Exempel på åtkomst till digitala nationella prov

Bilaga till Vägledning för skolhuvudmän – Tekniska förutsättningar för digitala nationella prov (DNP)

inera

Sveriges Kommuner och Regioner

Exempel på åtkomst till digitala nationella prov

Bilaga till Vägledning för skolhuvudmän – Tekniska förutsättningar för digitala nationella prov (DNP)

Upplysningar om innehållet:
Mikael Svensson, mikael.svensson1@skr.se
Börje Shameti Lewin, borje.shameti.lewin@inera.se

ISBN: 978-91-8047-116-9
Illustration: Maja Larsson
Produktion: Advant

Inledning

Det är Skolverket som ansvarar för att realisera digitala nationella prov (DNP)[1], men för att eleverna ska kunna genomföra proven digitalt behöver alla skolor ha nödvändig teknik och kompetens på plats. Införandet av digitala nationella prov kommer att ske successivt med start år 2024 och berör tusentals skolor och hundratusentals elever. Även verksamheter inom kommunal vuxenutbildning berörs av digitala nationella prov.

Som stöd för skolhuvudmännen i förberedelserna, har SKR tillsammans med Inera tagit fram en vägledning med huvudsakligt fokus på kraven på åtkomstlösningar och hur de kan realiseras. Denna bilaga pekar ut de vanligaste kombinationerna av vägval som skolhuvudmännen kan göra.

Vägledningen[2] har ett upplägg liknande SKR:s vägledning om eIDAS.

Målgruppen för vägledningen och denna bilaga är beslutsfattare, CIO, it-ansvarig eller motsvarande samt nyckelpersoner som arbetar med e-legitimationer och åtkomst i kommuner, regioner och andra berörda organisationer.

Målbilden är att varje organisation i möjligaste mån ska kunna använda befintliga lösningar för e-legitimering av skolpersonal och elever, förutsatt att de möter de kvalitetskrav som Skolverket ställer. Kraven är inte unika för just DNP utan är en direkt följd av regulatoriska krav som exempelvis dataskyddsförordningen och offentlighets- och sekretesslagen (2009:400).

Not. 1 https://www.skolverket.se/om-oss/var-verksamhet/skolverkets-prioriterade-omraden/digitalisering/digitala-nationella-prov.

Not. 2 https://skr.se/tjanster/merfranskr/rapporterochskrifter/publikationer/vagledning-foranslutningtilleidas.31541.html.

Innehåll

KAPITEL 1

Kravbild

Kravbild för åtkomst med avseende på e-legitimering

Skolverket ställer krav på e-legitimering av skolpersonal[1] motsvarande tillitsnivå 2[2] eller högre enligt *Tillitsramverket för kvalitetsmärket Svensk e-legitimation*[3] vid hantering och genomförande av digitala nationella prov och bedömningsstöd i Skolverkets provtjänst[4]. Med tillitsnivå[5] menas grad av säkerhet och tillförlitlighet.

Skolverket ställer inte krav på stark autentisering i form av e-legitimering eller andra lösningar, såsom multifaktorsautentisering (MFA) för elever som genomför digitala nationella prov eller betygsstödjande bedömningsstöd. Eleverna kommer att logga in i provtjänsten med de konton som skolan normalt använder.

Huvudmännen ansvarar för att elevernas uppgivna identitet vid inloggning till provplattformen vid provtillfället är tillförlitlig. Här kan huvudmannen påföra skyddsåtgärder som exempelvis MFA för att öka tilliten till elevens uppgivna identitet vid inloggningstillfället.

Not. 1 Med personal avses huvudman, skolchef, rektor, lärare eller annan administrativ personal som kan komma att behöva tillgång till digitala nationella prov och it-stöd för sådana prov.

Not. 2 https://www.skolverket.se/om-oss/var-verksamhet/skolverkets-prioriterade-omraden/digitalisering/digitala-nationella-prov/tekniska-forutsattningar-for-skolorna-att-kunna-genomfora-digitala-nationella-prov.

Not. 3 Tillitsramverket för Kvalitetsmärket Svensk e-legitimation, 2019-09-19, Myndigheten för digital förvaltning ärendenummer 219-277. För mer information, se https://www.digg.se/digital-identitet/e-legitimering/tillitsnivaer/tillitsramverket.

Not. 4 Skolverkets provtjänst är en helhetslösning för planering, genomförande och resultathantering för digitala nationella prov och bedömningsstöd. Det är en elektronisk samverkan mellan skolor och Skolverket som består av en säker inloggning, möjlighet till överföring av uppgifter, provgenomförande i en provplattform samt resultathantering.

Not. 5 För mer information, se https://www.digg.se/digital-identitet/e-legitimering/tillitsnivaer.

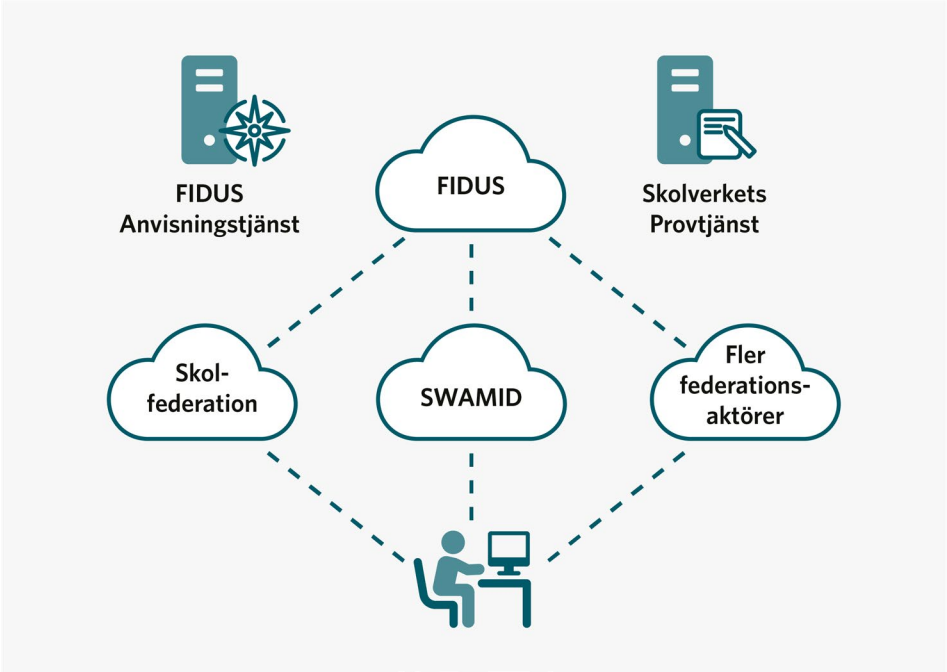
Kravbild för åtkomst med avseende på teknisk anslutning

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.

Det finns för närvarande två identitetsfederationer anslutna till FIDUS som möter Skolverkets krav[6]:

- Skolfederation[7] (grundskola, gymnasieskola och komvux)
- SWAMID[8] (universitets- och högskolesektorn)

Figur 1: Interfederationen FIDUS



Not. 6 https://github.com/FIDUSFederation/policy.
Not. 7 https://www.skolfederation.se/.
Not. 8 https://www.sunet.se/services/identifiering/swamid.

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. Förmågan måste också möta de mer detaljerade krav som ställs av den federation som är aktuell att ansluta sig till.

Avgränsning

Alla kommuner och övriga huvudmän har olika förutsättningar att hantera åtkomst. De förslag vi redovisar här tar utgångspunkt från idag vanligt förekommande lösningar, inte sällan likt ekosystem av nationella och internationella e-legitimationer, e-tjänstelegitimationer och egna autentiseringslösningar.

