One Signature Certificates

Proposed new LAMPS WG item

https://github.com/Razumain/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

signedDocumentBinding extension

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

SignedDocumentBinding ::= SEQUENCE {
dataTbsHash      OCTET STRING,
hashAlg          DigestAlgorithmIdentifier,
bindingType      UTF8String OPTIONAL }
```

bindingType

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

Next

- Publish 00
- Take to list
- Call for adoption