SWAMID Identity Provider MDUI requirements

Konfigurationerna på denna sida görs inte i indentitetsutgivaren (IdP) utan endast i federationens metadata om indentitetsutgivaren.

Inom SWAMID rekommenderas det starkt att åtminstone utökningarna <mdui:DisplayName> och <mdui:Description> används av alla indentitetsutgivare. I kommande SWAMID AL1 införs krav på användning av vissa MDUI-element.

För att möjliggöra en mer användarvänlig anvisningtjänst (Discovery Service) har OASIS tagit fram SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0 (MDUI). Denna utökning av metadata gör det möjligt att ge en bättre användarupplevelse i anvisningstjänsten, möjlighet för en tjänsteleverantör (Service Provider) att ge information om använd indentitetsutgivare (Identity Provider) och möjlighet för en indentitetsutgivare att ge information om tjänsteleverantören på inloggningssidan. Denna sida är inriktad på informationen om en indentitetsutgivare som kan användas i anvisningstjänsten och hos tjänsteleverantören.

För att lägga MDUI-information om din identitetsutgivare ska du skapa XML-data enligt nedanstående information och skicka den till SWAMID Operations.

Motsvarande information om utökning av metadata för tjänstelerantörer finns på sidan SP Metadata Extensions for Login and Discovery User Interface (MDUI). Shibboleth Idp 2.3 och senare kan via särskilda taggar inkludera MDUI-informationen från tjänsteleverantörer på inloggningssidan.

Information för visning i webbgränssnitt (User Interface Information)

Utökningarna för webbgränssnitt är inriktade mot att ge mer och bättre information om indentitetsutgivaren. Utökningarna består bland annat av namn på identitetsutgivaren, kommentar om identitetsutgivaren, webbadress till ytterligare information om indentitetsutgivaren samt webbadress till indentitetsutgivarens integritetspolicy.

MDUI SAML tag	Basic	SWAMID AL1
mdui:DisplayName	SHOULD	MUST
mdui:Description	SHOULD	MUST
mdui:InformationURL	MAY	SHOULD
mdui:PrivacyStatementURL	MAY	MUST
mdui:Logo	MAY	SHOULD

Visningsnamn (<mdui:DisplayName>)

Det namn på indentitetsutgivaren som ska visas anvisningstjänsten. Lämpligt att använda lärosätets namn. Med <mdui:DisplayName xml:lang="sv"> och <mdui:DisplayName xml:lang="en"> går det att definiera olika namn på svenska och engelska.

Beskrivning (<mdui:Description>)

En kortare beskrivning om maximalt 140 tecken om identitetsutgivaren. Det är lämpligt att ha beskrivningar på både svenska och engelska.

Webbadress för ytterligare information (<mdui:InformationURL>)

Webbadress för ytterligare information om identitetsutgivaren. Det är möjligt att olika adresser för olika språk.

Webbadress för integritetspolicy (<mdui:PrivacyStatementURL>)

Webbadress till identitetsutgivarens integritetspolicy för de indentiteter som tillhandahålls genom identitetsutgivaren. Det är möjligt att olika adresser för olika språk.

Webbadress för logotyp (<mdui:Logo>)

Webbadress till logotyp för identitetsutgivaren.

Följande gäller för logotypen:

- Webbadressen ***SKA*** vara av typen HTTPS, d.v.s. krypterad.
- Logotypen ***SKA*** vara publicerad via en oskyddad länk, d.v.s. den ska inte behöva inloggning för att få visas.
- Logotypen ***SKA*** vara publicerad på en värddator i en domän som ägs av identitetsutgivaren.
- Logotypen ***SKA*** vara i formaten PNG (bäst) eller GIF.
- Storlek i pixlar på logotypen ***SKA*** anges i XML-tagen, se exemplet.
- Logotypen ***BÖR*** vara i liggande format, inte stående, d.v.s. bredd är större eller lika med höjd.
- Bakgrunden ***BÖR*** vara genomskinlig och fungera lika bra på vit som grå bakgrund.
- Det är möjligt att ha flera logotyper i olika storlekar för anpassning till olika anvisningstjänster.