I denna vägledning används begreppet e-legitimation oavsett vilken form av autentiseringslösning eller autentiseringsmetod som avses, oavsett också om e-legitimationen används i tjänsten eller privat. Gemensamt är att de autentiserar en fysisk person.

Behov av konsolidering av de egna lösningarna?

Det är viktigt att åtkomst till Skolverkets provtjänst inte blir ett stuprör i den egna organisationen. Skolverkets vägval för åtkomst till provtjänsten följer bland annat SKR:s, Ineras, regionernas och kommunernas önskan om öppna och inkluderande åtkomstlösningar. För e-legitimering följer Skolverket DIGG:s tillitsramverk med avseende på kravställning av tillräcklig tillitsnivå för inloggning. För den tekniska anslutningen har Skolverket valt en federerad lösning. Lösningen är således öppen och inkluderande. Det gör att det finns en stor frihetsgrad, även över tid, för den egna organisationen att realisera kraven för genomförande av DNP.

Det är inte ovanligt att en organisation av olika skäl har flera olika lösningar för e-legitimering. Därför kan det också vara aktuellt att resonera om en konsolidering av lösningar i det här sammanhanget. Det är sällan något självändamål att ha flera olika lösningar som inte samverkar.

Osammanhållna lösningar motverkar också möjligheterna till att åstadkomma en sömlös single sign-on (SSO) för e-legitimationsinnehavaren där det är önskvärt.

Identitetsbegreppet eppn

Skolverket har valt eppn[9] 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[10] 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.

Not. 9 https://www.skolverket.se/om-oss/var-verksamhet/skolverkets-prioriterade-omraden/digitalisering/digitala-nationella-prov/tekniska-forutsattningar-for-skolorna-att-kunna-genomfora-digitala-nationella-prov/eppn.

Not. 10 https://www.sis.se/produkter/informationsteknik-kontorsutrustning/ittillampningar/ittillampningar-inom-utbildning/ss-120002020korr-12022/.

KAPITEL 2

Vägval för elevåtkomst till DNP

Den sammanfattande kravbilden för elevåtkomst är att huvudmannen ska säkerställa förmågan att presentera ett eppn för provtjänsten med tillräcklig tillförlitlighet. Skolverket ställer alltså inte specifika krav som exempelvis multifaktorautentisering (MFA) för elever. Målbilden är att eleverna kommer att logga in i provtjänsten med de konton och de metoder som skolan normalt använder, förutsatt att de är tillräckligt tillförlitliga.

Om organisationen redan idag är ansluten till en federation som är ansluten till Skolverkets interfederation FIDUS, är ni sannolikt redo för elevåtkomst till DNP, exempelvis via Skolfederation eller Swamid.

Vetenskapsrådets (Sunets) lösning för e-legitimation, eduID[11], är ett alternativ för dem som inte har några ambitioner att lösa åtkomst för elever till andra e-tjänster som exempelvis lärresurser. Viktigt att notera är att eduID enbart kan användas för åtkomst till DNP. Annan åtkomst är inte tillåten med eduID.

Vi redogör här för tre scenarier för elev-åtkomst, utan inbördes ordning:

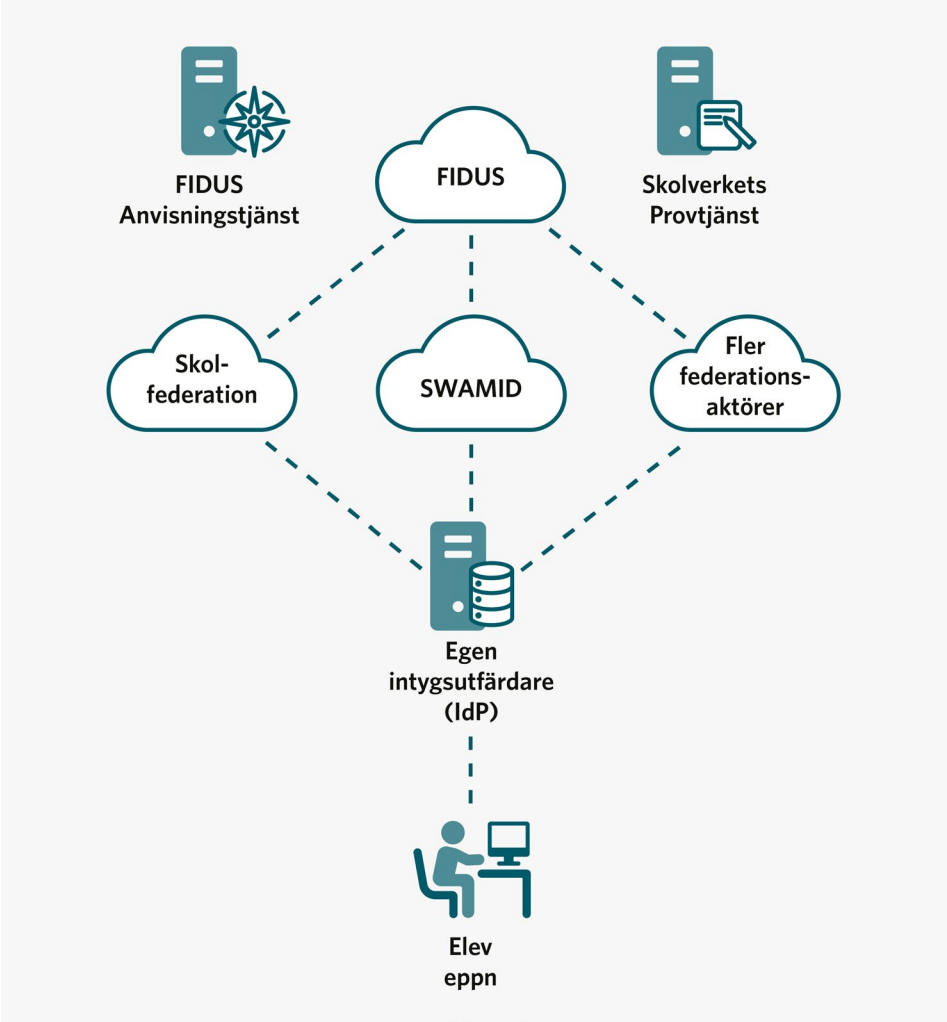
1. Egen lösning för elever
2. Upphandlad lösning för elever
3. eduID för elever.

Not. 11 https://eduid.se/.

Egen lösning för elever

I detta scenario har huvudmannen sannolikt en befintlig lösning i egen regi, där organisationen redan har anslutit sig till exempelvis Skolfederation för åtkomst till olika lärresurser. Skolverkets provtjänst för DNP är enbart att betrakta som ytterligare en e-tjänst som tillgängliggörs i federationen.

