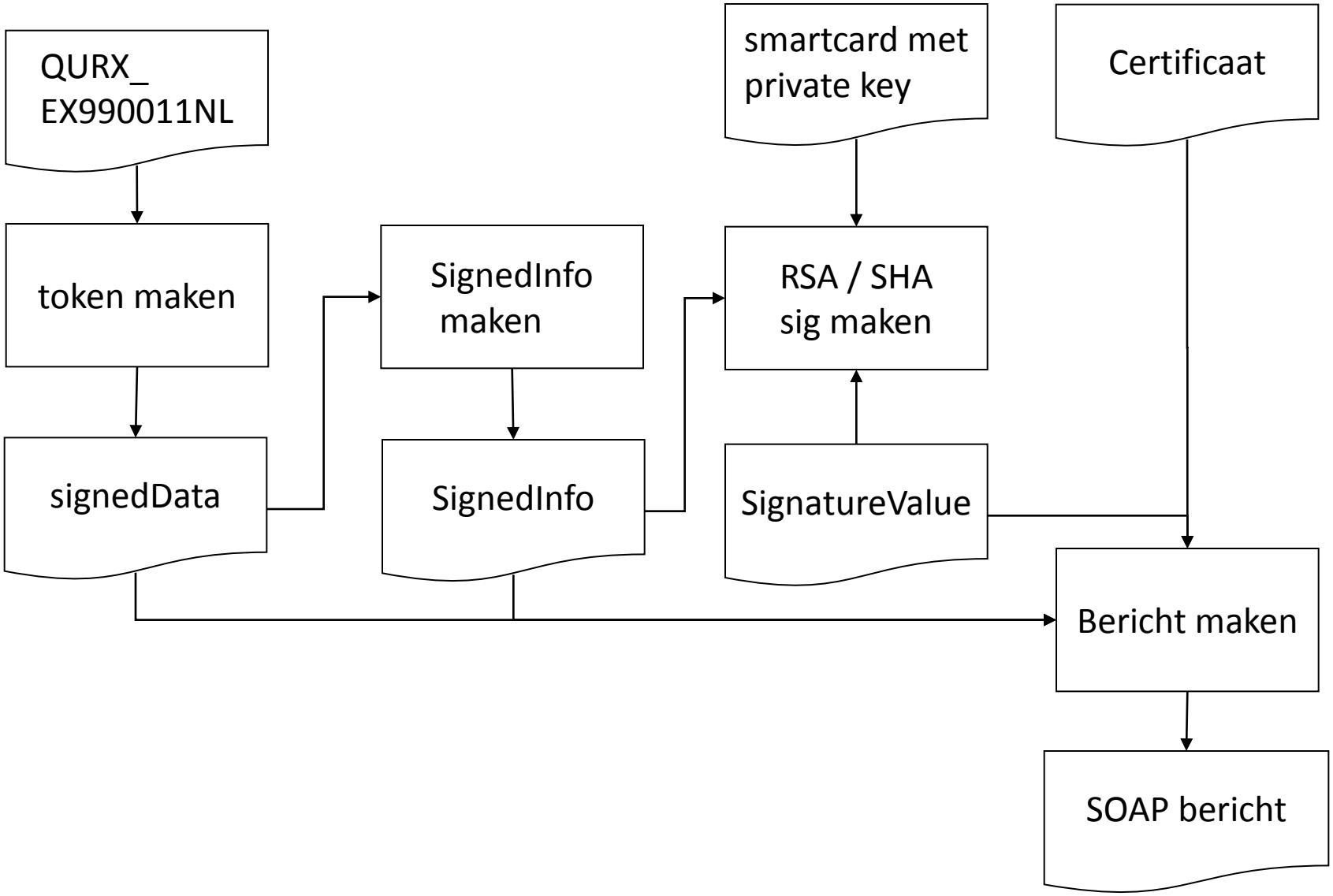
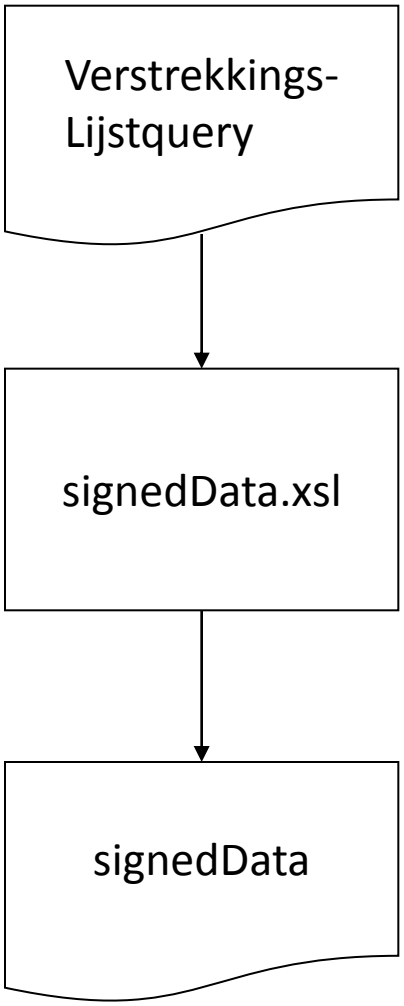
Tokenauthenticatie
&
XML Signature
in detail

Tokenauthenticatie



Transformatie XML 2 SignedData



QURX_IN990111NL_01.xml

QURX_IN990111NL_01_signedData.xml

VerstrekkingsLijstquery

```xml
<?xml version="1.0" encoding="UTF-8"?>
<?oxygen SCHSchema="../schematron/QURX_IN990111NL.sch"?>
<!-- example QURX_IN990111NL-1 Verstrekkingsquery (lijst verstrekkingen): Zoek verstrekkingen bij LSP op BSN
-->
<QURX_IN990111NL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:hl7-org:v3 ../schemas/QURX_IN990111NL.xsd" xmlns="urn:hl7-org:v3">
    <id extension="0123456789" root="2.16.528.1.1007.3.3.1234567.1"/>
    <creationTime value="20050128173600"/>
    <versionCode code="NICTIZEd2005-Okt"/>
    <interactionId extension="QURX_IN990111NL" root="2.16.840.1.113883.1.6"/>
    <profileId root="2.16.840.1.113883.2.4.3.11.1" extension="810"/>
    <!-- Training berichten (gebruik P voor Productie), geen acknowledgement berichten -->
    <processingCode code="T"/>
    <processingModeCode code="T"/>
    <acceptAckCode code="NE"/>
    <attentionLine>
        <keyWordText code="PATID" codeSystem="2.16.840.1.113883.2.4.15.1">Patient.id</keyWordText>
        <value xsi:type="II"  extension="012345672" root="2.16.840.1.113883.2.4.6.3"/>
    </attentionLine>
    <receiver>
        <device>
            <id extension="1" root="2.16.840.1.113883.2.4.6.6"/>
            <!-- LSP -->
        </device>
    </receiver>
    <sender>
        <device>
            <id extension="01234567" root="2.16.840.1.113883.2.4.6.6"/>
            <!-- EVS van ziekenhuis Medisch Centrum Oost o.b.v. landelijke applicatie ID -->
        </device>
    </sender>
    <ControlActProcess moodCode="EVN">
        <authorOrPerformer typeCode="AUT">
            <participant>
                <AssignedPerson>
                    <id extension="012345678" root="2.16.528.1.1007.3.1"/>
                    <!-- specialist Dr. Jansen o.b.v. UZI nummer -->
                    <code code="01.000" codeSystem="2.16.840.1.113883.2.4.15.111" displayName="Arts"/>
                    <Organization>
                        <id extension="01234567" root="2.16.528.1.1007.3.3"/>
                        <name>Medisch Centrum Oost </name>
                        <!-- ziekenhuis Medisch Centrum Oost o.b.v. UZI abonneenummer -->
```

signedData

- X.509 Strong Authentication
  - message id
    - nonce
    - unieke indentificatie van bericht
    - (if duplicate removal has already taken place)
  - notBefore & notAfter
    - time to live
    - security semantics can expire
    - time to store & check nonce
  - addressedParty
    - replay against other receivers
- Koppeling met bericht
  - BSN
    - voor patiëntgerelateerde berichten
  - Trigger Event Id
    - versieonafhankelijk, itt. InteractionId

signedData.xml (pretty print)

