Embedded Certificates in Metadata & Related Policy Changes

SWITCH

Serving Swiss Universities

Thomas Lenggenhager
thomas.lenggenhager@switch.ch

Today

- Accepted Root CA certificates embedded in metadata.xml
- Certificates for IdPs and SPs are issued by one of the accepted Root CAs, or one of its subordinates.
  - only KeyName in metadata.xml
  - only few exceptions embedded
    - IdP pilot: ZHB Luzern, PHSG
    - Some recently added SPs

```
<KeyDescriptor use="signing">
  <ds:KeyInfo>
    <ds:KeyName>aai.unil.ch</ds:KeyName>
  </ds:KeyInfo>
</KeyDescriptor>
```

Why Embedded Certificates?

- Allows to encrypt SAML assertions with the key of the intended recipient
  - Content (e.g. attribute values) not readable by third parties

- Intermediate/issuing CA certs not needed anymore
  - No problem with alternate issuing CAs of lower quality

- Allows to use self-signed certificates…
  - …as long as minimal requirements are met

Some of the Minimal Requirements

- Key generation
  - strong random number generator (RNG) and sufficient entropy
- Protection of the private key
  - The private key MAY only be stored unencrypted form on the system where it is going to be used.
  - It MUST be protected with adequate file permissions.
  - If stored on any other system, it MUST only be stored in encrypted form, i.e. protected with a strong pass phrase.
- Key reuse
  - NO reuse of any existing key pair
- Validity
  - The validity MUST NOT exceed 3 years. (notBefore - notAfter dates)
- Key size
  - The key MUST be an RSA key with a size of 2048 bits

How does it look like in metadata.xml?

```
<KeyDescriptor use="signing">
  <ds:KeyInfo>
    <ds:KeyName>aai-rr.switch.ch</ds:KeyName>
    <ds:X509Data>
      <ds:X509Certificate>
MIIEaDCCA1CgAwIBAgIJAOSsXNN7+2lVMA0GCSqGSIb3DQEBBQUAMGoxCzAJBgNV
...
k9JNfW2tdxW022cTClKQQnacKN1DjJg3nfUaoQ==
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</KeyDescriptor>
<KeyDescriptor use="encryption">
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>
MIIEaDCCA1CgAwIBAgIJAOSsXNN7+2lVMA0GCSqGSIb3DQEBBQUAMGoxCzAJBgNV
...
k9JNfW2tdxW022cTClKQQnacKN1DjJg3nfUaoQ==
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</KeyDescriptor>
```

Proposal…

- Which Certificates to Accept for Embedding?
  - Certificates issued under a well-known CA
    - 'Organization Validated' (OV) and
    - Issued by a CA that is either
      - a member of the Microsoft Root Certificate Program, or
      - has been accepted by the Mozilla Foundation for inclusion in their browser family
    - Minimal requirements
  - Self-signed certificates
    - Minimal requirements
    - Fingerprint of the private key to be verified via an independent channel (e.g. phone, fax)