Skolverket

DNP-projektet 2023-06-15

Signalering av tillitsnivå till Skolverkets provtjänst

Innehåll

Bakgrund

Den 21 september 2017 fick Skolverket i uppdrag av regeringen att utveckla och tillhandahålla digitaliserade nationella prov och bedömningsstöd i grundskolan och på gymnasial nivå.

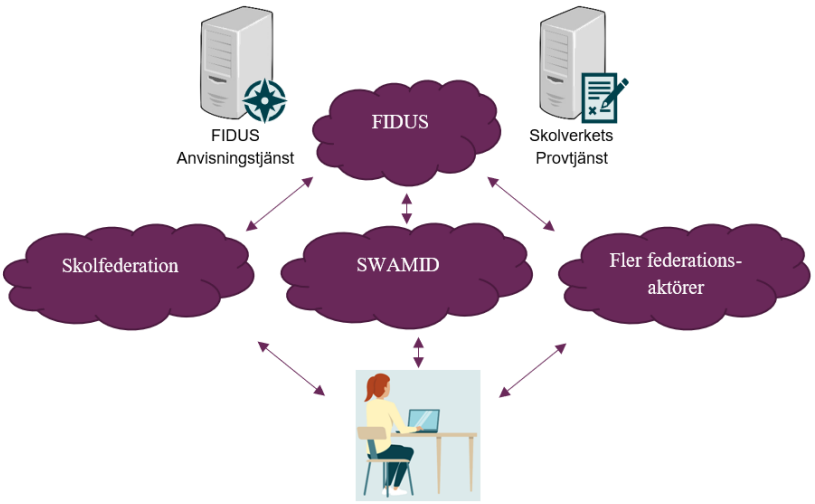
Införandet av digitala nationella prov (DNP) kommer att ske successivt med start år 2024 och berör tusentals skolor och hundratusentals elever. Det finns två centrala delar i digitaliseringen av nationella prov: utveckling av den digitala provtjänsten och det förändringsarbete som behöver göras på skolorna.[1]

Det är Skolverket som ansvarar för att realisera digitala nationella prov men för att eleverna ska kunna genomföra proven digitalt behöver alla skolor ha nödvändig teknik och kompetens på plats.

Detta dokument beskriver olika tillvägagångssätt och en del tekniska förutsättningar för åtkomst till Skolverkets provtjänst med fokus på hur anslutande part ska signalera på vilken tillitsnivå densamma har autentiserat sig.

Kravbild för åtkomst med avseende på teknisk anslutning

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



[1] För mer information, se https://www.skolverket.se/om-oss/var-verksamhet/skolverkets-prioriterade-omraden/digitalisering/digitala-nationella-prov/digitalisering-av-de-nationella-proven---overgripande-information.

Det finns för närvarande två identitetsfederationer anslutna till FIDUS som möter Skolverkets krav:

- Skolfederation[2] (grundskola, gymnasieskola och komvux)
- SWAMID[3] (universitets- och högskolesektorn)

För att möjliggöra federerad inloggning behövs förmåga att ställa ut digitala identitetsintyg i form av SAML-intyg (Security Assertion Markup Language), 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 identitetsintygstjänst, även kallad IdP och legitimeringstjänst. Förmågan måste också möta de mer detaljerade krav som ställs av den federation som är aktuell att ansluta sig till.

Skolverket ställer **inte** krav på att själva identitetsintygstjänsten (IdP) ska vara granskad och godkänd av DIGG.

