Inkubator

Auktorisation och grupphantering

Slutrapport

Webadress https://portal.nordu.net/display/Inkubator/Projektrapporter			
Dokumentnamn AoG Kartläggning.pdf			
Dokumentansvarig Maria Valtersson			
Dokumentidentitet N/A	**Version** 1.0	**Datum** 2013-12-20	**Status** Publicerad

Innehåll

1 Sammanfattning

Auktorisation och grupphantering är ett gemensamt behov för samtliga universitet och högskolor i Sverige. Då det är ett stort område, kan en del av områdesorienteringen och utvärderingen av verktyg göras gemensamt. Det är syftet med denna utredning.

Projektet har gjort en kartläggning av nuläge och behov på svenska lärosäten, en begreppsdefinition, flera user stories, use cases och scenarios, samt en första version av rekommendationer. I januari 2014 levereras en jämförelse mellan gruppverktygen Grouper och FIM.

Auktorisation kan dels skötas centralt, dels automatiserat. Med centraliserad hantering menas att användarnas behörighetsuppgifter lagras centralt, en av fördelarna blir att de kan användas i mer än ett system. Med automatiserad hantering av auktorisation menas att behörighetsuppgifter skapas automatiskt. T ex kan kurstillfällesgrupper automatiskt skapas och underhållas med hjälp av Ladok.

Ett grupphanteringsverktyg behöver stöd för manuella grupper, som en enskild person äger, samt automatiska grupper. Den stora mängden grupper ställer krav på logisk och transparent organisation av grupper. Verktyget behöver kunna skapa grupper av andra grupper, genom olika mängdoperationer. För att vara effektivt måste även andra objekt som attribut, behörighet och roller kunna kopplas till grupperna och individerna. Grupperna ska kunna användas både för informationsspridning och för att ange behörighet. Olika typer av medlemmar ska kunna behandlas, lokala, federerade och andra externa.

Kartläggningen visar att AD är ett av de vanligaste verktygen i den lokala hanteringen. Många har utvecklat eget stöd, eller har separata lösningar. Inom LMS är det vanligt med automatgenererade grupper, och om man ser på specifika roller, ex webbredaktör i intranätet, kan hälften hantera det centralt och resten lokalt. För HR, Ladok och ekonomisystem (företrädelsevis feta klienter) är det vanligt att tilldelning sker i systemet. För många lärosäten så är det mycket vanligt med systemintern hantering av behörigheter.
9 av 10 anger finjusterade behörigheter som ett lokalt behov. Av utredningens användningsfall bedöms de viktigaste vara manuell undergrupp, öppen grupp och sammanslagen grupp. Möjlighet att hantera externa intressenter är också ett uttalat behov.

Utredningens user stories ska spegla typiska behov runt verksamheten på ett lärosäte, och visa exempel på vad grupphanteringssystem kan användas till. Naturligtvis är antalet user stories närmast oändliga i praktiken. Utredningen visar bland annat hur grupper underlättar hanteringen av:

- Hanteringen av passagerättigheter
- Rättighetsstyrning för Intranät, studentportal och LMS
- Forskargrupper och samarbetsytor
- Federerade grupper och grupper med lärosätesexterna medlemmar

Utredning har som ambition att bena ut vilka pusselbitar (schematiska typer av funktioner) som finns runt ett grupphanteringssystem. Kombinationer av dessa pusselbitar krävs för att realisera user stories. Pusselbitarna redovisas som användningsfall. Totalt 10st indelade i tre kategorier:

- Första kategorin handlar om hur grupper skapas, d.v.s. hur grupphanteraren fylls på med grupper.
- Andra kategorin handlar om hantering av befintliga grupper i grupphanteraren. Till exempel finns användningsfall runt hur nya grupper skapas av existerande grupper.
- Tredje kategorin fokuserar på export av grupper, d.v.s. till vad och hur grupperna används.

Utredningen presenterar tre scenarios, som är exempel på omfattningar av implementation av grupphantering. Tre scenarios redovisas. I växande storlek från small till large. Minsta omfattningen innebär att ett grupphanteringssystem inte används. Gruppfunktioner i befintliga ramverk, till exempel AD, används. Medium-scenariot tar upp införande av ett grupphanteringsverktyg. Large-scenariot beskriver en större satsning som även omfattar stora investeringar i det närliggande området Identity Lifecycle Management.

Sista kapitlet, rekommendationer, redovisar erfarenheter vunna av de lärosäten som implementerat grupphantering. Val av verktyg och strategier samt en stor skillnad i omfång för grupphanteringen innebär att rekommendationerna är spridda. Men, de handlar generellt om förhållningssätt och fallgropar inför uppstart av ett projekt i syfte att införa grupphantering med hjälp av ett grupphanteringsverktyg.

2 Beskrivning av projektet

2.1 Bakgrund

Antalet IT-system ökar stadigt hos Sveriges universitet och högskolor. Många individer i form av anställda, studenter och andra intressenter använder systemen. Tillväxten innebär att antalet IT-system som varje enskild individ behöver tillgång till, för att kunna utföra sitt arbete eller bedriva sina studier, också har ökat. En student ska använda olika IT-system beroende på vilka kurser som den är registrerad på, och vilken fakultet och institution som kurserna tillhör. Motsvarande gäller för den anställde, som utifrån sin organisatoriska roll och arbetsuppgifter, behöver tillgång till flera system. Behovet av att effektivisera behörighetsadministrationen har därför ökat. Administrationen måste också vara säker.

Många lärosäten har ökat användningen av single sign-on (SSO) de senaste åren. Effekterna av SSO är bl.a. att användarna inte behöver hålla reda på flera olika användarnamn och lösenord. Efter den första inloggningen kommer användaren åt alla resurser på nätet som denne har tillgång till. Lösenordet behöver bara anges till en säker tjänst på en välkänd webbadress, vilket underlättar för användaren att upptäcka konstigheter om denne blir uppmanad att ange användarnamn och lösenord på en annan webbadress. En annan fördel är att trycket på helpdesk minskar eftersom det inte blir så många ärenden om glömda lösenord till olika system.

Efter att autentiseringen på detta vis har effektiviserats, så blir auktorisationen nästa område för förbättringar.

Om vi tittar i backspegeln så administrerades behörigheter på varje enskilt system. Det accepterades eftersom varken systemen eller individerna var så många. De tekniska alternativen var inte speciellt avancerade. Idag finns goda tekniska möjligheter att lyfta administrationen från de enskilda systemen. Goda tillfällen att effektivisera finns inom hanteringen av de stora mängderna användare, inom kategorierna anställd och student. För detta blir det naturligt att använda grupper, vilket leder till utredningens fokus på just grupphantering. Därmed inte sagt att grupper är den bästa lösningen för alla olika typer av behörighetshantering.

2.2 Varför gör SUNET Inkubator denna utredning?

Auktorisation och grupphantering är ett gemensamt behov för samtliga universitet och högskolor i Sverige, och många lärosäten är intresserade av att vidareutveckla behörighetshanteringen. Men det är ett stort område, och det är ett mäktigt jobb för varje universitet/högskola att orientera sig, hitta och utvärdera alternativ samt presentera ett lösningsförslag. En del av detta arbete kan göras gemensamt. Styrgruppen för SUNET Inkubator har därför beviljat detta projekt.

2.3 Projektets målsättning

Projektet är en del i SUNET Inkubators mål att driva samsyn och skapa rekommendationer när det gäller e-infrastrukturfrågor.

2.3.1 Projektmål

1. Publicerad kartläggning av central hantering av behörigheter på de flesta svenska lärosäten, så som det ser ut våren 2013.

2. Publicerad beskrivning med definitioner på begrepp inom behörighetshantering, så att lärosätena får en gemensam grund att stå på.

3. En första version av publicerade rekommendationer för auktorisering och grupphantering. En övergripande beskrivande av området för att ge en helhetsbild. De ska vara på funktionell och konceptuell nivå, mer än teknisk nivå, men även behandla huvudspåren inom de produkter som är tillgängliga.

4. Genomföra teknikgenomlysning. Jämförelse mellan de mest intressanta verktygen på marknaden.

5. Rekommendationerna ska rikta sig till de som ska implementera ett stöd för hantering av behörigheter. Mottagare är IT-chefer och IT-arkitekter.

Enligt projektplanen skulle även ett Proof of Concept genomföras. Projektet har övervägt ett antal POC-förslag. För att utförandet ska bli till nytta för lärosätena så var kravet att det skulle vara ett realistiskt förslag som är väl förankrat i den lokala verksamheten. Inom avgränsningarna tyckte vi inte att något uppslag var tillräckligt bra. Inför 2014 finns däremot ett förslag för Proof of Concept. Det förslaget handlar om federerad grupphantering, något som inte ingick i projektet under 2013.

2.3.2 Effektmål

1. En strukturering i detta område ger lättare och mer kostnadseffektiva förändringar kopplat till behörighet och auktorisation.

2. Lättare att leva upp till framtida krav från verksamheten

3. Lättare att underhålla och bygga ut befintliga lösningar

4. Standardisering mellan lärosäten ger effektiviseringar och kostnadsbesparingar, att man jobbar med grupper och auktorisation ungefär på samma sätt och har samma ambitioner.

2.4 Organisation

Projektledare: Maria Valtersson, ITS, maria.valtersson@umu.se
Teknisk resurs: Jan Rundström, ITS, jan.rundstrom@umu.se
Uppdragsgivare: Per Hörnblad, projektkoordinator SUNET Inkubator, per.hornblad@umu.se

Projektet har en referensgrupp, bestående av personal från ett par olika lärosätens IT-avdelningar. Gruppens uppgift är att hjälpa till att leda projektet i rätt riktning, och säkra en involvering i projektet från flera lärosäten.

Medlem	**Lärosäte**	**Epost-adress**
Andreas Karlsson	Linköpings Universitet	andreas.karlsson@liu.se
Eskil Swahn	Lunds Universitet	eskil.swahn@ldc.lu.se
Leif Lagebrand	Blekinge Tekniska Högskola	leif.lagebrand@bth.se
Ola Ljungkrona	Chalmers Tekniska Högskola	ola.ljungkrona@chalmers.se
Pål Axelsson	Uppsala Universitet	pal.axelsson@uadm.uu.se
Enrico Pelletta	KTH	pelletta@kth.se

2.5 Tidplan

Projektet startade 21 januari 2013 och avslutas 31 december 2013.

