SWAMID

Swedish Academic Identity Federation

Tjänster kommer att begära tillitsinformation vid inloggning, hur gör en IdP?

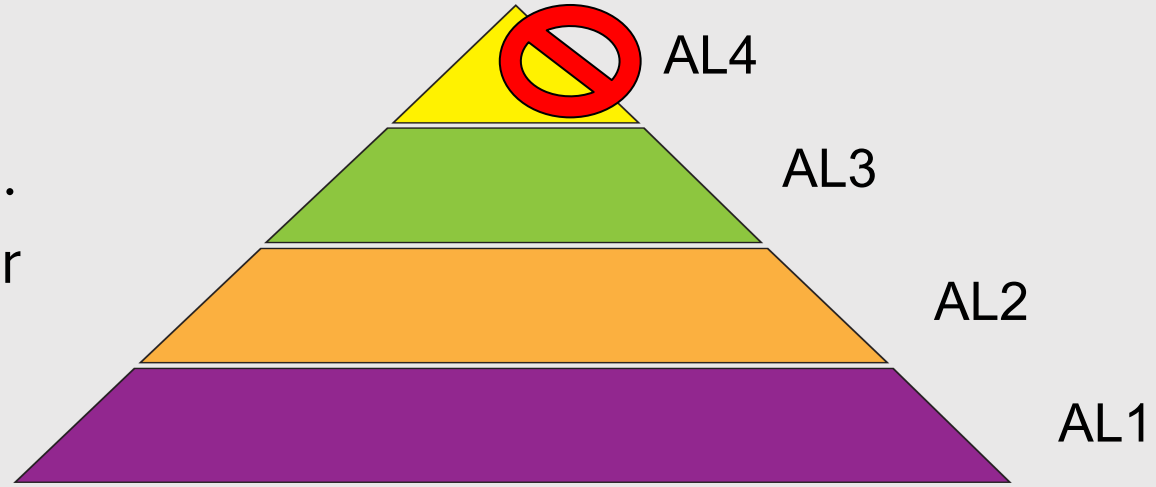
SWAMID

Vad är en tillitsprofil

- Tillitsprofiler är ett formaliserat sätt att beskriva
  - hur väl en organisation sköter sin användarhantering baserat på en fördefinierad skala
  - hur väl en organisation vet att en användare är den som han/hon utger sig att vara.
- Tillitsprofiler kallas ofta även för tillitsnivåer

Tillitspyramiden för användare

- **SWAMID AL1:** Vet att det är en person (obekräftad).
  Personuppgifterna är självuppgivna.
- **SWAMID AL2:** Vet vem personen är (bekräftad).
  Personuppgifter är hämtade från annan källa.
- **SWAMID AL3:** Vet mycket väl vem personen är (verifierad).
  Personen har uppvisat legitimation



SWAMID

Status för tillitsprofiler i SWAMID

- Från och med i år måste alla identitetsutfärdare i SWAMID vara godkända för minst en tillitsnivå
- 21 medlemmar är godkända för SWAMID AL1
- 39 medlemmar är godkända för SWAMID AL1 och AL2
- 3 medlemmar är godkända för SWAMID AL1, AL2 och AL3

Varför använda tillitsprofiler i SWAMID?

- Inom identitetsfederationen är tillit till att vi alla gör på liknade sätt väldigt viktigt
- Vissa tjänster har av personuppgifts-, spårbarhets- och riktighetsskäl behov av att veta att det är rätt person på en viss tillitsnivå som loggar in
- Tjänster med känsligt data kommer i framtiden kräva AL3
- Tjänster med personuppgifter kommer i framtiden kräva minst AL2
- AL1 är basnivån som alla måste uppfylla.

Hur signaleras tillitsprofil i SWAMID?

- I metadataattributet assurance-certification finns beskrivet vilka av SWAMIDs tillitprofiler en identitetsutgivare är godkänd för
- Identitetsutgivaren använder attributet eduPersonAssurance för att signalera vilka tillitsprofiler en användare är godkänd för
  - Signalera aldrig högre än vad identitetsutgivare är godkänd för
  - Om SWAMID AL1 signaleras SWAMID AL1
  - Om SWAMID AL2 signaleras SWAMID AL1 och SWAMID AL2
  - Om SWAMID AL3 signaleras SWAMID AL1, SWAMID AL2 och SWAMID AL3

Kräver någon tillitsprofiler för inloggning?

- Nais – samordning av riktat pedagogisk stöd
  - Idag krävs SWAMID AL3 för handläggare vid lärosätena beroende på att systemet innehåller känsliga personuppgifter
- Ladok kommer att kräva SWAMID AL2
  - 2023-01-01: Anställda med tillgång till nationell översikt
  - 2023-07-01: Alla anställda som loggar in i Ladok
  - 2024-01-01: Alla studenter med svenskt personnummer

SWAMID

Används tillitsprofiler internationellt?

- Inom eduGAIN används REFEDS Assurance Framework (RAF) för att signalera tillit
- Forskningstjänster är på väg att införa krav på tillitssignalering
  - Superdatormiljön LUMI i Finland som används av forskare i Sverige använder kommer från och med oktober komma börja ställa krav på minst tillitsnivån RAF Medium
  - National Institute of Health (NIH) i USA ställer krav på RAF Medium för vissa av sina tjänster
  - Flera forskningstjänster inom EU är på väg att börja ställa krav

Vad ska signaleras vid SWAMID AL1

- http://www.swamid.se/policy/assurance/al1
- https://refeds.org/assurance
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/ATP/ePA-1m

Vad ska signaleras vid SWAMID AL2

- http://www.swamid.se/policy/assurance/al1
- http://www.swamid.se/policy/assurance/al2
- https://refeds.org/assurance
- https://refeds.org/assurance/profile/cappuccino
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/IAP/medium
- https://refeds.org/assurance/IAP/local-enterprise
- https://refeds.org/assurance/ATP/ePA-1m

SWAMID

Vad man signaleras vid SWAMID AL3

- http://www.swamid.se/policy/assurance/al1
- http://www.swamid.se/policy/assurance/al2
- http://www.swamid.se/policy/assurance/al3
- https://refeds.org/assurance
- https://refeds.org/assurance/profile/cappuccino
- https://refeds.org/assurance/profile/espresso
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/IAP/medium
- https://refeds.org/assurance/IAP/high
- https://refeds.org/assurance/IAP/local-enterprise
- https://refeds.org/assurance/ATP/ePA-1m

Och nu till tekniken...

- Attributrelease av tillitsnivåer i
  - Shibboleth
  - ADFS

Shibboleth ”enklast” ?

Plocka attributet rakt från LDAP

```
<AttributeDefinition xsi:type="Simple" id="eduPersonAssurance">
    <InputDataConnector ref="myLDAP" attributeNames="eduPersonAssurance"/>
   <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonAssurance" encodeType="false" />
   <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11" friendlyName="eduPersonAssurance"
encodeType="false" />
</AttributeDefinition>
```

SWAMID

```
<AttributeDefinition xsi:type="ScriptedAttribute" id="eduPersonAssurance">
    <InputDataConnector ref="myLDAP" attributeNames="extensionAttribute1" />
    <Script><![CDATA[
      if (typeof extensionAttribute1 !== 'undefined') {
        if (extensionAttribute1.getValues().get(0) == "AL2") {
          eduPersonAssurance.getValues().add("http://www.swamid.se/policy/assurance/al1");
          eduPersonAssurance.getValues().add("http://www.swamid.se/policy/assurance/al2");
          eduPersonAssurance.getValues().add("https://refeds.org/assurance");
        ...och övriga RAF-attribut...}
      if (extensionAttribute1.getValues().get(0) == "AL1") {
        eduPersonAssurance.getValues().add("http://www.swamid.se/policy/assurance/al1");
        eduPersonAssurance.getValues().add("https://refeds.org/assurance");
      ...och övriga RAF-attribute... }
     }
    ]]></Script>
    <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonAssurance" encodeType="false" />
    <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11" friendlyName="eduPersonAssurance"
encodeType="false" />
</AttributeDefinition>
```

SWAMID

Shibboleth bäst ?

https://wiki.sunet.se/display/SWAMID/Example+of+a+standard+attribute+resolver+for+Shibboleth+IdP+v4+and+above

För stor för att klistra in här :-)

SWAMID

Swedish Academic Identity Federation

Länkar

- https://wiki.sunet.se/display/SWAMID/Example+of+a+standard+attribute+resolver+for+Shibboleth+IdP+v4+and+above
- https://wiki.sunet.se/display/SWAMID/Release+of+assurance+statements+in+the+attribute+eduPersonAssurance+based+on+SWAMID+Identity+Profiles
- https://refeds.org/assurance (RAF)
- https://refeds.org/specifications

SWAMID