Digital Signatures (XAdES)

University of Tartu

Spring 2019
Article 3:
(10) ‘electronic signature (ES)’ means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
(11) ‘advanced electronic signature (AdES)’ means an electronic signature which meets the requirements set out in Article 26 (uniquely linked to the signatory);
(12) ‘qualified electronic signature (QES)’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

Article 25:
2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

---

Estonian Digital Signature – QES

No card readers found

Container: /home/user/Downloads/Rahvusvahelise sanktsiooni seadus.bdoc

Container files

VP_07032019_0419.rtf

Container signatures

KERSTI KALJULAID - Signature is valid
46912302711 - Signed on 07. March 2019 at 14:38

SIGN WITH MOBIIL-ID
Legal Effect of Qualified Electronic Signature

The same as of a handwritten signature
• Can be used to sign contracts
  • Most of the contracts do not have to be in writing
• Must be used to sign legal acts
• Can be used in court as a proof
  • Can unsigned e-mails be used as a proof?

Code of Civil Procedure:
§ 277. Contestation of authenticity of documents
(3) Authenticity of an electronic document bearing a digital signature may be contested only by substantiating the circumstances which give reason to presume that the document has not been prepared by the holder of the digital signature.
• What could be these circumstances?
Qualified Trust Service Provider (QTSP) – CA

- Only QTSP may issue qualified certificate for electronic signature
- Qualified status granted by supervisory body
  - Estonian Information System Authority (RIA)

Article 22
1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

- EU-level PKI
Qualified Electronic Signature Creation Device (QSCD)

ANNEX II
1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
   (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
   (b) the electronic signature creation data used for electronic signature creation can practically occur only once;
   (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
   (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

Security certification according to Common Criteria EAL4+

- EN 419 211 - Protection profiles for secure signature creation device²

Validation of Qualified Electronic Signature

Article 32
1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:
   (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;
   (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
   (c) the signature validation data corresponds to the data provided to the relying party;
   (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
   (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
   (f) the electronic signature was created by a qualified electronic signature creation device;
   (g) the integrity of the signed data has not been compromised;
   (h) the requirements provided for in Article 26 were met at the time of signing.

DigiDoc software verifies QES validity according to these requirements
Trusted Timestamping

Article 3:
(33) ‘electronic time stamp’ means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;


Signed statement of timestamping authority (TSA):
> This data [data] was presented to me at this time: [time]
> --
> TSA [signature]

QES file container contains:
- Signed files
- Signature of files
- Signer’s certificate
- Timestamp of the signature
  - Proves that signature was given before the time specified
- OCSP response (acquired after timestamping)
  - Proves that certificate was valid after the signature was given

Does this provide long-term validity?
Digital Signature File Formats

Advanced electronic signature (AdES) file format specifications to be recognised by public sector bodies:

- **XML** – XAdES Baseline Profile (ETSI TS 103171)
  - Used in Estonia (.asice/.bdoc/.ddoc formats)
- **CMS** – CAdES Baseline Profile (ETSI TS 103173)
- **PDF** – PAdES Baseline Profile (ETSI TS 103172)

   Implemented using Associated Signature Container (ASiC) Baseline Profile (ETSI TS 103174)

asic-container.asice: Zip ("application/vnd.etsi.asic-e+zip")
   + mimetype
   + document.docx
   + META-INF/manifest.xml
   + META-INF/signatures0.xml
   + META-INF/signatures1.xml

---

XML Signature (ASICE)