2.6 Avgränsningar

Auktorisation är ett stort område, och som projekttiteln indikerar, har projektet avgränsat sig till just grupphantering. Projektet har inte fördjupat sig i behörighetsbärare som roller och attribut.

Sammanställningen behandlar lokala behörigheter på ett lärosäte. Federerad gemensam grupphantering hanteras av SWAMID. De rekommendationer som tas fram i projektet är av initial karaktär. Detaljering av dessa bör genomföras under 2014.

Angående kartläggningen, är de lärosäten som har kartlagts tjugonio av de största högskolorna och universiteten i Sverige, sett till antal helårsstudenter på grund- och avancerad nivå inräknat både statliga och privata lärosäten. Detta är samma avgränsning som gjordes i Swami-projektet ”Kartläggning e-infrastruktur” under 2011.

Gränsen har dragits vid de som har mer än ett tusen hst (helårsstudenter). Begränsningen gjorde att alla konstnärliga och teologiska utbildare samt enskilda utbildare med examensrätt enbart inom psykoterapi hamnade utanför urvalsgruppen.

2.7 Genomförande

Projektet inleddes med grundläggande informations- och kunskapsinhämtning, och en projektplan skapades. Medlemmar till referensgruppen tillsattes och Adobe Connect-möten med denna bokades in. Till en början diskuterades projektets syfte och mål livligt. Projektplanen bearbetades därför en vända till.

Delmomentet kartläggning inleddes med en ganska grundläggande kartläggning av behörighets- och grupphantering på Umeå universitet, med intervjuer med flera olika enheter på universitetet, förutom intervjuer med tekniskt ansvariga för specifika system på ITS. Detta var en del av informations-och kunskapsinhämtningen i området. Men även för tillfälle för en sådan mer omfattande kartläggning bara fanns på det lärosäte, där projektets medlemmar också fanns. SLU i Umeå besöktes också.

I början var tanken att kartläggningen skulle ske med intervjuer. Men referensgruppen tyckte kartläggningen var viktig, men inte projektets viktigaste del. Därför bedömdes att det skulle ta oproportionerligt lång tid att intervjua och dokumentera 29 lärosäten. Det blev istället en enkät i SurveyMonkey.

I enkäten ingick även frågor om lärosätenas behov kring auktorisation och grupphantering, och vilka förväntningar som finns på projektet.

Projektet har också arbetat på ett kapitel med begreppsdefinitioner, för att ha en kort beskrivning av begrepp inom området. En del av projekttiden har ägnats åt att beskriva två grupphanteringsverktyg (FIM och Grouper), och att göra en jämförelse mellan dessa. I det arbetet har vi haft stor hjälp av Uppsala universitet och Linköpings universitet, som använder alternativt planerar att använda dessa verktyg.

Projektet har också tagit fram use cases och user stories, för att visa på möjligheter/visioner med grupphanterare. Tanken är lärosäten som tänker jobba med dessa frågor kan utgå från projektets use cases och user stories.

Varje lärosäte utgår från sina förutsättningar, både tekniskt och verksamhetsmässigt. Resonemang och rekommendationer för grupphanteringsverktyg blir olika beroende på vilken ansats ett lärosäte har. Därför har vi arbetat med ett koncept kring tre olika scenarios för grupphantering; Small, Medium och Large. Antingen vill ett lärosäte göra mindre förändringar (Small), lite mer övergripande (Medium) eller helt genomgående förändringar som också innefattar identitetshanteringen (Large).

I november genomfördes en workshop på KTH med ca 25 deltagare från olika lärosäten. Vi fick då ytterligare material till relevanta user stories, och även uppslag till innehåll i projektets andra del, som ska genomföras under 2014. Resultatet efter workshopen är ett förslag på kapitelindelning för den ”kokbok” som projektet ska skriva. Kokboken är tänkt som en vägledning för lärosäten som vill förbättra sin behörighetshantering lokalt.

Under året har arbetet löpande dryftats med uppdragsansvarig och referensgrupp, som kommit med många synpunkter på materialet. Detta har varit värdefull hjälp till utredningen.

2.8 Presentation av resultat

I slutet av året har tidsbrist uppstått i projektet. Presentationen av resultatet kommer därför att delas upp i två delar.

I denna första del ingår följande dokumentation:

- Beskrivning med definitioner på begrepp inom behörighetshantering samt en övergripande beskrivning.
- Kartläggning av central hantering av behörigheter på de flesta svenska lärosäten, så som det ser ut våren 2013.
- Use cases, user stories och scenarios
- Första versionen av rekommendationer

I den andra delen, som levereras i januari 2014, ingår:

- Produktutvärdering av gruppverktygen Grouper och FIM

2.9 Målgrupp

IT-chefer, IT-arkitekter och de som arbetar med implementering.

3 Begrepp inom behörighetshantering

3.1 Kapitlets syfte

I detta kapitel beskrivs protokoll, verktyg, produkter och allmänna begrepp inom området. Informationen ska tjäna som en allmän områdesorientering. Syftet är därmed inte att endast definiera begrepp som används längre fram i utredningen.

Det har varit svårt att helt dra gränsen mellan autentisering och auktorisation, eftersom auktorisation implicit kan innebära även autentisering. Och det är svårt att diskutera auktorisation utan att beskriva autentiseringen. Inom kartläggningen innehåller flera svar t ex projekt inom autentisering. Därför finns även begrepp kring autentisering med i denna översikt.

3.2 Autentisering – auktorisation

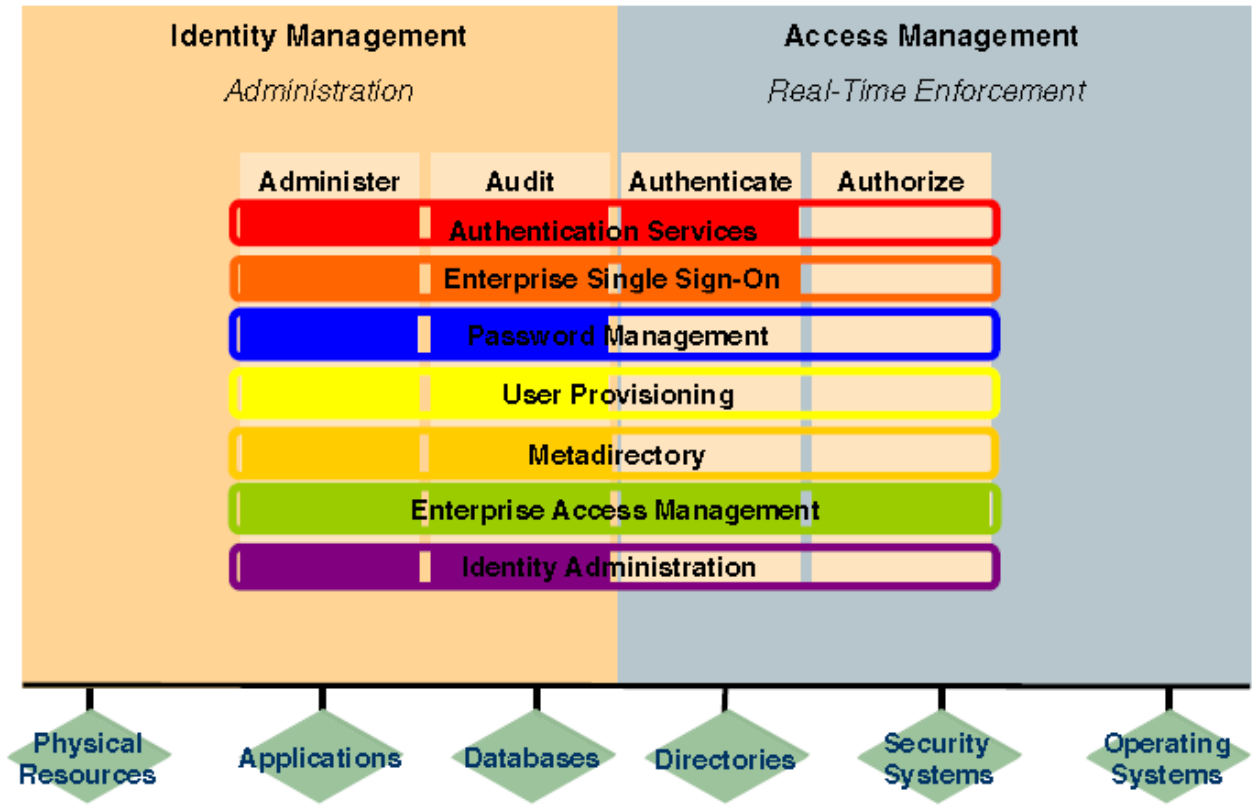
Med autentisering menas processen att identifiera en individ, baserat på någon av följande faktorer:

- Något individen har (kort, dosa)
- Något individen vet (lösenord, pinkod)
- Något individen är eller gör (fingeravtryck, signatur, röst)

Auktorisation innebär processen att verifiera om en autentiserad användare har behörighet att göra det den försöker göra. Auktorisation förutsätter därmed autentisering, om det inte är så att användaren tillåts vara anonym.

I en organisation krävs ett konsoliderat synsätt och sätt att hantera användarnas behörigheter på – det är administration. Organisationen behöver också veta säkert att aktiviteter som associeras med användarbehörighet (administration och realtidstillämpning) loggas i övervakande, undersökande och föreskrivna syften – detta är revision (audit). Dessa fyra faktorer (se figur 1) ingår i identitets- och accesshantering.

Figur 1



Källa: Gartner Research, Identity and Access Management Defined

Projektet “Kartläggning e-infrastruktur” fokuserade på lärosätenas processer för identitetsadministration och vilka verktyg som användes för autentiseringen. Detta projekt fortsätter på så vis där e-infrastruktur-projektet slutade; med att kartlägga hur lärosätena hanterar auktorisation.

