Autentisering med uppdragslös IdP

Tjänst under avveckling

Dessa sidor kommer att tas bort 2023-01-01

Uppdragslös IdP möjliggör att autentisering av en web-klient kan ske utan att man behöver göra ett uppdragsval, vilket exempelvis är användbart i de fall man bara har krav på identifiering och inte vill ha behörighetsstyrande attribut.

Detta kan uppnås genom att man nyttjar delar som är specificerade inom SAML och kombinerar data i entiteterna *IDPSSODescriptor*, *SPSSODescriptor* samt *AuthnRequest*.

För att kunna nyttja uppdragslös IdP måste de SP som vill ha denna funktionalitet uppdatera sitt SP-metadata (SPSSODescriptor). En SP som vill kunna välja om uppdragsval skall göras eller ej måste införa ett nytt element (med sub-element) i sitt metadata: <AttributeConsumingService>.

Specifikation enligt SAML v2.0

IDPSSODescriptor (IdP-metadata)

IdP:n specificerar i sitt metadata vilka attribut som den kan leverera. Nedanstående bild beskriver hur IdP-metadatat kan se ut med exempel på olika attribut som IdP:n kan tillhandahålla.

IDPSSODescriptor

```
<saml:Attribute Name="urn:sambi:names:attribute:levelOfAssurance" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="levelOfAssurance"/>
<saml:Attribute Name="http://sambi.se/attributes/1/employeeHsaId" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="employeeHsaId"/>
<saml:Attribute Name="http://sambi.se/attributes/1/givenName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri" FriendlyName="givenName"/>
<saml:Attribute Name="http://sambi.se/attributes/1/systemRole" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri" FriendlyName="systemRole"/>
<saml:Attribute Name="http://sambi.se/attributes/1/commissionHsaId" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="assignmentHsaId"/>
```

SPSSODescriptor (SP-metadata)

En SP kan välja att lägga till 0..n <AttributeConsumingService> i sitt metadata som sub-element till SPSSODescriptor. Dessa kommer sedan via sitt index matchas mot angivet värde i ett AuthnRequest. Baserat på vilka attribut som en SP begär vid ett specifikt autentiseringstillfälle kommer IdP:n avgöra om uppdragsval (eller HSA-uppslag generellt) behöver göras eller ej.

Nedan följer tre exempel som en SP kan ange för att kunna uppnå olika sorters attributuppslag i sin autentisering av användare.

OBS! Notera att nedanstående enbart är exempel! Dvs det är inte dessa specifika attribut som styr om ett uppdragsval skall göras eller ej, utan dessa är enbart exempel.

Utan HSA-uppslag

```
<AttributeConsumingService index="0" isDefault="true">
  <ServiceName xml:lang="sv">TestSP utan HSA-uppslag</ServiceName>
  <RequestedAttribute Name="urn:sambi:names:attribute:levelOfAssurance" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="levelOfAssurance"/>
</AttributeConsumingService>
```

Då denna AttributeConsumingService är satt till default så är det denna som kommer användas om SP:n i sitt AuthnRequest avstår från att ange vilken service som skall användas.

Servicen för detta index innehåller enbart ett attribut som IdP:n skall leverera. Eftersom detta attribut inte kräver något HSA-uppslag kommer IdP:n att autentisera användaren utan att använda HSA-katalogen. IdP:n kommer alltid försöka göra så lite som möjligt för att uppnå en SP:s begäran om önskade attribut. Enbart de attribut som efterfrågas kommer tillhandahållas (försöka tillhandahållas).

Med HSA-uppslag

```
<AttributeConsumingService index="1">
  <ServiceName xml:lang="sv">TestSP med HSA-uppslag</ServiceName>
  <RequestedAttribute Name="urn:sambi:names:attribute:levelOfAssurance" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="levelOfAssurance"/>
  <RequestedAttribute Name="http://sambi.se/attributes/1/givenName" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="givenName" isRequired="true"/>
  <RequestedAttribute Name="http://sambi.se/attributes/1/systemRole" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="systemRole"/>
</AttributeConsumingService>
```

Om denna AttributeConsumingService efterfrågas kommer IdP:n vara tvungen att utföra en HSA-slagning för att ta reda på värden för (åtminstone) "systemRole". Dock kommer inget uppdragsval göras då båda dessa attribut är oavhängiga av ett uppdrag. "givenName" har i detta fall tillägget "isRequired". Detta innebär att SP:n kräver att detta attribut finns med. Om IdP inte kan få fram detta attribut kommer den misslyckas med autentisering.

Med uppdragsval

```
<AttributeConsumingService index="2">
  <ServiceName xml:lang="sv">TestSP med uppdragsval</ServiceName>
  <RequestedAttribute Name="urn:sambi:names:attribute:levelOfAssurance" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="levelOfAssurance"/>
  <RequestedAttribute Name="http://sambi.se/attributes/1/givenName" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="givenName"/>
  <RequestedAttribute Name="http://sambi.se/attributes/1/systemRole" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" FriendlyName="systemRole"/>
  <RequestedAttribute Name="http://sambi.se/attributes/1/commissionHsaId" NameFormat="urn:oasis:names:tc:SAML:
2.0:attrname-format:uri" FriendlyName="assignmentHsaId"/>
</AttributeConsumingService>
```

I denna AttributeConsumingService begär SP:n attribut som enbart kan tillhandahållas då IdP:n ber aktören om ett uppdragsval. IdP:n kommer att göra sitt bästa för att tillhandahålla de attribut som SP:n begär, men då inget av attributen är angivna som required så kommer autentisering lyckas, oavsett hur många attribut som SP:n får tillbaka. Det är senare upp till SP:n att avgöra vad man vill göra med biljetten.