Identitetsbegreppet eppn

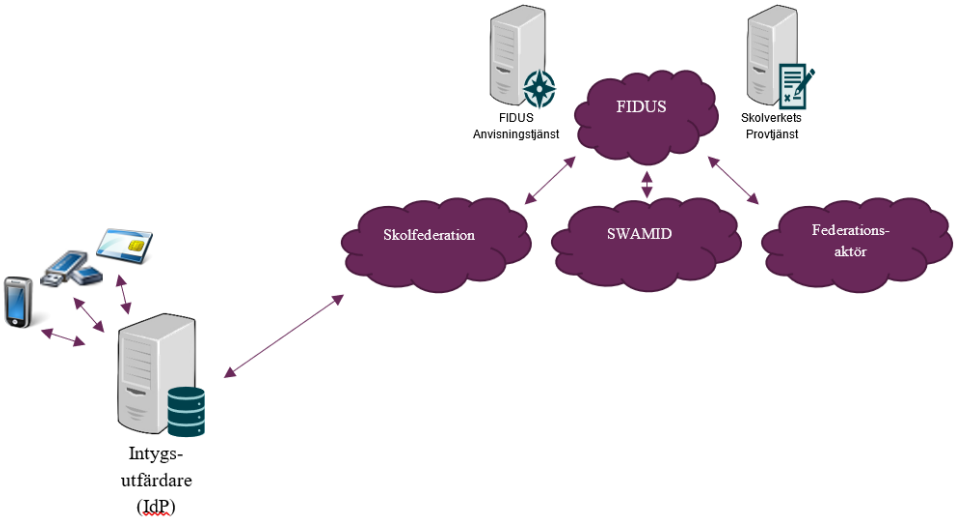
Skolverket har valt eppn[4] som identitetsbegrepp. Det är ett internationellt vedertaget identitetsbegrepp som används i grundskola, gymnasieskola och komvux samt inom universitets- och högskolesektorn. Identitetsbegreppet finns också med i standarden SS12000[5] för informationsutbyte mellan verksamhetsprocesser i skolan. Identitetsbegreppet eppn uttrycks som [unik identitet]@[huvudman].se. Alla identiteter, oavsett eppn eller ej, ska vara unika över tid. Det är också viktigt att det inte finns någon synlig koppling mellan den unika identiteten och den fysiska personen, utan eppn ska ses som en pseudonym. Det innebär också att det inte går att urskilja eller identifiera personer som har skyddad identitet.

[2] https://www.skolfederation.se

[3] https://www.sunet.se/services/identifiering/swamid
[4] https://www.skolverket.se/om-oss/var-verksamhet/skolverkets-prioriterade-omraden/digitalisering/digitala-nationella-prov/tekniska-forutsattningar-for-digitala-nationella-prov/eppn
[5] https://www.sis.se/standardutveckling/tksidor/tk400499/sistk450/ss-12000/

Åtkomst för skolpersonal till Skolverkets provtjänst via identitetsintygsutfärdare (IdP)

Den sammanfattande kravbilden för skolpersonalens åtkomst till DNP, är att e-legitimering ska ske på minst tillitsnivå 2 enligt *Tillitsramverket för kvalitetsmärket Svensk e-legitimation*[6] 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 tillitnivå 2. Skolverket ställer inte krav på att själva identitetsintygsutfärdaren (IdP) ska vara granskad och godkänd av DIGG. Identiteten på den som ansluter kan presenteras i form av ett eppn. För att identitetsintygsutfärdaren (IdP) på ett korrekt sätt ska kunna presentera detta för Skolverkets provtjänst finns vissa förutsättningar.

[6] 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.

