Elektronische Handtekening in de Zorg

Marc de Graauw

Elektronische Handtekening

- Wettelijke aspecten
  - Geneesmiddelenwet
  - Wet op de Elektronische handtekening
- Hoe: Uitvoering
  - UZI pas, andere smartcard
  - Proces
- Wat te ondertekenen?
  - Alleen gegevens uit voorschrift?
  - WYSIWYS (What You See Is What You Sign)
- Overig

Wetten

Voorschrijven

- IGZ: Gebruik Elektronisch Voorschrijfsysteem wordt verplicht
- Op papier: handtekening verplicht
- IGZ: Faxrecept (of elektronisch recept) is werkopdracht, geen vervanger receptbriefje
- Dus: ondertekend papieren recept moet volgen
- Praktijk: wordt nu gedoogd als het niet volgt
- Fraaiere oplossing: elektronisch recept + elektronische handtekening

Geneesmiddelenwet

- recept: een door een met naam en werkadres aangeduide beroepsbeoefenaar als bedoeld in artikel 36, veertiende lid, van de onder ll genoemde wet, opgesteld document waarin aan een persoon of instantie als bedoeld in artikel 61, eerste lid, een voorschrift wordt gegeven om een met zijn stofnaam of merknaam aangeduid geneesmiddel in de aangegeven hoeveelheid, sterkte en wijze van gebruik ter hand te stellen aan een te identificeren patiënt, en dat is ondertekend door de desbetreffende beroepsbeoefenaar dan wel, zonder te zijn ondertekend, met een zodanige code is beveiligd dat een daartoe bevoegde persoon of instantie de authenticiteit ervan kan vaststellen;

- Artikel 36, veertiende lid .Wet op de beroepen in de individuele gezondheidszorg.
- Artikel 61, eerste lid. Geneesmiddelenwet

Wet op de Elektronische Handtekening

1. EH is uniek verbonden aan de ondertekenaar
2. identificeert EH de ondertekenaar
3. middelen onder exclusieve controle ondertekenaar
4. wijziging achteraf is te detecteren
5. EH is gebaseerd op een gekwalificeerd certificaat (Telecomwet)
6. EH is “gezet” met een “Veilig Middel” (Telecomwet)

Wet op de Elektronische Handtekening

- Wet biedt keus tussen:
- De “gewone” elektronische handtekening, d.w.z. een handtekening waarvan door partijen onderling is overeengekomen dat die voldoende betrouwbaar is.
- Een “geavanceerde” elektronische handtekening, d.w.z. gebaseerd op PKI.
- Een “gekwalificeerde” elektronische handtekening (meest betrouwbaar niveau): een geavanceerde elektronische handtekening op basis van een Gekwalificeerd Certificaat en een Veilig Middel.

Besluit Elektronische Handtekeningen (AMvB)

- Het Veilig Middel en het stelsel voor uitgifte moeten garanderen dat de erop uitgegeven sleutels uniek zijn.
- Het moet naar de huidige stand van de techniek bestand zijn tegen afleiden van de sleutels en vervalsen van de elektronische handtekening.
- Het beschermt de sleutels tegen gebruik door anderen.
- Het laat de te ondertekenen gegevens ongewijzigd en belet niet dat die gegevens vóór de ondertekening aan de ondertekenaar worden voorgelegd.