Figur 2: Egen lösning för elever



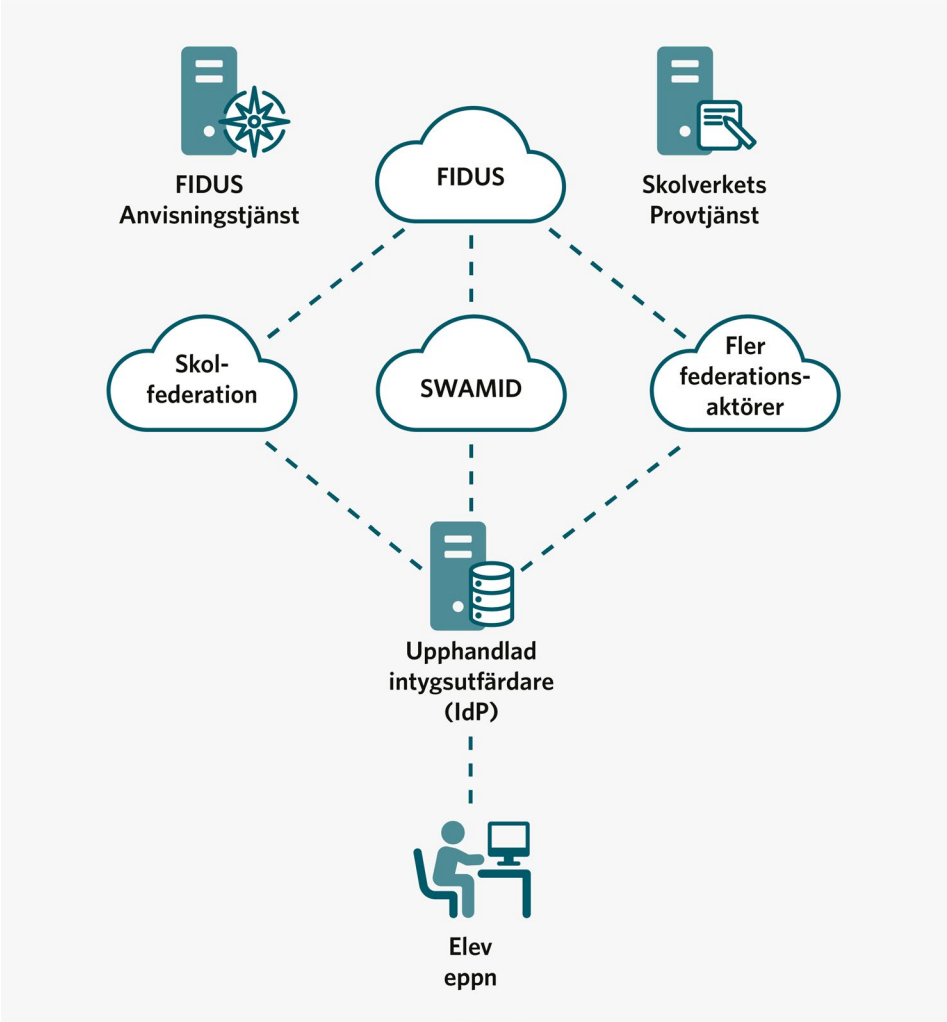
Viktigt att notera:

- Skolverket ställer krav på att huvudmannen kan uppvisa ett tillförlitligt eppn som representerar eleven. Detta krav kan mötas på flera sätt och varierar såväl över tid som med organisationens riskaptit.
- Huvudmannen ansvarar för anslutningen av den egna lösning till federation som är medlem i FIDUS. Detta är normalt en enkel standardprocedur.

Upphandlad lösning för elever

I detta scenario väljer huvudmannen en upphandlad lösning som tjänst, där organisationen via den upphandlade tjänsten ansluter sig till exempelvis Skolfederation. Via Skolfederation finns åtkomst till olika lärresurser och till Skolverkets provtjänst för DNP. DNP betraktas som ytterligare en e-tjänst som tillgängliggörs i federationen.

Figur 3: Upphandlad lösning för elever



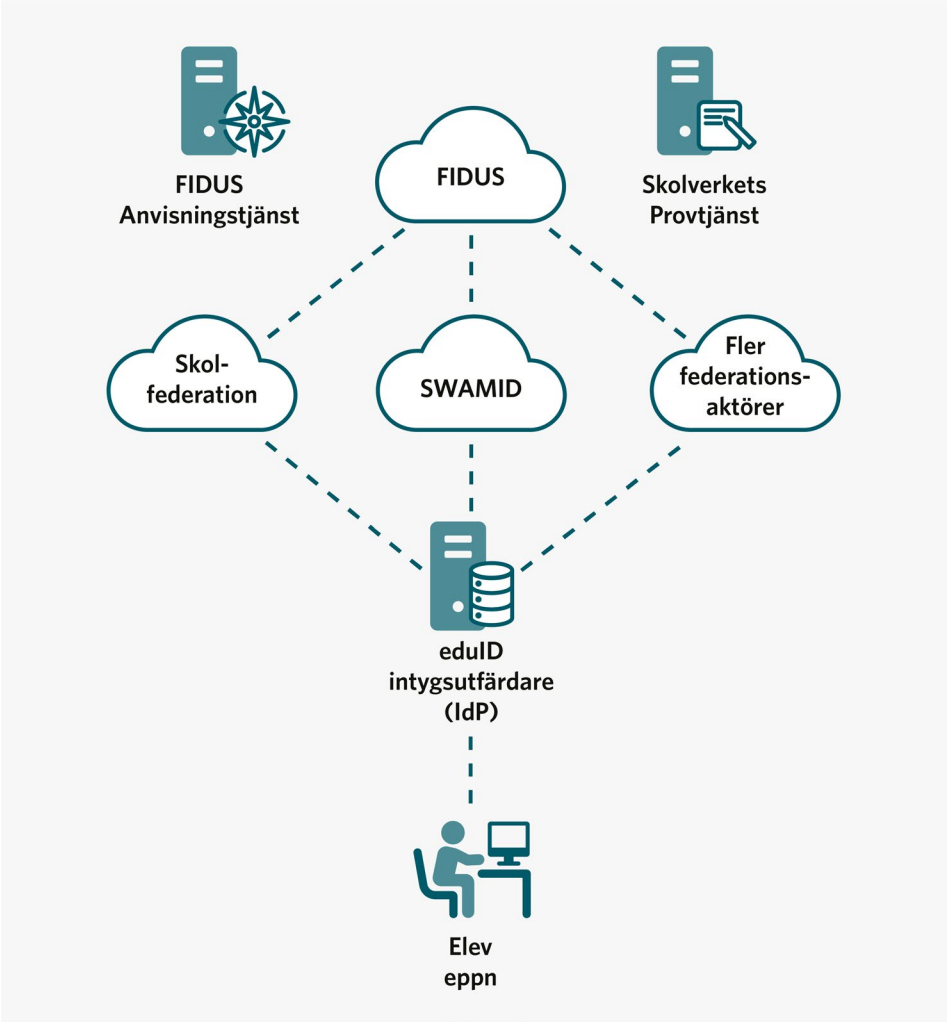
Viktigt att notera:

- Skolverket ställer krav på att huvudmannen kan uppvisa ett tillförlitligt eppn som representerar eleven. Detta krav kan mötas på flera sätt och varierar såväl över tid som med organisationens riskaptit. Här kan den upphandlade lösningen innehålla extra skyddsåtgärder som ökar tilliten till det eppn som representerar eleven.
- Upphandlad aktör ansvarar för att ansluta lösningens IdP till federation som är medlem i FIDUS. Detta är en enkel standardprocedur som normalt ingår i tjänsten.

eduID för elever

Detta scenario är snarlikt den upphandlade lösningen. Det innebär att Vetenskapsrådet (Sunet) ansvarar för lösningen som upplåts för de huvudmän som ska genomföra digitala nationella prov. Lösningen är ansluten till federationen SWAMID som är medlem i interfederationen FIDUS.

Figur 4: eduID för elever



Viktigt att notera:

- Skolverket ställer krav på att huvudmannen kan uppvisa ett tillförlitligt eppn som representerar eleven. eduID innehåller skyddsåtgärder som kan öka tilliten till det eppn som representerar eleven.
- Vetenskapsrådet (Sunet) ansvarar för lösningen och den är redan ansluten till federationen SWAMID som är medlem i FIDUS.

