Guide: Scope in metadata

Introduktion

Ett scope används för att förhindra sammanblandning av identiteter. Om användare från två olika användarorganisationer loggar in i en tjänst till exempel en digital lärresurs och har likadana användarnamn uppfattar tjänsten att det är samma användare. Att sätta scope på ett attribut gör det möjligt för tjänsten att knyta attributet till utfärdande Identity Provider (IdP). Om man sätter scope på ett identitetsattribut till exempel eduPersonPrincipalName (EPPN) kommer inte Pelle Andersson från skolhuvudmannen Lerum och Pelle Andersson från skolhuvudmannen Mjölby ses som samma användare av tjänsten.

I Skolfederation gäller att (minst) ett unikt scope måste finnas för varje skolhuvudman som är medlem i och har ett avtal med Skolfederation.

Om en IdP blir komprometterad kan den IdP:n användas för att skicka identitetsattribut med värdet satt till valfri användare i hela federationen. Med scopade attribut kan en SP filtrera inkommande attribut och avgöra om en IdP skickar attribut för rätt användarorganisation. Det medför att den komprometterade IdP:n bara kan skicka attribut för den användarorganisation som IdP:n representerar.

För att en SP ska kunna använda sig av scope behöver mjukvaran ha stöd för det, samt vara konfigurerad på korrekt sätt. Tillsvidare avråder vi från att slå på kontrollen då man stänger ute de IdPer som inte har sitt scope i metadata. Vi kommer att informera när det är dags att aktivera kontrollen.

Format

Scope är en utökning, en så kallad Extension, och formateras enligt nedan.

```
<md:Extensions xmlns:shibmd="urn:mace:shibboleth:metadata:1.0">
  <shibmd:Scope regexp="false">exempelskolan.se</shibmd:Scope>
</md:Extensions>
```

För att Skolfederation ska kunna validera att er skola äger den domän ni deklarerar måste domänen i Scope vara en ägd domän som går att kolla upp.

Exempel

Nedan följer exempel på hur Scope kan placeras i metadata.

Scope som gäller alla roller i metadata

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09
/xmldsig#" entityID="https://exempelskolan.se/idp">
    <md:Extensions xmlns:shibmd="urn:mace:shibboleth:metadata:1.0">
      <shibmd:Scope regexp="false">exempelskolan.se</shibmd:Scope>
    </md:Extensions>
    <md:IDPSSODescriptor>
      ...
    </md:IDPSSODescriptor>
    <md:AttributeAuthorityDescriptor>
      ...
    </md:AttributeAuthorityDescriptor>
    <md:Organization>
      ...
    </md:Organization>
    <md:ContactPerson>
      ....
    </md:ContactPerson>
</md:EntityDescriptor>
```

Scope som gäller en roll i metadata

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09
/xmldsig#" entityID="https://exempelskolan.se/idp">
    <md:IDPSSODescriptor>
      <md:Extensions xmlns:shibmd="urn:mace:shibboleth:metadata:1.0">
        <shibmd:Scope regexp="false">exempelskolan.se</shibmd:Scope>
      </md:Extensions>
      ...
    </md:IDPSSODescriptor>
    <md:AttributeAuthorityDescriptor>
      ...
    </md:AttributeAuthorityDescriptor>
    <md:Organization>
      ...
    </md:Organization>
    <md:ContactPerson>
      ....
    </md:ContactPerson>
</md:EntityDescriptor>
```

Flera Scope i metadata

Har ni flera säkerhetsdomäner att deklarera i metadata så gör detta på fristående rader, enligt nedan:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09
/xmldsig#" entityID="https://exempelskolan.se/idp">
    <md:IDPSSODescriptor>
      <md:Extensions xmlns:shibmd="urn:mace:shibboleth:metadata:1.0">
        <shibmd:Scope regexp="false">exempelskolan.se</shibmd:Scope>
        <shibmd:Scope regexp="false">edu.exempelskolan.se</shibmd:Scope>
      </md:Extensions>
      ...
    </md:IDPSSODescriptor>
    <md:Organization>
      ...
    </md:Organization>
    <md:ContactPerson>
      ....
    </md:ContactPerson>
</md:EntityDescriptor>
```

Scope stödjer reguljära uttryck, men det rekommenderas **inte** att använda sig utav det då det finns problem med att konsumerande SP-produkter inte kan hantera det. Deklarera istället varje domän och underdomän som ni använder er av för sig enligt ovan.

Skolfederation tillåter inte reguljära uttryck i Scope.