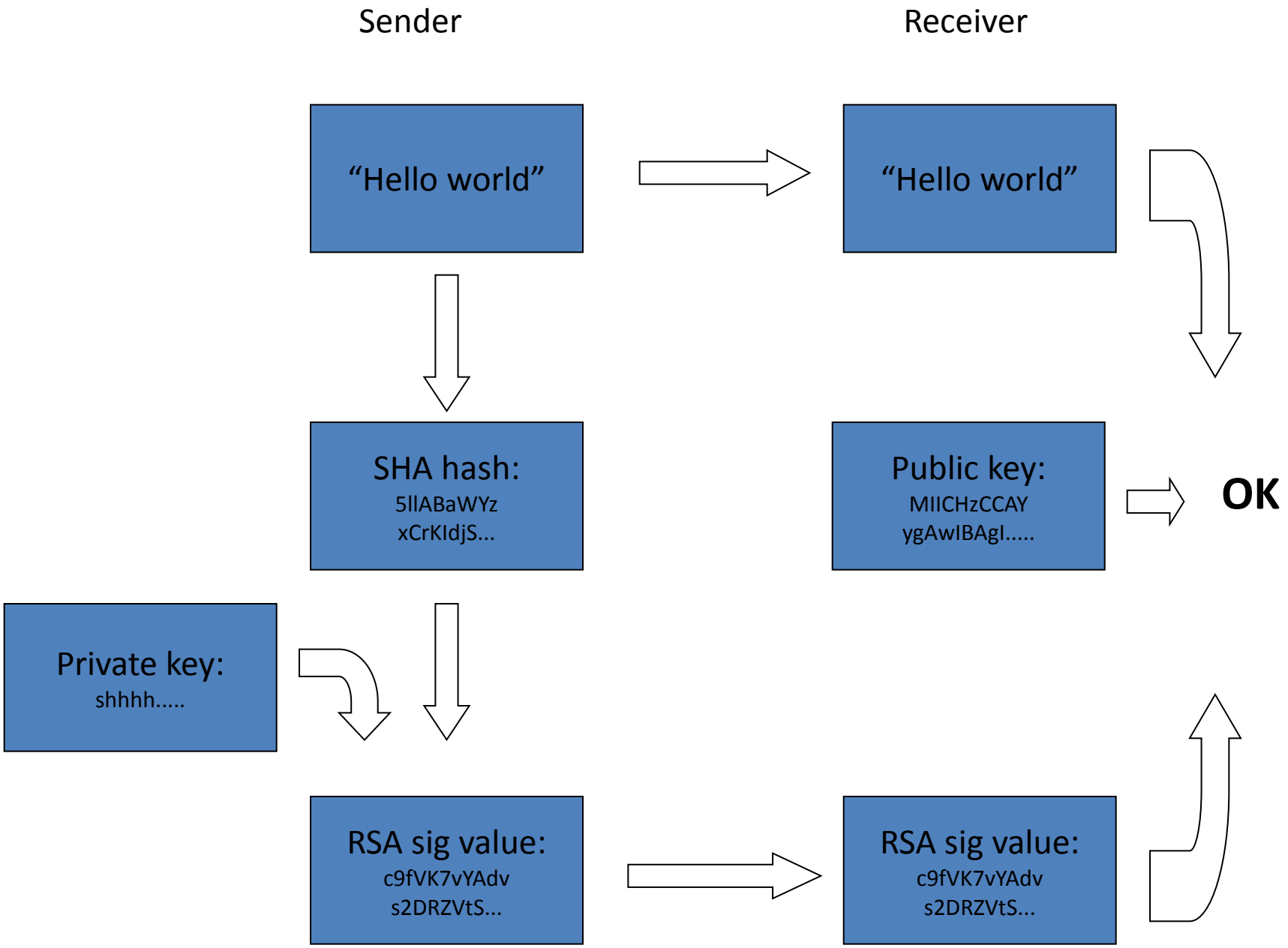
Eisen aan proces van tekenen

- Als de applicatie gedistribueerd is moet **communicatie veilig** zijn; bij ASP wederzijdse authenticatie nodig; afgeschermde omgeving.
- De te ondertekenen gegevens moeten **ondubbelzinnig kenbaar** gemaakt worden aan de ondertekenaar, voordat deze tekent (WYSIWYS).
- De te ondertekenen data moet **ondubbelzinnig duidelijk** zijn voor de ondertekenaar, zodat misinterpretatie is uitgesloten.
- De te ondertekenen data moet **statisch** zijn.
- Het **handtekeningcertificaat** moet worden geselecteerd en de gebruiker moet zich ervan **bewust** zijn welk certificaat gebruikt wordt.
- Telkens voorafgaand aan het zetten van de elektronische handtekening moet de gebruiker een **niet-triviale bewuste handeling** verrichten, bijv. (opnieuw) de **pincode** ingeven.

Hoe?

Smartcard, b.v.UZI pas

- Smartcard (zoals de UZI pas) met:
  - private/publiek sleutelpaar (RSA)
  - X.509 certificaat (met publieke sleutel)
- Bij voorkeur certificatenregister (UZI-register)
- PKI-Overheid
- Persoonlijke pas
  - veilig bewaren
  - PIN code
- Kan ook met andere smartcard


Sender
Receiver
“Hello world”
“Hello world”
SHA hash:
5llABaWYz
xCrKIdjS...
Public key:
MIICHzCCAY
ygAwIBAgI.....
OK
Private key:
shhhh.....
RSA sig value:
c9fVK7vYAdv
s2DRZVtS...
RSA sig value:
c9fVK7vYAdv
s2DRZVtS...

Wat?

