Slutrapport
Nationellt IAM-projekt

Sammanfattning

IAM är ett viktigt begrepp inom en organisations verksamhet. IAM betyder *"Identity and Access Management"* (på svenska identitets- och behörighetshantering). Kortfattat är detta område processerna och den tillhörande tekniska infrastrukturen som hanterar elektroniska identiteter tillhörande organisationen resp. vilka IT-tjänster dessa elektroniska identiteter får teknisk tillgång till och vilka systemrättigheter identiteterna har inom resp. IT-tjänst.

Projektet har genomfört ett arbete som definierar betydelsen av IAM för sektorn högre utbildning i Sverige. På så sätt har arbetet skapat viktiga förutsättningar för att konkretisera såväl gemensamma krav på lärosätenas lokala processer resp. lokala tekniska infrastruktur som gemensamma krav på en gemensam nationell infrastruktur.

Projektet har identifierat sex ingående processer inom området IAM för högre utbildning i Sverige

- Skapa elektronisk identitet
- Verifiera elektronisk identitet
- Avsluta elektronisk identitet
- Automatisk tilldelning av behörighet till IT-tjänst
- Attestbaserad tilldelning av behörighet till IT-tjänst
- Återkallande av behörighet till IT-tjänst

Projektet har vidare identifierat fyra logiska komponenter inom området IAM för högre utbildning i Sverige

- Identitetshanterare
- Behörighetshanterare
- Personregister
- Organisationsregister

Projektets rekommendation är att ett fortsätt arbete i syfte att konkretisera krav och behov kopplade till både processer och de logiska komponenterna baserade på ett modulärt uppbyggd koncept. Konceptet inkluderar tydliga gränsytor mellan ingående tekniska komponenter så att de kan finnas en nationell gemensam bas-tjänst som går att kombinera med lokala tekniska komponenter för de lärosäten som har komplexa krav. Projektet ser också att nästa steg är att ta fram ett beslutsunderlag som innehåller tydliga kostnadsuppskattningar för vad ett sådant koncept skulle innebära.

Bakgrund

Hantering av elektroniska identiteter och behörigheter är centralt vid alla lärosäten. Hanteringen har växt fram i olika takt vid olika lärosäten. I takt med att kraven på lärosäten ökat, framför allt gällande kostnadseffektivitet och möjlighet att använda externa IT-tjänster ökar behoven om samsyn kring frågor om identitetshantering inom sektorn.

Inom samarbetsorganet ATI har behov att inventera och göra en gemensam kravställning på hur IAM ska kunna komma att hanteras i ett framtidsperspektiv identifierats. Projektet har genomförts på uppdrag av SUNET Inkubator.

Utgångspunkt

Tre olika paradigm för IAM inom högre utbildning är identifierade och definierade av Gartner vilka beskriver helt skilda mönster för hur IAM hanteras vid ett lärosäte. Nedan beskrivs mönstren mycket övergripande.

- *Organisationscentrisk*
  Den organisationscentriska IAM-hanteringen innebär en IAM-hantering där organisationen står helt fristående och där organisationen själv äger hela processen för att länka e-identiteter samman med aktörer och de attribut som kopplas till e-identiteten.

  Hela förtroendekedjan mellan konsumerande tjänster och tilldelandet av rättigheterna finns inom organisationen. Ett typexempel på denna hantering är den traditionella knytningen där man sköter autentisering och auktorisation för en IT-tjänst genom att ansluta den till ett Active Directory och hantera användarna av IT-tjänsten genom säkerhetsgrupper.

- *Federationscentrisk*
  Den federationscentriska IAM-hanteringen handlar om att världen breddas och att e-identiteterna inte bara hanteras inom en organisation. Det innebär att det måste finnas ett förtroende mellan de olika ingående organisationerna i federationen. Att en organisation litar på tilldelningen av rättigheter som kommer med den hävdade rätten.

  Det är i SWAMID som vi har grunden till den federationscentriska IAM-hanteringen. Det saknas idag samsyn för hur behörighetsstyrning fungerar inom resp lärosäte och vilka krav som är rimliga att ställa där. Några basprocesser finns definierade inom ramen för SWAMIDs tillitsramverk men fokus för federationen är återanvändning av elektroniska identiteter för inloggning. Typexempel på detta område är de IT-tjänster som används genom olika former av nationella samarbeten, t ex Adobe Connect, Box och kommande version av Ladok (Ladok3). Antagning.se och NyA-webben är också exempel inom området

där vissa delar av NyA-webben även har behörighetsstyrning på detta sätt.

- *Användarcentrisk*
  När e-identiteten sätts i fokus och rättigheter inte längre tilldelas vid den enskilda organisation där e-identiteten ursprungligen hör hemma får vi ett användarcentriskt perspektiv. Tilldelningen flyttas ut ur organisationen till den sammanslutning där organisationen finns.

  För användarcentrisk IAM-hantering finns idag ingenting inom lärosätessverige även om SWAMID utgör en stark utgångspunkt. Som privatperson kommer man i kontakt med denna paradigm t ex genom konceptet att man använda ett Facebook-konto för inloggning i många IT-tjänster. I detta exempel saknas dock behörighetshanteringen.

  I dagsläget har de flesta lärosätena tekniska lösningar där fokus varit organisationscentriskt. Några få lärosäten har genomfört förändringar där de tekniska lösningarna på ett tydligare sätt har vävt in identitetsfederationer som en naturlig del av den tekniska lösningen.

Arbetsgång i projektet

Projektarbetet är genomfört av Markus Jardemalm (Uppsala universitet), Ola Ljungkrona (Göteborgs universitet), Eskil Swahn (Lunds universitet) samt Per Hörnblad (Umeå universitet). Gruppen har träffats för gemensamt arbete fyra gånger samt genomfört regelbundna arbets- och avstämningsmöten varannan vecka.

Referensgruppen har innefattat Daniel Blomberg (Mälardalens högskola), Fredrik Jönsson (Kungliga tekniska högskolan), Johan Peterson (Linköpings universitet), Mats Törnblom (Stockholms universitet) och Leif Lagebrand (Blekinge tekniska högskolan). Referens- och arbetsgrupp har träffats separat vid ett tillfälle samt vid IT-arkitetsforumet ATI vid två tillfällen.

Styrgruppen har utgjorts av Valter Nordh (SUNET), Stefan Edholm (Sveriges Lantbruksuniversitet), Fredrik Nilsson (Riksidrottsuniversitetet), Johan Nordgren (Blekinge Tekniska Högskola), Ann Öhrn (Örebro universitet) samt som reserv Otto Ramirez (Försvarshögskolan). Styrgruppen har sammanträtt fyra gånger under projektarbetets gång.

IAM

Hur gemensam är kravbilden?

Identitets- och behörighetshantering är en kärnfunktion inom IT-infrastrukturen vid respektive lärosäte i Sverige. En följd av detta är att levererad funktionalitet behöver stödja verksamheten på ett väldigt tydligt sätt. Det är dock inte kartlagt hur överensstämmande krav och behov är *mellan* olika lärosäten är.

Några faktorer som påverkar är t ex

- Antal anställda, studenter resp. övriga verksamma
- Antal inresande studenter resp. internationella forskare
- Forskningsintensivt kontra utbildningsintensivt lärosäte
- Används federativ inloggning som primär autentisering även för IT-tjänster inom lärosätet fokuseras federativ inloggning primärt för att nyttja nationella/internationella IT-tjänster (t ex Sunet Box, Adobe Connect och eduroam)
- Behov av autentisering för lokala IT-tjänster som ej kommer att stödja federativ inloggning inom överskådlig framtid (t ex datorer i lokala datorsalar, utskriftslösningar resp. passagesystem)
- Mognadsgrad hos lärosätet vad gäller informationsmodell kopplad till identitets- och behörighetshanteringen (dvs hur mycket information finns idag lagrad om användarna resp. deras organisatoriska tillhörighet inom lärosätet)

För fortsatt arbete inom området krävs att det tydliggörs hur stor samsyn det finns inom området. Ett arbete som i praktiken måste innebära att samtliga lärosäten förmedlar (eller åtminstone bekräftar) vilka krav och behov de ser det som rimligt att tillgodoses genom gemensamma tjänster. De behöver också bedöma vilka lokala tjänster som måste kunna integreras inom samma koncept. Denna rapport möjliggör det fortsatta arbetet genom att ha definierat en vilka begrepp, processer och logiska komponenter som ingår inom ramen för IAM.

Övergripande processer

Inom ramen för IAM finns ett antal stödprocesser till organisationen. Fokus för dessa processer är att säkerställa att livscykelhanteringen för elektroniska identiteter stödjer organisationens behov. Projektet har identifierat sex övergripande processer som tillsammans beskriver livscykeln för elektroniska identiteter vilka finns dokumenterade på en översiktlig nivå. För att kunna definiera resp. process vid ett lärosäte krävs dessutom en kategorisering av användare. Vid de flesta lärosäten finns åtminstone tre huvudkategorier av användare; anställda, studenter samt övriga verksamma. En mer finkornig indelning kan behövas, exempelvis enligt följande:

- Anställda
- Studenter
- Studenter ifrån andra lärosäten
- Forskarstuderande
- Gästforskare/gästföreläsare
- Timavlönade
- Industridoktorander
- Konferensdeltagare
- Extern person
- Konsulter
- Servicepersonal
- Vaktbolag

Huvudorsaken till en kategorisering av användare är framför allt att en mer finkornig indelning av användare påverkar processerna för att inleda resp. avsluta elektroniska identiteter.

Det som driver komplexiteten inom lärosätessektorn är dels att det finns betydligt fler olika typer av relationer mellan personer och lärosätet än det finns inom en hel del andra sektorer, dels att omsättningen av personer som ska hanteras inom lärosätets IAM vida överskrider andra sektorer.

Skapa elektronisk identitet

Processen *Skapa elektronisk identitet* innefattar skapandet av en elektronisk identitet. Vanligen sker det antingen genom direktkontakt mellan administratör på lärosätet och användaren alternativt genom s.k. identitetsväxling där användaren skapar ett konto knutet till lärosätet genom att bevisa innehav av ett konto som tillhörande en pålitlig utgivare. Exempel på pålitlig utgivare för aktivering av studentkonton kan t.ex. vara annat lärosäte inom identitetsfederationen SWAMID eller UHR.

Verifiera identitet

Processen *Verifiera identitet* innefattar verifiering av identiteten hos en kontoinnehavare genom uppvisande av godkända identitetshandlingar (t ex nationellt ID-kort, körkort eller pass) alternativt genom att bevisa innehavet av ett annan verifierad elektronisk identitet inom SWAMID (dvs ett konto som uppfyller SWAMID AL2). I dag finns tillitsprofiler framtagna inom SWAMID som innehåller riktlinjer på hur denna process ska implementeras för att uppfylla tillitsprofilerna.

Avsluta elektronisk identitet

Processen *Avsluta elektronisk identitet* innefattar hur man avslutar en elektronisk identitet och vad som bör ske då. Idag saknas ofta tydlig hantering av vad som händer i de IT-tjänster användaren nyttjat under kontots livscykel. Vikten av en tydlig hantering kommer att få ytterligare fokus genom nya Dataskyddsförordningen.

Automatisk tilldelning av behörighet till IT-tjänst

Processen *Automatisk tilldelning av behörighet i IT-tjänst* innefattar hur en organisation tilldelar behörigheter till IT-tjänster baserat på förutbestämda regelverk. Vanliga exempel på detta är att tilldela behörighet till samarbetsytor inom ett LMS till samtliga studenter som läser en specifik kurs eller ge grundläggande passagerättigheter till samtliga anställda, studenter och övriga verksamma till de byggnader/korridorer/grupprum som är relevanta för dem.

Attestbaserad behörighetstilldelning till IT-tjänst

Processen *Attestbaserad behörighetstilldelning i IT-tjänst* innefattar flödet för att tilldela användare behörighet till en IT-tjänst där ett förutbestämt regelverk inte är möjligt att definiera och där lärosätets delegationsordning specificerar vem som ska godkänna detta. Vanligen innefattar denna typ av behörighetstilldelning ett flöde där en enskild användare ansöker om en behörighet och användares chef godkänner eller nekar behörigheten. Flödet kan även innefatta ett godkännande steg av systemförvaltaren för IT-tjänsten som t. ex. ställer krav på att användaren ska ha genomgått internutbildning och därmed ha nödvändig kompetens för att arbeta som användare i IT-tjänsten.

Återkallande av behörighet till IT-tjänst

Processen *Återkallande av behörighet* innefattar flödet för att säkerställa att behörigheter kan återkallas ifrån användare, vanligen p.g.a. förändrade arbetsuppgifter, förändrad organisatorisk placering eller att relationen mellan organisationen och personen inte längre finns.

Generellt om verksamhetsprocesser kopplade till IAM

Identitets- och behörighetshantering är i praktiken framtagande och fastställande av hur dessa processer ska implementeras i ett verktygsstöd. Ju mer överensstämmande implementationen av processerna är mellan lärosätena desto enklare är det att ha ett gemensamt verktygsstöd på nationell nivå som stöttar processerna. Ju mer implementationen av processerna skiljer mellan lärosätena desto större blir behov att ett nationellt koncept innebär frikopplade moduler där respektive modul kan

implementeras lokalt och därigenom hela eller delar av en process kan skilja mellan lärosätena.

Fortsatt arbete behöver fokusera djupare på att ta fram eller få tillgång till ett antal dokumenterade implementationer av dessa processer ifrån olika lärosäten för att säkerställa hur mycket detta område skiljer mellan lärosätena.

Övergripande beskrivning av funktioner

Identity and Access management (IAM) definieras i en fri översättning till identitets- och behörighetshantering. Hanteringen och behovet av funktionellt IT-stöd är komplext med många ingående komponenter som ofta, baserat på implementation och vilken mjukvara implementationen är baserad på, grupperas till en enda enhet, IAM. I en omvärldsanalys av sektorn för högre utbildning har det visat sig att begreppet IAM har olika betydelse för olika lärosäten:

- IAM som *Identity Management (IdM)* dvs. enbart en hantering av elektroniska identiteter i syfte att möjliggöra kontroll av en IT-användares elektroniska identitet (autensiering)
- IAM som inkluderar både autentisering och behörighetskontroll (auktorisation) där behörighetskontroll har en mer finkornig betydelse än enbart åtkomst till en IT-tjänst
- IAM som inkluderar autentisering, behörighetskontroll samt administrativa försystem som baserat på olika verksamhetsprocesser samlar in grundläggande information om person- och organisationsinformation – i syfte att informationsförsörja identitets- och behörighetshantering

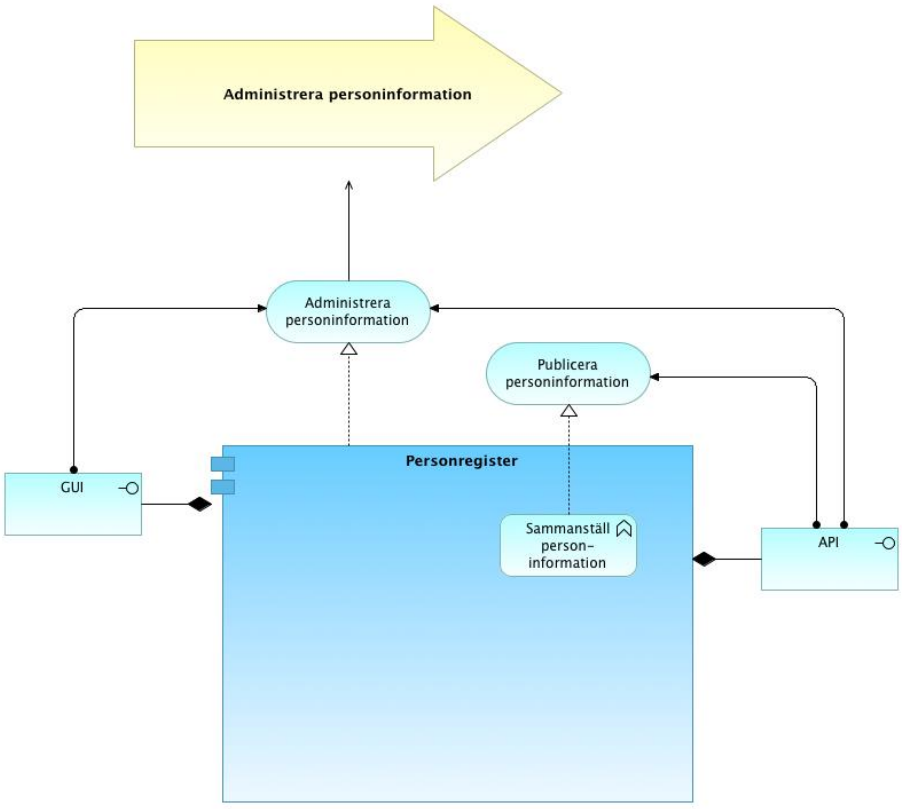
Inom ramen för IAM för högre utbildning i Sverige är identitetsfederationen SWAMID en viktig del. Många forskningsprojekt sker genom samarbeten mellan lärosäten och möjligheten för forskarna att kunna använda sin lokala elektroniska identitet för att nyttja IT-tjänster vid andra lärosäten (s k federerad inloggning) är en väsentlig del och skiljer sig en del ifrån hur t ex ett privat företag normalt ser sina behov.

För att kunna föra en fortsatt diskussion om en sektorgemensam arkitektur för identitets- och behörighetshantering behöver det finnas en gemensam definition av grundbegrepp. Den gemensamma definitionen görs bäst genom en logisk uppdelning där de olika ingående logiska delarna försörjer helheten med olika funktioner.

Baserat på omvärldsanalysens totala bild av IAM definieras de ingående delarna som; personregister, organisationsregister, identitetshanterare samt behörighetshanterare.

Personregister

Ett personregister beskrivs huvudsakligen genom de tjänster som personregistret tillhandahåller, *administrera personinformation* och *publicera personinformation* (*Figur 1 Logisk vy av tillämpningen Personregister*). Hos de lärosäten där det finns ett implementerat personregister är informationsförsörjningen i huvudsak automatiserad genom tekniska integrationer där information i första hand hämtas från studiedokumentationssystem och personalsystem. Ofta är den automatiserade informationsförsörjningen kompletterad av ett grafiskt användargränssnitt där administrativ personal kan lägga till och ändra personinformation. I den logiska modellen visualiseras informationsförsörjningen med funktionen *Sammanställ personinformation*. Publiceringen av personinformation görs antingen genom regelbundna integrationer alternativt direkt från identitetshanteraren vid behov.

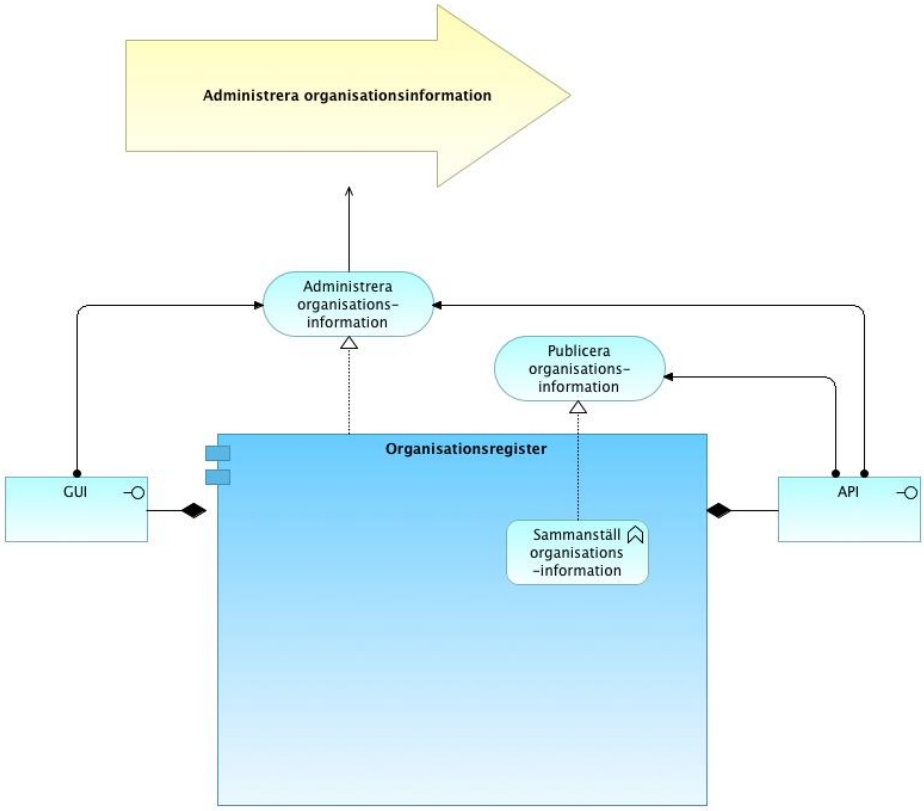


Figur 1 Logisk vy av tillämpningen Personregister

Organisationsregister

Den logiska komponenten *Organisationsregister* är funktionellt identiskt med personregistret med skillnaden att komponenten beskriver organisationens olika delar, dess förhållande till varandra samt eventuell relation till personer.

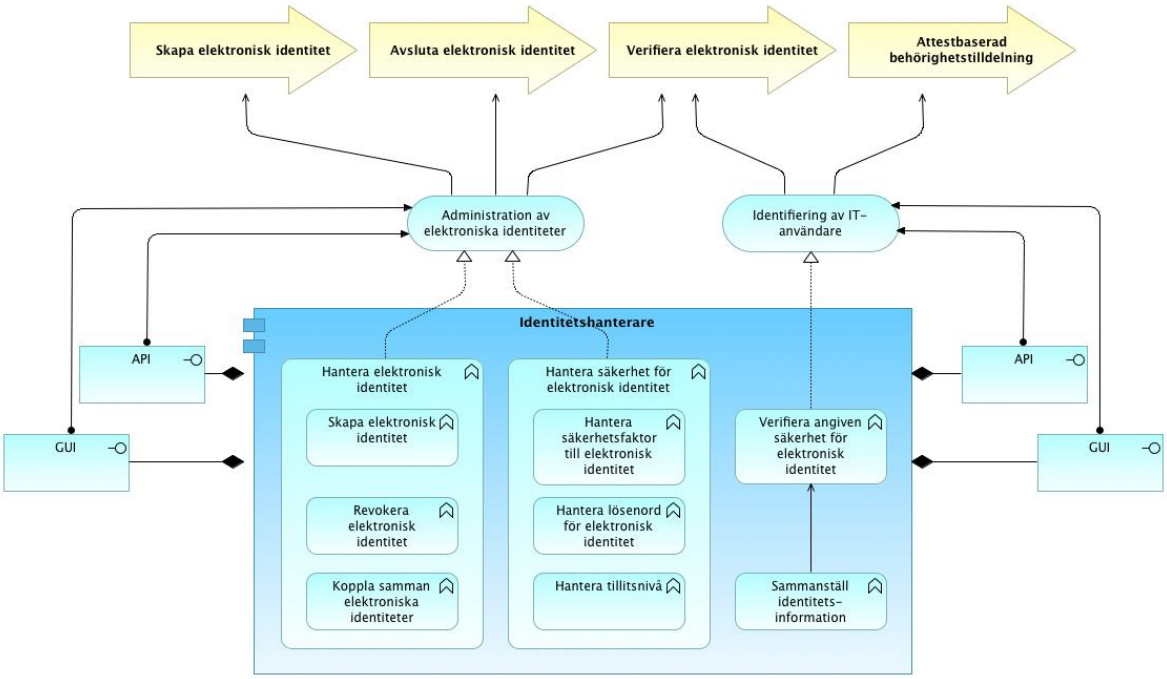
Vid de lärosäten som har ett implementerat organisationsregister är ofta organisationsregistret implementerat tillsammans med personregistret i en och samma tekniska lösning.



Figur 2 Lokisk vy av tillämpningen Organisationsregister

Identitetshanterare

Den logiska komponent som hanterar identiteter kan också i huvudsak beskrivas genom de tjänster komponenten exponerar, *Administration av elektroniska identiteter* och *Identifiering av IT-användare*.



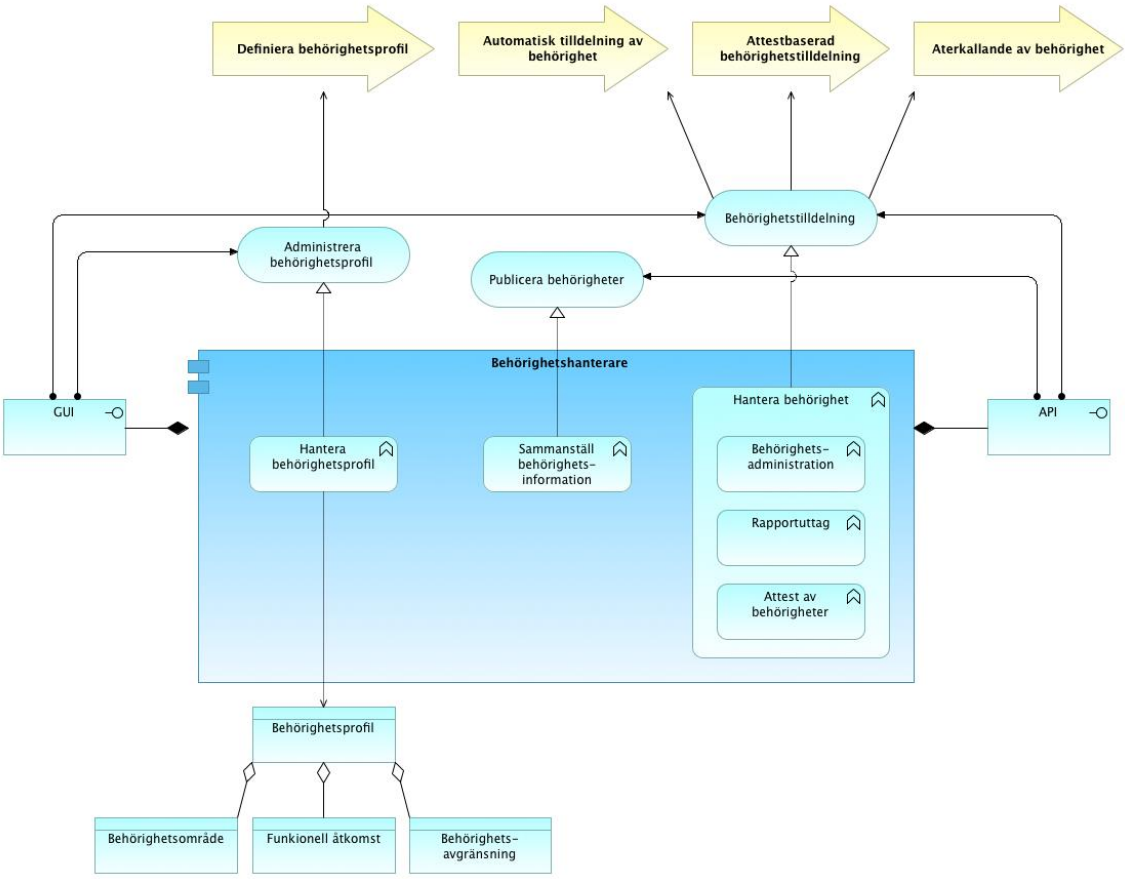
Figur 3 Logisk vy av tillämpningen Identitetshanterare

Tjänsten *Administration av elektroniska identiteter* omfattar livscykelhanteringen för elektroniska identiteter där de skapas, revokeras samt kopplas till andra elektroniska identiteter. Kopplingen till andra elektroniska identiteter görs genom s.k. identitetsväxling där en befintlig annan elektronisk identitet används vid skapandet av en ny elektronisk identitet samt hantering av tillitsnivå för en elektronisk identitet. Som en ytterligare ingående del i administrationen av elektroniska identiteter finns hanteringen av säkerhet, dvs. lösenord och andra typer av faktorer som används vid identifiering av en IT-användare.

Tjänsten *Identifiering av IT-användare* används varje gång en användare ska identifiera sig i en IT-tjänst inkl. de funktioner inom IAM där användare behöver vara identifierade.

Behörighetshanterare

Tjänsterna *Administration av behörighetsprofiler*, *Behörighetshetstilldelning* samt *Publicering av behörighetsinformation* är de logiska tjänster som en behörighetshanterare implementerar.



Figur 4 Logisk vy av tillämpningen Behörighetshanterare

En behörighetsprofil innebär en generell beskrivning av *åtkomst*. En behörighetsprofil delas in i de tre olika delarna område, rättighet och avgränsning. Område kan där relateras till IT-tjänstbegreppet och exemplifieras med *ekonomiadministration*, rättighet beskriver funktionell åtkomst som *godkännande av faktura* och avgränsning definierar vilken information som en funktionell behörighet får appliceras på som exempelvis *fakturor knutna till institution X*. Begreppet *behörighet* avser en specifik elektronisk identitet i relation till en beskriven åtkomst, behörighetsprofil.

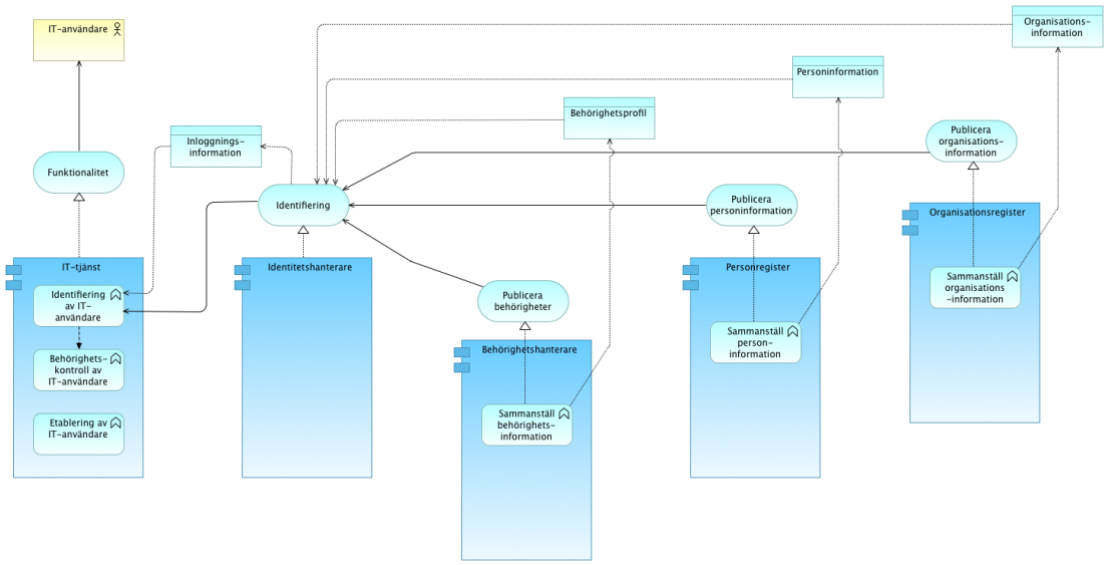
Tjänsten *Publicera behörigheter* används i huvudsak på två olika sätt. Det ena sättet genom att en identitetshanterare hämtar och förpackar behörighetsinformation tillsammans med den identitetsinformation som skickas vid en autensiering. Det andra sättet sker genom en integration där behörighetsinformation förmedlas till den IT-tjänst som ska applicera en behörighetsbegränsning. Förhållandet mellan de olika komponenterna specificeras vidare i kapitlet *Komponenternas samspel*.

Komponenternas samspel

IAM som helhet omfattar i sin mest omfattande form ett samspel mellan de logiska komponenter som definierats i kapitlen Personregister, Organisationsregister, Identitetshanterare samt Behörighetshanterare. I analysarbetet av hur befintlig IAM är implementerad vid olika lärosäten har tre olika mönster för hur de olika logiska komponenterna kan användas tillsammans identifierats. Mönstren definieras enligt:

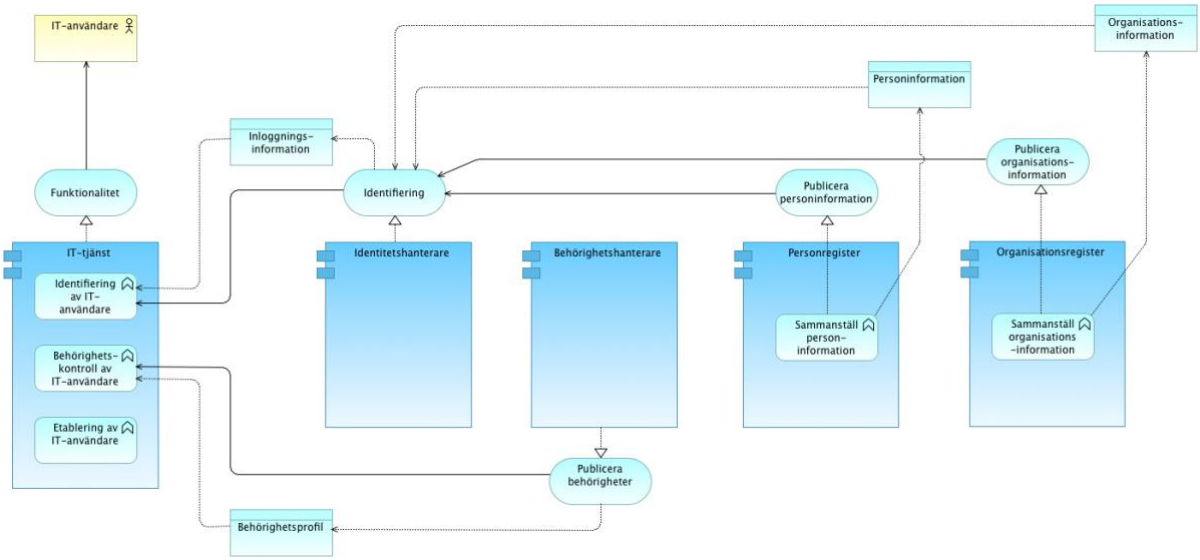
- Synkron gemensam distribution av identifierings- och behörighetsinformation
- Separat distribution av identitets- och behörighetsinformation initierad från IT-tjänst
- Separat distribution av identitets- och behörighetsinformation initierad från behörighetshantering

De olika mönstren illustreras i *Figur 5*, *Figur 6* och *Figur 7*.



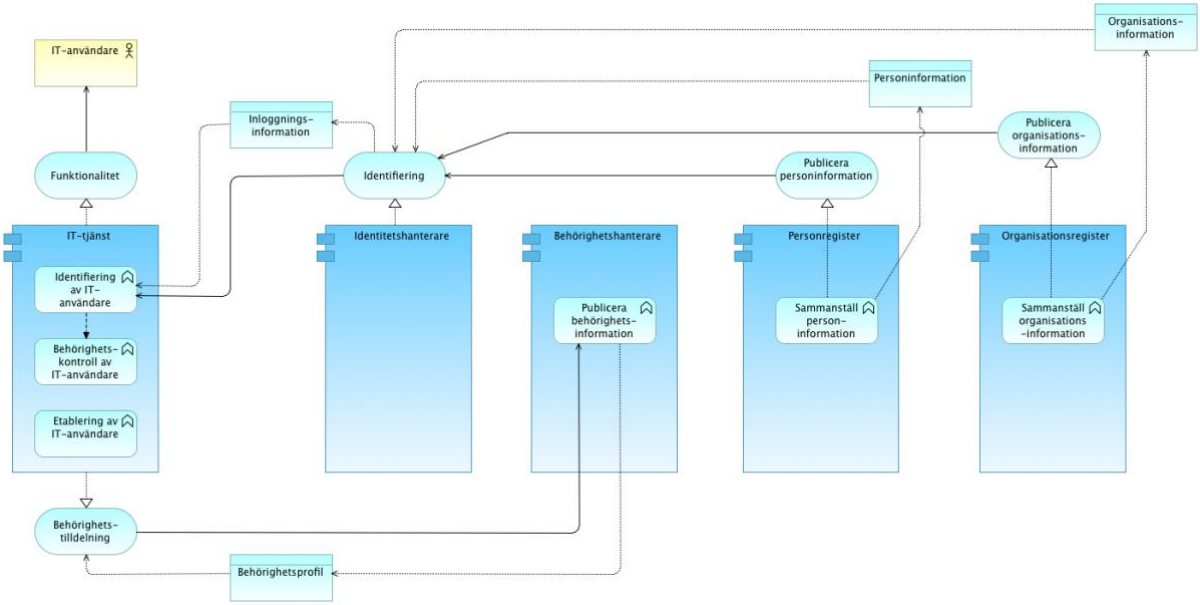
Figur 5 Synkron gemensam distribution av identifierings- och behörighetsinformation

Mönstret *Synkron gemensam distribution av identifierings- och behörighetsinformation* kan exemplifieras genom identifiering av en IT-användare i en webbaserad IT-tjänst som baseras på standarderna *Security Assertion Markup Language 2.0 (SAML v2.0)* och *General Model for Authorization Information* (*GMAI)*. I exemplet hänvisar IT-tjänsten autentisering till en identitetshanterare (IdP) som verifierar användarens säkerhet samt förpackar person- och informationsinformation enligt SAML 2.0 samt behörighetsinformation enligt GMAI.



Figur 6 Separat distribution av identitets- och behörighetsinformation initierad från IT-tjänst

Ett exempel för användning av komponenterna enligt mönstret *Separat distribution av identitets- och behörighetsinformation initierad från IT-tjänst* kan beskrivas genom en webbaserad IT-tjänst vars autentisering är knuten till *Active Directory*. Efter en lyckad inloggning hämtas ytterligare information från *Active Directory* genom att användaren knyts till behörighetsgrupper. I exemplet är det sannolikt att information från de olika logiska komponenterna alla är publicerade i *Active Directory* som då utgör ett informationsnav för de olika informationsdomänerna.



Figur 7 Separat distribution av identitets- och behörighetsinformation initierad från behörighetshanterare

I mönstret *Separat distribution av identitets- och behörighetsinformation initierad från behörighetshanterare* är IT-tjänsten helt självförsörjande gällande behörighetsinformation men beroende av en extern komponent som kan identifiera en

IT-användare. IT-tjänsten är självförsörjande i den mening att den inte förlitar sig på andra komponenters aktiva tillgänglighet och har hela informationsmodellen för behörighet implementerad och lagrad direkt i IT-tjänsten. Däremot har organisationen som använder mönstret valt att centralisera behörighetsadministrationen till en separat logisk komponent som flera olika IT-tjänster sedan kan nyttja. För att behörighetsinformationen ska komma IT-tjänsten till godo behöver en integration implementeras som läser en behörighet i behörighetshanteraren och förmedlar den till IT-tjänsten. Integrationen utgörs i den grafiska vyn av en implementerad integration (funktionen *Publicera behörighetsinformation*) men kan också hanteras genom manuella rutiner och grafiska gränssnitt.

Samtliga tre ovan beskrivna scenarier kommer vara relevanta för de flesta lärosäten inom en överskådlig framtid. De är kompletterande baserat på hur olika IT-tjänster valt att implementera autentisering resp. auktorisation. Något en organisation inte kan påverka då externa IT-tjänster används, oavsett om de är lokalt installerade eller externa enligt definition ”molnet”.

Övergripande beskrivning av infrastrukturkomponenter

Fokus på kommande kapitel ligger på att försöka sätta de infrastrukturella delarna som realiserar de logiska komponenterna i ett infrastrukturellt sammanhang, beskriva deras syfte tillsammans med både möjligheter och begränsningar samt att beakta olika kategorier av användare.

De logiska komponenternas i infrastrukturkontext

I tidigare kapitel har de fyra logiska komponenterna identifierats som:

- Personregister
- Organisationsregister
- Identitetshanterare
- Behörighetshanterare

Det är inte givet att fyra logiska komponenter är likställt med fyra enskilda infrastrukturella delar. Troligt är att en eller flera logiska delar implementeras i samma eller ett mindre antal infrastrukturella komponenter.

De flesta av lärosätena har utvecklat lokala system som stödjer flera av ovan nämnda logiska komponenter. Den logiska komponent som oftast hanteras separat och som dessutom ofta har flera implementationer per lärosäte är identitetshanteraren. Exempel på sådana implementationer är:

- Azure AD
- Lokalt Active Directory
- Heimdal/MIT Kerberos
- Shibboleth IdP
- Active Directory Federation Services
- CAS

Generellt sett löser varje implementation ett eller flera olika protokoll för autentisering.

Nedan följer ett antal scenarier som är aktuella i en framtida infrastruktur:

- Möjliggöra federativa tjänster
- Stödja/ersätta lokalt Active Directory
- Stödja Azure Active Directory
- Inloggning; IT-tjänster, lokala datorer och andra enheter
- Behörigheter; IT-tjänster, lokala datorer och andra enheter
- Stödja/ersätta person- och organisationsregister

Genom att beskriva scenarier för infrastrukturella utmaningar som behöver beaktas kan ett underlag för möjliga implementationer sammanställas.

Det finns ett stort antal kommersiella produkter (t. ex. Ping Identity, SailPoint, produktsviter ifrån IBM eller CA resp. Azure AD för delar av de logiska komponenterna) inom området som stödjer delar av eller helheten gällande de logiska komponenterna. I ett vidare arbete med en lärosätesgemensam hantering för IAM bör en djupare marknadsundersökning och kravanalys göras ang. kommersiella produkter i syfte att se huruvida de kommersiella alternativen är realistiska alternativ som kan realisera en framtida IAM-lösning. Det är dock oklart hur mycket stöd av exempelvis auktorisation av lokala klienter som de olika produkterna stödjer.

Scenarier

Generellt för samtliga scenarier som en nationell lösning måste stödja är att det måste finnas tydligt definierade tjänstegränssnitt, både för asynkront och synkront beteende. Tjänstegränssnitt måste kunna erbjuda nyttjande genom olika interface men bör i grunden vara samma tjänst. Standardiserade gränssnitt och gemensamma format är en förutsättning för att inte hamna i en förvaltningssituation där varje enskilt lärosäte kravställer på en egen tjänst. I huvudsak handlar det om att slippa anpassa varje meddelande per konsument vilket kommer att leda till en svår underhållssituation med

olika livscykler för varje meddelande och gränssnitt. En så lös koppling som möjligt skall vara målet för gränssnittet mot konsumenterna.

Vidare är scenerierna en mix av tydliga infrastrukturella produkter såsom AD eller Azure AD vilka kan realisera en eller flera av de identifierade logiska komponenterna. Andra scenarier är mer generiska vilket en gemensam lösning behöver beakta och stödja. Det finns överlapp mellan vissa produkter och scenarier och vilka logiska komponenter de realiserar. Detta beror till stor del att det idag finns olika lösningar på lärosäten som en gemensam lösning behöver stödja eller ersätta.

Möjliggöra federativa tjänster

Det har under många år varit möjligt att baserat på federationen SWAMID göra ett stort antal IT-tjänster tillgängliga för användare inom sektorn. Genom att konfigurera en *Service Provider (SP)* till att lita på federationen går det relativt enkelt att genom en *Identity Provider (IdP)* autentisera och vissa fall även auktorisera användare. Dvs. den som tillgängliggör en tjänst behöver inte hantera lokala konton och passord. Exempel på sådana tjänster är nationella IT-tjänster som nya Ladok, SUNET Connect, SUNET Box, SUNET Projektplace samt minst lika viktigt IT-tjänster som tas fram inom ramen för forskningsprojekt som spänner över flera lärosäten. Tröskeln för att göra en ny tjänst tillgänglig är låg och det går att återanvända sin egen IdP i många tjänster. Många lärosäten använder dessutom sin IdP som den primär webbaserad *Single Sign On (SSO)* för det egna lärosätet.

De olika produkterna stödjer flera protokoll men det är endast SAML2 som idag finns inom SWAMID-federationen, Det finns dock arbete som pågår inom eduGAIN med SWAMID som aktiva aktörer för att skapa en federation baserad på OIDC. Detta arbete är dock inte klart men det finns ett tidigt utkast för hur detta skulle kunna ske.

En framtida IAM-lösning måste stödja lärosätesspecifika IdP:er vare sig dessa är implementerade lokalt på lärosätet eller via nyttjande av t.ex. Azure AD eller andra molnbaserade lösningar. Sättet att implementera identitetsfederationer framför allt för forskningssamarbeten är relativt unikt inom sektorn högre utbildning. Fokus är decentraliserad administration och oftast saknas det i förväg en bild av vilka IT-tjänster som är relevanta för ett visst lärosäte. Konsekvensen är att det finns få produkter som stödjer hanteringen. Det enda fullgoda stödet som fullt ut stöder federationskonceptet är i dagsläget Shibboleth IdP v3 resp. derivat av pySAML (eduID). Microsofts produkter (och motsvarande autentisieringslösningar från andra leverantörer) går att använda med begränsningen att all information om vilka SP:er resp IdP:er som finns tillgängliga (metadatahantering) måste hanteras lokalt i autentisieringstjänsterna. Det finns i dagsläget halvautomatiserade rutiner framtagna för ADFS för att stödja hanteringen men inbyggt stöd i produkten saknas.

Stödja/ersätta lokalt Active Directory

På sikt är det tydligt att lokala Active Directory kommer att försvinna till förmån för det molnbaserade Azure AD. Det går redan idag att registrera lokala datorer (Microsoft Windows 10) så att det går att logga in och styra behörigheter via Azure AD. Däremot så kommer behovet för ett lokalt Active Directory kvarstå under en övergångstid. I ett IAM-perspektiv med fokus på processer och provisionering samt behörigheter går det att säga att ett lokal Active Directory är en konsument av data från en gemensam IAM. I korthet betyder det att lärosätet har sin primära IAM i en nationell implementation och sedan transporteras data från nationell IAM till lokalt Active Directory via tydliga och väl definierade tjänstegränssnitt.

En av de stora drivkrafterna att behålla ett lokalt Active Directory är behovet av att styra och kontrollera policys på lokal dator. Även programdistribution via lokala tjänster som är beroende av Active Directory är också en drivkraft för ett lokalt Active Directory. I en ganska nära framtid bedöms detta förfarande förändras och därmed försvinner drivkraften för att behålla de lokala implementationerna. Redan inom ett par tre års sikt kommer det sannolikt inte gå att paketera och distribuera exempelvis Microsoft Office lokalt längre utan för att få tag i programvara och licenser måste mjukvaran installeras direkt från Office365.

I nuvarande version av Azure AD finns dock inte tillräckligt med funktionalitet för att kunna ersätta ett lokalt Active Directory för alla lärosäten men för vissa lärosäten täcker funktionaliteten behovet redan idag.

Stödja Azure AD

Eftersom att ett lokalt Active Directory bedöms att på sikt komma att avvecklas till förmån för Azure AD så bör en framtida lösning för IAM inrikta sig på att stödja Azure AD. Därför är det inte aktuellt att skapa en infrastruktur som erbjuder en alternativ lösning för Microsoft-baserade klienter baserat på något annat än Azure AD. Att upprätthålla en lösning som skall vara ett alternativ till Azure AD bedöms bli komplex, i synnerhet med ny funktionalitet på klientsidan enbart stödd av Azure AD.

En nationell lösning bör istället inrikta sig på att skapa robusta integrationer med Azure AD genom exempelvis standardiserade gränssnitt som SCIM[1]. Det kan betyda att såväl nationell som lokal IAM-hantering har det gemensamma behovet av en adapter som asynkront underhåller data i Azure AD. Samma SCIM-baserade tjänst bör erbjuda flera olika sätt att ansluta, både asynkrona och synkrona.

Förutom att erbjuda autentisering via SAML2 stödjer Azure AD autentisering via ett flertal andra protokoll (t ex OIDC och OAUTH) vilka kan vara relevanta om lärosätet har

[1] Standardiserat gränssnitt: System for Cross-domain Identity Management

behovet. Stöd för OIDC i federativ miljö finns i dagsläget inte i Azure AD eftersom standarden för protokollet ej är färdigställd. Därefter kan bedömningen göras om Azure AD kommer att stödja standarden eller inte.

Inloggning; IT-tjänster, lokala datorer och andra enheter

På ett typiskt lärosäte används flera produkter för att realisera autentisering. Såsom exempelvis:

- Active Directory – Lokala Windows/Mac/Linux-klienter
- Heimdal/MIT-Kerberos – Primärt Linux/Unix-klienter
- Azure AD – Lokala klienter, Azure tjänster
- ADFS – federerade tjänster
- Shibboleth – federerade tjänster
- eduID – federerade tjänster
- Radius – för eduroam och liknande nätrelaterade tjänster
- Andra kommersiella lösningar – ofta helhetslösningar för samtliga logiska komponenter

Även om det nu sker en förflyttning mot molnlösningar även för lokal autentisering behöver en gemensam lösning kunna stödja och hålla dessa olika lösningar och produkter i synk och stödja federerad autentisering i alla fall under en övergångstid. Många lärosäten kommer befinna sig i olika lösningar under en ganska lång tid, vilket betyder att integrationer mellan dessa lösningar blir nödvändiga.

Det skulle kunna betyda att lärosäten använder sig av delar av en gemensam lösning i kombination med lokala lösningar

Det finns också relativt många kommersiella IAM-lösningar på marknaden som skulle vara bra att utvärdera utifrån de behov som sektorn har när det gäller SWAMID-federationen, Azure-tjänster och lokala klienter. Flera av de kommersiella produkterna löser flera av de logiska komponenterna och bl.a. Ping Identity har precis släppt stöd för Azure AD.

Dock så behöver ofta en egen plugin installeras på lokala klienter för att stödja lösningarna som ersätter klientens inbyggda modul.

Behörigheter; IT-tjänster, lokala datorer och andra enheter

Rent tekniskt är detta relativt enkelt. Behörighetsgrupper skapas i ngn katalog eller direkt i exempelvis ett AD och sedan sätts behörigheterna på resurser alternativt så släpps de attribut som behövs inom ramen för exempelvis SAML2. Dvs. implementationerna är kända och väl etablerade och har en god spridning inom lärosäten idag. Även en stor del egenutvecklade tillämpningar för att bygga behörighetsstrukturer finns också i sektorn.

Genom att flytta upp behörighetsstrukturerna och hanteringen i en gemensam lösning förändras ovan inte speciellt mycket så länge det genom robusta integrationer går att föra över behörighetsstrukturerna till de lokala tillämpningarna, såsom lokala kataloger som populerar egna AD eller en helt molnbaserad behörighetstjänst. När det gäller att utföra en behörighetskontroll är det upp till det enskilda systemet/tjänsten att göra valideringen.

Utmaningen ligger i att stödja en komplex struktur med rekursiva relationer för att kunna uttrycka flera nivåer av strukturer som kan ha arv. Nästa utmaning ligger i verksamheten för att uttrycka behörigheter på ett sådant sätt att de är löskopplade från tjänsten. För att få en bild över hur ett generiskt mönster kan se ut för att uttrycka behörigheter finns i Martin Fowlers; Accountability Pattern[2].

Beroende på mognadsgrad och hur pass strukturerad grundinformationen är för att skapa behörighetsstrukturer är det nödvändigt att implementationen tillåter ett flexibelt sätt att uttrycka behörighetsstrukturer. Det blir svårt att definiera en gemensam struktur som passar alla lärosäten. Grundmodellen för hur behörigheter uttrycks kan troligtvis vara generell.

Stödja/ersätta person- och organisationsregister

En grundbult för att kunna hantera och administrera behörigheter och identiteter är att kunna samla så mycket information runt personen så att provisioneringen kan göras korrekt. En vanlig referens för den här typen av register är metakatalog. Det är inte helt ovanligt att olika system har olika identifierare för en person. Ett tydligt exempel på detta är personnummer som uttrycks olika i Primula, Ladok samt att skatteverket ger ut samordningsnummer som kan skilja sig åt från Primula och Ladoks personnummer. Det betyder att för att kunna identifiera att det är samma person som skall tilldelas exempelvis en behörighet kan krävas ytterligare attribut för att se sambanden mellan olika identiteter som faktiskt är samma person. Det är önskvärt att inte ha flera identiteter som uppträder som inte är kopplade till samma person. Detta ger dålig datakvalitet och dåliga underlag för beslut.

[2] https://martinfowler.com/apsupp/accountability.pdf

På samma sätt är problemet liknande för organisationsid:n Det är återigen skillnad mellan de organisationsidentiteter som finns i Primula och Ladok och för att kunna använda organisationsinformationen för att skapa behörigheter krävs en tillgång till alla mappningar mellan de olika applikationernas användande av organisationsid:n.

För att kunna erbjuda en gemensam metakatalog behöver den klara av integrera med flertalet källsystem för att skapa en metakatalog som ger en entydig bild av en person och organisationen. Det ligger en stor utmaning att skapa en informationsmodell som klarar av att generiskt kan uttrycka alla typer av organisationstyper såsom; linjeorganisation, projektorganisationer, centrumbildningar etc. Det ligger också mycket utmaningar i att kunna uttrycka en persons relation till olika typer av organisationer.

Utmaningar kring autentisering och auktorisation

För att sätta scenarierna i en kontext och hur implementationen löser ovan nämnda scenarier behövs en nedbrytning av autentisering (AuthN)och auktorisation (AuthZ).

Det är inte helt ovanligt att de olika komponenterna endast används för att identifiera en användare i en IT-tjänst och att själva behörigheten tilldelas lokalt i IT-tjänsten. Dvs. autentiseringen sker med en SWAMID-ansluten IdP, men behörigheten sker genom att behörigheterna redan finns och administreras i IT-tjänsten eller förs över till systemet men en integration (ref. Figur 7 Separat distribution av identitets- och behörighetsinformation initierad från behörighetshanterare). Ovan beskrivning gäller exempelvis för nya Ladok där behörigheter inom ett lärosäte tilldelas till en användare som sedan använder en SWAMID IdP för att autentisera sig. Detta gäller dock administratörer – för studenter görs en ren federativ autentisering och behörighetstilldelning[3]. Nackdelen med lokala behörigheter inom resp. IT-tjänst är att det framför allt ofta saknas möjligheter att få fram en bra sammanställning över en användares samtliga behörigheter samt strukturerade flöden för att tilldela resp. återkalla behörigheter för användarna. Detta går att kan uppnå genom en strukturerad behörighetshantering vid en central punkt och aktiva integrationer mellan den centrala punkten och de IT-tjänster som har en egen implementation av behörighetshantering.

Projektgruppen är medveten om att det även finns andra tekniker än de som tas upp i denna rapport gällande autentisering och auktorisation. Projektgruppen bedömer dock att de tekniker som omnämns i rapporten täcker behovet av autentisering och auktorisation. Framförallt finns det mycket proprietär mjukvara på marknaden men många av dem implementerar öppna protokoll som täcks av komponenterna listade i Tabell 1. Vidare kan vissa protokoll och tekniker inte användas för både AuthN och AuthZ utan kräver att behörigheterna finns tillgängliga som exempelvis grupper eller liknade i ett Active Directory eller en LDAP. Vissa produkter såsom Active Directory

[3] Inte helt korrekt då man mappar personnummer och vilken IdP studenten använt. Ladok 3 läser inte attributet affiliation.

implementerar både öppna och stängda protokoll och flera andra delar som i en helhet är nödvändiga för att få övriga produkter att fungera med framförallt behörigheter.

De protokoll och tillämpningar som listas nedan är möjliga som delar av en nationell IAM-tjänst. Listan är inte komplett utan visar på att det finns begränsningar i infrastukruten som måste beaktas. Det som listan försöker visa är att vissa protokoll utför antingen autentisering eller/och auktorisation

Protokoll/tillämpning	***Autentisering***	***Auktorisation***
SAML2 i SWAMID	X	X
Kerberos	X	--
Active Directory	X	X
OAuth och OpenID-Connect	X	X
SCIM, API	--	X
Radius	X	--
CAS	X	(X)

Tabell 1

Utmaningar i den närmsta framtiden

En av de största utmaningarna inom den närmaste framtiden är att båda de stora leverantörerna av operativsystem för traditionella skrivbordsdatorer, Microsoft resp. Apple, bygger in mer och mer funktionalitet i operativsystemet som förutsätter att användaren ligger kontinuerligt uppkopplad mot leverantörernas molntjänster. Förutom för att på det sättet kunna erbjuda användarna olika sorters funktionalitet i stil med molnlagring av dokument så är det naturligtvis ett steg i leverantörernas strategi för att hålla kvar användarna inom ekosystemet. I Apples fall sträcker detta sig tydligt över till operativsystemen för de mobila enheterna medan i Microsofts fall i stället är fokus på de programvaror som erbjuds via Office365. Även andra leverantörer i stil med Adobe går mer och mer mot en situation där programvarorna kräver aktiv knytning mot molnet åtminstone för den initiala installationen.

Denna ändrade strategi ifrån leverantörerna i kombination med den inom sektorn sedan länge etablerade BYOD-situation gör att det redan idag är ganska tveksamt att försöka sätta för stor vikt vid att knyta användare till en viss enhet via t ex en Active Directory-inloggning. Det är naturligt för användarna att kunna använda vilken enhet som helst för att komma åt dokument och IT-tjänster och oavsett vad man tycker arbetsrättsligt så tar nog många användare för givet att de ska kunna komma åt samma information och samma IT-tjänster ifrån sin hemdator som från datorn som står kvar på arbetsplatsen. Att kunna stödja användare med bra IT-support utan kontroll över den specifika enheten som de för stunden arbetar ifrån kommer absolut vara ett krav framöver och ställer tvärtom högre krav på att strukturen för identitets- och behörighetshantering fungerar helt frikopplat ifrån ev. stödsystem för IT-support för användarnas enheter.

Slutsatser

Projektets bild är att det finns två olika frågeställningar att hantera inom sektorn för stunden. Dels behöver de mindre lärosätena stöd att tillhandahålla en identitets- och behörighetshantering där huvudutmaningarna främst gäller tröskelkostnad för både arbetsinsats och kompetens medan det andra huvudspåret är att de större lärosätena främst har utmaningar i form av komplexa organisationer med t.ex. situationer att på ett säkert sätt kunna hantera anställda, studenter och övriga verksamma som aldrig är fysiskt på lärosätet. Sammantaget skapar detta en situation där det är orimligt att se att behoven tillgodoses av *en* teknisk lösning. De större lärosätena är också i högre grad påverkade av omvärlden i form av vilka krav som måste tillgodoses för att federerad inloggning ska kunna vara en fungerande byggsten för att få ihop IT-infrastruktur för nationella och internationella forskningssamarbeten. Det är också så att det sällan finns några sammanhållna helhetslösningar då identitets- och behörighetshantering traditionellt innehållit många byggklossar.

Det positiva är att läget är gynnsamt för att skapa en samsyn om baserad på ett modulärt koncept där lämpliga delar finns via nationella gemensamma tjänster. Det ger att det då finns tydliga gränslinjer mellan resp. modul så att det inte finns någon oklarhet i hur ett lärosäte bygger utökad funktionalitet inom en eller flera moduler men ändå kan samverka med de nationellt tillgängliga modulerna. Faktorerna som talar för att detta skulle vara rätt tidpunkt är att det finns en bra mix mellan lärosäten som har erfarenheter ifrån nyligen genomförda lokala projekt och lärosäten som har ett tydligt behov av att modernisera befintliga lösningar. Det finns också ett par kommande tekniker och behov som behöver struktureras upp och förankras.

Projektets arbete under året visar också tydligt på att det finns en relativt hög samsyn inom området om hur ett modulärt koncept skulle kunna vara uppbyggt. Det behövs däremot en bredare förankring utanför de lärosäten som varit aktiva i projektet via projektgruppen resp. referensgruppen. Det har också varit en nödvändig aktivitet för projektet att enas om begrepp och beskrivningsmodeller.

Följande områden är också tydligt att det kommer att krävas vidare utredning om

- Hur gemensamma är våra processer inom området och hur bra kan en nationell lösning stödja processerna?
- Går det att nå en samsyn om hur en informationsmodell inom området ser ut?
- Hur hanterar man ett nationellt koncept med skillnader i informationsmodell mellan lärosätena?

Rekommendation

Det bör ges ett uppdrag att arbeta vidare med att konkretisera och förankra ett modulärt uppbyggt identitets- och behörighetskoncept. Det behöver tas fram ett konkret förslag på hur detta skulle kunna se, arbeta fram en kravspecifikation på resp. modul och även ta fram en sammanställning av hur man kan tillgodose kraven via nyutveckling, upphandling eller befintliga tjänster samt sammanställa en bild av vilket intresse det finns av nationella tjänster inom resp. modul.

Fortsatt arbete

Inom IAM projektet så har ett antal processer på hög nivå identifierats som är nödvändiga kopplat till IAM. Även logiska applikationskomponenter och infrastrukturkomponenter på en hög nivå har identifierats. Vidare så har IAM-projektet identifierat att behoven av IAM-stöd för olika lärosäten är divergerat d.v.s. kraven på IAM skiljer sig framför all mellan stora och små lärosäten. Detta betyder att kraven på en sektorgemensam lösning riskerar att bli komplex och att ansatsen måste vara att erbjuda en uppsättning gemensamma IAM-komponenter som kan användas av lärosäten i de fall dessa passar in i den lokala behovsbilden. Till detta kommer och krav på lokala komponenter som skall kunna passa in ett nationellt sammanhang.

Ett fortsatt arbete skulle kunna fokusera på att ta fram ett beslutsunderlag med följande innehåll

- Vidare processkartläggning över processer kopplat till IAM i ett sektorgemensamt sammanhang. Samt kartläggning av existerande tjänster kopplat till IAM i ett sektorsgemensamt sammanhang
- Rekommendation för hur en sektorgemensam IAM-infrastruktur kan implementeras
- Utifrån framtagna processer identifiera gemensamma infrastrukturkomponenter – IAM infrastrukturarkitektur för sektorn.
- Identifiera nationella komponenter och lärosätesspecifika komponenter samt hur dessa komponenter kan dessa komponenter interagerar med varandra.
- Rekommenderat innehåll och grov planering för ett implementationsprojekt
- Estimerade kostnadsramar för ett införande av en sektorgemensam lösning.