Skolverket

DNP-projektet 2023-09-08

Signalering av tillitsnivå till Skolverkets provtjänst

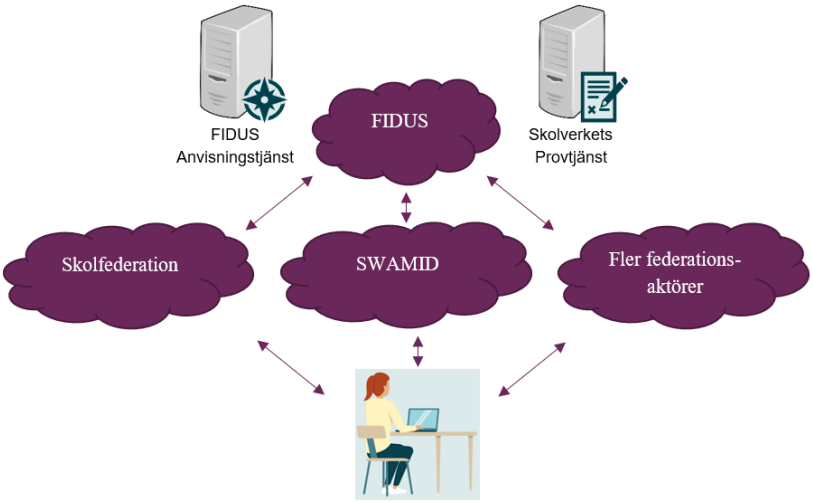
Innehåll

Bakgrund

Detta dokument beskriver olika tillvägagångssätt och en del tekniska förutsättningar för åtkomst till Skolverkets provtjänst med fokus på hur anslutande part ska signalera på vilka tillitsnivåer densamma har möjlighet att autentiserat sina användare. Läsaren behöver ha kunskaper i SAML-federationer och tillhörande tillitsramverk.

Tekniska krav på anslutning till provtjänsten

Skolverket ställer krav på att åtkomsten till Skolverkets provtjänst sker genom en så kallad federerad inloggning. Det innebär att inloggningen sker i en inloggningstjänst (IdP) som är betrodd av någon av de federationer som Skolverket litar på genom interfederationen Fidus[1].



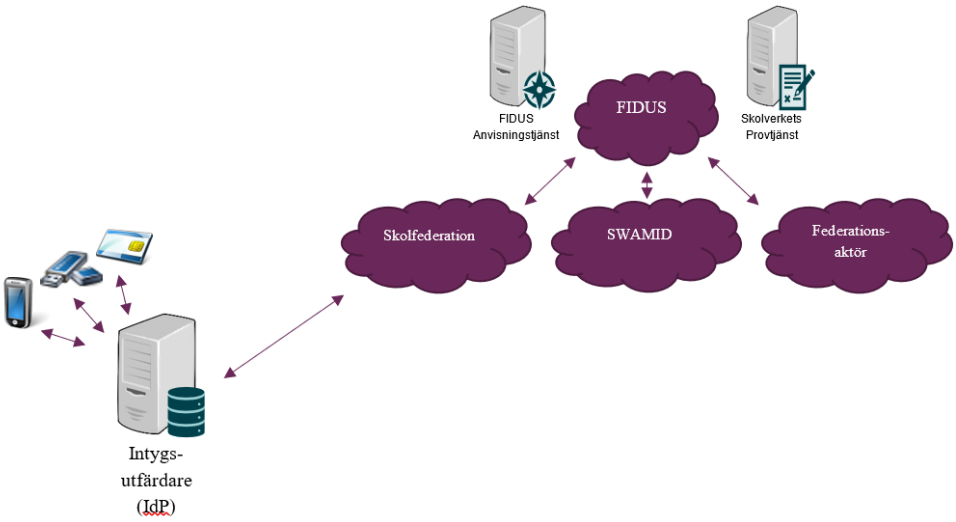
Vilka federationer som är ansluta till Fidus framgår på interfederationens hemsida[2]

För att möjliggöra federerad inloggning behövs förmåga att ställa ut digitala identitetsintyg baserade på SAML-standarden[3] (Security Assertion Markup Language). Det är en metod för att utbyta data för autentisering och auktorisering mellan olika parter som bevis på en lyckad inloggning. Denna förmåga återfinns oftast i en inloggningstjänst, även kallad IdP (*eng. Identity Provider*), legitimeringstjänst och inloggningstjänst. Förmågan måste också möta de mer detaljerade krav som ställs av den federation som är aktuell att ansluta sig till.