3.2.1 Faktorer för auktorisation

Fem faktorer kan påverka auktorisation; vem har behörighet, vad har personen rätt att göra, varifrån, när och hur. Med dessa olika typer av begränsningar blir bilden av auktorisation ganska komplex.

3.2.2 Modeller för auktorisation

Det finns ett par olika typer av auktorisationsmodeller.

Role-based access control (RBAC)
Rollbaserad auktorisation är en metod för att styra behörighet till objekt utifrån roller. Behörigheten att utföra en viss arbetsuppgift tilldelas en viss roll. På detta sätt skapas en roll-struktur inom organisationen. Användare tilldelas roller utifrån deras plats i organisationen och deras ansvar inom organisationen. Roller kan kombineras i en hierarki där en roll på högre nivå summerar behörigheterna på lägre roller i hierarkin.

Attribute-based access controll (ABAC)
Attributbaserad auktorisation innebär att auktorisationen baseras på användarens attribut. Ett attribut innehåller någon slags information om användaren, t ex födelsedatum. En abac-policy specificerar vilka krav som måste uppfyllas, för att dela ut tillgången till objektet, t ex ”äldre än 18”. Accesshanteringen innebär att en användares attribut matchas mot objektets policy.

Policyn kan sättas upp så att användaren tillåts vara anonym.

ABAC är mer flexibelt än rollbaserad auktorisation. Attribut kan också bära mer information än det som handlar om behörighet, t ex e-postadress, fullständigt namn osv.

Discretionary access control (DAC)
Enligt DAC styr objektets ägare behörighetsnivån. Denna kan bestämma vem som har behörighet till objektet, och vilka rättigheter de har.

Mandatory access control (MAC)
Obligatorisk behörighetskontroll. Behörighet till ett objekt ges endast om det finns en regel som tillåter en viss användare att få tillgång till objektet. Kan användas när kraven på säkerhet är höga. För att styra behörigheten kan man märka objekten utifrån deras sensitivitet. Ett objekts märkning specificerar vilken nivå användaren minst behöver för att få tillgång. Kallas ibland non-discretionary access control, eftersom det kan sägas vara motsatsen till DAC.

3.2.3 Centraliserad hantering

Med centraliserad hantering av auktorisation menas att användarnas behörighetsuppgifter lagras centralt.

Att använda ett centralt system för att skapa grupper och/eller roller ger fördelen att uppgifterna kan användas i mer än ett system. Det blir mindre dubbellagring, än om man t ex använder en lokal kurstillfällesgrupp för att ge tillgång till lärplattformen, och en annan lokal kurstillfällesgrupp för att ge tillgång till lokaler. Tilldelning behöver bara utföras på ett ställe. Tilldelningen sker också på ett enda sätt, inte på olika sätt beroende på vilket system som avses. Auktorisation kan hanteras av färre administratörer. Det förekommer inte heller någon risk att samma person får flera användare till samma system.

En nackdel med centraliserad auktorisation (och autentisering) är att om användaruppgifterna hamnar i orätta händer, får den falske användaren också tillgång till den samlade behörigheten. Det är å andra sidan relativt enkelt att spärra behörighet och tillträde till systemen, när det hanteras centralt.

3.2.4 Automatiserad hantering

Med automatiserad hantering av auktorisation menas att användarnas behörighetsuppgifter skapas automatiskt.

Fördelen är främst tidsbesparingen av att skapa och underhålla grupper, samt att tillhörigheten utgår från ett utpekat källsystem.

Hanteringen av nyanställda kan effektiviseras, om behörigheter kan sättas med automatik utifrån t ex vilken organisatorisk enheten den anställde kommer att tillhöra, eller vilken yrkesroll denne kommer att ha. Motsvarande gäller i slutet på identitetens livscykel, d v s när en användare har slutat på lärosätet. Då är det viktigt att användarens alla systembehörigheter justeras. Om behörigheterna finns centralt lagrade underlättas detta arbete i stor grad. Hanteringen bör också helst vara automatiserad, för att undvika personberoende. Om behörigheterna ligger ute på varje enskilt IT-system, och ingen flaggning sker att behörighetsuppgifterna blivit inaktuella, kan behörigheterna finnas kvar en lång tid efter att användaren har slutat.

3.3 Begrepp A-Ö

ADFS
Active Directory Federation Services. Microsofts implementering av en IdP.

3.3.1 Användarprovisionering

Användarprovisionering (User Provisioning) omfattar skapandet, underhåll och terminering av användarobjekt och -attribut. Dessa kan existera i ett eller flera system, katalogen eller applikationer, som ett resultat av automatiserade eller interaktiva processer. Mjukvara för user provisioning kan omfatta en eller flera av följande processer; spridning av förändringar, arbetsflöde för användartjänster, centraliserad eller decentraliserad användaradministration, och federerad ändringskontroll. Användarobjekt kan representera anställda, studenter, konsulter, partners och andra mottagare av en tjänst. Tjänster kan t ex vara e-post, katalogtjänst, databasrättigheter, tillgång till nätverk, datorer mm.

Axiomatics
Axiomatics är ett företag med fokus på produkter runt fingraderad behörighetskontroll (Attribute-based Access Control). Företagets produkter och tjänster kretsar kring standarden XACML.

eduPerson LDAP Schema
eduPerson är ett LDAP-schema som hanterar vanligt förekommande personattribut inom högskolesektorn. Exempelvis eduPersonEntitlement, som kan användas för att hantera behörigheter som styrs centralt istället för i enskilda applikationer. Schemat har utvecklats av Internet2.

FIM
Forefront Identity Manager, Microsoft. I första hand en identitetshanterare, med diverse stöd för grupphantering. FIM utvärderas i detta projekt.

GMAI
GMAI - General Model for Authorization Information - är en modell för att beskriva behörigheter. Stöd för att hantera behörigheter centralt. GMAI använder sig av två eller fler informationsmängder; applikation/applikationsområde, roll/användartyp och begränsningar.

Grouper
Grouper är ett grupphanteringsverktyg som utvecklas och underhålls av the Internet2 Middleware Initiative. Ett av de verktyg som utvärderas i detta projekt.

Identitetsfederation
Samordnad identitetshantering (identitetsfederation) - när användares identitet fungerar i flera organisationers datasystem (webbaserade tjänster). Organisationerna utgör en identitetsfederation med gemensam inloggning. Identiteten omfattar användarnamn, lösenord och eventuellt också behörighet. Användaren behöver alltså bara logga in på en organisations webbsida så kan hon sedan gå vidare till en annan organisations webbsida utan att behöva logga in där också. Detta är särskilt användbart i så kallade web services där flera organisationers tjänster kan kopplas ihop. T ex man beställer något på en webbsida och blir sedan direkt länkad till bankens webbsida där man betalar.

IdP
Identity Provider, identitetsutgivare. Utfärdar elektroniska identiteter och knyter dessa till fysiska personer.

IETF
The Internet Engineering Task Force. En organisation för öppen standard, inga formella medlemskrav. Utvecklar Internet-standarder, specifikt för TCP/IP.

Internet2
Internet2 är ett amerikanskt konsortium av lärosäten, industri och myndigheter. De utvecklar och distribuerar applikationer och tekniker inom många områden, bl a auktorisation.

LoA Förtroendenivåer för identitetskontroll
Level of Assurance. Förtroendenivåer med utgångspunkt utifrån med vilken säkerhet en utlämnare av en elektronisk identitet kan verifiera mottagarens identitet. Det finns fyra LoA-nivåer, där den lägsta (LoA1) ger liten eller ingen möjlighet att fastställa vem som innehar och använder en elektronisk identiet, ex Facebook. Högsta nivån (LoA4) ger mycket god möjlighet för detta, gm kontroll av giltig identitetshandling, som pass, körkort el dyl.

OASIS
The Organization for the Advancement of Structured Information Standards (OASIS). Globalt konsortium som driver utveckling, samarbete och spridning av standarder för e-business och webb-tjänster.

OAuth
Open Authorization (OAuth) – är ett protokoll för säker auktorisation. Det är en metod för användare att ge andra tillgång till deras resurser utan att behöva lämna ut sitt användarnamn och lösenord till den andra tjänsten. I stället skapas en speciell nyckel (teckenserie, på engelska tokens). Nyckeln kan sedan användas för att via andra tekniska lösningar ge den ena tjänsten möjlighet att komma åt viss information på den andra tjänsten. OAuth 2.0 utvecklas av IETF.

OpenID
System som låter användarna logga in på många webbsidor med ett gemensamt lösenord. Användarens identitet knyts till en av de webbplatser, identifieraren, som användaren har användarnamn och lösenord till. (Webbplatsen måste vara med i OpenID.) När användaren vill logga in på en annan webbplats, hänvisaren, som också är med i OpenID kontrollerar hänvisaren att användaren kan logga in på identifieraren. I så fall släpps användaren också in på hänvisarens webbplats. De flesta stora it-företag och webbtjänster stöder OpenID. Systemet är skrivet i öppen källkod och utvecklas av OpenID Foundation.

OpenID Connect
OpenID Connect är en profilering av OAuth, med utökad information om själva autentiseringen. Hur gick den till, när gjordes den. Det finns även tillgång till mer information om användaren. Nyckeln från OAuth kan användas för att komma åt information om användaren, t ex namn, epost-adress, men även behörighetsroller och -attribut. Utvecklas av OpenID Foundation.

Provisionering
Provisionering innebär konfiguration av system för att ge användare, resurser och tjänster access till data och tekniska resurser. Det omfattar alla typer av informationsresurser i ett företag.

SAML
Security Assertion Markup Language är ett XML-ramverk för att kommunicera autentiserings- och behörighetsinformation. SAML fokuserar på tre typer av information:

- Autentisering
- Attribut (information om användaren)
- Behörigheter

Ett typiskt användningsområde för SAML är SSO. Det finns tre versioner av SAML, V1.0, V1.1 och V2.0. SAML underhålls av OASIS, som också har definierat det som en standard.

SCIM
System for Cross-domain Identity management. Hantering av användaradministration i molnet. En definition av ett schema över hur användare och grupper ska representeras, samt ett REST API för alla nödvändiga CRUD-operationer. Utvecklas av IETF.

