ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

Aanbevelingen betreffende de bescherming van de vertrouwelijkheid bij de transmissie van medische persoonsgegevens via internet

Doc	a092004
Publicatiedatum	17/02/2001
Origine	NR
Thema's	Informatica Beroepsgeheim Internet

Op 22 april 1995 bracht de Nationale Raad een advies uit aangaande de veiligheidsvoorwaarden die noodzakelijk zijn bij de transmissie van identificeerbare medische persoonsgegevens langs elektronische weg (Tijdschrift Nationale Raad nr. 69, september 1995, p. 13). Na vijf jaar praktische ervaring dringen volgende bijkomende aanbevelingen zich op.

Advies van de Nationale Raad :

De arts is wettelijk en deontologisch verplicht het medisch geheim te eerbiedigen. De elektronische transmissie van medische persoonsgegevens ontkomt niet aan deze verplichting.

1. Medische gegevens gedekt door het beroepsgeheim van de arts mogen alleen door een arts, natuurlijke persoon, doorgezonden en ontvangen worden. Binnen een instelling mag een arts alleen in eigen naam medische gegevens doorzenden of ontvangen.

2. Het dubbele-sleutelsysteem, ook nog asymmetrisch mathematisch systeem genoemd, biedt voldoende veiligheid.

3. De arts kan zelf op zijn PC zijn eigen sleutels aanmaken, door middel van een software van een leverancier die los van de mail-server optreedt.

4. Om de elektronische handtekening te legaliseren, zal de openbare sleutel voor echt verklaard moeten worden door een certificatiedienstverlener die gekwalificeerde certificaten aflevert en los staat van de mail-server.

5. De toegang tot de geheime sleutel wordt onherroepelijk beperkt tot de enige eigenaar ervan.

6. Het gebruikte algoritme moet bekend zijn en een voldoende lengte bezitten, voor zijn symmetrisch zowel als voor zijn asymmetrisch gedeelte.

7. Het coderen en decoderen van de gegevens wordt respectievelijk verricht in de computer van de verzender en van de bestemmeling.

In geen geval zullen deze handelingen verricht mogen worden in een tussencomputer bestemd voor of verbonden aan de brievenbus.

Advies van de Nationale Raad van 22 april 1995, TNR nr. 69, september 1995, p. 13 :

1. De Nationale Raad heeft zich gebogen over het probleem betreffende de eerbiediging van het beroepsgeheim bij de transmissie van medisch-vertrouwelijke gegevens via een elektronische brievenbus.

Brieven en advies van de Nationale Raad aan de Provinciale Raden en aan de Raden van beroep :

In zijn vergadering van 22 april 1995, heeft de Nationale Raad de tekst aan-genomen van de aanbevelingen betreffende de bescherming van de vertrouwelijkheid bij de transmissie van medisch-vertrouwelijke gegevens via een elektronische brievenbus.

U vindt een fotocopie als bijlage.

U gelieve uw advies te willen doen kennen betreffende de praktische toepassing van de punten 5 en 6, eerste alinea.

Aanbevelingen betreffende de bescherming van de vertrouwelijkheid bij de transmissie van medisch-vertrouwelijke gegevens via een elektronische brievenbus

Krachtens artikel 458 van het Strafwetboek is de arts verplicht het medisch geheim te eerbiedigen. De elektronische transmissie van post die persoonsgegevens bevat, ontkomt niet aan deze wettelijke en deontologische verplichting.

1. Medisch-vertrouwelijke gegevens mogen alleen doorgezonden worden door een arts, natuurlijke persoon.
Binnen een instelling mag een arts alleen in eigen naam medische gegevens doorzenden of ontvangen.

2. Het dubbele-sleutelsysteem, ook nog asymetrisch mathematisch systeem genoemd, biedt voldoende veiligheid.

3. Teneinde het geheim karakter ervan te bewaren dient de arts zelf de hem eigen sleutels aan te maken op zijn PC. Tijdens deze handeling mag deze computer niet aangesloten zijn op het netwerk.

4. De toegang tot de geheime sleutel is strikt voorbehouden aan de eigenaar ervan. Deze toegang moet beveiligd worden door een paswoord, dat niet medegedeeld mag worden.

5. De arts dient een kopie van de geheime sleutel op diskette toe te vertrouwen aan de Raad van de Orde onder wiens bevoegdheid hij valt. De toegang tot deze diskette moet beveiligd worden door een paswoord of paszin, die afzonderlijk in een verzegelde omslag wordt bewaard.

6. De publieke sleutel mag samen met een door de Raad van de Orde ondertekende "fingerprint" ervan medegedeeld worden aan een vennootschap die instaat voor de bestelling van elektronische post.
Deze vennootschap dient zich ertoe te verbinden deze publieke sleutel enkel door te geven aan artsen die meewerken aan de uitwisseling van medisch-vertrouwelijke gegevens. Zij moet alle maatregelen treffen om te verhinderen dat deze sleutel voor andere doeleinden wordt gebruikt.

7. Deze publieke sleutels worden het best bewaard en naar de gebruikers doorgezonden via een server die verschillend is van deze die gebruikt wordt voor de transmissie van gegevens. De numerieke "fingerprint" van de publieke sleutel, die toelaat de authenticiteit ervan te controleren, moet bewaard en doorgezonden worden

door een betrouwbare autoriteit.

8. De codering en de decodering van de gegevens vinden respectievelijk plaats in de PC van de afzender en van de bestemmeling. Deze procedures mogen in geen geval via een tussencomputer verlopen (BBS, hostcomputer of netwerkserver).

