Slutrapport
Arkitektur för identitet och behörighet ur ett lärosätesgemensamt perspektiv del 2

Sammanfattning

Under 2017 genomförde *SUNET Inkubator* projektet *Nationellt IAM-projekt*. Projektet tog en differentierad beskrivning av begrepp i kontexten *identiteter- och behörigheter inom högre utbildning* till en gemensam bild av det totala omfånget. I beskrivningen gjordes en uppdelning i fyra olika applikationskomponenter:

- identitetshanterare,
- behörighetshanterare,
- personregister samt
- organisationsregister.

Kortsiktiga och långsiktiga förändringsmöjligheter har analyserats ur ett helhetsperspektiv. De kortsiktiga har fokus på behov av IAM för studenter där behovet har identifierats såsom webbinloggning, datorinloggning, åtkomst av resurser som ex. filareor, utskrifter samt trådlöst nätverk. Den snabbaste förändringsmöjligheten på kort sikt är genomförande av applikationslösenord och centralisering av *eduroam* vilket ger vinster inom såväl infrastruktur som kompetens. Det mer långsiktiga behovet är att skapa en sektorsgemensam identitetshantering med en fullskalig hantering för sektorgemensam hantering av person-, organisations- samt behörighetsinformation (metakatalog). Det finns befintliga komponenter, ex. *eduID*, som kan utgöra en stomme i ett sådant arbete och i rapporten har just *eduID* använts som ett begrepp men bör tolkas som en benämning för ett nytt koncept.

Projektets rekommendation är att utöka *eduID* inkrementellt till att på sikt omfatta den funktionalitet som krävs för en lärosätesgemensam hantering av IAM. Målet bör vara att alla lärosäten använder *eduID* som enda inloggningstjänst, person- och organisationsregister och underlag för behörighetshantering (metakatalog).

Sammanfattningsvis rekommenderas följande åtgärder:
Kortsiktigt

- Förändra eduroam-infrastruktur
- Komplettera eduID med AD-funktionalitet
- Implementera ett gemensamt register för studenter (person- och organisationsregister och underlag för behörighetshantering)

Långsiktigt

- Inkludera personal och andra kategorier än studenter i det gemensamma registret
- Komplettera det gemensamma registret med övrig saknad funktionalitet

Bakgrund

Under 2017 genomförde *SUNET Inkubator* projektet *Nationellt IAM-projekt*. Projektet tog en differentierad beskrivning av begrepp i kontexten *identiteter- och behörigheter inom högre utbildning* till en gemensam bild av det totala omfånget. I beskrivningen gjordes en uppdelning i fyra olika applikationskomponenter:

- identitetshanterare,
- behörighetshanterare,
- personregister samt
- organisationsregister.

Varje komponent har en väl avgränsad uppgift och behovet av olika komponenter kan skilja från lärosäte till lärosäte.

Projektet identifierade möjligheter att effektivisera sektorns hantering av IAM genom en möjlig lärosätesgemensam infrastruktur. Därför rekommenderades ett projekt som tog resultatet till en mer detaljerad nivå i syfte att kunna utgöra underlag för fortsatt kravställnings- och implementationsarbete.

Direktivet för projektet *Arkitektur för identitet och behörighet ur ett lärosätesgemensamt perspektiv del 2* beskriver syftet att ”ta fram ett beslutsunderlag för framtida implementationsprojekt för sektorgemensamma IAM-komponenter”. Direktivet beskriver också att utgångspunkten ska vara de identifierade applikationskomponenterna.

Arbetsgång i projektet

Projektarbetet är genomfört av en projektgrupp med representation från

- Göteborgs universitet,
- Linköpings universitet,
- Luleå tekniska universitet,
- Lunds universitet,
- Stockholms universitet,
- Umeå universitet,
- SUNET samt
- Uppsala universitet.

Projektgruppen har vid tre tillfällen, á två dagar, träffats för gemensamt arbete. Vidare har arbetet bedrivits vid respektive hemort och koordinerats genom regelbundna avstämningar via videokonferens.

Styrgruppen har utgjorts av Valter Nordh (SUNET), Magnus Bodelson (Mälardalens högskola), John Westerlund (Lunds universitet) samt Jan Lundmark (Luleå tekniska universitet). Styrgruppen har sammanträtt fyra gånger under projektarbetets gång.

Projektets måluppfyllnad

Projektet har fokuserat på rekommendation av helhetsstruktur och tagit fram kortsiktiga och långsiktiga implementationsmål. Andra delar i direktivet har inte bedömts vara möjliga att genomföra i detta stadium.

IAM

Lärosätesgemensam IAM

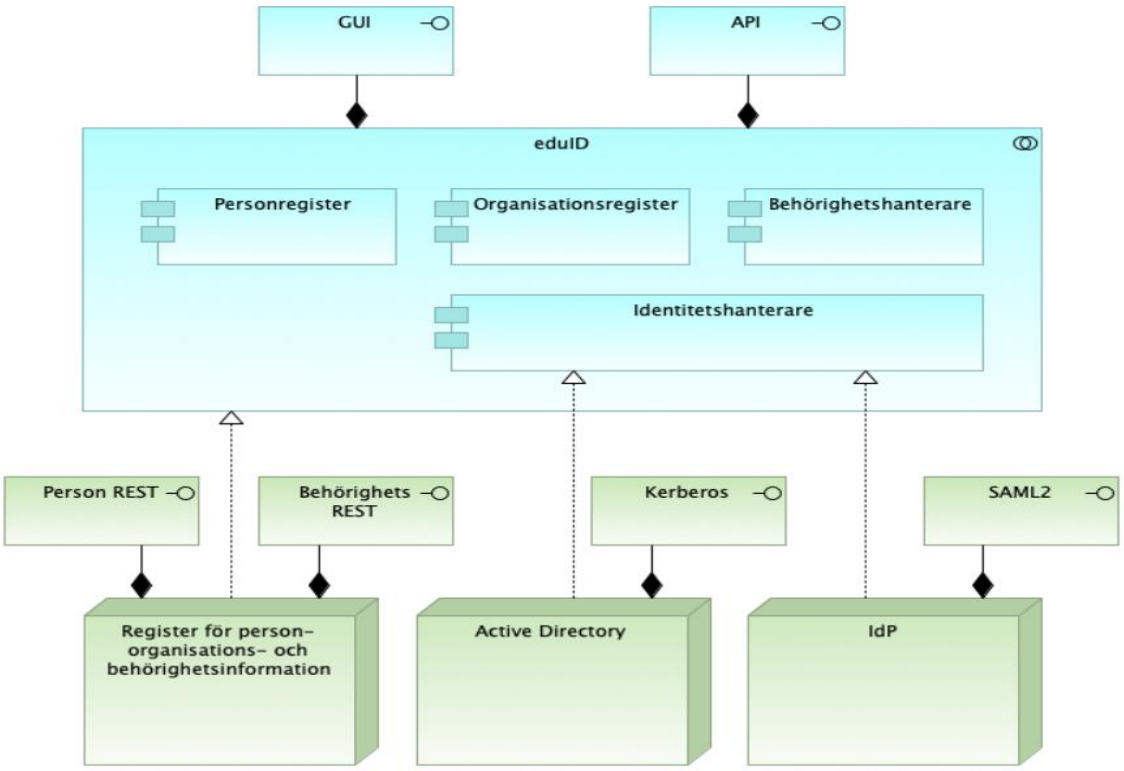
Målbild

Redan i direktivet till det tidigare projektet konstaterades att många lärosäten har en omfattande och kostnadsdrivande hantering av person- och organisationsbeskrivningar tillsammans med identitets- och behörighetshantering. Storleken på organisationen är drivande i behovet av en automatisering, både gällande etablering av konton men även för automatiserad behörighetstilldelning.

I dess bredaste bemärkelse kräver en lärosätesgemensam hantering av IAM en omfattande implementation. Därför är det viktigt att målbilden baseras på helheten men att det samtidigt går att nå målet med delmål på vägen där varje delmål på ett givet sätt ger en rationaliserings och effektiviseringsvinst.

Målbilden för helheten är sålunda en lärosätesgemensam IAM som innefattar såväl identitets- som behörighetshantering men även person- samt organisationsregister som underlag för ex. automatiserad behörighetstilldelning (metakatalog). Identitetshanteringen kommer att behöva förändras med nya krav, standarder och tekniska gränssnitt men samtidigt kunna baseras på en stabil uppsättning information för de olika domänerna person, organisation och behörigheter (metakatalog).

