Authentication & Digital Signature

an overview

Marc de Graauw
marc@marcdegraauw.com

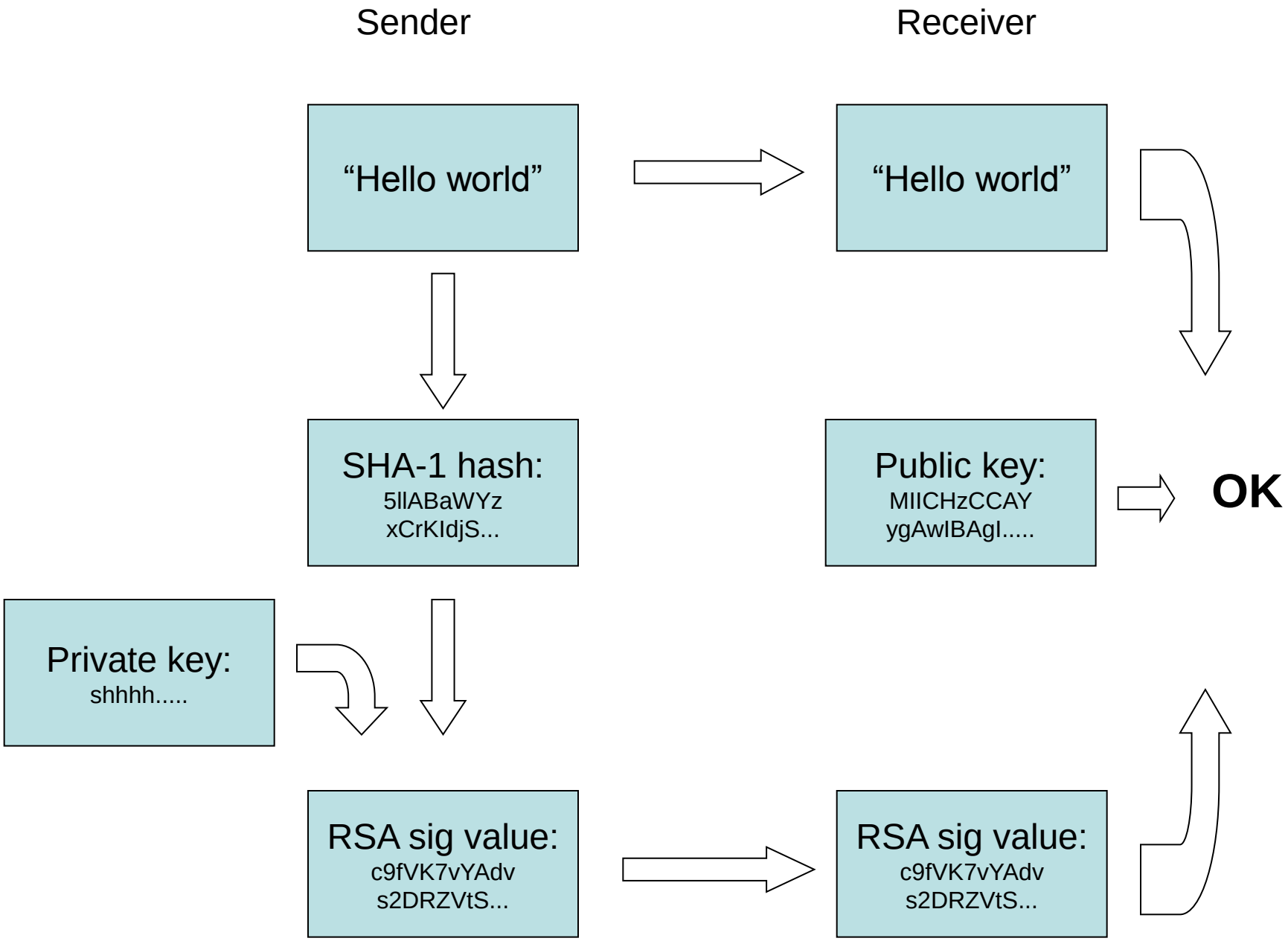
Authentication

Marc de Graauw
marc@marcdegraauw.com

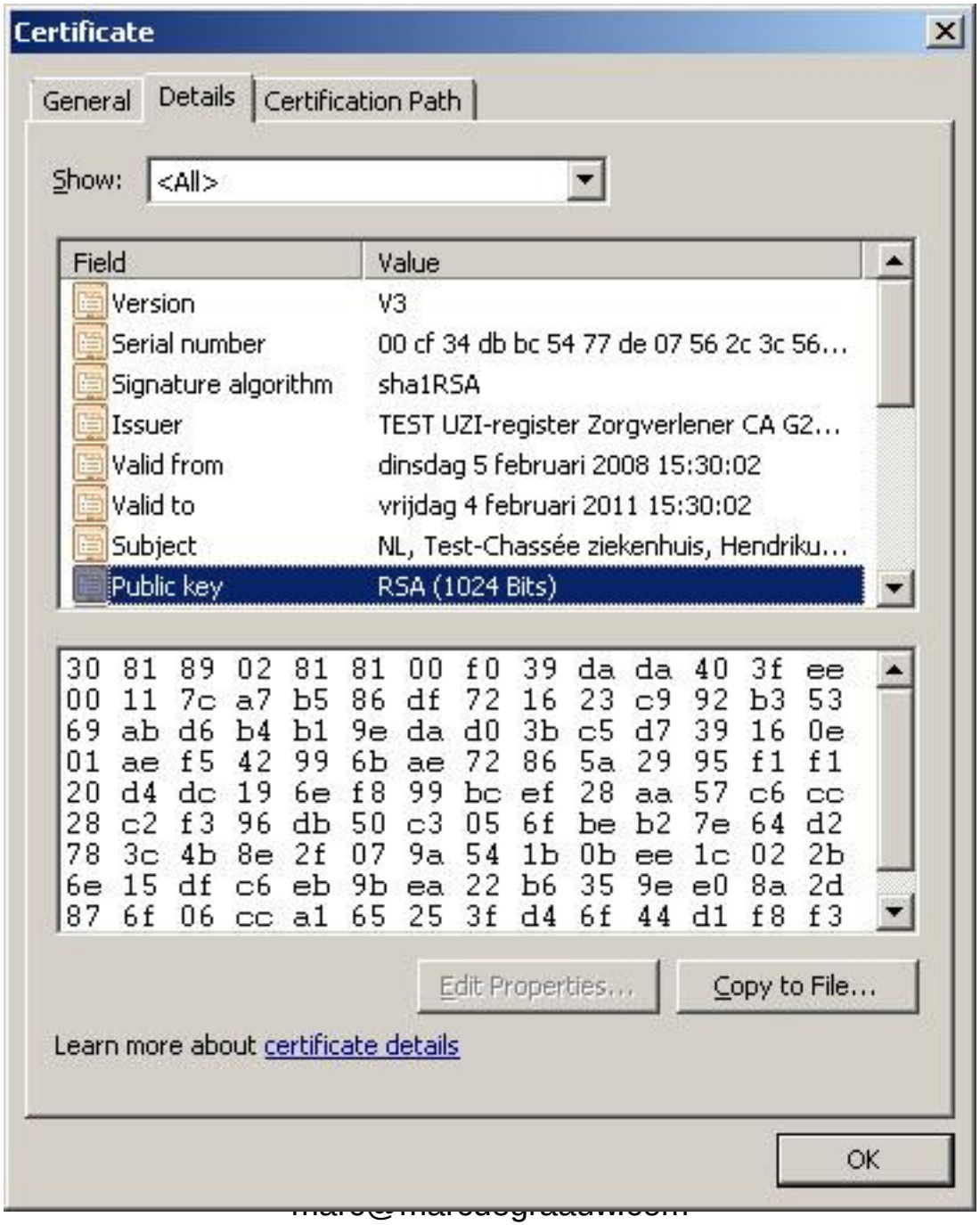
Authentication

- Smartcard (UZI pass) with:
  - private key (RSA)
  - X.509 certificate (includes public key)
- PKI-Government
- Personal pass
  - guard safely
  - no sharing
  - PIN protected