[1] https://www.skolverket.se/om-oss/var-verksamhet/skolverkets-prioriterade-omraden/digitalisering/digitala-nationella-prov/tekniska-forutsattningar-for-digitala-nationella-prov/interfederationen-fidus
[2] https://github.com/FIDUSFederation
[3] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

Åtkomst för skolpersonal till Skolverkets provtjänst

Kravet för skolpersonalens åtkomst till Skolverkets provtjänst är att e-legitimering ska ske på tillitsnivå 2, 3 eller 4 enligt *Tillitsramverket för kvalitetsmärket Svensk e-legitimation*[4] vid hantering och genomförande av digitala nationella prov och bedömningsstöd.



För att inloggningstjänsten (IdP) på ett korrekt sätt ska kunna presentera detta för Skolverkets provtjänst måste vissa förutsättningar finnas på plats vilket beskrivs i detta dokument.

Tekniska förutsättningar

Användningen av olika tillitsnivåer i Skolverkets provtjänst ställer krav på att provtjänsten i rollen som e-tjänst (Service Provider, SP) kan ställa krav på att vissa inloggningar kräver en viss tillitsnivå. Exempelvis ska skolpersonalen logga in med en e-legitimation på tillitsnivå 2, 3 eller 4, och att det måste signaleras för e-tjänsten enligt vissa regler. Det innebär att inloggningstjänsten (IdP) måste ha förmåga att hantera den signaleringen.

Skolverket ställer **inte** krav på att inloggningstjänsten (IdP) ska vara granskad och godkänd av DIGG för att få möjlighet att ansluta mot Skolverkets provtjänst. Detta innebär att det inte är samma krav som ställs på en IdP som enbart ska användas för att ansluta mot Fidus som en IdP som ska ansluta mot exempelvis Sweden Connect[5], där av DIGG godkänd IdP krävs.

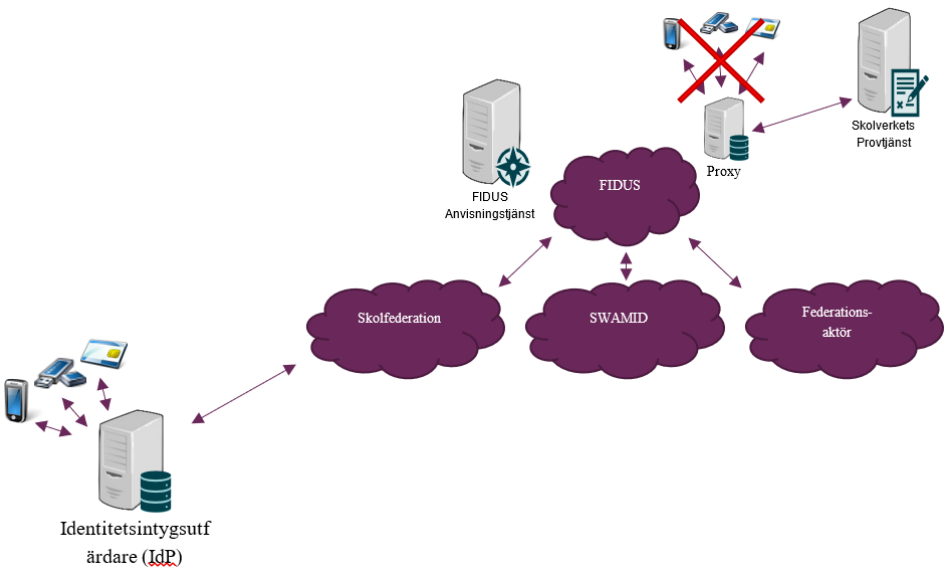
[4] https://www.digg.se/digitala-tjanster/e-legitimering/tillitsnivaer-for-e-legitimering/tillitsramverk-for-svensk-e-legitimation
[5] https://www.swedenconnect.se

Signalering av tillitsnivå

För att på ett korrekt sätt kunna presentera för Skolverkets provtjänst på vilken tillitsnivå en individ har autentiserats krävs att ett antal inställningar görs i inloggningstjänsten (IdP).

Att en inloggningstjänst (IdP) har förmåga att hantera tillitssignalering anges i metadata som delas med samtliga e-tjänster (SPs) i federationen. Därutöver ska en IdP kunna konfigureras att i utfärdade identitetsintyg ange den exakta tillitsnivå som gäller för specifikt provtjänsten.

För de mjukvaror för identitetsintygsutfärdande (IdP) som inte har signaleringsförmågan finns möjlighet att antingen stänga av signaleringsförfarandet eller ställa in så att den är agnostisk, dvs. accepterar inloggningar både med och utan signalering av tillitsnivå. Det innebär då att Skolverket påför en av DIGG godkänd e-legitimering i form eduID som e-legitimation[6] vid autentiseringstillfället.

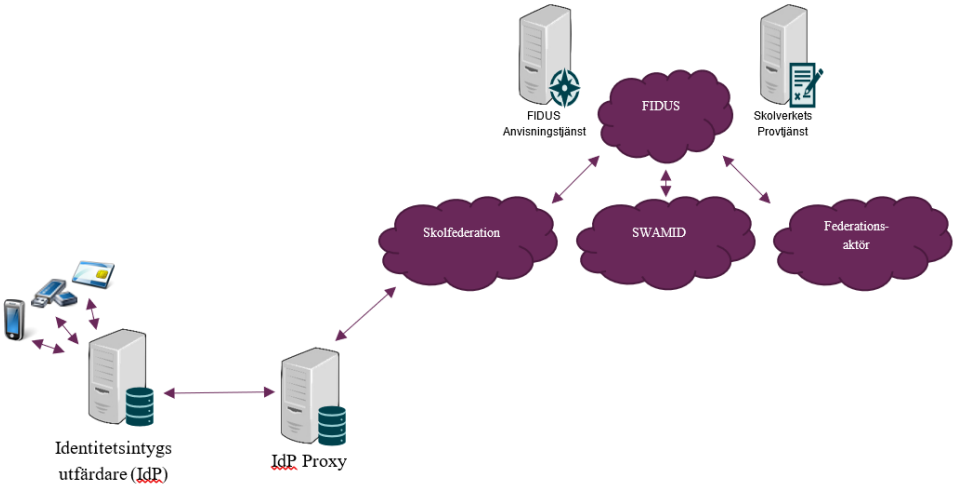


I ett scenario där förmågan att signalera tillitsnivå saknas men inloggningstjänsten är ansluten till en av DIGG godkänd e-legitimation så kan det vara aktuellt att använda en IdP-proxy.

[6] Beställs av Skolverket via en e-tjänst

IdP Proxy

Beroende på val av e-legitimationslösning så kan en organisation behöva påföra en IdP-proxy. Det innebär att ytterligare en komponent som å ena sidan kan agera e-tjänst mot en annan intygsutfärdare (IdP), å andra sidan kan agera intygsutfärdare (IdP) mot Skolverkets provtjänst.



Ett vanligt scenario är att den upphandlade e-legitimationslösning som organisationen använder också tillhandahåller en IdP från vilken e-legitimationsutfärdaren ställer ut identitetsintyg som organisationens inloggningstjänst tar emot för att sedan vidarebefordra till Skolverkets provtjänst.

Ett annat vanligt scenario är att organisationens nuvarande IdP inte har förmågan att signalera tillitsnivå varför en IdP-proxy tillförs för att tillgodose detta behov.

I båda dessa fall är det viktigt att den IdP som agerar proxy har förmågan att översätta genomförd autentisering till korrekt tillitsnivå för att kunna presentera detta för Skolverkets provtjänst genom den signalering som beskrivs i detta dokument.

Medge signalering av tillitsnivå

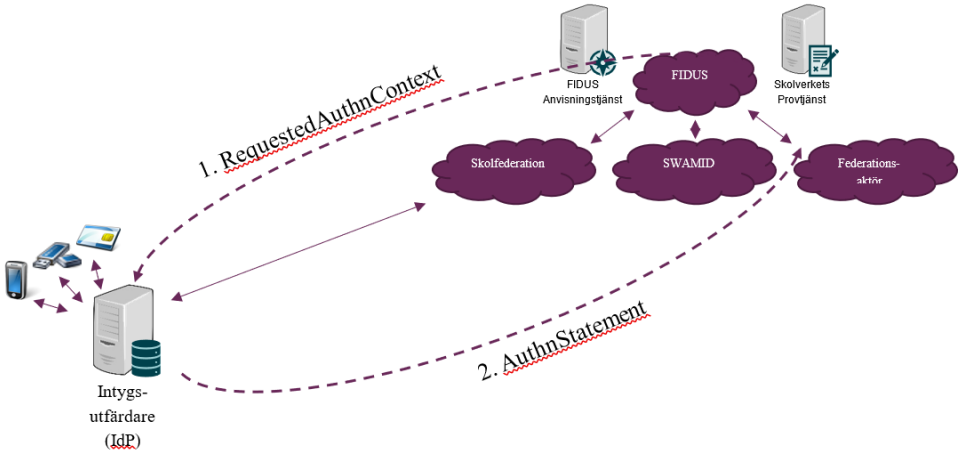
För en identitetsintygsutfärdande (IdP) som har förmåga att signalera tillitsnivå måste följande markering göras i SAML-metadata på inloggningstjänsten (IdP).

```
<md:Extensions>
  <mdattr:EntityAttributes
   xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
    <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-
     certification" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
     format:uri”>
    <saml:AttributeValue>https://fidus.skolverket.se/authentication/e-
     leg</saml:AttributeValue>
    </saml:Attribute>
  </mdattr:EntityAttributes>
</md:Extensions>
```

Om ovanstående markering inte görs kommer Skolverket att påföra en extra inloggning med en DIGG-godkänd e-legitimation i form eduID som e-legitimation[7].

Anslutning med tillitssignalering

När en inloggningstjänst (IdP), där tillitsignalering har medgivits enligt ovan, ansluter mot Skolverkets provtjänst så kommer e-tjänsten att svara med en förfrågan med krav på att den tillitsnivå för den e-legitimation som användaren loggar in med finns med i en lista av tillåtna tillitsnivåer. Denna förfrågan kallas *RequestedAuthnContext*.



Identitetsintygsutfärdanden (IdP) inkluderar i sitt identitetsintyg (svar) ett *AuthnStatement* med vilken av de godkända tillitsnivåerna som använts samt individens autentiseringsdata.

[7] Beställs av Skolverket via en e-tjänst

Exempel RequestedAuthnContext

Nedan är ett exempel på hur en lista med tillåtna tillitsnivåer kan presenteras i en RequestedAuthContext[8] från provtjänsten:

```
<saml2p:RequestedAuthnContext Comparison="exact">
<saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/uncertified-loa2
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/uncertified-loa3
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/loa2
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/loa3
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef> http://id.swedenconnect.se/loa/1.0/uncertified-eidas-low
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef> http://id.swedenconnect.se/loa/1.0/uncertified-eidas-sub
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa2-nonresident
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa3-nonresident
</saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
```

Exempel AuthnStatement

Nedan är ett exempel på hur svaret från en inloggningstjänst (IdP) till provtjänsten kan se ut[9]:

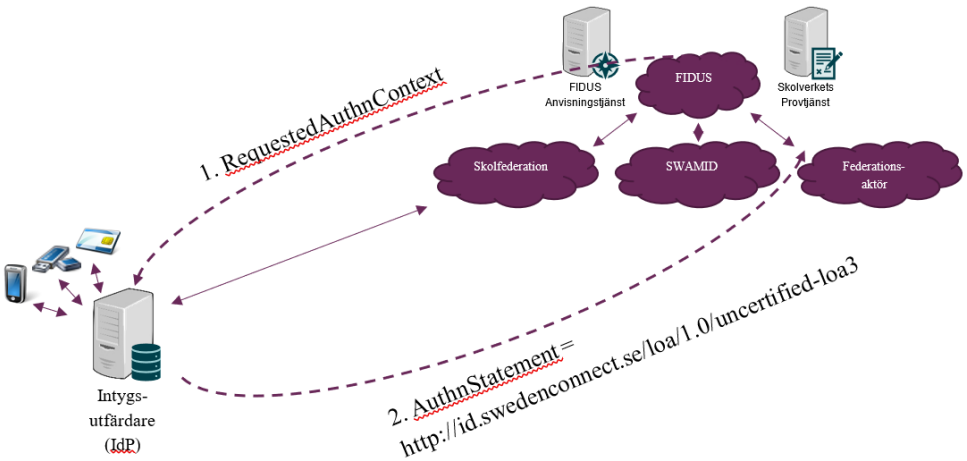
```
<saml2:AuthnStatement AuthnInstant="2022-11-28T13:00:00"
 SessionIndex="ac7891…" >
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>
     http://id.swedenconnect.se/loa/1.0/uncertified-loa2
    </saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
```

I detta exempel autentiserar sig anslutande part på tillitsnivå 2 med en av DIGG godkänd e-legitimation via en inloggningstjänst (IdP) som **inte** är godkänd av DIGG. Sannolikt det vanligaste scenariot vid anslutning till Skolverkets provtjänst.

[8] Deployment Profile for the Swedish eID Framework [EidDeploy] ver 1.7 kap 5.3.1.
[9] Deployment Profile for the Swedish eID Framework [EidDeploy] ver 1.7 kap 6.2 & 6.3.4

Exempel anslutning på tillitsnivå 3 med ej godkänd IdP

Exempel på anslutning med en godkänd e-legitimation på tillitsnivå 3 med en IdP som inte är godkänd av DIGG:

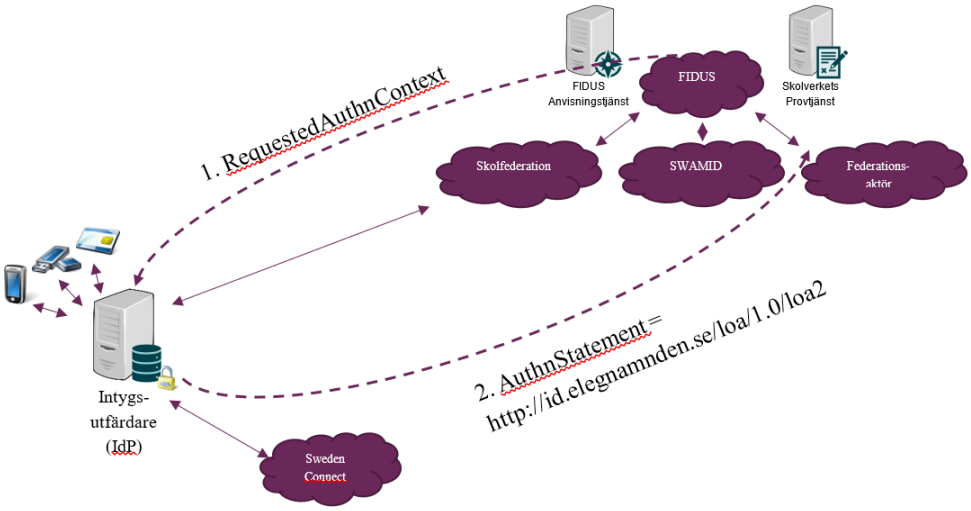


Exempel på godkända e-legitimationer på tillitsnivå 3 är:

- BankID
- Freja+
- SITHS

Exempel anslutning på tillitsnivå 2 med godkänd IdP

Exempel på anslutning med en godkänd e-legitimation på tillitsnivå 2 med en IdP som är godkänd av DIGG:



Exempel på godkända e-legitimationer på tillitsnivå 2 är:

- eduID

Tillitsnivåer som accepteras av Skolverkets provtjänst

Skolverket har valt att använda DIGG:s definitioner[10] i Sweden Connect för signalering av tillitsnivå. I tabellen nedan listas de olika tillitsnivåerna som Skolverkets provtjänst litar på.

Vilken av dessa URI:er en Intygstjänst (IdP) ska presentera beror dels på tillitsnivå på e-legitimationen som har använts vid autentiseringen och dels på om anslutande IdP är godkänd av DIGG eller inte.

Felaktig signalering bryter mot Skolverkets regler.

URI	Tillitsnivå för DIGG-godkänd e-legitimation eller eIDAS tillitsnivå	DIGG godkänd IdP
http://id.swedenconnect.se/loa/1.0/uncertified-loa2	2	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-loa3	3	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-loa4	4	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-eidas-low	Låg	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-eidas-sub	Väsentlig	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-eidas-high	Hög	NEJ
http://id.elegnamnden.se/loa/1.0/loa2	2	JA
http://id.elegnamnden.se/loa/1.0/loa3	3	JA
http://id.elegnamnden.se/loa/1.0/loa4	4	JA
http://id.swedenconnect.se/loa/1.0/ loa2-nonresident	2	JA
http://id.swedenconnect.se/loa/1.0/ loa3-nonresident	3	JA
http://id.swedenconnect.se/loa/1.0/ loa4-nonresident	4	JA

[10] Swedish eID Framework - Registry for identifiers [EidRegistry] ver 1.7 kap 3.1.