Tjänstekategorier i SWAMID

Leif Johansson SWAMID WS2 2012

Problemen vi försöker lösa

- Attributrelease kräver ofta CM på varje IdP
- Svårt att planera och förutsäga introduktion av nya SPer
- Förvirrade användare som inte kommer in på sina SPer eftersom attributen inte skickas

Lösningen...

- Många nya SPer men ***få nya typer*** av SPer
- Alla SPer av en viss typ/kategori kan hanteras på samma sätt

Viktig princip #1

Varje medlem i SWAMID fattar egna beslut om hantering av persondata.

Viktig princip #2

SWAMID kan inte fatta beslut åt medlemmar men kan göra information tillgänglig som gör besluten enklare att fatta.

macedir.org/entity-category

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
      entityID="https://service.example.com/entity">
  <md:Extensions>
    <mdattr:EntityAttributes
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          Name="http://macedir.org/entity-category">
        <AttributeValue>http://example.org/category/dog</AttributeValue>
        <AttributeValue>urn:oid:1.3.6.1.4.1.21829</AttributeValue>
      </Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
</md:EntityDescriptor>
```

Hur fungerar det i SWAMID

- Operations ansvarar för kategorisering
- I swamid-2.0.xml finns följande kategorier:
  - Research & Education
  - SFS 1993:1153
- Två typer av kategorier
  - typ-kategorier
  - beteende-kategorier

Typ-kategorier

- Tjänsten **är** något
- SWAMID definierar 2 typ-katagorier:
  - Research & Education
  - SFS 1993:1153

Research & Education

- Baserat på InCommons Research and Scolarship
- Låg-risk-tjänster som är knutna till högskole-sektorn på något sätt.
- Tjänsterna i denna kategori hanterar bara grundläggande persondata

SFS 1993:1153

- Tjänster som lyder under "ladokförordningen"
- Endast VHS, SCB och högskolor/universitet kan äga tjänster i denna kategori.
- Tjänster i denna kategori har rätt att hantera känsliga personuppgifter (tex personnummer)

Beteende-kategorier

- Tjänsten **beter sig** på ett visst sätt

Beteende-kategorier

- EU Adequate Protection
  - Tillräckligt bra PII-hantering enligt EUs krav
- HEI-service
  - Tjänsten drivs av en högskola/universitet i SWAMID
- NREN-service
  - Tjänsten drivs av SUNET
- Signed Code-of-Conduct
  - cf Påls presentation av C-o-C
  - eg inte en kategori...

Exempel: antagning.se

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
      entityID="https://www.antagning.se/ecs-sp">
  <md:Extensions>
    <mdattr:EntityAttributes
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          Name="http://macedir.org/entity-category">
       <AttributeValue>http://www.swamid.se/category/sfs-1993-
1153</AttributeValue>
      </Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
</md:EntityDescriptor>
```

attribute-filter.xml

```
<AttributeFilterPolicy id="eduReleasePolicy">
      <PolicyRequirementRule xsi:type="saml:AttributeIssuerEntityAttributeExactMatch"
                  attributeName="http://macedir.org/entity-category"
                  attributeValue="http://www.swamid.se/category/sfs-1993-1153"/>
    ....
</AttributeFilterPolicy>
```

Vad händer nu?

- SWAMID Operations...
  - lägger på kategorier på ett antal tjänster
  - producerar dokumentation på wiki:n
  - publicerar exempel på XML till attribute-filter.xml
- IdP-ägare...
  - uppgradera Shibboleth IdP till 2.4.5 eller senare
  - skapa attribut-regler till attribute-filter.xml