

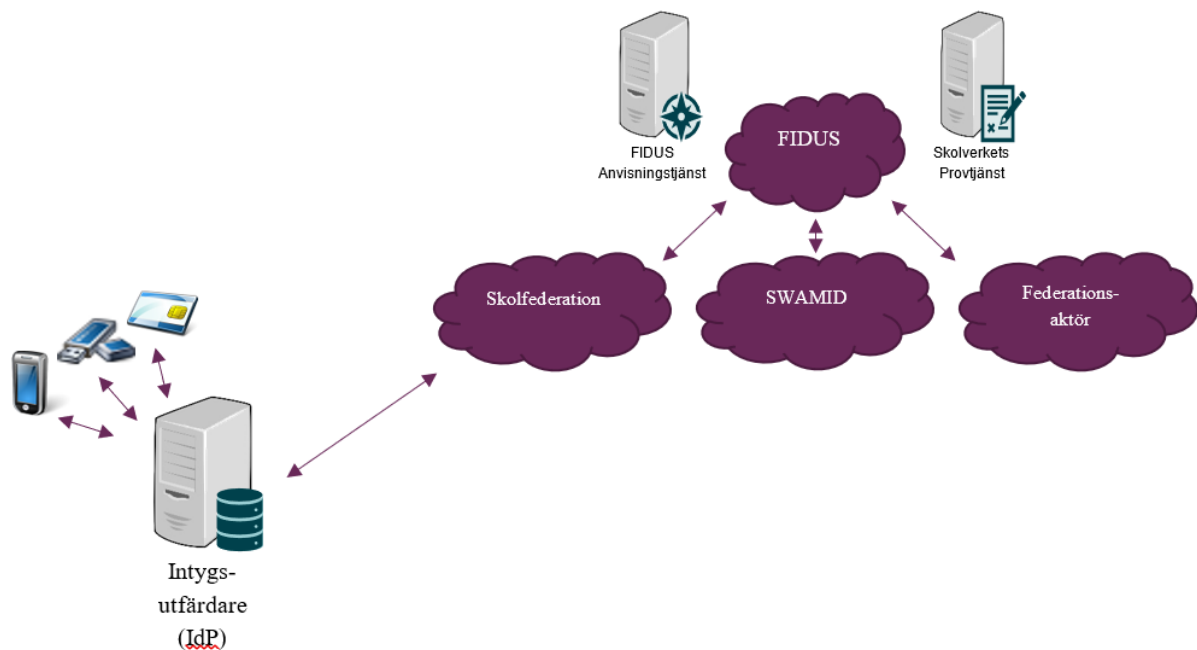
Signalering av tillitsnivå till Skolverkets provtjänst

Innehåll

<i>Åtkomst för skolpersonal till Skolverkets provtjänst</i>	<i>3</i>
<i>Tekniska förutsättningar avseende identitetsintygsutfärdare (IdP)</i>	<i>4</i>
IdP Proxy	4
<i>Krav på signalering av tillitsnivå</i>	<i>5</i>
Medge signalering av tillitsnivå	6
Anslutning med tillitssignalering	6
Exempel RequestedAuthnContext	7
Exempel AuthnStatement	7
Lista på av Skolverkets provtjänst accepterade tillitsnivåer	8

Åtkomst för skolpersonal till Skolverkets provtjänst

Den övergripande kravbilden för skolpersonalens åtkomst till DNP, är att e-legitimering ska ske på minst tillitsnivå 2 enligt *Tillitsramverket för kvalitetsmärket Svensk e-legitimation*¹ vid hantering och genomförande av digitala nationella prov och bedömningsstöd i Skolverkets provtjänst.



Grundförutsättningen för att ansluta sig till Skolverkets provtjänst är att e-legitimeringen sker med en av DIGG godkänd e-legitimation på lägst tillitsnivå 2. Skolverket ställer inte krav på att själva identitetsintygsutfärdaren (IdP) ska vara granskad och godkänd av DIGG. Identiteten på den som ansluter ska presenteras i form av ett eppn som också måste finnas provisionerat i provtjänsten. För att identitetsintygsutfärdaren (IdP) på ett korrekt sätt ska kunna presentera detta för Skolverkets provtjänst finns vissa förutsättningar.

