SUNET

Personlig integritet, PUL och federationer

Attributöverföring från IdP till SP

Attribut som skickas delas in i fyra olika kategorier:

- Personinformation
  - Exempel: namn, e-postadress, personnummer, pseudonym identifierare, eduPersonPrincipalName
- Organisationsinformation
  - Exempel: organisationsnamn, organisationsland
- Övrig information t.ex. auktorisering
  - Exempel: eduPersonAffiliation, eduPersonEntitlement
- Teknisk information (IdP, IP-adress mm.)

Överföring av personinformation

- Personinformation i attributöverföring är behandling av personuppgifter
- För behandling av personuppgifter gäller PUL (om inte annan lag gäller)
- PUL säger att personuppgifter får behandlas utan samtycke om behandlingen är nödvändig
- Detta innebär att en IdP får skicka nödvändiga attribut för att tjänsten ska fungera utan att användaren behöver ge sitt aktiva samtycke.

Överföring av personnummer

Personuppgiftslagen 22 §

- Uppgifter om personnummer eller samordningsnummer får utan samtycke behandlas bara när det är klart motiverat med hänsyn till
  a) ändamålet med behandlingen,
  b) vikten av en säker identifiering, eller
  c) något annat beaktansvärt skäl.

Överföring av personuppgifter till tredje land

Personuppgiftslagen 33 §

Det är förbjudet att till tredje land föra över personuppgifter som är under behandling om landet inte har en adekvat nivå för skyddet av personuppgifterna. Förbudet gäller också överföring av personuppgifter för behandling i tredje land.

- Enligt 34 § är det tillåtet att överföra personuppgifter efter samtycke till överföringen eller om överföringen är nödvändig (t.ex. fullföljande eller tecknande av avtal)
- Enligt 35 § är det i vissa fall även tillåtet med överföring om tillräckligt skydd finns, s.k. safe harbor

Code of Conduct (eduGAIN)

- Inom interfederationen eduGAIN (tillgänglig via SWAMID 2.0) arbetas det på ett ta fram en modell ***Code of Conduct*** (CoC) där SP kan deklarera att de hanterar personuppgifter korrekt och att de endast begär nödvändiga attribut för att underlätta överföring
  - Förankring pågår med företrädare för den specialistgrupp som jobbar med EU-direktivet som styr PUL, tongångarna är positiva
- Detta innebär att en IdP i framtiden kan fatta automatiska och informerade beslut om överföring av personuppgifter till en SP om CoC finns.
- SWAMID kommer lägga in info om SP CoC i metadata

SUNET

SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0 (MDUI)

Vad är MDUI

- MDUI är ett antal utökade attribut som placeras i metadata för IdP eller SP
- MDUI har två syften
  1. Förbättra utseende och möjliggöra intelligenta gissningar på lämplig IdP i anvisningstjänster (Discovery Service, DS)
  2. Tillgängliggöra, för IdP och DS, information om tjänster (SP) som användaren ska logga in i

MDUI User Interface Information DisplayName

- Visningsnamn på ett eller flera språk, kan ge bättre information än organisationsinformation i metadata
- Rekommenderas starkt för alla IdP och SP
- Exempel:
  - <mdui:DisplayName xml:lang="**sv**">**Uppsala universitet**</mdui:DisplayName>
  - <mdui:DisplayName xml:lang="**en**">**Uppsala University**</mdui:DisplayName>

MDUI User Interface Information Description

- En kortare beskrivning på max 140 tecken på ett eller flera språk om IdP resp. SP
- Rekommenderas starkt för alla IdP och SP
- Exempel:
  - <mdui:Description xml:lang="sv">Identity Provider för anställda, studenter och övriga verksamma vid Uppsala universitet.</mdui:Description>
  - <mdui:Description xml:lang="en">The Uppsala University Identity Provider is used by employees and students at the university.</mdui:Description>

MDUI User Interface Information InformationURL

- Webbadress till fördjupad information om IdP resp. SP
- Frivillig information i metadata för IdP och SP
- Exempel:
  - <mdui:InformationURL xml:lang="**sv**”> **https://cas.user.uu.se/cas/om.html** </mdui:InformationURL>
  - <mdui:InformationURL xml:lang="**en**"> **https://cas.user.uu.se/cas/about.html** </mdui:InformationURL>

MDUI User Interface Information PrivacyStatementURL

- För identitetsutgivare (IdP): Webbadress till identitetsutgivarens integritetspolicy för de identiteter som tillhandahålls genom identitetsutgivaren
- För tjänster (SP): Webbadress till tjänstens integritetspolicy som beskriver hur de hanterar information om användaren, dvs. ***Code of Conduct***. Policyn ska bl.a. innehålla vilka attribut som krävs av tjänsten samt vad de används till.
- Frivillig information i metadata för IdP och SP

MDUI User Interface Information Logo

- HTTPS-baserad webbadress till en logotyp för IdP resp. SP
- Frivillig information i metadata för IdP och SP men anges informationen krävs att vissa villkor är uppfyllda runt åtkomst till och format för logotypen (mer information finns på wikin)
- Exempel:
  - <mdui:Logo height="**125**" width="**125**"> **https://cas.user.uu.se/cas/uu_img/125_uu_logo_white.gif**</mdui:Logo>

MDUI Discovery Hinting Information

- Information för att ge intelligenta gissningar på lämplig IdP i en anvisningstjänst (DS)
- Frivillig information för IdP
- Finns tre typer av MDUI DHI
  - IP-adresser i CIDR-block
    - Exempel: <mdui:IPHint>**130.238.128.0/17**</mdui:IPHint>
  - Domännamn
    - Exempel: <mdui:DomainHint>**uu.se**</mdui:DomainHint>
  - Geolokalisering
    - Exempel: <mdui:GeolocationHint>**geo:59.857583,17.629500** </mdui:GeolocationHint>

Mer information om MDUI

- MDUI för IdP (information på svenska)
  - https://portal.nordu.net/x/nh7cAQ
- MDUI för SP (information på engelska)
  - https://portal.nordu.net/x/Xx-cAQ

- SWAMID Operations lägger in MDUI i metadata på uppmaning av respektive IdP och SP