One Signature Certificates

LAMPS WG - IETF 126

https://github.com/lamps-wg/draft-ietf-lamps-one-signature-certs

Stefan Santesson
Russ Housley

Basic characteristics

- Used only for one signed document
  - Key pair generation
  - Certificate issued
  - Document signed
  - Private key destroyed
- Certificate never expires
  - notAfter field = GeneralizedTime 99991231235959Z
- No revocation
  - id-ce-noRevAvail extension
- Bound to one signature
  - New signedDocumentBinding extension

Updates since last IETF

- In current draft
  - Changed requirements
    - SHOULD include noRevAvail extension (was MUST)
    - SHOULD have infinite validity (was MUST)
  - Updated rationale for no revocation
    - Signatures are valid if a certificate is revoked after signing time. OSC carries the time of signature creation as certificate validity start time. Revocation has no effect on signature validity even if provided.
  - Added example certificates
- Agreed for next draft
  - OID instead of string as binding type identifier
  - Update IANA considerations
  - New example certificates

signedDocumentBinding extension - change

```
name                id-pe-signedDocumentBinding
OID                 { id-pe TBD }
syntax              SignedDocumentBinding
criticality         SHOULD be FALSE

SignedDocumentBinding ::= SEQUENCE {
dataTbsHash          OCTET STRING,
hashAlg              DigestAlgorithmIdentifier,
bindingType          OBJECT IDENTIFIER OPTIONAL }
```

bindingType

- **Default = absent**
  - The bytes that are signed
  - Not usable if certificate data is signed (JWS, COSE, ETSI)
- **cades – OID TBD**
  - Exclude SigningCertificate and SigningCertificateV2 attributes from signedAttrs
- **xades – OID TBD**
  - Exclude Ref type http://uri.etsi.org/01903#SignedProperties from SignedInfo
- **jws and cose – OID TBD**
  - Hash payload only

Open issues

- None recorded
  - All issues on GitHub resolved

Implementations

- Sweden Connect
  - https://github.com/swedenconnect/signature-validation/blob/master/cert-extensions/src/main/java/se/swedenconnect/cert/extensions/SignedDocumentBinding.java
- Fully supported by the related CA open source
  - https://github.com/swedenconnect/ca-engine
  - https://github.com/swedenconnect/ca-engine/blob/main/src/test/java/se/swedenconnect/ca/engine/ca/issuer/OneSignatureCertificateTest.java (generated the test certificates in the draft)

- Others have expressed interest to implement and use as soon as possible.

Next

- Other issues?
- Ready for WG last call?