¹ <https://www.digg.se/digitala-tjanster/e-legitimering/tillitsnivaer-for-e-legitimering/tillitsramverk-for-svensk-e-legitimation>

Tekniska förutsättningar avseende identitetsintygsutfärdare (IdP)

Det finns tekniska förmågor för att ställa ut och konsumera elektroniska identitetsintyg (så kallade SAML-intyg) som behöver beaktas avseende DNP.

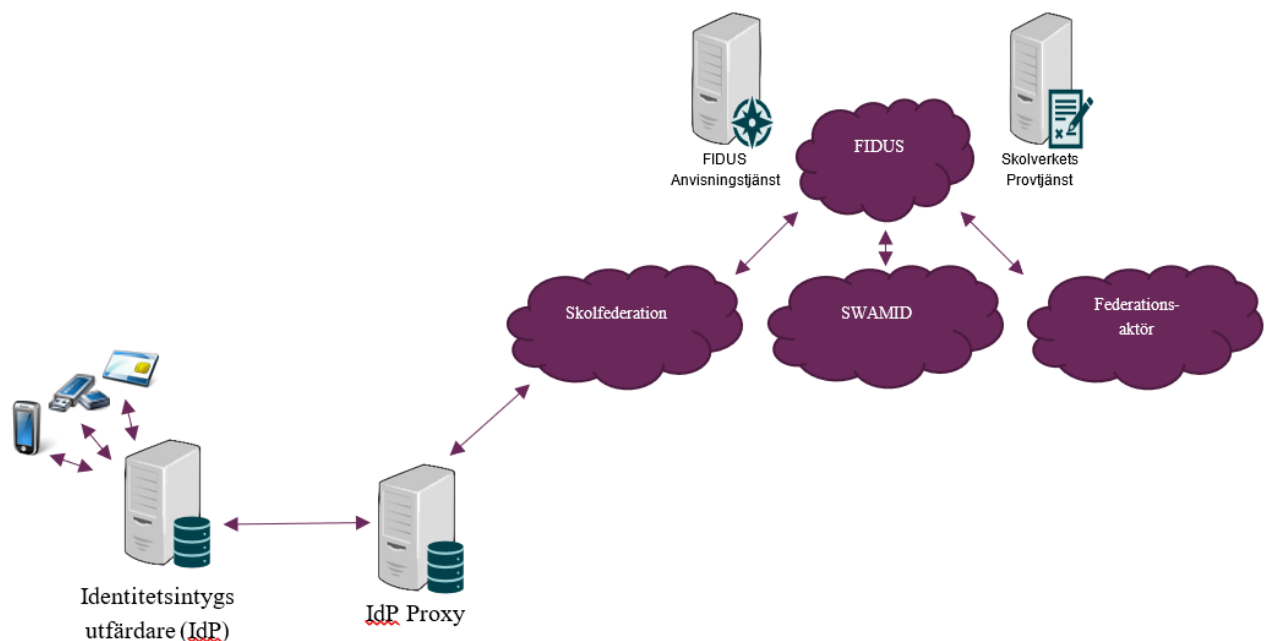
Användningen av olika tillitsnivåer i DNP ställer krav på att provtjänsten i rollen som e-tjänst (Service Provider, SP) kan ställa krav på att vissa inloggningar kräver en viss tillitsnivå. Exempelvis skolpersonalen som ska logga in med en e-legitimation på minst tillitsnivå 2. Det innebär att identitetsintygsutfärdaren (Identity Provider, IdP) måste ha förmåga att hantera den signaleringen.