Marc de Graauw
marc@marcdegraauw.com



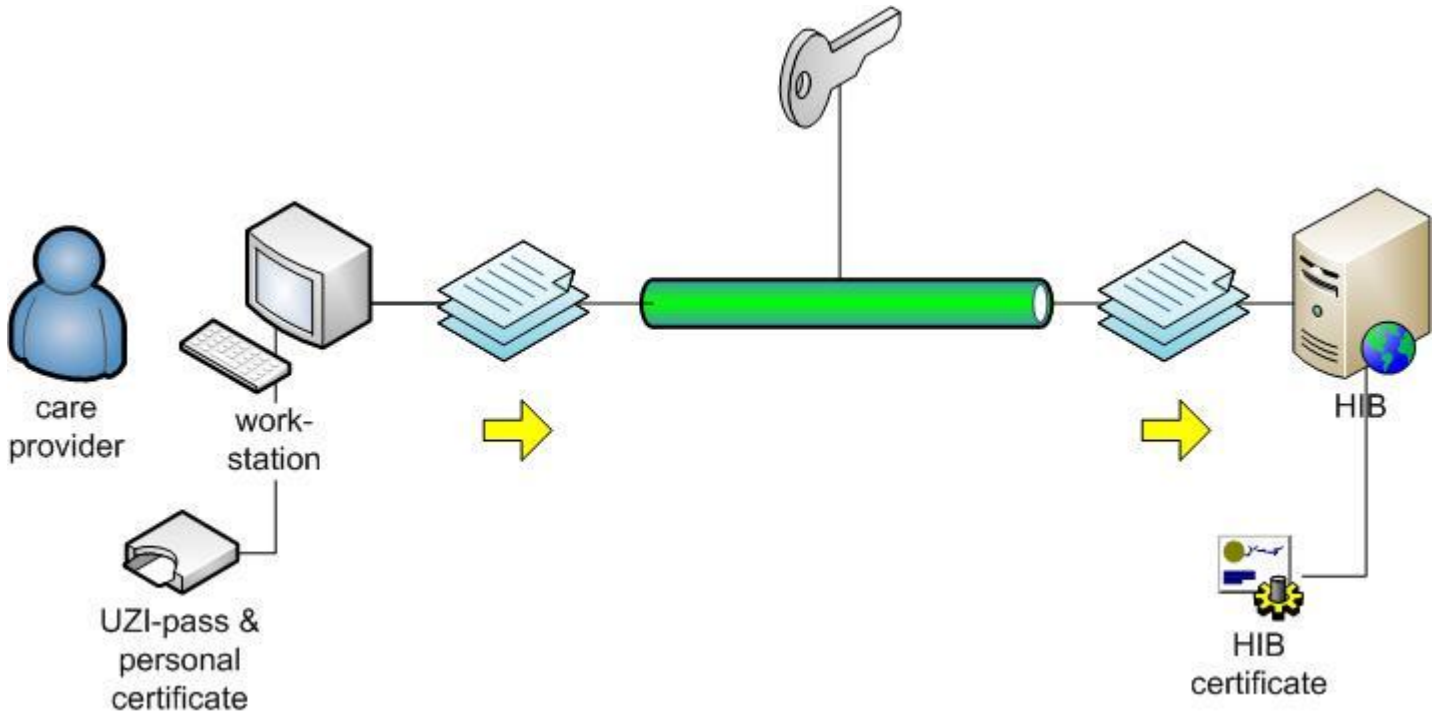
Marc de Graauw
marc@marcdegraauw.com


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
00 cf 34 db bc 54 77 de 07 56 2c 3c 56...
Signature algorithm
sha1RSA
Issuer
TEST UZI-register Zorgverlener CA G2...
Valid from
dinsdag 5 februari 2008 15:30:02
Valid to
vrijdag 4 februari 2011 15:30:02
Subject
NL, Test-Chassée ziekenhuis, Hendriku...
Public key
RSA (1024 Bits)
30 81 89 02 81 81 00 f0 39 da da 40 3f ee
00 11 7c a7 b5 86 df 72 16 23 c9 92 b3 53
69 ab d6 b4 b1 9e da d0 3b c5 d7 39 16 0e
01 ae f5 42 99 6b ae 72 86 5a 29 95 f1 f1
20 d4 dc 19 6e f8 99 bc ef 28 aa 57 c6 cc
28 c2 f3 96 db 50 c3 05 6f be b2 7e 64 d2
78 3c 4b 8e 2f 07 9a 54 1b 0b ee 1c 02 2b
6e 15 df c6 eb 9b ea 22 b6 35 9e e0 8a 2d
87 6f 06 cc a1 65 25 3f d4 6f 44 d1 f8 f3
Edit Properties...
Copy to File...
Learn more about certificate details
OK

Security Services (X.800)