KAPITEL 3

Vägval för skolpersonalens åtkomst till DNP

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* vid hantering och genomförande av digitala nationella prov och bedömningsstöd i Skolverkets provtjänst.

Om organisationen redan idag är ansluten till en federation som är ansluten till Skolverkets interfederation FIDUS, är organisationen sannolikt tekniskt redo för åtkomst till DNP, exempelvis via Skolfederation eller Swamid. Detta behöver sedan kompletteras med en e-legitimationslösning som är godkänd av DIGG. Det kan vara en befintlig lösning som möter kraven i DIGG:s tillitsramverk på minst tillitsnivå 2, eller en upphandlad e-legitimationslösning som redan är godkänt av DIGG.

E-legitimationslösningen måste vara granskad och godkänd vid det tillfälle som åtkomst krävs. Granskning- och godkännandeprocessen tar normalt mellan tre och sex månader, vilket behöver beaktas.

Det är fullt möjligt att upphandla en komplett e-legitimationslösning som också innefattar förmågan att ställa ut elektroniska identitetsintyg via de federationer som nämns här, men även andra federationer som Sweden Connect[12] och Sambi[13].

Not. 12 https://www.swedenconnect.se/.
Not. 13 https://www.sambi.se/.

Vetenskapsrådets (Sunets) lösning för e-legitimation, eduID, är ett alternativ för dem som inte har några ambitioner att lösa åtkomst för skolpersonalen till andra e-tjänster som exempelvis lärresurser. Viktigt att notera är att eduID enbart kan användas för åtkomst till DNP. Annan åtkomst är inte tillåten med eduID.

Vi redogör här för sex scenarier för skolpersonalens åtkomst, utan inbördes ordning:

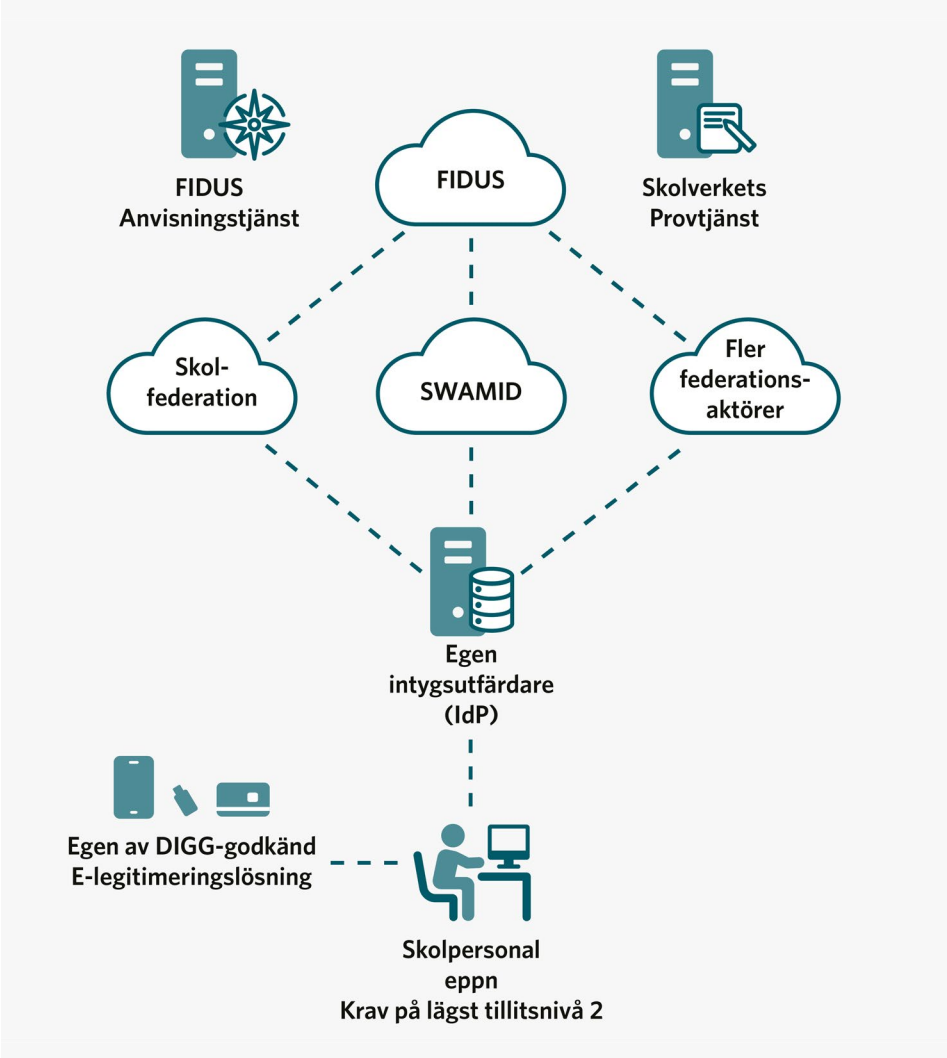
1. Egen e-tjänstelegitimeringslösning för skolpersonal
2. Upphandlad e-tjänstelegitimation och egen IdP för skolpersonal
3. Upphandlad lösning för skolpersonal
4. Privat införskaffad e-legitimation och egen IdP för skolpersonal
5. Privat införskaffad e-legitimation och upphandlad IdP för skolpersonal
6. eduID för skolpersonal.

Egen e-tjänstelegitimeringslösning för skolpersonal

I detta scenario har huvudmannen sannolikt en befintlig lösning i egen regi, där organisationen redan anslutit sig till exempelvis Skolfederation för åtkomst till olika lärresurser. Skolverkets provtjänst för DNP är enbart att betrakta som ytterligare en e-tjänst som tillgängliggörs i federationen.

Organisationen har i detta scenario också en egen e-tjänstelegitimeringslösning med tillräcklig kvalitet som möter Skolverkets krav på minst tillitsnivå 2 enligt DIGG:s tillitsramverk. Om lösningen inte redan är granskad och godkänd av DIGG, måste det ske innan lösningen kan användas för åtkomst till Skolverkets provtjänst för DNP.

Figur 5: Egen e-tjänstelegitimeringslösning för skolpersonal



Viktigt att notera:

- E-legitimationslösningar granskas och godkänns av Myndigheten för digital förvaltning (DIGG). En granskning tar normalt mellan tre och sex månader.
- Huvudmannen ansluter efter godkännande av DIGG egen lösning till federation som är medlem i FIDUS. Först därefter kan den egna e-legitimeringslösningen användas för åtkomst till Skolverkets provtjänst för DNP. Detta är normalt en enkel standardprocedur.

