SAML Profile for Privacy-enhanced Federated Identity Management

Rainer Hörbe, Identinetics GmbH

Abstract

This profile for the SAML WebSSO use case specifies an enhancement that allows users to limit their observability by IdPs and APs. It is based on the general Model for Privacy-enhanced Federated Identity Management[1], which describes a 3-tier model resembling an enhanced hub-and-spoke federation model. It includes the SAML WebSSO and SLO profiles, and adds messaging capabilities.
1 Interfaces

This section describes the extensions to a SAML WebSSO use case as specified in the PE-FIM model referenced above.

Fig. 1 High-level layout of the PEFIM model (WebSSO use case)

The following overview describes the interfaces that deviate from standard SAML WebSSO profiles, corresponding to the numbered references in Fig. 1.

1. The CA provides an interface for pseudonymous short-term certificates. An SP may obtain encryption certificates that assert that the SP is a federation member in good standing. Certificate serial numbers must be well randomized to diffuse any relationships to SPs that obtain certificates in blocks. CSRs may be authenticated using either a secure channel or signed messages.

2. An SP must implement the complementary interface to (1). Each authentication request must use a unique encryption key certified by the CA. For efficiency, signing multiple CSRs in batch-mode using CMS-signatures is recommended.

3. The metadata feed describes entities according to SAML2MetaIOP [2] with an SP-side view. That is, that IdPs are represented by proxies in the SB. <EntityDescriptor>
elements must not include encryption keys in the `<SPSSODescriptor>` element, because these keys are for one-time use only and therefore submitted in the authentication request.

4. An SP needs
   a. to send an `<AuthnRequest>` with a new one-time certificate in the `<Extensions>` element, as specified in 2.2 and
   b. understand the `<Response>` as specified in 2.3.

5. SB/IdP proxy for the SAML WebSSO profile. The SB proxies `<AuthnRequest>` and `<Response>` elements as follows:

<table>
<thead>
<tr>
<th></th>
<th>IdP</th>
<th>SB</th>
<th>SP</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthnRequest</td>
<td></td>
<td>Rewrite AuthnRequest, filtering SP-identifying attributes (destination, audience and issuer)</td>
<td>Issue AuthnRequest to IdP proxy.</td>
</tr>
<tr>
<td>Response</td>
<td>Target Proxy-SP. Provide TID₁ in NameID. Encrypt attribute assertion.</td>
<td>Rewrite Response. Create TID₂ from TID₁.</td>
<td>Decrypt attributes.</td>
</tr>
</tbody>
</table>

SB/IdP proxy for the SLO profile.

6. An IdP or AP using and validating the SP’s encryption key contained in `<pefim:SPCertEnc>` MUST search the certificate using the public key and MUST NOT use the subject name or serial number. The encryption key MUST be verified using X.509 path validation.

7. Like SP-side metadata, but for IdP-side.

8. The SB implements a pseudonymous consent service. It allows users to grant, review and revoke consent. It may only operate on attribute names, not values to protect pseudonymity. Consent data is stored using TID₂ and SP-entityID as keys.

9. SB/Message Broker: MTA rewriting (a) TLD₂ to TLD₁ addresses or (b) TLD₂(SP₁) to TLD₂(SP₂) addresses and in the reverse direction.

10. IdP/Message Broker: MTA rewriting (a) TLD₁ to email addresses and in the reverse direction.
Note 1: This model requires SP-first authentication flows, as the IdP must not know about the principal’s registered services. Service discovery may be implemented by an SB.

Note 2: The typical size of encryption certificates in PEM-format will be around 2k. Internet Explorer limits the URL length to 2083 characters, hence POST-binding is recommended to convey the AuthnRequest.

Note 3: Message content must not contain PII, because the SB or IDP could link this up with other data and violate the unobservability requirement. Solutions are end-to-end encryption or sending links to authenticated contents.
2 Data Structures

2.1 Namespaces

<table>
<thead>
<tr>
<th>Prefix</th>
<th>XML Namespace</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ds:</td>
<td><a href="http://www.w3.org/2000/09/">http://www.w3.org/2000/09/</a></td>
<td>This namespace is defined in the XML Signature Syntax and Processing specification [XMLSig] and its governing schema [XMLSig-XSD].</td>
</tr>
<tr>
<td></td>
<td>xmldsig#</td>
<td></td>
</tr>
<tr>
<td>pefim:</td>
<td>urn:net:eustix:names:tc:</td>
<td>Namespace for elements introduced by this spec.</td>
</tr>
<tr>
<td></td>
<td>PEFIM:0.0:assertion</td>
<td></td>
</tr>
<tr>
<td>saml:</td>
<td>urn:oasis:names:tc:SAML:2.0:a</td>
<td>This is the SAML V2.0 assertion namespace, defined in a schema [SAML-XSD]. The prefix is generally elided in mentions of SAML assertion-related elements in text.</td>
</tr>
<tr>
<td></td>
<td>ssertion</td>
<td></td>
</tr>
<tr>
<td>samlp:</td>
<td>urn:oasis:names:tc:SAML:2.0:</td>
<td>This is the SAML V2.0 protocol namespace, defined in a schema [SAML-P-XSD]. The prefix is generally elided in mentions of XML protocol-related elements in text.</td>
</tr>
<tr>
<td></td>
<td>protocol</td>
<td></td>
</tr>
</tbody>
</table>

2.2 AuthnRequest

<AuthnRequest> elements must contain the encryption certificate used to encrypt the assertion with the attribute statement. The encryption key is represented within a <ds:KeyInfo> element. Its XPath is:
ds:X509Data/ds:X509Certificate.

2.3 Response

A <Response> contains a single assertion that has following properties:

- It MUST have a subject, containing the Targeted ID in a <NameID> element;
- It MUST have an authentication statement;
- It MAY have (and usually will have) one or more <EncryptedAssertion> element contained in the <advice> element, each itself containing an attribute statement. Multiple <EncryptedAssertion> elements are useful to aggregate
attributes from multiple attribute providers without any other party than the SP reading them in clear.

- The encrypted assertion issued by the IDP must be self-contained with respect to XML namespaces\(^1\).

An encrypted assertion MUST NOT contain a subject (because the TID\(_1\) in nameID MUST NOT be revealed to the SP)

\(^1\) The SB is creating a new <Response> element with its own QNAMES and does not know about namespace definitions in the encrypted part. Including all namespace definitions from the IDP or even having pre-defined QNAMES do not seem viable alternatives for the implementation.
2.4 Sample Instances

2.4.1 Authentication Request

(Non-normative – always implement according to specification – do not copy examples)

```xml
<authn-request xmlns:samlp1.0="urn:oasis:names:tc:SAML:2.0:protocol"
                xmlns:saml1.0="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:ds="http://www.w3.org/2000/09/xmldsig#
                xmlns:pefim="urn:net:eustix:names:tc:PEFIM:0.0:assertion"
                ID="_d11257d39d92042c860f5e8ee147a160"
                IssueInstant="2014-02-07T11:30:31Z"
                ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                Version="2.0">
  <assertion ConsumerServiceURL="https://echo.kuk.portalverbund.at/SAML2/POST">
    <saml:Issuer>
      https://echo.kuk.portalverbund.at/sp.xml
    </saml:Issuer>
    <samlp:Extensions>
      <pefim:SPCertEnc>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
              MIIC8jCCAlugAwIBAgIJAJHg2V5J3118MA0GCSg6GSlb3DQEBBQAMBwMQCAJSAsB
              BTA1MQwCwYDVQQHEwTVbWVhMjBhMjBhMIIBIjANBgkqhkiG9w0BAQUAA4GNAD
              CQIBgEDEQYJKoZIhvcNAQEFBQADggEPADCCAQoD=]
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </pefim:SPCertEnc>
    </samlp:Extensions>
  </assertion>
</authn-request>
```

2.4.2 Response

T.B.D.
3 Glossary

Attribute Assertion
An <EncryptedAssertion> element containing an <AttributeStatement>.

Targeted Identifier (Targeted ID)
A persistent, non-reassigned, privacy-preserving identifier for a principal shared between a pair of IdPs and SPs. An IdP uses the appropriate value of this attribute when communicating with a particular SP (or SP affiliation), and does not reveal that value to any other service provider except in limited circumstances. Many similar definitions can be found for EduPersonTargetedID2. Synonym: Persistent ID
NOTE: This concept is extended for the PE-FIM model by decomposing the Targeted ID into TID1 and TID2.

Targeted Identifier 1 (TID1)
A targeted ID between an IdP or AP and an SB.

Targeted Identifier 2 (TID2)
A targeted ID between an SB and an SP.

2 e.g. SWITCH AAI attributes: http://www.switch.ch/it/nai/support/documents/attributes/
References


# Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>17. January 2014</td>
<td>Initial version</td>
</tr>
<tr>
<td>1.1</td>
<td>5. March 2015</td>
<td>Encrypted assertion issued by the IDP must be self-contained with respect to XML namespaces.</td>
</tr>
<tr>
<td>1.2</td>
<td>6. May 2015</td>
<td>Corrected type with samlp:Extensions being in Singular</td>
</tr>
</tbody>
</table>