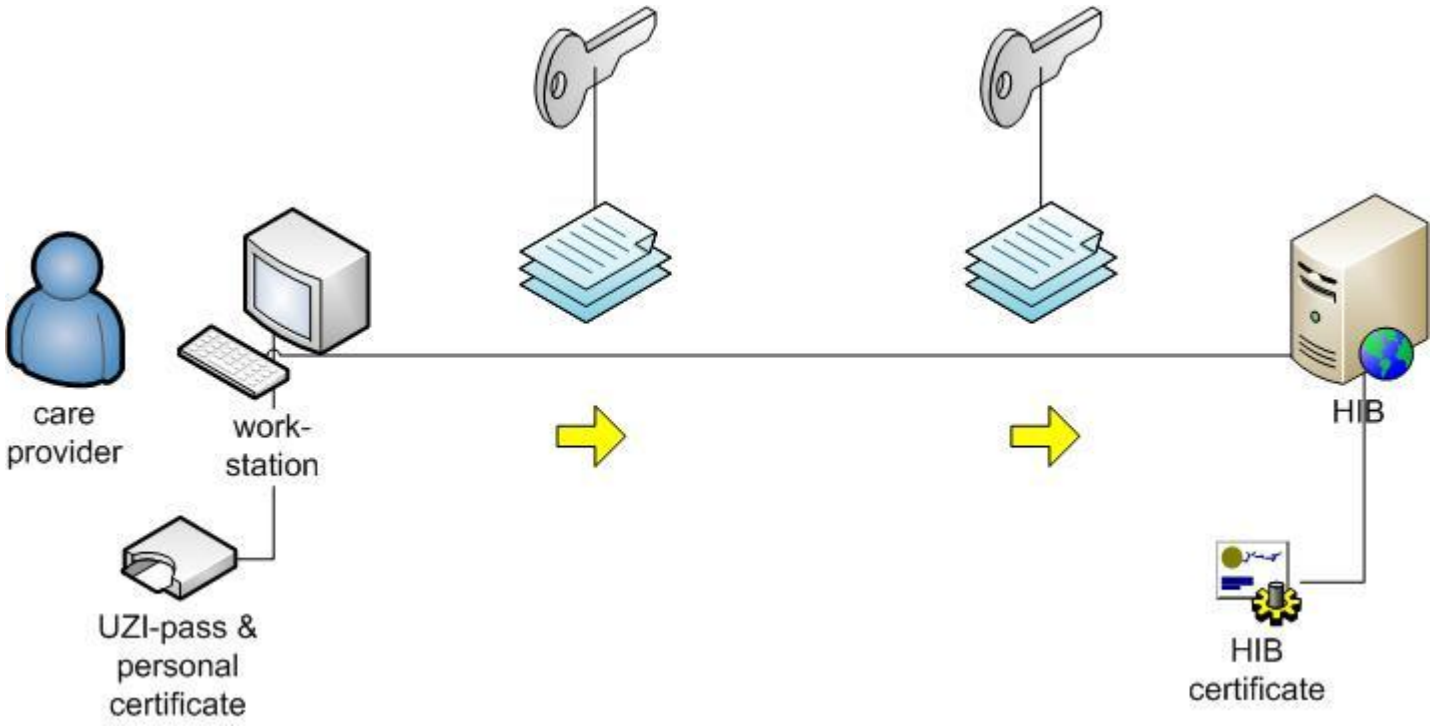
- Authentication
- Authorization
- Data Confidentiality
- Data Integrity
- Non-repudiation