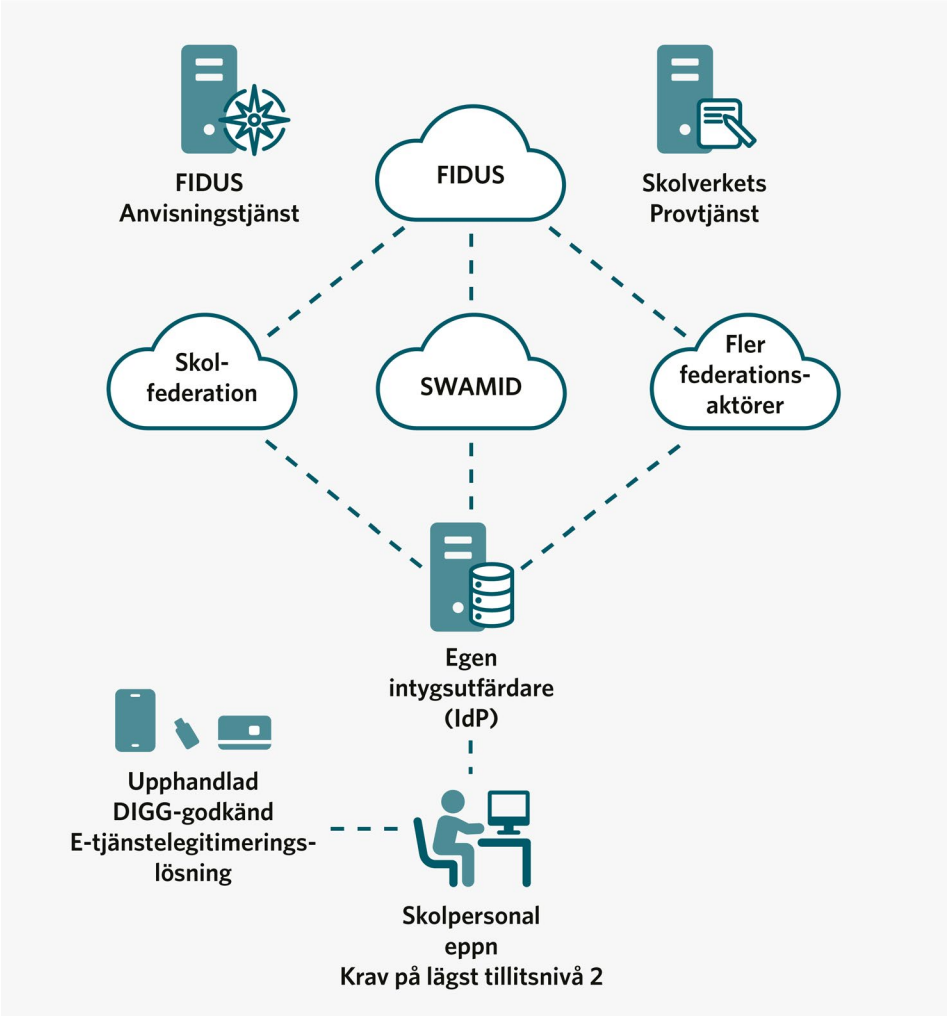
Upphandlad e-tjänstelegitimation och egen IdP för skolpersonal

I detta scenario har huvudmannen sannolikt en befintlig lösning i egen regi, där organisationen redan har anslutit sig till exempelvis Skolfederation för åtkomst till olika lärresurser. Skolverkets provtjänst för DNP är enbart att betrakta som ytterligare en e-tjänst som tillgängliggörs i federationen.

Organisationen har i detta scenario en eller flera upphandlade e-tjänstelegitimationslösningar som är godkända av DIGG till den egna intygsutfärdaren (IdP). I detta scenario avses e-tjänstelegitimationer på minst tillitsnivå 2.

Den upphandlade e-tjänstelegitimationen kan ofta konsumeras av identitetsintygsutfärdaren (IdP) via ett öppet och inkluderande gränssnitt likt SAML, och allt oftare kan den konsumeras via DIGG:s federation Sweden Connect.

Figur 6: Upphandlad e-tjänstelegitimation och egen IdP för skolpersonal



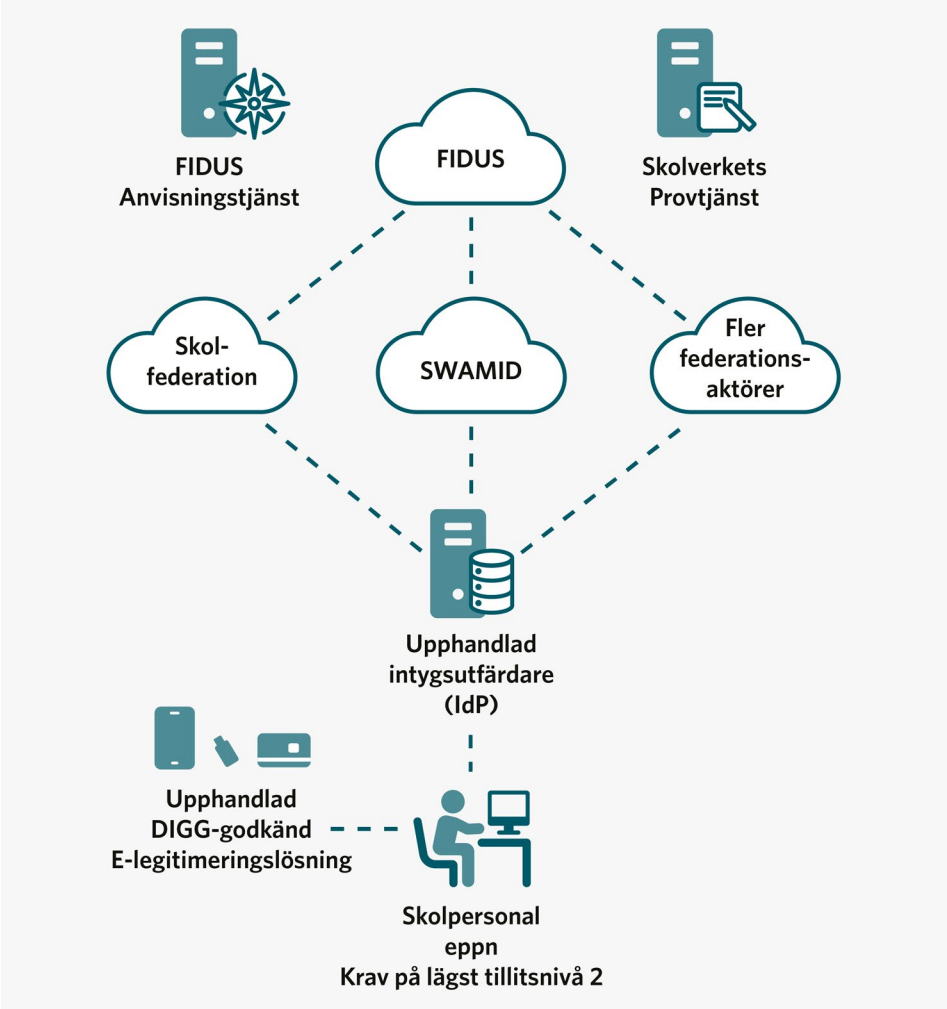
Viktigt att notera:

- Kravställ rätt tillitsnivå för e-tjänstelegitimationen och tillse att den är godkänd av DIGG. E-tjänstelegitimationen kanske ska användas för fler e-tjänster som kan ställa högre krav på tillitsnivå än nivå 2.
- Huvudmannen ansvarar för att ansluta DIGG-godkänd e-tjänste-legitimationslösning med egen IdP till federation som är medlem i FIDUS. Detta är normalt en enkel standardprocedur.

Upphandlad lösning för skolpersonal

I detta scenario väljer huvudmannen en upphandlad komplett lösning med e-tjänstelegitimation och tjänst för identitetsintygsutfärdande (IdP). Lösningen är sannolikt redan tillgängliggjord i Skolfederation och andra federationer. Skolverkets provtjänst för DNP är enbart att betrakta som ytterligare en e-tjänst som tillgängliggörs via federationen.

