Signature Validation
- a black art?

Peter Lipp

TU Graz
Deed ("concambium") of Philip of Swabia, Jan. 15, 1207
Validating Signatures

• on paper:
  – complex
  – known to validator or specimen signature required
  – still: forged signatures difficult to detect (impossible for laymen)
What's easier to validate?

- This?
- Or This?
Assume you have this:

**Prüfbericht**

<table>
<thead>
<tr>
<th>Dokument</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dateiname</td>
<td>bakiiorrarfiyer_signed.pdf</td>
</tr>
<tr>
<td>Hash-Wert</td>
<td>ak23ArM1m6By9ioDWyahrKwdf1– (SHA-1, Base64-kodiert)</td>
</tr>
<tr>
<td>Größe</td>
<td>391,14 KB</td>
</tr>
<tr>
<td>Typ</td>
<td>PDF Signatur (Adobe PKCS#7)</td>
</tr>
</tbody>
</table>

**Signatur**

<table>
<thead>
<tr>
<th>Prüfungen</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Signatur-bzw. Prüfpunkt (UTC)</td>
<td>2015-04-17T11:00:36Z</td>
</tr>
<tr>
<td>Signatur</td>
<td>Die Überprüfung des Werts der Signatur konnte erfolgreich durchgeführt werden.</td>
</tr>
</tbody>
</table>

**Zusatzinformationen**

<table>
<thead>
<tr>
<th>Zusatzinformationen</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaturtyp</td>
<td>Adobe PKCS#7</td>
</tr>
</tbody>
</table>

**Unterzeichner**

<table>
<thead>
<tr>
<th>Unterzeichner</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Peter Alfons Mario Lipp</td>
</tr>
<tr>
<td>Titel</td>
<td>Dr.</td>
</tr>
<tr>
<td>Staat</td>
<td>AT</td>
</tr>
<tr>
<td>Seriennummer</td>
<td>dez.: 554053062614, hex.: 81:60:22:cf:3d</td>
</tr>
</tbody>
</table>

**Aussteller**

<table>
<thead>
<tr>
<th>Aussteller</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>a-sign-premium-mobile-03</td>
</tr>
<tr>
<td>Organisationsseinheit</td>
<td>a-sign-premium-mobile-03</td>
</tr>
<tr>
<td>Organisation</td>
<td>A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH</td>
</tr>
<tr>
<td>Staat</td>
<td>AT</td>
</tr>
</tbody>
</table>

**Zertifikat**

<table>
<thead>
<tr>
<th>Zertifikat</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Seriennummer</td>
<td>dez.: 446000, hex.: 06:0e:8a</td>
</tr>
<tr>
<td>Qualität</td>
<td>Qualifiziertes Zertifikat, sichere Signaturerstellungseinheit</td>
</tr>
<tr>
<td>Verwendungszweck</td>
<td>Digitale Signatur, Nichtsverschieblichkeit</td>
</tr>
<tr>
<td>Zertifizierungsstatement</td>
<td><a href="http://www.a-trust.at/docs/cp/a-sign-premium-mobile">http://www.a-trust.at/docs/cp/a-sign-premium-mobile</a></td>
</tr>
</tbody>
</table>

Hinweis: Österreichische Zertifizierungsstellearbeiter für qualifizierte Zertifikate stehen nach Signatursgesetz unter Aufsicht der Telekom-Control-Kommission, deren Gesamtstelle RTR dieses Prüfservice anbietet. Für elektronische Signaturen auf Basis von Zertifikaten ausländischer Zertifizierungsstellearbeiter bietet das Prüfservice der RTR die Möglichkeit einer automatisierten Prüfung, in diesem Fall können aber keine Garantien für eine korrekte technische Interpretation der Zertifikate gegeben werden.
Validating electronic signatures

• Is easy...

Signed Document
Certificate
Trust Anchor
Validating electronic signatures

• Is easy...
• ... or is it?
Validity Questions

• What is the status of a signature
  – When the certificate has expired?
  – When the certificate is revoked?

X.509:
NOT VALID
### Requirements for the validation of qualified electronic signatures

- The certificate ... was, at the time of signing, a qualified certificate...
- The qualified certificate .... was valid at the time of signing
- ...
- The requirements provided for in Article 26 were met at the time of signing.
Requirements for the validation of qualified electronic signatures

- the certificate ... was, at the time of signing, a qualified certificate...
- the qualified certificate .... was valid at the time of signing
- ...
- the requirements provided for in Article 26 were met at the time of signing.
Requirements for the validation of qualified electronic signatures

• state Nothing on
  – „not expired“ or
  – „not revoked later“

• Certificate must have been valid at time of signing!
Expiration

signature  expiration  validation

timeline

Validation Result

- EIDAS: valid
- X.509: expired
Revocation

Validation Result

- EIDAS: valid
- X.509: revoked
What do we do?

• We need to know that the signature was produced „in time“
  – before revocation
  – before expiration
  – before the used algorithms became weak
  – before the key sizes became too small

• signature may contain a time value
  – but it is only a *claimed* time
What do we do?

- assume the claimed time is true
- ensure that we know the status of the certificate at time of signing
Believe claimed time

• About as good as „Berlin, November 10th 2015“ on paper
• most of the time sufficient
• standard assumption e.g. in Austria
Ensuring time

Time-assertion (signature time stamp)
Proof of Existence

• The signature time-stamp proves, that the signature existed at the time of the time-stamp.

• A time-assertion consists of
  – a representation of the object (here: the signature)
  – a time
  – a digital signature by the issuer
Time Assertion

• *proof of existence* of the signature before revocation

• But since this assertion contains a digital signature:
  – requires a certificate and a validation of the signature.
  – that certificate
    • may have expired
    • may have been revoked
    • ....
Ensuring time

Time assertion: archive time stamp
Yes, it's recursive

- This time-stamp contains a signature
- requires a certificate and a validation of the signature.
- that certificate
  - may have expired
  - may have been revoked
  - ...

Very recursive...

• Also true for certs of e.g. CRL- or OCSP-services
  – Expire... revoked...
• Plus: Algorithms, key sizes...
• Almost arbitrarily complex
  – At least in theory
Standardisation

• ETSI EN 319 102-1: Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

• specifies procedures for:
  – the creation of AdES digital signatures
  – establishing whether an AdES digital signature is technically valid
Total What?

<table>
<thead>
<tr>
<th>TOTAL-PASSED</th>
</tr>
</thead>
<tbody>
<tr>
<td>• cryptographic checks of the signature succeeded</td>
</tr>
<tr>
<td>• applicable constraints to the signer’s identity certification have been positively validated</td>
</tr>
<tr>
<td>• signature has been positively validated against the validation constraints</td>
</tr>
<tr>
<td>TOTAL-FAILED</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>• cryptographic checks of the signature failed</td>
</tr>
<tr>
<td>• proven that the generation of the signature took place after the revocation of the signing certificate.</td>
</tr>
</tbody>
</table>
Total What?

INDETERMINATE

• available information is insufficient to ascertain the signature to be TOTAL-PASSED or TOTAL-FAILED.
• More information may help to decide
• Sub-indications give more info on „what’s missing“
Example

INDETERMINATE/REVOKED_NO_POE

signature  revocation  validation

timeline

Proof-of-existence missing
Reality check

• What is the real situation?

Valid signature created before revocation
• but validation fails - we miss the POE

Certificate was revoked, legitimate user still produced signature
• „de facto“ a valid signature - we will never be able to validate

Key was really stolen or broken
• an invalid signature create - the really bad case
• we can't decide which of them is reality
Who decides?

• The policy decides.
• There is always a policy involved:
  – formal policy (TS 119 172)
  – parameter set by the driving application
  – implementation specifics
• Policy rules all...
Accept revoked certificates?

- Feels strange
- Seems difficult
- But may be the right thing to do...
- E.g.:
  - Yesterday I produced a signature with my citizen card
  - I lose my Austrian citizen card today - revocation
  - no time-stamps were added
  - but my signature is still a valid one
Accepting revoked certificates? Risky?

• Legally my signature is certainly valid.
• Technically most standard applications will reject the signature.
• Not all problems can be solved using technology.

• When problems occur ...

• **IF** problems occur ...

• ... consult your lawyer ...
Thank you very much

• ... for your attention.

• Questions?