Secure connection



Marc de Graauw
marc@marcdegraauw.com

Secure data

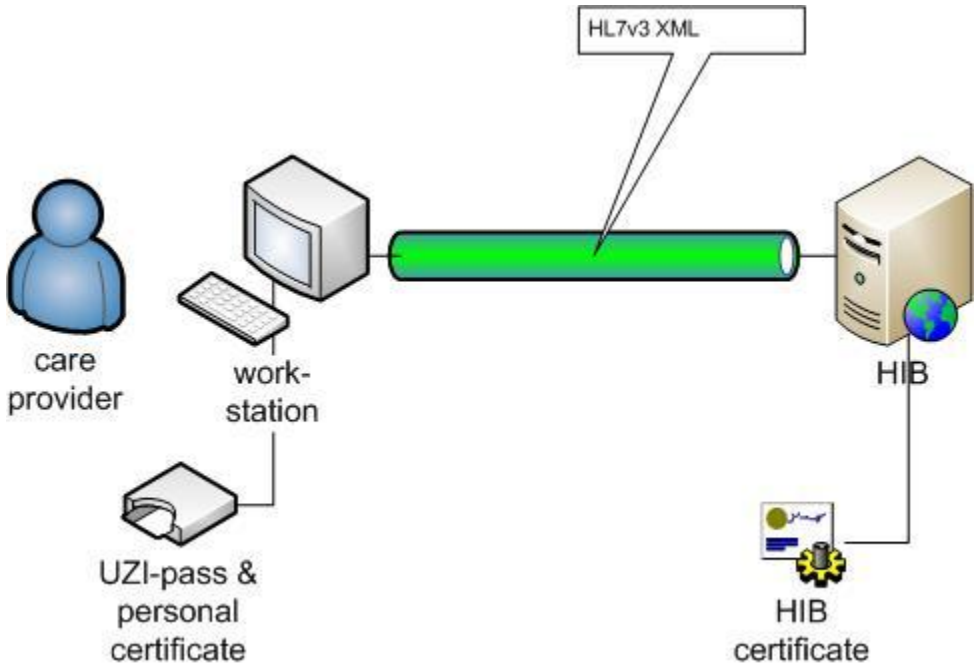


Marc de Graauw
marc@marcdegraauw.com

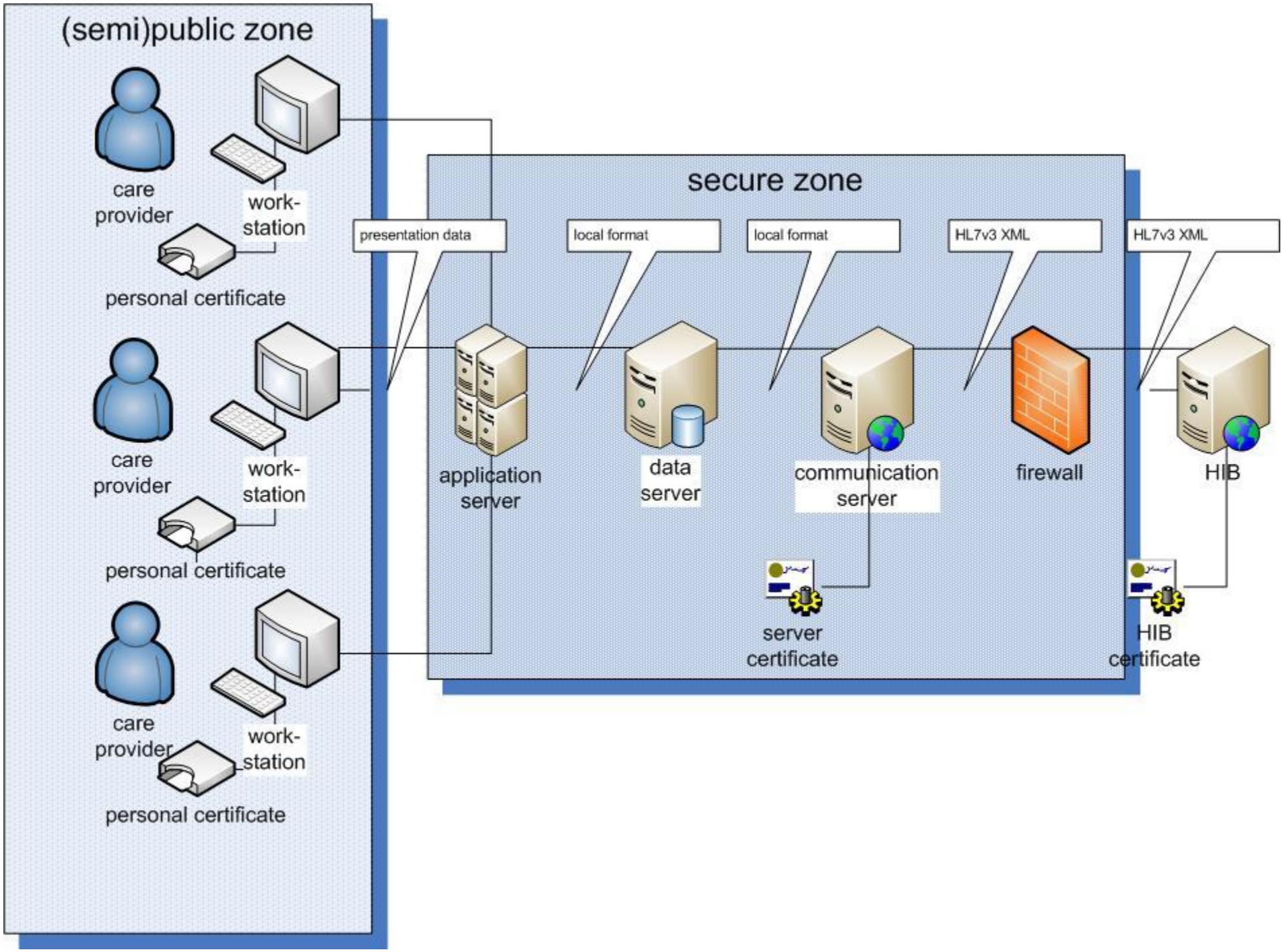
Security services

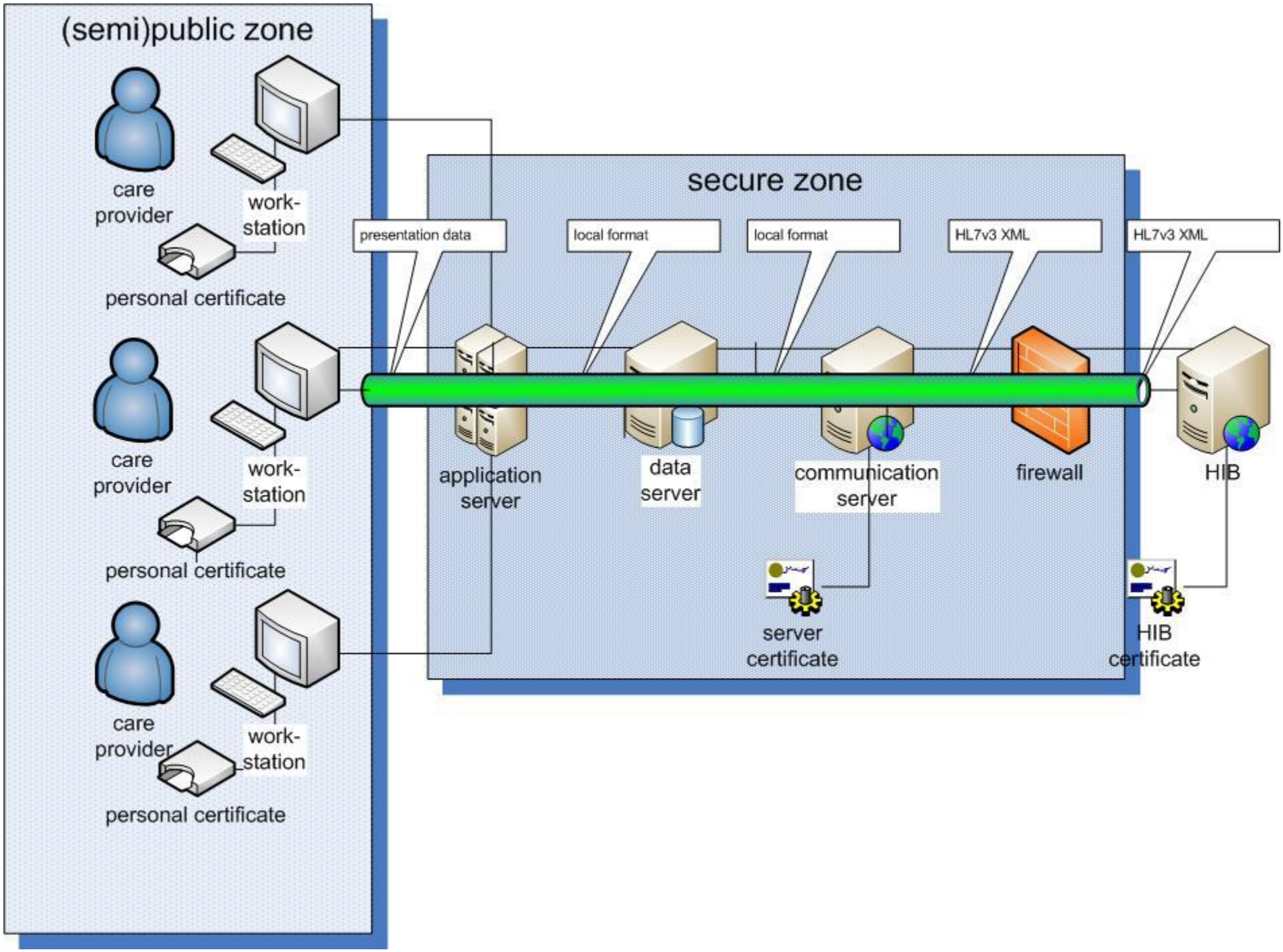
	Secure connection	Authentication Token	Digital Signature
Authentication	√	√	√
Authorization			
Confidentiality	√		
Integrity	√		√
Non-repudiation			√