Verschillen

Papier	Elektronisch
Duidelijk wat je tekent	Niemand leest bits
Lezer ‘ziet’ hetzelfde als ondertekenaar	View hangt af van software
Tekst, paar codes	Meestal veel codes, die mens niet kent
Kopie is niet exact	Kopie is wel exact
Archief: papier blijft leesbaar	Software om te lezen bewaren
Archief: handtekening blijft geldig	Cryptografie kan gekraakt worden

WYSIWYS

- What You See Is What You Sign
- een handtekening is een wilsuiting
- wilsuiting veronderstelt dat je het begrijpt

Wat onderteken je?

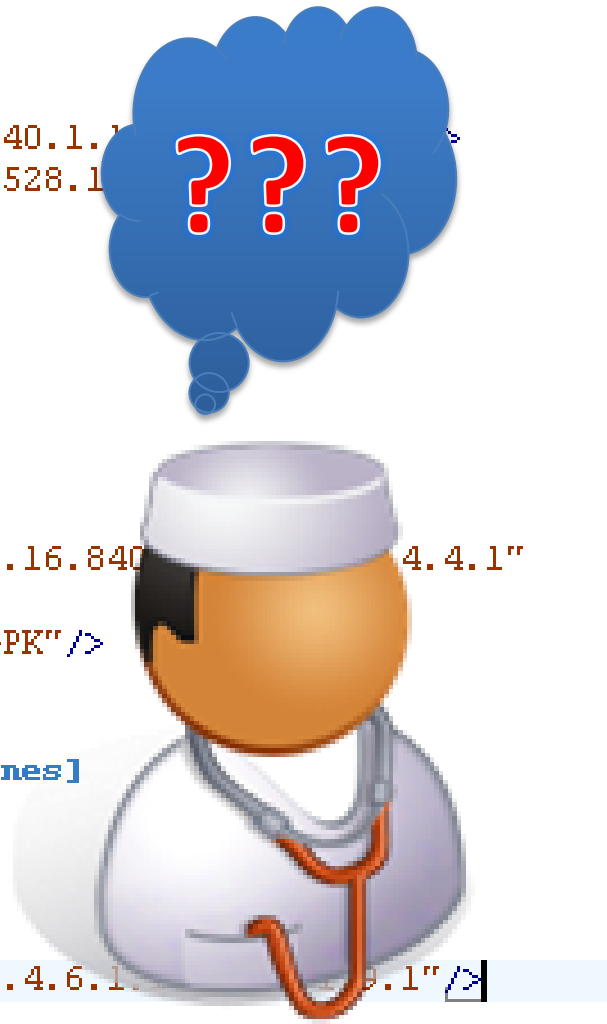
- Drie oplossingen:

1. (deel van) een HL7v3 XML bericht
2. andere machine-leesbare representatie (ander XML, HTML, CSV o.i.d.)
3. leesbare tekst b.v. een schermafdruk of scan (als bitmap of jpg)

- Drie problemen:

1. wilsuiting
2. semantiek
3. versiebeheer

```
124             <time value="200408100931"/>
125             <AssignedPerson>
126                 <id extension="01028432" root="2.16.840.1.
127                 <id extension="006797896" root="2.16.528.1
128                 <assignee>
129                     <assigneePerson> [7 lines]
137                 </assignee>
138             </AssignedPerson>
139         </author>
140         <directTarget>
141             <prescribedMedication>
142                 <MedicationKind>
143                     <code code="999999" codeSystem="2.16.840
                                                              4.4.1"
144         displayName="Propanolol hcl tablet 10mg"
145                         codeSystemName="G-Standaard GPK"/>
146                 </MedicationKind>
147                 <productOf>
148                     <medicationDispenseRequest> [4 lines]
153                 </productOf>
154                 <therapeuticAgentOf>
155                     <medicationAdministrationRequest>
156                         <id extension="0001912011"
157                             root="2.16.840.1.113883.2.4.6.1
                                                              .1"/>
```



Voorschrift 0003000201

Voorschriftnummer:	0003000201
Tijdstip voorschrift:	18-07-2010, 15:10
Patient:	J.M. Breed
Geslacht:	Man
Geboortedatum:	16-08-1968
BSN:	012345672
Voorschrift van:	Dr. Frans Rijtje, Huisarts
UZI-nummer:	012345678
Adres:	Waterstraaat 14, Nattelanden
Medicatie:	Propanolol hcl tablet 10mg
Hoeveelheid:	56
Iter:	2
Eenheden:	stuks
Dosering:	eerst 2 weken lang 2x daags 2 tabletten dan aansluiten lang 2x daags 1 tablet en 4 weken lang 1x daags 1 tablet