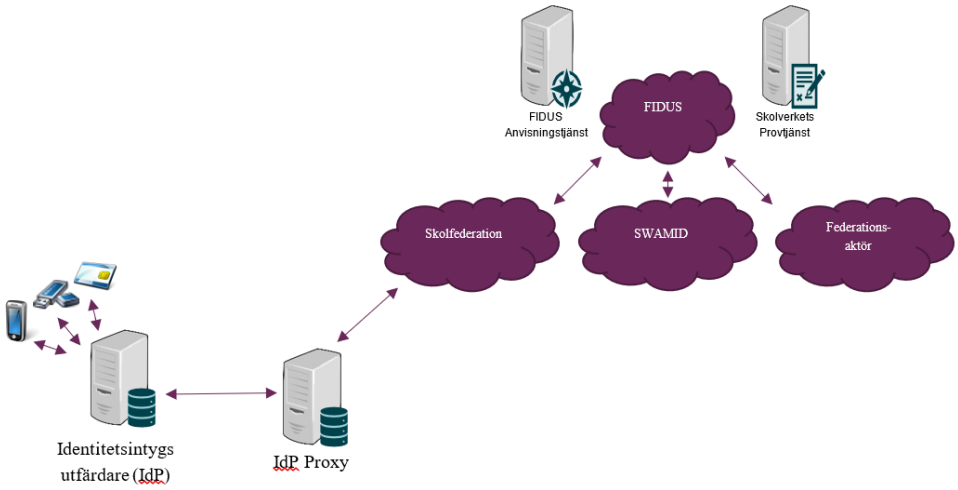
Användningen av olika tillitsnivåer i DNP ställer krav på att provtjänsten i rollen som e-tjänst (Service Provider, SP) kan ställa krav på att vissa inloggningar kräver en viss tillitsnivå. Exempelvis skolpersonalen som ska logga in med en e-legitimation på minst tillitsnivå 2. Det innebär att identitetsidentitetsintygsutfärdaren (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 Connect[7], 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.



[7] https://www.swedenconnect.se

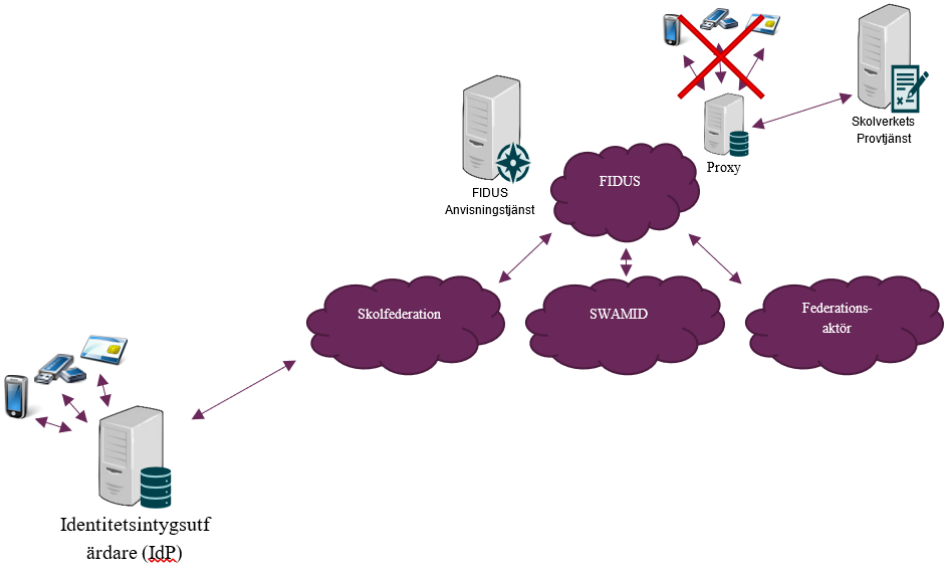
Signalering av tillitsnivå

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 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