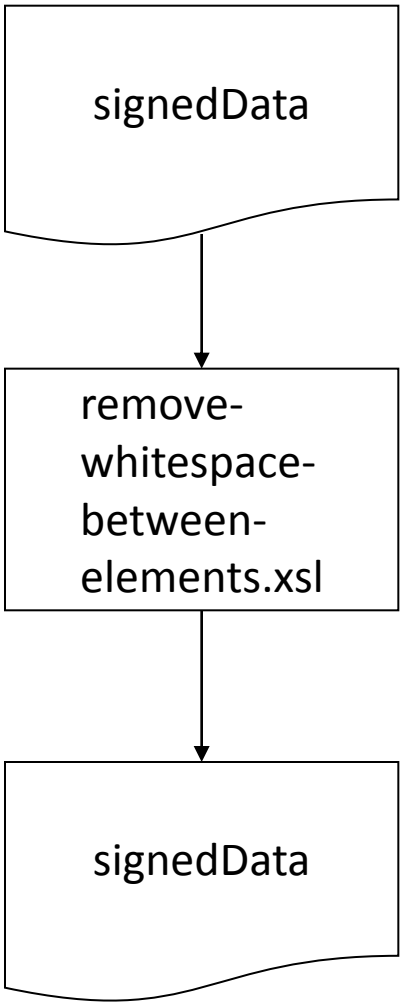
```xml
<signedData xmlns="http://www.aortarelease.nl/805/"
    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
    wsu:Id="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
    <authenticationData>
        <messageId>
            <root>2.16.528.1.1007.3.3.1234567.1</root>
            <extension>0123456789</extension>
        </messageId>
        <notBefore>20050128173600</notBefore>
        <notAfter>20050128174059</notAfter>
        <addressedParty>
            <root>2.16.840.1.113883.2.4.6.6</root>
            <extension>1</extension>
        </addressedParty>
    </authenticationData>
    <coSignedData>
        <triggerEventId>QURX_TE990011NL</triggerEventId>
        <patientId>
            <root>2.16.840.1.113883.2.4.6.3</root>
            <extension>012345672</extension>
        </patientId>
    </coSignedData>
</signedData>
```

Token versus bestand

```xml
<?xml version="1.0" encoding="UTF-8"?>
<?oxygen SCHSchema="../schematron/QURX_IN990111NL.sch"?>
<!-- example QURX_IN990111NL-1 Verstrekkingsquery (lijst verstr
<QURX_IN990111NL xmlns:xsi="http://www.w3.org/2001/XMLSchema-in
    <id extension="0123456789"
        root="2.16.528.1.1007.3.3.1234567.1"/>
    <creationTime value="20050128173600"/>
    <versionCode code="NICTIZEd2005-Okt"/>
    <interactionId extension="QURX_IN990111NL" root="2.16.840.1
    <profileId root="2.16.840.1.113883.2.4.3.11.1" extension="8
    <processingCode code="T"/>
    <processingModeCode code="T"/>
    <acceptAckCode code="NE"/>
    <attentionLine> [3 lines]
    <receiver>
        <device>
            <id extension="1" root="2.16.840.1.113883.2.4.6.6",
        </device>
    </receiver>
    <sender> [5 lines]
    <ControlActProcess moodCode="EVN">
        <authorOrPerformer typeCode="AUT"> [13 lines]
        <overseer typeCode="RESP"> [21 lines]
        <queryByParameter>
            <queryId extension="0123456789" root="2.16.528.1.10
            <statusCode code="executing"/>
            <responseModalityCode code="B"/>
            <responsePriorityCode code="I"/>
            <dispenseEventEffectiveTimeInterval> [6 lines]
            <patientID>
                <value extension="012345672"
                    root="2.16.840.1.113883.2.4.6.3"/>
                <semanticsText>Patiëntnummer</semanticsText>
                <!-- patiënt A. de Vries o.b.v. BSN -->
            </patientID>
        </queryByParameter>
    </ControlActProcess>
</QURX_IN990111NL>
```

```xml
<signedData xmlns="http://www.aortarelease.nl/805/"
    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
    wsu:Id="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
    <authenticationData>
        <messageId>
            <root>2.16.528.1.1007.3.3.1234567.1</root>
            <extension>0123456789</extension>
        </messageId>
        <notBefore>20050128173600</notBefore>
        <notAfter>20050128174059</notAfter>
        <addressedParty>
            <root>2.16.840.1.113883.2.4.6.6</root>
            <extension>1</extension>
        </addressedParty>
    </authenticationData>
    <coSignedData>
        <triggerEventId>QURX_TE990011NL</triggerEventId>
        <patientId>
            <root>2.16.840.1.113883.2.4.6.3</root>
            <extension>012345672</extension>
        </patientId>
    </coSignedData>
</signedData>
```

