SAML related Federation Update

Thomas Lenggenhager
thomas.lenggenhager@switch.ch
TRID WG Meeting, 26.5.2021

Overview

- Updated Certificate Acceptance Policy
- Improved Encryption Method for SAML
- Shibboleth IdPv4.0 & 4.1
- Update due for the Attribute Specification
- SAML Interoperability Pitfalls
- Kantara SAML Interoperability Profiles

Updated Certificate Acceptance Policy

- The new policy is active since end of March 2021
- Goal was to
  - align it with major federations
  - reduce the risk to break services that require manual intervention for certificate rollover
- Major changes
  - recommended key size 3072 bits
  - certificate lifetime 10+ years instead of max 3 years
  - renewal of a private key only if it is lost or stolen
  - no more strict rules about subject information in self-signed certs

https://www.switch.ch/aai/support/certificates/certificate-acceptance/

SWITCH

Improved Encryption Method for SAML

- The encryption method IdPs use for assertion encryption needs to be improved.
- SAML standard requires SPs only to support AES128-CBC decryption; AES128-GCM would be stronger.
- The IdP needs to know which encryption methods an SP supports.
- The RR will support a smooth roll out of the `<EncryptionMethod>` for SP entries, so that an IdPv4 will know when to use the better method.
- We will inform via aai-operations once the plan is ready.

```
<md:KeyDescriptor use="encryption">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>
      <ds:X509Certificate>
      ...
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
  <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-gcm"/>
  <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
</md:KeyDescriptor>
```

Shibboleth IdPv4.0 & 4.1

- New features
  - OIDC OP integrated, no longer an add-on
  - SAML proxy login flow
  - `AttributeRegistry` Configuration
  - Cross-Site Request Forgery (CSRF) Protection

- No specific IdPv4 guide by SWITCH
  SWITCHaai specific v4 `AttributeRegistry` config files to be provided

https://wiki.shibboleth.net/confluence/display/IDP4/ReleaseNotes

Update due for the Attribute Specification

Documenting attributes adopted since the last version in April 2017.
Most of them are already supported in the Resource Registry, currently as ‘local’.

For affiliations & private identity

```
schacCountryOfCitizenship
sshPublicKey
subject-id, pairwise-id
uidNumber
swissEduPersonMinimumAgeCategory
swissEduPersonPrivateMail
```

For edu-ID extended attribute model

```
swissEduIDAssociatedMail
swissEduPersonAdditionalEmail
swissEduIDLinkedAffiliation
swissEduIDLinkedAffiliationMail
swissEduIdLinkedAffiliationUniqueID
swissEduIDUsagely
```

For input and disussion, subscribe to *aai-tf-attr*
The draft will be announced on *aai-operations*

https://lists.switch.ch/

SAML Interoperability Pitfalls (1)

- Higher education federations expect SPs to
  - regularly load the federation metadata file and use a Discovery Service to pick the user's IdP;
  - accept a signed SAML response;
    The SAML assertion included is unsigned and encrypted.
  - accept SAML NameID format: `transient` (or `persistent`) and use an attribute (like `swissEduPersonUniqueID`) as user identifier, **not** the NameID value;
  - accept `eduPerson` attributes that were mostly derived from LDAP standards
- Often cloud based services support SAML only by bilateral configuration with their own expectations.

SAML Interoperability Pitfalls (2)

- SAML has no certification process, unlike OpenID Connect (OIDC).
  - Vendors can claim to support SAML, even with some limited subset implemented.
- Many ignore the **Robustness principle** also known as **Postel's law**:
  Be conservative in what you send, be liberal in what you accept.

➜SAML Proxy, the following presentation

Kantara SAML Interoperability Profiles

- Interoperability with the IdPs in SWITCHaai will be no issue if
  - your SAML service provider uses software implemented according to [1]
  - you deployed it according to [2].
- Otherwise, it is unlikely that your SAML service provider will properly interoperate.
- No problem for a Shibboleth SP configured along to the SP config guide.

[1] SAML V2.0 Implementation Profile for Federation Interoperability
https://kantarainitiative.github.io/SAMLprofiles/fedinterop.html

[2] SAML V2.0 Deployment Profile for Federation Interoperability
https://kantarainitiative.github.io/SAMLprofiles/saml2int.html