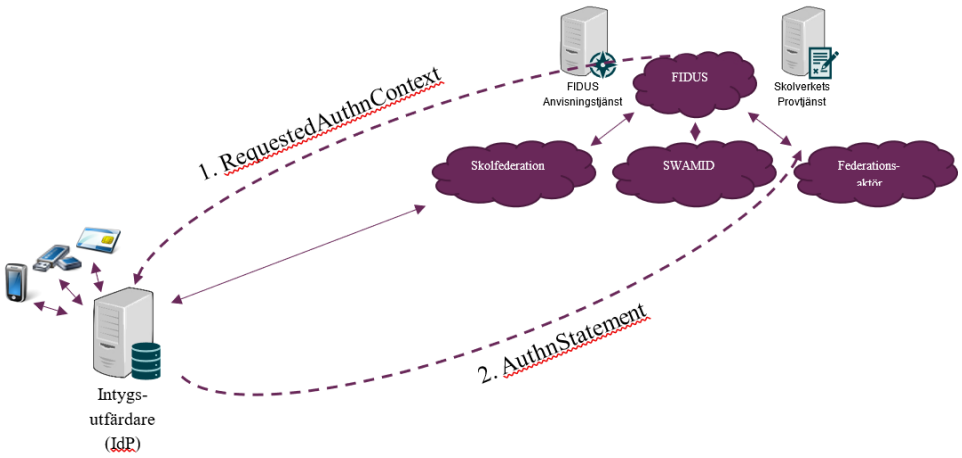
För en identitetsintygsutfärdande (IdP) som har förmåga att signalera tillitsnivå måste följande markering göras i SAML-metadata på identitetsintygsutfärdanden så att en stark autentisering inte påförs vid anslutningstillfället:

```
<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/authent
    ication/e-leg</saml:AttributeValue>

    </saml:Attribute>

  </mdattr:EntityAttributes>

</md:Extensions>
```

Anslutning med tillitssignalering

När en identitetsintygsutfärdande (IdP), där tillitsignalering 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 provtjänsten[8]:

```
<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 identitetsintygsutfärdare (IdP) till provtjänsten skulle kunna se ut[9]:

```
<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 identitetsintygsutfärdare (IdP) som är godkänd av DIGG och ansluten till Sweden Connect.

[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

Lista på av Skolverkets provtjänst accepterade tillitsnivåer

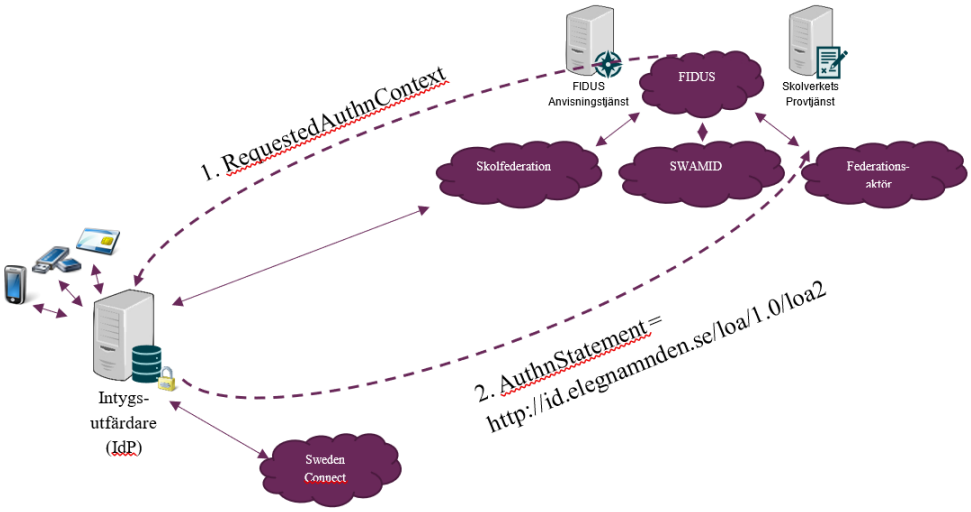
Sweden Connect är DIGG:s ekosystem för e-legitimering, såväl nationellt som inom ramen för samverkan i EU (eIDAS). I Sweden Connect finns signaleringen av tillitsnivå definierat[10]. I nedan tabell listas de olika tillitsnivåerna som är Skolverkets provtjänst litar på. De är skrivna i den form, *Authentication 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 tilllitsnivå 2, men ej av DIGG godkänd IdP
http://id.swedenconnect.se/loa/1.0/uncertified-loa3	Av DIGG godkänd e-leg utfärdare på tilllitsnivå 3, men ej av DIGG godkänd IdP
http://id.swedenconnect.se/loa/1.0/ loa2-nonresident	Av DIGG godkänd e-leg utfärdare och

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

	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.

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: