SWAMID

Standardkonfiguration Shibboleth - vad är med?

Ta upp följande i er browser

- http://wiki.swamid.se/display/SWAMID/Standard+attribute-resolver.xml
- http://wiki.swamid.se/display/SWAMID/Standard+attribute-filter.xml

Standard attributdefinitioner

- I attribute-resolver.xml anger man hur man hämtar de attributvärden som man vill lämna ut till olika Service Providers
- I attribute-filter.xml anger man vilka attribut som skall lämnas till Service providers
- Genom att SWAMID inför entitetskategorier kommer det att bli lättare att konfigurera attribute-filter.xml, men inte nödvändigtvis lättare att hantera attribute-resolver.xml
- Vi kommer att publicera exempelversioner av attributfilerna, för att göra det enklare att konfigurera

Kort repetition av resolverns syntax

Lokal attributidentifierare

Typ av attribut (Simple/Scoped/Script/…)

```
<resolver:AttributeDefinition id="uid" xsi:type="Simple”
                              xmlns="urn:mace:shibboleth:2.0:resolver:ad”
                              sourceAttributeID="uid">
    <resolver:Dependency ref="myLDAP" />

    <resolver:AttributeEncoder xsi:type="SAML1String”
        xmlns="urn:mace:shibboleth:2.0:attribute:encoder”
        name="urn:mace:dir:attribute-def:uid" />

    <resolver:AttributeEncoder xsi:type="SAML2String"
        xmlns="urn:mace:shibboleth:2.0:attribute:encoder”
        name="urn:oid:0.9.2342.19200300.100.1.1"
        friendlyName="uid" />
</resolver:AttributeDefinition>
```

Attributnamn i källan

Behövd datakälla alt. annat attribut

Formell attribut-definition SAML1

Formell attribut-definition SAML2

Standardresolverns avsnitt

- **Core schema attributes, inetOrgPerson attributes**. Dessa scheman är standardscheman i LDAP och de flesta finns även i AD. Har man LDAP och/eller AD som källa kan attributen i allmänhet hämtas i källan utan omskrivningar. I vissa fall kan ett attribut heta något i källan men presenteras som något annat till Service providers, ex sAMAccountName (även om uid också finns i AD:s schema) som presenteras som uid (oid: 0.9.2342.19200300.100.1.1). Vissa av attributen som tillhör dessa scheman är av den arten att man kan presentera dom statiskt eftersom attributvärdet är det samma för hela IdP:n, ex c, o, co, schacHomeOrganization
- **eduPerson attributes, norEdu* attributes**. Dessa scheman finns normalt inte i en standard LDAP eller AD, så dessa får man lägga till eller skapa med hjälp av script och/eller andra attribut i sina källor. På SWAMIDs wiki finns åtskilliga exempel på hur detta görs. I detta sammanhang dyker också ”scope” upp, eduPersonScopedAffiliation och eduPersonPrincipalName, som det finns stöd för i Shibboleth, genom att ett scope läggs till efter ett attributvärde. Ett uid med värde admhn blir på KI ett eppn= admhn@ki.se. Här dyker också eduPersonTargetedID (EPTID) upp, som har en speciell konstruktion. PÅ SWAMIDs wiki finns beskrivning hur man sätter upp stöd för detta attribut.

Resolverns avsnitt (forts.)

- I standardresolvern finns tre datakällor, en statisk, en LDAP och en StoredID (för EPTID). Man kan ha flera olika datakällor även om de angivna är de vanliga.
- Datakällorna beskrivs som resolver:DataConnector och deras id hänvisas till som referens i attributdefinitionerna ovan
- Transient ID och persitant ID har sina hänvisningar som PrincipalConnector

Kort repetition av attributfiltersyntax

- I attribute-filter.xml definieras vilka attribut som skickas till vilken SP

Exempel:

Lokal filteridentifierare

Regel för vilka SP filterpolicyn gäller

```
<AttributeFilterPolicy id="entity-category-sfs-1993-1153">
    <PolicyRequirementRule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch”
                           attributeName=http://macedir.org/entity-category
                           attributeValue="http://www.swamid.se/category/sfs-1993-1153"/>
    <AttributeRule attributeID="norEduPersonNIN">
        <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```

Vilket attribut som ska skickas via attributets lokala identifierare

Särskilda regler för just detta attribut

Standardfiltrets delar

- Standardfiltret kan delas in i:
- Attribut som ges till alla (transient ID, eptid)
- Speciella SP som skall ha speciella attribut (i standardfiltret är NyA webben – *eduPersonEntitlement*, VHS – *personnummer* och Box – email och *eduPersonScopedAffiliation* med som exempel. En normal IdP på en högskola har i allmänhet flera sådana ”specialare”, som grundar sig på en bilateral överenskommelse mellan högskolan och en speciell SP
- En grupp av SP som man med förtroende kan lämna personuppgifter till dock ej personnummer

Standardfiltrets delar (forts.)

- entity-category-sfs-1993-1153 som får personnummer
- entity-category-research-and-education som innehåller följande swamidkategorier:
  - eu-adequate-protection
  - nren-service
  - hei-service
  - research-and-education
- Ovanstående får namn, email, eppn, scoped affiliation
- Alla som har metadata i SWAMIDs MD får namn och organisationsdata

Kan dessa standardfiler användas

- Ja förutom att de flesta nog har attributdefinitioner och attributvärden som behöver masseras i resolvern och vissa har speciella attribut som releasas till speciella Service Providers
- SWAMIDs wiki är full av exempel på hur man har skapat och masserat attribut lokalt
- Kommentarer?