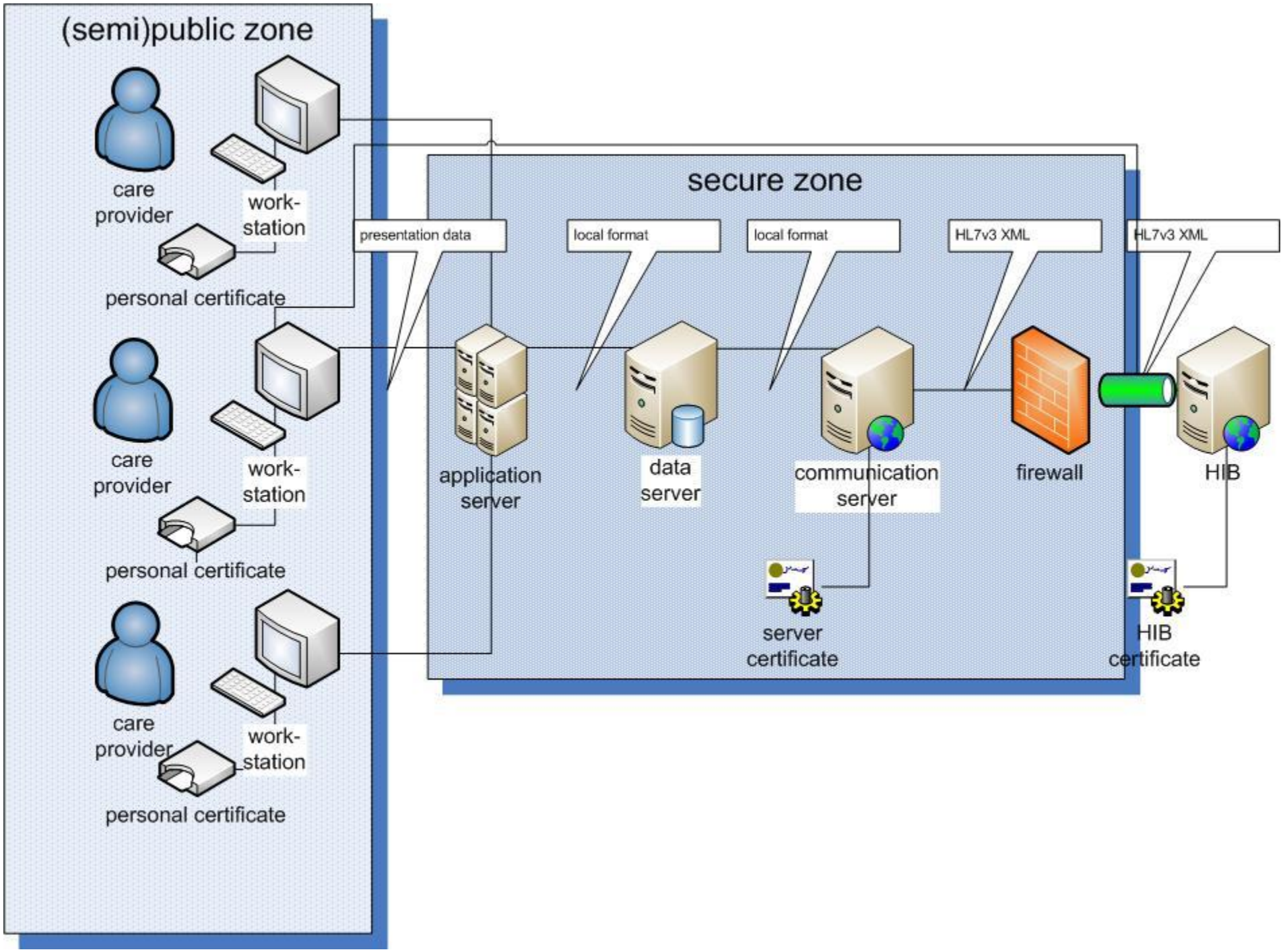
Authentication with SSL



Marc de Graauw
marc@marcdegraauw.com


(semi)public zone
care provider
work-station
personal certificate
care provider
work-station
personal certificate
care provider
work-station
personal certificate
secure zone
presentation data
local format
local format
HL7v3 XML
HL7v3 XML
application server
data server
communication server
firewall
HIB
server certificate
HIB certificate


(semi)public zone
care provider
work-station
personal certificate
care provider
work-station
personal certificate
care provider
work-station
personal certificate
secure zone
presentation data
local format
local format
HL7v3 XML
HL7v3 XML
application server
data server
communication server
firewall
HIB
server certificate
HIB certificate


(semi)public zone
care provider
work-station
personal certificate
care provider
work-station
personal certificate
care provider
work-station
personal certificate
secure zone
presentation data
local format
local format
HL7v3 XML
HL7v3 XML
application server
data server
communication server
firewall
HIB
server certificate
HIB certificate

Security with SSL

- Works well only in simple scenario’s
- There is no HL7v3 XML at the client
- The client is (relatively) unsecure
- SSL lays an impenatrable tunnel across the instution’s secure zone
- SSL from server to server is fine, but:
- provides no care provider authentication

Context: clients

- all hospitals, GP's, pharmacists, other healthcare pros
- clients: any kind of client
- latest .NET / Java
- older dev environments (Delphi, BV, etc.)
- thin client/browser
- XSLT heavy
- XML / no XML
- WS-* / no WS-*
- HL7v3 / no HL7v3

Marc de Graauw
marc@marcdegraauw.com

Context: HL7v3

- no HL7v3 at client (HL7v2, OZIS, other)
- not all data at client
  - Act.id
  - medication codes
  - patient id (BSN) not yet, is reasonable demand
- destination not always known at client
- either: require all data available at client
- or: sign subset of data

Marc de Graauw
marc@marcdegraauw.com

‘Lightweight’ authentication token

- X.509 style
  - message id
    - nonce
    - provides unique identification of message
    - (if duplicate removal has already taken place)
  - time to live
    - security semantics can expire
    - time to store & check nonce
  - addressedParty
    - replay against other receivers

Marc de Graauw
marc@marcdegraauw.com

SSL security

- premises:
  - healthcare pro keeps smartcard + pin safe
  - software to establish SSL tunnel not corrupted
  - PKI, RSA etc. not broken
- assertion:
  - healthcare pro sets up SSL tunnel
- assumption:
  - messages going over SSL tunnel come from healthcare pro
- weakness:
  - insertion of fake messages in SSL tunnel
- measures:
  - abort SSL tunnel after period of inactivity, refresh regularly

Marc de Graauw
marc@marcdegraauw.com

Lightweight token security

- premises:
  - healthcare pro keeps smartcard + pin safe
  - software to sign token not corrupted
  - PKI, RSA etc. not broken
- assertion:
  - healthcare pro signed auth token
- assumption:
  - message and auth token belong together
- weakness:
  - fake message attached to valid token

Marc de Graauw
marc@marcdegraauw.com

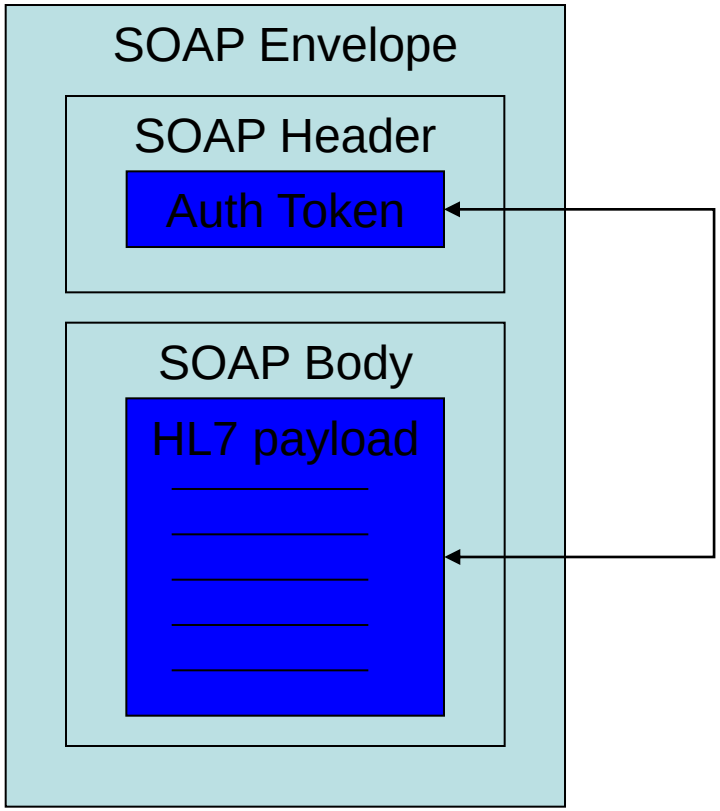
Lightweight token security

- signedData:
  - message id
  - notBefore / notAfter
  - addressedParty
- coSignedData
  - patient id (BSN)
  - message type (HL7 trigger event id)
- only possible to retrieve same kind of data for same patient at same time from same destination
- weakness: tampering with other message parameters
- for queries: acceptable (privacy not much more broken)
- for prescription: use full digital signature