Skolverket ställer inga krav på att identitetsintygsutfärdaren (IdP) ska vara granskad och godkänd av DIGG för att få möjlighet att ansluta mot Skolverkets provtjänst. Detta innebär att samma krav inte ställs på en IdP som enbart ska användas för att ansluta mot FIDUS som en IdP som ska ansluta mot exempelvis Sweden Connect², där av DIGG godkänd IdP krävs.

IdP Proxy

Beroende på val av e-legitimationslösning så kan en organisations interna identitetsintygsutfärdare (IdP) behöva agera som IdP proxy. Om den e-legitimationslösning en organisation använder innehåller en egen IdP från vilken den ställer ut identitetsintyg som organisationen tar emot för att sedan vidarebefordra till Skolverkets provtjänst.

I detta fall är det viktigt att den IdP som agerar proxy har förmågan att kunna översätta genomförd autentisering till korrekt tillitsnivå för att kunna presentera detta för Skolverkets provtjänst.



² <https://www.swedenconnect.se>

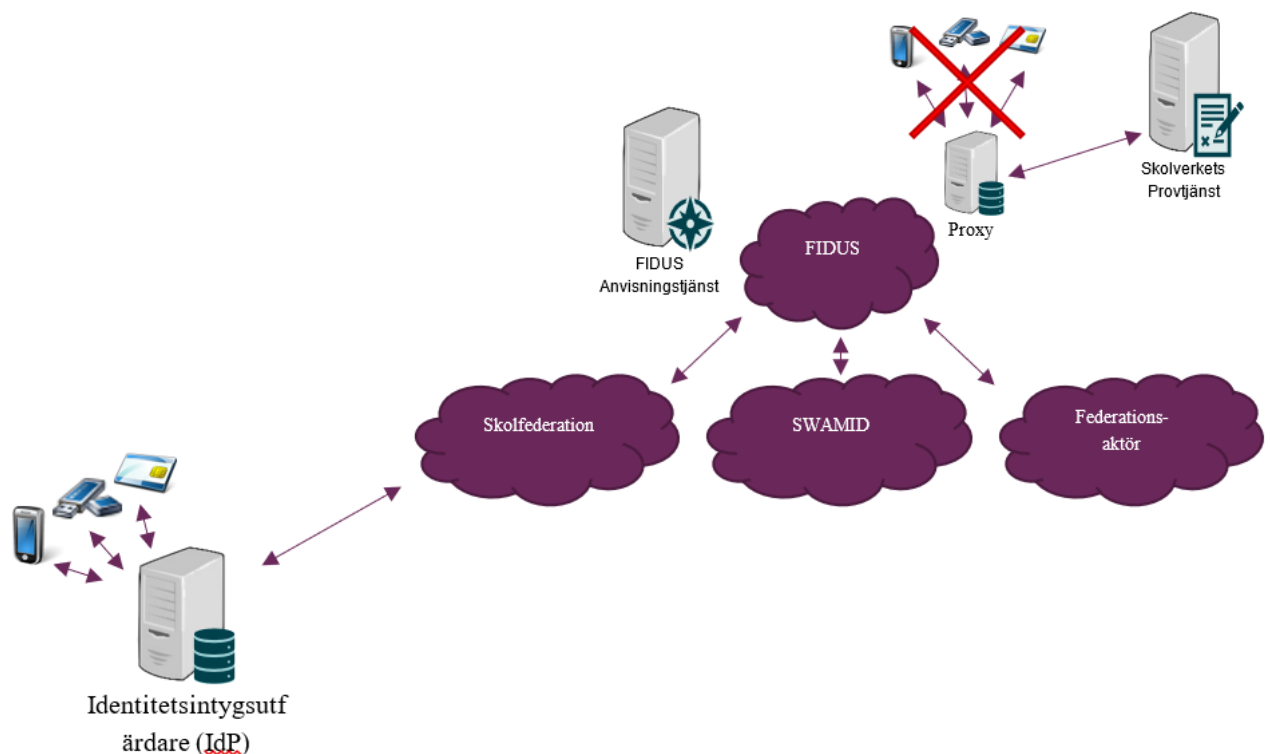
Krav på signalering av tillitsnivå

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 identitetsidentitetsintygsutfärdaren (IdP).