Shibboleth

En IdP, baserad på SAML, utvecklas av Internet2.

simpleSAMLphp

En IdP, implementation av SAML. Utvecklas av UNINETT.

SPML
SPML - services provisioning markup language - språk för beskrivning och hantering av informationsförsörjning i företag och myndigheter. SPML ska ge möjlighet att automatiskt ange vilka användare eller datorer som ska ha tillgång till viss elektronisk information och att ändra och återkalla sådana rättigheter. Detta ska kunna göras med ett enda SPML-meddelande även om det gäller många informationskällor. SMPL bygger på XML och har utvecklats inom OASIS.

SPOCP
Simple Policy Control Protocol (SPOCP) är en regelmotor för auktorisation. Den har utvecklats av Swami.

SSO
Single sign-on (SSO) – är ett samlingsnamn för tekniker för samlad inloggning, d v s när användaren bara behöver ange användarnamn och lösenord en gång för att logga in på flera lösenordsskyddade program eller webbsidor under ett arbetspass. Efter den första inloggningen ser ett centralt program i nätet till att användaren kommer åt alla resurser på nätet som hon har behörighet till. Kallas också för singelinloggning och enkelinloggning. Skillnaden gentemot gemensam inloggning är att samlad inloggning främst är till för att underlätta för en anställd att använda företagets applikationer. Gemensam inloggning är ett samarbete mellan organisationer för att underlätta för användare. Det finns alltså ingen skarp gräns.

SURFConext Teams
SURFTTeams är en holländsk tjänst för att skapa virtuella organisationer baserade på medlemmar i en identitetsfederation. Grupperna som skapas har tillgång till samarbetsplattformen SURFConext. Till exempel kan forskargrupper bestående av medlemmar från flera lärosäten bildas och få tillgång till diverse samarbetsverktyg online. En federerad medlem kan skapa en grupp genom inbjudan och själv administrera gruppen eller dela ut rättigheter i form av roller till andra gruppmedlemmar. En rad tjänster finns till hands för grupperna inom ramen för SURFConext:.

- Webbplats
- Videokonferenser
- Dokumentdelning
- Diverse gadgets
- Epostlistor
- Wikis

Mjukvaran för grupphanteringen i Teams är Internet2s Grouper.

SWAMI
Tidigare underorganisation till SUNET. Föregångare till SUNET Inkubator.

SWAMID
Swedish Academic Identity. En identitetsfederation för forskning och högre utbildning i Sverige. De flesta lärosäten är medlemmar.

The Kantara Initiative organization
En sammanslutning som arbetar med innovationer inom identitets- och auktorisationshantering.

VOOT
Virtual Organisation Orthogonal Technology är ett protokoll som används för att kommunicera grupper. VOOT är i första hand tänkt för att hantera virtuella organisationer baserade på identitetsfederationer inom forskning och utbildningssektorn. VOOT specificerar autentisering med hjälp av OAuth protokollet och innefattar ett fåtal tjänster för att hämta listor på grupper, medlemmar i grupper osv.

UMA
User Managed Access (UMA) är ett ramverk för behörighetshantering. En användare som vill ge en internetbaserad tjänst tillgång till användarens information på en annan tjänst, ska själv kunna styra vilka behörighetsuppgifter som tjänsten får tillgång till. Det innehåller också funktionalitet för att den klient som frågar en resursserver ska förstå de argument som kommer UMA bygger på OAuth 2.0. The Kantara Initiative organization utvecklar protokollet, och arbetar för att UMA ska bli en standard.

UNINETT
Norges motsvarighet till Sunet.

XACML
Extensible Access Control Markup Language (XACML)– är ett programspråk för beskrivning av behörighet för inloggade användare i datorsystem. XACML ger stöd för attributbaserad behörighetshantering. Det är en tillämpning av XML och utvecklas av OASIS, som även har definierat det som en standard.

4 Om grupphantering

Uppsala universitet har delat med sig av underlaget till detta kapitel.

4.1 Typer av grupper

Generellt finns två typer av basgrupper. Automatiskt och manuellt skapade grupper.

Automatiska grupper kan identifieras och skapas maskinellt genom de attribut som finns kopplade till identiteterna i olika kärnsystem. Automatiska grupper kan också ges diverse individ- och gruppattribut från kärnsystem.

En automatiskt skapad grupp kan vara anställda vid en organisatorisk enhet, till exempel en institution. Genom systemintegration kan gruppen skapas och underhållas automatiskt över tid. Nyanställda läggs till i gruppen och vid avslutad anställning tas en person bort via logik i en integrationsplattform. Gruppattributen organisationsid och organisationsnamn kan också sättas och underhållas automatiskt.

Andra exempel på automatiskt skapade grupper

- Grupper baserade på studenter som läser samma kurstillfälle, kurs, program etc.
- Funktionella grupper med medlemskap utifrån innehav av funktion i ett system, t.ex. en grupp för alla katalogadministratörer.
- Platsbaserade grupper med medlemskap utifrån arbetsplatsplacering, t.ex. alla som har sin arbetsplats i Hus A.

En manuellt skapad grupp skapas och underhålls genom att en användare väljer personer som skall inkluderas i eller exkluderas från gruppen. Ett exempel kan vara att ett antal personer bildar en arbetsgrupp.

Det finns också andra exempel på hur grupper skapas:

- Intressegrupper med öppet medlemskap
- Grupper med medlemskap genom riktad inbjudan

4.2 Stammar, hierarkier och undergrupper

Erfarenheter att implementera grupphantering pekar på att antalet grupper snabbt tenderar att bli många. Därför behövs det möjlighet att organisera grupper på ett logiskt och transparent sätt. En stam (jämför rot i ett filsystem) kan utgöra antingen toppen i en hierarki eller tematisk behållare för grupper med någon slags släktskap. Till exempel kan stammen ”anställda” innehålla grupper ordnade efter hierarki. Informatikinstitutionen skulle till exempel vara en undergrupp till den samhällsvetenskapliga fakulteten. I stammen ”Diverse” kan kortlivade intressegrupper läggas.

4.3 Användningsområde

Grupper kan användas för auktorisation, men även för att sprida information.
Exempel på användning av grupper för information:

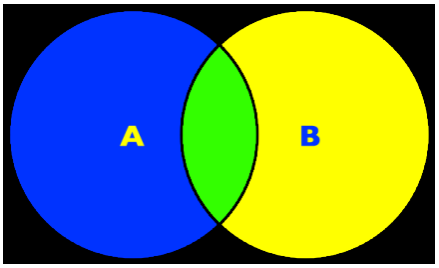
- En institution vill kunna informera alla andra på institutionen.
- Fakultetskansli vill kunna nå de som jobbar på fakultetens institutioner.
- En lärare vill kunna informera alla studenter på ett kurstillfälle.

4.4 Sammansatta grupper och mängdoperationer

Användare av ett grupphanteringsverktyg behöver sannolik kunna skapa grupper baserat på existerande grupper och individer. Den enklaste varianten är att två grupper slås ihop och bildar en tredje gemensam grupp. Men grupper kan också skapas genom andra mängoperationer, annan logik eller manuella tillägg av individer i en befintlig grupp.

4.4.1 Mängdoperationer

- Union (A _ B): Ger en grupp som innehåller medlemmarna av både grupp A och grupp B, d.v.s. blått, grönt och gult område.
- Snitt (A _ B): Ger en grupp som innehåller de som är medlemmar i både grupp A och grupp B, d.v.s. grönt område.
- Komplement (A – B): Ger en grupp som innehåller alla som är medlemmar i grupp A men inte i grupp B, d.v.s. blått område.



4.5 Attribut, roller och behörighet

Förutom stammar, grupper och individer behöver ett grupphanteringsverktyg kunna hantera andra objekt för att vara effektivt på stora populationer.

- Attribut: Objekt eller egenskap som kan knytas individ, grupp eller roll.
- Behörighet: Vem som får göra vad med vilken resurs.
- Roll: Gruppering av en eller flera behörigheter (och eller medlemskap, attribut osv)

4.6 Medlemmar

I grupphanteringssammanhang kallas personer (eller identiteter) för medlemmar. Medlemmar kan ha olika ursprung.

- Lokala användare vid ett lärosäte
- Federerade användare via SWAMID och andra federationer
- Externa användare via externa inloggningstjänster t.ex. Google Accounts, Windows Live ID, Facebook etc.
- Externa användare utan konto vid extern inloggningstjänst

4.7 Attribut kopplat till en grupp & individ

Vilka attribut som kopplas till en grupp beror sannolikt på hur gruppen skall användas. Generellt är dock minimikravet:

- Grupp id (teknisk nyckel)
- Gruppnamn
- Behörigheter/rättigheter för att administrera gruppen

Andra attribut som kan vara nödvändiga för en grupp

- Beskrivning av gruppen
- Grupper som gruppen består av
- Grupp som gruppen är en del av
- Datumstyrning av gruppens existens
- Beskrivning av (logisk) regel för inkludering i gruppen
- Roller som finns i gruppen

Attribut kopplade till individer kan också vara intressant för grupphantering

- Individens roll i gruppen
- Datumstyrning av individens existens i gruppen
- Individens behörighet/rättighet i gruppen
- Individens urspungsgrupp (vid grupp i grupp)
- Alla grupper som individen är medlem i

5 Kartläggning av svenska lärosäten

För att kartlägga nuläget på svenska universitet och högskolor har projektet skickat ut en enkät om hur man arbetar med behörighetshantering lokalt idag, samt vilka behov som finns.

I listan nedan presenteras alla utbildningsanordnare, våren 2013. De som är markerade med fet stil har fått enkäten. Från dessa lärosäten inkom 22 svar. Som nämndes i kapitel 2, så har begränsningen av lärosäten kopierats från projektet ”Kartläggning e-infrastruktur”.