AuthnRequest

För varje AuthnRequest så anger SP:n vilken av tidigare specificerade AttributeConsumingService som skall användas. Detta gör att en SP kan begära olika beteende för olika autentiseringar. SP:n väljer att ange AttributeConsumingServiceIndex som skall kunna matchas mot ett index som finns i dess metadata. Nedan följer fyra exempel.

Utan HSA-uppslag

```
<samlp:AuthnRequest xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ForceAuthn="false" IsPassive="false" ProviderName="Sp Example Name"
    ID="ID850325636986645032969715339748802383986121801227" Version="2.0"
    IssueInstant="2013-03-21T09:31:17.235Z" Destination="https://acctest.sakerhetstjanst.inera.se:8445/idp/saml
/sso/HTTP-Redirect"
    Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
        AttributeConsumingServiceIndex="0">
```

SP:n skickar in att index=0 skall nyttjas. Detta mappar i våra exempel ovan mot att HSA-uppslag **inte** kommer göras.

Med HSA-uppslag

```
<samlp:AuthnRequest xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ForceAuthn="false" IsPassive="false" ProviderName="Sp Example Name"
    ID="ID850325636986645032969715339748802383986121801227" Version="2.0"
    IssueInstant="2013-03-21T09:31:17.235Z" Destination="https://acctest.sakerhetstjanst.inera.se:8445/idp/saml
/sso/HTTP-Redirect"
    Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
        AttributeConsumingServiceIndex="1">
```

SP'n skickar in att index=1 skall nyttjas. Detta mappar i våra exempel ovan mot att HSA-uppslag kommer göras.

Med uppdragsval

```
<samlp:AuthnRequest xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ForceAuthn="false" IsPassive="false" ProviderName="Sp Example Name"
    ID="ID850325636986645032969715339748802383986121801227" Version="2.0"
    IssueInstant="2013-03-21T09:31:17.235Z" Destination="https://acctest.sakerhetstjanst.inera.se:8445/idp/saml
/sso/HTTP-Redirect"
    Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
        AttributeConsumingServiceIndex="2">
```

SP'n skickar in att index=2 skall nyttjas. Detta mappar i våra exempel ovan mot att uppdragsval kommer krävas.

Beror på...

```
<samlp:AuthnRequest xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ForceAuthn="false" IsPassive="false" ProviderName="Sp Example Name"
    ID="ID850325636986645032969715339748802383986121801227" Version="2.0"
    IssueInstant="2013-03-21T09:31:17.235Z" Destination="https://acctest.sakerhetstjanst.inera.se:8445/idp/saml
/sso/HTTP-Redirect"
    Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified">
```

Här har skickar SP:n inte med något index. I exemplen ovan så leder detta till att index=0 kommer att användas (dvs utan HSA-uppslag), eftersom index=0 var satt som default.

Om SP-metadata inte innehåller några definitioner för AttributeConsumingService, eller där ingen av dessa är satt som default, så hade denna AuthnRequest lett till att IdP:n begär uppdragsval och kommer leverera så många attribut den kan. Detta är det beteende som IdP:n haft innan funktionen Uppdragslös IdP infördes och säkerställer alltså bakåtkompabilitet.

Aktiviteter för SP

För att kunna nyttja funktionaliteten för uppdragslös IdP så kommer de SP:s som vill ha detta att behöva uppdatera sitt metadata samt sina AuthnRequest. Beskrivningarna nedan sammanfattar vad som krävs från en SP:s synsätt.

Implicit uppdragsval (Bakåtkompabilitet)

Innebär att IdP:n kommer att begära att ett uppdragsval görs. För detta så krävs ingen förändring från SP:n, samma metadata och AuthnRequest kan användas.

Explicit uppdragsval

SP:n måste skicka in metadata som innehåller minst en AttributeConsumingService där man specificerat vilka attribut man är intresserad av för detta index. För att uppdragsval skall begäras så måste minst ett av dessa attribut vara härlett ur ett uppdrag.

SP:n måste uppdatera sitt AuthnRequest med att begära detta index. Alternativt kan de i sitt metadata ange att detta index skall vara default, och då krävs ingen uppdatering av AuthnRequest.

Utan uppdragsval

SP:n måste skicka in metadata som innehåller minst en AttributeConsumingService, där man specificerat vilka attribut man är intresserad av för detta index. För att uppdragsval **inte** skall ske så får inget av dessa attribut vara härledda från ett uppdrag.

SP'n måste uppdatera sitt AuthnRequest med att begära detta index. Alternativt kan de i sitt metadata ange att detta index skall vara default, och då krävs ingen uppdatering av AuthnRequest.