Signature Validation
- a black art?

The Challenge to Create and Validate an Electronic Signature across Europe, ETSI Security Week

Sophia Antipolis, June 25th 2015
Validation of the Deed ("concambium") of Philip of Swabia, Jan. 15, 1207

Introduction

Validate this!
Validating Signatures

- on paper:
  - complex
  - known to validator or specimen signature required
  - still: forged signatures difficult to detect (impossible for laymen)
Validating Signatures

What’s easier to validate?

Full Name: Peter Lipp
Signature:
Date: 1.6.2015
Introduction

Signature Validation - Exceptions

... is „easy“ .... or is it?

expired certificate

Certificate

not after: 2015-01-01

revoked certificate

Certificate

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,...
- the qualified certificate .... was valid at the time of signing
- ...
- the requirements provided for in Article 26 were met at the time of signing.
EIDAS

Requirements

- state Nothing on „not expired“ or „not revoked later“
- Certificate must have been valid at time of signing.
Examples

Expiration

Validation Result

- EIDAS: valid
- X.509: expired
Examples

revocation

Validation Result

- EIDAS: valid
- X.509: revoked
What to 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
Examples

What to do

Two Options

- 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 „Sophia Antipolis, June 25th 2015“ on paper
- most of the time sufficient
- standard assumption e.g. in Austria
Examples

Ensuring time

signature
revocation
validation

timeline

time-assertion (signature time-stamp)
Examples

Time Assertion

- proof of existence of the signature before revocation
- but

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    - may have been revoked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

signature
expiration signer cert
expiration TS-cert
validation
timeline
time-assertion (archive time-stamp)
Examples

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
    - ....

- Also true for certs of e.g. CRL- or OCSP-services

Examples

Reality check

situation can be
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 valid
Accept revoked certificates? Risky?

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

... consult your lawyer ...