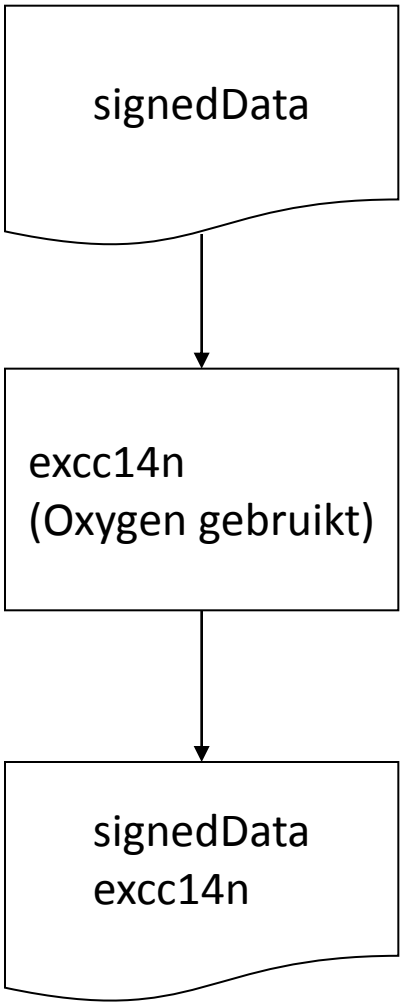
Whitespace eruit



QURX_IN990111NL_01_signedData.xml

QURX_IN990111NL_01_signedData.xml

Exclusive Canonicalization



QURX_IN990111NL_01_signedData.xml

signedData_ excc14n.xml

Exclusive Canonicalization

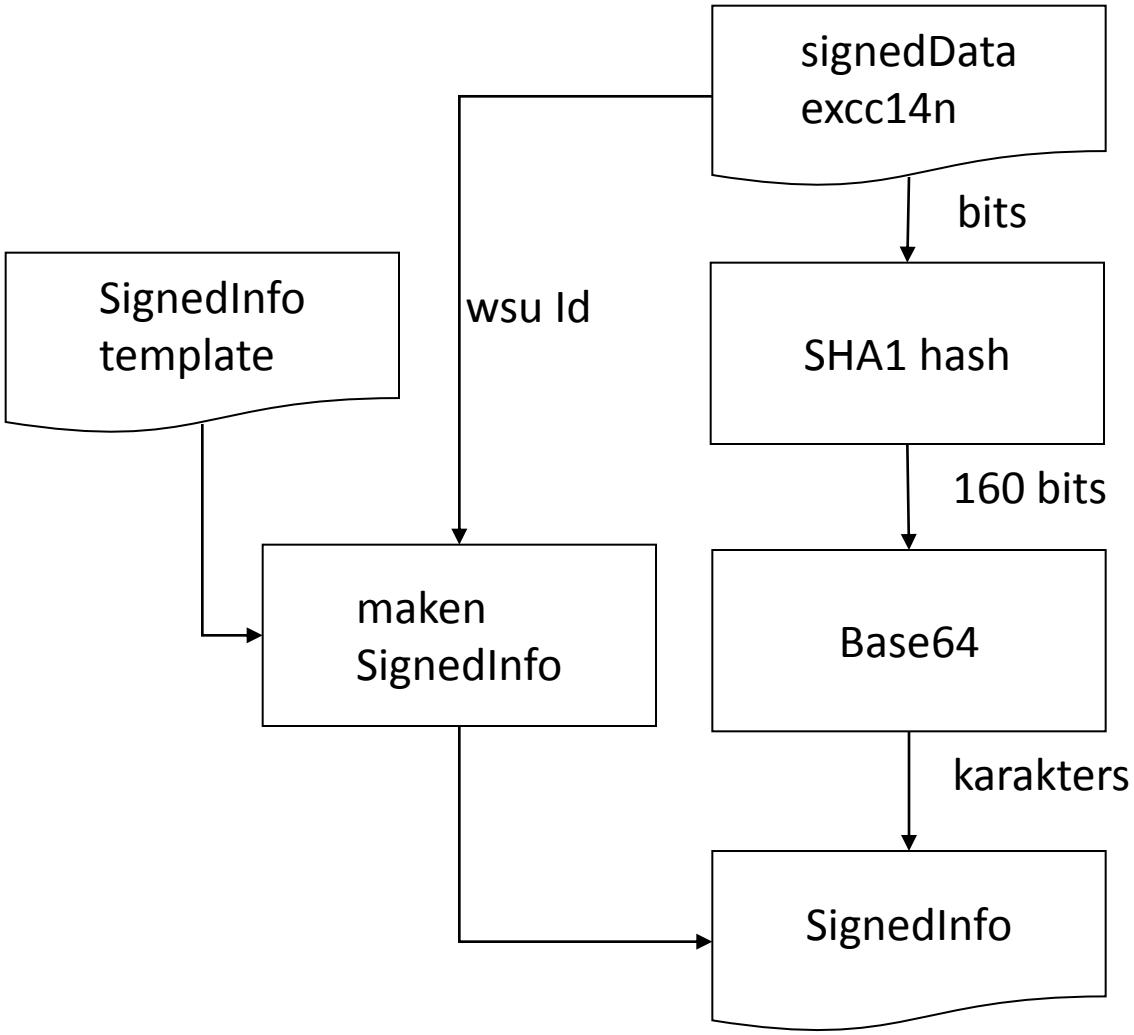
```
<signedData xmlns:wsu='http://docs.oasis-open.org/wss/2004
    wsu:Id='token_2.16.528.1.1007.3.3.1234567.1_0123456789
    xmlns='http://www.aortarelease.nl/805/'>
    <authenticationData>
        <messageId>
            <root>2.16.528.1.1007.3.3.1234567.1</root>
            <extension>0123456789</extension>
        </messageId>
        <notBefore>20050128173600</notBefore>
        <notAfter>20050128174059</notAfter>
        <addressedParty>
            <root>2.16.840.1.113883.2.4.6.6</root>
            <extension>1</extension>
        </addressedParty>
    </authenticationData>
    <coSignedData>
        <triggerEventId>QURX_TE990011NL</triggerEventId>
        <patientId>
            <root>2.16.840.1.113883.2.4.6.3</root>
            <extension>012345672</extension>
        </patientId>
    </coSignedData>
</signedData>
```

```
<signedData xmlns="http://www.aortarelease.nl/805/"
    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-20
    wsu:Id="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
    <authenticationData>
        <messageId>
            <root>2.16.528.1.1007.3.3.1234567.1</root>
            <extension>0123456789</extension>
        </messageId>
        <notBefore>20050128173600</notBefore>
        <notAfter>20050128174059</notAfter>
        <addressedParty>
            <root>2.16.840.1.113883.2.4.6.6</root>
            <extension>1</extension>
        </addressedParty>
    </authenticationData>
    <coSignedData>
        <triggerEventId>QURX_TE990011NL</triggerEventId>
        <patientId>
            <root>2.16.840.1.113883.2.4.6.3</root>
            <extension>012345672</extension>
        </patientId>
    </coSignedData>
</signedData>
```

Exclusive Canonicalization

- Dubbele quotes ipv. enkele
- Namespace declaraties vóór attributen
- Namespaces alfabetisch rangschikken
- Linefeed, geen carriage return of CR/LF
- Geen Byte Order Mark
- UTF-8

Signed Info element

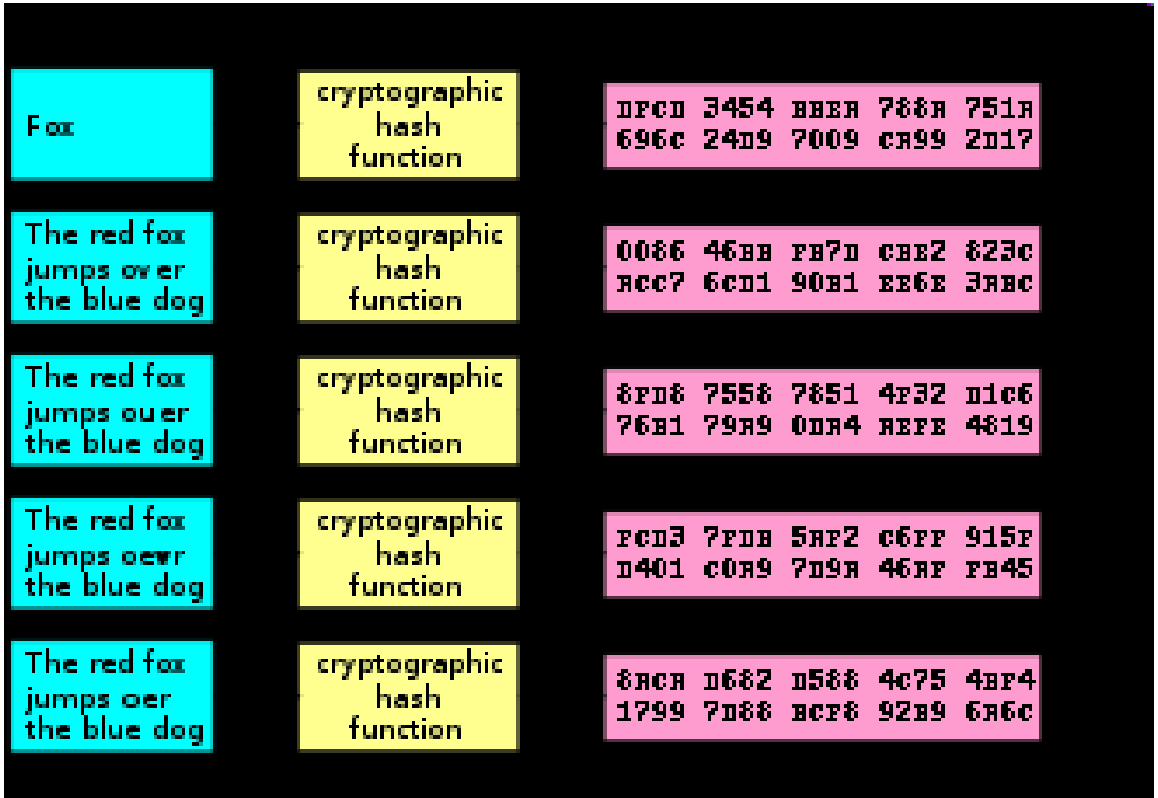


signedData_ excc14n.xml

SignedInfo.xml

SHA: Cryptographic hash

Wikipedia: A **cryptographic hash function** is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (**cryptographic**) **hash value**, such that an accidental or intentional change to the data will change the hash value.



SHA

- SHA1 ... SHA256
  - 1995: SHA-1 NSA
  - 2005: zwaktes in SHA-1 ontdekt
  - 2001: SHA-2 (225, 256, 384, 512)
  - 2008 – 12: SHA-3, open competitie
- SHA-1
  - input: message maximum $(2^{64} - 1)$ bits
  - output: 160 bits

Base 64

- UTF-8: niet alle octets zijn toegestaan!
- Ergo: binaire data kunnen niet zomaar in XML / UTF-8
- Oplossing: bits -> karakters
- RFC2045 (MIME) alfabet: [A-Z][a-z][0-9]+/

Text content	**M**								**a**								**n**							
ASCII	77								97								110							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19								22								5							
Base64-Encoded	**T**								**W**								**F**							

SHA + Base64

Input (bits)

```
<signedData xmlns="http://www.aortarelease.nl/805/"
    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
    wsu:Id="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
    <authenticationData>
        <messageId>
            <root>2.16.528.1.1007.3.3.1234567.1</root>
            <extension>0123456789</extension>
        </messageId>
        <notBefore>20050128173600</notBefore>
        <notAfter>20050128174059</notAfter>
        <addressedParty>
            <root>2.16.840.1.113883.2.4.6.6</root>
            <extension>1</extension>
```

```
00000000h: 3C 73 69 67 6E 65 64 44 61 74 61 20 78 6D 6C 6E ; <signedData xmln
00000010h: 73 3D 22 68 74 74 70 3A 2F 2F 77 77 77 2E 61 6F ; s="http://www.ao
00000020h: 72 74 61 72 65 6C 65 61 73 65 2E 6E 6C 2F 38 30 ; rtarelease.nl/80
00000030h: 35 2F 22 20 78 6D 6C 6E 73 3A 77 73 75 3D 22 68 ; 5/" xmlns:wsu="h
00000040h: 74 74 70 3A 2F 2F 64 6F 63 73 2E 6F 61 73 69 73 ; ttp://docs.oasis
00000050h: 2D 6F 70 65 6E 2E 6F 72 67 2F 77 73 73 2F 32 30 ; -open.org/wss/20
00000060h: 30 34 2F 30 31 2F 6F 61 73 69 73 2D 32 30 30 34 ; 04/01/oasis-2004
00000070h: 30 31 2D 77 73 73 2D 77 73 73 65 63 75 72 69 74 ; 01-wss-wssecurit
00000080h: 79 2D 75 74 69 6C 69 74 79 2D 31 2E 30 2E 78 73 ; y-utility-1.0.xs
```

SHA1 (160 bits)

```
00000000h: E2 F0 4F E4 AE 4C E6 59 40 05 A5 98 CF 10 AB 28 ; âðOä®LæY@.¥˜Ï.«(
00000010h: 87 63 4B 62                                     ; ‡cKb
```

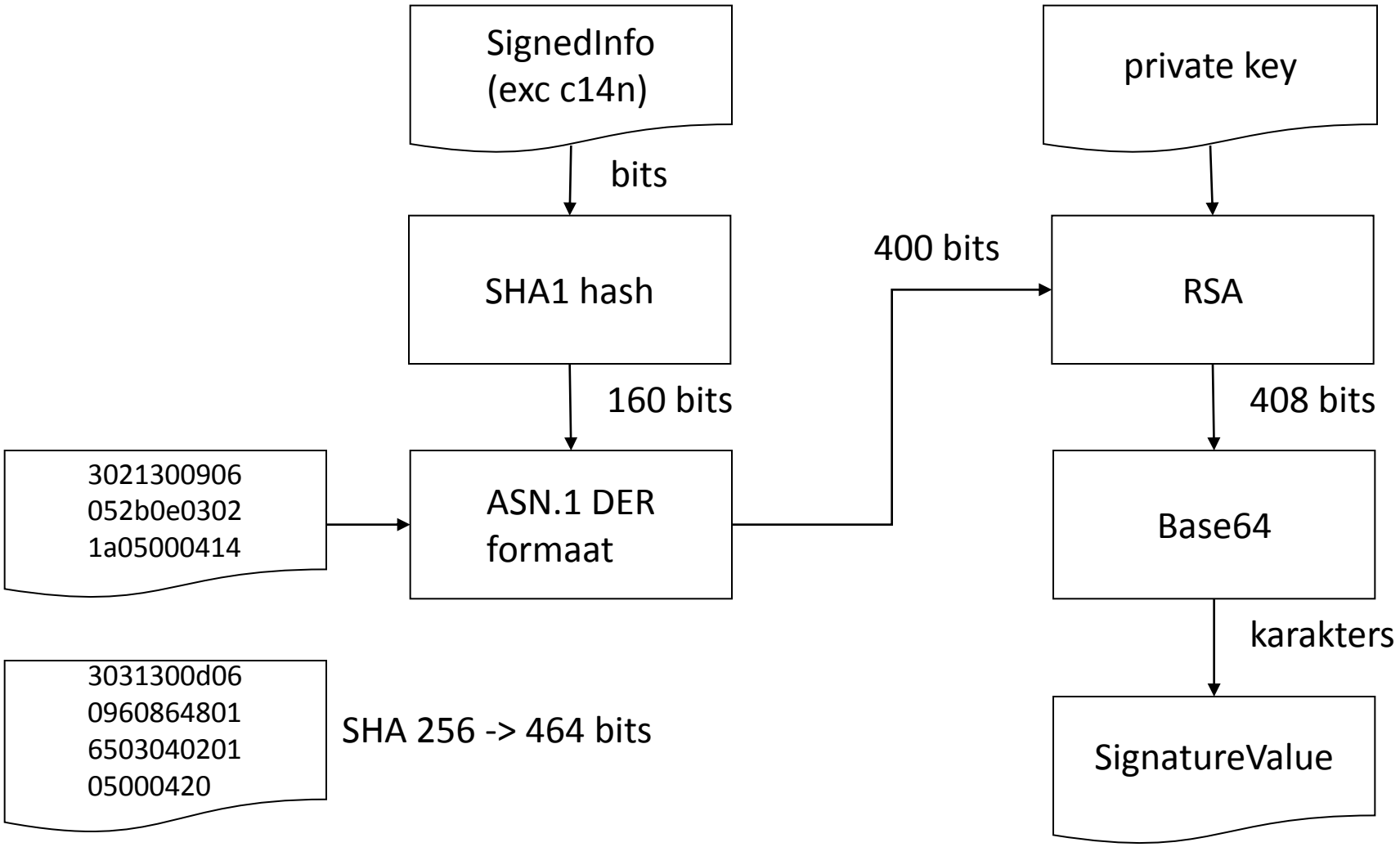
Base 64

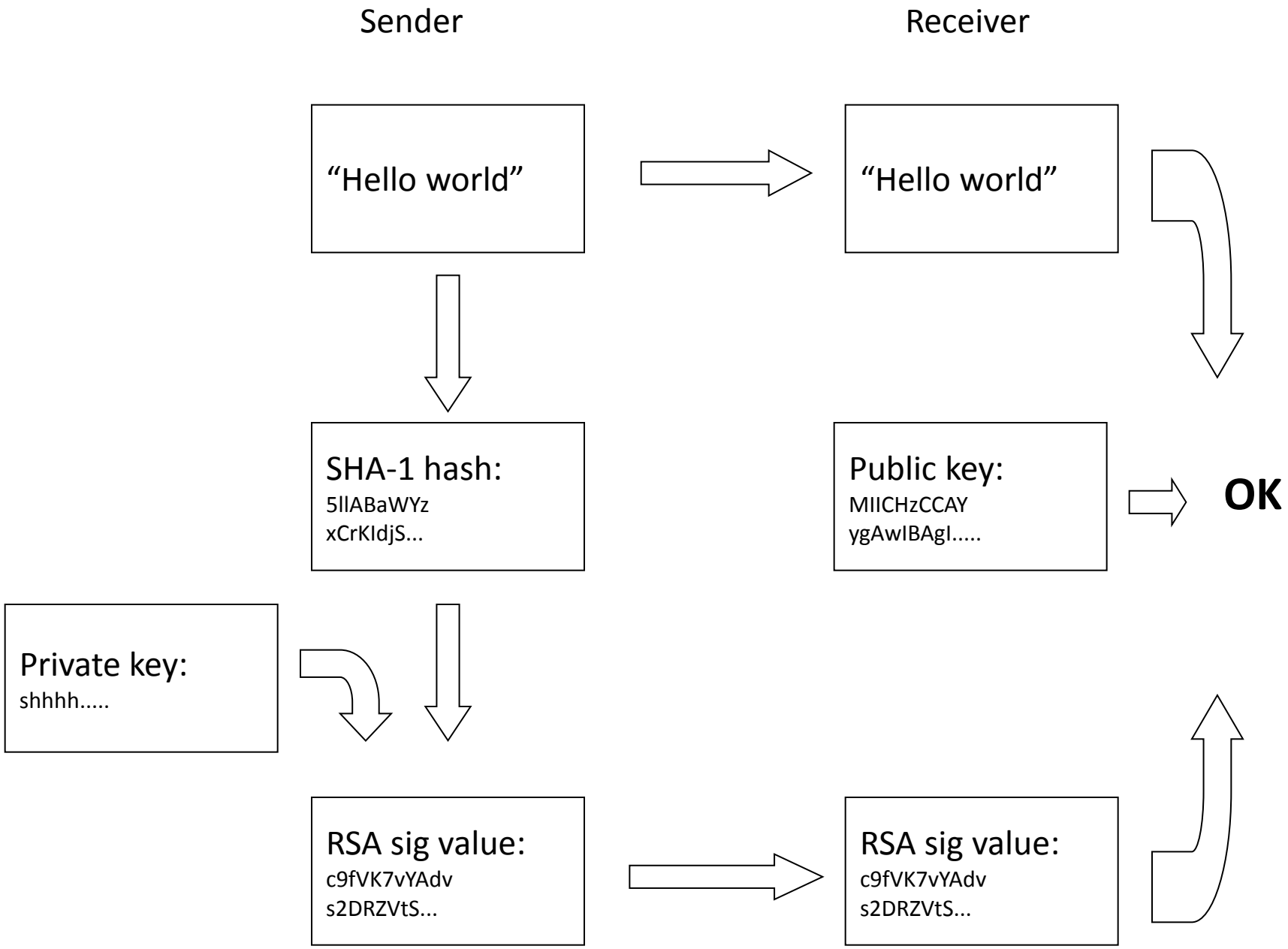
4vBP5K5M5llABaWYzxCrKIdjS2I=

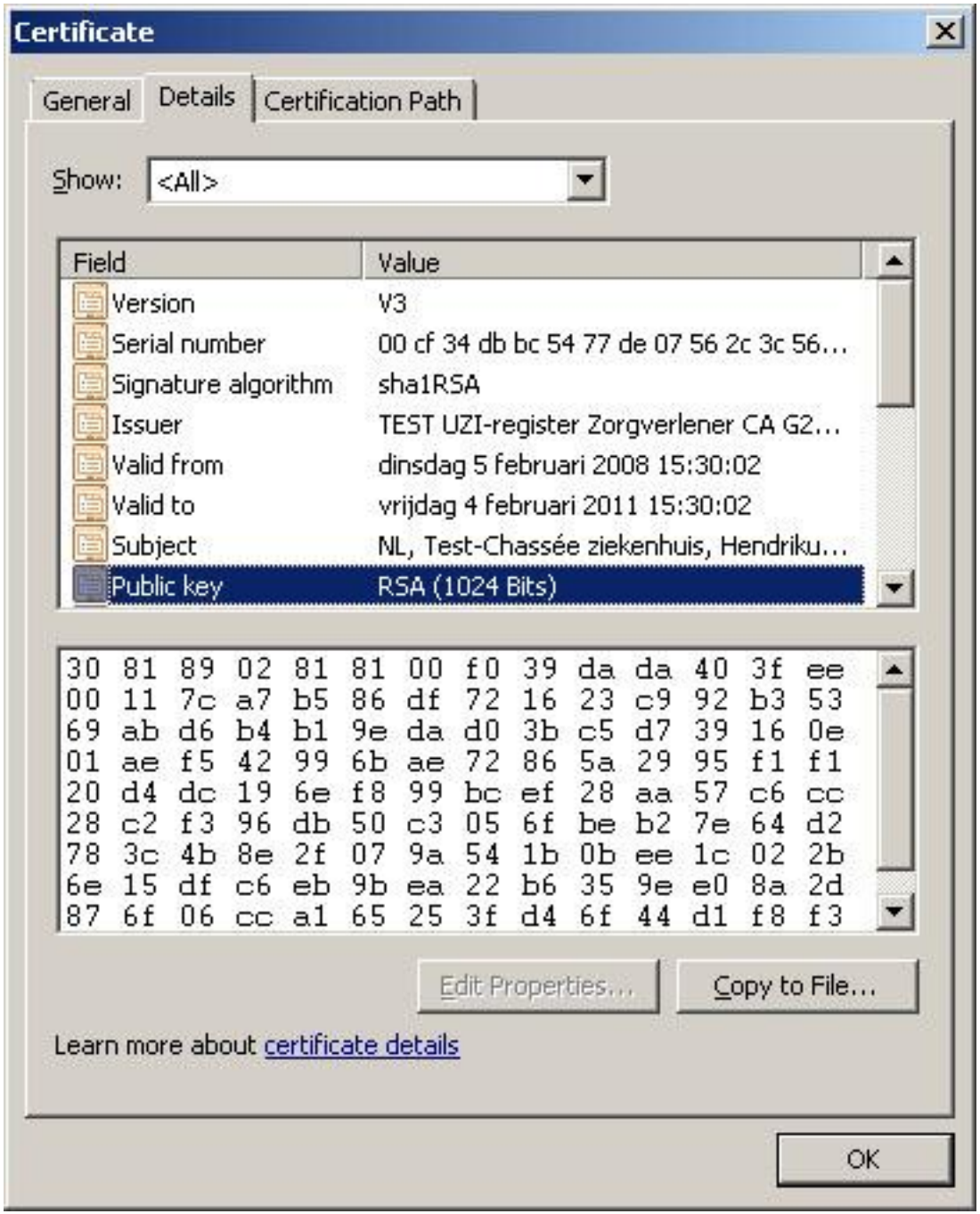
SignedInfo

```
<SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference URI="#token_2.16.528.1.1007.3.3.1234567.1_0123456789">
        <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>4vBP5K5M5llABaWYzxCrKIdjS2I=</DigestValue>
    </Reference>
</SignedInfo>
```

RSA with SHA


SignedInfo
(exc c14n)
bits
SHA1 hash
160 bits
3021300906
052b0e0302
1a05000414
ASN.1 DER
formaat
3031300d06
0960864801
6503040201
05000420
SHA 256 -> 464 bits
400 bits
private key
RSA
408 bits
Base64
karakters
SignatureValue


Sender
Receiver
“Hello world”
“Hello world”
SHA-1 hash:
5llABaWYz
xCrKIdjS...
Public key:
MIICHzCCAY
ygAwIBAgI.....
OK
Private key:
shhhh.....
RSA sig value:
c9fVK7vYAdv
s2DRZVtS...
RSA sig value:
c9fVK7vYAdv
s2DRZVtS...


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

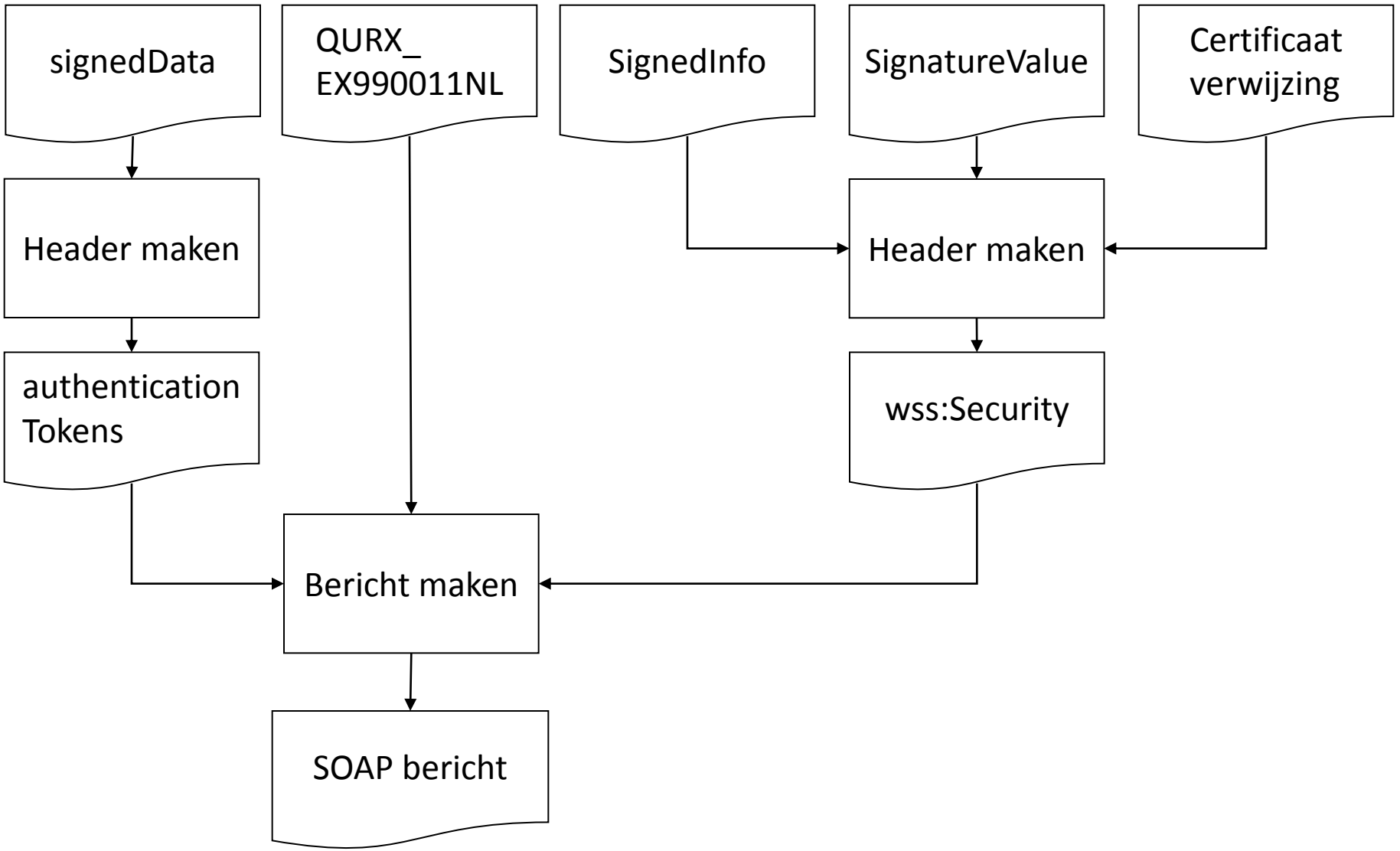
Security services

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

Key usage

Naam	**Key Usage omschrijving**	**Toepassing**	**Key usage hexadecimaal**
authenticiteit-certificaat	digitalSignature	tokenauthenticatie	0x80
handtekening-certificaat	NonRepudiation	elektronische handtekening	0x40
vertrouwelijkheid certificaat	keyEncipherment, dataEncipherment, keyAgreement		0x38 (OR'ed 0x20, 0x10, 0x08)

SOAP bericht

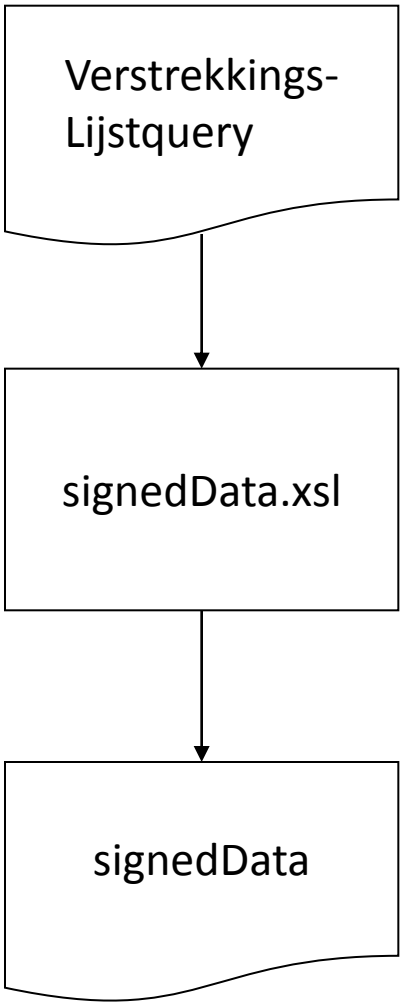


SOAP bericht

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <ao:authenticationTokens xmlns:ao="http://www.aortarelease.nl/805/" soap:mustUnderstand="1">
            <signedData xmlns="http://www.aortarelease.nl/805/" [22 lines]
        </ao:authenticationTokens>
        <wss:Security
            xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
            xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
            soap:mustUnderstand="1">
            <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#"> [10 lines]
                <SignatureValue>TI9mfk0ZgTgURWnh23gFFXV0YtsfE5qPNmJ2c9yelxurErtor4iDZLXiMQ0M4RnL2YjvGygkJ71DnWTBF8BokJ+lGNWCQDa
                <KeyInfo>
                    <wss:SecurityTokenReference>
                        <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                            <ds:X509IssuerSerial>
                                <ds:X509IssuerName>CN=TEST UZI-register Zorgverlener CA G2,
                                    O=agentschap Centraal Informatiepunt Beroepen Gezondheidszorg,
                                    C=NL</ds:X509IssuerName>
                                <ds:X509SerialNumber>327210172562264327138620193674491460601</ds:X509SerialNumber>
                            </ds:X509IssuerSerial>
                        </ds:X509Data>
                    </wss:SecurityTokenReference>
                </KeyInfo>
            </Signature>
        </wss:Security>
    </soap:Header>
    <soap:Body>
        <QURX_IN990011NL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:schemaLocation="urn:hl7-org:v3 ../schemas/QURX_IN990011NL.xsd"
            xmlns="urn:hl7-org:v3">
            <id extension="0123456789" root="2.16.528.1.1007.3.3.1234567.1"/>
            <creationTime value="200501281736"/>
            <versionCode code="NICTIZEd2005-Okt"/>
            <interactionId extension="QURX_IN990011NL" root="2.16.840.1.113883.1.6"/>
```

Functie	Algoritme	URI
Signature	RSA+SHA-1	`<SignatureMethod Algorithm= "http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>`
Digest	SHA-1	`<DigestMethod Algorithm= "http://www.w3.org/2000/09/xmldsig#sha1"/>`
Signature	RSA+SHA-256	`<SignatureMethod Algorithm= "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>`
Digest	SHA-256	`<DigestMethod Algorithm= "http://www.w3.org/2001/04/xmlenc#sha256"/>`

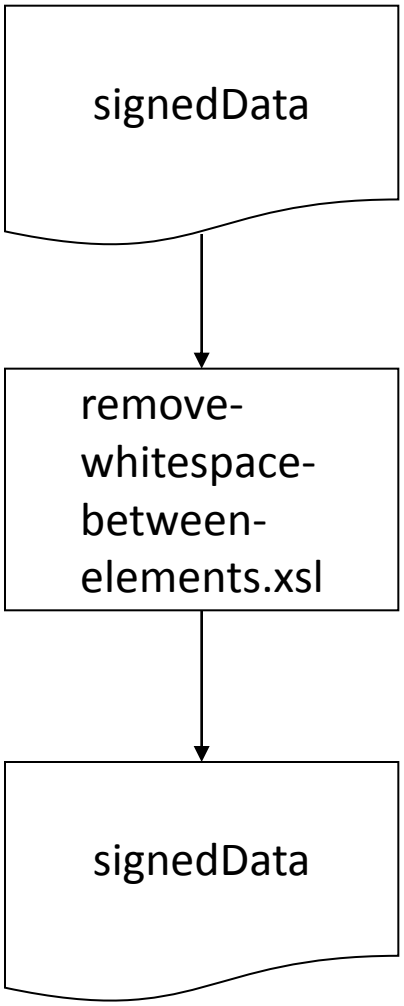
Transformatie XML 2 SignedData



QURX_IN990111NL_01.xml

QURX_IN990111NL_01_signedData.xml

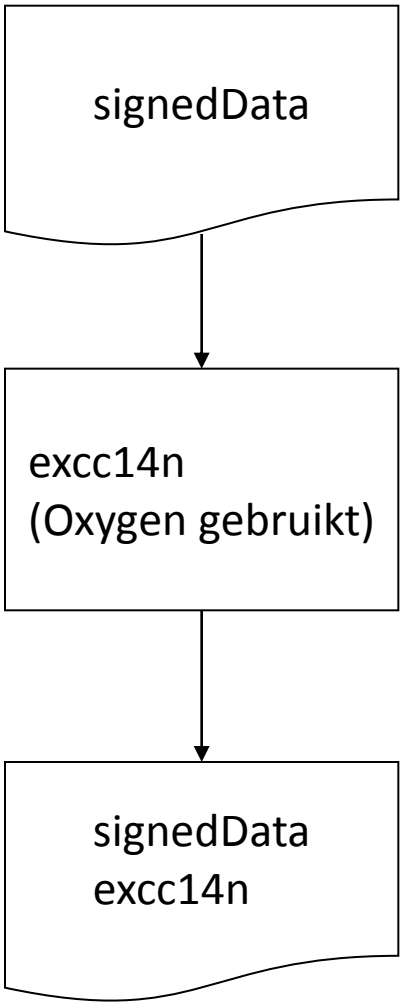
Whitespace eruit



QURX_IN990111NL_01_signedData.xml

QURX_IN990111NL_01_signedData.xml

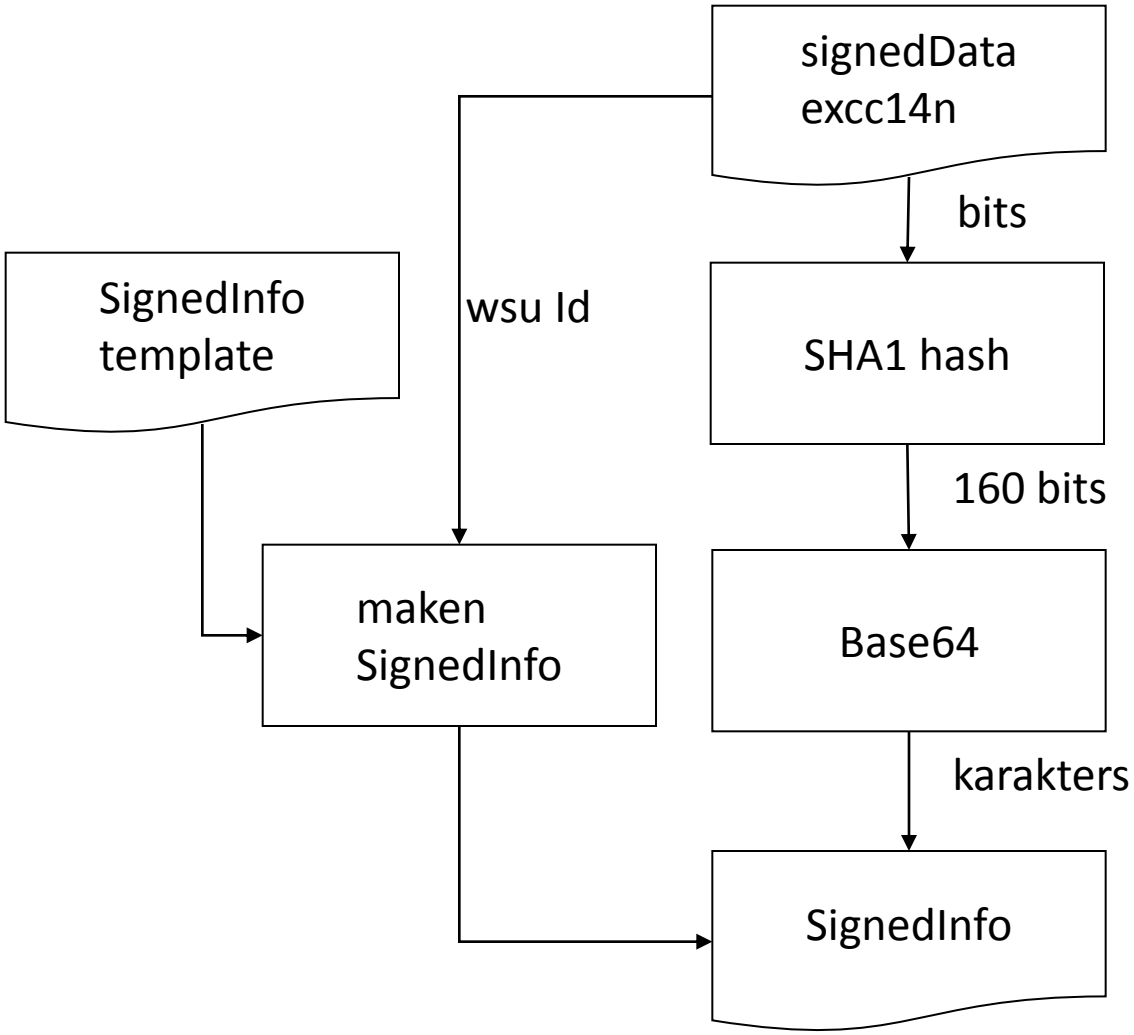
Exclusive Canonicalization



QURX_IN990111NL_01_signedData.xml

signedData_ excc14n.xml

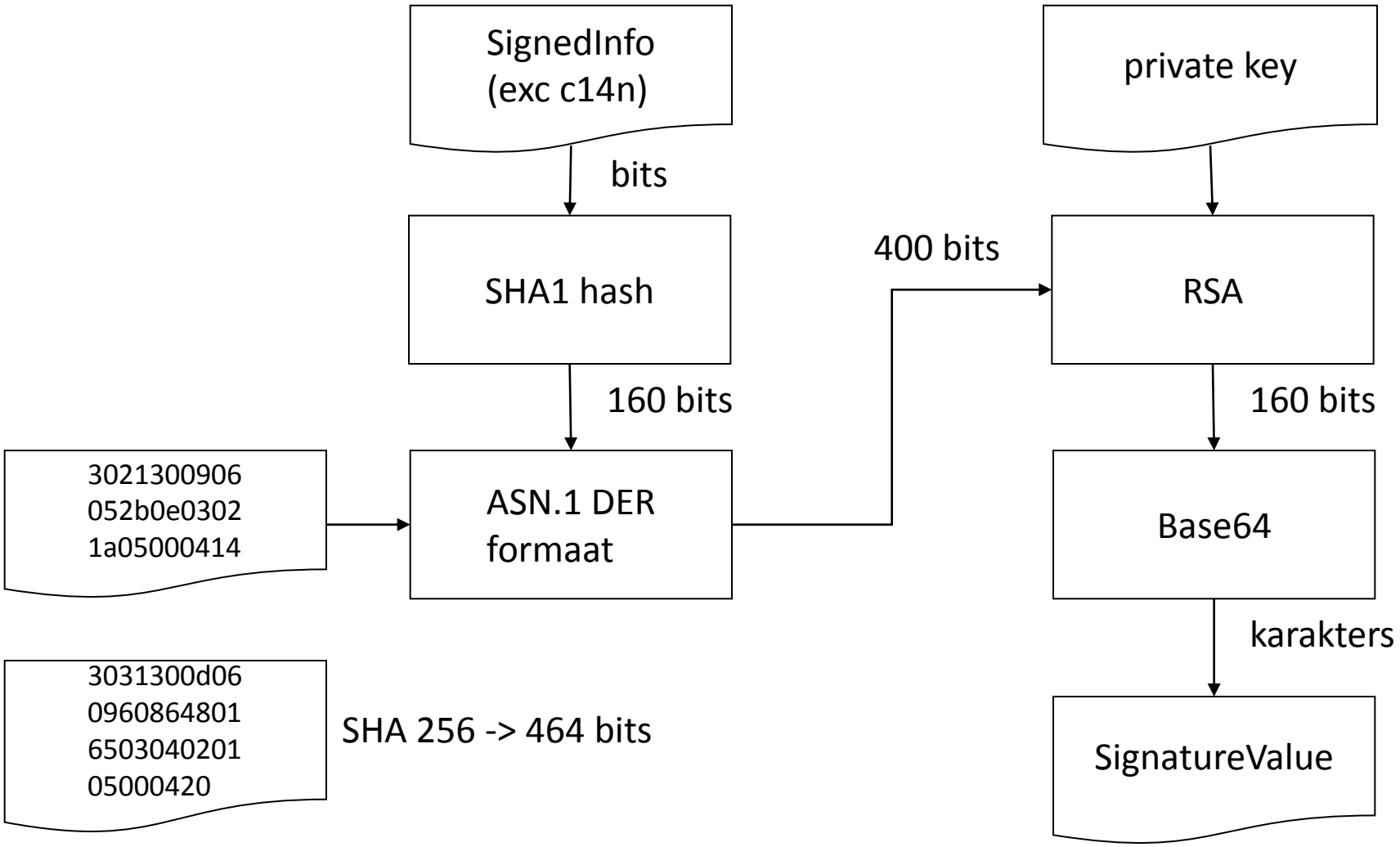
Signed Info element



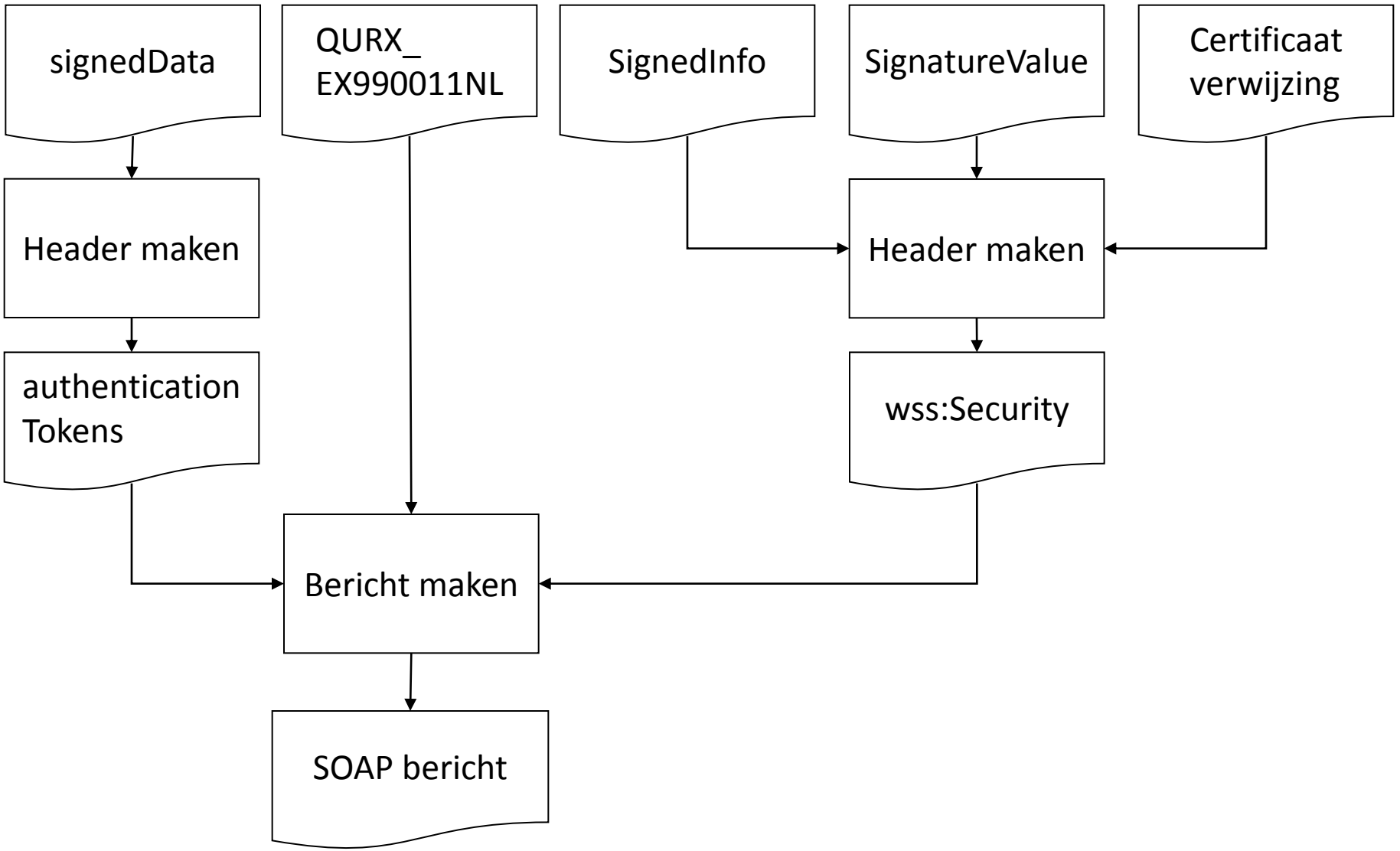
signedData_ excc14n.xml

SignedInfo.xml

RSA with SHA


SignedInfo
(exc c14n)
bits
SHA1 hash
160 bits
3021300906
052b0e0302
1a05000414
ASN.1 DER
formaat
3031300d06
0960864801
6503040201
05000420
SHA 256 -> 464 bits
400 bits
private key
RSA
160 bits
Base64
karakters
SignatureValue

SOAP bericht



Tokenauthenticatie