Skolfederation

Hantering av tillitsnivåer

Version 1.2

Innehåll

Skolfederation.se
Box 7399, 103 91 Stockholm Tel 08-452 35 00 Fax 08-452 35 02
www.skolfederation.se

Skolfederation

1 Inledning

Detta dokument beskriver hur tillitsnivåer ska signaleras mellan intygsutfärdare (IdP) och tjänsteleverantör (SP) inom Skolfederation.

2 Tillitsnivåer

Följande tillitsnivåer tillämpas inom federationen:

1. `[http://id.skolfederation.se/loa/bas]`
2. `[http://id.skolfederation.se/loa/2fa]`

Numreringen anger nivåernas inbördes relation där högre numrering innebär högre tillit.

Följande nivåer finns registrerade men tillämpas för nuvarande inte:

- `[http://id.skolfederation.se/loa/loa2]`
- `[http://id.skolfederation.se/loa/loa3]`

Ovanstående nivåer är ännu inte specificerade och bör inte användas för att signalera tillitsnivå inom federationen.

3 Profiler och referenser

Hanteringen av tillitsnivåer som beskrivs i detta dokument refererar inte till några andra standarder eller profiler än de som tillämpas generellt inom Skolfederation.

3.1 Förtydligande gällande deploymentprofil

Den, inom Skolfederation, tillämpade deploymentprofilen `http://saml2int.org/profile/current`. rekommenderar att en `<saml2p:AuthnRequest>` endast bör innehålla elementet `<saml2p:RequestedAuthnContext>` i de fall där en uppgörelse träffats mellan IdP och SP.

> The `<saml2p:AuthnRequest>` message MAY contain a `<saml2p:RequestedAuthnContext>` element, but SHOULD do so only in the presence of an arrangement between the Identity and Service Providers regarding the Authentication Context definitions in use.

I detta dokument beskrivs hur signaleringen ska utföras på ett enhetligt sätt inom federationen, men ansvaret att besluta om vilken tillitsnivå som ska tillämpas för åtkomst av en specifik kvarstår hos intygsutgivaren och tjänsteleverantören.

4 Signalering av tillitsnivå

Tillitsnivå signaleras genom att addera aktuell `<saml:AuthnContextClassRef>` till elementet `<saml2p:RequestedAuthnContext>` i `<saml2p:AuthnRequest>` och `<saml2p:AuthnResponse>`.

I det fall ingen tillitsnivå begärs ska alla signalerade tillitsnivåer godkännas såväl som utebliven signalering av tillitsnivå. Det innebär i praktiken att inget annat än federationens lägsta tillitsnivå kan säkerställas, vilket är ekvivalent med `[http://id.skolfederation.se/loa/bas]`.

Context Class för respektive URI finns beskrivet på http://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml

4.1 Service Provider

SP:n anger vilken tillitsnivå som krävs för att nå en specifik resurs genom att signalera detta i `<saml2p:AuthnRequest>`.

Attributet `[Comparison]` bör sättas till ”`exact`” då vissa SAML-mjukvaror endast har stöd för exakt matchning av `<saml:AuthnContextClassRef>`. För att undvika problem för en användare som redan är autentiserad med en högre tillitsnivå än tjänsten kräver, bör autentiseringsfrågan innehålla samtliga tillitsnivåer som uppfyller tjänstens krav. En `<saml2p:AuthnRequest>` kommer därför att innehålla fler än en `<saml:AuthnContextClassRef>` i de fall en annan tillitsnivå än den starkaste efterfrågas. Tillitsnivåerna i autentiseringsfrågan ska listas i fallande ordning, med den föredragna tillitsnivån överst i listan (Exempelvis; om tjänsten kräver tillitsnivå `[Bas]`, placeras den högst i listan. Eftersom även tillitsnivå `[2FA]` är godkänd så signaleras även den, men placeras efter `[Bas]` i listan).

Om `[Comparison]` helt utelämnas, kommer det att tolkas av IdP på samma sätt som ”`exact`” i enlighet med SAML-Core-2.0.

Om ingen annan tillitsnivå än `[http://id.skolfederation.se/loa/bas]` krävs för den aktuella tjänsten så kan signalering av tillitsnivå utelämnas helt som ett alternativ till att signalera den faktiska nivån. Detta innebär att tjänsten inte behöver ha kännedom om federationens tillitsnivåer över huvud taget och användaren kommer att autentiseras oavsett vilken tillitsnivå IdP:n stödjer.

4.2 Identity Provider

IdP:n besvarar en begärd tillitsnivå i `<saml2p:AuthnRequest>` genom att, i `<saml2p:AuthnResponse>`, signalera den tillitsnivå som användaren autentiserats för.

En autentiseringsfråga kan innehålla fler än en `<saml:AuthnContextClassRef>` i en ordnad lista. Listan ska tolkas i fallande ordning med föredragen tillitsnivå överst. Om IdP:n inte kan matcha någon av de efterfrågade tillitsnivåer, ska `<StatusCode>` `[urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext]` anges i svaret.

5 Anvisningstjänst

Det finns några tänkbara scenarion där en användare som, i normalfallet, enbart ansluter till tjänster genom IdP-initerade inloggningar, kommer att bli omdirigerad till anvisningstjänsten. Det kan exempelvis ske om användaren är autentiserad med en viss tillitsnivå och sedan begär en resurs som kräver en högre tillitsnivå. En användare som vanligtvis inte nyttjar anvisningstjänsten kan uppleva det en aning förvirrande att plötsligt behöva interagera med den, vilket bör beaktas vid utformning av den specifika implementation.

Skolfederation har för närvarande inga specifika rekommendationer avseende hur detta bör hanteras. Två lösningar som kan reducera/förenkla användandet är under utvärdering och kan komma att tillämpas inom federationen framöver. Dessa beskrivs kortfattat nedan.

- Filtrering av presenterade IdP:er i anvisningstjänsten baserat på tillitsnivå:
  Syftet med denna funktion är att användaren inte ska kunna välja en IdP som inte uppfyller den efterfrågade tillitsnivån. Detta förutsätter att anvisningstjänsten känner till vilka IdP:er som uppfyller vilka tillitsnivåer, samt vilken tillitsnivå som efterfrågas i varje given autentiseringsfråga som dirigeras via anvisningstjänsten. Behovet av funktionen antas vara lågt i nuläget, men den kan komma att implementeras i framtiden.
- Common Domain Cookie:
  En gemensam domän beslutas för federationen (ex. skolfederation.se) och respektive IdP/SP ges möjlighet att dirigera autentiseringsfrågor/svar via domänen. Information om de IdP:er användaren nyttjas lagras i form av en lista där senast använda IdP placeras högst upp i listan. IdP/SP har möjlighet att skriva/läsa `[Common Domain Cookie]` och en SP kan därmed dirigera en autentiseringsfråga direkt till den IdP användaren nyttjat senast. Funktionen utreds för närvarande inom federationen Sambi och kan komma att införas i Skolfederation framöver.

Utöver de centrala lösningar som beskriv ovan, kan tjänsteleverantörer som väljer att tillämpa embedded discovery hantera logiken i den egna tjänsten.

6 Context Classes [.xsd]

Nedanstående scheman finns även här: http://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml

6.1 LoA Bas

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="http://id.skolfederation.se/loa/bas"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://id.skolfederation.se/loa/bas"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-open.org/security/saml/v2.0/saml-
schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier: http://id.skolfederation.se/loa/bas Defines the basic
level of the Skolfederation.se Assurance Framework
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef"
          type="xs:anyURI"
          fixed="http://id.skolfederation.se/loa/bas"
          use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```

6.2 LoA 2fa

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="http://id.skolfederation.se/loa/2fa"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://id.skolfederation.se/loa/2fa"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-open.org/security/saml/v2.0/saml-
schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier: http://id.skolfederation.se/loa/2fa Defines the strong
authentication level of the Skolfederation.se Assurance Framework
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef"
          type="xs:anyURI"
          fixed="http://id.skolfederation.se/loa/2fa"
          use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```

6.3 LoA 2 (tillämpas inte för närvarande)

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="http://id.skolfederation.se/loa/loa2"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://id.skolfederation.se/loa/loa2"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier: http://id.skolfederation.se/loa/loa2 Defines
Level 2 of the Skolfederation.se Assurance Framework
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef"
          type="xs:anyURI"
          fixed="http://id.skolfederation.se/loa/loa2"
          use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```

6.4 LoA 3 (tillämpas inte för närvarande)

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="http://id.skolfederation.se/loa/loa3"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://id.skolfederation.se/loa/loa3"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier: http://id.skolfederation.se/loa/loa3 Defines
Level 3 of the Skolfederation.se Assurance Framework
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef"
          type="xs:anyURI"
          fixed="http://id.skolfederation.se/loa/loa3"
          use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```