En identitetsidentitetsintygsutfärdare (IdP) måste ha förmåga att hantera tillitssignalering. Det sker inom ramen för standardiseringen av SAML men det finns trots detta leverantörer av mjukvara för identitetsintygsutfärdande (IdP) som inte har den förmågan.

För de mjukvaror för identitetsintygsutfärdande (IdP) som inte har den här signaleringsförmågan, finns möjlighet att stänga av signalering som beskrivs ovan. Det innebär då att Skolverket påför en av DIGG godkänd e-legitimering på lägst tillitsnivå 2 vid autentiseringstillfället.

Mjukvaror för identitetsintygsutfärdande (IdP) som inte har signaleringsförmågan, har sannolikt heller inte möjlighet att märka sitt SAML-metadata för att stänga av signalering, varför Skolverket har valt att göra märkningen omvänt. Om mjukvaror för identitetsintygsutfärdande (IdP) har signaleringsförmågan och dessutom av DIGG godkända e-legitimationer anslutna till den, behövs en märkning i SAML-metadata som anger att Skolverket vid autentiseringstillfället **inte** påför en av DIGG godkänd e-legitimering på lägst tillitsnivå 2.



Medge signalering av tillitsnivå

För en identitetsintygsutfärdande (IdP) som har förmåga att signalera tillitsnivå måste följande markering göras i SAML-metadata på identitetsintygsutfärdanden så att en stark autentisering inte påförs vid anslutningstillfället:

```
<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>

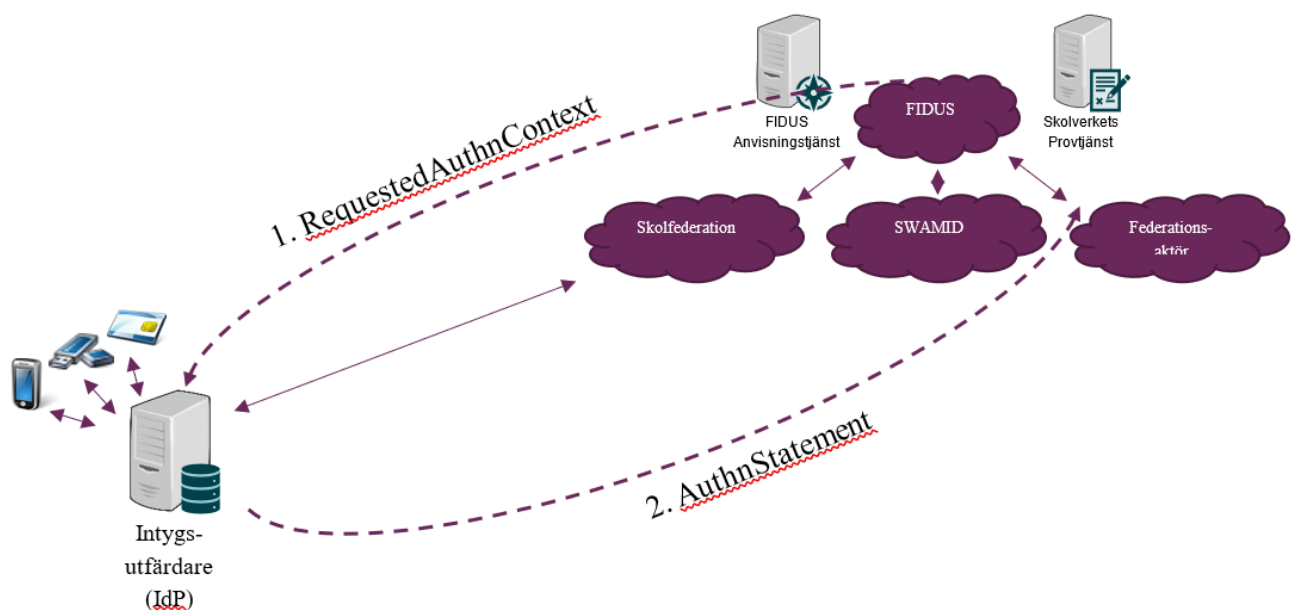
  </mdattr:EntityAttributes>

</md:Extensions>
```