Utbildningsanordnare med rätt att utfärda svenska examina (maj 2013):

1. Beckmans designhögskola, Sthlm
2. **Blekinge tekniska högskola, Karlskrona**
3. **Chalmers tekniska högskola, Gbg**
4. Dans- och cirkushögskolan, Sthlm
5. Ericastiftelsen, Sthlm
6. Ersta Sköndal högskola, Sthlm
7. Evidens AB, Gbg
8. Försvarshögskolan, Sthlm
9. Gammelkroppa skogsskola, Filipstad
10. Gymnastik- och idrottshögskolan, Sthlm
11. **Göteborgs universitet**
12. **Handelshögskolan i Stockholm**
13. **Högskolan i Dalarna, Borlänge/Falun**
14. **Högskolan i Borås**
15. **Högskolan i Gävle**
16. **Högskolan i Halmstad**
17. **Högskolan i Jönköping**
18. **Högskolan i Skövde**
19. **Högskolan i Kristianstad**
20. **Högskolan på Gotland, Visby**
21. **Högskolan Väst, Trollhättan**
22. Johannelunds teologiska högskola, Uppsala
23. **Karlstads universitet**
24. **Karolinska institutet, Sthlm**
25. Konstfack, Sthlm
26. Kungliga Konsthögskolan, Sthlm
27. Kungliga Musikhögskolan, Sthlm
28. **Kungliga Tekniska Högskolan, Sthlm**
29. **Linköpings universitet**
30. **Linnéuniversitetet, Kalmar/Växjö**
31. **Luleå tekniska universitet**
32. **Lunds universitet**
33. **Malmö högskola**
34. **Mittuniversitetet, Sundsvall/Östersund/Härnösand**
35. **Mälardalens högskola, Västerås/Eskilstuna**
36. Newmaninstitutet, Uppsala
37. Operahögskolan i Stockholm
38. Röda korsets högskola, Sthlm
39. Sophiahemmet högskola, Sthlm
40. Stockholms Akademi för Psykoterapiutbildning
41. Stockholms dramatiska högskola
42. Stockholms Musikpedagogiska institut
43. **Stockholms universitet**
44. Svenska institutet för kognitiv psykoterapi
45. **Sveriges lantbruksuniversitet, Uppsala m.fl**.
46. **Södertörns högskola, Sthlm**
47. Teologiska Högskolan Stockholm
48. **Umeå universitet**
49. **Uppsala universitet**
50. Örebro Teologiska Högskola
51. **Örebro universite**

5.1 Nuläge

Först och främst ville vi veta vilka verktyg som används för den centrala behörighetshanteringen. Nästan alla, 85 %, använder AD som ett av sina verktyg och LDAP nämndes i åtta av svaren. Relativt många har utvecklat eget stöd för delar av behörighetshanteringen, knappt 70 %. Många lärosäten hanterar grupper på mer eller mindre avancerad nivå, t ex med hjälp av integration med AD, andra har separata lösningar.

Hur hanteras behörigheter till t ex LMS, intranät och passagesystem? Detta är system där man kan använda grupper/roller i en centraliserad lösning. Studentgrupper lagras ofta internt i LMS:et, även om grupperna automatgenereras centralt. Anställdas tillgång till intranätet hanteras ofta genom autentisering mot lärosätets källsystem. Specifika roller i intranätet, t ex webbredaktör, fördelar svaren ganska jämnt mellan central/lokal hantering. Hälften av de svarande kan lagra sådan behörighet i en central applikation, den andra hälften sätter behörigheten lokalt i intranätet.

Vad gäller passagesystemen så överför drygt hälften av de svarande sina uppgifter om studenter och personal automatiskt från PA-system och Ladok. Resten har svarat att behörighetssättning för passage sker manuellt och internt i systemet.

Angående behörighet till HR-systemet, så svarar hälften att uppgifter hämtas från AD/LDAP, resterande hanterar det internt i personalsystemet. Ekonomisystemet utmärker sig genom sin isolerade hantering, drygt 80 % har helt intern behörighetstilldelning. Även för Ladok sker tilldelningen i systemet. Dessa system kännetecknas av feta klienter, där det är ett större steg att centralisera behörigheter jämfört med webbklienter.

En slutsats är att för många lärosäten så är det mycket vanligt med systemintern hantering av behörigheter.

Hälften av de u/h som svarat använder GMAI för NyA institutionswebben, men inte till något annat system. Tre lärosäten har implementerat GMAI för flera system och två av dessa uttrycker också att det är deras policy att använda GMAI för behörighetshantering där det är tillämpligt.

35 % saknar policy för behörighetshantering. De som har riktlinjer tycker att de uppfylls i ganska god utsträckning. Som undantag nämndes stora inköpta system med feta klienter.

5.2 Behov

Uppfyller nuvarande lösning de behov som finns? Hälften tycker att lösningen uppfyller behoven, även om det finns vissa saker som kunde fungera bättre. Sex lärosäten svarar ”Ja”, men flera av dessa lade dock till ”för närvarande” och liknande formuleringar. De återstående fyra svarade ”Nej”.

Vilka är behoven? 9 av 10 anger behov av finjusterade behörigheter, ex roll i enskilda applikationer utifrån funktion i organisationen. Utredningens förslag på användningsfall listades, och de viktigaste bedöms vara manuell undergrupp, öppen grupp och sammanslagen grupp.

I fritextsvaret på denna fråga ligger ”externa intressenter” i topp. Grupphantering till inpassering, bättre koll på livscykeln för rättigheter samt default bas-behörighet till anställda är också med på listan.

Nästan hälften av de svarande u/h har en mer eller mindre uttalad vision kopplad till grupphantering och auktorisation. Många u/h har pågående eller planerade projekt med anknytning till identitets-, behörighets- eller grupphanteringen.

En mer utförlig sammanställning av enkätsvaren finns bakom inloggning på portal.nordu.net.

6 User stories – Användningsfall - Scenarios

I detta kapitel konkretiseras grupphantering. Här visas exempel på vad grupphanteringssystem kan användas till i from av user stories. Användningsfallen visar vilka schematiska funktioner som finns runt grupphantering. De representerar med andra ord de pusselbitar som behöver kombineras för att realisera olika user stories.

Scenarios är exempel på omfattningar av implementationer av grupphantering vid ett universitet. Naturligtvis finns det ett oändligt antal tänkbara scenarios i verkligheten. I rapporten presenteras tre stycken. Small, medium och large. En diskussion förs runt de erfarenheter och idéer som samlats i verkligheten av olika lärosäten givet storlek och ambitionsnivå på deras satsningar.

Det finns en röd tråd mellan user stories, användningsfall och scenarios. Ett scenario består av ett antal user stories. En user story består i sin tur av ett antal användningsfall.

Låt säga att beslut tas att starta ett projekt för att införa grupphantering. Projektets omfång definieras sannolikt genom vilka user stories som skall införas, som i sin tur ger att ett antal användningsfall måste realiseras.

6.1 User stories

Antalet tänkbara user stories kopplade till grupphantering i U/H-världen är förmodligen närmast oändlig. Här presenteras ett antal med koppling till typiska behov runt verksamheten på ett lärosäten.

6.1.1 Mail

”Institutionssekreteraren Edvin Edvinsson behöver hålla kontakten med klassen SVP15H (Systemvetenskapligt program med start höstterminen 2015) i syfte att stimulera studenterna att jobba mot en examen. Edvin vill till exempel maila erbjudanden om nya kurser vid institutionen eller påminna om att det är dags att välja kurser inför nästa termin.”

Efter ett par år är klassen mer eller mindre spridd för vinden. Olika kursval, avhopp, inhopp, pauser och utlandsstudier mm gör att det är svårt att ha en överblick över klassen. Men när klassen började progamet 2015 skapades automatiskt en kullgrupp för SVP15H (UC 3.1.1). Edvin har inte tagit bort någon ur gruppen (utom de som uttryckligen sagt till) däremot har han manuellt lagt till ett par fristående studenter som velat ansluta sig till klassen. Gruppen finns i universitetets grupphanterare och synkroniseras med AD:et. Därför kan Edvin enkelt nå klassen via en mailgrupp.

”Budgetsamordnaren Erika Eriksson på fakultetskansliet behöver informera prefekterna inom fakulteten om det kommande budgetarbetet, vilka datum som gäller och vilken information som institutionerna förväntas lämna.”

I universitetets katalogtjänst finns en prefektroll och i grupphanteringssystemet finns en fakultetsintern grupp som innehåller de personer som innehar denna roll. Gruppen uppdateras automatiskt när någon person börjar eller slutar som prefekt, vilket markeras genom att personen tilldelas rollen i katalogtjänsten (UC 3.1.1). Genom att använda den gruppen som maillista kan Erika alltid nå prefekterna inom fakulteten.

”Kursansvarige Knut Knutsson vill kunna maila alla alumner på sin avslutade kurs för att få synpunkter på kursens utformning.”

Alla studenter som deltar i ett kurstillfälle sparas som en grupp i grupphanteringssystemet. En kurstillfällesgrupp blir också en mailgrupp.

6.1.2 Passagesystemet

”Studenten Per Persson vill ha tillträde till de lokaler på universitetet där hans kurser hålls.”

När Per registrerar sig på ett kurstillfälle inkluderas han som medlem i en kurstillfällesgrupp i grupphanteraren. Detta sker med hjälp av systemintegration mellan LADOK- och grupphanteringssystemet (UC 3.1.1). En annan applikation på universitetet matchar kurstillfällesgruppen (UC 3.2.6) med de lokaler där kursen hålls. Passagesystemet får informationen att Per Persson passerkort (och alla andra studenter i kurstillfällesgruppen) är giltigt för passage till lokalerna under den tid som kurstillfället ges. Dessutom har Per tillgång till alla huvudentréer på universitetet eftersom han tillhör gruppen studenter.

”Doktoranden Patricia Patriksson vill ha tillträde till superdatorlabbet på sin institution”

Eftersom Patricia tillhör gruppen forskarskarstuderande på datavetenskapliga institutionen kan administratören Anders Andersson lägga till henne i undergruppen superdatorforsning (UC 3.2.1). Patricia är också medlem i gruppen anställda vid datavetenskap. Att hon finns i gruppen anställda ger passagerättigheter till alla entréer. Medlemskapet i gruppen forskarstuderande på D.V.I. ger rättigheter till institutionens ytterdörrar och medlemskapet i undergruppen gör att hon kommer in i superdatorlabbet.