För att konkretisera begreppet *lärosätesgemensam IAM* har projektet använt *eduID*. Med bakgrund av det innebär begreppet *eduID* fortsättningsvis mer än den funktionalitet som *eduID* idag omfattar.



Figur 1 eduID i ett helhetsperspektiv med exemplifierande delar av implementationen

I Figur 1 beskrivs lärosätesgemensam IAM genom *eduID* som även innefattar applikationskomponenter för person- och organisationsregister samt identitets- och behörighetshantering (metakatalog). Figuren beskriver vidare att tillämpningarna behöver ge åtkomst via både tekniska och grafiska gränssnitt samt att såväl AD som SAML2 utgör tekniska gränssnitt för identitetshantering. Vidare visar figuren en implementation av ett gemensamt register för person-, organisations- och behörighetsinformation (metakatalog).

Implementationsplanering

I arbetet med att forma en väg mot målbilden, som samtidigt ger successiv vinsthemtagning, har utgångspunkten framför allt varit det behov av IAM som bedömts finnas vid ett lärosäte utan en omfattande egen implementation. Dvs. ett begränsat behov av automatiserad behörighetstilldelning och med fokus på studenter där behovet definieras med

- webbinloggning,
- datorinloggning,
- åtkomst av resurser som ex. filareor,

- utskrifter samt
- trådlöst nätverk.

eduID har redan idag funktionalitet för webbinloggning. Datorinloggningar, åtkomst av resurser samt utskrifter är i de allra flesta fall knutna till Microsoft Active Directory (AD), Microsoft Azure AD eller LDAP och åtkomst till *eduroam* kräver en RADIUS-implementation.

Det innebär att ett första steg bör innefatta rationaliseringsmöjligheter genom centralisering av lärosäteslokalhantering för *eduroam* och tjänster som idag kräver AD samt att *eduID* även måste inkludera en hantering för att signalera kopplingen mellan en användare och ett eller flera lärosäten. Det sistnämnda krävs bland annat för möjligheten att filtrera åtkomst för lärosätesspecifika tjänster.

För ett lärosäte, med ett behov som överensstämmer det som beskrivs ovan, är det då möjligt att rationalisera all hantering av studentkonton. Såväl de tekniska underliggande komponenterna som de administrativa rutiner som krävs för att verifiera kopplingen mellan person och elektronisk identitet. För ett lärosäte, som redan har implementerad automatiserad hantering, blir vissa av de första stegen mindre givande men bör samtidigt kunna ge en viss effektiviserad hantering, ex. genom en centraliserad hantering av åtkomst till *eduroam*.

Åtgärder för att implementera ovan beskrivna behov benämns vidare som *kortsiktiga förändringsmöjligheter*.

Det mer långsiktiga behovet - att komplettera *eduID* med en fullskalig hantering för beskrivning av person-, organisations- samt behörighetsinformation - benämns vidare som *långsiktiga förändringsmöjligheter*.

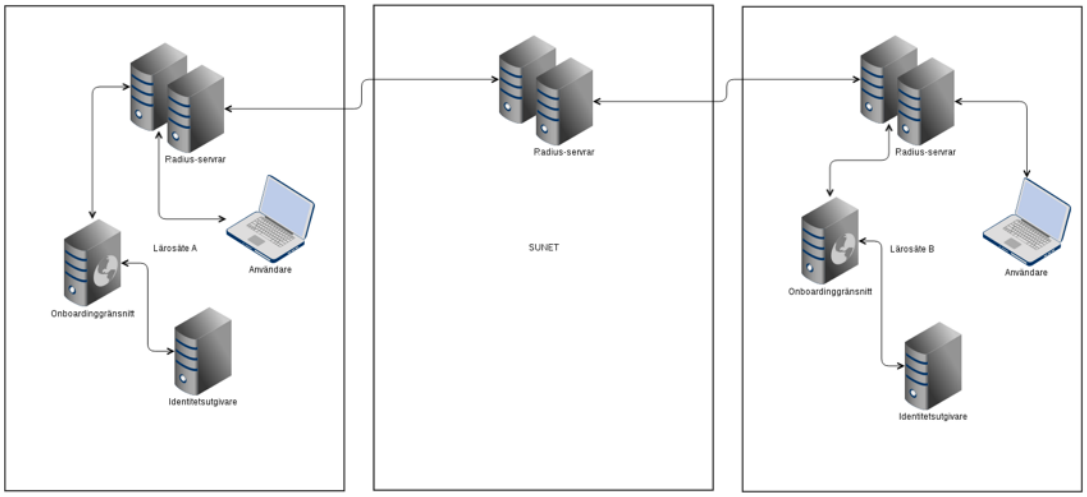
Kortsiktiga förändringsmöjligheter

Applikationslösenord som nationell tjänst

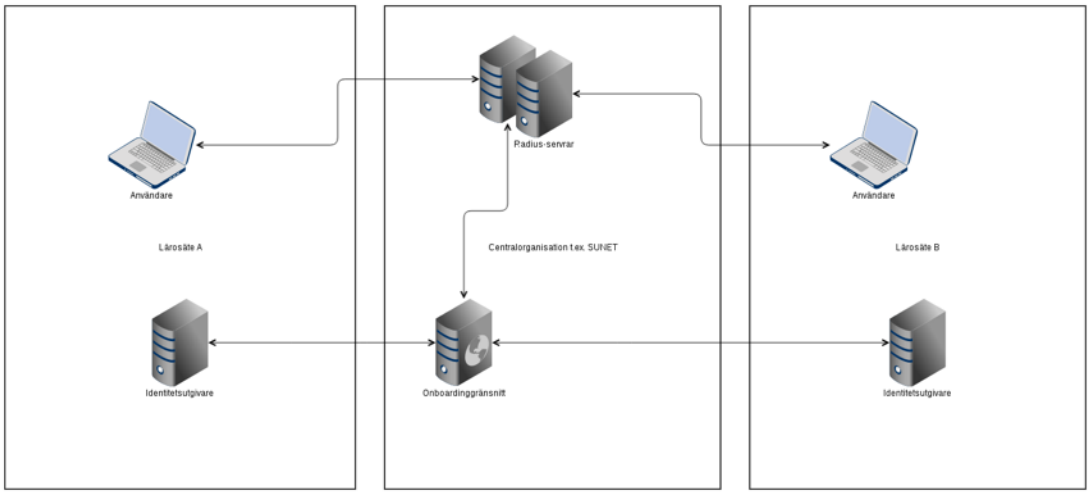
En del tjänster har behov av ett separat lösenord kopplat till användaren, skilt ifrån användarens normala lösenord. Det kan bero på tekniska förutsättningar eller för att man inte ska använda sitt vanliga lösenord av säkerhetsskäl. Ett applikationslösenord väljs vanligtvis inte av användaren utan genereras av tjänsten.

Inom sektorn har vi ett tydligt exempel på en tjänst, *eduroam*, som kräver applikationslösenord och som driver kostnader lokalt på varje lärosäte.

Idag har varje lärosäte sin egen RADIUS-infrastruktur (Figur 2) för att kunna leverera *eduroam*. Då RADIUS i de allra flesta fall enbart används för *eduroam* blir det en infrastruktur och ett kompetensområde som blir dyrt att underhålla. Genom centralisering av *eduroam* uppnås vinster inom såväl infrastruktur som kompetens (Figur 3). I de fall då *eduroam*-identiteter kopplas direkt till AD-användare finns det också en risk att förändrade licensvilkor kan påverka kostnadsbilden för att driva *eduroam* på ett sätt som är svårt att förutsäga.



Figur 2 Distribuerad RADIUS-infrastruktur



Figur 3 Centraliserad RADIUS-infrastruktur

Om *eduroam* istället levereras som en central tjänst medför det att flera komponenter kan centraliseras vilket summeras genom

- kompetens kring drift och administration av RADIUS,

- kostnader för RADIUS-infrastruktur samt
- dokumentation kring hur *eduroam* konfigureras på olika enheter.

En följd av en *eduroam som nationell tjänst med en* central RADIUS-infrastruktur är att ett driftavbrott i den centrala tjänsten skulle kunna få en lokal följdeffekt genom att om lärosätet tappar sin anslutning till Internet och den nationella tjänsten slutar även lokalt åtkomst inom lärosätet via trådlöst nät att fungera. Detta kan dock enkelt motverkas genom att göra bra teknikval för den nationella tjänsten.

