

Säkerhetsheader

Web Services Security Header och SAML v2.0 Assertions

Dokumentet specificerar säkerhetsheaderns struktur och innehåll och är normerande för att kunna nyttja tjänsterna. Samtliga av Apotekens Service egendefinierade attribut redovisas.

Innehåll

1	Inledning	3
2	Definitioner	3
3	Säkerhetsheader	3
3.1	Exempel på SOAP-meddelande med säkerhetsheader och tre intyg	4
4	Autentiseringsintyg	5
4.1	Exempel på autentiseringsintyg med attribut	6
5	Auktorisationsintyg	7
5.1	Exempel på auktorisationsintyg med attribut	9
6	Informationsintyg	10
	Revisionshistorik	11

1 Inledning

Detta dokument specificerar den struktur och innehåll som säkerhetsheadern måste ha för att ett anrop ska kunna accepteras av de tjänster som tillhandahålls av Apotekens Service AB.

Med struktur och innehåll avses i första hand de av Apotekens Service definierade SAML v2.0 attribut.

2 Definitioner

Term	Förklaring
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol

3 Säkerhetsheader

För att ett anrop ska kunna genomföras krävs att tre olika intyg bifogas i säkerhetsheadern.

De intyg som ska skickas med är: 1) Autentiseringsintyg (SAML-Assertion), 2) Auktorisationsintyg och 3) Infodataintyg. Se bild 1.

Intygen beskrivs i detalj under respektive kapitel. Det som är gemensamt för alla intyg är att de ska vara enligt SAML v2.0 och signerade med en XML-signatur.

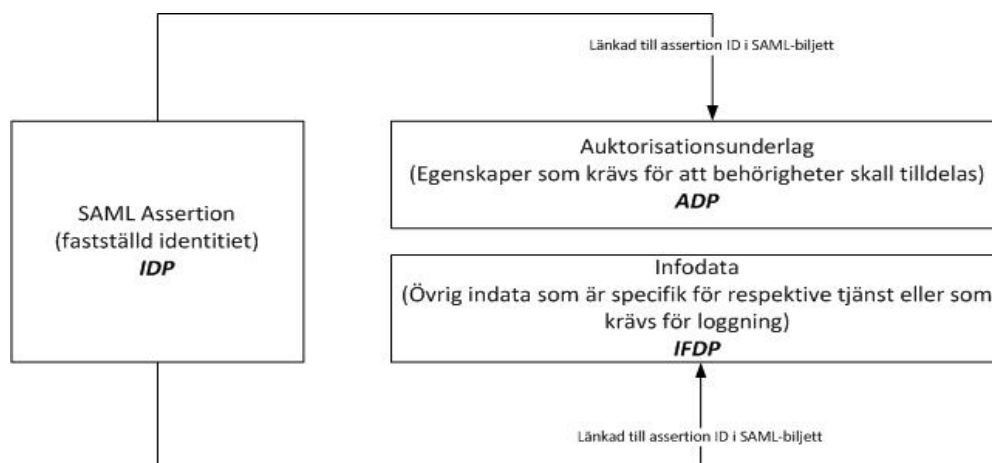


Bild 1

De tre intygen hålls ihop med ett egendefinierat attribut, *connectedAssertionId*.

Attributet sätts för auktorisationsintyget och informationsintyget och ska ha samma värde som autentiseringsintygets *assertionId*.

Attributet är en del av den informationen som signeras och på så vis hålls intygen ihop på ett säkerhetsmässigt tillfredsställande sätt.

3.1 Exempel på SOAP-meddelande med säkerhetsheader och tre intyg

```
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
  secext-1.0.xsd"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <soapenv:Header>
    <wsse:Security >
      <saml2:Assertion ...> ... </saml2:Assertion>
      <saml2:Assertion ...> ... </saml2:Assertion>
      <saml2:Assertion ...> ... </saml2:Assertion>
    </wsse:security>
  </soapenv:Header>
  ...
```

4 Autentiseringsintyg

Identifierar den anropande användaren.

Validering sker att *AuthnContextClassRef* har angivits. Detta är en del av det *AuthnStatement* som ingår i ett SAML v2.0 intyg.

Attributen anges som en del av det *AttributeStatement* som ingår i intyget enligt SAML v2.0 standarden.

Attribut ska namnges enligt **urn:apotekensservice:names:federation:<attributnamn>** där **<attributnamn>** byts ut enligt följande tabell.¹

Intyget ska signeras.

Attributnamn	Max längd	Beskrivning
DirectoryID	255	Obligatorisk. Beskriver biljetтинnehavarens unika ID i den katalog som aktören i fråga är ansluten till och som anges vid etablering av federation mot/med denna aktör. Motsvarar katalog-id.
OrganizationID	25	Obligatorisk. Globalt unikt ID för aktören för vars räkning biljetten är utställd för. Ska vara antingen ett svenskt organisationsnummer eller OID (Object Identifier). OID ska vara registrerat hos en av IETF(Internet Engineering Task Force) accepterad utfärdare som t ex ANSI (American National Standards Institute) eller SIS (Swedish Standards Institute)

¹ Observera att detta gäller under en övergångsperiod tills etablerad identitetsfederation finns på plats

