1 Exempel på att kontrollera XML-signatur manuellt

Detta är exempel på hur man kan kontrollera en XML-signatur enbart med enkla kommandoradsverktyg i Linux. Exemplen är avsedda att öka förståelsen hur signaturberäkningarna görs och kan även användas för felsökning. Det är också möjligt att skapa signaturer med utgångspunkt från exemplen.

Exemplen använder reguljära uttryck som inte är anpassade för generell användning utan enbart för dessa exempel.

1.1 Koncept

Signaturen beräknas på SignedInfo.

SignedInfo innehåller checksummor på och referenser till de delar som ska ”låsas”, i exemplet KeyInfo (använt signeringscertifikat), Payload (dokumentet) och SignedProperties (XAdES-tilläggen).

Allmän information finns på *Tullverket.se – Företag – Framtida tullhantering – IT-system*, http://www.tullverket.se/sv/foretag/framtidatullhantering/itsystem.4.226de36015804b8cf353005.html samt *Tullverket.se – Företag – Framtida tullhantering – IT-system – Tekniska specifikationer – Tullager, tekniska specifikationer*, http://www.tullverket.se/sv/foretag/framtidatullhantering/itsystem/itsystemtekniskaspecifikationer/tullagertekniskaspecifikationer.4.226de36015804b8cf353024.html

Paket för nedladdning med kuvertspecifikationer, XML-scheman och exempelfiler finns på *Tullverket.se – Företag – Framtida tullhantering – IT-system – Tekniska specifikationer – Tullager, tekniska specifikationer – Kuvert_1.0*,

http://www.tullverket.se/download/18.5c3d004415b89fa6ac7148/1493729103994/SCTS-ENV_2017-05-02.zip

I den packade filen http://www.tullverket.se/download/18.5c3d004415b89fa6ac7148/1493729103994/SCTS-ENV_2017-05-02.zip

finns bland annat den exempelfil, ENV-Envelope-UseCase1.xml, som används i nedanstående exempel.

För att visa dokumentet i ett mer läsbart format (som dock förstör signaturen):

xmllint --format ENV-Envelope-UseCase1.xml

1.2 Exklusiv kanonisering av deldokument

Exklusiv kanonisering görs i exemplen med xmllint --exc-c14n, men eftersom denna utförs på hela filen istället för på det deldokument som ska checksummeberäknas blir resultatet inte korrekt. För att den ”manuella” checksummeberäkningen skall bli rätt måste namespace ändras enligt följande exempel:

Original:

```
<ds:SignedInfo>
```

Efter kanonisering av hela filen:

```
<ds:SignedInfo>
```

Efter ”korrigering”:

```
<ds:SignedInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

1.3 Kontrollera checksumma för deldokument KeyInfo

Börja med att beräkna checksumman på deldokument KeyInfo:

```
xmllint --exc-c14n ENV-Envelope-UseCase1.xml | sed
's+<ds:KeyInfo+<ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"+' | awk
'/<ds:KeyInfo/,/<\/ds:KeyInfo>/' | sed
's/.*<ds:KeyInfo/<ds:KeyInfo/' | sed
's/<\/ds:KeyInfo>.*/<\/ds:KeyInfo>/' | xmllint --exc-c14n - |
openssl dgst -sha256
```

Resultat:

```
(stdin)=
b78c611113a0624653ca6c650996bba7a95a45daa20b6a6b6dc90b09c2d81fb0
```

Extrahera den angivna checksumman (DigestValue) för KeyInfo från SignedInfo:

```
awk '/<ds:Reference .*KeyInfo/,/<\/ds:Reference>/' ENV-Envelope-
UseCase1.xml | awk '/<ds:DigestValue/,/<\/ds:DigestValue/' | sed
's/.*<ds:DigestValue>//' | sed 's/<\/ds:DigestValue>.*//' |
openssl enc -d -a -A | xxd -p -c256
```

Resultat:

```
b78c611113a0624653ca6c650996bba7a95a45daa20b6a6b6dc90b09c2d81fb0
```

Checksumman för KeyInfo stämmer alltså överens med den angivna checksumman för KeyInfo i SignedInfo.

1.4 Kontrollera checksumma för deldokument Payload

Observera att detta är ”ett hack”, skilj mellan Object (Payload) från Object (xades)! Exklusiv kanonisering "#WithComments" är tyvärr hårdkodad i programmet xmllint, vilket gör att kommentaren i exempelfilen måste tas bort (<\!--.*-->).

Börja med att beräkna checksumman på deldokument Payload:

```
xmllint --exc-c14n ENV-Envelope-UseCase1.xml | sed 's+<ds:Object
+<ds:Object xmlns:ds="http://www.w3.org/2000/09/xmldsig#" +' | awk
'/<ds:Object .*Payload/,/<\/ds:Object>/' | sed 's/.*<ds:Object
/<ds:Object /' | sed 's/<\/ds:Object>.*/<\/ds:Object>/' | sed
's/<\!--.*-->//' | xmllint --exc-c14n - | openssl dgst -sha256
```

Resultat:

```
(stdin)=
a4b09417c50be236b74d55659b5ee6884f0697c49ea72280c62a0b56f6e2cb34
```

Extrahera den angivna checksumma för Payload från SignedInfo:

```
awk '/<ds:Reference .*Payload/,/<\/ds:Reference>/' ENV-Envelope-
UseCase1.xml | awk '/<ds:DigestValue/,/<\/ds:DigestValue/' | sed
's/.*<ds:DigestValue>//' | sed 's/<\/ds:DigestValue>.*//' |
openssl enc -d -a -A | xxd -p -c256
```

Resultat:

```
a4b09417c50be236b74d55659b5ee6884f0697c49ea72280c62a0b56f6e2cb34
```

Checksumman för Payload stämmer alltså överens med den angivna checksumman för Payload i SignedInfo.

1.5 Kontrollera checksumma för deldokument SignedProperties

Börja med att beräkna checksumman på deldokument SignedProperties:

```
xmllint --exc-c14n ENV-Envelope-UseCase1.xml | sed
's+<xades:SignedProperties +<xades:SignedProperties
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" +' | awk
'/<xades:SignedProperties/,/<\/xades:SignedProperties>/' | sed
's/.*<xades:SignedProperties /<xades:SignedProperties /' | sed
's/<\/xades:SignedProperties>.*/<\/xades:SignedProperties>/' |
xmllint --exc-c14n - | openssl dgst -sha256
```

Resultat:

```
(stdin)=
435a84b43223396641b8a6ef55920fe1cd8e2ba2ddabb84371e889f37df73274
```

Extrahera den angivna checksumma för SignedProperties från SignedInfo:

```
awk '/<ds:Reference .*SignedProperties/,/<\/ds:Reference>/' ENV-
Envelope-UseCase1.xml | awk
'/<ds:DigestValue/,/<\/ds:DigestValue/' | sed
's/.*<ds:DigestValue>//' | sed 's/<\/ds:DigestValue>.*//' |
openssl enc -d -a -A | xxd -p -c256
```

Resultat:

```
435a84b43223396641b8a6ef55920fe1cd8e2ba2ddabb84371e889f37df73274
```

Checksumman för SignedProperties stämmer alltså överens med den angivna checksumman för SignedProperties i SignedInfo.

1.6 Beräkna checksumma för deldokument SignedInfo

Beräkna checksumman som sedan ska jämföras med checksumman som finns i själva signaturen:

```
xmllint --exc-c14n ENV-Envelope-UseCase1.xml | sed
's+<ds:SignedInfo>+<ds:SignedInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">+' | awk
'/<ds:SignedInfo/,/<\/ds:SignedInfo>/' | sed
's/.*<ds:SignedInfo/<ds:SignedInfo/' | sed
's/<\/ds:SignedInfo>.*/<\/ds:SignedInfo>/' | xmllint --exc-c14n -
| openssl dgst -sha256
```

Resultat:

```
(stdin)=
a0b60f20fde784d34654989cf757b6a6052b6ffce096e646a111f97e48a9ab5a
```

1.7 Extrahera publik nyckel från KeyInfo

Den publika nyckeln extraheras från certifikatet som finns i KeyInfo:

```
awk '/<ds:X509Certificate>/,/<\/ds:X509Certificate>/' ENV-
Envelope-UseCase1.xml | sed 's/.*<ds:X509Certificate>//' | sed
's/<\/ds:X509Certificate>.*$//' | awk 'BEGIN {print "-----BEGIN
CERTIFICATE-----"} END {print "-----END CERTIFICATE-----"}
{print}' | fold -b -w 66 | openssl x509 -noout -pubkey > cert.pub
```

Innehåll i cert.pub:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv2eNX34iwor7/Huh7TBJ
144swczaFnjKDcu3qt9nx86EZ2m/aPW6iBYzh2ZO1ILaiAni9nI7Or74WJlmbA52
3qFrabNZZ3pW/dYqDI7RIufSdY59KI1IK8IJ7ZGEjJuPRnhyAlFi2eirKGAUpidi
HqScUMtYpC7vf5ybDuZG5DMz9adT6jtGhNJ5Cra9Pb2R6tOYdgZdeHApDHUxjnrO
gJv7EI83NVtB7+IHjUVwVKGCW26Ff4XX8j/Emq1ICGTh41CUTs6psU6diCEyXvJL
q8RBdoIKpggcIj4AUqQGs3gCCEgBS0VbhnCcx4+HS6cKn5qYZPJ3Bo8zsGRzPhpV
xQIDAQAB
-----END PUBLIC KEY-----
```

1.8 Visa innehåll i certifikatet (vid intresse)

```
awk '/<ds:X509Certificate>/,/<\/ds:X509Certificate>/' ENV-
Envelope-UseCase1.xml | sed 's/.*<ds:X509Certificate>//' | sed
's/<\/ds:X509Certificate>.*$//' | awk 'BEGIN {print "-----BEGIN
CERTIFICATE-----"} END {print "-----END CERTIFICATE-----"}
{print}' | fold -b -w 66 | openssl x509 -text -nameopt multiline
```

Resultat:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            13:86:c7:b8:db:be:52:ce:44:85:aa:38:2a:70:95:b5
    Signature Algorithm: sha256WithRSAEncryption
        Issuer:
            countryName               = SE
            organizationName          = Tullverket
            organizationalUnitName    = Swedish Customs
            organizationalUnitName    = TEST Public Intermediate
Certificate Authority
            organizationalUnitName    = For testing purposes only
            serialNumber              = SE2021000969
            commonName                = Swedish Customs TEST
Public CA 0.1
        Validity
            Not Before: Sep 14 07:23:24 2015 GMT
            Not After : Sep 14 07:23:24 2035 GMT
        Subject:
            countryName               = SE
            organizationName          = Testf\F6retag
            organizationalUnitName    = IT department
            serialNumber              = SE9999999999
```

```
            commonName                = Test company for signature
validation tests
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bf:67:8d:5f:7e:22:c2:8a:fb:fc:7b:a1:ed:30:
                    49:d7:8e:2c:c1:cc:da:16:78:ca:0d:cb:b7:aa:df:
                    67:c7:ce:84:67:69:bf:68:f5:ba:88:16:33:87:66:
                    4e:d4:82:da:88:09:e2:f6:72:3b:3a:be:f8:58:99:
                    66:6c:0e:76:de:a1:6b:69:b3:59:67:7a:56:fd:d6:
                    2a:0c:8e:d1:22:e7:d2:75:8e:7d:28:8d:48:2b:c2:
                    09:ed:91:84:8c:9b:8f:46:78:72:02:51:62:d9:e8:
                    ab:28:60:14:a6:27:62:1e:a4:9c:50:cb:58:a4:2e:
                    ef:7f:9c:9b:0e:e6:46:e4:33:33:f5:a7:53:ea:3b:
                    46:84:d2:79:0a:b6:bd:3d:bd:91:ea:d3:98:76:06:
                    5d:78:70:29:0c:75:31:8e:7a:ce:80:9b:fb:10:8f:
                    37:35:5b:41:ef:e2:07:8d:45:70:54:a1:82:5b:6e:
                    85:7f:85:d7:f2:3f:c4:9a:ad:48:08:64:e1:e3:50:
                    94:4e:ce:a9:b1:4e:9d:88:21:32:5e:f2:4b:ab:c4:
                    41:76:82:0a:a6:08:1c:22:3e:00:52:a4:06:b3:78:
                    02:08:48:01:4b:45:5b:86:70:9c:c7:8f:87:4b:a7:
                    0a:9f:9a:98:64:f2:77:06:8f:33:b0:64:73:3e:1a:
                    55:c5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:

keyid:8B:66:F6:70:E9:0B:D5:9B:21:41:52:38:8F:27:A9:32:89:D2:FF:73

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage:
                Non Repudiation
            X509v3 Subject Key Identifier:

DA:7E:A5:90:D5:DA:54:80:68:60:D4:27:B3:E7:F9:57:F0:54:5D:57
    Signature Algorithm: sha256WithRSAEncryption
         4d:23:74:f7:53:84:a8:51:70:61:c1:70:9a:fa:2c:ae:4c:73:
         fa:ed:f4:6d:9a:d6:57:e5:5f:8a:34:59:e2:34:3a:6e:ca:9b:
         69:87:48:6f:e2:fa:9a:55:01:ea:fc:f0:40:fb:02:ab:48:f4:
         7d:a7:41:ab:05:8e:c5:03:34:5b:a1:c4:47:69:79:3e:56:11:
         da:ef:65:0f:70:b5:42:b3:cf:93:be:38:1c:e9:3e:dc:60:8d:
         a6:12:ec:5b:9d:70:d5:26:60:5b:c5:75:1a:a6:db:3c:95:1a:
         df:3d:3e:cb:67:10:db:90:86:c5:f7:34:82:82:35:a9:38:ed:
         ab:fc:4d:b2:5a:ea:dd:9f:04:24:18:36:00:f0:b3:df:6a:d8:
```

```
        1e:ff:86:d0:17:6b:c7:08:45:b8:82:2d:12:70:e7:4e:12:5c:
        19:49:5e:f8:50:33:36:83:ef:c2:f0:07:20:1f:91:07:fd:73:
        fa:16:f3:cb:93:13:95:85:5a:18:8e:c3:e3:0e:00:89:15:3a:
        7e:72:20:ed:5a:42:88:94:91:54:0f:6f:b4:fc:18:9a:37:62:
        27:ac:d4:98:f3:a9:ee:a6:08:79:c5:fd:fe:f6:5a:f0:2e:a7:
        81:99:65:d7:59:59:39:f2:80:cd:4b:77:2b:0e:99:16:01:56:
        aa:74:df:33
-----BEGIN CERTIFICATE-----
MIIETzCCAzegAwIBAgIQE4bHuNu+Us5Ehao4KnCVtTANBgkqhkiG9w0BAQsFADCB
3TELMAkGA1UEBhMCU0UxEzARBgNVBAoMClR1bGx2ZXJrZXQxGDAWBgNVBAsMD1N3
ZWRpc2ggQ3VzdG9tczE3MDUGA1UECwwuVEVTVCBQdWJsaWMgSW50ZXJtZWRpYXRl
IENlcnRpZmljYXRlIEF1dGhvcml0eTEiMCAGA1UECwwZRm9yIHRlc3RpbmcgcHVy
cG9zZXMgb25seTEVMBMGA1UEBRMMU0UyMDIxMDAwOTY5MSswKQYDVQQDDCJTd2Vk
aXNoIEN1c3RvbXMgVEVTVCBQdWJsaWMgQ0EgMC4xMB4XDTE1MDkxNDA3MjMyNFoX
DTM1MDkxNDA3MjMyNFowgYkxCzAJBgNVBAYTAlNFMRUwEwYDVQQKDAxUZXN0ZsO2
cmV0YWcxFjAUBgNVBAsMDUlUIGRlcGFydG1lbnQxFTATBgNVBAUTDFNFOTk5OTk5
OTk5OTE0MDIGA1UEAwwrVGVzdCBjb21wYW55IGZvciBzaWduYXR1cmUgdmFsaWRh
dGlvbiB0ZXN0czCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL9njV9+
IsKK+/x7oe0wSdeOLMHM2hZ4yg3Lt6rfZ8fOhGdpv2j1uogWM4dmTtSC2ogJ4vZy
Ozq++FiZZmwOdt6ha2mzWWd6Vv3WKgyO0SLn0nWOfSiNSCvCCe2RhIybj0Z4cgJR
YtnoqyhgFKYnYh6knFDLWKQu73+cmw7mRuQzM/WnU+o7RoTSeQq2vT29kerTmHYG
XXhwKQx1MY56zoCb+xCPNzVbQe/iB41FcFShgltuhX+F1/I/xJqtSAhk4eNQlE7O
qbFOnYghMl7yS6vEQXaCCqYIHCI+AFKkBrN4AghIAUtFW4ZwnMePh0unCp+amGTy
dwaPM7Bkcz4aVcUCAwEAAaNdMFswHwYDVR0jBBgwFoAUi2b2cOkL1ZshQVI4jyep
MonS/3MwDAYDVR0TAQH/BAIwADALBgNVHQ8EBAMCBkAwHQYDVR0OBBYEFNp+pZDV
2lSAaGDUJ7Pn+VfwVF1XMA0GCSqGSIb3DQEBCwUAA4IBAQBNI3T3U4SoUXBhwXCa
+iyuTHP67fRtmtZX5V+KNFniNDpuyptph0hv4vqaVQHq/PBA+wKrSPR9p0GrBY7F
AzRbocRHaXk+VhHa72UPcLVCs8+Tvjgc6T7cYI2mEuxbnXDVJmBbxXUapts8lRrf
PT7LZxDbkIbF9zSCgjWpOO2r/E2yWurdnwQkGDYA8LPfatge/4bQF2vHCEW4gi0S
cOdOElwZSV74UDM2g+/C8AcgH5EH/XP6FvPLkxOVhVoYjsPjDgCJFTp+ciDtWkKI
lJFUD2+0/BiaN2InrNSY86nupgh5xf3+9lrwLqeBmWXXWVk58oDNS3crDpkWAVaq
dN8z
-----END CERTIFICATE-----
```

1.9 Kontrollera signaturen

Extrahera binär signatur till signaturevalue.bin:

```
awk '/<ds:SignatureValue>/,/<\/ds:SignatureValue>/' ENV-Envelope-
UseCase1.xml | sed 's/.*<ds:SignatureValue>//' | sed
's/<\/ds:SignatureValue>.*$//' | tr -d '\n' | openssl enc -d -a -A
-out signaturevalue.bin
```

Verifiera signatur:

```
openssl rsautl -verify -inkey cert.pub -in signaturevalue.bin -
pubin -asn1parse
```

Resultat:

```
    0:d=0  hl=2 l=  49 cons: SEQUENCE
    2:d=1  hl=2 l=  13 cons:  SEQUENCE
    4:d=2  hl=2 l=   9 prim:   OBJECT            :sha256
   15:d=2  hl=2 l=   0 prim:   NULL
   17:d=1  hl=2 l=  32 prim:  OCTET STRING
      0000 - a0 b6 0f 20 fd e7 84 d3-46 54 98 9c f7 57 b6 a6   ...
....FT...W..
      0010 - 05 2b 6f fc e0 96 e6 46-a1 11 f9 7e 48 a9 ab 5a
.+o....F...~H..Z
```

Presentera checksumman från signaturen mer lättläst än ovanstående:

```
openssl rsautl -verify -inkey cert.pub -in signaturevalue.bin -
pubin -asn1parse | grep '-' | cut -b14-60 | tr '-' ' ' | xxd -r -p
| xxd -p -c256
```

Resultat:

```
a0b60f20fde784d34654989cf757b6a6052b6ffce096e646a111f97e48a9ab5a
```

Jämför checksumman för deldokument SignedInfo med den extraherade checksumman från signaturen:

```
(stdin)=
a0b60f20fde784d34654989cf757b6a6052b6ffce096e646a111f97e48a9ab5a
```

```
a0b60f20fde784d34654989cf757b6a6052b6ffce096e646a111f97e48a9ab5a
```

Checksummorna stämmer överens, alltså är själva signaturen korrekt.

1.10 Slutsatser

I ovanstående exempel görs inga kontroller av dokumentinnehåll eller av certifikatets giltighet.

För ENV-Envelope-UseCase1.xml stämmer samtliga beräkningar och vi kan då dra slutsatsen att dokumentet är oförändrat och signerats med det bifogade certifikatet.

2 Alternativ metod för signaturkontroll med xmlsec

Xmlsec är ett C-bibliotek för XML-signatur och som även innehåller ett hjälpprogram, xmlsec1, som används i nedanstående exempel. För mer information, se https://www.aleksey.com/xmlsec/index.html. Observera att version 1.2.20 inte verkar fungera som den ska, det verkar däremot version 1.2.21 och 1.2.22 göra.

2.1 Testcertifikathierarki

Exempelfilen ENV-Envelope-UseCase1.xml har skapats med följande rot- och CA-certifikat, som inte skall användas till annat än för nedanstående exempel.

Rotcertifikat, rotcertifikat.pem:

```
subject= /C=SE/O=Tullverket/OU=Swedish Customs/OU=TEST Root
Certificate Authority/serialNumber=SE2021000969/CN=Swedish Customs
TEST Root CA 0.1
issuer= /C=SE/O=Tullverket/OU=Swedish Customs/OU=TEST Root
Certificate Authority/serialNumber=SE2021000969/CN=Swedish Customs
TEST Root CA 0.1
notBefore=Sep 14 07:23:22 2015 GMT
notAfter=Sep 14 07:23:22 2035 GMT
serial=8E76B5668CD1E639134754593E9B9E09
-----BEGIN CERTIFICATE-----
MIIGHzCCBAegAwIBAgIRAI52tWaM0eY5E0dUWT6bngkwDQYJKoZIhvcNAQELBQAw
gagxCzAJBgNVBAYTAlNFMRMwEQYDVQQKDApUdWxsdmVya2V0MRgwFgYDVQQLDA9T
d2VkaXNoIEN1c3RvbXMxKDAmBgNVBAsMH1RFU1QgUm9vdCBDZXJ0aWZpY2F0ZSBB
dXRob3JpdHkxFTATBgNVBAUTDFNFMjAyMTAwMDk2OTEpMCcGA1UEAwwgU3dlZGlz
aCBDdXN0b21zIFRFU1QgUm9vdCBDQSAwLjEwHhcNMTUwOTE0MDcyMzIyWhcNMzUw
OTE0MDcyMzIyWjCBqDELMAkGA1UEBhMCU0UxEzARBgNVBAoMClR1bGx2ZXJrZXQx
GDAWBgNVBAsMD1N3ZWRpc2ggQ3VzdG9tczEoMCYGA1UECwwfVEVTVCBSb290IENl
cnRpZmljYXRlIEF1dGhvcml0eTEVMBMGA1UEBRMMU0UyMDIxMDAwOTY5MSkwJwYD
VQQDDCBTd2VkaXNoIEN1c3RvbXMgVEVTVCBSb290IENBIDAuMTCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBALDJE/AO4zoEVU40KXiTd73mylR2V+0ZrBQX
EHbgC65so51GvDqYjYGihQ9D2ka5mTJLadeDGHvSN6KwJZqYpqE76M3ULyZ7F546
NeOPNxqTJyON89AT0HJELmCedjNQ7P+D4sHXgE28AfkSMtSP1K7Osd9gBMGSzvg+
uIp8MEJRvvfAxzULc564VcbrU99wK1JeYwCtwDTbhAfd87cUumLXUvoSHPylres5
DLu5GWo1eWxu7YAJKOsDZXWtLFhcN/Zhx2mfl+i7SBYNzrmhAQL7P1L0MyR2/aMC
NceWcya0gjN2gHq6YrAHkZ0vzHYduFvaLdXDI5IuEuXjBW7EMBtMIH0evJohQ5e3
+5kiqnEBinBNqCma+pkQMJRGMqsfaWe6Qnq6k6bJqxpevqMzOPnl3UWfD388/X3j
It2uO3Z1fp+bvUg7/yT2gPACe0YS7kM0IfTnU5Mve167RKCTh3yr9atDh8ebA30T
LaKlDXFLiRT4ZRI9bhfYQ3tGU6dap9RTqmlkBQ/eSfNsGDmtVSUK0TLKY0MEXrQL
YtYSA4ugY2O5YK+oOP+nUN/fy2eJw3Red6r0dO2nfUiWATt3qti0xQZxdyQvatrd
aDbr2u6UjMklh7LfnCDbrYdU92njlEXeYyufVIesQn8MewJ04/fVU2SHhRNguB3F
m74Cwd4BAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEG
```

MB0GA1UdDgQWBBSkTttsqJ6iUwwy+03e9X3Q+i3WaTANBgkqhkiG9w0BAQsFAAOC
AgEAZ4baoE0kWXKfeL8n1HalzsP7ChYRHV/vBnH6L5li1EnIIfNjRk1ib+Ki5k0r
5D5rJBv1ywb6Z1Y0TiH8sjJm1VLtceVnp7gBWPd4Y7ZWPt3905hrWWYuEViJz/bT
qe7nRltnlzEhdpn4BsB7FF0zTypsWDb6mV7BjHMW+wE+XTh4Uo+ZUO52gC2qbey5
1GfktLRCB43M3Bsm/AOC8SD+y1Fe/6Rq3zsYJl9+m7zySUz6cP33jTIchjDdtAR8
l7u0yFUijnAxmdP+mtkLk6uiHsAtCTx0q3fRVR/bJ9TSC8XTfwelMWOIoP/aYMiF
92dNS6ff/774iu1pmaucwE1kHpDtKVeiX/5Hmd63+nYNkErjjVobq3wxUccs22Rg
UaQKTzkdbecaQKvVgwJk4WNvyRMkS2wK/Yl2APnq5p5hkdlGR4FE2vsL/AQEnzBZ
VCYjn1RF8FA/UOMx3LFxWBmUAOKUSJA43p4QQk/IqwwPjGazWuG7n+eUTyiIU7xz
MD5+h1Z8cvf/QiGcXJ0xZnCVLgx+AiyEIellOnLJCVcRpdcsi+zolCK9cVpDHn96
y/on4GJ2Pkn2iRU0g5kQn7EKSDi3dHmRDCvW1d1YnQNQXok8nAvpfGGqjzMounRh
Lz8H/yopv1TWNPwisplQFbVqzWJ6LGLWPlb4itPVo2A75Ok=
-----END CERTIFICATE-----

CA-certifikat, cacertifikat.pem:

subject= /C=SE/O=Tullverket/OU=Swedish Customs/OU=TEST Public Intermediate Certificate Authority/OU=For testing purposes only/serialNumber=SE2021000969/CN=Swedish Customs TEST Public CA 0.1
issuer= /C=SE/O=Tullverket/OU=Swedish Customs/OU=TEST Root Certificate Authority/serialNumber=SE2021000969/CN=Swedish Customs TEST Root CA 0.1
notBefore=Sep 14 07:23:23 2015 GMT
notAfter=Sep 14 07:23:23 2035 GMT
serial=DE43DA6EF65CA1F345CCCCA5130D1486
-----BEGIN CERTIFICATE-----
MIIFeDCCA2CgAwIBAgIRAN5D2m72XKHzRczMpRMNFIYwDQYJKoZIhvcNAQELBQAw
gagxCzAJBgNVBAYTAlNFMRMwEQYDVQQKDApUdWxsdmVya2V0MRgwFgYDVQQLDA9T
d2VkaXNoIEN1c3RvbXMxKDAmBgNVBAsMH1RFU1QgUm9vdCBDZXJ0aWZpY2F0ZSBB
dXRob3JpdHkxFTATBgNVBAUTDFNFMjAyMTAwMDk2OTEpMCcGA1UEAwwgU3dlZGlz
aCBDdXN0b21zIFRFU1QgUm9vdCBDQSAwLjEwHhcNMTUwOTE0MDcyMzIzWhcNMzUw
OTE0MDcyMzIzWjCB3TELMAkGA1UEBhMCU0UxEzARBgNVBAoMClR1bGx2ZXJrZXQx
GDAWBgNVBAsMD1N3ZWRpc2ggQ3VzdG9tczE3MDUGA1UECwwuVEVTVCBQdWJsaWMg
SW50ZXJtZWRpYXRlIENlcnRpZmljYXRlIEF1dGhvcml0eTEiMCAGA1UECwwZRm9y
IHRlc3RpbmcgcHVycG9zZXMgb25seTEVMBMGA1UEBRMMU0UyMDIxMDAwOTY5MSsw
KQYDVQQDDCJTd2VkaXNoIEN1c3RvbXMgVEVTVCBQdWJsaWMgQ0EgMC4xMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw1B+jd+wl+gRai3WTur100oqBhJV
Y9idswXgW27CSW9UraffJD5LXLP4wUqXVo6fDiZ0/Yy/WL4jXJ90lNxh9YReVH2W
xEvtzySOEG3vejByGiZE7oVFla+EL2ggSSbGX+ByEsWvLsGbMgZ/XjgCiyvwHqBk
5xu92gQI0dF3mq1xE3ZjGlueUrkFI+yCHaNQBd+yaOW3/4zres79cq9SeZNCJTkF
cESvTefILGekLwOFcJhwAWINAX/6OOkgtCWZc3hXkrDtIMm38q28PvwJpPm8OF2V
9KPFx1ljcmx/NKzhT5IPNM8qMC5OX+ZzaZWJcXKvP4X3JKDVU4U1ePy4XQIDAQAB
o2YwZDAfBgNVHSMEGDAWgBSkTttsqJ6iUwwy+03e9X3Q+i3WaTASBgNVHRMBAf8E
CDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUi2b2cOkL1ZshQVI4
jyepMonS/3MwDQYJKoZIhvcNAQELBQADggIBAG/8kVdonKy573wzgDlPHQYUOhGT

```
Az+Em4jBNKblTWXwNOFxM9T7AuNyz1c0dKmXiSq9gAFWgMiIdcNrTcbKlIRvayuz
B7F29I/lP4uISdCv6puL3QtOZ6xeVvsIIOCXu1MQyb639c9vY+GZ71Bqj1QLAPZN
kyi2UlmrShAd7Sh8UAe/Lf92Pc503eC7Afu3tLWGOLTzIWmNSnLbvIXZ+9c1fqIU
GfRFG2jTAugbDma8UEaEfiK/fj1eN3oylaXxdSvF9UnrzC59IdTlgmHO9q/fW6R2
b40F5mn84YqKCmOzvOi/r1M2RrPju+0wwHAj12ojQX1H+ws7gMS7mI8tA4YUpToQ
oMOIYcaaeIFn69OzdqhDiueoU77ckoIALSNtW8pTCC3qf5bq8mICF2IDJKhTN8WE
CEmxl3FTDz+7VQzKHBxMqzJRlXp8jrqyaXy3GyHvXxUg91OKM4ptb+QI2B0r/cur
Ro17lIX0GDwI3MzTBKZdr98vvQNBkkhOOmJVmQnjDtkp5YXMrkArIv2xPm65Hf3m
ak1nuiiHEUXa5Wa7OQn+R2SCaKrf1sK62bwys2Ga3gpLEhxivGoc48/ezjuFzUDn
D9PYjB2Yrne6p/316diRfy3X43PhHufISUKVrNGeLg+OmAK+jQFNP8FdtRHyq+Yt
ysyAmNlQVUGgJYH0
-----END CERTIFICATE-----
```

2.2 Kontroll av signatur med xmlsec

```
xmlsec1 --verify --trusted-pem rotcertifikat.pem  --trusted-pem
cacertifikat.pem ENV-Envelope-UseCase1.xml
```

Resultat:

```
OK
SignedInfo References (ok/all): 3/3
Manifests References (ok/all): 0/0
```

2.3 Skapa signatur med xmlsec

Det går även att skapa signaturer med xmlsec. Då utgår man från en mallfil med rätt struktur men där de variabla delarna som hör till signaturen är ersatta med tomma element, <ds:DigestValue/>, <ds:SignatureValue/> och <ds:X509Certificate/>. Observera att version 1.2.20 inte verkar fungera som den ska, det verkar däremot version 1.2.21 och 1.2.22 göra.

Exempel:

```
xmlsec1 --sign --output signerad_fil.xml --pkcs12
certifikat_och_privat_nyckel.p12 --pwd lösenordp12
osignerad_fil.xml
```