Figur 7: Upphandlad lösning för skolpersonal



Viktigt att notera:

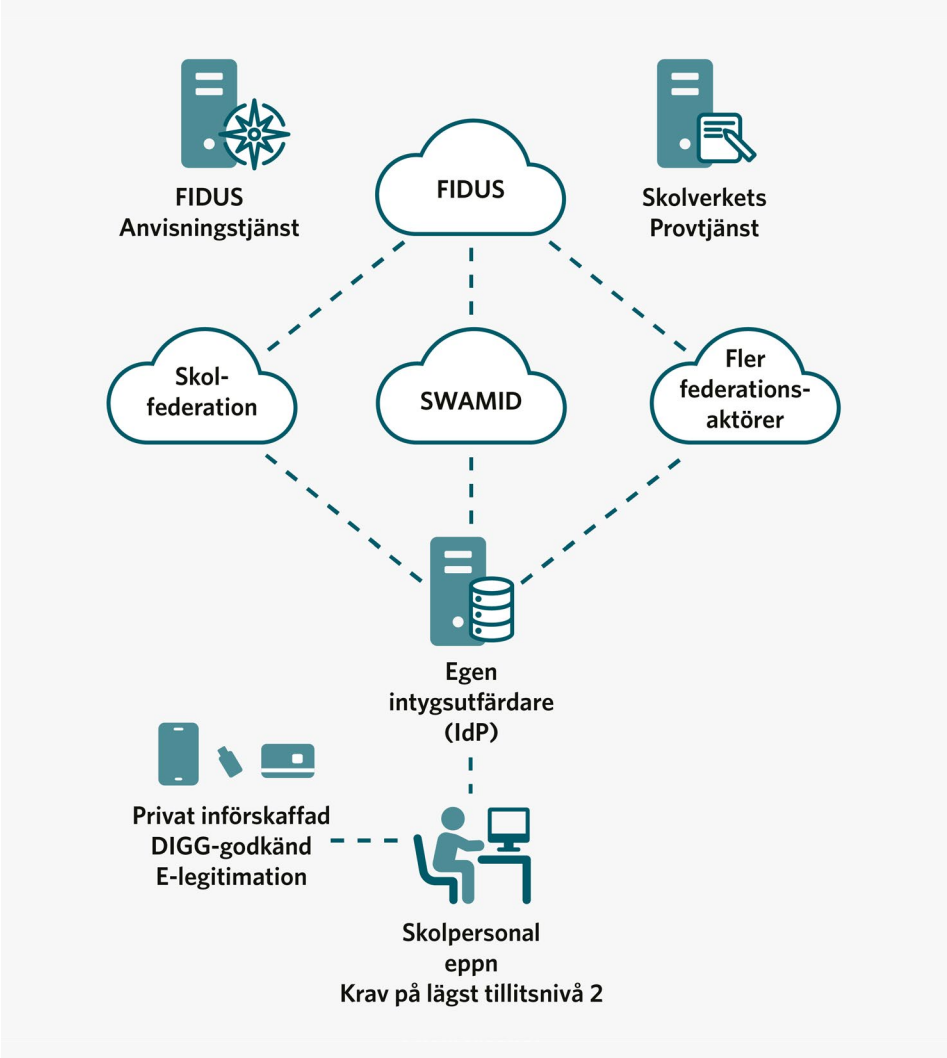
- Kravställ rätt tillitsnivå för e-tjänstelegitimationen och tillse att den är godkänd av DIGG. E-tjänstelegitimationen kanske ska användas för fler e-tjänster som kan ställa högre krav på tillitsnivå än nivå 2.
- Den upphandlade aktören ansvarar för att ansluta DIGG-godkänd e-tjänstelegitimationslösning med egen IdP till federation som är medlem i FIDUS. Detta är normalt en enkel standardprocedur.

Privat införskaffad e-legitimation och egen IdP för skolpersonal

Detta scenario skiljer sig inte nämnvärt från scenariot med en upphandlad e-tjänstelegitimation och egen IdP för skolpersonal. Skillnaden är att här är det en privat införskaffad e-legitimation, exempelvis BankID, som har anslutits till den egna identitetsintygsutfärdaren (IdP). Sannolikt finns den anslutningen sedan tidigare, om organisationen också tillhandahåller e-tjänster för allmänheten.

Om organisationen inte redan är ansluten till exempelvis Skolfederation för åtkomst till olika lärresurser, behöver anslutning ske. Skolverkets provtjänst för DNP är enbart att betrakta som ytterligare en e-tjänst som tillgängliggörs i federationen.

Figur 8: Privat införskaffad e-legitimation och egen IdP för skolpersonal



Viktigt att notera:

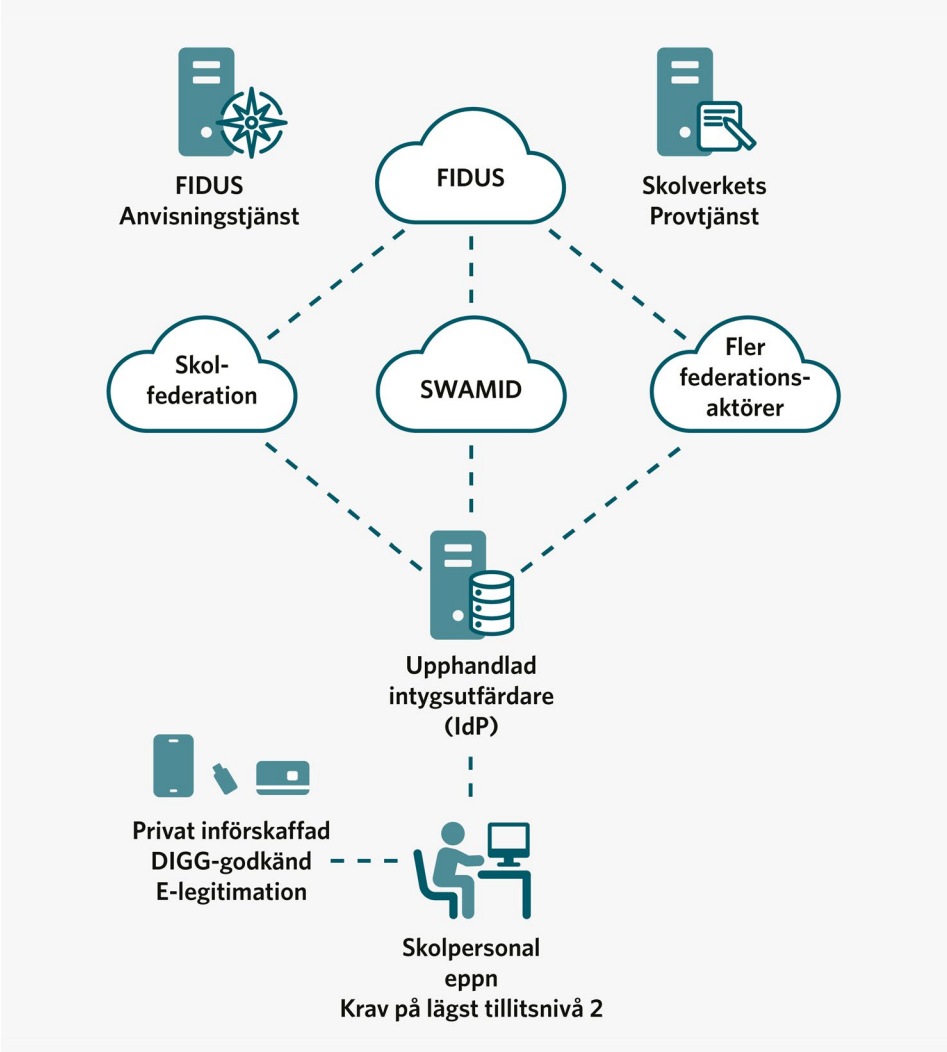
- Säkerställ rätt tillitsnivå för e-legitimationen och att den är godkänd av DIGG.
- Huvudmannen ansvarar för att ansluta DIGG-godkänd e-legitimationslösning med egen IdP till federation som är medlem i FIDUS. Detta är normalt en enkel standardprocedur.

