SWAMID

Swedish Academic Identity Federation

Rekommenderad attributrelease i SWAMID

Hur gör vi?

2022-10-20

SWAMID

Nyheter i Release-check

Björn Mattsson

SWAMID

Nyheter i Release-check

Lite nya tester

- **assurance - Assurance Attribute test**
- noec - No EC (shall not send any attributes!)
- **anonymous - REFEDS Anonymous Access**
- **pseudonymous - REFEDS Pseudonymous Access**
- **personalized - REFEDS Personalized Access**
- **cocov2-1 - REFEDSCoCo (v2) part 1, from SWAMID**
- **cocov2-2 - REFEDSCoCo (v2) part 2, from SWAMID**
- **cocov2-3 - REFEDSCoCo (v2), from outside SWAMID**
- cocov1-1 - GÉANTCoCo (v1) part 1, from SWAMID
- cocov1-2 - GÉANTCoCo (v1) part 2, from SWAMID
- cocov1-3 - GÉANTCoCo (v1), from outside SWAMID
- rands - REFEDS R&S

SWAMID

Nyheter i Release-check

- Möjlighet att köra alla tester i ett svep eller en i sänder på 1:a sidan.

- Möjlighet att köra om en test från resultatsidan

SWAMID

Tekniskt implementation av de nya entitetskategorierna för Shibboleth

Paul Scott

SWAMID

Ändringar i korthet

- Ändringar behöver göras i:
  - Attribute Resolver
    - Två nya AttributeDefinition
      - samlPairwiseID
      - samlSubjectID
    - En ny DataConnector för samlPairwiseID
  - Attribute Filter
    - Tre nya entitetskategorier
      - Anonymous
      - Pseudonymous
      - Personalized
    - Uppdateringar och kompletteringar till Code of Conduct
      - Stöd för Code of Conduct v1 och v2
      - Stöd för EntityAttribute subject-id:req

SWAMID

Attribute resolver

- Nya attributer för subject identifiers
  - samlSubjectID (subject-id)
  - samlPairwiseID (pairwise-id)

```
<!-- Schema: SAML Subject ID Attributes -->
<AttributeDefinition xsi:type="Scoped" id="samlSubjectID" scope="%{idp.scope}">
    <InputDataConnector ref="myLDAP" attributeNames="%{idp.persistentId.sourceAttribute}"/>
    <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oasis:names:tc:SAML:attribute:subject-id" friendlyName="subject-id" encodeType="false" />
</AttributeDefinition>

<AttributeDefinition xsi:type="Scoped" id="samlPairwiseID" scope="%{idp.scope}">
    <InputDataConnector ref="computed" attributeNames="computedId"/>
    <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oasis:names:tc:SAML:attribute:pairwise-id" friendlyName="pairwise-id" encodeType="false" />
</AttributeDefinition>
```

SWAMID

Attribute resolver

- Ny ComputedId DataConnector för pairwise-id
  - sourceAttribute ska vara uid/samAccountName
    - samma unscoped-attribut som till eduPersonPrincipalName
  - Salt kan vara samma salt som till StoredId
  - Använd default algorithm och encoding

```
<!-- DataConector for pairwise-id (example depends on saml-nameid.properties). -->
<DataConnector id="computed" xsi:type="ComputedId"
        generatedAttributeID="computedId"
        salt="%{idp.persistentId.salt}"
        algorithm="%{idp.persistentId.algorithm:SHA}"
        encoding="%{idp.persistentId.encoding:BASE32}">
    <InputDataConnector ref="myLDAP" attributeNames="%{idp.persistentId.sourceAttribute}" />
</DataConnector>
```

Attribute filter

- Nya AttributeFilterPolicy för
  - https://refeds.org/category/anonymous
  - https://refeds.org/category/pseudonymous
  - https://refeds.org/category/personalized
  - Subject identifiers
- Uppdaterad AttributeFilterPolicy för Code of Conduct

SWAMID

Anonymous

- Skickar enbart affiliation och home organization

```
<!-- REFEDS Anonymous Authorization Entity Category -->
<AttributeFilterPolicy id="releaseToRefedsAnonymous">
  <PolicyRequirementRule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/anonymous" />
  <AttributeRule attributeID="eduPersonScopedAffiliation">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>
  <AttributeRule attributeID="schacHomeOrganization">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>
</AttributeFilterPolicy>
```