× Find: kuit Next Previous Highlight all Ma

Done

Tekenen en tonen

```
<medication>
    <codeSystem>2.16.840.1.113883.2.4.4.7</codeSystem>
    <code>999999</code>
    <displayName>Propanolol hcl tablet 10mg</displayName>
</medication>
<quantity>
    <iter>2</iter>
    <value>56</value>
    <unit>
        <code>1</code>
        <displayName>stuks</displayName>
    </unit>
</quantity>
```

R/	Propanolol hcl tablet 10mg
da	56 1 stuks
S.	eerst 2 weken lang 2x daags 2 tabletten da tablet en 4 weken lang 1x daags 1 tablet
	iter 2


```
<tr>
   <td valign="top"><b>R/</b></td>
   <td colspan="2">Propanolol hcl tablet 10mg</td>
</tr>
<tr>
   <td><b>da</b></td>
   <td>1 stuks</td>
</tr>
<tr>
   <td valign="top"><b>S.</b></td>
   <td colspan="2">eerst 2 weken lang 2x daags 2 tabl
</tr>
<tr>
```

Tekenen en tonen

- ondertekenaar en ontvanger moeten *het ondertekende op soortgelijke wijze in kunnen zien*
- HTML tonen is niet verplicht, soortgelijke wijze mag

Codes

- code: voor digitale communicatie
- tekst: voor menselijke communicatie
- WYSIWYS: tekst tekenen
- code: tekst halen uit lokale database
- maar: is code -> tekst bij huisarts gelijk aan code -> tekst apotheker
- dus: code én tekst tekenen
- dus: tekst uit het ondertekende deel tonen

Recept

- Receptnummer
  - uniek
  - OID niet tonen, alleen nummer
  - datum: tonen en leesbaar opmaken

```
<prescription>
    <id>
        <root>2.16.840.1.113883.2.4.6.1.1028432.1.9</root>
        <extension>0000191201</extension>
    </id>
    <dateTime>20100718151043</dateTime>
    <patient>...</patient>
    <author>...</author>
    <medication>...</medication>
    <quantity>...</quantity>
    <usage>...</usage>
</prescription>
```

Patientgegevens

- BSN tonen, OID niet
- BSN moet matchen met bericht
- Naam:
  - als enkele string
  - niet matchen
- Geslacht (M of Man etc.), geboortedatum

```
<patient>
    <id>
        <root>2.16.840.1.113883.2.4.6.3</root>
        <extension>012345672</extension>
    </id>
    <name>J.M. Breed</name>
    <gender>Man</gender>
    <birthdate>19680816</birthdate>
</patient>
```

Voorschrijvende arts

- Id: UZI nummer tonen, OID niet
  - = prescription.author
  - = subject.serialNumber certificaat
- Rolcode (tekst tonen), naam, adres

```
<author>
    <id>
        <root>2.16.528.1.1007.3.1</root>
        <extension>006797896</extension>
    </id>
    <rolcode>
        <codeSystem>2.16.840.1.113883.2.4.15.111</codeSystem>
        <code>01.015</code>
        <displayName>Huisarts</displayName>
    </rolcode>
    <name>Dr. Frans Rijtje</name>
    <address>Waterstraaat 14, Nattelanden</address>
</author>
```

Medicatie

- Code, alleen tekst tonen

```
<medication>
    <codeSystem>2.16.840.1.113883.2.4.4.7</codeSystem>
    <code>999999</code>
    <displayName>Acetylcyteine pch poeder skvr 600mg in sachet</displayName>
</medication>
```

- Magistrale receptuur: alleen tekst

```
<medication>
    <desc>Hier staat een beschrijving van de magistrale receptuur.</desc>
</medication>
```

Hoeveelheid

- Iter alleen vullen bij herhalingen
- Units volgens UCUM, als in HL7
- display: 1 == ‘stuks’
- anders: milliliter, microgram

```
<quantity>
    <iter>2</iter>
    <value>56</value>
    <unit>
        <code>1</code>
        <displayName>stuks</displayName>
    </unit>
</quantity>
```

Gebruiksomschrijving

- alleen als text opnemen

```
    <usage>eerst 2 weken lang 2x daags 2 tabletten dan aansluitend 2 weken lang 2x
daags 1 tablet en 4 weken lang 1x daags 1 tablet</usage>
```

Overige punten

- Techniek
  - SOAP
  - HL7v3 XML
  - WS-Security headers
- Tekenen zonder LSP?
  - techniek staat los van Aorta of LSP
  - tekenen van ieder willekeurig stuk XML (of HTML)
- Archivering
  - techniek kan gekraakt worden
  - goed documenteren, procedures
  - heel zwaar: Trusted Third Parties
- Diginotar
- Vragen