HPI Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Conveying Attribute Assurance with Attribute Context Classes

Contribution to OASIS Security Services TC

Ivonne Thomas

Research School on "Service-Oriented Systems Engineering"
Hasso-Plattner-Institute, University of Potsdam

September 2010

Use Case I

- A relying party can have different requirements for identity assurance
  - e.g. low assurance is required to access and read a document
  - but high assurance is required to delete or update this document
- As identity proofing processes are cost-intensive and time-consuming due to the effort required to verify a user's identity attributes, a verification of an attribute might not be desired as long as a user is not involved in transactions that demand a higher trust level. Therefore a user might decide to register with an identity provider without proper identity proofing and getting involved in the identity proofing only upon concrete requirement.
- This requires a different trust level per user and does not allow to rate an identity provider as a whole.

Use Case II

- Identity providers are inherently different due to their affiliation with an organization or institution and might be suitable for asserting certain identity attributes only to a limited extent.
- For example, a banking identity provider will be in particular suitable to assert that a user can pay for a certain service, but might have weak records of the user's status as a student while for a university's identity provider it would probably be the opposite.
- Therefore different attributes have different levels of trust, which need to be communicated to the relying party.

Problem Statement

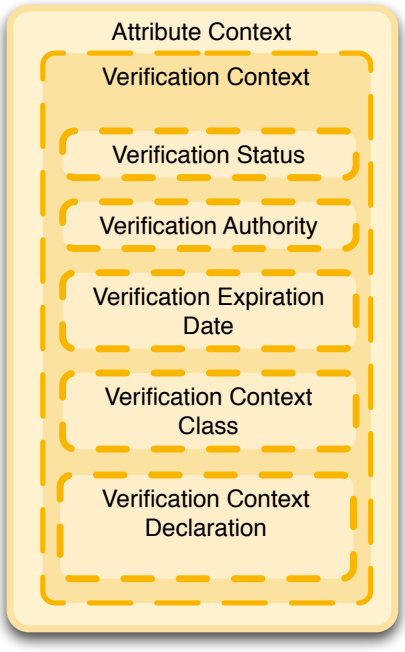
- Levels of Assurance mostly refer to the identity of a user and the IdP managing this identity as a whole (Usually one level covers Operational Factors, the strength of Registration and Identity Proofing processes as well as technical requirements)
- This makes it difficult to reflect varying trust requirements of specific attributes
- SAML is used for exchanging attribute data between an IdP and a relying Party
- SAML V2.0 Identity Assurance Profiles allow to transfer a level of assurance with the assertion in the Authentication Context
- But, there is **no mechanism** to enable an IdP to transmit information about the verification process of an attribute to the relying party

Proposal

- We propose to have trust levels for attributes transferred within SAML assertions as well as additional meta information about the strength of the attribute verification
- Similar to the Authentication Context Classes, we propose Attribute Context Classes that describe the strength of attribute verification
- Attribute Context Classes contain certain verification pattern as
  - **in-person-proofing** that applies for attributes as name, address, age, ...
  - **out-of-bound proofing** as a verification e-Mail to prove the existence of an email address or sending a letter to prove the existence of an address
  - ....

Attribute Context Classes

Data model:



• **Attribute Context** This data element holds the attribute context, which is comprised of all additional information to the attribute value itself. This element is the upper container for all identity metadata.

• **Verification Context** This data element holds the verification context, which comprises all information related to the verification of an identity attribute value. The Verification Context is one specific context within the Attribute Context.

• **Verification Status** This data element indicates the verification status of an identity attribute value, which can be for example something as verified, not verified or unknown. The verification status is part of the verification context.

• **Verification Authority** This data element indicates who has performed the verification and is part of the Attribute Context. This can be for example another identity provider, some authority as a certificate authority or the user himself who entered the data.

• **Verification Expiration Date** This data element indicates the validity of the verification status.

•**Verification Context Class** contains the name of the verification context class.

•**Verification Context Declaration** The verification context declaration holds the verification process details. Such a detail could for example be the method that has been used for verifying the correctness of the attribute.

Example 1: Identity Proofing


```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlext="http://de.hpi.ip/saml20/ext">
  [...]
  <saml:Subject>
    <saml:NameID>MaxMustermann
    </saml:NameID>
  </saml:Subject>
  [...]
  <saml:AttributeStatement>
    <saml:Attribute
      FriendlyName="givenName">
      <saml:AttributeValue
        xsi:type="xs:string">Mustermann
      </saml:AttributeValue>
      <samlext:AttributeContext>
        <samlext:VerificationContext>
          <samlext:VerificationStatus>
            verified
          </samlext:VerificationStatus>
          <samlext:VerficationAuthority>
            http://identity.company.de
          </samlext:VerficationAuthority>
          <samlext:VerificationExpirationDate>
            003-24-11T10:33:18Z
          </samlext:VerificationExpirationDate>
          <samlext:VerificationContextClass>
            In-Person-Proofing
          </samlext:VerificationContextClass>
          <samlext:VerificationContextDecl
            xmlns:samlextInPersonProof="http://de.hpi.ip/saml20/ext/InPersonProofing">
            <samlextInPersonProof:VerificationDocument>
              Drivers License
            </samlextInPersonProof:VerificationDocument>
          </samlext:VerificationContextDecl>
        </samlext:VerificationContext>
      </samlext:AttributeContext>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```


Example 2: Verification Email


```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlext="http://de.hpi.ip/saml20/ext">
  [...]
  <saml:Subject>
    <saml:NameID>MaxMustermann
    </saml:NameID>
  </saml:Subject>
  [...]
  <saml:AttributeStatement>
    <saml:Attribute
      xmlns:x500="urn:oasis:names:tc:SAML:1.1:
                  nameid-format:emailAddress"
      FriendlyName="emailAddress">
      <saml:AttributeValue
        xsi:type="xs:string">staff@company.de
      </saml:AttributeValue>
      <samlext:AttributeContext>
        <samlext:VerificationContext>
          <samlext:VerificationStatus>
            verified
          </samlext:VerificationStatus>
          <samlext:VerficationAuthority>
            http://identity.company.de
          </samlext:VerficationAuthority>
          <samlext:VerificationExpirationDate>
              2011-05-21
          </samlext:VerificationExpirationDate>
          <samlext:VerificationContextClass>
            ConfirmationEmailReceived
          </samlext:VerificationContextClass>
        </samlext:VerificationContext>
      </samlext:AttributeContext>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Conclusion

- HPI asks the SS TC to
  - discuss this approach
  - working on a specification similar to the AuthenticationContextClasses that covers the ides about AttributeContextClasses as outlined in these slides
  - to define a consistent set of *Verification Context Declarations*
  - to align the approach with the SAML 2.0 Identity Assurance Profiel, Version 1.0