SWAMID

Pseudonymous

- Skickar pairwise-id som identifierare

```
<!-- REFEDS Pseudonymous Authorization Entity Category -->
<!-- Supports data minimalisation to prevent use together with anonymous -->
<AttributeFilterPolicy id="releaseToRefedsPseudonymous">
  <PolicyRequirementRule xsi:type="AND">
    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/pseudonymous" />
    <Rule xsi:type="NOT">
      <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/anonymous" />
    </Rule>
  </PolicyRequirementRule>
  <AttributeRule attributeID="samlPairwiseID">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonScopedAffiliation">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>
  <AttributeRule attributeID="schacHomeOrganization">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonAssurance">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
</AttributeFilterPolicy>
```

Personalized

- Skickar subject-id som identifierare

```
<!— REFEDS Personalized Access Entity Category —>
<!— Supports data minimalisation to prevent use together with anonymous and pseudonymous—>
<AttributeFilterPolicy id="releaseToRefedsPersonalized">
  <PolicyRequirementRule xsi:type="AND">
    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/personalized" />
    <Rule xsi:type="NOT">
      <Rule xsi:type="OR">
        <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/anonymous" />
        <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/pseudonymous" />
      </Rule>
    </Rule>
  </PolicyRequirementRule>
  <AttributeRule attributeID="samlSubjectID">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="displayName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="givenName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="sn">
```

SWAMID

Code of Conduct

- Support för v1 och v2

```
<!-- GEANT Data protection Code of Conduct or REFEDS Data Protection Code of Conduct Entity Category -->
<AttributeFilterPolicy id="releaseToCodeOfConduct">
  <PolicyRequirementRule xsi:type="OR">
    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1" />
    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/code-of-conduct/v2" />
  </PolicyRequirementRule>
  <AttributeRule attributeID="eduPersonTargetedID">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
  </AttributeRule>
  <AttributeRule attributeID="eduPersonPrincipalName">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
  </AttributeRule>
  <AttributeRule attributeID="eduPersonOrcid">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
  </AttributeRule>
  <AttributeRule attributeID="norEduPersonNIN">
    <PermitValueRule xsi:type="AND">
      <Rule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
      <Rule xsi:type="RegistrationAuthority" registrars="http://www.swamid.se/" />
    </PermitValueRule>
  </AttributeRule>
  <AttributeRule attributeID="personalIdentityNumber">
```

SWAMID

Subject identifiers

- I kombination med Code of Conduct

```
<!— Rule to honour Subject ID requirement tag in metadata. Used in combination with Geant/Refeds Code of Conduct v* —>
<!— Code of Conduct can be combined with other entity categories —>
<!— Supports data minimalisation to prevent subject-id and pairwise-id being released together —>
<AttributeFilterPolicy id="subject-identifiers">
  <PolicyRequirementRule xsi:type="OR">
    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1" />
    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/code-of-conduct/v2" />
  </PolicyRequirementRule>
  <AttributeRule attributeID="samlPairwiseID">
    <PermitValueRule xsi:type="AND">
      <Rule xsi:type="NOT">
        <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/personalized" />
      </Rule>
      <Rule xsi:type="OR">
        <Rule xsi:type="EntityAttributeExactMatch" attributeName="urn:oasis:names:tc:SAML:profiles:subject-id:req" attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" attributeValue="pairwise-id" />
        <Rule xsi:type="EntityAttributeExactMatch" attributeName="urn:oasis:names:tc:SAML:profiles:subject-id:req" attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" attributeValue="any" />
      </Rule>
    </PermitValueRule>
  </AttributeRule>
  <AttributeRule attributeID="samlSubjectID">
    <PermitValueRule xsi:type="AND">
      <Rule xsi:type="NOT">
        <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="https://refeds.org/category/pseudonymous" />
      </Rule>
      <Rule xsi:type="EntityAttributeExactMatch" attributeName="urn:oasis:names:tc:SAML:profiles:subject-id:req" attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" attributeValue="subject-id" />
    </PermitValueRule>
  </AttributeRule>
</AttributeFilterPolicy>
```

Exempel filer...

- Finns på wiki under ”SAML IdP Best Current Practice”
  - https://wiki.sunet.se/display/SWAMID/SAML+IdP+Best+Current+Practice
    - Example of a standard attribute resolver for Shibboleth IdP v4 and above
    - Example of a standard attribute filter for Shibboleth IdP v4 and above

Teknisk implementation av de nya entitetskategorierna för ADFS

Johan Peterson

Tommy Larsson

SWAMID

New version of the ADFS Toolkit!

- Version 2.2.0
- Includes
  - The new Entity Categories
  - ADFS Toolkit Store
  - Subject ID Request
  - Timefix for TransientID
  - Bugfix for schacDateOfBirth
- New code signing cert since 2.0.1-> Uninstall – Install
- See https://github.com/fedtools/adfstoolkit for documentation

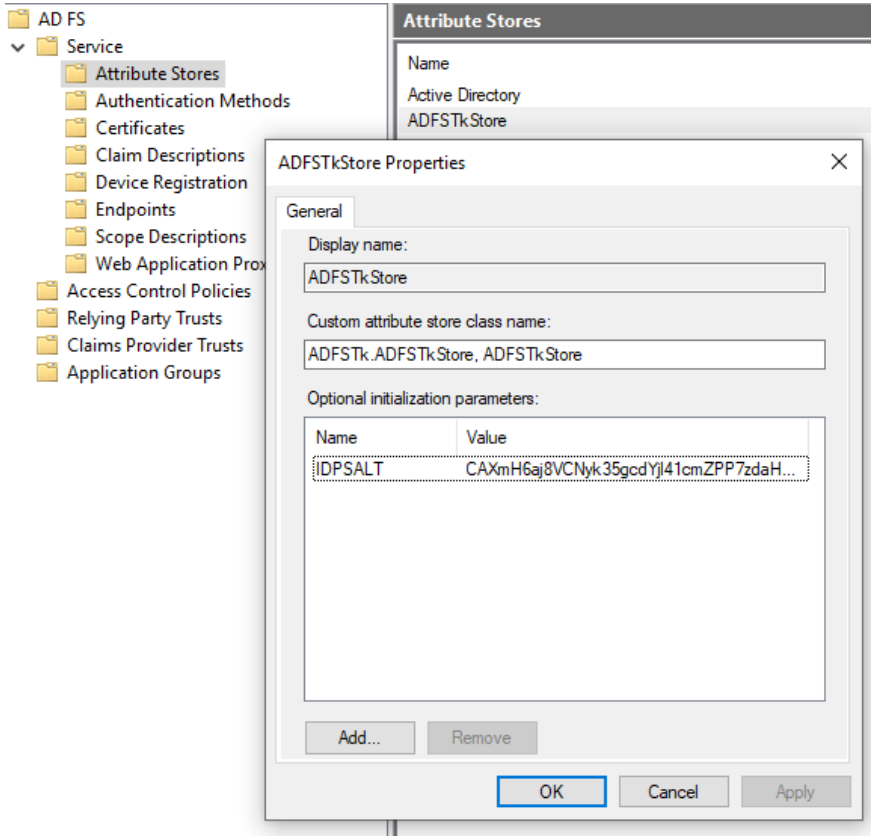
SWAMID

ADFS Toolkit Store

- Used for calculations/tranformations that ADFS can’t handle internally
- Calls C# .NET code for execution
- Used in the config.[federation].xml file

SWAMID

ADFS Toolkit Store - Installation



- Install-ADFSTkStore
  - Run on *all* ADFS servers!
- Generate Hash Salt or enter it manually on first Server

SWAMID

ADFS Toolkit Store - Configuration

```
<attribute type="urn:oasis:names:tc:SAML:attribute:pairwise-id" store="Active Directory" name="norEduPersonLIN" >
  <transformvalue adfstkstorefunction="pairwiseid" />
</attribute>

<attribute type="urn:oasis:names:tc:SAML:attribute:subject-id" store="Active Directory" name="samaccountname" >
  <transformvalue adfstkstorefunction="subjectid" />
</attribute>

<attribute type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" store="Active Directory" name="mail">
  <transformvalue adfstkstorefunction="tolower" />
</attribute>
```

- Add `<transformvalue adfstkstorefunction="storefunction" />` to the attribute where you want to use the ADFS Toolkit Store
- Store Functions:
  - pairwiseid
  - subjectid
  - toupper/tolower
  - hash
  - base32

SWAMID

Subject ID Request

- SP can save what ID to use in the Metadata
  - subject-id
  - pairwise-id
  - none
  - any
    - We will choose the attribute with least personal data = pairwise-id
- Use `Get-ADFSTkToolSpInfoFromMetadata` to look at specific SP's in the Metadata

SWAMID

SchacDateOfBirth

- Old Regex:

```
^(18|19|20)?
[0-9]{2}
((0[0-9])|(10|11|12))
(((0-2][0-9])|(3[0-1]))|((6[1-9])|([7-8][0-9])|(9[0-1])))
[0-9]{4}$
```

- New Regex:

```
^(18|19|20)?
[0-9]{2}
((0[0-9])|(10|11|12))
(((0-2][0-9])|(3[0-1]))|((6[1-9])|([7-8][0-9])|(9[0-1])))
([A-Z0-9]{1}[0-9]{3}){0,1}$
```

SWAMID

SWAMID

Swedish Academic Identity Federation