    - Tillhandahåll en logotyp i lärosätets standardformat för webben helst inom storleksområdet 64px till 350px bred och 64px till 146px hög.
    - Tillhandahåll eventuellt en särskild logotyp på 16x16 punkter för Shibboleth EDS, ingår i Shibboleth SP 2.4 och senare.
- Det är möjligt att ha olika logotyper för olika språk på samma sätt som visningsnamnet.

Exempel på utökat metadata för Exempelorganisationen

```
<mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
  <mdui:DisplayName xml:lang="sv">Exempelorganisationen</mdui:DisplayName>
  <mdui:DisplayName xml:lang="en">Example organization</mdui:DisplayName>
  <mdui:Description xml:lang="sv">Identity Provider för Exempelorganisationen.</mdui:Description>
  <mdui:Description xml:lang="en">Identity Provider for Example organization.</mdui:Description>
  <mdui:InformationURL xml:lang="sv">https://idp.exempel.se/info/om.html</mdui:InformationURL>
  <mdui:InformationURL xml:lang="en">https://idp.exempel.se/info/about.html</mdui:InformationURL>
  <mdui:PrivacyStatementURL xml:lang="sv">https://idp.exempel.se/info/integritet.html</mdui:PrivacyStatementURL>
  <mdui:PrivacyStatementURL xml:lang="en">https://idp.exempel.se/info/privacy.html</mdui:PrivacyStatementURL>
  <mdui:Logo height="100" width="100">https://idp.exempel.se/images/logo.png</mdui:Logo>
</mdui:UIInfo>
```

Information för automatiskt förslag på identitetsutgivare (Discovery Hinting Information)

Det är ur ett användarperspektiv bra om anvisningstjänsten automatiskt kan föreslå, men inte automatiskt välja, lämplig identitetsutgivare när en användare ska logga in. Med utökningen Discovery Hinting Information är det möjligt för en identitetsutgivare att för en anvisningstjänst tala om att inom dessa begränsningar är "jag" troligaste identitetsutgivaren. I utökningen finns det tre olika sätt att beskriva detta; via domännamn, via IP-adresser och via geolokalisering. Observera att denna typ av lokaliseringstjänst är att endast ses som förslag och får därför inte användas till automatiskt val av identitetsutgivare.

MDUI SAML tag	Basic	SWAMID AL1
mdui:IPHint	MAY	MAY
mdui:DomainHint	MAY	MAY
mdui:GeolocationHint	MAY	MAY

IP-adresser (<mdui:IPHint>)

IP4- eller IPv6-adressområde som identitetsutgivaren äger eller agerar inom skrivet som CIDR-block (RFC4632). CIDR-block har formen IP-nät /signifikanta-bitar, t.ex. 192.168.1.0/24 innebär alla IP-adresser inom området 192.168.1.0 till 192.168.1.255. Det är möjligt att noll eller flera <mdui:IPHint>.

Domännamn (<mdui:DomainHint>)

Domännamn som identitetsutgivaren äger eller agerar inom. Det är möjligt att noll eller flera <mdui:DomainHint>.

Geolokalisering (<mdui:GeolocationHint>)

Latitude och longtitud för platsen där identitetsutgivarens användare troligtvis befinner sig. Koordinaterna skrivs på URN-form enligt geo URI-schemat (RFC 5870). Den enklaste formen är geo:decimal latitude,decimal longitude, t.ex. geo:59.3267,18.07175 för Stockholms slott. Det är möjligt att noll eller flera <mdui:GeolocationHint>.

Exempel på utökat metadata för Exempelorganisationen

```
<mdui:DiscoHints xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
  <mdui:IPHint>192.1068.1.0/24</mdui:IPHint>
  <mdui:DomainHint>exempel.se</mdui:DomainHint>
  <mdui:GeolocationHint>geo:59.3267,18.07175</mdui:GeolocationHint>
</mdui:DiscoHints>
```