2.2 Attributstyrning SAML

Revisionshistorik

Version	Datum	Författare	Kommentar
0.8	13 Jun 2018	Okänd användare (peterssond)	Upprättad
1.0	25 Oct 2018	Okänd användare (peterssond)	Fastställd
2.2	23 Nov 2021	Ehlert, Stefan	Uppdaterad med information kring allCommissions, allEmployeeHsaIds och ADFS-metadata

1. Inledning

SAML attributstyrning innebär att en SP själv kan ange i sitt metadata (i kombination med sitt `<AuthnRequest>`) vilka attribut som efterfrågas för alla, eller en specifik autentisering. Detta 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>`.

En SP som förväntar sig ta emot attribut via `<AttributeStatement>` från IdP:n måste ange 1..* `<AttributeConsumingService>` i sitt metadata. Detta ligger till grund för funktionaliteten som beskrivs nedan.

Specifikation enligt SAML v2.0

2. 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"/>
```

3. SPSSODescriptor (SP-metadata)

En SP kan välja att lägga till 1..* `<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 ett gäng 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.

3.1. AttributeConsumingService utan HSA-uppslag

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. Enbart de attribut som efterfrågas kommer tillhandahållas (försöka tillhandahållas).

3.2. AttributeConsumingService med HSA-uppslag

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.

3.3. AttributeConsumingService med uppdragsval

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 *"isRequired"* 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.

3.4. AttributeConsumingService med samtliga uppdragsval

Samtliga uppdragsval utan val i IdP:n

```
<AttributeConsumingService index="3">
  <ServiceName xml:lang="sv">TestSP med samtliga uppdragsval</ServiceName>
  <RequestedAttribute Name="urn:allCommissions" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
FriendlyName="allCommissions"/>
</AttributeConsumingService>
```

Om man vill undvika uppdragsval i de fall som en användare har flera uppdrag och man vill ha all uppdragsinformation så kan man begära attributet allCommissions som i denna `<AttributeConsumingService>`. Detta kan vara användbart i situationer då SP:n vill ha användarens fullständiga behörighet. Detta kommer leda till att IdP:n gör en slagning mot HSA för att hämta samtliga uppdragsval för användaren. Däremot kommer IdP:n i detta scenario inte be användaren göra något uppdragsval. Samtliga uppdragsval kommer skickas tillbaka i biljetten.

3.5. AttributeConsumingService med samtliga uppdragsval med val i IdP:n

Samtliga uppdragsval med val i IdP:n

```
<AttributeConsumingService index="4">
  <ServiceName xml:lang="sv">TestSP med samtliga uppdragsval och uppdragsval i IdP:n</ServiceName>
  <RequestedAttribute Name="urn:allCommissions" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
FriendlyName="allCommissions"/>
  <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 attributen allCommissions och assignmentHsaId. I detta fall kommer IdP:n precis som ovan hämta samtliga uppdragsval från HSA och returnera dessa i biljetten. Dock så kommer användaren i det här fallet ändå behöva göra ett uppdragsval i IdP:n för att IdP:n ska kunna returnera ett värde för assignmentHsaId.

3.6. AttributeConsumingService med samtliga HSA ID:n

Samtliga HSA ID:n

```
<AttributeConsumingService index="5">
  <ServiceName xml:lang="sv">TestSP med samtliga HSA ID:n för användaren</ServiceName>
   <RequestedAttribute Name="urn:allEmployeeHsaIds" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:
uri" FriendlyName="allEmployeeHsaIds"/>
</AttributeConsumingService>
```

Om man vill undvika uppdragsval i de fall som en användare har flera HSA ID:n och/eller flera uppdrag och man bara vill ha ett HSA ID:n kan man begära attributet allEmployeeHsaIds som visas i denna `<AttributeConsumingService>`. Då returneras en lista av HSA ID:n och SP:n kan då välja ett av dessa, t.ex. via en användardialog.

3.7. Utan AttributeConsumingService (ADFS-metadata)

IdP:n stödjer även metadata där ingen `<AttributeConsumingService>` finns med. Dessa fall borde uteslutande vara när ADFS-metadata tillhandahålls för anslutning mot Ineras IdP. I dessa fall kan det anslutande systemet fortfarande begära attribut från IdP:n. Vid anslutningen måste en lista av attribut anges som det anslutande systemet vill ha i varje biljett efter lyckad autentisering. Det är denna lista av attribut som IdP:n alltid kommer försöka lösa in. I stunden då autentiseringen utförs finns alltså ingen möjlighet att begära ett annat set av attribut än de som finns registrerade hos oss och angivna i förstudien. Listan på attributen kan dock ändras genom att skicka in en ny förstudie.

4. 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 attributet *"AttributeConsumingServiceIndex"* som skall kunna matchas mot ett index som finns i dess metadata. Nedan följer fyra exempel.

4.1. AuthnRequest utan HSA-uppslag

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://auth.dev.inera.test:443/saml/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.

4.2. AuthnRequest med HSA-uppslag

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://auth.dev.inera.test:443/saml/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.

4.3. AuthnRequest med uppdragsval

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://auth.dev.inera.test:443/saml/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.

4.4. AuthnRequest utan index

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://auth.dev.inera.test:443/saml/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.

4.5. AuthnRequest med PrincipalSelection

Som SP finns möjligheten att på förhand göra ett specifikt val över vilket HSA-id, organisationsnummer, personnummer eller orgAffiliation som användaren ska bli inloggad med. Dess värden användas enskilt men också kombineras med varandra. När filtreringen görs försöker IdP:n göra ett val automatiskt baserad på den informationen som tagits emot i den AuthnRequest som skickats in. Om det är möjligt kan alltså exempelvis ett specifikt tjänste-id pekas ut och användaren slipper göra ett aktivt val i IdP:n.

I exemplet nedan förväntas användaren bli inloggad med HSA-id:t **TSTNMT2321000156-10NG** för organisationen med organisationsnumret **232100-0214**.

PrincipalSelection

```
<saml2p:Extensions>
    <psc:PrincipalSelection xmlns:psc="http://id.swedenconnect.se/authn/1.0/principal-selection/ns">
        <psc:MatchValue Name="http://sambi.se/attributes/1/employeeHsaId" xmlns:psc="http://id.swedenconnect.se
/authn/1.0/principal-selection/ns">TSTNMT2321000156-10NG</psc:MatchValue>
        <psc:MatchValue Name="http://sambi.se/attributes/1/organizationIdentifier" xmlns:psc="http://id.
swedenconnect.se/authn/1.0/principal-selection/ns">232100-0214</psc:MatchValue>
    </psc:PrincipalSelection>
</saml2p:Extensions>
```