”Ekonomiassistenten Peder Pedersson jobbar på universitetets centrala förvaltning. Men är under höstterminen tillfälligt utlånad till institutionen för nordiska språk på halvtid. Peder måste komma in på två arbetsplatser”

Passagerättigheterna till Peders ordinarie arbetsplats är inget problem då han är medlem i gruppen anställda vid centrala administrationen. Men att få tillträde på nordiska språk kommer inte att ske per automatik eftersom Peder inte har någon anställning där, han är bara utlånad. Administratören Anders Andersson får en idé, han lägger manuellt till en undergrupp till anställda på nordiska språk(3.2.1). Han kallar gruppen Gäster htXX och låter den ärva alla rättigheter. Anders ser för säkerhets skull till att gruppen bara existerar under htXX (UC 3.2.4).

6.1.3 Intranätet, studentportalen & LMS

”Inge Ingesson jobbar på informationsavdelningen och behöver ha tillgång till alla delar av intranätet som innehåller information för personal. Han är också redaktör för den del av intranätet som innehåller avdelningens egna intranät”

Eftersom Inge är medlem i gruppen anställda vid informationsavdelningen och är avdelningens redaktör och detta finns representerat som GMAI i universitetets katalogtjänst, kommer Inge per automatik att ha rätt behörigheter tack vara universitetets SSO inloggning. På universitet har man med hjälp av systemintegration sett till så att alla anställdas position i organisationen och vissa specifika roller kopplade till ett antal allmänna system hämtas i grupphanteringssystemet och tolkas om till GMAI syntax för att sedan skrivas ner i LDAP. Inge är medlem i flera rollgrupper och har en del begränsningar kopplat till sin identitet i grupperna.

- Katalogansvariga (får bara hantera anställda i sin egen organisation)
- Intranätpublicister (får bara hantera avdelningens information)
- Fakturamottagare (Attest- och konteringsbehörighet upp till 100 000 kr)

”Lars Larsson är student och tänker ta en magisterexamen i Informatik. Lars läser lite olika kurser över tid. Han blandar hel- och halvfartskurser på olika institutioner, vissa läser han på distans. Lars behöver tillgång till all information runt de kurser han läser i universitetets LMS.”

Den mesta informationen runt kurserna, labbuppgifter, litteraturlistor, deltagarlista, kontaktinformation till lärare och scheman mm finns upplagda i universitetets LMS. Lars får automatisk behörighet till informationen runt en kurs genom att registrera sig på ett kurstillfälle. Han hamnar då i en kurstillfällesgrupp som LMS:et använder för att verifiera Lars identitet och ge behörigheter när han loggar in. LMS:et publicerar också deltagarlistor för varje kurs baserat på kurstillfällesgrupperna i grupphanteraren.

”Studenten Sven Svensson ska ha tillgång till sitt personliga schema med både föreläsningar och labbkurser.”

Schema för kursen läggs in i schemasystemet. Via uppgifter om deltagarna i kurstillfällesgruppen som hör till kursen, kan schemat visas för studenterna i studentportalen. Läraren kan skapa undergrupper till kurstillfällesgruppen i LMS:et, t ex för labbgrupper. Dessa kan också schemaläggas i schemasystemet, och visas för studenten i studentportalen.

"Studenten Jonas Jonasson praktiserar på ett sjukhus, hans handledare är Filippa Philipsson. Hon är inte anställd av lärosätet. Handledaren behöver åtkomst till LMS:et för att kunna rapportera studentens insats.”

Filippa får tillgång till epostlistan för kurstillfällesgruppen och läggs in som administratör av kurstillfällesgruppens samarbetsyta i LMS:et.

”Studenten Ove Ovesson på lärosäte X läser en kurs som hålls av lärosäte X och Y tillsammans. Kursen presenteras i lärosäte Y:s LMS. Studenten behöver åtkomst till LMS på lärosäte Y.”

Kursansökan sker till lärosäte X. Det innebär att lärosäte X har uppgifter om kursdeltagare, och en grupp för kurstillfället. En federerad grupp skapas på en lärosätesgemensam plattform. I plattformen sätts rättigheter för gruppen. Gruppen (identiteter plus gemensamma rättigheter) importeras av lärosäte Y som slår ihop X-gruppen med de studenter som läser samma kurs på lärosäte Y. Detta ger att studenterna från lärosäte X kan logga in med sina befintliga identiteter. Ett exempel där både federerade identiteter och federerad grupphantering används.

6.1.4 Forskargrupper & samarbetsytor

”Fredrika Fredriksson sysslar med nischad forskning och vill dela sitt arbete och resultat med ett fåtal forskarkollegor runt om i Sverige. Fredrika publicerar fortlöpande sina framsteg på en wiki och i en blogg som kräver inloggning i universitetets intranät.”

Universitetets grupphanteringssystem ger möjligheten att skapa en grupp och skicka riktade inbjudningar. Fredrikas forskarkollegor får ett mail där de erbjuds medlemskap i hennes grupp. Kollegorna tackar ja genom att klicka på en länk i mailet. Kollegornas mailadresser och identiteter finns tillgängliga genom identitetsfederationen SWAMID. Detta gör att kollegorna inte behöver några speciella inloggningsuppgifter för att ta del av Fredrikas publikationer. Det räcker med att de är inloggade i sin egen organisations SSO.

”Martin Martinsson leder en internationell forskargrupp som behöver tillgång till rad delade tjänster. Forskarna behöver en delad webbplats för delade dokument, wikis, videokonferenser mm.”

Eftersom en av forskarna i Martins grupp är holländare har Martin hört talas om SURFTeams, vilket är en tjänst för att skapa virtuella organisationer baserade på medlemmar i en identitetsfederation. Grupperna som skapas har tillgång till samarbetsplattformen SURFConext. Till exempel kan forskargrupper bestående av medlemmar från flera universitet bildas och få tillgång till diverse samarbetsverktyg online. En federead medlem kan skapa en grupp genom inbjudan och själv administrera gruppen eller dela ut rättigheter i form av roller till andra gruppmedlemmar. En rad tjänster finns till hands för grupperna inom ramen för SURFConext, till exempel:

- Webbplats
- Wikis
- Videokonferenser
- Dokumentdelning

”Petra Pettersson leder en forskningsgrupp med deltagare från tre lärosäten och ett par företag, bl a Ericsson. Forskningsprojektet finansieras av Ericsson. De behöver en gemensam arbetsyta för forskardata och arbetsmaterial.”

Kollegornas identiteter finns tillgängliga genom identitetsfederationen SWAMID. Detta gör att kollegorna inte behöver några speciella inloggningsuppgifter. Det räcker med att de är inloggade i sin egen organisations SSO. Företagen kommer med största sannolikhet inte att vara intresserade av en federerad hantering för sina användare, så för dem är det enklast att lägga upp konton på ett av lärosätena.

6.2 Användningsfall

Nedan följer de användningsfall som identifierats runt grupphantering. Användningsfallen visar vilka schematiska funktioner som finns runt grupphantering. De representerar med andra ord de pusselbitar som behöver kombineras för att realisera olika user stories.

Användningsfallen är de uppdelade i tre kategorier.

- Första delen handlar om hur grupper skapas, d.v.s. hur grupphanteraren fylls på med grupper.
- Andra delen handlar om hantering av befintliga grupper i grupphanteraren. Här finns också användningsfall runt hur man skapar nya grupper av existerande grupper.
- Tredje delen fokuserar på export av grupper, d.v.s. till vad och hur grupperna används.

En user story består typiskt av en portion från respektive kategori. En grupp skapas på något sätt, den hanteras i grupphanteraren och gruppen tillämpas i någon applikation.

6.3 Del 1 - Skapa grupper

6.3.1 UC Skapa grupp maskinellt

NAMN	UC Skapa grupp maskinellt
BESKRIVNING (KORT)	Grupper skapas genom maskinellt urval och systemintegration.
VEM (ROLLER)	Administratören kan administrera basgruppen
MOTIV	• Det finns många tänkbara grupper som kan skapas på det här sättet. Möjligheter och begränsningar styrs av vilka attribut som finns tillgängliga för urvalet av individer via systemintegration. • Ett exempel är studenter som läser samma kurs, en kurstillfällesgrupp. • Gruppen kan användas för maillistor, behörighetsstyrning av LMS eller andra system som behövs under kursen.
FÖRUTSÄTTNINGAR	• Grupphanteringssystemet har ett API för att skapa och underhålla grupper. • Systemintegration: I exemplet ”kurstillfällesgrupp” hålls gruppen uppdaterad givet vilka studenter som är registreras eller avregistreras på kurstillfället i LADOK.
HÄNDELSEFÖRLOPP	• Gruppen skapas när ett nytt kurstillfälle läggs upp i LADOK. • Gruppen namnges automatiskt, till exempel efter den nyckel som specificerar kurstillfället. • Studenter inkluderas eller exkluderas automatiskt allt eftersom de registrerar eller avregistrerar sig i LADOK.
VARIANTER	• På samma sätt går det att skapa hierarkier av grupper, stammar, undergrupper etc. • Andra varianter på grupper kan vara intressantare: Studenter som är antagna till ett kurstillfälle, studenter med samma starttermin på ett program som bildar en klass etc. • Grupper kan importeras från LDAP eller AD om de redan existerar där.
RESULTAT/UTGÅNGLÄGE	En grupp är skapad och underhålls maskinellt allt eftersom den förändras.

6.3.2 UC Skapa grupp manuellt

NAMN	UC Skapa grupp manuellt
BESKRIVNING (KORT)	Grupper skapas genom manuellt urval ur en IDP.
VEM (ROLLER)	Alla tillgängliga individer kan knytas till gruppen, administratör blir per default den som skapar gruppen.
MOTIV	Det finns många skäl att skapa grupper manuellt: Till exempel intressegrupper, behörighetsgrupper som inte går att skapa automatiskt med hjälp av systemintegration.
FÖRUTSÄTTNINGAR	Att grupphanteringssystemet kan kopplas ihop med en IDP där urval kan göras.
HÄNDELSEFÖRLOPP	• Administratör av grupphanteringsystemet namnger den grupp som skapas. • Administratören sätter tidsintervall för gruppen existens eller andra gruppattribut. • Gruppen fylls på med de aktuella medlemmarna. • Administratören kan utse ytterligare medlemmar i gruppen till administratörer. • Administratören kan inkludera eller exkludera medlemmar i gruppen med tiden.
VARIANTER	• Grupper kan skapas med urval ur federerade IDP:er. • Genom grupphanteringsystemets API kan grupper skapas från andra applikationer.
RESULTAT/UTGÅNGLÄGE	• En grupp är skapad och underhålls manuellt allt eftersom den behöver förändras.

6.3.3 UC Skapa en grupp genom inbjudan

NAMN	UC Skapa grupp genom inbjudan
BESKRIVNING (KORT)	Individer bjuds in till att bli medlemar i en grupp.
VEM (ROLLER)	Administratören skapar gruppen och väljer vem som erbjuds gruppmedlemskap.
MOTIV	Ett sätt att med hjälp av automatik skapa en riktad intressegrupp.
FÖRUTSÄTTNINGAR	Att grupphanteringssystemet i så hög grad som möjligt stöder processen nedan.
HÄNDELSEFÖRLOPP	• En administratör gör på något sätt ett urval (på individ eller gruppnivå) av potentiella medlemmar till en grupp. • En inbjudan om medlemskap skickas till de potentiella medlemmarna (via email). • De som tackar ja inkluderas i gruppen. • Flera förfrågningar skall kunna skickas till samma person över tid. • Nya individer skall kunna läggas till som potentiella medlemmar.
VARIANTER	• Beroende på syftet med gruppen, d.v.s. vilka behörigheter som gruppmedlemskapet skall ge, finns olika krav på medlemmarnas identitet. Inbjudningarna kan baseras på medlemmarna finns i en lokal IDP, federerade IDPer, eller bara att den som skapar gruppen känner till en mailadress etc. • Funktionen kan sannolikt byggas i en annan applikation än grupphanteringssystemet.
RESULTAT/UTGÅNGLÄGE	Grupper skapas där medlemmarna har bekräftat att de vill vara medlemmar.

6.3.4 UC Skapa en öppen grupp

NAMN	UC Skapa en grupp genom anmälan
BESKRIVNING (KORT)	I öppna grupper kan medlemmar själv välja att inkludera eller exkludera sig.
VEM (ROLLER)	Administratören skapar en öppen grupp, medlemmar anmäler sig till gruppen.
MOTIV	Ett sätt att med hjälp av automatik skapa en öppen intressegrupp.
FÖRUTSÄTTNINGAR	• Att grupphanteringssystemet i så hög grad som möjligt stöder processen nedan.
HÄNDELSEFÖRLOPP	• En grupp skapas av en administratör. • En offentlig inbjudan går ut på något sätt. • Den som vill inkluderar sig i gruppen. • Den som vill exkluderar sig från gruppen.
VARIANTER	• Funktionen kan sannolikt byggas i en annan applikation än grupphanteringssystemet.
RESULTAT/UTGÅNGLÄGE	Grupper skapas där medlemskapet är öppet.

6.4 Del 2 - Hantera grupper

6.4.1 UC Skapa manuell undergrupp

NAMN	UC Skapa manuell undergrupp
BESKRIVNING (KORT)	Baserad på en befintlig (bas)grupp skapas undergrupper.
VEM (ROLLER)	Urvalet utgörs av alla tillgängliga identiteter i en basgrupp. Administratör blir per default den som skapar gruppen.
MOTIV	• Det finns många skäl att skapa grupper i en grupp. Studenter kan delas in labbgrupper, projektgrupper kan bildas etc.
FÖRUTSÄTTNINGAR	• Att grupphanteringssystemet ger möjlighet att skapa och namnge undergrupper baserat på alla tillgängliga individer i en basgrupp.
HÄNDELSEFÖRLOPP	• Administratör av grupphanteringssystemet namnger den undergrupp som skapas. • Administratören sätter tidsintervall för gruppen existens. • Gruppen fylls på med de aktuella individerna. • Administratören kan utse ytterligare deltagare i gruppen till administratörer. • Administratören kan inkludera eller exkludera individer i gruppen med tiden.
VARIANTER	Andra varianter på basgrupper kan vara intressantare: Studenter som är antagna till ett kurstillfälle, studenter med samma starttermin på ett program som bildar en klass etc.
RESULTAT/UTGÅNGLÄGE	En basgrupp är skapad och underhålls maskinellt allt eftersom den förändras.

6.4.2 UC Skapa en sammanslagen grupp

NAMN	UC Skapa en sammanslagen grupp
BESKRIVNING (KORT)	Baserad på flera befintliga (bas)grupper skapas en sammanslagen grupp.
VEM (ROLLER)	Alla individer som ingår i de underliggande grupperna.
MOTIV	• Flera manuella grupper bör kunna slås ihop till en större. • Det finns sannolik också scenarion där en önskad grupp inte går att skapa (eller inte finns skapad) genom maskinellt urval. Men kan skapas genom sammanslagning.
FÖRUTSÄTTNINGAR	• Att grupphanteringssystemet ger möjlighet att skapa och namnge sammanslagna grupper baserat på alla tillgängliga individer i flera grupper.
HÄNDELSEFÖRLOPP	• Administratör av grupphanteringssystemet namnger den sammanslagna grupp som skapas. • Administratören sätter tidsintervall för gruppen existens. • Basgrupperna pekas ut. • Den sammanslagna gruppen växer och minska i takt med att individer inkluderas och exkluderas i de underliggande grupperna.
VARIANTER	• Genom grupphanteringssystemets API kan sammanslagna grupper skapas från andra applikationer. • Det finns andra varianter på mängdoperationer för att skapa en grupp baserat på existerande grupper. Enligt mängdläran kallas en sammanslagning för en union. Det finns eventuellt också ett behov att skapa snitt och komplement av grupper.
RESULTAT/UTGÅNGLÄGE	En sammanslagen grupp är skapad och underhålls automatiskt av grupphanteringssystemet allt eftersom den förändras. Om en individ inkluderas eller exkluderas till/från en basgrupp försvinner den också ur den sammanslagna gruppen.

6.4.3 UC Skapa en grupp genom attribut

NAMN	UC Skapa en attributbaserad grupp
BESKRIVNING (KORT)	En administratör kan skapa en villkorstyrdgrupp.
VEM (ROLLER)	
MOTIV	• Ett smidigare sätt att sköta inkludering i grupper än via systemintegration eller manuellt.
FÖRUTSÄTTNINGAR	• Att grupphanteringssystemet stöder villkor.
HÄNDELSEFÖRLOPP	• En grupp skapas av en administratör. • En offentlig inbjudan går ut på något sätt. • De som anmäler sig till gruppen inkluderas. • Anmälan identifieras genom mailadress eller annat id.
VARIANTER	• Funktionen kan sannolikt byggas i en annan applikation än grupphanteringssystemet.
RESULTAT/UTGÅNGLÄGE	Grupper skapas där medlemskapet är öppet.

6.4.4 UC **Administration av grupp**

NAMN	UC Administration av grupp
BESKRIVNING (KORT)	Uppräkning av administrativa operationer på en grupp.
VEM (ROLLER)	Administratör
MOTIV	• En tom grupp skapas och namnges • En grupp döps om • Gruppens livstid sätts eller ändras • En grupp tas bort • Diverse andra gruppattribut sätts eller ändras • Individer inkluderas eller exkluderas • Individers medlemskap i gruppen tidsbestäms • Administratörsrättigheterna för en grupp delas ut till flera administratörer.
FÖRUTSÄTTNINGAR	• Att grupphanteringssystemet ger möjlighet att göra ovan administrativa uppgifter
HÄNDELSEFÖRLOPP	
VARIANTER	• Att administratörsrättigheter delas ut till den som skapar gruppen eller en medlem i gruppen. • Att operationerna ovan går att göra via en annan applikation via grupphanterarens API.
RESULTAT/UTGÅNGLÄGE	Ordning och reda i grupphanteraren.

6.5 Exportera grupper

6.5.1 UC **Grupper propageras till katalogtjänster (AD/LDAP)**

NAMN	Grupper propageras till katalogtjänster
BESKRIVNING (KORT)	Grupper (eller information baserat på gruppmedlemskap) exporteras till en katalogtjänst.
VEM (ROLLER)	Systemintegration: Detta sker automatiskt.
MOTIV	• Ett gruppmedlemskap kan vara synonymt med behörighet till en resurs. • Attribut kopplade till en medlem kan också kopplas till en behörighet.
FÖRUTSÄTTNINGAR	Systemintegration: Att grupphanteraren har API för att exportera information till katalogtjänsten.
HÄNDELSEFÖRLOPP	Katalogtjänsten hålls automatiskt uppdaterat givet förändringar i grupphanteraren.
VARIANTER	Informationen kan gå andra vägen. Grupper kan skapas och uppdateras i katalogtjänsten och exporteras till grupphanteraren.
RESULTAT/UTGÅNGLÄGE	En uppdaterad katalogtjänst som diverse applikationer kan använda för behörighetskontroll.

6.5.2 UC **Grupper propageras till applikationer**

NAMN	Grupper propageras till applikationer
BESKRIVNING (KORT)	Grupper (eller information baserat på gruppmedlemskap) exporteras till en applikation.
VEM (ROLLER)	Systemintegration: Detta sker automatiskt.
MOTIV	• Ett gruppmedlemskap kan vara synonymt med behörighet till en applikation. • Attribut kopplade till en medlem kan också kopplas till en behörighet.
FÖRUTSÄTTNINGAR	Systemintegration: Att grupphanteraren har API för att exportera information till katalogtjänsten.
HÄNDELSEFÖRLOPP	Applikationen hålls automatiskt uppdaterat givet förändringar i grupphanteraren.
VARIANTER	
RESULTAT/UTGÅNGLÄGE	Uppdaterad behörighetsinformation i en applikation.

6.6 Scenarios

6.6.1 Small

Typiskt för detta scenario är att det finns behov för grupphantering kopplat till ett fåtal user stories. Investeringen skall vara minimal och främst innefatta befintliga verktyg och plattformar. Kanske används också egenutvecklade applikationer och integrationer för att skapa önska funktionalitet.