Anslutning med tillitssignalering

När en identitetsintygsutfärdande (IdP), där tillitssignalering har medgivits, ansluter mot Skolverkets provtjänst så kommer e-tjänsten att svara med en förfrågan om vilken tillitsnivå det är på e-legitimationen som användaren har loggat in med. Frågan innehåller även en lista med de tillitsnivåer som tjänster godkänner. Denna förfrågan kallas *RequestedAuthnContext*.

Identitetsintygsutfärdanden (IdP) svarar med ett *AuthnStatement* med någon av de godkända tillitsnivåerna samt individens autentiseringsdata.



Exempel RequestedAuthnContext

Nedan är ett exempel på hur en listning med tillåtna tillitsnivåer skulle kunna presenteras i en RequestedAuthContext från provtjänsten³:

```
<saml2p:RequestedAuthnContext Comparison="exact">
<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.elegnamnden.se/loa/1.0/loa4
</saml2:AuthnContextClassRef>
<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.swedenconnect.se/loa/1.0/loa2-nonresident
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa3-nonresident
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa4-nonresident
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/nf-low
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/nf-sub
</saml2:AuthnContextClassRef>
<saml2:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/nf-high
</saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
```

Exempel AuthnStatement

Nedan är ett exempel på hur svaret från en identitetsintygutfärdare (IdP) till provtjänsten skulle kunna se ut⁴:

```
<saml2:AuthnStatement AuthnInstant="2022-11-28T13:00:00" SessionIndex="ac7891..." >

  <saml2:AuthnContext>

    <saml2:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/loa2</saml2:AuthnContextClassRef>

  </saml2:AuthnContext>

</saml2:AuthnStatement>
```

I detta exempel autentiserar sig anslutande part på tillitsnivå 2 via en identitetsintygutfärdare (IdP) som är godkänd av DIGG och ansluten till Sweden Connect.

³ Deployment Profile for the Swedish eID Framework [EidDeploy] ver 1.7 kap 5.3.1.

⁴ Deployment Profile for the Swedish eID Framework [EidDeploy] ver 1.7 kap 6.2 & 6.3.4

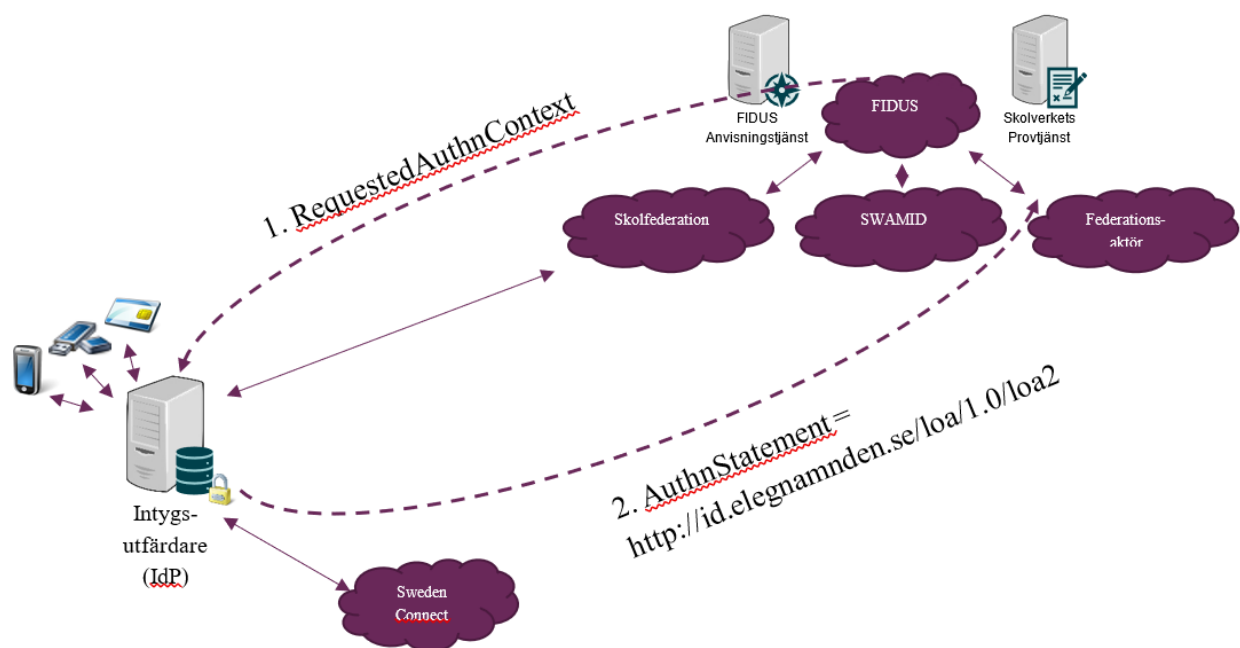
Lista på av Skolverkets provtjänst accepterade tillitsnivåer

Sweden Connect är DIGG:s ekosystem för e-legitimering, såväl nationellt som inom ramen för samverkan i EU (eIDAS). I Sweden Connect finns signaleringen av tillitsnivå definierad⁵. I nedan tabell listas de olika tillitsnivåerna som är Skolverkets provtjänst litar på. De är skrivna i den form, *Authentication Context URI*, som de ska presenteras för provtjänsten. Vilken av dessa URIs en 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.

URI	Kommentar
http://id.elegnamnden.se/loa/1.0/loa2	Av DIGG godkänd e-leg utfärdare och godkänd IdP på tillitsnivå 2.
http://id.elegnamnden.se/loa/1.0/loa3	Av DIGG godkänd e-leg utfärdare och godkänd IdP på tillitsnivå 3.
http://id.elegnamnden.se/loa/1.0/loa4	Av DIGG godkänd e-leg utfärdare och godkänd IdP på tillitsnivå 4.
http://id.swedenconnect.se/loa/1.0/uncertified-loa2	Av DIGG godkänd e-leg utfärdare på tillitsnivå 2, men ej av DIGG godkänd IdP
http://id.swedenconnect.se/loa/1.0/uncertified-loa3	Av DIGG godkänd e-leg utfärdare på tillitsnivå 3, men ej av DIGG godkänd IdP
http://id.swedenconnect.se/loa/1.0/loa2-nonresident	Av DIGG godkänd e-leg utfärdare och godkänd IdP på tillitsnivå 2 där e-leg innehavaren saknar svenskt personnummer eller samordningsnummer.
http://id.swedenconnect.se/loa/1.0/loa3-nonresident	Av DIGG godkänd e-leg utfärdare och godkänd IdP på tillitsnivå 3 där e-leg innehavaren saknar svenskt personnummer eller samordningsnummer.
http://id.swedenconnect.se/loa/1.0/loa4-nonresident	Av DIGG godkänd e-leg utfärdare och godkänd IdP på tillitsnivå 4 där e-leg innehavaren saknar svenskt personnummer eller samordningsnummer.
http://id.elegnamnden.se/loa/1.0/nf-low	Notifierad enligt eIDAS på tillitsnivå låg.
http://id.elegnamnden.se/loa/1.0/nf-sub	Notifierad enligt eIDAS på tillitsnivå väsentlig.
http://id.elegnamnden.se/loa/1.0/nf-high	Notifierad enligt eIDAS på tillitsnivå hög.

⁵ Swedish eID Framework - Registry for identifiers [EidRegistry] ver 1.7 kap 3.1.

Exempel anslutning på tillitsnivå 2 med IdP som är godkänd av DIGG och ansluten till Sweden Connect:



Exempel anslutning på tillitsnivå 3 med IdP som ej är godkänd av DIGG:

