemeenschappen, 19.1.2000). Er zal ook worden samengewerkt met de gemengde nationale commissie 'Informatiemaatschappij voor de overheidssector'.

1.1.4. Er moet een onderscheid worden gemaakt tussen identiteitscertificaten en attribuutcertificaten. De beoordeling van de identiteit en van de attributen kan gebeuren door verschillende registratie-instanties. Verschillende certificaten kunnen onder een sleutelpaar[3] worden gegroepeerd.

---

[1] De werkgroep Veiligheid heeft een onderscheid gemaakt tussen een elektronische handtekening en een digitale handtekening. De term 'Elektronische Handtekening'wordt gebruikt in de context van 'wettelijke geldigheid of bewijskracht' ongeacht de techniek die gebruikt wordt om een elektronische handtekening te verkrijgen (bijvoorbeeld een 'smartpen'). Met 'Digitale handtekening' bedoelt de werkgroep de techniek die gebruik maakt van 'hashing' en asymmetrische cryptografie.

[2] De registratie-autoriteit controleert de persoonsgegevens van de aanvrager vooraleer een certificaat wordt verleend. De certificatie-autoriteit verleent de certificaten. De certificatie kan on-line of off-line gebeuren.Voorbeelden van de verschillende types van certificaten zijn : identiteitscertificaten, attribuut-certificaten, certificaat 'rol in een organisatie', mandaatcertificaat, voor rechtspersonen : relatiecertificaten.

[3] Elkeen (met inbegrip van bijvoorbeeld gezondheidswerkers) zou de mogelijkheid moeten hebben om de certificaten selectief te gebruiken als hij/zij dat wil in bepaalde omstandigheden (zonder de verplichting om andere attribuutcertificaten te tonen die in dat geval niet relevant zijn).

1.1.5. Overeenkomstig de Belgische wet zijn de Orde van Geneesheren (via haar Provinciale Raden) en de Orde van Apothekers de verantwoordelijke autoriteiten voor de registratie en de revocatie van artsen en apothekers. In België zou men het eens moet worden over de keuze van de organisatie(s) belast met het bijhouden van een volledige directory met nauwkeurige identificatiegegevens van gezondheidswerkers[4] om bijvoorbeeld hun identiteit en beroepsbekwaamheden[5] te beoordelen. Het Ministerie van Volksgezondheid en Sociale Zaken kan samen met andere relevante organisaties (bv. Orde van Geneesheren/Nationale Medische Raad/Raad van Apothekers,…) en in samenwerking met de derde betaler (RIZIV-INAMI) een dergelijk initiatief nemen. Zo'n platform zou kunnen dienen als nationale registratie-autoriteit voor de beroepsbekwaamheden en als interface met certificatiedienstverleners (bv. privé-bedrijven die handelen als vertrouwde derde partij (Trusted Third Party= TTP)).

1.1.6. Een kader zou de rollen, de rechten, de verantwoordelijkheden en de verplichtingen moeten definiëren van de verschillende actoren die betrouwbare diensten betrokken bij de implementatie van de digitale handtekening (cf. probleem van de aansprakelijkheid).

1.1.7. In de domeinen waar digitale handtekeningen gebruikt zullen worden, zouden de belangrijkste gezondheidsinformatiestromen en communicatiescenario's (met type en doel van de boodschap, type zender en ontvanger[6], identiteitscertificatie en attribuutcertificatie) geïdentificeerd moeten worden.

1.1.8. Een sleutelpaar dat voor digitale ondertekening wordt gebruikt, mag nooit voor andere doeleinden (bv encryptie) worden aangewend.

1.1.9. Identiteitsbewijzen moet zo dicht mogelijk bij de persoon als dusdanig bewaard worden. De privé-sleutels voor digitale handtekeningen kunnen bewaard worden op chipkaarten die als veilig worden beschouwd.

1.1.10. Toegangsrechten tot middelen moeten dicht bij het systeem bewaard blijven en beheerd worden door de organisatie die verantwoordelijk is voor de beslissing en/of de implementatie van de toegang.

1.1.11. Multifunctionaliteit moet worden bevorderd ; bv. het zou mogelijk moeten zijn om over verschillende attribuutcertificaten te beschikken die aan één identiteit gekoppeld zijn.

---

[4] Met gezondheidswerkers bedoelt men niet alleen artsen (huisartsen of specialisten) maar ook alle andere actoren van de gezondheidszorg zoals verpleegkundigen, apothekers, tandartsen, logopedisten, diëtisten,…en het administratieve personeel van de gezondheidssector.

[5] Een natuurlijke persoon kan verschillende bekwaamheden hebben (die overeenkomen met attribuutcertificaten) die door verschillende organisaties en instellingen worden verleend (afgeleverd door certificatie-autoriteiten).

[6] De communicatiepartners kunnen ofwel natuurlijke personen ofwel privaat-of publiekrechtelijke personen zijn, of zelfs machines (bv. servers).

1.1.12. Het er een belangenconflict[7] [8] zou ontstaan door de verschillende kwalificaties van een persoon valt het onder diens verantwoordelijkheid het (de) correcte attribuutcertifica(a)t(en) te gebruiken (de invoeging van een certificaat moet een 'bewuste' handeling zijn : het is een niet-technisch probleem). Niettegenstaande moeten de gebruikersapplicaties procedures volgen waarbij - waar dit aangewezen is – de gebruiker wordt gewaarschuwd, gevraagd en aangespoord om 'geëigende' certificaten te gebruiken.

1.1.13. Attribuutcertificaten kunnen - onder bepaalde voorwaarden - gebruikt worden zonder identiteitscertificaat of met pseudoniemen.

1.1.14. Certificaten mogen nooit zonder iemands medeweten worden afgegeven. De persoon moet worden geïnformeerd.

## 1.2. Vertrouwde diensten (Trust services).

1.2.1. In de gezondheidssector is er een zeer grote behoefte aan diensten van Thrusted Third Parties (TTP). De rol van dergelijke vertrouwde dienstverleners kan zeer uiteenlopend zijn vermits zij diensten kunnen verlenen in verschillende veiligheidsdomeinen zoals ondersteuning m.b.t. de 'Public Key Infrastructure (PKI)' (sleutelbeheer, personalisatie en verspeiding van de chipkaart, directorydiensten,…), anonimiserings- en pseudonimiseringsdiensten ('Privacy Enhancing Techniques, PET' : technische middelen die de privacy op de elektronische snelweg kunnen beschermen) en notarisdiensten (bv. tijd-en datumstempel, leveringsbewijs).

1.2.2. De prioriteiten de gezondheidssector zijn de PKI-diensten (om de digitale handtekeningen in de gezondheidszorg te kunnen toepassen) alsook de anonimiserings- en peudonimiseringsdiensten via de TTP (om het coderen van gegevens voor bv. medisch onderzoek en beheersdoeleinden mogelijk te maken).

1.2.3. Er dienen dan ook algemene richtlijnen voor dergelijke TTP-diensten in de gezondheidssector te worden opgesteld.

[7] Bv. klinisch en/of medisch adviseur van een verzekeringsmaatschappij en/of arbeidsgeneesheer en/of inspecteur.

[8] Een lid van de werkgroep meent nog steeds dat in het geval van een belangenconflict (tegenstrijdige bekwaamheden) en in het belang van de patiënten, twee identiteitscertificaten meer garanties bieden dan één identiteitscertificaat met een of meer attribuut-certificaten. Dit is in tegenspraak met wat de overige leden van de werkgroep denken.

## Referenties


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.


## Bijlagen

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.

...