Privat införskaffad e-legitimation och upphandlad IdP för skolpersonal

Detta scenario skiljer sig inte nämnvärt från scenariot med en komplett upphandlad lösning för skolpersonal. Skillnaden är att här är det en privat införskaffad e-legitimation, exempelvis BankID, som har anslutits till den upphandlade IdP. Sannolikt finns den anslutningen sedan tidigare, om organisationen också tillhandahåller e-tjänster för allmänheten.

Den upphandlade lösningen är sannolikt också redan tillgängliggjord i Skolfederation och andra federationer. Skolverkets provtjänst för DNP är enbart att betrakta som ytterligare en e-tjänst som tillgängliggörs via federationen.

Figur 9: Privat införskaffad e-legitimation och upphandlad IdP för skolpersonal



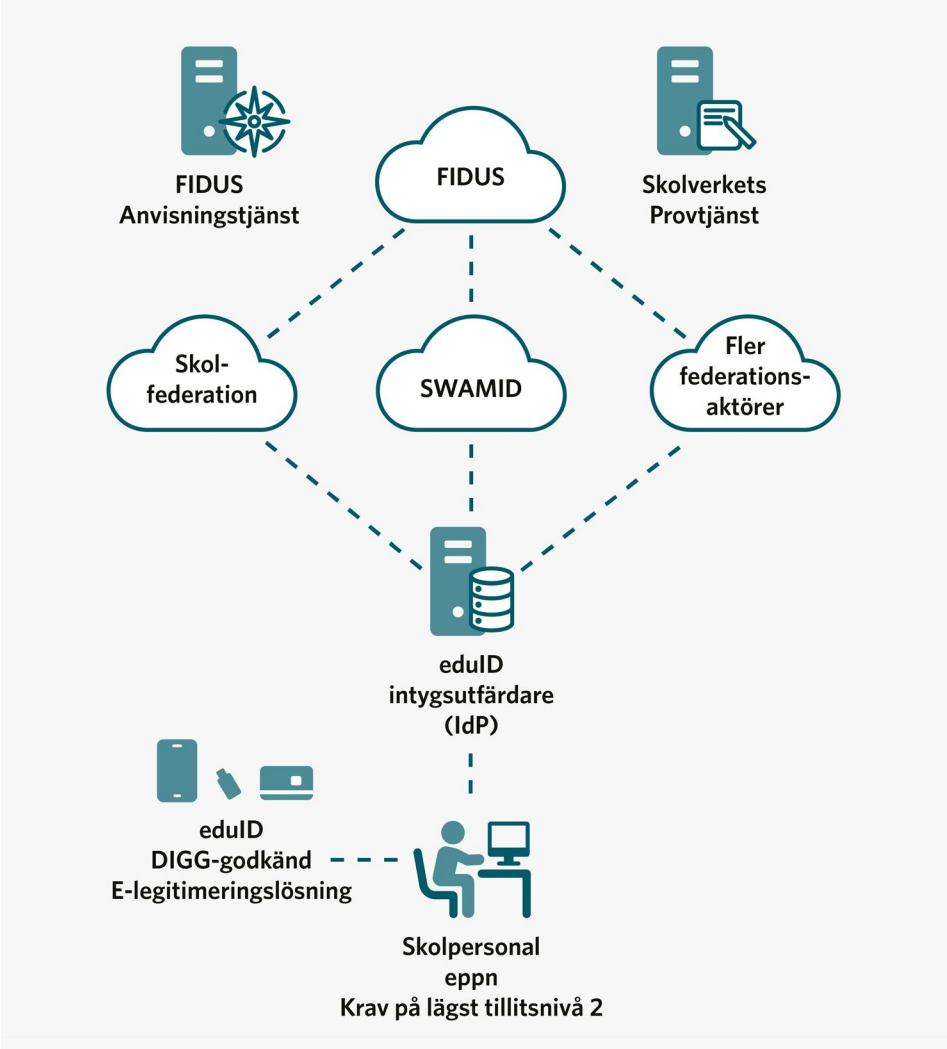
Viktigt att notera:

- Säkerställ rätt tillitsnivå för e-legitimationen och att den är godkänd av DIGG.
- Den upphandlade aktören ansvarar för att ansluta DIGG-godkänd e-legitimationslösning med egen IdP till federation som är medlem i FIDUS. Detta är normalt en enkel standardprocedur.

eduID för skolpersonal

Detta scenario är snarlikt det upphandlade scenariot. Det innebär att Vetenskapsrådet (Sunet) ansvarar för lösningen som upplåts för de huvudmän som ska genomföra digitala nationella prov. Lösningen är ansluten till federationen SWAMID som är medlem i interfederationen FIDUS.

Figur 10: eduID för skolpersonal



Viktigt att notera:

- Vetenskapsrådet (Sunet) ansvarar för lösningen och den är redan ansluten till federationen SWAMID som är medlem i FIDUS.

KAPITEL 4

Godkända e-legitimationer

Här redovisas e-legitimationer som är godkända eller på väg att bli godkända i skrivande stund (december 2022). För en dagsaktuell förteckning se DIGG:s webb[14].

Redovisningen är indelad i

- e-legitimationer som bekostats av arbetsgivaren
- e-tjänstelegitimationer
- privat införskaffade e-legitimationer.

Det är just införskaffandet av e-legitimationen som är den faktiska skillnaden. E-tjänsten som konsumerar e-legitimationen gör ingen skillnad på om e-legitimationen införskaffats privat eller om e-legitimationen bekostats av arbetsgivaren. Det finns heller ingen skillnad i hur innehavaren presenteras för e-tjänsten, utan önskat identitetsbegrepp och önskvärda attribut kan påföras oavsett val av e-legitimation.

Idag godkända e-tjänstelegitimationer

Här redovisas e-legitimationer som införskaffas av arbetsgivaren i syfte att användas i tjänsten:

Följande är i dag godkända av DIGG:

- EFOS på kort (nivå 4) och på mobil (nivå 3) från Försäkringskassan
- Freja Organisations eID på mobil (nivå 3) från Freja eID Group AB
- SITHS på kort (nivå 3) och på mobil (nivå 3) från Inera AB.

Not. 14 https://www.digg.se/digitala-tjanster/e-legitimering#DIGGsgranskningav-elegitimationer.

Ytterligare aktörer är i processen att bli godkända utfärdare enligt DIGG:

- eduID (nivå 2)
- Freja Org ID (nivå 2)
- Nexus (nivå 3 & 4)
- Pointsharp (nivå 3)
- Stockholms stad (nivå 2)

Idag godkända e-legitimationer som införskaffats privat

Följande privat införskaffade e-legitimationer är i dag godkända av DIGG:

- BankID på kort (nivå 3) och mobil (nivå 3) från Finansiell ID-Teknik BID AB
- Freja eID Plus på mobil (nivå 3) från Freja eID Group AB
- Skatteverket/AB Svenska Pass på kort (nivå 3 & 4) från AB Svenska Pass.

Ytterligare aktörer är i processen att bli godkända utfärdare enligt DIGG, exempelvis följande:

- Freja (nivå 2)

KAPITEL 5

Särskilda tekniska förmågor

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. Det sker inom ramen för standardiseringen av SAML, men det finns trots detta leverantörer av mjukvara för identitetsintygsutfärdande (IdP) som inte har den förmågan. Det är därför en viktig del i kravställningen.