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<asic:XAdESSignatures xmlns:asic="http://uri.etsi.org/02918/v1.2.1#" [...]>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="S1">
  <ds:SignedInfo Id="S1-SignedInfo">
    <ds:Reference Id="S1-ref-1" URI="document.docx">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>SJO7h/iCeb9jDLXMZ6qEx8nYkhNR+MWBLge6YfyU7+U=/</ds:DigestValue>
    </ds:Reference>
    <ds:Reference Id="S1-ref-SignedProperties" Type="http://uri.etsi.org/01903#SignedProperties" URI="#S1-SignedProperties">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>qRlc2fxIYkqde3/1sHpZuk+eBKMZ7rIsgBZbYhigV5g=/</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>MtKIgLOB...3D62QA==</ds:SignatureValue>
  <ds:X509Certificate>MIIIyDCCB7...SVU=/</ds:X509Certificate>
  <xades:SignedProperties Id="S1-SignedProperties">
    <xades:SigningTime>2018-06-05T15:01:11Z</xades:SigningTime>
    <xades:SigningCertificate>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>cuPIt8LpJIs+eFUgUwIrNsUikaH/NTezVgkRXixABB0=/</ds:DigestValue>
    </xades:SigningCertificate>
    <xades:DataObjectFormat ObjectReference="#S0-RefId0">
      <xades:MimeType>application/octet-stream</xades:MimeType>
    </xades:DataObjectFormat>
  </xades:SignedProperties>
</ds:Signature>
</asic:XAdESSignatures>

(signature of <SignedInfo>
XML Signature (BDOC and DDOC)

BDOC (2015 – today):
- OCSP response serves also as a timestamp
- Hash of signature included in OCSP nonce extension
- This hack is not recognized by eIDAS standards

- Single self-contained XML file
- Signed files base64-encoded in Datafile element
- Supports only SHA-1

```
<?xml version="1.0" encoding="UTF-8"?>
<SignedDoc format="DIGIDOC-XML" version="1.3" xmlns="http://www.sk.ee/DigiDoc/v1.3.0#">
  <DataFile Filename="document.doc" Id="D0">UEsDBQABgA...ASlEAAAAA</DataFile>
  <Signature Id="S0">
    <SignedInfo>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="#D0">UEsDBQABgA...ASlEAAAAA</Reference>
      <Reference URI="#S0-SignedProperties">UEsDBQABgA...ASlEAAAAA</Reference>
      <DigesterMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>Q43ti5R/wgi8q0HsygLFTXE0qU=</DigestValue>
      <DigestValue>G0HmQqHCqMxULzfWSONIL2i0mIU=</DigestValue>
    </SignedInfo>
    <SignatureValue Id="S0-SIG">kgsCQ6...M4rkcj8=</SignatureValue>
    <X509Certificate>IID4z....V8APa</X509Certificate>
  </Signature>
</SignedDoc>
```
Task: ASiC-E XAdES verifier – 5p

Implement utility that verifies ASICE XAdES digital signature.

$ ./asice_verify.py good.asice
[+] Signatory: PARŠOVŠ, ARNIS, 38608050013
[+] Signed file: hello.txt
[+] Timestamped: 2019-04-03 14:04:52
[+] Signature verification successful!

$ ./asice_verify.py bad1.asice
[+] Signatory: PARŠOVŠ, ARNIS, 38608050013
[+] Signed file: hello.txt
[-] wrong certificate hash included under the signature!

$ ./asice_verify.py bad(2|3|4|5|6|7|8).asice
[...]

- Error messages have to be meaningful
- Must support:
  - single signed file and single signature
  - only the algorithms used in the testcase file
- Not required to verify:
  - signature on certificates, timestamp, OCSP response
Task: ASiC-E XAdES verifier

- Hash is calculated on canonicalized XML elements
- Code for parsing timestamp and OCSP response is in the template
- Use zipfile for reading ZIP container:

```python
import zipfile
archive = zipfile.ZipFile(filename, 'r')
xml = archive.read('META-INF/signatures0.xml')
```

- Use BeautifulSoup for XML traversal:

```python
from bs4 import BeautifulSoup
x = BeautifulSoup(xml, features="xml")
x.XAdESSignatures.KeyInfo.X509Data.X509Certificate.encode_contents()
x.XAdESSignatures.Signature.SignedInfo.Reference['URI']
x.XAdESSignatures.Signature.SignedInfo.find('Reference',
    attrs={'URI': '#S0-SignedProperties'})
```
Questions

• The main requirements for signature to have QES status?
• The benefits of QES compared to electronic signature?
• Can the authenticity of QES be contested?
• Can unsigned e-mail be used as a proof in the court?
• How can the TSP became a QTSP?
• What is required for a product to be recognized as a QSCD?
• Why MIME type and certificate included under the signature?
• How to prove that the certificate was valid at the time of signing?
• Will it be possible to verify ASICE signature after TSA/OCSP certificates expire?