2. Een provinciale raad verzoekt de Nationale Raad om advies aangaande een "Reglement tot het gebruik van een elektronisch communicatiesysteem via een centraal postbussysteem", dat hem voorgelegd werd door de vennootschap X in oprichting.

Advies van de Nationale Raad :

In antwoord op uw brief van 14 december 1994 met betrekking tot het elektronisch communicatiesysteem X dat door Dr. Y aan uw Raad werd voorgelegd, delen wij u mede dat de Nationale Raad bijzonder belang hecht aan het probleem betreffende de veiligheid van de transmissie van medische documenten die onder het medisch geheim vallen. Over dit onderwerp werden reeds verschillende adviezen verstrekt (zie Officieel Tijdschrift van de Nationale Raad van maart 1994, nr. 63, p. 20-23, en Officieel Tijdschrift van de Nationale Raad van september 1994, nr. 65, p. 22-24). Bijgaand vindt u kopie van deze adviezen. De Nationale Raad werkt momenteel een aantal aanbevelingen uit betreffende de elektronische uitwisseling van medisch-vertrouwelijke gegevens tussen artsen.

In verband met het door X beoogde systeem dienen de volgende opmerkingen geformuleerd te worden :

- ofschoon de elektronische-mailsystemen "open" dienen te zijn, m.a.w. toegankelijk voor alle gebruikers, moet het systeem voorbehouden worden aan de artsen, natuurlijke personen, met uitsluiting van alle associaties en vennootschappen, die overigens geen handtekening kunnen plaatsen. Deze maatregel is in het bijzonder gericht op de bescherming van het beroepsgeheim binnen de verzorgingsinstellingen.

- wij herinneren eraan dat elke overeenkomst tussen X en iedere gebruiker goedgekeurd moet worden door uw Raad.

- de gebruikte standaarden worden zeer algemeen beschreven. De volgende gegevens zijn onontbeerlijk om de veiligheid van de voorgestelde systemen te kunnen beoordelen :

- beschrijving en identificatie van het gebruikte coderingsalgoritme

- identificatie van de cryptografische software

- identificatie van de gebruikte communicatiesoftware.

In verband met de manipulatie van de vertrouwelijke gegevens dient rekening gehouden te worden met de volgende opmerkingen :

Authenticiteit

- aanmaak van de dubbele publieke/geheime sleutel. De sleutel mag niet aangemaakt worden in het bijzijn van een afgevaardigde van X. Er mag geen enkel risico genomen worden op dit vlak; de geheime sleutel is strikt persoonlijk en mag niet gedeeld worden. X dient bijgevolg alle inlichtingen te verstrekken die de gebruiker nodig heeft om de sleutel te kunnen aanmaken op zijn PC.

- mag de geheime sleutel noch kennen noch bewaren. Om elke onbeschikbaarheid van de eigenaar van de geheime sleutel te ondervangen, is het aan te bevelen een kopie

van de geheime sleutel en van het paswoord op diskette toe te vertrouwen aan de Provinciale Raad.

- het paswoord of de paszin die toegang geeft tot de beveiligingskopie is het best verschillend van het dagelijks gebruikte paswoord.

- alleen de publieke sleutel mag medegedeeld worden aan X. Deze laatste dient zich ertoe te verbinden deze sleutel alleen mede te delen aan de medische gebruikers van haar netwerk. X moet voorts van al diegenen aan wie deze "sleutelbos" toevertrouwd wordt, de verbintenis krijgen dat zij de sleutels uitsluitend zullen gebruiken voor de transmissie tussen artsen van gegevens die onder het beroepsgeheim van de geneesheer vallen.

Een 'fingerprint' van deze publieke sleutel biedt diegene die post zendt naar de eigenaar van de sleutel de mogelijkheid een controle uit te oefenen op de authenticiteit ervan. De afzender moet deze 'fingerprint' dus ontvangen hebben via post die hem gezonden wordt door de eigenaar of via een betrouwbare persoon of autoriteit.

- X dient bijkomende informatie te verstrekken met betrekking tot de drager waarop de geheime sleutel bewaard wordt door de eigenaar : betreft het een magneetkaart of een chipkaart of gaat het over een gelokaliseerde sleutel op de disk van de gebruiker ? In het laatste geval bestaat er een reëel gevaar dat de veiligheid teloorgaat, aangezien de sleutel alleen nog beveiligd is door het paswoord.

- men moet tevens voorbereid zijn op een transmissie van de geheime sleutel via het netwerk door onachtzaamheid van de eigenaar. Er moeten garanties geboden worden dat een dergelijke handeling uitgesloten is.

Vertrouwelijkheid

- codering en decodering : geen opmerking.

- de rol van X dient nader bepaald te worden. X zou zich vooral tot taak moeten stellen de artsen-gebruikers op te leiden inzake het gebruik van de elektronische briefwisseling en de toepassing van de veiligheidsmaatregelen.
X mag niet aanwezig zijn bij de aanmaak van de sleutels, aangezien dit meer onveiligheid dan oplossingen voor de problemen met zich zou brengen. X moet voorstellen formuleren voor een adequaat beheer van de publieke sleutels. Daarnaast staat X in voor de terbeschikkingstelling van de software en van alle nodige protocollen, die in overeenstemming moeten zijn met de voorschriften van de Raad.

- central Host computer : er dient nader bepaald te worden welke werkings- en/of doubleringswaarborgen geboden worden wanneer de centrale hostcomputer defect is.

Wanneer de transmissie van de publieke sleutels via het netwerk verloopt, is het om veiligheidsredenen wenselijk dat de publieke sleutels bewaard worden op en doorgezonden worden via een verschillende server.

Betrouwbaarheid

Geen opmerking

Beschikbaarheid

Geen opmerking