4.1 Exempel på autentiseringsintyg med attribut

Ett avkortat exempel på ett autentiseringsintyg där *DirectoryID* har värdet **123456** och *OrganizationID* har värdet **1.2.752.123.1.3**.

```
<Assertion . . .>
  . . .
  <AttributeStatement>
    <Attribute Name="urn:apotekensservice:names:federation:attributeName:DirectoryID"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <AttributeValue>123456</AttributeValue>
    </Attribute>
    <Attribute Name="urn:apotekensservice:names:federation:attributeName:OrganizationID"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <AttributeValue>1.2.752.123.1.3</AttributeValue>
    </Attribute>
  </AttributeStatement>
</Assertion>
```

5 Auktorisationsintyg

De attribut som ingår i auktorisationsintyget används dels för att avgöra vilken roll som den autentiserade användaren agerar som, dels ytterligare rättighetskontroller utöver den grundbehörighet som rollen medför.

Exempel: En användare i rollen "förskrivare" har rätt att anropa tjänster som är relaterade till förskrivning av läkemedel. Ytterligare kontroller sker inne i tjänsten så att kombination av det tilltänkta läkemedlet och användarens förskrivningsrätt inte är i konflikt.

Attributen anges som en del av det *AttributeStatement* som ingår i intyget enligt SAML v2.0. Intyget ska signeras av utställaren.

Attribut ska namnges enligt `urn:apotekensservice:names:federation:<attributnamn>` där `<attributnamn>` byts ut enligt följande tabell.²

Attributnamn	Max längd	Beskrivning
apoteksld	13	Unik identitet för apotek.
arbetsplats	35	Lokalitet i klartext (adress 1). Exempelvis Vårdcentralen Humlan eller Privat, kirurgi/ortopedi.
arbetsplatskod	13	Arbetsplatskod eller grupparbetsplatskod
assertionType	-	Obligatorisk. Ska sättas till: AuthorizationData
befattningskod	64	Befattningskod.
connectedAssertionId	64	Obligatorisk. Länk till autentiseringsinformationen. Ska ha samma värde som det id som unikt identifierar autentiseringsintyget.
efternamn	35	Efternamn.
fornamn	35	Förnamn.

² Observera att detta gäller under en övergångsperiod tills etablerad identitetsfederation finns på plats

Attributnamn	Max längd	Beskrivning
forskrivarkod	7	Förskrivarens individuella legitimationskod eller förskrivarens gruppförskrivarkod då individuell kod saknas.
legitimationskod	6	Legitimationskod för vårdpersonal.
organisationsnummer	12	Organisationsnummer.
personnummer	12	Personnummer för privatperson som anropar tjänst.
postadress	35	Arbetsplatsens gatuadress (Adress 2).
postnummer	5	Arbetsplatsens postnummer.
postort	35	Arbetsplatsens postort.
roll	-	<p>Obligatorisk.</p> <p>Den roll som den autentiserade användaren agerar som. Sluten värdemängd, en av följande:</p> <p>FORSKRIVARE</p> <p>LEG_VARDPERSONAL</p> <p>EJ_LEG_VARDPERSONAL</p> <p>FARMACEUT_APOTEK</p> <p>PERSONAL_APOTEK</p> <p>PRIVATPERSON</p>
telefonnummer	15	Telefonnummer till användaren eller arbetsplatsen.
telefonnummerDirekt	15	Telefonnummer direkt till användaren.
yrkeskod	2	Yrkeskod

5.1 Exempel på auktorisationsintyg med attribut

Ett exempel på ett auktorisationsintyg där autentiseringsintyget har ett *assertionId* med värdet **123456789** och attributet *yrkeskod* angivits till värdet **LK** (läkare) kan se ut enligt följande.

```
<Assertion . . .>
  . . .
  <AttributeStatement>
    <Attribute Name="urn:apotekensservice:names:federation:attributeName:connectedAssertionId"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri ">
      <AttributeValue>123456789</AttributeValue>
    <Attribute Name="urn:apotekensservice:names:federation:attributeName:assertionType"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri ">
      <AttributeValue>AuthorizationData</AttributeValue>
    <Attribute Name="urn:apotekensservice:names:federation:attributeName:yrkeskod"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri ">
      <AttributeValue>LK</AttributeValue>
    </Attribute>
  </AttributeStatement>
</Assertion>
```

6 Informationsintyg

De attribut som ingår i informationsintyget används i första hand för spårbarhet och innehåller information om anropande system eller applikation.

Attributen anges som en del av det *AttributeStatement* som ingår i intyget enligt SAML v2.0.

Attribut ska namnges enligt **urn:apotekensservice:names:federation:<attributnamn>** där **<attributnamn>** byts ut enligt följande tabell.³

Attributnamn	Max längd	Beskrivning
connectedAssertionId	64	Obligatorisk. Länk till autentiseringsinformationen. Ska ha samma värde som det id som unikt identifierar autentiseringsintyget.
assertionType	--	Obligatorisk. Ska sättas till: InfoData
requestId	20	Unikt id för anropet hos anropande system.
systemnamn	30	Namn på anropande system.
systemversion	25	Version på anropande system.
systemIp	53	IP adress för anropande system. Anges som IPv4 eller IPv6.

³ Observera att detta gäller under en övergångsperiod tills etablerad identitetsfederation finns på plats

Revisionshistorik

Utgåva	Datum	Kommentar
V 1.0	2011-03-22	Första utgåvan