Ett par frågeställningar som måste hanteras av ett tänkbart framtida införandeprojekt är:

- Vid anslutning till tjänsten sker kontroll av att användaren är behörig, t.ex. via kontroll av förhållande till ett lärosäte, för vilket tidsspann gäller en kontroll och hur genomförs förnyelse?
- Kan risken för driftavbrott håll utan hög komplexitet för lösningen?

Framtida implementation av anslutning till tjänsten *eduroam* bör möjliggöra att stora delar kan återanvändas till andra tjänster enligt modellen för applikationslösenord. Det ger en möjlighet till en generaliserad tjänst för anslutning av ytterligare tjänster som kräver lösenord (tex utskriftstjänster) via applikationslösenord.

Active Directory för *eduID*

För att ett lärosäte uteslutande ska kunna använda *eduID* för studenter behöver *eduID* inkludera möjlighet till datorinloggning samt behörighetsstyrning för åtkomst av resurser genom den elektroniska identiteten. Den teknik med störst utbredning bland landets lärosäten för ovanstående syfte är Microsoft Active Directory.

Det innebär att *eduID* måste inkludera ett tekniskt gränssnitt motsvarande AD som kan verifiera ett konto genom inloggning samt svara för den behörighetstilldelning som hanteras inom *eduID*. Hur finkornig behörighetstilldelningen är beror på övrig implementation av *eduID*, exempelvis baserat på provisionering av profildata (). Alternativt kan *eduID* inkludera ett gränssnitt för provisionering av sekundära identiteter i AD där kraven på behörighetstilldelning för AD-anslutna identiteter kan uppfyllas oförändrat.

Effektivare hantering av information knuten till användare

En grundförutsättning för en väl fungerande identitetshanterare är att kunna automatisera knytande av information till korrekt användare för att minimera manuella

insatser och därigenom spara både pengar och minska risken för felkällor. Att kunna automatisera processer för att stötta en livscykelshantering av elektroniska identiteter och därigenom kunna aktivera resp. inaktivera konton är också en grundpelare. Naturligaste implementationen av detta är att kunna förlita sig på befintliga källsystem lokalt på lärosätena (i stil med *Ladok* som källsystem för studenter och Primula som källsystem för anställda) och möjligheten att överföra informationen till *eduID* via tekniska gränssnitt.

Utveckling av tekniska gränssnitt (API) kommer av naturliga skäl att behöva gå hand i hand med ett koncept för en implementation av en nationell katalog för person-, organisation- och behörighetsinformation (metakatalog) som innefattar möjligheten att tillhandahålla en mer komplett bild av information som knyter an till elektroniska identiteter. Det tekniska gränssnittet innefattar ett standardiserat sätt att överföra information knuten till individerna, en lagringsplats för informationen måste naturligtvis finnas.

I dag finns några informationsobjekt resp. enskilda informationsattribut identifierade som potentiellt går att använda för att skapa en första generations tekniska gränssnitt.

Organisatorisk tillhörighet för studenter

Ett första steg att implementera är ett stöd för att kunna knyta organisatorisk tillhörighet till ett lärosätes studenter. I dagsläget finns ett standardiserat sätt inom SAML2 att uttrycka denna information genom attributet *eduPersonScopedAffiliation*. Hanteringen i sig är relativt enkelt då den enda förmedlade informationen är värdet "student@lärosäte.se" (till skillnad från "employee@lärosäte.se" för anställda resp. "member@lärosäte.se" samt "affiliate@lärosäte.se" för att representera övriga verksamma med närmare eller lösare koppling till lärosätet) där attributet redan idag är tänkt att kunna bära information om multipla organisatoriska tillhörigheter. Ett tekniskt gränssnitt skulle därmed behöva stödja nedan definierade flöden i syfte att hantera organisatorisk tillhörighet för ett lärosätes studenter. Ex. via anrop ifrån lärosätets integrationsplattform alternativt direkt från *Ladok* för de lärosäten som önskar så.

Knyt organisatorisk tillhörighet till identitet

Startpunkt för organisatorisk tillhörighet initieras lämpligen i samband med att studenten får aktiva kurs- och/eller programregistreringar på lärosätet. Startpunkten kan variera baserat på vilken nivå av registreringen som ligger till grund för den organisatoriska tillhörigheten men förväntat studiedeltagande är det vanligaste tolkningen bland landets lärosäten idag.

Ta bort organisatorisk tillhörighet från identitet

Det finns en hel del utmaningar med att avgöra när en student inte längre räknas som aktiv vid ett lärosäte och även att utläsa det baserat på den informationen som finns tillgänglig i *Ladok*. Grunden kan i många fall ligga i avsaknaden av aktiva registreringar följt av en ”karantänperiod”, t.ex. att organisatorisk tillhörighet ska tas bort två terminer efter sista aktiva kursregistrering. Utmaningar knutet till detta är framför allt att studenter ofta har planerade eller oplanerade studieuppehåll som kan påverka detta. Det är också vanligt att studenter läser en eller flera terminer vid annat lärosäte (vanligen utomlands) men ändå förväntas vara aktiv i vissa perspektiv vid sitt ursprungliga lärosäte och därför ha kvar en organisatorisk tillhörighet på sitt konto.

Livscykel för studentkonton

En implementerad livscykelhantering för studentkonton kommer att vara nödvändig för att säkerställa att ett lärosäte ska kunna lita på att samtliga studenter har tillgång till ett lärosätesanknutet konto. Därav följer att även nedan användningsfall behöver stödjas.

Skapa elektronisk identitet

I det fall en student ska knytas till ett lärosäte men saknar befintlig elektronisk identitet i *eduID* behöver en elektronisk identitet kunna skapas tillsammans med grundläggande personinformation knuten till den elektroniska identiteten. Studenten behöver därefter få tillgång till aktiveringsinformation för den elektroniska identiteten på ett säkert sätt.

Uppdatera personinformation knutet till identitet

Lärosätet behöver kunna ha tillgång till tekniska gränssnitt för att kunna uppdatera personinformationen knuten till en elektronisk identitet. För svenska medborgare tillgodoses delar av dessa behov av en informationsöverföring ifrån folkbokföringen. För mer lärosätesspecifik information resp. hantering av inresande studenter krävs en struktur där lärosätet tar ett tydligt ansvar för att säkerställa att personinformationen är korrekt under livslängden för den elektroniska identiteten.

Avsluta elektronisk identitet

Slutet för en elektronisk identitet behöver också säkerställas. Tydlighet behöver säkerställas för hur en elektronisk identitet är skapad. Huvudfallen definieras genom samtycke för lagring av personinformation baserat på att användaren på eget initiativ skapat en elektronisk identitet resp. genom allmänt intresse som grund för lagring av personinformation i fall det är på initiativ ifrån ett lärosäte som den elektroniska identiteten är skapad. I det sistnämnda fallet medför det att när studenten inte längre är

knuten till något lärosäte organisatoriskt (dvs. inte längre bedriver studier aktivt) bör den elektroniska identiteten inaktiveras efter lämplig karantänperiod. För att tillgodose behov där studenten vid ett senare tillfälle behöver återaktivera sin elektroniska identitet behöver mekanismer finnas för att säkerställa att det är rätt individ som gör det (t.ex. med hjälp av verifiering via Svensk e-legitimation eller motsvarande).

Något som kan övervägas som alternativ till avslut av en elektronisk identitet är att via samtycke från studenten fortsätta hantera den elektroniska identiteten. I det fallet skulle även en elektronisk identitet skapad av ett lärosäte kunna fortsätta vara aktiv utan aktiv anknytning till en organisatorisk tillhörighet. Det krävs dock vidare utredning för att avgöra om det är ett reellt alternativ.

Alumner

Ett specialfall av organisatorisk tillhörighet är behov av anknytning till organisatorisk tillhörighet som ”alumn@lärosäte.se”. För alumner krävs ett aktivt samtycke av personen för att kunna göra en organisatorisk anknytning men lärosäten som efterfrågar denna funktionalitet skulle kunna få tillgång till ett tekniskt gränssnitt för att initiera denna funktionalitet i samband med att lärosätet ta bort den organisatoriska knytningen ”student@lärosäte.se”. Vanligen innebär det t.ex. ett e-postutskick till studentens senast kända e-postadress där studenten uppmanas bekräfta fortsätt kontakt med sitt lärosäte.

Användarupplevelsen i ett lärosätesgemensamt IAM

Inom sektorn finns idag olika sätt att hantera personliga konton. De flesta lärosäten skapar olika konton för studenter och anställda. I de fall en person är både anställd och student skapas två olika konton knutna till samma person. Andra lärosäten har valt att istället alltid använda samma konto och skapar därför endast ett konto per individ även om personen är både anställd och student vid lärosätet.

Så som *eduID* fungerar idag skapas endast ett konto för en individ men däremot existerar egentligen idag inget rollbegrepp i *eduID*. Funktionaliteten i *eduID* måste därför utökas med funktionalitet för att hantera rollbegrepp, antingen genom att ett konto kan ha flera roller eller möjlighet för en individ att ha flera konton i *eduID*.

Om man har ett gemensamt nationellt konto ställer det antingen krav på att alla IT-tjänster *(Service Providers)* i federationen måste kunna ta emot en inloggning med flera roller/anknytningar, eller att inloggningstjänsten (IdP:n) ger användaren möjlighet att välja vilken roll/anknytning inloggningen avser, ex. som student eller som anställd på ett specifikt lärosäte och därmed filtrera bort alla ovidkommande roller/anknytningar för den aktuella inloggningen.

I inloggningsförfarandet finns även perspektivet att lärosäten har behovet av att komplettera ett nationellt konto med information ifrån en lokal källa, t ex för att underlätta ett stegvis införande av en gemensam lösning.

Sammantaget innebär detta att inloggningsprocessen blir mer komplex än i dagens lokala identitetshanterare och högre krav ställs på en gemensam hänvisningstjänst. En specifikation behöver tas fram dels för att detaljera hur användarupplevelsen bör se ut för att bli tydlig för hur användarna fortfarande förknippar sig vid sitt lärosäte och samtidigt guidas igenom de eventuella val av organisation och roller de behöver göra, dels behöver ett motsvarande tekniskt flöde tas fram som detaljerar hur IT-tjänster och identitetshanterare samverkar för att t ex signalera vilken funktionalitet aktuell IT-tjänst stödjer.

Ett förslag som exemplifierar användarupplevelsen finns med i Bilaga 1. Detta förslag illustrerar avancerad funktionalitet som är möjlig att åstadkomma inom ramen för nationellt samordnade IT-tjänster men som blir svårare att åstadkomma utanför landets gränser.
Projektets analys för att få en så enkel och smidig upplevelse för slutanvändaren är att det bör startas en utredning för att bygga ut SWAMID:s metadata enligt Bilaga 1 samt att utreda en utbyggnad av discoverytjänsten och eduID för att de ska läsa den.Långsiktiga förändringsmöjligheter

Gemensam tjänst för person-, organisations- och behörighetsinformation (metakatalog)

En målbild för IAM i sektorn är att skapa en nationell hantering av person-, organisations- och behörighetsinformation (metakatalog) som kan använda av samtliga lärosäten. Funktionaliteten bör i ett införande finnas tillgänglig på ett sätt så att lärosäten gradvis kan gå över till den gemensamma tjänsten. En nationell tjänst för person-, organisations- och behörighetsinformation (metakatalog) kan utgöra basen för en sektorgemensam identitets- och behörighetshantering.

Tjänsten bör i ett första skede innehålla information om identiteter, personer, organisationer och behörigheter, men även annan gemensam information kan på sikt bli aktuell. Tjänsten ska vara anpassad för att kunna hantera olika typ av information och relationer. Tjänsten måste därför baseras på en informationsmodell som inte låser en fast struktur utan ger möjlighet att successivt lägga på nya vyer. Tjänsten behöver ett användargränssnitt för att kunna anpassa innehållet för varje lärosäte där t.ex. definition av organisationen kan variera. Vidare behöver det även finnas stöd för

gemensam funktionalitet kopplat till rätten att bli glömd eller funktioner för registerutdrag (GDPR).

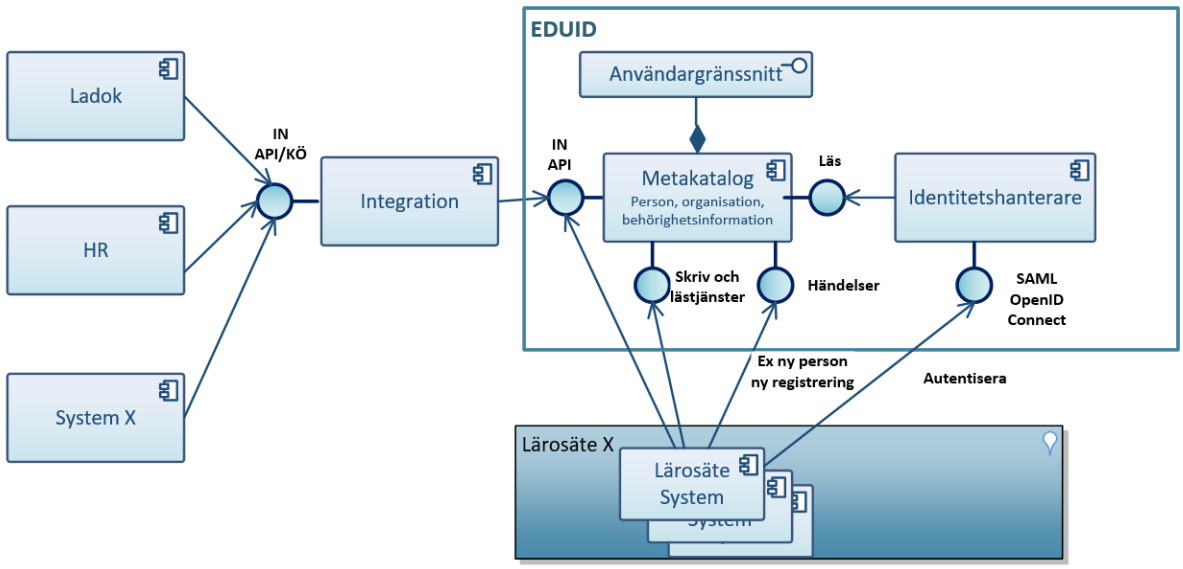
Det skall finnas tydliga och väl definierade tekniska gränssnitt för att skriva och läsa information. Tjänsten ska kunna signalera händelser genom ett tekniskt gränssnitt som andra system skall kunna ta emot. En lärosätesgemensam tjänst för person-, organisations- och behörighetsinformation (metakatalog) kräver gemensam integrationsfunktionalitet för att hämta information direkt från *Ladok* samt från de HR-system som används i sektorn. De tekniska gränssnitten skall kunna användas av andra system.

En nationell tjänst för person-, organisations- och behörighetsinformation (metakatalog) är en förutsättning för en gemensam identitets- och behörighetshantering i sektorn. Tjänsten kan ses som en vidareutveckling av tjänsten *eduID*.

Tidigare erfarenheter har visat att det finns goda möjligheter till att skapa gemensamma strukturer och tjänster istället för att varje lärosäte gör sin egen implementation. I all väsentlighet skiljer sig inte identitets- och behörighetshantering ur ett infrastrukturperspektiv särskilt mycket mellan olika lärosäten. Det betyder att det finns goda förutsättningar för en gemensam tjänst som kan minska sektorns totala kostnader för identitets- och behörighetshantering.

Ett lämpligt nästa steg är att starta ett utredningsprojekt som mer detaljerat kan göra en design för tjänsten och hur den bäst bör implementeras.

Ingående komponenter i en gemensam lösning



Figur 4 Övergripande vy av gemensamt person-, organisations- och behörighetsregister (metakatalog)

Begreppet *eduID* omfattar i Figur 4 en identitetshanterare samt ett register för person-, organisations- och behörighetsinformation (metakatalog) med ett tillhörande webbgränssnitt för administratörer samt självservice för användare.

I ett första steg skulle tjänsten omfatta studenter men kan på sikt även innehålla anställda på lärosäten. Tjänsten föds med information via gemensam systemintegration med *Ladok* och i ett senare skede även med de HR-system som används i sektorn. Exempel på uppgifter som tjänsten håller för en student är personuppgifter som personnummer, namn, adress samt vilket lärosäte och vilka program och kurser som studenten är antagen och registrerad på. Tjänsten erhåller ständigt uppdateringar från källsystemen.

Tekniska integrationsgränssnitt

Se även *Effektivare hantering av information knuten till* användare. Tjänsten innehåller väldefinierade tekniska gränssnitt för att skriva och läsa information ur tjänsten. Det behöver också vara möjligt att från källsystem etablera och uppdatera information. Tjänsten behöver ge ifrån sig händelser på vad som händer i tjänsten som kan konsumeras av t.ex. lokala system vid landets lärosäten. Alla tekniska gränssnitt bör så långt det är möjligt baseras på definierade standarder, ex. AMQP, SCIM.

Identitetshanteraren behöver kunna stödja – antingen direkt eller via sekundära identiteter - flera olika protokoll för autentisering, ex. SAML2 och OpenID Connect. Även applikationslösenorden kan ses som en sekundär identitet kopplat till användningen av RADIUS för autentisering av användare för bland annat *eduroam*.

Gemensam identitets- och behörighetshantering

En nationell tjänst ger en grund för en gemensam identitetshantering. Studenter och anställda skapar sin identitet i *eduID* och den elektroniska identiteten är sedan användbar i andra tjänster som används vid landets lärosäten. Det enskilda lärosätet skapar inte egna identiteter utan förlitar sig på den nationellt skapade identiteten. Behörigheter kan på ett automatiserat sätt skapas i tjänsten baserat på information från olika källsystem. Specifika behörigheter kan även sättas direkt via tjänstens grafiska gränssnitt.

Kraven på tillgänglighet för komponenter för sektorgemensam identitets- och behörighetshantering är höga då varje oplanerad otillgänglighet snabbt kommer att orsaka problem i hela sektorn. Tjänsten måste därför konstrueras för en väldigt hög tillgänglighet.

Gemensamma mönster för metakatalog

Det finns mönster för att beskriva hur en organisation kan beskrivas. Ett av de mest kända mönster är ”accountability pattern” som bl.a. Martin Fowler har beskrivit i artikeln: https://martinfowler.com/apsupp/accountability.pdf. Modellen beskriver en generalisering av organisationsstrukturen som beskriver alla ingående komponenter som parter och dess relationer till varandra. Dessa mönster kan vara till hjälp för att möjliggöra en generisk och flexibel modell för hur en organisation och dess relationer kan uttryckas. En utförligare beskrivning av mönstret går att finna som bilaga 2 till rapporten.

En identitet, specifik resurs

När en elektronisk identitet skall användas för både nationella och lärosätesspecifika tjänster ställer det högre krav på att det finns specifika behörigheter definierade. Det kommer att krävas vidare utredning för hur den gemensamma identiteten skall kunna samexistera i både ett lokalt och ett nationellt perspektiv. Idag erbjuder *eduID* möjligheten att en individ kan koppla flera elektroniska identiteter till sin person, vilket också öppnar för att samla även lokala elektroniska identiteter i *eduID*. På så sätt skulle det förenkla lösenordshantering åtminstone för en student, som då har lösenorden på samma ställe för de olika elektroniska identiteter.

Successivt genomförande
Införandet av en gemensam tjänst för person-, organisations- och behörighetsinformation (metakatalog) vilken kan utgöra grund för en gemensam identitets- och behörighetshantering i sektorn måste i hög grad vara flexibel för att tillåta ett succesivt införande. Lärosäten behöver i en övergångsperiod kunna använda delar av den nationella tjänsten parallellt med den lokala. Genom tydliga tekniska gränssnitt och uppdelning i olika komponenter skall olika delar av lösningen kunna användas utan att ett specifikt lärosäte initialt behöver använda tjänsten fullt ut. T.ex. så skulle den gemensamma tjänsten för person-, organisation- och behörighetsinformation(metakatalog) kunna användas utan att den gemensamma komponenten *identitetshanterare* används. *eduID* skulle kunna användas för studenter medan anställda fortfarande hanteras av lärososätet genom lokala elektroniska identiteter. Nyckeln till en lyckad tjänst är att den är flexibel och kan ge möjlighet till ett succesivt införande.

Slutsatser

Det är viktigt att arbetet med att nå målbilden med en lärosätesgemensam IAM lösning genomsyras av ett inkrementellt arbetssätt. Arbetet bör delas upp i tydliga delmål där varje delmål ska skapa nytta i sektorn för de enskilda lärosätena. Det skall därför vara möjligt för lärosäten att använda delar av den framtagna lösningen och kombinera det med lokal infrastruktur. Det är därför viktigt att lösningen byggs med tydliga tekniska gränssnitt baserat på öppna standarder så långt det är möjligt.

Rekommendation

Projektets rekommendation är att utöka *eduID* inkrementellt till att på sikt omfatta den funktionalitet som krävs för en fullskalig lärosätesgemensam hantering av IAM. Sätt målet att alla lärosäten använder *eduID* som enda inloggningstjänst, person- och organisationsregister och underlag för behörighetshantering (metakatalog).

Sammanfattningsvis rekommenderas följande åtgärder:
Kortsiktigt
- Förändra eduroam-infrastruktur
- Komplettera eduID med AD-funktionalitet
- Implementera ett gemensamt register för studenter (person- och organisationsregister och underlag för behörighetshantering)

Långsiktigt
- Inkludera personal och andra kategorier än studenter i det gemensamma registret
- Komplettera det gemensamma registret med övrig saknad funktionalitet

Fortsatt arbete

Det kommer behöva bedrivas en behovsfångst för att kunna utveckla en tjänst som löser flera av knutarna som rapporten ovan har redovisat. En av de största utmaningarna blir att hitta en lösning som erbjuder möjligheten att kunna använda olika komponenter i en succesiv process mot att mer och mer använda de gemensamma komponenterna, men samtidigt ha lokal infrastruktur som fungerar tillsammans med den gemensamma lösningen.

Det rimliga blir att som tidigare sagts börja med exempelvis gemensam lösenordshantering och processerna runt provisionering av konton. Här bör det gå att använda tidigare lösningar från exempel SE-leg. Ett gemensamt sätt att erbjuda säkra lösenordbyten skulle kunna vara en del av en sådan lösning.

Ett arbete borde omgående initieras för att analysera hur en gemensam behörighetshanterare baserad på en person- och organisationskatalog (metakatalog) skulle kunna realiseras.

Kommande steg kan vara:

- SUNET/eduID tar fram ett kostnadsförslag
- Finansieringsmodell tas fram gemensamt av ITCF och SUNET/eduID
- ITCF formulerar en beställning till eduID

Bilaga 1. Exempel på användarupplevelse i en gemensam identitetshanteringstjänst

Branding och Användarupplevelse

Projektets vision är att alla lärosäten använder *eduID* som enda inloggningstjänst (IdP). Naturligtvis kommer det inte ske från en dag till en annan. Vi får anta att en del lärosäten har lättare att genomgå en transformation än andra och att det kommer ske i olika omgångar för studenter och anställda. Man kan också tänka sig att en del lärosäten väljer att införa inloggning via *eduID* endast för vissa tjänster.

Hur ska då inloggningsupplevelsen se ut? Från federativa inloggningar via SWAMID är användare vana vid att välja lärosäte i en lång lista (discoverytjänsten) för att sedan slussas till lärosätets inloggningstjänst (IdP). En fråga som bör ställas är om det är önskvärt att göra så även efter övergång till *eduID* eller om användarna ska välja *eduID* i listan? Nedan listas några för- och nackdelar med att behålla förfarandet då användaren väljer det lokala lärosätet, men blir skickad till *eduID* för autentisering till, antingen specifika tjänster eller för alla tjänster. Fördelar kan ses i att:

- användaren känner till sitt lärosäte och är van vid att söka upp och välja det,
- lärosätet står i fokus och behåller till viss del sitt varumärke i inloggningsupplevelsen,
- det fungerar likadant för alla tjänster samt att
- lärosätet kan välja om *eduID* ska användas för en viss tjänst eller inte. Lärosätet kan också ändra detta i efterhand utan att lära om alla användare.

Identifierade nackdelar är att:

- det kan kännas som fishing om man blir skickad till en helt annan inloggningstjänst (IdP) när man väljer inloggning via lärosätet.

Nackdelen kan dock göras mindre märkbar genom att direkt vid val av lärosäte tydliggöra att inloggningen kommer ske med *eduID* och inte med en lärosätesspecifik inloggningstjänst (IdP). Exempel på hur det skulle kunna se ut:

Nedan identifieras några för- och nackdelar med att välja eduID i listan med inloggningstjänster (discoverylistan), antingen för specifika tjänster eller för alla

tjänster. Fördelarna är att:

- varumärket *eduID* stärks samt att
- användaren får en större förståelse att det är skillnad mellan olika konton.

Två nackdelar har identifierats i att:

- användaren måste veta i vilka fall *eduID* ska väljas och i vilka fall det lokala lärosätets IdP ska väljas samt att
- lärosätet inte står i fokus.

Det finns sannolikt fler för- och nackdelar för de olika scenarierna. I ett införandeprojekt bör en djupare analys göras.

Utveckling av discovery-tjänsten

En möjlighet är att utveckla discoverytjänsten och genom detta kunna använda den för att konfigurera tjänster (SP:s) olika för olika lärosäten. Då kan varje lärosäte bestämma vilken inloggningstjänst (IdP) som ska användas i olika scenarier. Konfigureringen skulle kunna göras på flera nivåer enligt:

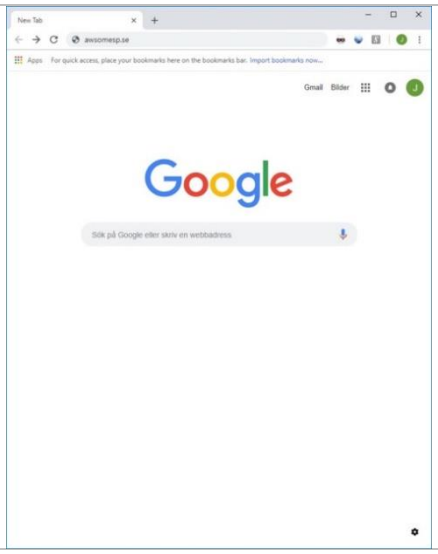
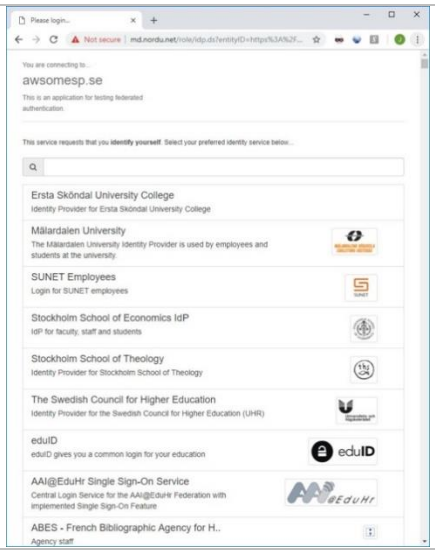
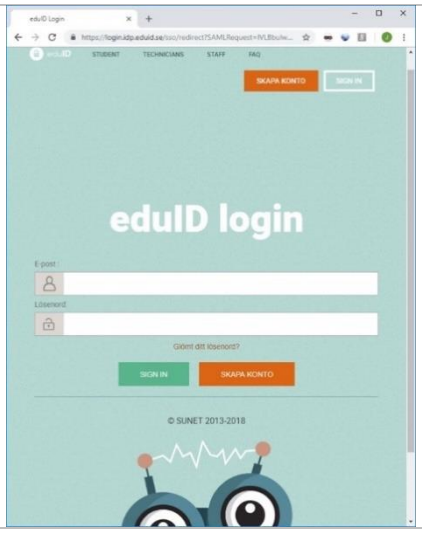
- Lärosätet väljer för *en viss tjänst (Service Provider)* eller *vissa tjänster (Service Providers)* att alla med en roll (ex. student) alltid ska logga in med *eduID*. Både lärosätets inloggningstjänst (IdP) och *eduID* kommer att användas beroende vilken *tjänst (Service Provider)* som användaren avser använda.
- Lärosätet väljer att *en viss roll* (ex student) alltid ska logga in med eduID för *alla tjänster (Service Providers)*. Inga lokala konton kommer användas för den specifika rollen.
- Lärosätet väljer att *alla* ska logga in med *eduID* för alla *tjänster (Service Providers)*. Inga lokala konton kommer i det här fallet att användas.

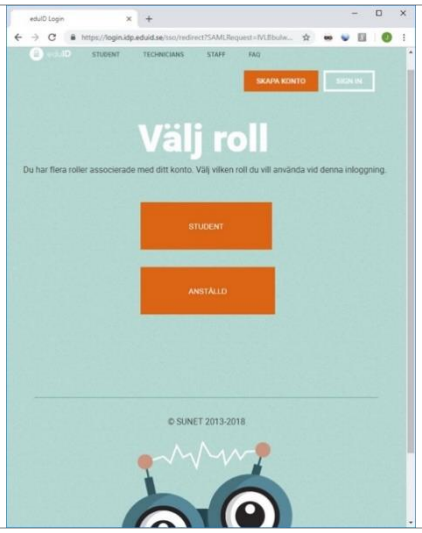
Inloggningsupplevelse

Avsnittet avser beskriva hur inloggningsupplevelsen kan vara för en student/anställd som vill nyttja en *tjänst (Service Provider)* via *eduID* (IdP).

Förutsättningarna i nedan beskrivet scenario är att personen som loggar in är både student och anställd på flera lärosäten samtidigt och att *tjänsten (Service Providern)* inte stödjer det. En annan förutsättning är att *eduID* har utvecklats så det innehåller anknytningsinformation för minst de lärosäten som avses samt har nya sidor för att välja lärosäte och roll.

Beskrivet scenario utgår från det mest komplicerade fallet och visar hur det kan hanteras genom i så få steg (1-5) som möjligt.

	➔	
1. Användaren går till en *tjänst (Service Provider)*		2. Om användaren inte är inloggad skickas man till discoverytjänsten för att välja inloggningstjänst (IdP) eller lärosäte
	➔	
3. Användaren hamnar på *eduID*:s inloggningssida och loggar in		4. Användaren får välja vilket lärosäte som inloggningen avser

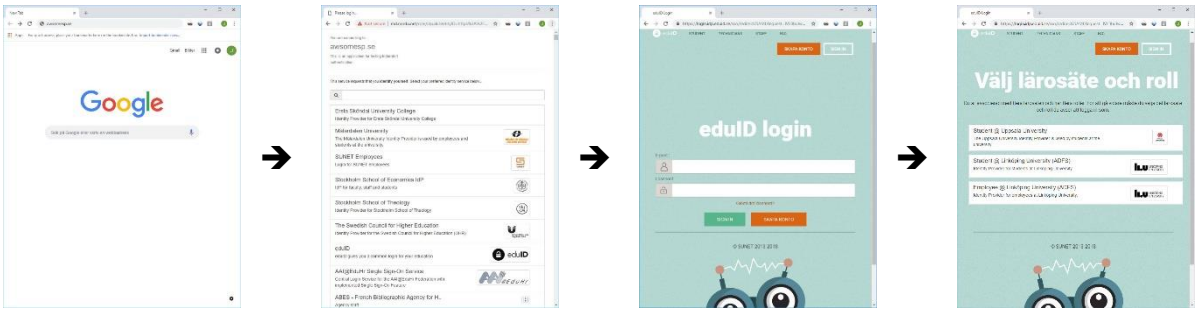
		
5. Användaren får välja vilken roll som inloggningen avser		

Åtgärder

Åtgärderna nedan kan införas separat eller tillsammans. Vissa åtgärder gäller generellt för alla *tjänster (Service Providers)* och en del är tjänstespecifika.

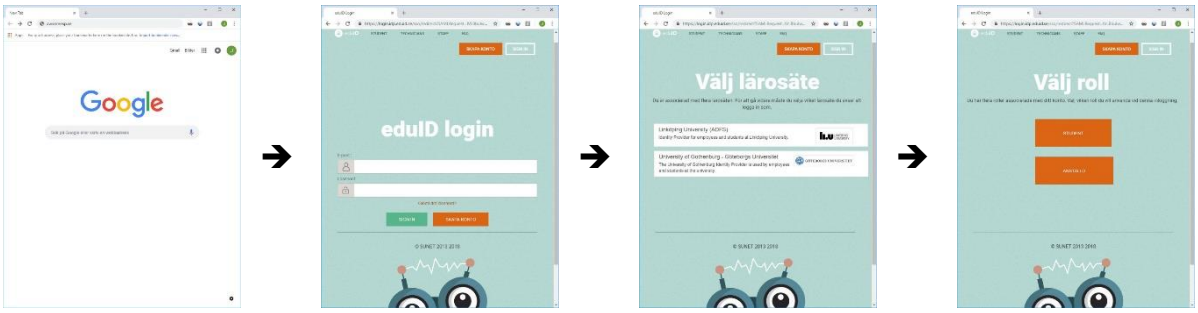
Lärosäten och roller på en sida

Vi kan anta att den sammanlagda listan på lärosäten och roller för en person har inte är så lång. I så fall kan steg 4 och steg 5 konsolideras, se exempel nedan:

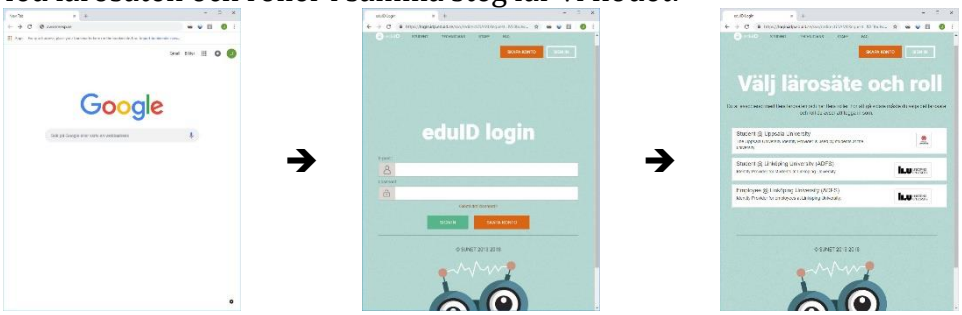


Konfigurera tjänst för endast eduID

Om en *tjänst (Service Provider)* endast använder *eduID* och har möjlighet att konfigureras för det behövs inte steg 2. Tjänsten konfigureras då direkt mot *eduID* och inte mot discoverytjänsten.

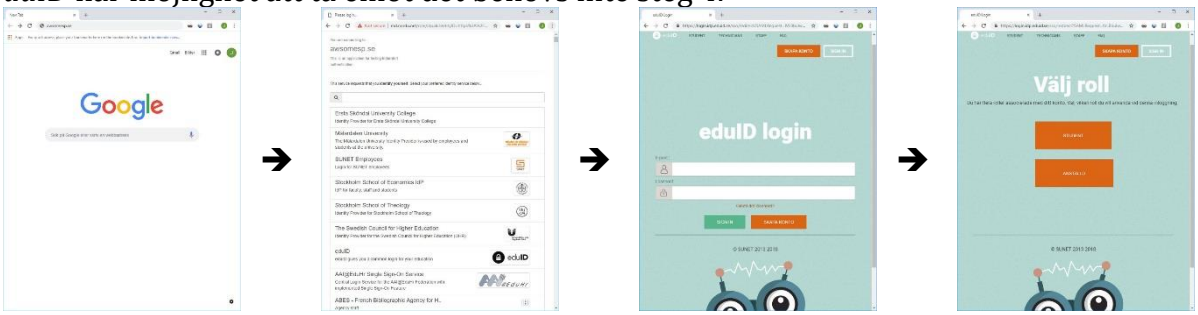


Med lärosäten och roller i samma steg får vi flödet:

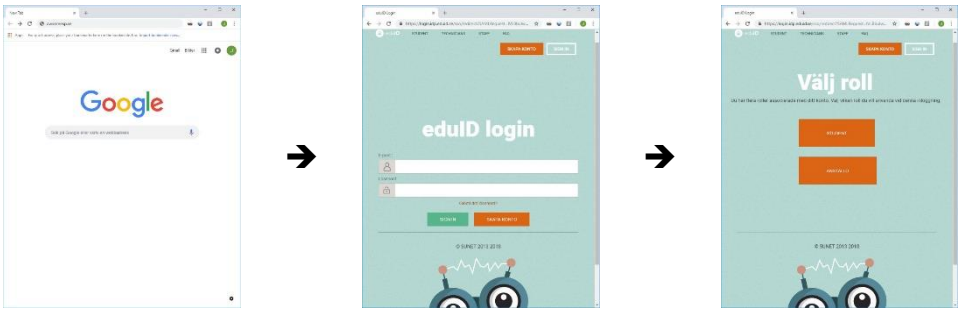


Lokal tjänst

Om en *tjänst (Service Provider)* har möjligheten att skicka med vilket lärosäte som avses användas (det kan till exempel vara en tjänst som är byggd för ett visst lärosäte) och *eduID* har möjlighet att ta emot det behövs inte steg 4.

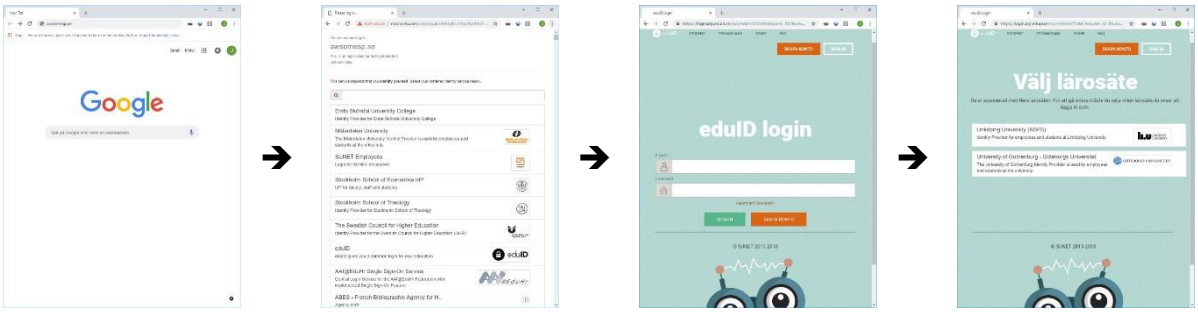


Tillsammans med att konfigurera den att gå direkt mot *eduID*:

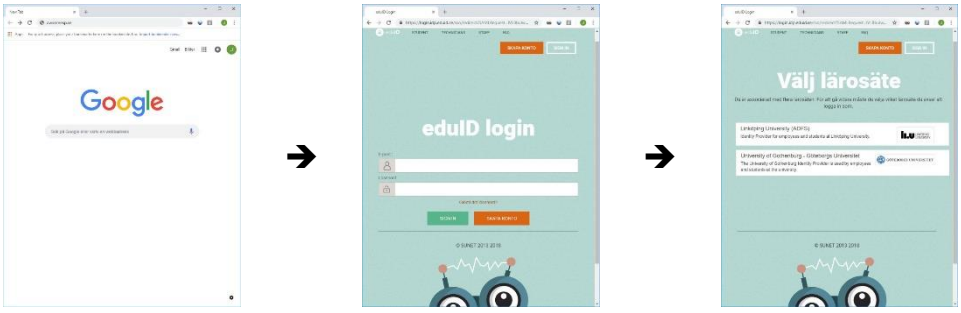


Lokal tjänst avsedd för endast en roll

Om en *tjänst (Service Provider)* har möjlighet att skicka med vilken roll som avses användas (det kan till exempel vara en tjänst som är byggd endast för anställda) och *eduID* har möjlighet att ta emot det behövs inte steg 5.

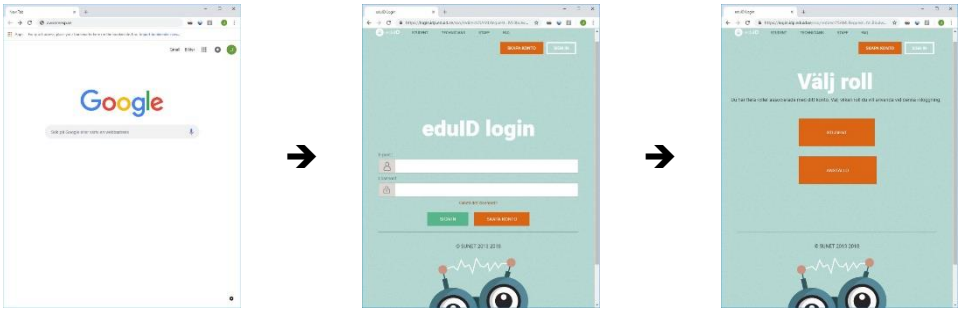


Tillsammans med att konfigurera den att gå direkt mot *eduID*:



Lokal tjänst konfigurerad i discoverytjänsten

Om en *tjänst (Service Provider)* endast är till för ett specifikt lärosäte och det är konfigurerat i discoverytjänsten enligt tidigare diskussion kommer inte frågan om vilket lärosäte som avses att behöva ett svar. Användaren dirigeras vidare och steg 2 behövs inte. Om informationen kan skickas vidare till *eduID* behövs inte heller steg 4.



Tjänst för endast en roll

Om en *tjänst (Service Provider)* endast är ämnad för en specifik roll (till exempel HR-system/ekonomisystem för anställda) och det är konfigurerat i discoverytjänsten enligt tidigare beskrivningar behöver discoverytjänsten inte fråga vilken roll som avses. Om informationen kan skickas vidare till *eduID* behövs inte heller steg 5.

Ett aktuellt exempel är Nais, där flera lärosäten väljer att använda *eduID* för inloggning med personverifierad MFA. Inloggningen är endast för anställda.

Branding

Discoverytjänsten kan designas så att ett lärosäte kan konfigurera, om och när, *eduID* ska användas som inloggningstjänst (IdP). I listan där man väljer lärosätet kan det visa att *eduID* används istället för lärosätets egen inloggningstjänst (IdP):

Utökning av SWAMID:s metadata

I stället för att kräva att en *tjänst (Service Provider)*, eller discoverytjänsten, ska skicka med information till *eduID* om vilket lärosäte och/eller roll som hanteras kan SWAMID:s metadata utökas till att inkludera även den informationen. En sådan utökning kan då läsas både av discoverytjänsten och av *eduID*.

I fallet då discoverytjänsten läser informationen kan det användas för att minska listan med giltiga inloggningstjänster (IdP:er), steg 2, eller helt skippa valet av inloggningstjänst i de fall där enbart en inloggningstjänst (IdP) och roll är giltig.

Om eduID kan läsa informationen kan den användas ~~för att~~ på samma sätt som för discoverytjänsten men för steg 4 och steg 5. Genom att använda SWAMID:s metadata behöver ingen information skickas till eduID från vare sig tjänst (Service Provider) eller discoverytjänst gällande vilka lärosäten eller roller som kan användas. Informationen kan även användas för att auktorisera användaren efter inloggning, dvs. om användaren inte tillhör ett giltigt lärosäte eller har en giltig roll så kommer användaren inte skickas vidare.

Utökningen skulle kunna göras genom ett nytt XML-element som innehåller en eller flera attribut. Se exemplet nedan.

Konfigurera tjänst (Service Provider) att endast gälla för en eller flera inloggningstjänster (IdP:er)

Pseudokonfiguration:

```
<SPExtendedConfiguration>
  <IdPConfiguration entityID="https://weblogin.uu.se/idp/shibboleth" />
  <IdPConfiguration
entityID="http://adfs.umu.se/adfs/services/trust">student</IdPConfiguration>
</SPExtendedConfiguration>
```

Ovan konfigurationsexempel betyder att *tjänsten (Service Provider)* endast godtar inloggningar från UU och UmU och att endast studenter kan logga in från UmU.

Discoverytjänsten visar en lista med UU och UmU i steg 2. I det fall då discoverytjänsten delar upp listan baserat på roll innehåller den student@uu.se, employee@uu.se och student@umu.se.

eduID måste då anpassa steg 4 och steg 5. Om användaren endast tillhör ett av angivna lärosäten visas inte steg 4 alls. Om användaren endast är student på UmU visas varken steg 4 eller 5.

Om användaren inte tillhör UU eller inte är student på UmU lämnar *eduID* ett felmeddelande och skickar inte användaren vidare till *tjänsten (Service Providern)*. Som ett alternativ kan användaren skickas tillbaka med information om nekad åtkomst.

Konfigurera tjänst (Service Provider) som kan hantera flera inloggningstjänster (IdP:er)

Om en *tjänst (Service Provider)* kan hantera att till exempel studenter kommer från flera lärosäten skulle det kunna konfigureras enligt följande exempel:

```
<SPExtendedConfiguration>
  <IdPConfiguration entityID="*">student</IdPConfiguration>
</SPExtendedConfiguration>
```

Konfigurera tjänst (Service Provider) som kan hantera flera inloggningstjänster (IdP:er) och roller

Om en *tjänst (Service Provider)* kan hantera att en användare har flera roller på flera lärosäten skulle det kunna konfigureras enligt följande exempel:

```
<SPExtendedConfiguration>
  <IdPConfiguration entityID="*" />
</SPExtendedConfiguration>
```

Proxy-IdP

Om ett lärosäte har en Proxy-IdP som använder *eduID* som inloggningstjänst (IdP) och skickar med information om vilket lärosäte som gör anropet behöver användaren varken gå igenom steg 2 eller steg 4.

Om Proxy-IdP:n kan skilja på roll, baserat på *eduID* inloggningen, kan Proxy-IdP:n även förmedla att den anropande *tjänsten (Service Providern)* kan hantera flera roller. I det fallet behövs inte heller steg 5.

I exemplet med Proxy-IdP behöver lärosätet spara en koppling mellan *eduID* eppn och id på det lokala kontot. ~~Alternativt kan det kopplas via personnummer.~~

Bilaga 2. Mönster för metakataloger

En part kan typiskt vara

- organisatorisk enhet,
- student,

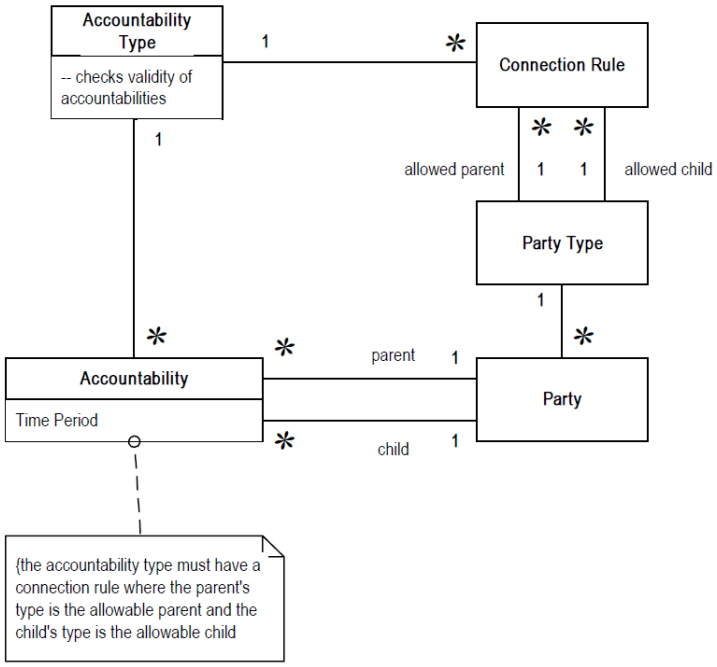
- anställd,
- person,
- roll,
- centrum,
- projekt,
- avtal,
- befattning,
- position,
- kurs,
- program,
- kurstillfälle,
- programtillfälle,
- etc.

Dvs. de objekt som brukar tas fram inom ramen för en informationsmodellering.

Den andra komponenten är relationer och dessa brukar typiskt vara

- linjeorganisation,
- projektägarskap,
- projektmedlem,
- centrumägare,
- anställd på,
- registrering,
- etc.

”Accountability pattern” är i sin helhet beskriven i Figur 5.



Figur 5 "Accountability pattern" beskriven som en graf

Figur 5 visar ett klassdiagram för en riktad graf. Anledningen att den är riktad är för att det alltid kommer finnas en toppnod som grafen utgår från. I en organisationsstruktur blir det typiskt den högsta lämpliga noden för att beskriva sin organisation. För ett lärosäte är det troligtvis lärosätet själv och i en gemensam nationell metadatalog blir det troligtvis Sverige.

I klassdiagrammet finns även ”Connection Rules”, vilket beskriver vilka tillåtna relationer parterna kan ha. Detta blir generella regler som det i linjerelationen får finnas organisatoriska enheter ovanför och under. För en anställning kan det endast finnas organisatoriska enheter ovanför. Att beskriva hur många anställningar en anställd har måste uttryckas i applikationslagret – modellen säger bara att det kan finnas en eller många anställningar.

Ett första steg blir att utvärdera vilken databastyp som är bäst lämpad både för att beskriva grunddata men också hur databasen bäst stödjer applikationslogik. Valet bör stå mellan:

- Traditionell relationsdatabas
- Grafdatabas
- Multi-model (Hybrid)

Behovet som bör styra är flexibilitet och prestanda. Det kommer finnas behov av att kunna uttrycka strukturen som olika versioner av strukturen.