Hospital workflow

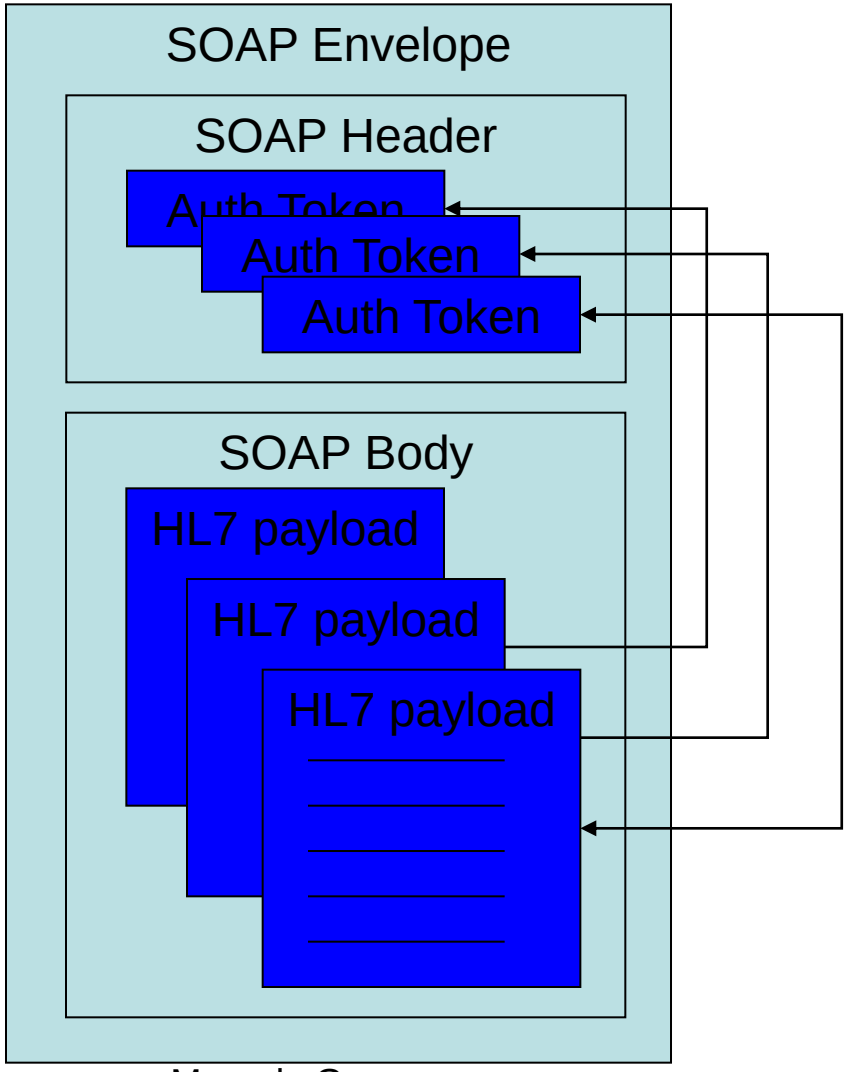
- doctor makes round
- 360 seconds per patient
- nurse has file ready
- retrieval times are not acceptable
- pre-signing tokens and pre-fetching data just in time
- possible with auth tokens, not (so much) with SSL

Authentication alternatives

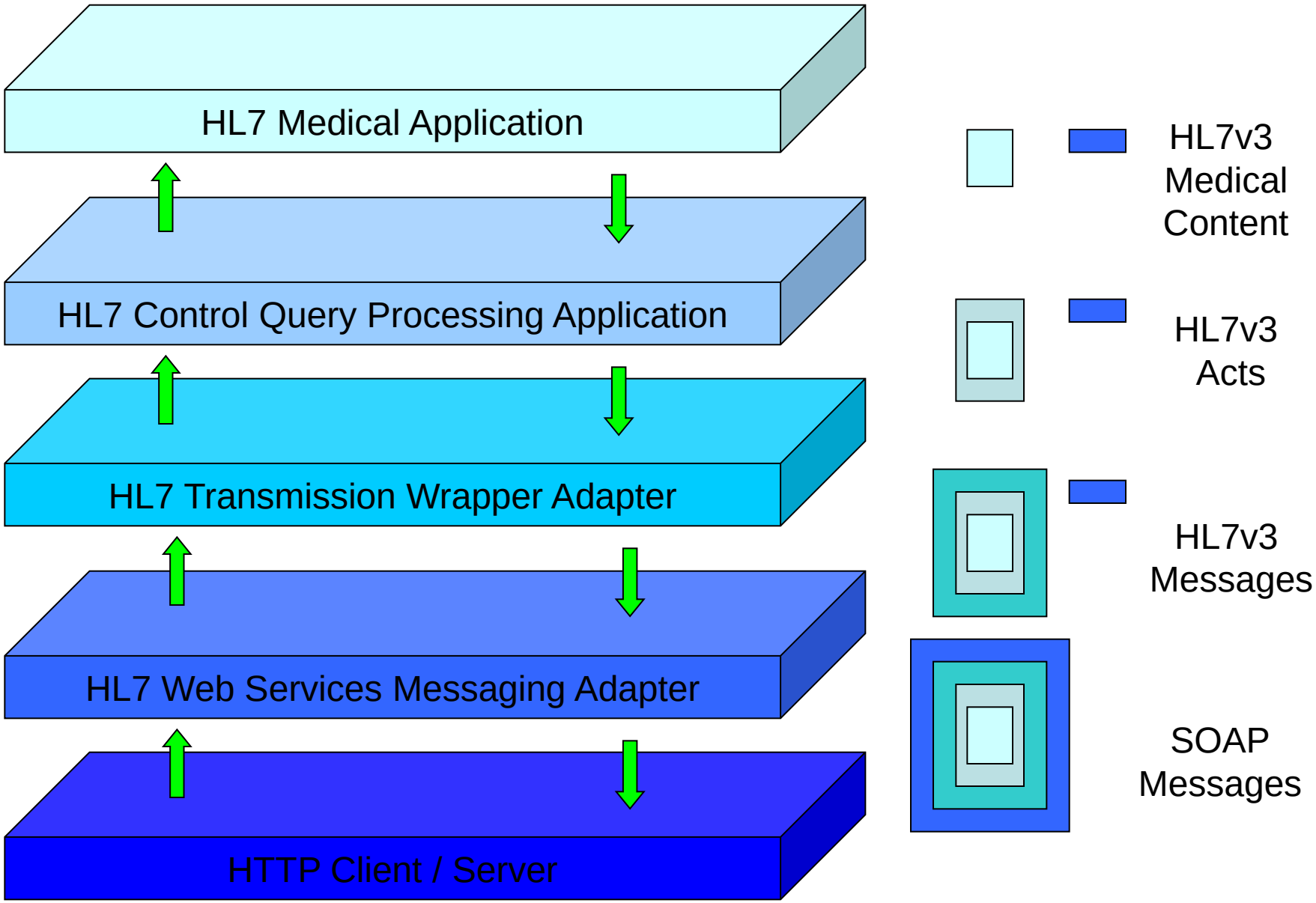


Marc de Graauw
marc@marcdegraauw.com

Authentication alternatives



Marc de Graauw
marc@marcdegraauw.com



marc@marcdegraauw.com

Authentication alternatives

- Authentication tokens in SOAP Headers separate them from the content
- HL7 sometimes allows multiple payloads, making this problem worse
- The token has to travel across layers with the paylaod
- This violates layering principles

WS-*

- WS-* is confused about whether it is a document format or a message format
- document: relevant to the end user
- message: relevant to the mailman
- keep metadata with the document
- putting document metadata in SOAP headers violates layering design principles

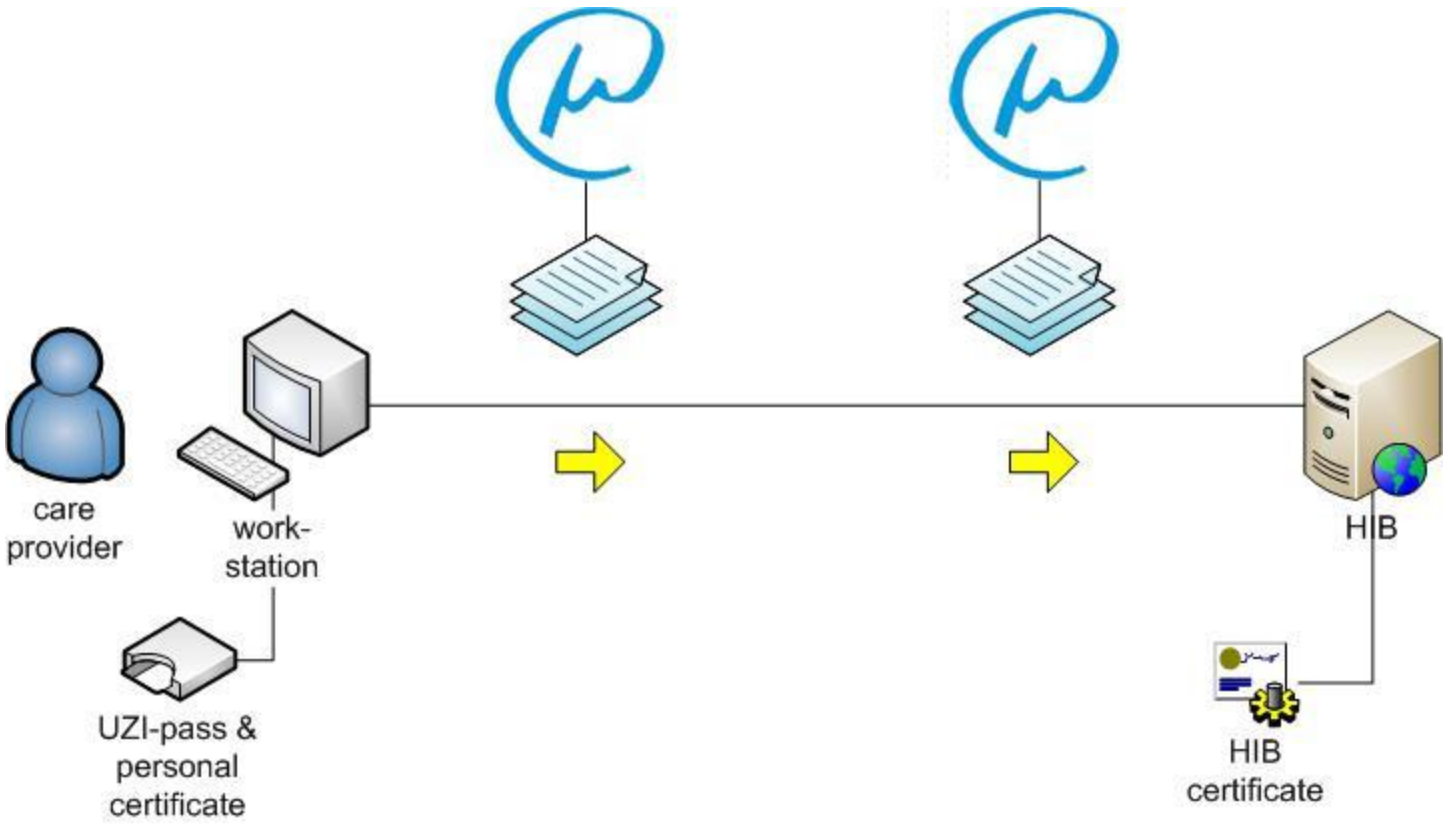
Digital Signatures

Marc de Graauw
marc@marcdegraauw.com

Some philosophy

- “The President of the United States is John McCain”
- “Karen believes ‘the President of the United States is John McCain’ ”
- “John says that ‘the President of the United States is John McCain’ ”
- “Dr. Jones says: ‘Mr. Smith has the flu’ ”

Signed Data



Marc de Graauw
marc@marcdegraauw.com

```
<code code=”27”
  codeSystem=”2.16.840.1.113883.2
  .4.4.5” />
```

"Dissolve in water"

Marc de Graauw
marc@marcdegraauw.com

XML fragment

```
<Prescription>
    <id extension="0003000201" root="2.16.840.1.113883.2.4.6.1.6005465.12.1"/>
    <statusCode code="active"/>
    <subject>
        <Patient>
            <id extension="012345672" root="2.16.840.1.113883.2.4.6.3"/>
            <statusCode code="active"/>
            <Person>
                <name>
                    <given qualifier="IN">J.M.</given>
                    <family>Breed</family>
                </name>
                <administrativeGenderCode code="M" codeSystem="2.16.840.1.113883.5.1"/>
                <birthTime value="19680816"/>
            </Person>
            <Organization>
                <id extension="06005465" root="2.16.840.1.113883.2.4.6.1"/>
            </Organization>
        </Patient>
    </subject>
```

Marc de Graauw
marc@marcdegraauw.com

Digitally signed token

```
<prescription caption="Voorschrift">
    <id>
        <root>2.16.528.1.1007.3.3.1234567.1</root>
        <extension caption="Voorschriftnummer:">0123456789</extension>
    </id>
    <date>10-12-2008</date>
    <patient>
        <name caption="Patient:">J.M. Breed</name>
        <gender>M</gender>
        <birthdate caption="Geboortedatum:">16-08-1968</birthdate>
        <id caption="BSN:">012345672</id>
    </patient>
    <author>
        <name caption="Voorschrift van:">Dr. Frans Rijtje</name>
        <id caption="UZI-nummer:">012345678</id>
    </author>
    <medication>
        <code>
            <code>999999</code>
            <codeSystem>2.16.840.1.113883.2.4.4.7</codeSystem>
        </code>
        <text caption="Medicatie:">Acetylcyteine pch poeder skvr 600mg in sachet</text>
    </medication>
    <usage caption="Gebruik:">1 x daags 1 sachet in water oplossen</usage>
</prescription>
```

Marc de Graauw
marc@marcdegraauw.com

What You See Is What You Sign

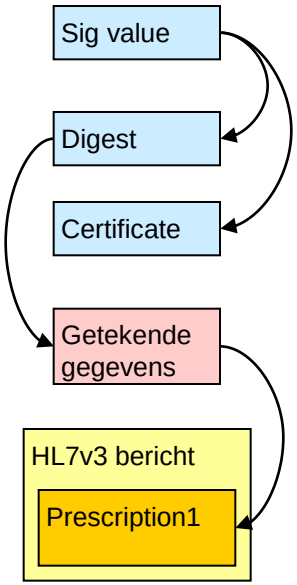
Voorschrift

Voorschriftnummer:	0123456789
Patient:	J.M. Breed
Geboortedatum:	16-08-1968
BSN:	012345672
Voorschrift van:	Dr. Frans Rijtje
UZI-nummer:	012345678
Medicatie:	Acetylcyteine pch poeder skvr 600mg in sachet
Gebruik:	1 x daags 1 sachet in water oplossen

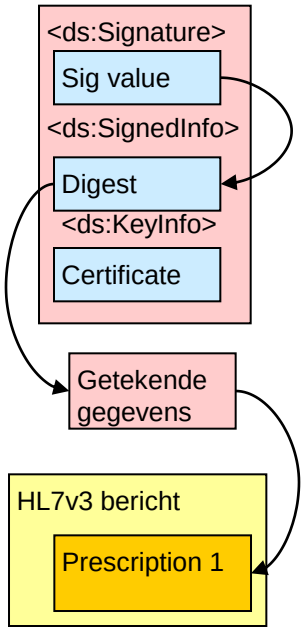
Marc de Graauw
marc@marcdegraauw.com

Token & XML Signature

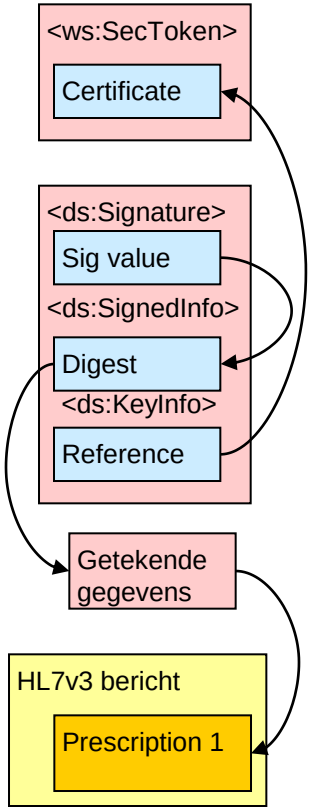
Componenten



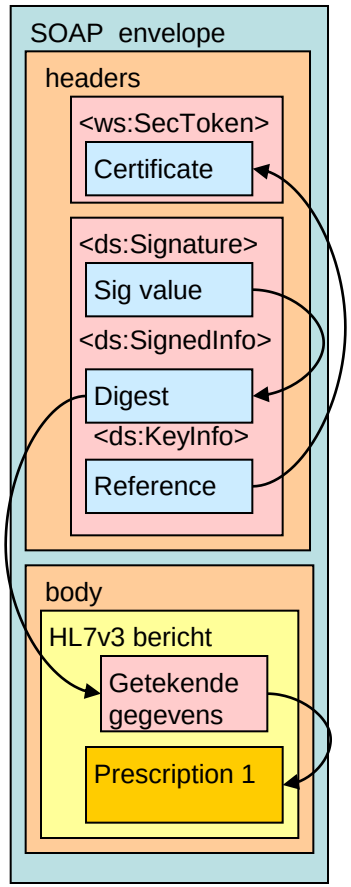
XML Signature



Met WSS



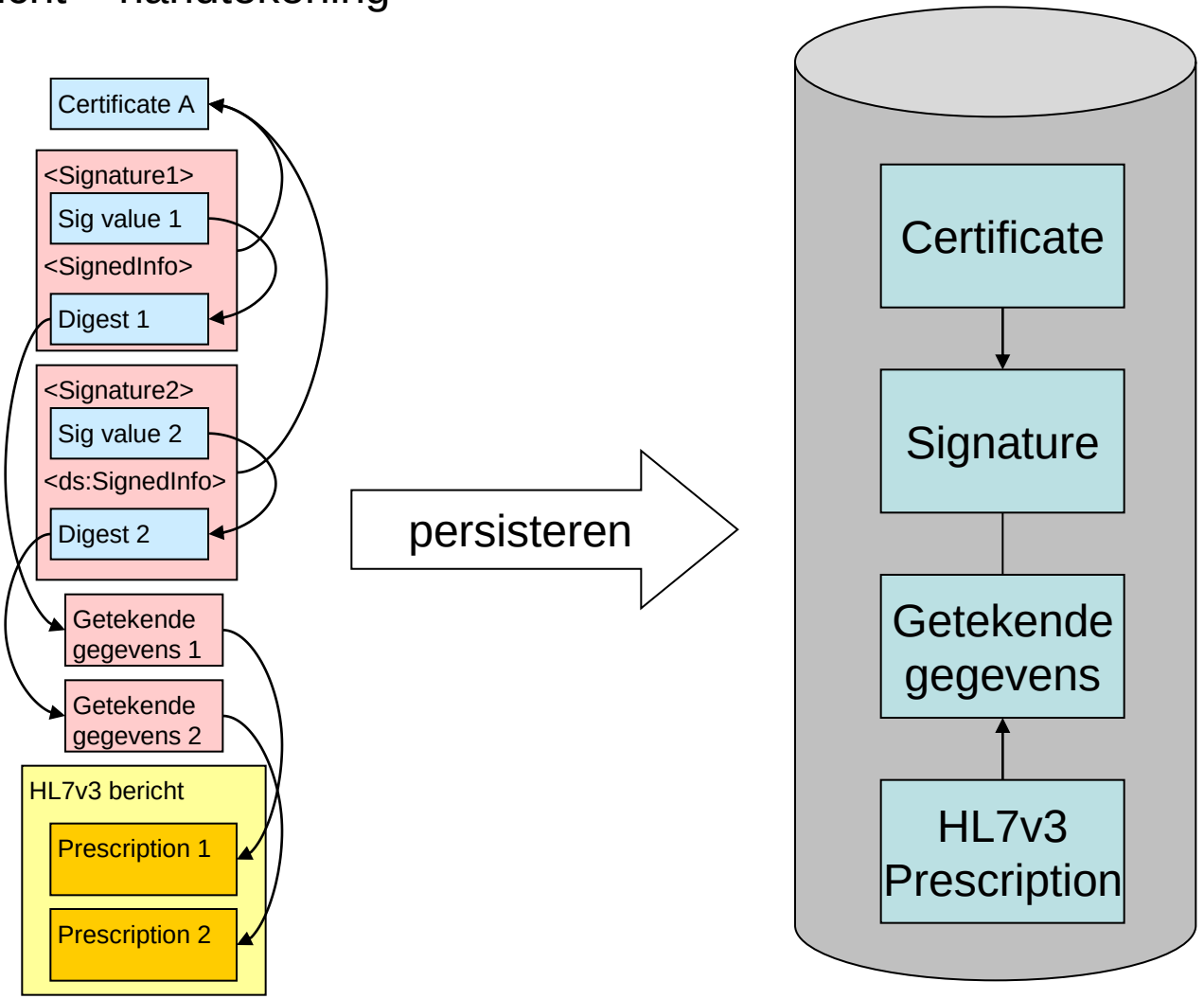
In SOAP Headers



Marc de Graauw
marc@marcdegraauw.com

Meerdere Signatures, 1 certificaat

Bericht + handtekening



Marc de Graauw
marc@marcdegraauw.com