Typiska verktyg och komponenter är:

- AD
- LDAP
- MS Outlook
- MS Sharepoint
- Integrationer
- Egenutvecklade applikationer för gruppadministration

Typiska user stories är:

- Mailgrupper
- Behörighetsgrupper för intranät
- Behörighetsgrupper för LMS
- Behörighetsgrupper för administrativa applikationer

Fördelarna med detta scenario är:

- Det går att komma igång någorlunda snabbt och enkelt med implementationer av enkla user stories
- Ingen investering i kunskap runt ett grupphanteringssystem krävs

Nackdelar:

- Det är svårare att ha kontroll över grupper och var och hur de används
- Återanvändningen av grupper blir svårare
- Ingen funktionalitet utanför den som finns i befintliga applikationer är gratis. Till exempel att genom operationer göra grupper av grupper osv.
- Det finns en risk att man investerar fast sig i en lösning utan grupphanterare

I dag befinner sig många U/H inom scenario small. En av de största utmaningarna med detta scenario är att bestämma när det är dags att strukturera upp situationen genom att ta beslutet att börja använda sig av ett grupphanteringssystem från en extern leverantör.

6.6.2 Medium

Typiskt för detta scenario är att det finns behov för grupphantering kopplat till ett större antal user stories. Förståelse finns för att antalet grupper kommer växa över tid och att överblick, struktur och automatisk hantering (t.ex. skapande, uppdatering och rensning) behövs. Kopplat till scenariot är också att det finns ett behov för att jobba med gruppoperationer. Samt att man ser behovet att återanvända grupper i flera applikationer/sammanhang.

Typiska verktyg och komponenter är:

- Grouper eller MS FIM (Se verktygsutvärdering)
- AD
- LDAP
- Egenutvecklade integrationer
- Diverse applikationer där grupperna används. Främst för behörighetsstyrning.

Fördelarna med detta scenario är:

- Ordning och struktur för grupper. En samlad behållare.
- Lättare återanvändning av grupper.
- Ett grupphanteringsverktyg ger stöd för implementation för alla tänkbara user stories.
- Lättare återanvändning av integrationer.
- Ett grupphanteringssystem som uppdateras och buggrättas över tid. Av någon annan.

Nackdelar:

- En större investering i kunskap. Då en ny mjukvara införs i lärosätets flora.
- Modulering av gruppstruktur kommer som ett brev på posten.
- För att tillgå potentialen krävs sannolik en hel del integrationer mot befintliga system som hanterar Identity lifecykle management.
- Automatik tenderar att få antalet grupper att växa fortare.
- Grupphanteringssystem kan kosta licenspengar.

Idag befinner sig ett fåtal U/H inom detta scenario. Tydligast är Uppsala universitet, som valt att investera i Grouper.

Det finns också exempel på lärosäten som idag använder sig av grupper i ganska stor omfattning, men som använder sig av egenutvecklad mjukvara som har mer eller mindre funktionalitet som liknar den i FIM eller Grouper. Exempel är Chalmers, Göteborgs universitet och Luleå tekniska universitet. En anledning till att man har egenutvecklad mjukvara kan vara att FIM och/eller Grouper inte fanns (eller var för omogna) när arbetet med grupphantering startades.

6.6.3 Large

Typiskt för detta scenario är att det finns samma eller större behov av grupphantering liknande de i scenario Medium. Skillnaden är att investeringar kring Identity Lifecykle Management behövs. Tänkbara anledningar till detta för svenska lärosäten kan vara att egenutvecklade system har förvuxit sig eller att krav och önskningar har ökat bortom rimlighet för egenutvecklade systemdelar.

ILM och grupphantering sitter ihop på många sätt. Detta scenario är för de lärosäten som har behovet att byta ut eller utveckla stödet för hantering av identiteter.

Typiska verktyg och komponenter är:

- FIM. Som huvudsakligen är en plattform för Identity Management.
- AD
- LDAP
- Egenutvecklade integrationer
- Diverse applikationer där grupperna används. Främst för behörighetsstyrning.

Fördelarna med detta scenario är:

- ILM och grupphantering integreras i ett verktyg
- FIM har ett bra stöd för ILM processer
- FIM har ett bra stöd för att hantera inkludering och exkludering av medlemmar i grupper per automatik. Kräver inte integrationer utanför FIM.
- Ordning och struktur för grupper. En samlad behållare.
- Lättare återanvändning av grupper.
- Lättare återanvändning av integrationer.
- Ett grupphanteringssystem som uppdateras och buggrättas över tid. Av någon annan.

Nackdelar:

- Att byta motor för ILM är ett mycket omfattande projekt för ett lärosäte.
- Att se över roller, processer och begrepp runt ILM tillsammans med verksamheten blir nödvändigt.
- En ännu större investering i kunskap. Då en ny produkt införs i lärosätets flora
- Gamla integrationer mot befintligt ILM system måste ses över.
- Modulering av gruppstruktur kommer som ett brev på posten.
- Automatik tenderar att få antalet grupper att växa fortare.
- Kostar licenspengar.

Idag finns önskningar kring konsolidering och ökat processtöd runt IML-lösningar på många håll bland svenska universitet och högskolor. Men detta är en stor fråga då hanteringen av identiteter är central i vår bransch och dessutom komplex då det de flesta av verksamhetssystemen på ett eller sätt sitter ihop med befintliga ILM-lösningar. Dock har processen att ta investeringar inom detta område startat på några håll. Linköpings universitet och Lunds universitet är två exempel med pågående projekt.

6.7 Rekommendationer runt grupphantering

I detta kapitel redovisas rekommendationer och tips som utredningen fångat från de lärosäten som intervjuats.

6.7.1 Satsa på en grupphanterare

Idag är både FIM och Grouper relativt mogna produkter. De ger ett gott stöd vad gäller organisation av grupper, integration mot diverse ramverk och API:n, administration och gruppoperationer. Erfarenheter pekar på att de initiala kraven och önskningarna på grupphantering inte behöver vara allt för omfattande för att det åtminstone på sikt blir en god investering att använda sig av en produkt i stället för att utveckla stöd på egen hand. Bland de som idag använder egenutvecklade lösningar har flertalet påbörjat sina satsningar innan FIM och Grouper fanns, eller uppnått rätt mognad.

6.7.2 Involvera verksamheten

Att komma igång med grupphantering är inte bara en teknisk utmaning. För att modulera och organisera grupper för bästa struktur, användbarhet och återanvändning krävs en översyn av roller, begrepp och processer. Räkna med att jobba en hel del med verksamheten för att det skall bli bra. Detta får förstås påverkan på projektets omfattning.

6.7.3 Stora kostnader finns i integrationer & underhåll

- Licenser för grupphanteringssystem är ingen tung budgetpost.
- Antalet integrationer (skapande av automatiska grupper och export av gruppinformation) är kostnadsdrivande.
- Precis som för alla andra system är kostnaden för implementation en relativt liten del av kostnadsmassan över tid. Det finns ingen anledning att tro att grupphantering skulle sköta sig själv.

6.7.4 Rätt organisationsschema

Det är centralt att ha en uppdaterad bild av hur organisationen ser ut i praktiken. I många fall så är HR-systemens organisationsschema inte användbart för modulering av gruppstrukturer som skall användas för att ge behörigheter. Traditionella organisationsscheman visar titlar eller tjänstebenämningar snarare än vilken funktion anställda har. Vanligt är att behörighetssystem är beroende av kopplingen mellan användare och den som i verkligheten fungerar som närmaste chef.

Några exempel:

- Auktorisation: Chefer ska ofta godkänna behörighetsförändringar för deras anställda.
- Eskalering: Om ett ärende behöver eskaleras är det naturliga att eskalera det till den ansvariges närmaste chef.

6.7.5 Sopa banan innan automatisk generering av grupper

- Skit in skit ut. De attribut och den datakvalitet som förmedlas av försystemen styr kvaliteten och användbarheten av automatiskt skapade grupper. En satsning på grupphanteringssystem kan betyda städning, omorganisering eller tillägg av rollbegrepp och andra attribut i försystem.
- Att ha god kontroll (tydliga definitioner) på attribut som ger rättigheter i diverse system höjer affärsnyttan. Är attributens definition däremot otydliga eller dubbeltydiga finns risken att nya måste skapas för varje applikation.

6.7.6 Antalet grupper tenderar att öka snabbt och grupperna blir svåra hålla reda på

- Håll tillbaka okontrollerad tillväxt
  - Skapa automatiska rensningsrutiner
  - Sätt en begränsad existenstid för alla grupper som skapas
- Se till att grupper inte skapas i onödan (undvik redundans)
  - Sökbarhet är A och O för återanvändning av existerande grupper
  - God struktur gör det lätt att leta bland existerande grupper
  - Transparent namnsättningsstandard
  - Beskrivande namn och förklarande text är viktiga attribut för grupper
  - Använd beräknade/konstruerade grupper (vyer) i stället för att skapa nya basgrupper

6.7.7 Behovet att inkludera externa (federerade) användare kommer som ett brev på posten

Universitetens och högskolornas natur kommer snabbt att ställa krav på möjligheter att inkludera externa gruppmedlemmar.

Exempel:

- Representanter från andra lärosäten i gemensamma forskargrupper
- Representanter från omvärlden i olika sammanhang
- Studenter från andra lärosäten i gemensamma utbildningssatsningar

6.7.8 Distribuera förvaltningen av grupper för bättre payback

- Implementationen skall borga för att någon blir ansvarig för förvaltningen/livscykeln av gruppen
- En verksamhetsperson bör ”äga” gruppen. Frikoppla systemadministratören om möjligt.
- Skaparen av en manuell eller sammansatt grupp (genom mängdoperationer) bör bli administratör. Låt administratören dela med sig eller vidarebefordra rättigheter till andra i gruppen.

7 Bilagor

Auktorisation och grupphantering Kartläggning.
https://portal.nordu.net/display/Inkubator/Projektrapporter

Auktorisation och grupphantering Produktjämförelse Grouper och FIM (levereras januari 2014)