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

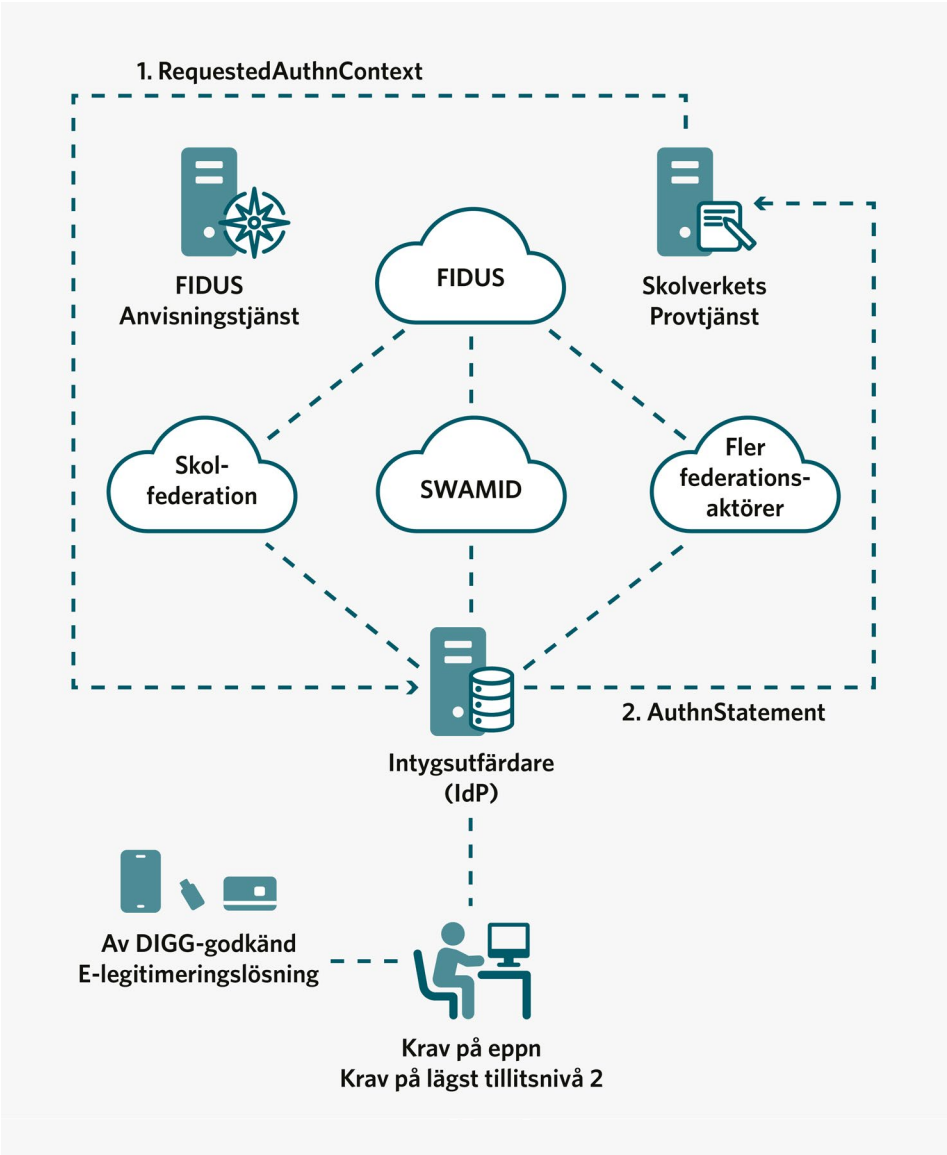
Mot bakgrund av att alla intygsutfärdare (IdP) inte har förmåga att signalera tillitsnivå, måste de intygsutfärdare (IdP) som har förmågan markera detta i sitt SAML-metadata. Det görs enligt följande:

```
<md:Extensions>
  <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:meta-
  data: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>
```

Den intygsutfärdare (IdP) som inte markerar sitt SAML-metadata enligt ovan, kommer att påföras en av DIGG godkänd e-legitimation på lägst tillitsnivå 2 vid autentiseringstillfället.

Signalering av tillitsnivå

Figur 11: Signalering av tillitsnivå



Signalering av tillitsnivå görs genom att provtjänsten begär att intygsutfärdaren (IdP) ska meddela vilken tillitsnivå som användaren har loggat in på. Provtjänsten gör det genom att inom ramen för ”RequestedAuthnContext” meddela vilka tillitsnivåer som provtjänsten accepterar (se nedan). Intygsutfärdarens (IdP) svar i form av ”AuthnStatement” måste vara något av de alternativ som provtjänsten begärt.

Exempel: RequestedAuthnContext från Provtjänsten (SP)

```
<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:AuthnContext
                              ClassRef>
   <saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/
                              uncertified loa3</saml2:AuthnContext
                              ClassRef>
   <saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa2-
                              nonresident</saml2:AuthnContextClass
                              Ref>
   <saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa3-
                              nonresident</saml2:AuthnContextClass
                              Ref>
   <saml2:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa4-
                              nonresident</saml2:AuthnContextClass
                              Ref>
   <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 från intygsutfärdare (IdP)

```
<saml2:AuthnStatement AuthnInstant="2022-12-24T15:00:00" SessionIn-
dex="ac7891..." >
    <saml2:AuthnContext>
        <saml2:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/
        loa2</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
</saml2:AuthnStatement>
```

Signalering enligt DIGG:s ramverk för Sweden Connect

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[15] och där har Skolverkets provtjänst valt att lita på följande:

Tabell 1: Signalering som Skolverkets provtjänst litar på

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.

Not. 15 Swedish eID Framework – Registry for identifiers [EidRegistry] ver 1.7 kap 3.1.

KAPITEL 6

Piloter

I samband med att SKR och Inera tagit fram *Vägledning för skolhuvudmän – tekniska förutsättningar för digitala nationella prov* (DNP), har flera skolhuvudmän agerat piloter för att belysa olika scenarier:

1. Egen lösning för elever
2. Egen e-tjänstelegitimeringslösning för skolpersonal
3. Upphandlad e-tjänstelegitimation och egen IdP för skolpersonal
4. Privat införskaffad e-legitimation och egen IdP för skolpersonal.

I skrivande stund (december 2022) är pilotverksamheten ännu inte avslutad. Dokumentation från pilotverksamheterna kommer att tillgängliggöras på skr.se i takt med att de är avslutade.

Exempel på åtkomst till digitala nationella prov

Bilaga till Vägledning för skolhuvudmän – Tekniska förutsättningar för digitala nationella prov (DNP)

Som komplement till *Vägledning för skolhuvudmän – tekniska förutsättningar för digitala nationella prov (DNP)*, har SKR och Inera också tagit fram denna exempelbilaga. Bilagan innehåller konkreta instruktioner för olika vägval när det gäller skolhuvudmännens förberedelser för de digitala nationella proven.

Denna bilaga har ett huvudsakligt fokus på kraven på åtkomstlösningar och hur de kan realiseras, med utgångspunkten att befintliga lösningar för e-legitimering av skolpersonal och elever ska kunna användas.

Målgruppen för vägledningen och exempelbilagan är beslutsfattare, CIO, it-ansvarig eller motsvarande samt nyckelpersoner som arbetar med e-legitimationer och åtkomst i kommuner, regioner och andra berörda organisationer.

ISBN 978-91-8047-116-9
Beställ eller ladda ner på skr.se/publikationer
Post: 118 82 Stockholm | **Besök:** Hornsgatan 20
Telefon: 08-452 70 00 | skr.se

Sveriges Kommuner och Regioner