KOKBOK
Grupphantering

I skenet av rådande tekniktrender, framtida forskning, global access och best practice inom Identity and Access Management

SUNET Inkubator

2014-12-22

helena.sandstrom@umu.se
therese.soderlund@umu.se

SAMMANFATTNING

Vi har en explosionsartad utveckling inom IT idag, där allt snart är uppkopplat mot allt. Användare reser omkring och kopplar upp sig mot sin arbetsplats och tillhörande molnresurser från jordens alla hörn, via marknadens allehanda uppkopplingsbara prylar. Denna teknikutveckling har förändrat sättet som organisationer exponerar affärskritiska tjänster och data. Vi står inför ett skifte där vi går ifrån den stängda skyddade organisationens värld till ett öppet men i den bästa av världar fortfarande pålitligt säkert universum av applikationer och mobila enheter som ständigt utvecklas. IT-infrastrukturer och våra verktyg för IAM, identitets- och accessmanagement behöver därför klara av att hantera relationer med allehanda partners både inom och utanför organisationen. Ett nytt begrepp har därför dykt upp och man börjar prata om Identity and Relationship Management, IRM. Det är den aktuella relationen med den du kommunicerar med som är intressant. Kopplar man upp sig med sin mobiltelefon via en NAT:ad IP-adress från Kina krävs kanske ytterligare en autentiseringsmetod, VPN samt kryptering av filer som lagras på telefonens hårddisk för att få tillträde till vissa resurser medan ett vanligt lösenord räcker när du kopplar upp dig med din kontorsdator internt.

En annan pågående trend är ett ökande behov från forskare i Sverige, Europa och världen över, att kunna samarbeta och dela resurser mellan universitet och forskningscentra nationellt och internationellt. I syfte att möte detta behov pågår en utbyggnad av ett globalt federerat accessnät. I det arbetet krävs att vi river alla mentala och tekniska barriärer som kan tänkas stå i vägen för utvecklingen och börjar tänka global access när vi tar beslut kring våra framtida IT-infrastrukturer. De e-infrastrukturer vi bygger idag bör kunna möta framtidens behov.

I princip alla lärosäten använder idag grupphantering i någon form internt på våra lärosäten. Grupper används i sammanhanget främst för att styra access till olika resurser. Många har till exempel grupper i AD. I AD skiljer man på säkerhetsgrupper och distributionsgrupper. En säkerhetsgrupp kan tilldelats behörigheter för delade resurser medan en distributionsgrupp bara kan ha en egen e-postlista. Förutom AD-grupper kan grupper finnas i identitetshanteringssystem och distribueras därifrån till sidosystem och i andra fall finns en grupp bara lokalt i ett system. Viss export av grupper av användare sker även ut till molntjänster som till exempel Office 365 eller Google Apps.

Det nästan alla lärosäten saknar är ett speciellt verktyg för att hantera grupper. Resultatet av det är att det inte finns en central funktion som håller reda på grupperna. Det medför dels att det kanske inte är någon som har total överblick över vad en användare har access till samt att administration av behörigheter medför en hel del manuell administration i olika system. Vinsten med att införa ett centralt grupphanteringsverktyg förutsatt att det är väl integrerat med övrig IT-infrastruktur är främst att du får ett verktyg som möjliggör:

- att överblicka och styra vad varje användare har access till
- att överblicka och styra hur många som har access till en viss resurs
- att delvis ta centrala IT ur loopen och reducera behovet av central administration genom att delegera administration av grupper till den som bäst vet vem som skall ingå i grupper och vilka grupper som behövs. Det kan vara institutioner, lärare på kurser, projektledare, etc
- att minska behovet för institutioner att bygga egen infrastruktur då delegerad administration möjliggör att resurser installeras och driftas av centrala IT men att access till resursen administreras av institutionerna själva

- finkornigare accesskontroll
- mera robusta processer för on-boarding och off-boarding med automatiserad tilldelning och tillbakadragning av behörigheter.
- Att ha externa federerade användare i grupper utan att behöva skapa lokala datakonton

Vi har studerat två varianter av egenuvecklad grupphantering. Dels hos Högskolan Väst där man har ett eget GUI ovanpå en MySQL-databas samt vid Luleå Tekniska Universitet där underliggande plattform är LDAP. Vi har även studerat grupphantering med två verktyg, Microsoft Forefront Manager, FIM samt Grouper som är open source och utvecklat av Internet2. Skillnaden mellan de båda är främst att Grouper är ett renodlat grupphanteringsverktyg medan FIM är en Identity Manager som kan användas som ett kombinerat identitetshanterings- och grupphanteringsverktyg.

Vår slutsats är att ett väldesignat grupphanteringssystem kan underlätta avsevärt när det gäller administration av användare och deras behörigheter samt öka säkerheten genom att det kan ge en total överblick av vem som får göra vad i systemen. Det främsta exemplet på hur bra det kan bli var Högskolan Väst som under flera år systematiskt arbetat för att bygga ett sådant system. Att införa ett genomtänkt system för grupphantering oavsett om du väljer att bygga det själv eller installera ett verktyg medför dock en hel del planeringsarbete initialt där målet är att försäkra dig om att alla processer är väldefinierade, att du har bra rådata som går att använda för att automatiskt skapa grupper samt att du har en bra uppfattning om vilka grupper du behöver och vad du skall använda dem till. Alla lösningar kommer att kräva konfiguration och anpassningar för att effektivt integreras i befintlig infrastruktur.

Vår rekommendation i sammanhanget är att om du har en fungerande identitetshantering som är väl integrerad med övriga system och bara vill ha ett verktyg för att skapa, överblicka och administrera grupper så är Grouper det främsta alternativet. Det har med version två fått ett mycket mer lättanvänt användargränssnitt och har bra integrationsmöjligheter mot LDAP, AD och SQL, WS, ESB och Shibboleth samt stödjer händelsebaserad notifieringar via sin changelog consumer. Den har stöd för olika typer av sammanslagna grupper och det finns många möjligheter till access management som är lite mindre beroende av fördefinierade objekt än i FIM. Den har även en struktur där du kan ordna grupper i hierarkiskt ordnade mappar och du skapar även enkelt grupper i grupper. Att byta namn på en grupp eller mapp eller flytta den i hierarkin är lika enkelt som i ett vanligt filsystem.

Du kan även använda FIM för grupphantering men om du inte vill använda den också för identitetshantering är det frågan om licenskostnaden är motiverad. Fördelen med FIM är att den är relativt enkelt att integrera med Microsoftprodukter vilket bland annat gör det enkelt att exportera grupper till AD samt att du kan integrera delegerad administration via Outlook. Funktionellt ser vi i övrigt inte att FIM är bättre ur grupphanteringsperspektiv. Behöver man dock ett verktyg för både identitetshantering och grupphantering så kan det vara intressant att titta på FIM.

När det gäller införande och förvaltning är Grouper som sagt open source vilket är både bra och dåligt, men det är en livaktig community runt Grouper och det finns mängder med information att tillgå både via en stor mängd instruktionsvideos och via Groupers wiki. Det finns även två maillistor att prenumerera på där folk postar sina frågor som i regel besvaras samma dag. När det gäller införande och förvaltning av FIM är erfarenheten från de som installerat FIM för identitetshantering att man är relativt konsulttung vid planering och införande.

INNEHÅLLSFÖRTECKNING

1 INLEDNING

När man googlar på group management får man först träff på vilka som ingår i ledningsgruppen på företag. Du kan även få träffar som gäller teambuilding. Du får mer troligt en bra träff om du skriver user and group administration. Men efter att ha googlat i ämnet ett tag så stod det ganska klart att det de flesta relaterar till i sammanhanget är Access Management. Grupphantering är inte liktydigt med, men en viktig pusselbit i det som idag ofta benämns IAM, Identity och Access Management. IAM benämns på svenska Identitets- och behörighetsstyrning eller behörighetshantering.

Med grupphantering menas i sin enklaste form helt enkelt att ordna saker/personer i grupper. Hur man väljer att gruppera beror på vad man behöver grupperna till och den tydligaste nyttan i vårt sammanhang inträder när du kopplar en grupp mot access i ett visst system. De allra flesta lärosäten använder idag troligen någon form av grupphantering men utan att ha ett speciellt verktyg för detta ändamål. Grupperna kan därför ligga i olika system och personer som byter anställning inom lärosätet läggs till i nya system och grupper men det är inte säkert att de tas bort från sina gamla trots att de byter organisatorisk tillhörighet och ansvarsområde. Löpande administration sker kanske också delvis manuellt utan robusta rutiner. Sammantaget kan det leda till att det blir svårt att presentera en överblick över vem som har access till vad. Förutom att systemet blir ineffektivt så medför det även en del säkerhetsproblematik.

En av de frågeställningar vi hade inledningsvis var, hur skapar vi en effektiv grupphantering och hur kan den ligga till grund för att skapa en effektiv, överblickbar och säker behörighetshantering. Det vi kan skönja är att den rådande trenden inom IAM är att organisationer och företag insett vikten av och i ökande grad satsar på att bygga skalbara IAM-system som klarar att möta de rådande kraven på mobilitet och flexibilitet i vår alltmer globaliserade värld. Ett effektivt och väl designat IAM-system genererar generellt stor affärsnytta samtidigt som det kan öka säkerheten mot intrång och identitetsstöld. Ett välutvecklat IAM-system skall även stödja molntjänster, federerad inloggning och andra funktioner så som kontroll av fysisk access till lokaler. I arbetet med kokboken har därför en ganska stor del upptagits av att ge en övergripande bild av IAM, då vi anser att det är nödvändigt för att få den förståelse som behövs för att se på vilket sätt grupphantering bäst kan tillföra stort värde i en IT-infrastruktur.

Förutom att studera rådande trender inom IAM har vi under arbetet med kokboken även lyft blicken och tittat oss om i världen för att identifiera vad forsknings- och utbildningsvärlden har för behov och förväntningar på oss, nu och i framtiden. Tittar vi globalt växer ett behov inom forskningsvärlden att på ett sömlöst sätt kunna samarbeta och en viktig ingrediens i att uppfylla detta behov är en smidig och flexibel e-infrastruktur som bygger system som tillåter och stödjer samarbete nationellt och internationellt. Denna kokbok i grupphantering inleds därför med ett avsnitt om trender och framtidsvisioner.

1.1 BAKGRUND

Projektet har genomförts på uppdrag av SUNET/Inkubator. Arbetet med att ta fram kokboken baserar sig på ett tidigare projekt som genomfördes under 2013 av Maria Valtersson och Jan Rundström där man sållat fram två grupphanteringsverktyg som speciellt intressanta att studera för

implementering av grupphantering vid Sveriges universitet och högskolor. De två grupphanteringsverktygen är Microsoft Forefront Identity Manager, FIM, samt Grouper, en open source programvara framtagen av Internet2.

Inför detta projekt hölls i november 2013 en workshop på KTH där drygt 25 personer från olika lärosäten deltog. Ett av momenten var att sammanställa vilken information man skulle vilja ha i en framtida kokbok om implementering av ett grupphanteringsverktyg. Vi har kanske inte svarat på alla frågor men hoppas att de som läser kokboken skall få en bra uppfattning om vad grupphantering är och har en övergripande bild av hur det bör designas och integreras med övriga system för att ge maximal nytta.

1.2 PROJEKTGRUPP OCH REFERENSGRUPP

Projektet har haft en referensgrupp bestående av Eskil Swahn, LU, Johan Petersson, LIU, Pål Axelsson, UU, Leif Lagerbrand, BTH, Ola Ljungkrona CTH. Telefonmöten med referensgruppen har hållits cirka varannan månad.

Projektgruppen bestod inledningsvis av Maria Valtersson och Jan Rundström. Efter inledande arbete under våren lämnade Jan och Maria över uppdraget eftersom de inte kunde avsätta den tid som behövdes. Under sensommaren och hösten är det Therese Söderlund och Helena Sandström som drivit projektet och huvuddelen av arbetet i projektet har skett under den tiden. Arbetsfördelningen har sett ut så att Therese har varit engagerad i projektet på cirka tjugo procent och formellt varit projektledare samt ansvarat för kapitlet om införande och förvaltning. Helena har ansvarat för övriga delar och varit engagerad på sjuttiofem procent med en viss ökning under november. Projektgruppen har haft kontinuerliga möten cirka en gång i veckan.

1.3 GENOMFÖRANDE OCH METOD

Under arbetet med att ta fram vägledning och rekommendationer kring att införa grupphantering blev en första fråga inte hur man gör det utan varför man skall göra det. Detta eftersom syftet och användningen av grupperna är det som styr hur du väljer att utforma och införa det. Arbetet inleddes därför med att göra en omvärldsanalys där vi hade ett antal frågeställningar. Bland annat:

- Hur ser utvecklingen på marknaden ut
- Vad kan vi lära oss av andra
- Varför har andra infört det
- Vilka goda exempel finns
- Vilka krav bör vi ställa
- Vad är syftet och målet
- Hur bygger vi system som klarar framtida krav så att vi inte måste designa om

Lärdomarna utifrån den omvärldsanalysen kom att omfatta de första tjugofem sidorna och hela två kapitel av rapporten men vi behöll det så långt eftersom vi fick feedback från referensgruppen och andra som läst att det var matnyttig läsning. Vår egen uppfattning är att man behöver sätta in grupphanteringen i ett större sammanhang för att förstå dess nytta och värde.

Själva kärnan i rapporten skall dock vara grupphantering. I syfte att få fram bra och konkret information kring införande av Grouper och FIM var planen att göra en PoC med FIM i samarbete

med LIU samt med Grouper i samarbete med MIUN. Dessa samarbetet fick skjutas på framtiden då ingen av organisationerna hade möjlighet att genomföra dessa PoC:ar inom given tidsram.

Det vi har haft tillgång till för utvärdering av verktygen är en egen lokal installation av Grouper samt intervjuer med lärosäten som redan använder Grouper för grupphantering. Vi har ingen i Sverige som använder FIM för grupphantering men vi har intervjuat de som använder FIM för identitetshantering. Utöver det har vi läst allmänt åtkomlig teknisk dokumentation om båda verktygen samt följt några webbinarer.

1.4 LÄSANVISNINGAR

Målgruppen för kokboken är främst IT-chefer och IT-arkitekter på universitet och högskolor men kokboken läses med god behållning för alla som på något sätt är inblandade i administration, utveckling och beslut som berör grupphantering eller identitets- och behörighetshantering.

Rapporten är indelad i fem kapitel. Den inleds med två ganska långa kapitel som beskriver rådande trender, teknikutveckling och framtidsvisioner. Kapitel ett beskriver alltså de rådande trender och framtidsvisioner vi snappat upp inom teknikutveckling, IAM och forsknings- och utbildningssektorn.

Kapitel två behandlar IAM, samt listar råd om best practice inom området. De båda inledande kapitlen ger tillsammans matnyttig information som vi anser bör ligga till grund för de designval du gör när du sätter dig ner och planerar och designar grupper.

Kapitel tre fokuserar på grupphantering och design av densamma. Det är uppbyggt i en FAQ-form för att det skall vara lättare att dyka rakt in i kapitlet utifrån de frågeställningar man kanske har.

Kapitel fyra är ett hands on kapitel och det beskriver grupphantering med Grouper och FIM samt de erfarenheter och lärdomar vi inhämtat från LTU och Högskolan Väst. De har inte ett separat verktyg för grupphantering men båda har en relativt utbyggd och smidig hantering av grupper via ett egenutvecklat användargränssnitt som går mot LDAP eller MySQL.

Avslutningsvis har vi kapitel fem som riktar sig främst till förvaltare och de som planerar införandeprojekt och rådgör på vägen mot ett införande av en grupphanterare och hur denna sedan kan förvaltas.

I slutet återfinns Termer och Förkortningar och Referenser. Kokboken avslutas av ett Appendix som innehåller ett underlag till ett gemensamt standardiserat Grupp-API samt ett avsnitt där vi går in på mer detaljer kring integrationsmöjligheter med Grouper.

2 TENDENSER OCH FRAMTIDSVISIONER

Forskning utgör själva grunden för kunskapsutvecklingen i samhället. Forskning delas ofta in i grundforskning och tillämpad forskning där grundforskning styrs av forskarens nyfikenhet medan tillämpad forskning utförs med en bestämd tillämpning i sikte. Världen står inför många utmaningar idag där vi behöver ny forskning och innovativa idéer för att klara av att ta oss an problem med bland annat energiförsörjning och miljöförstöring.

> *Innovation is the ability of individuals, companies, and entire nations*
> *To continuously create their desired future*
>
> *John Kao, "innovation nations", 2007*

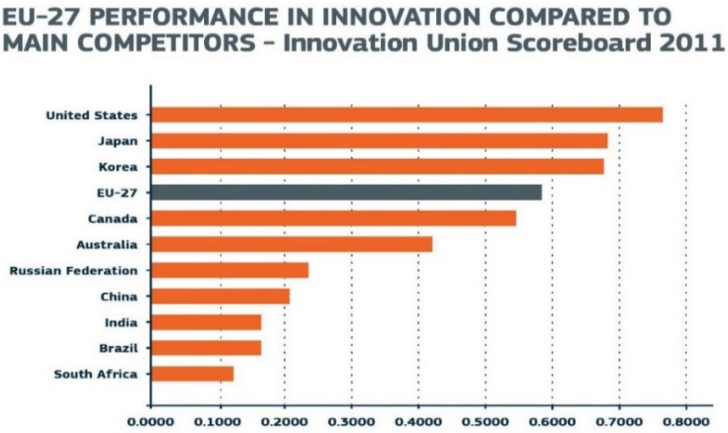
Internet och den explosionsartade tekniska utvecklingen öppnar för många möjligheter. Världen över pratar man om vilka nya möjligheter nya tekniker ger att koppla samman människor, ta fram nya lösningar, samarbeta och utveckla idéer i kollaboration, samt utföra komplicerade beräkningar med stora datamängder. Vi som levererar IT inom universitet och högskolevärlden har här en viktig uppgift. Den består i att göra vad vi kan för att leverera den tekniska plattform som på bästa sätt servar vår sektor och möjliggör samarbete mellan toppforskare på våra lärosäten och industrin.

I det arbetet får vi vara lika framsynta som våra forskare, som i allt högre grad söker samarbete och samarbeta även vi. Vi lever i en tid där applikationer föds nästan lika fort som de dör, eller ersätts av något bättre, och den stationära datorn ersätts eller kompletteras av mobila enheter med alltmer avancerad funktionalitet. Utifrån det perspektivet är det sannolikt att vi kommer att gå mot en framtid där vår IT-infrastruktur behöver vara mer flexibel, dynamisk och effektiv för att vara redo att möta våra användares framtida behov.

2.1 POLITIK OCH FORSKNING

2.1.1 Globalt

När det gäller utveckling och innovation så visar Figur 1 att länder som Kina, Brasilien och Indien har seglat upp som starka aktörer i sammanhanget. Europa ligger dock fortfarande relativt högt och USA är nummer ett.



Figur 1 Från EU:s pocket guide om Innovativa unionen Europa 2020 [1]

I USA är Internet2 den universitetsledda organisation som tillsammans med amerikanska staten och industrin driver utvecklingen inom e-infrastruktur. De lanserade i somras en ny instans, TIER, som står för Trust and Identity in Education and Research. Deras uppdrag omfattar att koordinera det växande ekosystemet av open source produkter som håller på att tas fram kring federerade identiteter och Middleware [2] av olika grupperingar inom Internet2. TIER koordinerar aktiviteter inom InCommon, Shibboleth, Grouper, COmanage, MACE register och edu* LDAP-scheman. Målsättningen är att accelerera IAM inom högre utbildningar i syfte att underlätta globalt samarbete samtidigt som alla medlemmar skall ha access till rätt tjänster, vid rätt tidpunkt, och med rätt säkerhet och integritet [3] [4] [5] [6].

Man pratar förstås om federerat samarbete inom USA men pratar lika mycket om att utöka samarbetet globalt genom interfederationer. EduGAIN [7] har bland annat förhandlat med InCommon i USA i syfte att komma fram till gemensamma policys kring data om våra användare som skickas mellan våra federationer. En kommentar från USA i sammanhanget var att våra lagar gjorde att vi européer hade en annan syn på vad vi ville lämna ut om våra användare så det var svårt att nå det de ville åstadkomma i dessa förhandlingar. Samarbetet har ändå inletts och InCommon är nu medlemmar i eduGAIN.

2.1.2 EU

EU:s framtida forskningssatsningar sker inom Horizon 2020 [8], ett finansiellt instrument för att implementera ”den innovativa unionen”. Det omnämns som ett flaggskepp för Europa 2020 vars syfte är att säkra Europas globala konkurrenskraft. Programmet sträcker sig över 7 år, från 2014-2020, där EU satsar 80 miljarder euro. Programmet är öppet för internationella medverkande och världens största satsning på forskning och innovation.

> *“Innovation Union is the European Union strategy to create an innovation-friendly environment that makes it easier for great ideas to be turned into products and services that will bring our economy growth and jobs.”*

När det gäller e-infrastruktur kan man läsa att EU liksom USA vill utveckla en e-infrastruktur i världsklass i syfte att utnyttja dess innovationspotential.

Kontentan är att Europa har ambitionen att öka samarbetet och överbrygga eventuella tekniska och mentala hinder för samarbete. Ett samarbete vars syfte är att bibehålla vår ställning som innovativ union och försvara Europas plats på innovations- och utvecklingstrappan.

2.1.3 Norden

Sverige deltar även i det nordiska forskningssamarbetet. Samarbetet mellan de nordiska länderna är ett av de äldsta och mest omfattande i världen och startade efter andra världskriget. De nordiska länderna samarbetar på många sätt och inom många områden.

När det gäller forskningssamarbetet i Norden är målsättningen att stärka de områden där Norden kan hävda sig internationellt eller inom områden där vi i Norden har speciella intressen eller förutsättningar. På Nordiska ministerrådets hemsida kan man läsa att man bland annat vill stödja samarbetet mellan nationella och nordiska forskningsorganisationer och ett flexibelt samspel även inom forskningsinfrastruktur, samt befrämja eScience och e-Infrastruktur.

e-Infrastruktur lika viktigt som vägar, järnvägar, flygplatser och det innebär en förändring i synen på finansiering och standardisering av den

I begreppet infrastruktur ligger även en standardiseringsaspekt. En e-infrastruktur behöver likväl som övrig infrastruktur bygga på standarder om sådana finns.

Tittar man på våra nordiska grannländer så vill man i Norge hitta gemensamma lösningar och standarder när det gäller ICT inom universitet och högskolor [9]. Lösningar som kan bidra till att:

- effektivt stödja nya och ändrade verksamhetsprocesser
- förenkla och effektivisera integration mellan och rapportering från olika lösningar
- reducera ICT kostnader
- underlätta gemensamma strategier när det gäller att följa statliga föreskrifter och standarder
- hindra framväxt av slutna system (silos) som har överlappande funktionalitet och information
- förenkla och effektivisera skräddarsydd portalbaserad tillgång till funktionalitet och information genom standardiserade tjänster och gränssnitt

En del i det arbetet är att skapa en samsyn mellan lärosäten eller kanske skapa en standard när det gäller synen och hanteringen av anställda och studenter, men även den grupp som inte tillhör någon av dessa båda grupper och som även varje lärosäte här i Sverige brottas med att hitta bra lösningar för. Det gäller bland annat:

- Gästföreläsare
- Gästforskare
- Externa konsulter
- Externa vikarier (t.ex från bemanningsföretag)
- Externfinansierade anställda
- Anställda på andra institutioner/lärosäten som man har samarbete med
- Externa studenter
- Alumni
- Osv…

2.1.4 Sverige

Sverige satsar ca 2.2 procent av sin BNP på forskning. Endast Israel, Finland och Sydkorea avsätter mer för FoU som andel av BNP. På regeringskansliets hemsida betonar man vikten av nationella och internationella forskningsinfrastrukturer samt betydelsen av att utveckla dessa gemensamt och öka samarbetet regionalt, nationellt och internationellt.

Sverige har sedan 1999 forskningsavtal med: Argentina, Indien, Japan, Kanada, Kina, Mexico, Singapore, Sydafrika, Sydkorea, och USA. Syftet med dessa avtal är att underlätta och fördjupa samarbetet inom FoU med dessa länder.

Vårt bidrag, i egenskap av lokala IT-leverantörer på svenska universitet och högskolor, blir i sammanhanget förstås att gemensamt skapa en e-infrastruktur som kan stödja dessa initiativ till samarbeten, nu och i framtiden.

2.2 TEKNIKUTVECKLING

Som nämndes i inledningen så pratar man i organisationer och företag alltmer om vikten av ett väldesignat och skalbart IAM-system som stödjer mobila användare, molntjänster och federerad inloggning. En högskola och ett universitet kan visserligen liknas vid ett företag där lärare och forskare samt förvaltningspersonal är anställda och studenterna är kunder.

Högskolor och universitet är dock mer komplexa och dynamiska organisationer än ett traditionellt företag eftersom människor hos oss ofta har multipla samtidiga roller och relationer. Speciellt för lärosäten är till exempel att en anställd kan vara anställd på flera institutioner och vara både lärare och student. Lärosäten knyter också ofta till sig nya löst anknutna samarbetspartners och gästföreläsare, kanske så ofta som dagligen. Nya projekt och samarbeten initieras och nya kurser med nya studenter startar året runt.

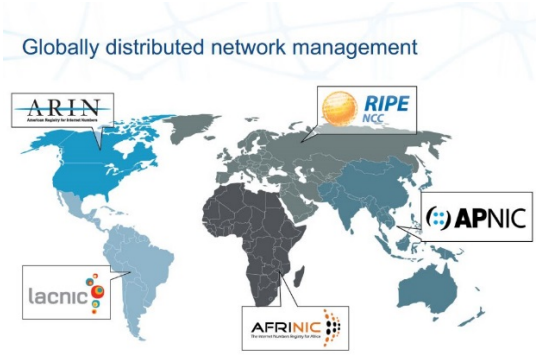
Komplexiteten innebär att vi inte riktigt kan liknas vid ett företag. Det innebär också att vi inte kan räkna med att hitta en kommersiell lösning som uppfyller våra behov eftersom de som finns främst är riktade mot företagsmarknaden. Väljer vi en kommersiell lösning skall vi därför räkna med att det kommer att kräva en hel del lokala anpassningar. Inom universitetsvärlden i USA anser man att lärosätenas komplexa miljö istället gör att vi är de som tvingas leda utvecklingen av IAM-lösningar eftersom vi helt enkelt måste. På Internet2:s Global Summit konferens 2014 hade man en presentation som handlade om strategier för att accelerera IAM inom högre utbildningar.

I presentationen poängteras att vi byggde ett globalt internet men att vi i det inte inkluderade accesstjänster. Traditionellt kommunicerar vi över internet i punkt till punkt sessioner där vi flyttar data mellan punkterna. Accesshanteringen i sammanhanget är traditionellt specifik för varje resurs med intern hantering av användaruppgifter och roller. Detta ger maximal smärta, minimal vinst och en situation som hindrar vetenskaplig utveckling och forskning.

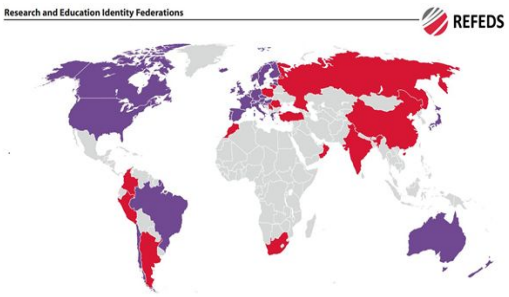
Internet2 menar att om vi fokuserar på forskningsvärlden så ligger prioriteringarna på:

- Virtuella organisationer och andra samarbeten
- Nätverk med väldigt hög bandbredd
- Ökat antal applikationer och tjänster som stödjer samarbete
- Specialiserade resurser för lagring, beräkningar och samverkan

- En mix av behov av access-policys tvärsigenom olika forsknings- och vetenskapsaktiviteter men även tvärsöver generella akademiska och administrativa aktiviteter med samarbeten spridda över organisationer och nationer



Figur 3 Internets fem koordinationscentras



Figur 2 Refeds karta över federationer i världen

En målbild skulle vara att kartan i Figur 2 ovan vore lika färgglad som kartan i Figur 3, med andra ord, att identitetsfederationerna och global access management är lika utbyggt som internet.

Inom existerande identitetsfederationer kan vi idag börja bygga upp vårt globala accessnät. Det finns dock en hel del arbete kvar innan vi når dit. Bland annat krävs:

- fler federationer
- standardiserade access management objekt som kan administreras och delas mellan instanser för
    - Namngivning
    - Scheman
    - Protokoll
    - Bindings
- att vi underlättar för internationella VO:s och andra samarbeten
- att vi ser till att interfederationer kan samverka effektivt
- att vi sänker tröskeln genom fler (open source?) IAM produkter med gemensamma API:er
- lokala IAM-tjänster som kan serva forsknings- och utbildningssektorns behov

Vi behöver alltså en global access service. Men hur skulle en sådan se ut? Internet2 listar följande:

- universitet, fakulteter, forsknings-Lab har IAM-instanser
- det finns samarbetsplattformar för virtuella organisationer (VO:s)
- lokala IAM finns tillgänglig som ”as a Service” till ovanstående
- IAM hanterar identiteter, säkerhetskriterier, attribut, grupper och roller
- IAM är integrerat med lagrings-, nätverks-, beräknings- och applikationsresurser
- allt är inbäddat i federationer, interfederationer, för att koppla samman människor, deras säkerhetskriterier, attribut och roller.

För att detta skall fungera så behöver access management vara delegerat och distribuerat då ingen kan veta vad varje person skall få rätt att göra. Delegation sker inom en organisation samt mellan organisationer. En generell regel är att den som vet vilka behov av access någon behöver skall också vara den som tar beslutet och har befogenhet att se till att personen får access.

I dokumentet ”Identity management in higher education: a view of the landscape – june 17, 2013” som producerats av TIER beskriver man att man nu befinner sig i ”Henry Ford”-stadiet när det gäller att utveckla sin modulbaserade IAM-infrastruktur som stödjer federerad identitetshantering där man går från specialutvecklade lösningar till löpandeband och ”off the shelf” lösningar i ett modulärt uppbyggt ekosystem som kommer att skala väl. Internet2 räknar med att ha utvecklat detta IAM-system inom några år.

TIER har identifierat att många universitet kämpar med att implementera effektiva identitetshanteringsprogram och att de bland annat behöver hjälp med:

- Struktur och organisation
- Värde och riskbedömning
- Flöden och processer
- Teknisk support och kompetens

CIFER – Community Identity Framework for Education and Research, har idag en första funktionell modell av ett IAM-system och sätter upp en plattform med en virtuell testbädd för demo av ett urval open source IAM-paket [10].

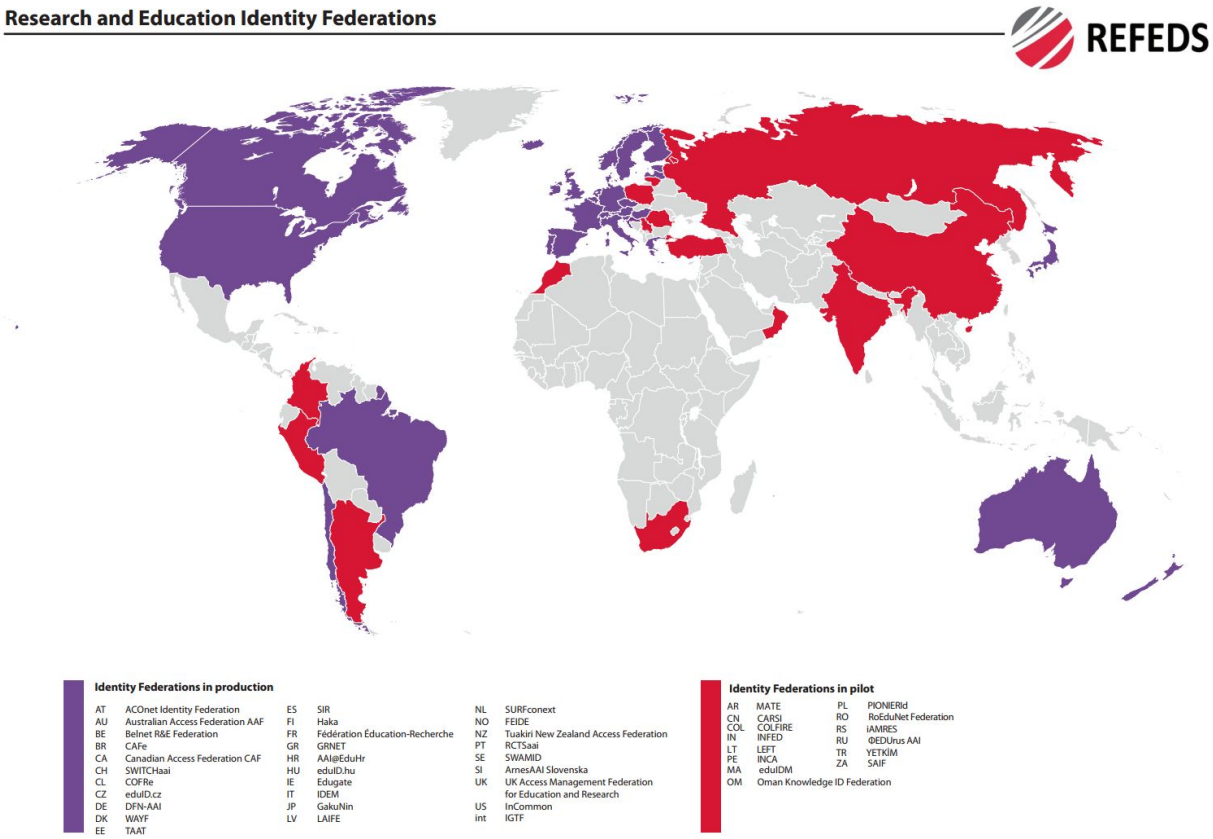
2.2.1 Federationer

Det kan i sammanhanget vara värt att nämna vad vi avser med en federation. En federation är ett ramverk för samarbete där institut och organisationer som ingår i federationen har kommit överens om att lita på den information de skickar till varandra. En interfederation är en federation av federationer.

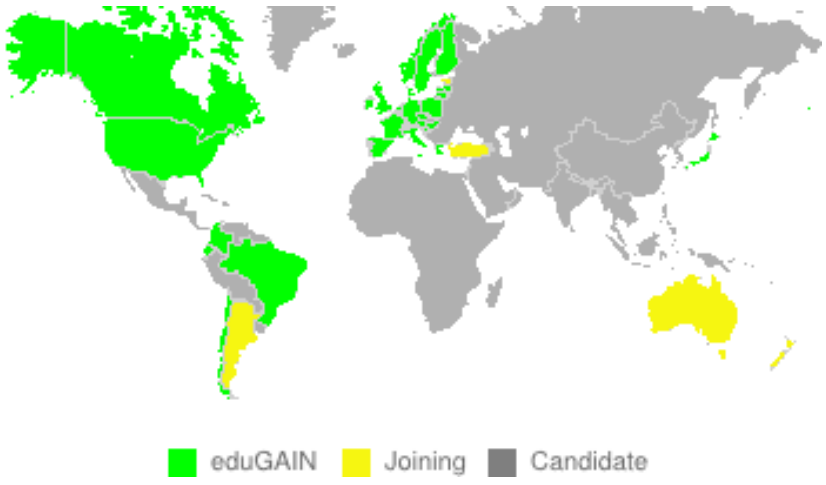
Federated Access Management möjliggörs genom att organisationer kommer överens om en gemensam modell där man etablerar vissa regler och policys som säkerställer att det gemensamma förtroendet går att lita på, utveckla och hantera praktiskt. Enligt modellen så hanteras en användares identitet av användarens hemorganisation. När en användare vill ha tillträde till ett externt system autentiserar hemorganisationen eller den centrala identitetsleverantören användaren och skickar, enligt de policys och regler man enats om inom federationen, de uppgifter om användaren som krävs för att det externa systemet skall kunna avgöra om användaren skall få tillträde till begärda resurser eller inte. För federerad access och inloggning är den service man vill använda företrädesvis implementerad som en webbtjänst där en identity provider, IdP, autentiserar en användare som vill komma åt en webbtjänst hos en Service provider, SP.

2.2.1.1 Federationer inom högre utbildning globalt

Utvecklingen med federationer inom universitets- och forskningsvärlden är intressant. Som man kan se i kartan nedan är det många länder, däribland även Kina och Ryssland som har instiftat federationer om än på pilotnivå.

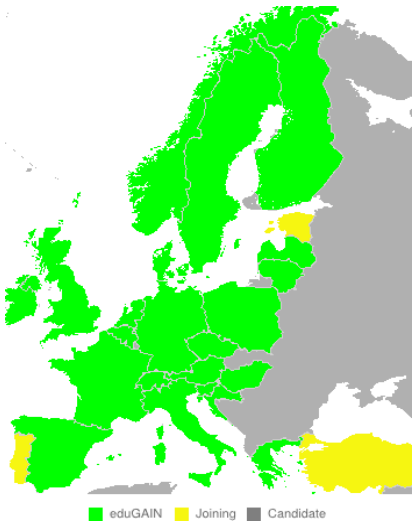


Kartan nedan visar vilka av dessa som har eller är på väg att ansluta sig till eduGAIN. En trolig utveckling är att alltfler kommer att ansluta sig för att forskare inom universitets- och högskolevärlden lättare skall kunna samarbeta och använda varandras resurser såsom data, forskningsinstrument och beräkningskapacitet.



Figur 4 Federationer i världen anslutna till eduGAIN

Aktuell status för vilka federationer inom Europa som anslutit sig till eduGAIN visas i Figur 5. Att SWAMID är med i eduGAIN innebär att universitet och högskolor i Sverige är med i en global accessfederation.



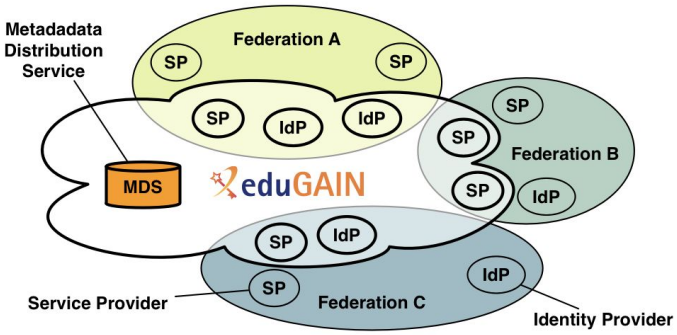
Figur 5 Federationer i Europa anslutna till eduGAIN

USAs federation InCommon blev relativt nyligen blev medlem i eduGAIN och gemensamma ansträngningar har lett fram till ett pilotprojekt i samarbete med Leonard E. Parker Center for Gravitation, Cosmology and Astrophysics (CGCA) vid universitetet i Wisconsin-Milwaukee, UWM [11]. Man kan vid deras observatorium bland annat studera astrofysiska objekt såsom svarta hål och supernovor. Pilotprojektet kommer att göra det möjligt för astronomer inom eduGAIN att använda sina lokala campusdata för att logga in i tre UWM-baserade tjänster:

- The Gravitational Wave Astronomy Community Registry
- The Gravitational Wave Astronomy Community Wiki
- The Gravitational Wave Astronomy Community List Server

2.2.1.2 Hur fungerar eduGAIN

EduGAIN tillhandahåller en Metadataservice som håller information om deltagande federationers SP:s och IdP:s och gör den informationen tillgänglig för alla medlemmar. EduGAIN koordinerar nödvändig teknisk infrastruktur och tillhandahåller det ramverk av policys som styr utbytet av information mellan federationerna.



Figur 6 EduGAIN håller information om federationernas IdP:er och SP:er

2.2.1.3 Attributrelease

Identitetsfederationer kan idag i huvudsak:

- fungera som en delegerad mekanism för hantering av användaridentiteter
- tillhandahålla en uppsättning attribut för autentiserad användare

Traditionellt har identitetsfederationer löst problemet med auktorisation med två motsatta tillvägagångssätt, dvs auktorisation hanteras av antingen IdP:n eller SP:n. Om auktorisation skall hanteras av SP:n utan att den själv lagrar data om en användare behöver den få en viss uppsättning attribut om användaren från IdP:n. Det har dock traditionellt funnits en ovilja hos IdP:er att releasa attribut om sina användare till SP:er, med hänvisning till säkerhet och integritetsfrågor.

2.2.1.4 Entitetskategori R&S

Inom eduGAIN har man idag ett system där en SP kan kategorisera sig som R&S. R&S är en entitetskategori som står för Research & Scholarship [12]. Policyn säger att om en SP är kategoriserad som R&S så får den en uppsättning attribut av IdP:n. InCommons IdP:er uppmanas bland annat att releasa följande attribut till R&S-klassade SP:er:

- Personal identifiers: email address, person name, `eduPersonPrincipalName`
- Pseudonymous identifier: `eduPersonTargetedID`
- Affiliation: `eduPersonScopedAffiliation`

2.2.1.5 Code of Conduct

Code of Conduct är ett annat sätt att försöka öka IdP:ers vilja att releasa attribut. Det har blivit formulerat som en servicekategori och det finns ambitioner inom REFED att standardisera det. I huvudsak så handlar det om att en Code of Conduct-enablad SP förbinder sig att säkerställa att följa Europeiska dataskyddslagar eller om det är utanför Europa skydda data på motsvarande sätt som våra lagar föreskriver [13] samt att inte lämna vidare attributdata till annan part.

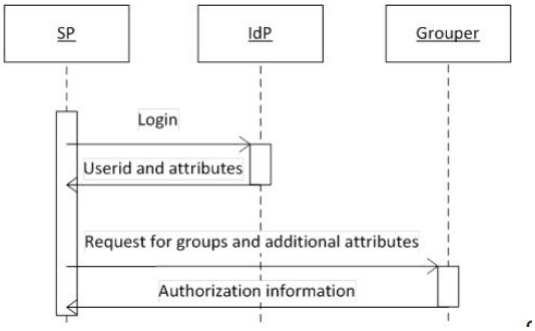
2.2.2 Aktuell forskning

Det pågår just nu ett forskningsprojekt finansierat av EU och lett av GARR, Italiens motsvarighet till SUNET, där syftet är att utöka autentiseringsfunktionen inom federationer och lägga till auktorisation. Man delegerar då just auktorisation till ett specifikt system som även kan vara centraliserat. Man har för det syftet valt att utvärdera Grouper för att användas över och inom organisationsgränser. Grouper används i sammanhanget för att hantera, på ett centraliserat sätt

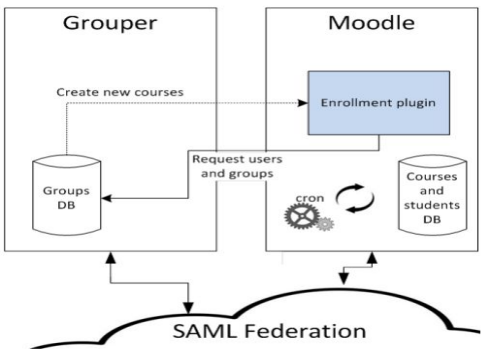
- grupper av användare
- utdelning av attribut för användare

De arbetar i projektet med en PoC där de testkör integration mot tre applikationer: MediaWiki, Moodle och en anpassningsbar testapplikation.

För MediaWiki är syftet att Grouper skall hantera användargrupper och läs/skriv access enligt modellen till höger. IdP:n autentiserar användaren och Grouper auktoriserar användaren.



Figur 7 Integration med MediaWiki



Figur 8 Integration med Moodle

För integrationen med Moodle är tanken att medlemmarna i de grupper i Grouper som motsvarar kursgrupper kan exporteras till Moodle som typ kurslistor. Integrationen görs via VOOT som är ett protokoll för att utbyta gruppinformation till

externa applikationer.

Med den anpassningsbara testapplikationen vill man utvärdera och förstå hur nya applikationer bäst kan designas för att bli fullt kompatibla med en delegerad auktorisationsprocess samt att studera hur man direkt kan hantera användares auktorisationsattribut och inte bara grupper.

2.2.3 Molntjänster

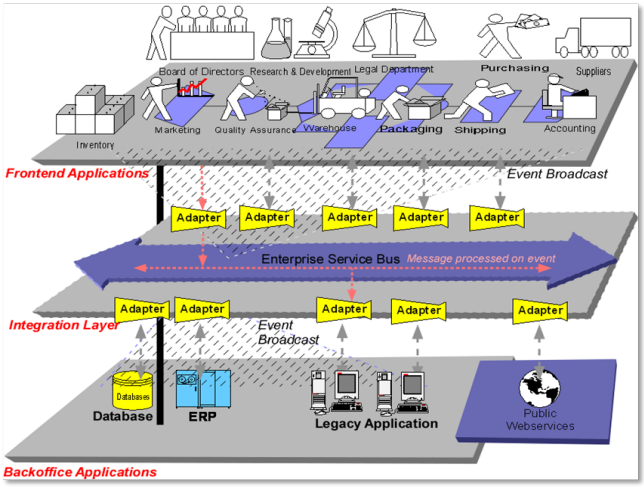
Den rådande trenden är att allt fler organisationer använder sig av molntjänster. Dessa kan främst sorteras i tre kategorier:

- SaaS-tjänster - Software as a Service. Det är något som redan används av universitets- och högskolevärlden. Många lärosäten använder sig idag av Office 365, andra exempel är Google Apps och Box.
- PaaS-tjänster – Platform as a Service. Levererar en middleware-plattform kanske främst för applikationsutveckling. Uppenbara fördelar är att det gör det snabbt att komma igång och utveckla din applikation, du behöver inte fundera på integrationsproblem samt att applikationen skalar upp av sig själv när antalet användare ökar. Heroku och Google App Engine är exempel på en sådana plattformar.
- IaaS-tjänster – Infrastructure as a Service. Levererar en mer komplex infrastruktur som kan innebära både fysiska och virtuella maskiner, lagring samt nätverkskomponenter.

SOA - service oriented architecture eller tjänsteorienterad arkitektur, är en arkitektur som erbjuder ett ramverk för att implementera ”software as services” som enkelt kan delas, återanvändas och integreras. En SOA är ofta uppbyggt av ett gäng fristående webbtjänster. SOA är också den bakomliggande arkitekturen i ESB, Enterprise Service Bus, som erbjuder ett agilt och flexibelt sätt att kommunicera mellan applikationer och system.

En ESB:s främsta uppgift är:

- Monitorera, kontrollera och förmedla meddelanden mellan tjänster
- Lösa kommunikationsproblem mellan kommunicerande komponenter
- Kontrollera driftsättning och versionshantering av tjänster
- Agera vakt mot användning av redundanta tjänster
- tillgodose bastjänster som händelsehantering, dataomvandling, mappning, meddelande- och händelseköer, sekvensering, säkerhet- eller felhantering, protokollkonvertering och upprätthållande av kommunikationskvalitet



Figur 9 Illustration av ESB från wikipedia

Utifrån ett identitetshanteringsperspektiv är en av nycklarna till att uppnå säkerhet i en SOA-arkitektur, ”identity externalization”. Det innebär att man lyfter ut användar- och säkerhetspolicydata från applikationerna själva. Det ökar säkerheten genom att användardata inte

behöver kopieras och ligga i flera system. Det underlättar också vid utveckling och integration av ny programvara då identitets- och behörighetskontrollen sker utanför själva applikationen/tjänsten i sig och inte behöver byggas in i applikationen.

SaaS-tjänster kan förekomma både lokalt och i molnet. Det vanligaste för oss inom universitets- och högskolevärlden är troligen en hybridlösning där vi använder både interna och externa Saas-tjänster men fortfarande har många andra tjänster lokalt.

Exempel på utmaningar i samband med molntjänster

- SSO-inloggning: Lokalt har många idag SSO för inloggning och det är en funktion man vill behålla istället för att användare skall ha olika användarnamn och lösenord för olika molntjänster.
- Aktivering och deaktivering av konton: När en person anställs vill vi snabbt och effektiv se till att den anställde får tillgång till alla applikationer och resurser, inklusive molntjänster, som den behöver för sitt arbete. När en person slutar sin anställning vill vi ha en lika effektiv och smidig process fast omvänt som säkerställer att denna person inte längre har tillgång till dessa applikationer och resurser. Den bästa molnanpassade IAM-hanteringen-bör tillhandahålla en centraliserad, out-of-the-box integration med en central AD och LDAP. När användare läggs till eller tas bort i AD eller LDAP skall tillträde till molntjänsterna aktiveras/inaktiveras automatiskt.
- Vem har tillträde till vad: Det är viktigt att förstå vem som har tillträde till vad samt var och när de har tillträde till det.
- Hur stödjer man ”var som helst, när som helst, från alla typer manicker som har kontakt med internet, och med webb-SSO från alla typer av webbläsare”, utan att tumma på säkerheten.
- Molnapplikationer förändras och uppdateras och det skall kunna ske transparent för användarna. Det vill säga integrationslösning, interface och kommunikation skall fortsätta att fungera även när applikationen förändras.
- Olika molntjänster kan administreras av olika enheter i organisationen. Hur implementerar man en säkerhetsmodell som delger rätt administrationsrättigheter till rätt användare.
- Hur får man ut bra rapporter över hur användare använder molntjänsten så att man vet att man bara betalar för det man utnyttjar?

2.2.4 Identiteter

I Norge har man infört en centraliserad identitetslösning i form av ***Feide*** [14], en elektronisk identitet som alla elever i Norge kan använda för federerad inloggning i sin nuvarande skolas portaler, lärplattformar, program för elevadministration, skolskjuts samt bibliotek med mera. Arbetet med Feide påbörjades år 2000 och idag är 82% av eleverna i grundskolan kopplade till Feide och 100% av studenterna i högre utbildningar (undantaget eventuellt några privata lärosäten). Federationen använder bland annat norEdu* Object Class specification. Senaste versionen 1.5.1 från January 2015 är den sjunde uppdaterade versionen av norEdu Object Class.

2.2.4.1 SWAMID och eduID

I Sverige har vi idag en centraliserad identitetsleverantör för studenter i form av eduID. Sveriges identitetsfederation för universitet och högskolor heter SWAMID [15].

SWAMID erbjuder en kvalitetssäkrad och säker identifiering av anställda, studenter, alumner och andra associerade med forskning och högre utbildning i Sverige, de nordiska länderna, övriga Europa samt även i USA och Asien. Exempel på teknologier där vår hemidentitet används idag är eduroam för trådlösa nätverk runt om i hela världen, samt SAML WebSSO för access till webbapplikationer.

När det gäller Federated Access Management har vi kanske inte kommit så långt i Sverige delvis på grund av att man inom SWAMID inte i någon vidare utsträckning har förhandlat fram gemensamma regler och policys för de attribut som kan användas för att tillstyrka respektive avslå tillträde till begärda resurser. Vidare underlättas för effektiva federerade lösningar att man på varje lärosäte implementerar lösningar som gör att man kan få tillträde till olika system och resurser via en SP, dvs en tjänsteleverantör som oftast pratar SAML.

Det traditionella alternativet om man inte har en federerad identitetslösning är att det skapas ett lokalt datakonto för den externa personen och att man manuellt administrerar tillträde till olika resurser för detta konto. Det finns dock ingen enhetlig policy kring hur man löser det utan det sker enligt varje lärosätes unika praxis eller beslutade policy.

eduID erbjuder en gemensam identitetsinfrastruktur till blivande och existerande studenter i Sverige. eduID erbjuds till lärosäten som är anslutna till SWAMID. Tjänsten förvaltas och styrs av SWAMIDs styrgrupp och den dagliga driften hanteras av NORDUnet och NUNOC. eduID är gratis för slutanvändare och erbjuds även gratis till lärosäten under 2014. Under 2015 är det sagt att en finansieringsmodell kommer att tas fram och beslutas [16].

Studenter skapar sitt eget eduID konto genom att registrera sig på eduID.se [17]. Identiteten är tänkt att kunna användas för

- Antagning.se
- Skapa användare/konto på lärosätet
- Sätta om sitt lösenord
- Logga in till tjänster I SWAMID för personifiering
- Interaktion mellan högskolor och externa organisationer

Inför framtiden så finns det i och med införandet av eduID möjlighet för Sverige att ha ett liknande system som Feide i Norge för elever från grundskola upp till högre utbildningar. Det skulle förmodligen underlätta på många sätt både för studieadministratörer och eleverna själva. Om vi når dit återstår ännu att se men det kan vara värt att ha i åtanke när man planerar för framtida IT-satsningar på våra lärosäten.

I Sverige skulle vi om vi vill kunna lita på varandra fullt ut i ett federerat sammanhang troligen behöva en samsyn på hur vi skall kategorisera våra olika typer av användare. Det vill säga, en samsyn och gemensamma regler för livscykelhantering kring när man räknas som student, hur man hanteras efter att man studerat klart och när man tar studieuppehåll. Likväl skulle vi behöva en samsyn för hur vi hanterar personal men framförallt hur vi hanterar ”övriga”, dvs de som faller utanför kategorin anställd och student. Gruppen ”övriga” bidrar bland annat till att göra licensarbetet juridiskt vanskligt. Liksom i Norge borde vi i Sverige fundera på om vi kan hitta en samsyn kring denna grupp och få denna samsyn accepterad tvärs över hela universitets- och högskolesektorn.

Om vi tittar globalt är en trend att identiteter används allt flitigare mellan våra sociala media. Till exempel kan du logga in i Spotify med din facebookidentitet. Om säkerhetsnivån inom social media ökar till en nivå som är acceptabel även i andra sammanhang så finns det de som tror att vi kanske på sikt bara kommer att ha en nätidentitet eller i varje fall kan använda den även på våra lärosäten. Det är en intressant tanke. Hur påverkar det våra system i så fall?

2.2.5 Från IAM till IRM

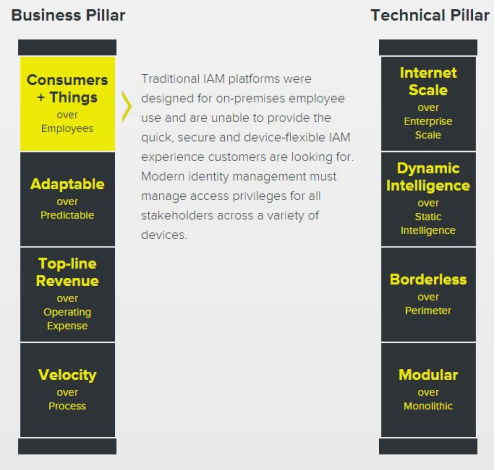
Den rådande trenden med ”the internet of things”, dvs att saker får identiteter samt att människor numera kan koppla upp sig med nästan vad som helst varsomhelst ifrån och utföra allehanda ärenden har lett till en utveckling från traditionell IAM som huvudsakligen servar en organisation internt till IRM, Identity and Relationship management. Grundpelarna i IRM är:

För business:

1. Konsumenter + saker före Anställda
2. Anpassningsbart före förutsägbart
3. Maximerad förtjänst före rörelsekostnader
4. Snabbhet före processer

För Tekniken:

1. Internet före internt
2. Dynamisk intelligens före statisk intelligens
3. Gränslöst före yttre försvarsverk
4. Modulärt före monolitiskt



Figur 10 Grundpelarna i IRM enligt Forgerock

Det man relaterar till när det gäller punkt ett, dvs översta nivån i pelarna i Figur 10, är att dagens medborgare och studenter förväntar sig att de skall kunna koppla upp sig med sin mobiltelefon, sin laptop, sin läsplatta eller kanske sin bil via internet mot sin bank, sin mataffär, sitt arbete och utföra allehanda saker såsom betala varor, beställa varor, beställa tjänster, hämta och editera dokument, läsa e-post, delta i videokonferenser osv...
Detta har lett till ett skifte där vi går ifrån den stängda skyddade organisationens värld till ett öppet men i den bästa av världar fortfarande pålitligt säkert universum av applikationer och mobila enheter som ständigt utvecklas. Verktyg för identitets- och accessmanagement behöver därför klara av att hantera relationer med partners både inom och utanför organisationen. Därav Identity and Relationsships Management istället för Identity and Access Management.

I andra steget i pelarna i Figur 10, Adaptable och Dynamic intelligence handlar det om att en användare loggar in utifrån eller från en annan enhet än de brukar så kan systemet känna av att nu är förhållandena mer osäkra än det skulle vara om användaren loggar in från det interna nätet eller från sin egen device. Det triggar då till exempel att systemet kräver ytterligare ett autentiseringssätt förutom enbart lösenord.

Nivå tre, Top line revenue och Borderless, berör det faktum att applikationer kan finnas både lokalt och i molnet och att lösningar skall vara så säkra och effektiva att både anställda och kunder/konsumenter skall kunna lita på att det är säkert att använda dem oavsett varifrån, vilken enhet, vem och när du vill använda dem.

Nivå fyra, Velocity och Modular, adresserar problemet med flexibilitet och snabbhet både när det gäller svarstider samt att koppla in nya tekniker och applikationer. Anställda har traditionellt fått finna sig i långsamma servicerutiner men dagens kunder kommer inte att finna sig i det. Angreppssättet är modulärt uppbyggda system som är designade att hantera komplexitet på ett snabbt och flexibelt sätt.

2.3 SUMMERING

Den samlade bilden är att kraven på IT-enheter på högskolor och universitet är densamma världen över när det gäller att leverera en effektiv och säker IT-miljö som så långt det är möjligt stödjer våra användares behov, det vill säga, att enkelt kunna samarbeta, samt ha tillgängliga och effektiva IT-applikationer, system och resurser. Molntjänster, mobila användare, sociala medier och federationer har ökat behovet av en effektiv, väldesignad och överblickbar IT-infrastruktur för identitetshantering och behörighetsstyrning, eftersom denna teknikutveckling har förändrat sättet som organisationer exponerar affärskritiska tjänster och data.

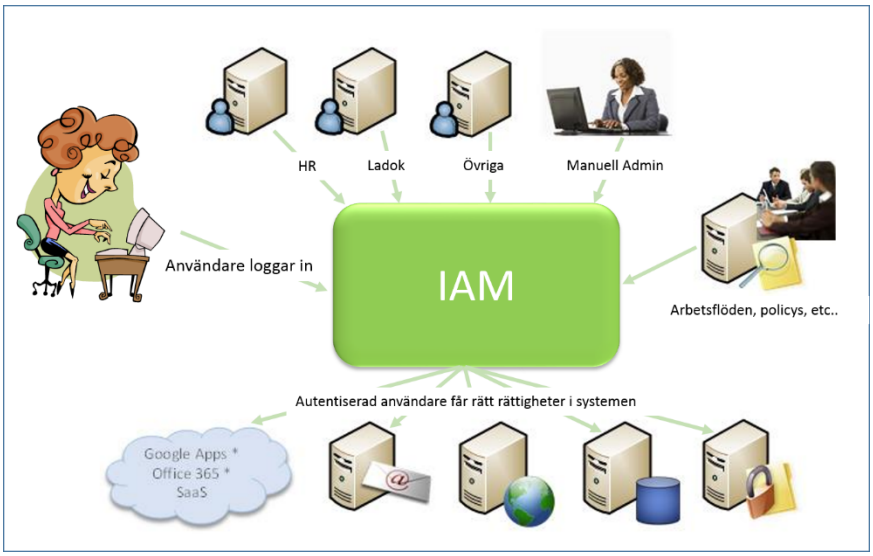
För oss inom universitets- och högskolevärlden gäller att vi, förutom att hålla jämna steg med omvärlden och möta våra användares behov av IT-lösningar, har krav på oss att beakta och i den mån vi har möjlighet, understödja både Sveriges och EU:s politiska visioner samt den globala forskningsvärldens nutida och potentiellt framtida behov av e-infrastruktur. En utmaning som både ställer stora krav på våra IAM- eller IRM-system och vår samarbetsförmåga.

Frågan är i vilken utsträckning vi i Sverige behöver följa Norges exempel och arbeta för att standardisera vissa processer kring vår användarhantering. Det handlar till exempel om processerna kring livscykelhantering, roller och attributvärden. Att alla lärosäten till exempel har samma regler för vem som är student, när man blir student och hur länge man får behålla ett studentkonto samt definitioner av roller och attribut för våra anställda som är gemensamma och kan exporteras till en SP. Ur rättssäkerhetssynpunkt kan det även vara värt att fundera över vissa saker som hör samman med myndighetsutövning, till exempel hur länge efter att man har avslutat sin anställning man kan skicka e-post från sitt anställdakonto med mera.

3 IAM - IDENTITY AND ACCESS MANAGEMENT

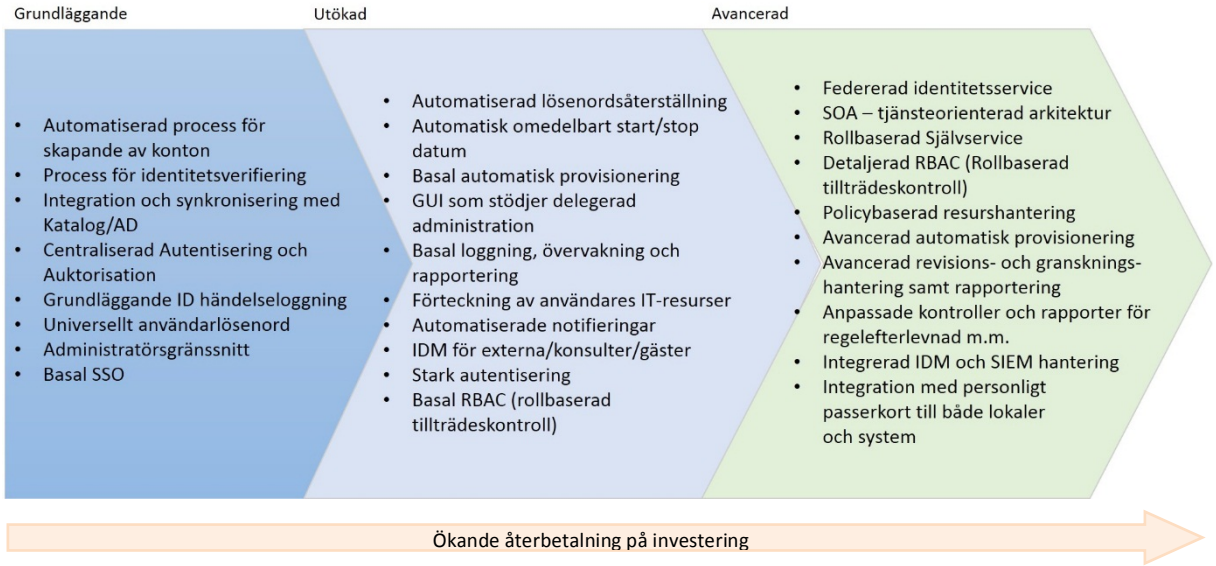
Kortfattat beskrivet är Identitets- och behörighetshantering den säkerhetsdisciplin som ger rätt individer tillgång till rätt resurser, vid rätt tidpunkt och av rätt orsak.

IAM kan definieras som ett antal processer och teknologier som effektivt och konsekvent hanterar ett antal användare och deras behörigheter i multipla system och applikationer. Målsättningen är att ge varje användare exakt de behörigheter de behöver.



En organisation som bygger upp en välutvecklad identitets- och behörighetshantering kan reducera en stor del av sina kostnader, och kanske ännu viktigare, blir mer flexibla när det gäller möjligheten att stödja nya utvecklings- och forskningsinitiativ.

Generellt har många organisationer kommit rätt långt när det gäller identitets- och kontohantering (se Figur 11 nedan) medan det fortfarande finns mycket att göra när det gäller att slå samman behörighetshantering för en organisations olika system och applikationer och införa en mer automatisk och enhetligt hantering.



Figur 11. Mognadsnivåer – Identitetshantering, enligt Novell 2008

I takt med att kraven på behörighetskontroll för olika system har uppstått har IT-enheter ofta utvecklat en mix av punktlösningar. Varje lösning har adresserat ett säkerhetsbehov för en viss applikation eller ett visst system. Resultatet är ofta ett lappverk av olika tekniker för behörighetskontroll vilket skapat IT-miljöer som både är komplexa att administrera samtidigt som de kanske naggat onödigt mycket på IT-budgeten.

I vissa fall har den komplexa miljön även fungerat som en bromsande faktor för IT-enheters möjligheter att möta sin organisations nya behov. Det kan i sin tur ha lett fram till att organisationer delvis valt att gå förbi sina IT-enheter och istället använt sig av så kallad ”Shadow IT” eller Saas-lösningar som inte är sanktionerade av IT-enheten. Detta kan bland annat orsaka att en organisation inte längre har bra kontroll och överblick på hur och var allt data lagras och vem som har tillgång till det, samt annan säkerhetsproblematik.

Genom att lyfta in behörighetshantering och kontroll från olika applikationer till en centralt administrerad funktion kan en organisation dels få en bättre överblick av vem som har behörighet att göra vad med företagets eller organisationens olika resurser. Det blir även lättare med övervakning och kontroll av regelefterlevnad och spårbarhet, där man kan se vem som gjort vad och när, samt att producera rapporter och statistik.

En väl utvecklad identitetshantering och behörighetsstyrning syftar bland annat till att

- införa användarprovisionering som gör skapande, underhåll och deaktivering av inloggningskonton, hemkataloger, e-postmappar, behörigheter och liknande snabbare, billigare och mer pålitligt.
- strömlinjeforma IT genom att ersätta behovet att administrera ett flertal sidosystem och webbagenter för att uppnå en komplett behörighetsstyrning.
- Supporta nya tjänster inklusive mobilitet och molnet (sociala identiteter?)
- Öka skalbarhet och flexibilitet
- Öka IT-effektivitet genom förenklad installation, konfiguration, integration och delegerad administration

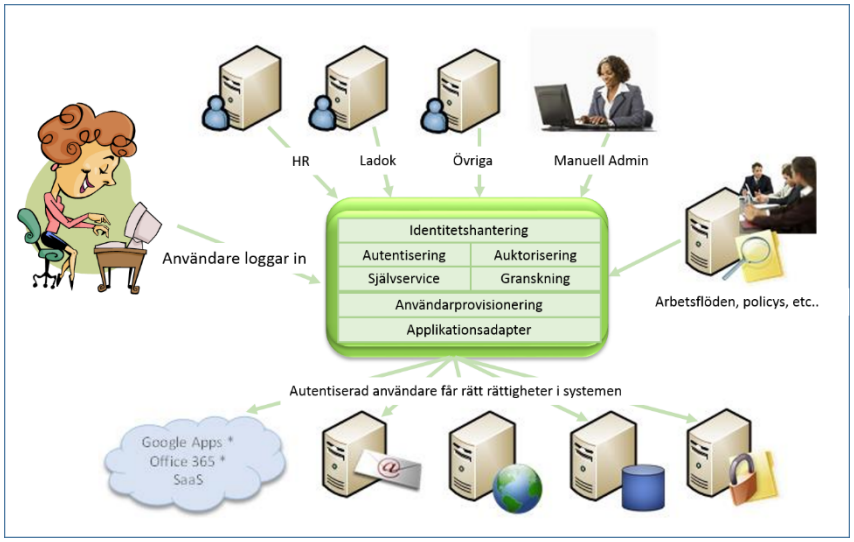
En centralt administrerad behörighetshantering erbjuder också fler möjligheter till behörighetsstyrning och kontroll än vad varje applikation erbjuder, då man i den centrala behörighetshanteringsfunktionen har möjlighet att addera mer finkorniga regler än vad enskilda applikationer i sig erbjuder. Detta i sin tur kan innebära att applikationer inte alltid behöver modifieras varje gång verksamheten ser ett behov av nya behörighetsnivåer eller regler.

I takt med att organisationers IT-infrastruktur växer blir det en utmaning att administrera infrastrukturen och speciellt att administrera användare, deras identitetsprofiler och säkerhetsprivilegier.

Det problem man bland annat vill adressera med ett väldesignat IAM-system är alltså att information om användares identiteter samt vilka resurser de har tillträde till är spritt på för många system vilket får som konsekvens att det är svårt att överblicka och administrera.

3.1 GENOMGÅNG AV BEGREPP OCH BEST PRATICE

Ett väldesignat IAM system tillhandahåller funktionalitet för Identitets- och livscykelhantering samt behörighetskontroll över resurser. Det inkluderar policys, processer och arbetsflöden för on-boarding, off-boarding, modifiering av identiteter, autentisering, auktorisering, användarprovisionering, verkställande av rättigheter, övervakning, statistik och rapportering.



3.1.1 Identitetshantering

Identitetshantering refererar till en uppsättning teknologier och processer som på ett enhetligt och pålitligt sätt hanterar information om användare i en organisation där användare typiskt har tillgång till multipla system och applikationer. Typiska identitetshanteringsscenarios är:

- Lösenordssynkronisering och automatiserad process för lösenordsåterställning,
- användarprovisionering inklusive identitetssynkronisering
- automatisk provisionering och deaktivering av konton,
- SSO, Webb SSO

3.1.2 Behörighetshantering

Behörighetshantering refererar till en uppsättning teknologier och processer som på ett enhetligt och pålitligt sätt hanterar säkerhetsprivilegier inom en organisation. Målsättningen är att reducera kostnader för administration, förbättra service, samt försäkra sig om att användare får exakt de rättigheter och behörigheter de behöver.

Denna målsättning uppnås genom att det skapas en uppsättning robusta, konsekventa processer som beviljar och återkallar behörigheter i organisationens system och applikationer enligt följande:

1. Skapa och regelbundet uppdatera en konsoliderad databas som håller behörigheter
2. Definiera roller, så att behörigheter kan tilldelas användare i grupper som är lättare för systemanvändare att förstå.
3. Möjliggöra självservice och delegerad administration, så att beslut om behörigheter kan tas av användare med kunskap om sammanhanget, hellre än av IT-personal.
4. Synkronisera behörigheter mellan system, där det är möjligt.
5. Regelbundet bjuda in aktuella aktörer att gå igenom behörigheter och användares roller och identifiera de som inte längre är aktuella och därmed föremål för framtida översyn och/eller borttagning.

3.1.3 SoD

SoD, Separation of Duties eller Segregation of Duties, är ett vedertaget begrepp inom finanssektorn men är nog inte lika vanligt i andra IT-sammanhang. En översättning blir ”separation eller uppdelning av arbetsuppgifter”. SoD är ett nyckelkoncept för interna säkerhetskontroller och dess främsta syfte är att undvika bedrägeri och missbruk men även felaktigheter som beror på misstag. Detta mål kan uppnås genom att sprida uppgifter och tillhörande behörigheter för en viss affärsprocess mellan flera användare.

Säkerhetskontroller syftar till att skydda informationssystem, både data och nätverk, när det gäller konfidentialitet, integritet och tillgänglighet. Säkerhetskontroller designas utifrån den riskbedömning man gjort på ett visst system. Kontroller kan bland annat begränsa hur mycket en och samma person kan göra i ett system. Med SoD kan man se till att en och samma person inte är ansvarig för att rapportera om sig själva till sina överordnade samt att en person inte kan ha två konfliktande funktioner eller kan introducera bedräglig eller skadlig kod utan att undgå upptäckt.

Strikt kontroll av förändringar i mjukvara eller data kräver till exempel att en och samma person endast har en av följande roller:

- Identifiera behov av förändring och lägga in en CR
- Besluta om förändring
- Designa och implementera förändring
- Bekräfta och testa förändring samt granska kod
- Driftsätta

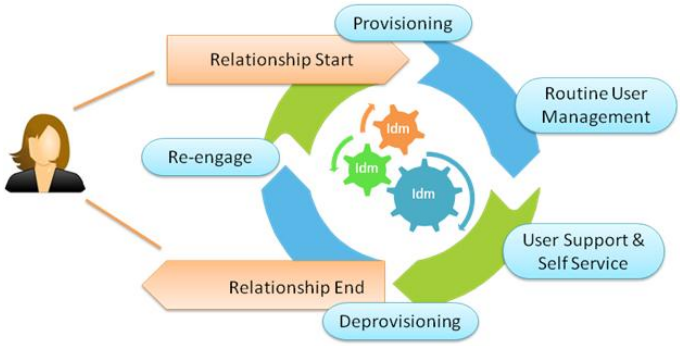
Om en säkerhetskritisk uppgift inte går att separera så får man införa kompenserande kontroller. Det kan handla om:

- att det krävs att ytterligare en person godkänner innan förändringen slår igenom
- att man delat en säkerhetsnyckel på två personer
- att man har steg för steg instruktioner där alla moment måste utföras i tur och ordning
- att man har bra audit-loggar som beskriver exakt vem som gjort vad och vilka filer och vilket data som uppdaterats

3.1.4 Livscykelhantering

3.1.4.1 On-boarding – relationen börjar

Nya användare behöver komma igång snabbt. Varje försening när det gäller behörigheter till system kostar pengar i form av förlorad produktivitet (och ibland förtroende).



IT-administratörer behöver vara säkra på att nya konton är korrekta. Processen att begära, granska och godkänna säkerhetsförändringar implementeras företrädesvis som ett automatiserat flöde där personer själva kan begära rättigheter där begäran automatiskt sänds till i förväg utsedda personer för elektroniskt

godkännande. Det kan bespara överdriven ansträngning av både tillståndsgivare och mottagare samt undvika onödig fördröjning.

En ny användare behöver typiskt rättigheter i flera system, t.ex. e-post, inloggning i nätverk och applikationer samt tillgång till filarea. Ifall dessa hanteras av olika administratörer och i olika verktyg blir det en kostsam dubblering i administrationskostnad för varje verktyg och även den processen bör automatiseras och hanteras enligt i förväg bestämda defaultmallar.

3.1.4.2 Användarprovisionering

Med användarprovisionering avses en gemensam IT-infrastruktur som lyfter in administrationen av användare, identitetsattribut samt säkerhetbehörigheter från individuella system och applikationer in till denna gemensamma infrastruktur. Avsikten med användarprovisionering är att göra skapande, underhåll och inaktivering av login-konton, hemkataloger, e-postfoldrar, säkerhetsprivilegier och liknande snabbare, billigare och mer pålitligt. Detta åstadkoms genom att automatisera och koda processer kring identitetshantering och koppla dessa till olika system.

System med användarprovisionering har automatiserat en eller flera av följande processer:

- Automatisk provisionering
- Automatisk inaktivering
- Identitetssynkronisering
- Självservice
- Delegerad administration
- Behörighetscertifiering
- Flöde för auktorisation
- Rapportering

Automatisk provisionering innebär att nya uppgifter och ändringar upptäcks av systemet (i till exempel i HR-systemet eller Ladok) vilket automatiskt triggar aktiviteter såsom skapande av konto, synkronisering av identiteter och tilldelning av tillbörliga behörigheter i mappar, e-postlistor, system och applikationer. Detta kräver att:

- Det finns ett registersystem med alla användare
- Systemet håller korrekt information
- Systemet uppdateras kontinuerligt

Hur mycket man kan göra per automatik är beroende av hur mycket information man kan få ut från källsystemen men även av hur väl fördefinierade roller och mallar för behörigheter man har.

RBAC, Rollbaserad Access Control, fungerar bra när man har ett stort antal användare som skall ha samma säkerhetsprivilegier men inte för användare som har unika säkerhetsprivilegier. RBAC kräver också väl definierade roller/funktioner med tillhörande rättighetsmallar inom hela organisationen samt att de är vedertagna och används lika av alla.

Om man enbart satsar på RBAC så finns risk för rollexplosion och man kan på sikt få ett system där antalet roller är fler än antalet anställda.

Bra provisionering bör vara konsekvent, pålitlig, flexibel, granskningsbar, skalbar och integreras.

Automatisk inaktivering innebär, att för användare som inaktiveras eller tas bort ur källsystem, inaktiveras eller tas användarkontot bort automatiskt samt att användarens säkerhetsprivilegier i alla system och applikationer automatiskt återkallas.

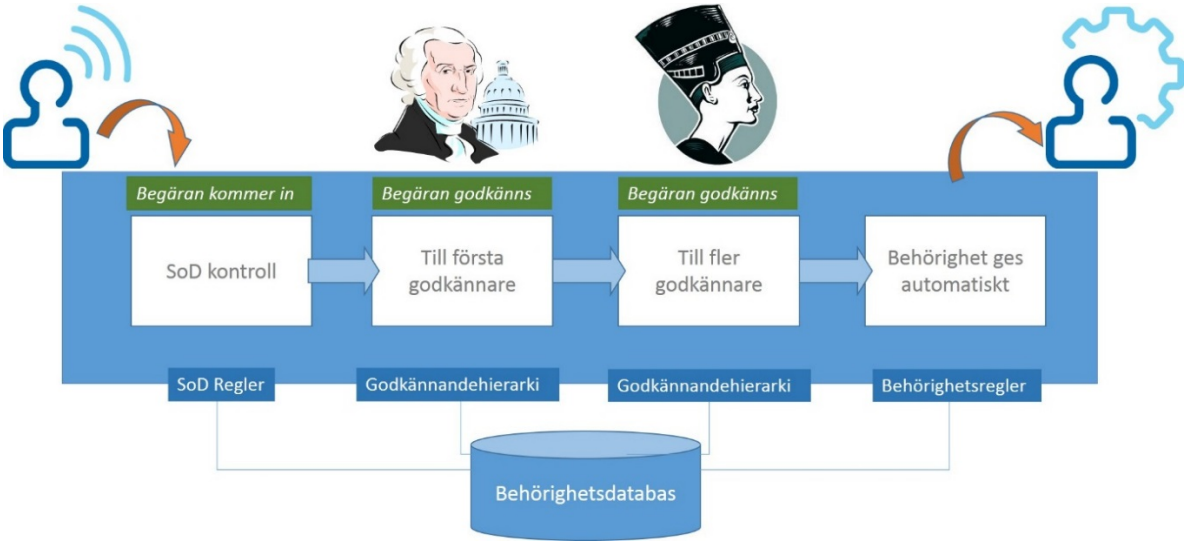
Identitetssynkronisering innebär att förändringar av persondata upptäcks av systemet och att förändringen automatiskt synkroniseras ut till alla system som berörs av ändringen. För effektiv hantering bör man identifiera vilket system som har den mest pålitliga informationen och synkronisera därifrån samt aldrig ha redundant information i system i onödan.

Självservice förutsätter någorlunda datorvana användare och ett användarvänligt system. Idealiskt erbjuds varje användare enbart möjlighet att begära behörigheter som de har förutsättningar att få. Självservice innebär att användare tillåts:

- uppdatera sina profiler såsom adress och telefonnummer
- begära medlemskap i grupper
- begära nya behörigheter
- begära återställning eller nytt lösenord

Delegerad administration innebär att chefer, systemägare eller andra intressenter ges rättighet att inom sina respektive auktorisationsområden godkänna eller avslå användares begäran om nya behörigheter samt att se listor på användare och deras respektive behörigheter. Se Figur 12

Behörighetscertifiering innebär att chefer och systemägare och andra med delegerad administrationsrätt på regelbunden basis tvingas gå igenom sina listor med användares behörigheter och bekräfta att de är korrekta.



Figur 12. Delegerad administration och automatiserat flöde för auktorisation

Flöde för auktorisation innebär att föreslagna förändringar skall styrkas genom att aktuella intressenter bjuds in att godkänna dem innan de genomförs i integrerade system och applikationer. Dessa intressenter utgörs typiskt av chefer, systemägare, informationsägare och säkerhetsansvariga. Detta bör gälla oberoende av förslagets ursprung. Av effektivitetsskäl kan tänkas att ändringar som kommer från en hundra procent pålitlig källa och som på inget sätt kan utgöra en säkerhetsrisk undantas från regeln. Överarbeta dock inte så att allt måste specificeras. Sträva efter att hitta övergripande generella regler för vem som ges auktorisation att godkänna baserat på vilken typ av begäran det gäller, vem som begär, vilken typ av resurs det gäller osv..

Frågor man bör besvara i detta sammanhang är:

- Hur skall olika typer av ändringsbegäran valideras (syntax, rätt ifyllda fält, konsekvenser)
- Vem skall godkänna
- Förväntad svarstid
- Vilka delar av begäran skall den som godkänner få se
- Vilka delar av begäran skall den som godkänner tillåtas modifiera
- Om en grupp personer skall godkänna, hur många av dessa behöver tillstryka för att begäran skall anses godkänd

Svaret på dessa frågor är förstås inte exakt lika för varje typ av begäran. En rekommendation är att man planerar att fler kan godkänna än vad som i realiteten behövs eftersom det händer att människor är bortresta, har tjänstledigt, har semester, eller blir sjuka. Lägg också in automatiska påminnelser till de som inte svarar inom rimlig tid. Bestäm även flöden och policys för, när man vid uteblivet svar, kontaktar nästa person som kan godkänna. Tillåt även att den som skall godkänna, temporärt kan delegera detta till någon annan, till exempel när de vet att de inte kommer att kunna nås.

Rapportering innefattar rapporter över vilka användare som har vilka säkerhetsprivilegier, grupptillhörigheter, vilande konton, föräldralösa konton, ändringshistorik osv, för alla system och applikationer. Alla användare, identitetsattribut och säkerhetsprivilegier skall gå att presentera på ett läsbart och överskådligt sätt. Data om användare, identitetsattribut och säkerhetsprivilegier bör lagras i en normaliserad relationsdatabas med ett väldokumenterat schema. Det gör det möjligt att utveckla anpassade rapporter utöver de som eventuellt finns inbyggda i systemet självt.

Rapporter används typiskt i följande sammanhang:

- I vardagsarbetet för att svara på specifika frågor och felsöka
- För regelbundna kontroller:
    - Identifiera om någon överträder SoD regler
    - Identifiera vilka som har tillträde till känsligt data/känsliga system
    - Övervaka prestanda och nyttjandegrad i systemet (typ hur många konton som skapas och antal förfrågningar om nya behörigheter osv)

3.1.4.3 Rutinmässig användaradministration

Samma utmaningar gäller generellt för ändringar och underhåll av användarkonton som när det gäller att skapa nya, dvs man vill att ändringar skall få genomslag direkt utan onödig fördröjning. Användare byter till exempel ofta roller och ansvarsområden inom en organisation och identitetsattribut såsom adress och telefonnummer ändras. En speciell utmaning i detta sammanhang är byte av interimspersonnummer.

Alla rutinändringar bör hanteras så smidigt och effektivt som möjligt.

3.1.4.4 Användarsupport och självservice

Vid daglig användning av system uppstår ofta samma typ av problem återkommande för användarna som kan kräva teknisk support:

- Glömt lösenord
- Utlåsning på grund av att någon försökt för många gånger med fel lösenord
- Felaktigt nekad access till en resurs/service/applikation

Detta är tillsammans de problem som ofta orsakar en stor del av de ärenden som hamnar hos IT-supporten. Det innebär direkta personalkostnader samt indirekta kostnader i produktionsbortfall och löses företrädesvis med självservice och delegerad administration där så är möjligt.

3.1.4.5 Terminering – deprovisionering

Alla användare slutar någon gång. När de gör det behöver det träda i kraft robusta processer som rensar användarens alla säkerhetsprivilegier i olika system. Dessa processer behöver vara:

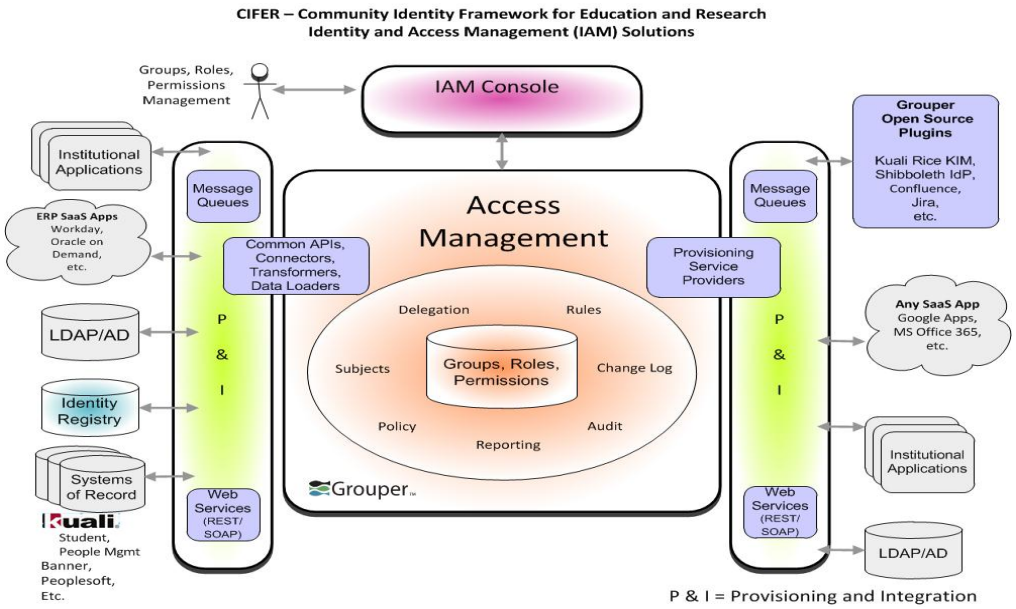
- Pålitliga
  - Om en organisation misslyckas med att inaktivera åtkomst av system för en användare som slutat, kan användaren använda systemet även efter den har slutat och eventuellt stjäla eller förändra data eller sälja möjligheten att logga in i systemet till en inkräktare.
- I rätt tid
  - Att avsluta en användares rättigheter att komma in i system skall ske snabbt för att hindra möjligheten att systemet används av en användare som inte längre skall ha rätt att använda systemet.
- Fullständiga
  - Det räcker inte att inaktivera en användares konto. Varje behörighet som användaren kan ha haft till olika system skall återkallas.

3.2 IAM INOM HÖGSKOLE- OCH UNIVERSITETSVÄRLDEN

Målbilden med IAM inom Internet2 är att åstadkomma en arkitektur som liknar den bild som presenteras i Figur 13.

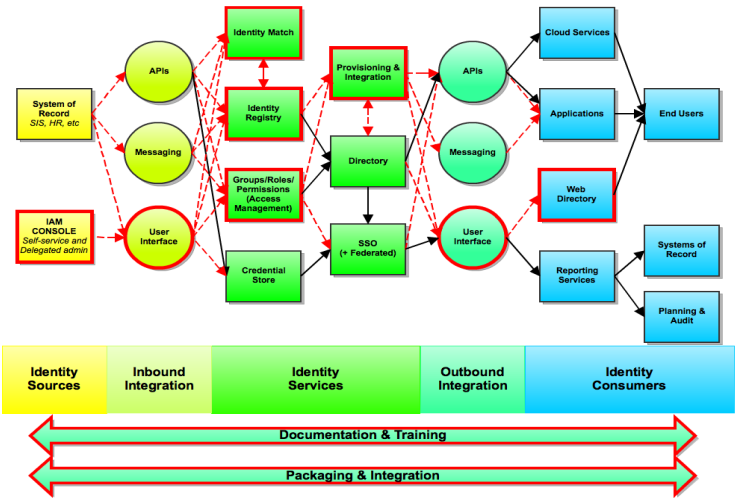
Bilden är hämtad från CIFER så det förekommer ett antal källsystem som mest används på amerikanska lärosäten men idén blir ändå tydlig. Ni får i tanken ersätta dessa med Ladok och Primula.

Att bygga en sådan arkitektur som presenteras i Figur 13 förutsätter att man bygger lösningar där man undviker applikationssilos samt på sikt planerar att integrera såväl källsystem som majoriteten av alla målsystem i det centrala IAM-systemet. Gärna med en integrationsplattform/ESB.



Figur 13 Konceptbild över IAM inom Internet2 och CIFER

Internet2 arbetar som tidigare nämnts med att accelerera införandet av IAM inom universitets- och högskolevärlden. Avsikten är att bygga open source produkter för att åstadkomma den modulbaserade IAM-arkitektur man siktar på att med gemensamma ansträngningar bygga. Eftersom vi har mycket gemensamt med dem och deras lösningar dessutom är open source så blir det förstås intressant för oss att titta på vilka aktiviteter som pågår där.



Figur 14 Funktions och flödesvy över CIFERS referensarkitektur (draft)

I Figur 14 markeras de områden som CIFER identifierat som potentiella områden för signifikant CIFER-samarbete med en tjock röd linje runt. Somliga av dessa skulle kanske även vara intressanta områden för oss i Sverige att samarbeta kring?

Även om vi har viss konkurrens mellan lärosäten när det gäller att attrahera studenter och få forskningsmedel så är vi i ett större perspektiv konkurrensutsatta från resten av världen.

I det perspektivet blir det mer intressant att tillsammans tillhandahålla en effektiv och smidig IT-infrastruktur för våra svenska forskare och studenter, vilket de facto är en grundförutsättning för att vi skall kunna utvecklas i takt med omvärlden och ligga i framkant kunskaps- och innovationsmässigt.

4 GRUPPHANTERING FAQ

Så var vi framme vid kärnan i den här kokboken, grupphantering. Med grupphantering avses här en centraliserad funktion som ingår som en viktig del i IAM, Identity and Access Management. Det vill säga, grupphanteringen är hjärtat i accesshanteringen som styr användares behörigheter.

Grupphanteringssektionen är uppbyggd i FAQ-form för att på bästa sätt strukturera upp och svara på de frågor som dök upp på den workshop som hölls inför detta projekt. Strukturen är som följer:

4.1 VAD ÄR GRUPPHANTERING?

En grupp är en mängd personer eller saker som vi valt att gruppera av någon anledning. Vi kan gruppera folk som spelar i studentfotbollslaget, de som spelade tvärflöjt när de var små, de som hejar på Arsenal eller alla som heter Julia. Vilka grupper man behöver bestäms dock utifrån sitt sammanhang. Det finns ingen mening med att ha grupper som inte används till något och det var en av de saker Högskolan Väst poängterade att man skulle fundera över innan man designade sin grupphierarki. Det vill säga, lägg tid på och fundera över samt se till att du vet svaret på frågan: Vad ska du använda grupperna till?

En uppenbar nytta i IT-sammanhang är att gruppera människor som skall ha samma access i ett eller helst flera system. Det gäller till exempel studentgrupper i en viss kurs som skall ha en gemensam e-postlista, komma in i samma kursrum i lärplattformen, ha tillträde till samma lokaler, tillåtas logga in i labbdatorer som hör till kursen med mera. Detsamma gäller många andra grupperingar såsom anställda som har samma organisatoriska tillhörighet, projektgrupper och forskargrupper, kårstyrelse, prefekter, medlemmar i studentidrottsföreningen, ledningsgrupper osv…

Det kan verka enkelt men det blir snabbt mer komplicerat när man inser att det inte bara finns rätlinjiga och strikt hierarkiska organisationsstrukturer utan att det även finns många tvärfunktionella grupperingar samt, att alla medlemmar i en grupp inte är jämlika utan kan ha olika roller i gruppen. Somliga i gruppen skall därför kanske ha andra privilegier än övriga. Vi går då från en ursprungligen ganska enkel tvådimensionell matris till tre eller fler dimensioner. Det gäller därför att hitta en strategi som trots komplexiteten gör gruppstrukturen både överblickbart och så renodlad som möjligt.

4.2 VARFÖR SKALL VI INFÖRA GRUPPHANTERING?

Den största vinsten med grupphantering är att använda den för kontroll och överblick av access. Inför man grupphantering som också skall styra accesshantering så tvingas man per automatik att tänka igenom och besluta om en genomtänkt strategi för access management. Det man främst vill adressera med en sådan strategi är:

- Minska kostnad och tid för införande av nya tjänster
- Öka möjligheten till mer finkornig accesskontroll såsom mellan vissa tider på dygnet, ett begränsat antal dagar, beroende på varifrån man loggar in med mera
- Förenkla för användare och de som administrerar deras access samt göra det mer enhetlig genom att använda samma grupp eller samma regel på alla ställen där den är applicerbar.
- Delegera rättigheten att administrera och besluta om access till den som är i bästa position att ta beslut kring det och därigenom ta centrala IT ur loopen kring ett flertal sådana beslut. Det kan till exempel gälla vilka som skall ingå i en forskningsgrupp eller vilka utöver de som är anställda som skall få access till en specifik avdelnings filarea eller annan resurs. Det är beslut som IT ändå inte kan avgöra utan att ringa och fråga eller skicka mailförfrågningar till ansvarig, vilket både orsakar fördröjning av ärendet och onödig administration för IT.
- Delegerad administration ger också möjlighet för institutioner att ha resurser hos centrala IT och få rättighet att administrera access till dessa själva. Det minskar behovet för institutioner att bygga en egen IT-infrastruktur för att kunna ha frihet att administrera vem som skall ha behörighet till deras system.
- Öka säkerheten genom att få en total kontroll och överblick och enkelt kunna presentera rapporter om vem som har rätt att göra vad i olika system och därmed undvika brandkårsutryckningar för att ta reda på det vid behov. Möjlighet att bevaka att SoD-regler inte överträds samt möjliggöra heltäckande robusta processer för on-bording och off-bording vid byte av organisationstillhörighet och funktion.
- Att möjliggöra access för federerade externa användare utan att behöva skapa lokala konton

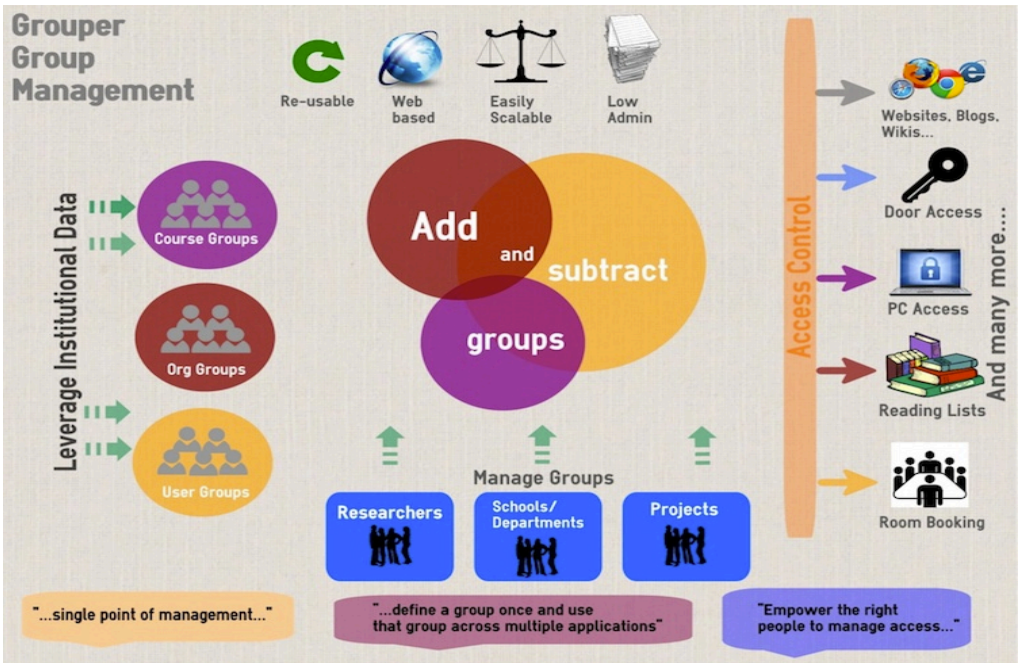
4.3 HUR BÖRJAR MAN?

Det finns två generella återkommande rekommendationer när det gäller planering och införande av grupphantering. De är:

1. Tänk allt
2. Bygg ut stegvis

4.3.1 *Tänk allt*

Med ”tänk allt” avses att du bör tänka att du, när systemet är fullt utbyggt, kommer att ha kopplat all accesshantering via ditt IAM-system och integrerat det mot alla resurser, system och applikationer. Ledorden är alltså skalbart och på sikt integrerat mot ”allt”. Allt innefattar fysisk access till lokaler, nät, lånekort, systemresurser, olika enheter, applikationer, vpn, etc,,,



Figur 15 Övergripande konceptbild från University of Newcastle

Om vi studerar bilden i Figur 15 så ser vi till vänster ”..single point of management”. Målsättningen är att ha ett enda ställe där man skapar och underhåller sina grupper. Ledorden för systemet anges högst upp, dvs man vill att grupperna skall vara återanvändbara, hanteringen webbaserad, det skall vara skalbart och administrationskostnaderna skall vara låga.

Grupperna till vänster, dvs Course Groups, Org Groups och User Groups skapas och underhålls automatiskt utifrån givna filter och kriterier såsom vilken kurs en student skall läsa, vilken organisatorisk tillhörighet man har samt andra användargrupper som kan skapas automatiskt utifrån till exempel definierade roller och attribut.

Nertill finns även “..define a group once and use that group across multiple applications”. En användargrupp återanvänds så mycket som det går. Specifikt så kan den till exempel bli medlem i ett antal accessgrupper och ha sin egen epost-lista. De blåa grupperna är i många fall sådana grupper som skapas via delegerad administration, där administration och underhåll av gruppen är delegerad och centrala IT i de flesta fall inte behöver agera alls. Användare har alltså skapat och underhåller sina grupper själva. Längst ner till höger ser vi ”Empower the right people to manage access…” Man delegerar alltså administration till den som bäst vet vem som har rätt att få access. Den eller dessa personer får rätt att administrera och besluta om det.

I mitten ser vi gruppoperationer som kan göras. Folk som har misskött sig hamnar i en svartlistningsgrupp och subtraheras/excluderas från ett visst system, andra grupper slås ihop för att skapa en ny typ av grupp.

Längst till höger ser vi ett antal system som är integrerade mot grupphanteringsverktyget. Det är framförallt här du skall tänka allt. Ju fler system som är integrerade på så sätt att deras access kontrolleras av systemet, ju större nytta ges av systemet och det ger även bättre överblick över vilka som har access i olika system.

4.3.2 Bygg ut stegvis

Det generella återkommande rådet i sammanhanget är att man börjar i liten skala med att integrera ett system och bygger ut stegvis. Det ger möjlighet till att iterera och utvärdera och eventuellt omvärdera och kanske delvis designa om din gruppstruktur på vägen i takt med nya erfarenheter och att man lär sig vad som fungerar bäst.

Vilket system man vill börja med avgörs kanske av vad man har mest behov av men med tanke på ekonomi och politik i sammanhanget så är en rekommendation att inledningsvis införa grupphantering i något sammanhang där det genererar tydlig affärsnytta och får stor effekt. Ett sätt att kartlägga det är att göra en skattning och presentera resultaten grafiskt. Se Figur 32 Uppskattningsgraf.

4.4 SKALL VI ANVÄNDA ROLLER, ATTRIBUT ELLER AFFILIATIONS?

Vid design av grupper är det idealiskt att använda en kombination av alla dessa och att inte låsa sig vid en specifik metod. Valet borde i varje unikt fall bli den strategi som bäst servar det man vill åstadkomma och som blir enklast att tillämpa praktiskt. Ett grupphanteringsverktyg bör stödja att man använder en kombination av dessa, enskilt eller tillsammans.

I alla sammanhang gäller att det måste råda en samsyn kring policys och datas tillämpning, det vill säga, att det går att lita på att processer och definitioner är klarlagda samt att data är korrekt och hålls uppdaterat.

Exempelvis måste livscykler vara definierade: vem som är student, när man blir student och när upphör man att vara student. Finns det en graceperiod eller några mellanlägen, till exempel när man är barnledig eller är utbytesstudent utomlands ett halvår, vad gäller då? Skall jag tas bort helt, avaktiveras jag eller läggs jag i en excludegrupp under tiden jag har uppehåll eller händer kanske ingenting. Detsamma gäller för anställda med olika ansvarsområden, organisatorisk tillhörighet och olika funktioner. Är flödes- och livscykelprocesserna samt ansvarsområden och roller väldefinierade går det att automatisera mycket av administrationen och då blir vinsten i kronor och ören samt robustheten i systemet ännu större.

4.4.1.1 RBAC

RBAC eller rollbaserad accesskontroll fungerar i gruppsammanhang bra för större grupperingar men mindre bra för unika, specifika roller. Om man går in för en helt och hållet rollbaserad strategi är risken att man får en rollexplosion där det till slut finns fler roller än antal personer. Rekommendationen är därför att främst använda roller för att sortera användare i större och mer generella grupperingar.

4.4.1.2 ABAC

ABAC eller attributbaserad accesskontroll fungerar bättre för mer finkornig behörighetsstyrning. Attributbaserad accesskontroll kan förutom att ta hänsyn till en enskild persons/grupps egenskaper/attribut använda sig av en kombination av attribut där alla måste vara rätt för att access skall tillåtas. Det kan till exempel vara vilken tid på dagen det är, från vilken enhet man loggar in eller om man befinner sig på sitt intranät eller befinner sig på konferens utomlands osv.

Till attribut kan man även koppla villkor som triggar en aktivitet. Om en person till exempel loggar in från ett osäkert ställe eller en okänd enhet så kan man till exempel kräva att personen autentiserar sig på ytterligare ett sätt.

4.4.1.3 Affiliations

Affiliations i LDAP och liknande berättar något om en persons relation med organisationen och dessa är typiskt lämpliga att använda i vissa gruppsammanhang. Student, faculty eller staff är till exempel lämpliga att filtrera på för att automatiskt skapa grupper.

4.5 HUR DESIGNAR VI VÅRA GRUPPER?

En grupp är en mängd personer eller saker som vi valt att gruppera av någon anledning. Vi har valt att kalla dessa användargrupper. Dessa kan vi gruppera utifrån organisationstillhörighet, vilken kurs man ha registrerat sig på eller vilket program man läser, vilken titel eller roll man har, vilket projekt man jobbar i osv…

Vi har även valt att se grupphantering från andra hållet, det vill säga om vi inte utgår från användarna, utan från de system som vi vill kontrollera access till. Sett från det hållet blir det mer renodlat att tänka att för varje typ av behörighet i ett system så skapar vi en så kallad accessgrupp i vårt grupphanteringssystem. Grundregeln är då för att inte få en onödigt komplex bild att **en** accessgrupp mappar mot **en** specifik behörighet i systemet.

En accessgrupp är alltså inte detsamma som en användargrupp. Du återanvänder en accessgrupp genom att alla personer eller grupper som skall ha just den behörigheten i systemet läggs in i just den accessgruppen. Du kan då alltid överblicka vilka som har en viss behörighet i ett visst system. En accessgrupp kan med en sådan strategi i enstaka fall innehålla endast en person, dvs om det bara är en person som skall ha just den behörigheten i systemet, likväl som den kan innehålla alla på lärosätet.

Om en accessgrupp alltid är kopplad mot access i ett system så är inte alltid en användargrupp det. Det kan finnas situationer då du vill skapa användargrupper för andra syften. En användargrupp kan till exempel representera ett urval frivilliga som deltar i ett 10-årigt forskningsprojekt om utvecklingen av Alzheimer, representera de som har anmält sig till lärosätets informationsbrev eller användas för att göra en statistisk undersökning av andelen studenter från Norrland på en viss utbildning.

Rekommendation är därför att skilja på användargrupper och accessgrupper.

1. Användargrupper kan vara
    - Automatiskt genererade
    - Manuellt skapade
2. Accessgrupper är normalt

- Manuellt skapade och har koppling till access i system eller applikationer etc.

Vilka användargrupper vi väljer att skapa beror på vad vi svarat på frågan: Vad ska du använda grupperna till?

4.5.1 Namngivning och struktur

När det gäller namn på grupper så skall namn generellt vara globalt unika för att fungera i alla sammanhang och namnet bör vara läsbart och lämpligen berätta något om i vilket kontext gruppen används. Globalt unika gruppnamn kommer vara nödvändigt i en framtid där vi kanske kommer exportera grupper och det är troligt att de kommer användas i sammanhang där man jobbar med global access.

4.5.1.1 Top down eller bottoms up

När man strukturerar och namnger grupper ställs man inför valet att designa strukturen från topp till botten eller från botten och upp.

4.5.1.1.1 Top Down

När det gäller namngivning så är det naturliga att tänka top down. Top down är också det naturliga om man vill ordna grupperna hierarkiskt i mappar.

4.5.1.1.2 Bottoms up

När det gäller att skapa grupper så blir det istället naturligt att i vissa fall tänka bottoms up. Det gäller speciellt när du använder dig av en strategi med sammansatta grupper.

4.5.1.2 Prefix

Vissa verktyg kan ha stöd för att sätta ett prefix före gruppnamnet vilket gör att man kan minska djupet i grupphierarkin. För svenska universitet blir prefixet typiskt vårt globalt unika domännamn (umu.se, kau.se, uu.se osv). Om verktyget inte stödjer prefix bör man ha gruppnamn eller grupphierarkier som innehåller våra unika domännamn eller själv skapa en lösning som kan lägga till prefixet vid eventuell export eller användande av grupper utanför den lokala domänen.

4.5.2 Användargrupper

Användargrupper används för att sortera och kategorisera användare. Användargrupper kan sorteras utifrån olika data såsom attribut, titlar, roller, affiliations, organisations- eller kurstillhörighet.

4.5.2.1 Automatiskt genererade användargrupper

Huvudsyftet med automatgenererade grupper är att effektivisera genom att reducera behovet av manuell IT-administration. Man genererar automatiskt grupper som man vet kommer att behöva gemensamma rättigheter i system eller gemensamma epostlistor och dessa skall också uppdateras automatiskt, dvs förändringar i källsystem skall synkroniseras med grupphanteringssystemet och få genomslag automatiskt.

Ett viktigt steg i planeringsfasen är därför att besluta vilka typer av grupper som skall genereras per automatik och du bör lägga ner en hel del tid i planeringsfasen på att fundera över vilka grupper som det är önskvärt och möjligt att generera och underhålla automatiskt.

För anställda genererar man med fördel grupper automatiskt utifrån organisationstillhörighet. För studenter utifrån program och/eller kurs, vilket år och vilken läsperiod. Organisationer på våra lärosäten har dock typiskt strukturen av en matris och grupper skapas därför inte enbart utifrån ett

organisationsträd utan kan även skapas av olika korsfunktioner. Du bör därför överväga om det är möjligt och önskvärt att automatgenerera även andra grupper såsom studieadministratörer, ekonomiansvariga, prefekter, etc.

Om det går att automatgenerera beror av information som kan fås från källsystemet eller den identitetsdatabas som man hämtar information till grupphanteringssystemet ifrån. Frågan man måste ha svar på är att man kan lita på att den informationen garanterat är pålitligt korrekt. Med pålitligt korrekt menas i detta sammanhang förutom att all persondata är korrekt att det också råder en samsyn och finns gemensamma policys kring de titlar, roller, attribut folk tilldelas och som man avser använda för automatgenerering av grupper.

Finns ingen sådan uppstyrning och samsyn behöver man överväga att lägga ner tid på att komma fram till en samsyn. Alternativet är att förlora i effektivitet då det inte går att automatgenerera på grund av att det data man vill använda för att automatisera denna process inte är tillräckligt pålitligt.

Av säkerhetsskäl skall automatiskt genererade grupper inte gå att editera manuellt!

Det skall till exempel inte gå att lägga in en person som inte är anställd på lärosätet i gruppen ”staff”. En annan anledning till att man inte skall kunna editera automatgenererade grupper manuellt är att rent praktiskt skall innehållet i dessa grupper alltid vara synkroniserat med källsystemets data. Om vi tar exemplet med staff, när systemen synkroniseras så kommer alla nya som anställs att läggas till och alla användare som slutat (och alltså inte längre finns i källsystemet) att tas bort. Det innebär att om man tillåter manuellt tillagda, som alltså inte finns i källsystemet, så kommer dessa att raderas varje gång systemen synkroniseras vilket blir opraktiskt och ohållbart. Att data synkroniseras på detta sätt är dock förstås helt korrekt.

Lösningen blir istället att om det till exempel finns samarbetspartners som behöver access till samma saker som ”staff” så använder man en egen användargrupp för dessa. Både användargruppen staff och gruppen med externa kan läggas i den/de accessgrupper som är aktuella.

4.5.2.2 Manuellt skapade användargrupper

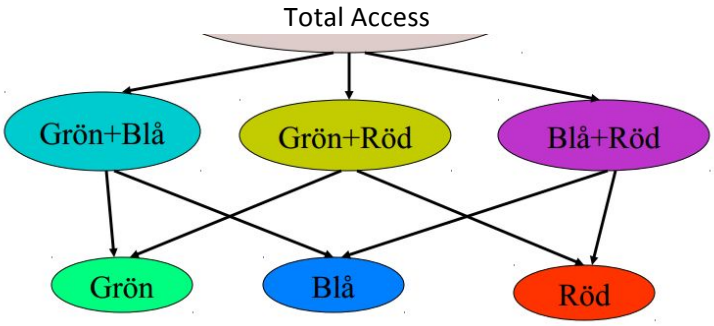
Alla grupper som inte genereras automatiskt skapas manuellt utifrån en i förväg genomtänkt strategi. Arbetet med planera strukturen för och att skapa manuella grupper är störst ”up front” men arbetet med dessa kommer vara mer dynamiskt och ad hoc än de automatgenererade.

När väl själva grupphierarkin och strategin finns på plats kommer en hel del arbete med att skapa och underhålla grupper att kunna delegeras vilket frigör centrala IT-administrationen från mycket administrativt arbete. Underhåll och självadministration av grupper delegeras utifrån behov och typiskt till den som bäst vet vem som skall ingå i olika grupper. Det kan vara institutionerna själva och deras avdelningar, kursansvariga, projektledare, chefer, förvaltningsadministratörer m.fl….

4.5.3 Accessgrupper

Accessgrupper skapas för de olika system man vill kontrollera access till. I sin mest renodlade form så tänker man att en accessgrupp representerar en behörighet i ett visst system. Den eller de användargrupper som skall ha rättighet att göra en viss sak i ett visst system läggs sedan till som medlem i motsvarande accessgrupp.

För accessgrupper är en bottoms up strategi naturlig. Där blir utgångspunkten det system man vill kontrollera behörighet till. En platshållare eller katalog skapas för detta system. Man funderar sedan på vilka olika behörigheter som finns i respektive system eller applikation. Här tänker man alltså behörighetskategorier utifrån målsystemet och skapar en accessgrupp för varje behörighetskategori.



Om vi studerar bilden ovan finns det tre separata behörighetskategorier i systemet, Grön, Blå och Röd. Dessa skapas först. Av dessa har man sedan möjlighet att skapa tre sammanslagna kombinationsgrupper, dvs grupper som har fler än en behörighet. Kombinerar man någon av dessa kombinationsgrupper så får man i detta fall full behörighet, dvs grön+röd+blå. I Vissa fall finns SoD-regler som gör att man inte skall kunna kombinera vissa eller har inget behov av en kategori och då skapas förstås ingen sådan grupp. I en accessgrupp lägger man sen till de användargrupper som skall ha den behörighet som just den accessgruppen ger.

Det kan finnas skäl att skapa fler än en accessgrupp för en behörighet om det till exempel för olika användare med samma behörighet finns knutet olika villkor för att behörigheten skall gälla. Man har då att fundera över vad som blir mest praktiskt, återanvändbart och enkelt att överblicka. Att skapa ytterligare en accessgrupp eller att sätta villkoret direkt på medlemmen (en medlem kan vara både en enskild användare eller en användargrupp).

4.5.3.1 Praktiskt exempel

För användargrupper generellt och automatgenererade grupper specifikt så är en given strategi att följa organisationskartan och välja en top down strategi för namngivning. En kompletterande strategi är tvärfunktionella grupperingar såsom studievägledare och studieadministratörer, webbredaktörer, ekonomiansvariga, prefekter, arbetsmiljörepresentanter, med flera.

4.5.3.1.1 Automatgenererade Personalgrupper

Figur 16 visar organisationskartan för Karlstads universitet som får fungera som exempel i detta fall.

Figur 16 organisation Karlstad universitet

I Figur 16 kan vi utläsa att de har Fakulteten för hälsa, natur- och teknikvetenskap - HNT. Inom HNT finner vi Institutionen för hälsovetenskaper - IHV. Vid IHV finns fem verksamheter, Biomedicinska vetenskaper – BMV, Folkhälsovetenskap – FHV, Idrottsvetenskap – IV, Omvårdnad –OMV, samt Oral hälsa – ORH. Om vi utifrån detta vill åstadkomma är en automatgenererad grupphierarki för Institutionen för hälsovetenskaper skulle det kunna se ut som följer[1]:

KAU:org:staff_all
KAU:org:HNT:HNT-staff_all
KAU:org:HNT:IHV:IHV-staff_all
KAU:org:HNT:IHV:BMV:BMV-staff_all
KAU:org:HNT:IHV:FHV:FHV-staff_all
KAU:org:HNT:IHV:IV:IV-staff_all
KAU:org:HNT:IHV:OMV:OMV-staff_all
KAU:org:HNT:IHV:ORH:ORH-staff_all

Ovanstående exempel visar de staff_all-grupper (grupper med alla anställda) som det blir naturligt att generera automatiskt. Det är förstås upp till varje lärosäte att själv besluta över hur man hierarkiskt ordnar sina grupper och det kommer troligen i många fall att styras av hur man redan har ordnat det hierarkiskt i LDAP eller AD.

När det gäller namngivning så observera att vi skriver ”**HNT-staff_all**” istället för bara ”**staff_all**”. Detta på grund av att när man bara ser gruppnamnet i eventuellt GUI skall veta vilken grupps staff_all man jobbar i och även för att kunna skilja de åt i listor som bara visar gruppnamnet. Om verktyget enbart visar gruppnamnet i GUI:t så bör denna praxis gälla för alla gruppnamn som inte i sig är unika.

[1] Förkortningarna är påhittade så institutioner och avdelningar förkortas kanske på annat sätt på Karlstad universitet.

Det vill säga, använd som regel att gruppnamnet skall ange gruppens kontext om GUI:t inte visar det på något sätt.

Som vi nämnde tidigare så blir en top down strategi mest självklar för att hierarkiskt ordna automatgenererade grupper som följer organisationskartan. Bas-strukturen ges av organisationens struktur eller hur strukturen är logisk ordnad i AD eller liknande.

Förutom ovanstående automatgenererade grupper kan det finnas anledning att även automatiskt generera tvärfunktionella grupper utifrån någon organisationsmatris. Det kan gälla personer med attesteringsrätt, webbadministratörer på internwebben, tvärvetenskapliga forskningscentra osv.

4.5.3.1.2 Studentgrupper

Studentergrupperna är våra mest dynamiska grupper och det finns stora vinster med att generera dessa automatiskt. Här utgår man inte främst från organisationshierarkin utan här är kursgrupper mest intressanta. Man genererar då grupper utifrån när, var och vad man studerar.

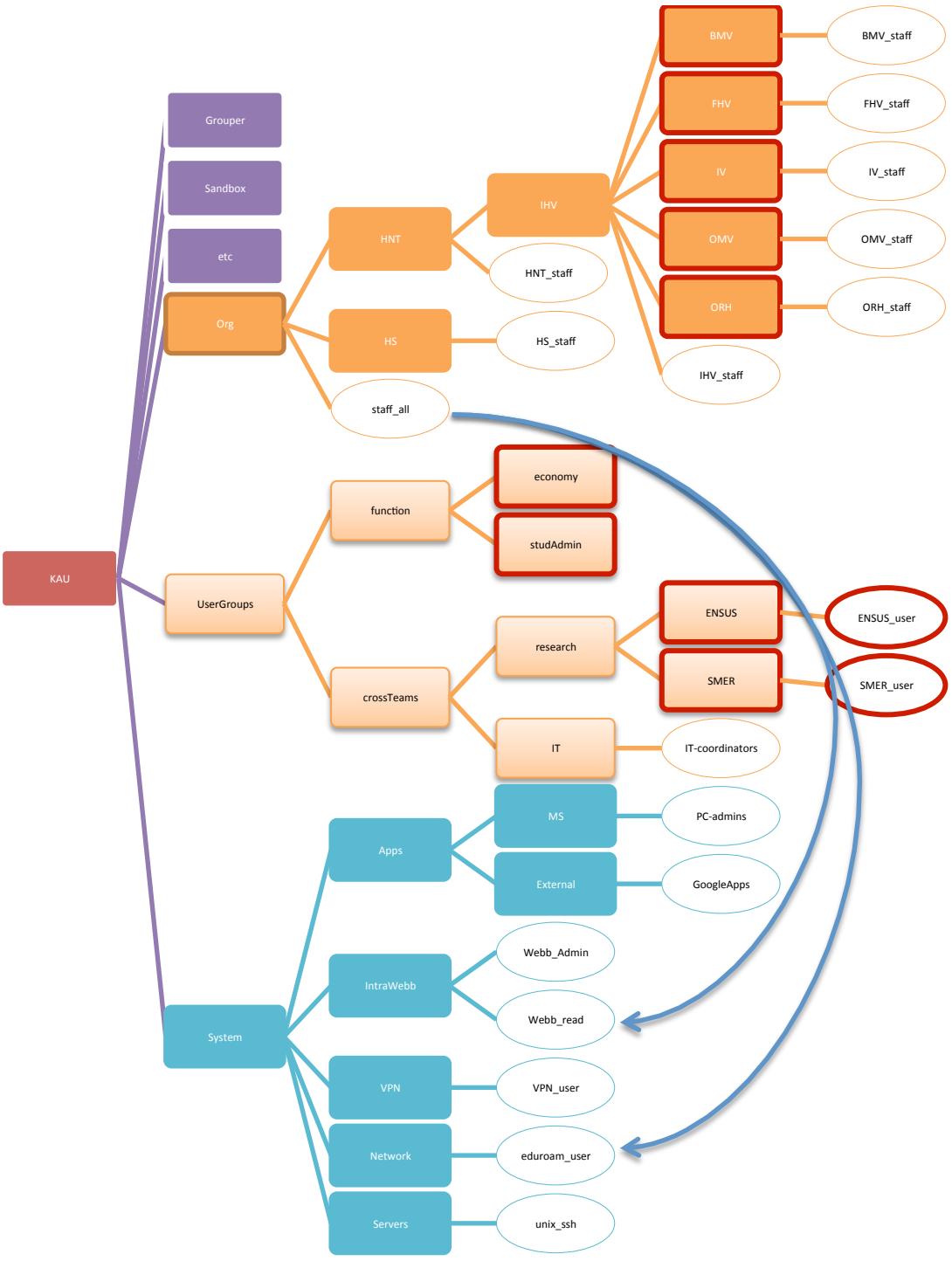
KAU:Students:2014:Q3:**Students_all**
KAU:Students:2014:Q3:IHV:**Students_all**
KAU:Students:2014:Q3:IHV:MedicalSciencesA:**Students_all**
KAU:Students:2014:Q3:IHV:DentistPrgm:**Students_all**
KAU:students:2014:Q3:IHV:DentistPrgm:**Students_excludes**

I ovanstående lista återfinns en grupp som benämns “Student_excludes”. Somliga grupphanterinsverktyg har stöd för att du kan välja att det samtidigt som du skapar en grupp skapas en relaterad includegrupp och en excludegrupp. I excludegruppen kan du lägga till användare som hör till huvudgruppen men av någon anledning inte skall ha access. Det kan till exempel vara sådana som svartlistats pga misskötsel eller har uppehåll för studier utomlands. På motsvarande sätt kan Includegruppen användas för att lägga in användare som skall ha access men normalt inte har det. Ett exempel kan vara en student som under en begränsad period behöver få aktuell kursinformation eftersom de frivilligt valt att läsa om en kurs för att klara en tentamen och därför behöver läggas in i en kurs maillista och ges behörighet till ett kursrum i en lärplattform. Ett annat kan vara några externa som tillfälligt behöver tillträde till en viss projektresurs.

4.5.3.1.3 Manuella personalgrupper

Användargrupper som inte kan skapas och underhållas automatiskt skapas manuellt. Strukturellt får man fundera över om man vill skilja på manuella och automatgenererade grupper. Motiv för det för det kan vara

- du vill kunna delegera administrationen för somliga av de grupper som skall skapas manuellt vilket du gör genom att sätta privilegier för den mapp under vilken en person med delegerad administration själv kan skapa grupper
- för grupphanteringsverktyg som stödjer en hierarkisk struktur med mappar så tänker vi oss för manuellt skapade grupper att barnen i många fall skall ärva föräldramapparnas inställningar och/eller privilegier. Det borde innebära att det blir IT-administrativt effektivare att ha de manuella skilda från de automatiserade eftersom rättigheterna skiljer. De manuellt skapade skall normalt kunna editeras men inte de automatiskt skapade.
- det blir lättare att skilja på vilka som är automatgenererade och vilka som är skapade manuellt samt överblicka vilka automatgenererade grupper som redan finns



Bilden ovan illustrerar en grupphirerarki för KAU där rektanglar representerar mappar och ovaler är grupper. Vi har valt att lägga accessgrupperna i mappen system. Många mappar och grupper under org är automatgenererade. Grupper i UserGroups är främst manuellt skapade. För att ge en grupp access till ett system läggs de in i en accessgrupp så som pilarna visar. Administrationen för mappar och grupper med röd tjock kant är delegerad till andra än centrala IT.

I vårt exempel har vi valt att lägga de manuellt skapade grupperna i en mapp som vi döpt till UserGroups och i den skapa två mappar function och crossTeams. I dessa hittar vi kanske funktionsgrupper av typen:

KAU:UserGroups:function:economy:**economyAdministrators**
KAU:UserGroups:function:studentAdmin:**StudentAdministrators**
KAU:UserGroups:function:headOffice:**HO_management**

Samt korsfunktionella grupper såsom forskningsgrupperingar och andra tvärfunktioner:
KAU:UserGroups:crossTeams:research:**ENSUS**
KAU:UserGroups:crossTeams:research:**SMEER**
KAU:UserGroups:crossTeams:it:**IT-coordinators**
KAU:UserGroups:crossTeams:it:**webb-editors**

Alla staff-grupper är skapade genom en bottoms upp strategi genom sammanslagning av underliggande staffgrupper. Till exempel är IHV_staff bildat av en union av BMV_staff, FHV_staff, IV_staff, OMV_staff och ORH_staff osv. enligt en bottoms up strategi.

Genom att man lägger alla accessgrupper i en egen huvudmapp kallad System så får man alla system och deras behörigheter på ett eget ställe (lite som Program Files i Windows eller /opt i Unix).

Utöver mappar för olika användargrupper samt för accessgrupper kan man för att få en bra struktur och överblickbarhet även överväga att skapa egna huvudmappar eller strukturer till exempel för:

1. Attributdefinitioner och regler (etc)
2. Administrationsbehörigheter för grupphanteringsverktyget (Grouper)
3. Test av nya saker i grupphanteringsverktyget innan man rullar ut i produktion (Sandbox)

För verktyg som inte stöder en hierarkisk uppbyggnad med mappar så kan man inledningsvis planera utifrån denna bild och sen översätta det till den struktur man senare skapar med sina objekt.

4.5.4 Planering av grupper

Ett införande föregås av en planeringsfas där man funderar över vilka automatgenererade grupper och vilka manuella grupper man behöver, samt vad dessa grupper skall ha access till. När man planerar sina grupper så bör man förstås initialt kartlägga och rita upp en överblick vilka grupper som redan finns i olika systemen idag eftersom det visar behovet och användandet i dagsläget.

Nedanstående tabell visar hur en övergripande målplanering skulle kunna se ut. A och M står för automatgenererad eller manuellt skapad. För tabellen gäller att i vänstra fältet återfinns den regel eller det filter som sorterar ut vilka som skall ingå i en automatgenererad grupp. Under kolumnen *Behörigheter administreras av* anges till vem administrationen över den delen av gruppträdet har delegerats. *Mapp* visar exempel på var man hierarkiskt kan placera gruppen. Kolumnen längst till höger exemplifierar vilka accessgrupper just denna användargrupp kan vara kopplad till.

4.5.4.1 Studenter

Filter/Regel:	**A**	**M**	**Behörigheter administreras av:**	**Mapp:**	**Gruppen är kopplad till access till**: (bestäms av mallar som beslutats efter överenskomna policys)
(student) && (Aktiv)			IT Centralt	KAU:student	SSO allmänna lokala applikationer och molntjänster Lärplattformar Eduroam/Wireless Passerkort till allmänna ytor Bibliotekskort E-postlista
(student) && (Aktiv) && (Institution X)			Utsedda administratörer på institution X	KAU:Student:InstitutionX	Labbsalar och institutionsgemensamma lagringsytor E-postlista Åtkomst till institutionens allmänna lokaler
(student) && (Aktiv) && (Institution X) && (Program Y)			Programansvarig på Y-programmet	KAU:student:InstitutionX: ProgramY	Lärplattform E-postlista Åtkomst till programspecifika lokaler
(student) && (Aktiv) && (Institution X) && (Kurs Z)			Kursansvarig på Z-kursen	KAUstudent:InstitutionX:KursZ	Kursrum i lärplattform E-postlista Schema för kursen Åtkomst till kursspecifika lokaler
(student) && (Aktiv) && (Institution X) && (Kurs Z) && (Grupp Q)			Kursansvarig som kan välja att delegera administration av undergrupp till en ansvarig (student eller lärare) per grupp alternativt öppna möjlighet för deltagarna att själva skapa grupper	KAU:student:InstitutionX:KursZ:GroupQ	Projektrum i lärplattform e-postlista Åtkomst till projekt eller labbspecifika lokaler
Fler förstås…					

Tabellen ovan illustrerar exempel för studentgrupper. Nedan illustrerar vi motsvarande exempel för personalgrupper. Tabellerna är inte på något sätt uttömmande eller fullständiga. Tanken är dock att exemplifiera hur man kan resonera.

I vissa fall ingår en användargrupp som är automatgenererad men där det parallellt finns behov av en manuellt skapad grupp med samma access. Det gäller t.ex. för projektgruppen Nyfiken Gul där det även ingår externa parter.

4.5.4.2 Personal

Filter/Regel:	**A**	**M**	**Behörigheter administreras av:**	**Mapp:**	**Gruppen är kopplad till access till**: (bestäms av mallar som beslutats efter överenskomna policys)
(Staff)			Utsedda IT administratörer på centrala IT	KAU:staff	SSO allmänna lokala applikationer och molntjänster Lärplattformar Eduroam/Wireless Passerkort till allmänna ytor Bibliotekskort E-postlista för alla anställda Intranät Internwebb
(Staff) && (Institution X)			Utsedda administratörer på institution X	KAU:staff:Fakulty:FakultyF:Institution X	Labbsalar och institutionsgemensamma lagringsytor E-postlista för institution Åtkomst till institutionens allmänna lokaler
(Staff) && (InstitutionX) && (Grupp: Lärare på Program P)			Programansvarig för P	KAU:staff:Fakulty:FakultyF:Institution X:ProgramP:lärare	Gemensamma ytor i Lärplattform E-postlista för program Åtkomst till programspecifika lokaler Skapa grupper i programfoldern
(Staff) && (InstitutionX) && (Lärare på Program P) && (lärare på kurs K)			Kursansvarig på kurs K	KAU:staff:Fakulty:FakultyF:Institution X:ProgramP:KursK:Lärare	Kursrum i lärplattform E-postlista för kursen Editera schema för kursen Åtkomst till kursspecifika lokaler Skapa grupper i kursfoldern
(Staff) && (Funktion Ledning)			Utsedd administratör	KAU:staff:centralServices:excutiveManagement	Ledningsinfo
(Staff) && (Fakultet F) && (Prefekt)			Utsedd fakultetsadministratör	KAU:staff:FakultyF: Prefekter	Information för prefekter på fakultet F
(Staff) && (Ekonomi-ansvarig)			Utsedd ekonomiadministratör	KAU:staff:centralServices:Economy:EconomyOfficers	Ekonomisystem och ekonomiinformation
(Staff) && (Studieväg-ledare)			Utsedd studievägledaradministratör	KAU:staff:CentralServices: StudentAdministration: studentCounselors	Studievägledningsinformation
(Staff) && (!SoD) && (System X)			IT centralt	KAU:staff:centralServices: ITS:systems:SystemX:Admins	IT-adminrättigheter i System X
((Staff) || (FedereradExtern)) && (Forskningsgrupp Nyfiken Gul)			Utsedd projektadministratör för Nyfiken Gul	KAU:Federated: Cooperations:Research:InstitutionX:DepartmentY: NyfikenGul	Superdatorlabb Hemliga Huset Filyta Nyfiken Gul Wiki Nyfiken Gul Webb Nyfiken Gul
Många fler förstås…….					

4.6 HUR SER EN GRUPPS LIVSCYKEL UT?

En grupp har generellt samma livscykel som en användare. Den skapas, den ändras, byter namn eller flyttas, samt inaktiveras eller tas bort när den slutar fylla ett syfte. Grupper som är tomma eller inte behövs längre skall inaktiveras eller tas bort. Liksom med användare bör man även kunna sätta start- och stoppdatum, kunna inaktivera/aktivera gruppen, bestämma attribut för och kategorisera en grupp samt bestämma villkor och regler som hör ihop med access management.

4.6.1.1 Värt att tänka ett extra varv på:

Ett vanligt problem är att implementera robusta rutiner kring när det är dags att inaktivera eller ta bort en grupp samt återkalla användares rättigheter.

Några tips på hur man attackerar det från de vi intervjuat och det vi läst är:

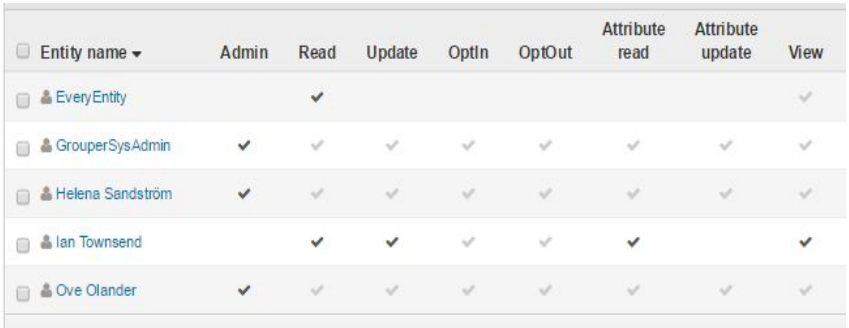
- Att generera varningar när grupper blir tomma eller för grupper där det inte förekommit någon aktivitet det senaste halvåret är några sätt att övervaka och vid behov hantera grupper som inte längre används.
- En grupp skall inte tillåtas sakna ansvarig huvudadministratör eller ägare. Om en person som är ensam ägare eller huvudadministratör av en grupp slutar på lärosätet bör IT automatiskt få en varning och en ny administratör utses.
- Huvudadministratören eller ägaren skall kunna delegera till eller dela administratörsrättigheterna med en annan.

4.7 HUR ÖVERBLICKAR VI GRUPPERS OCH ENSKILDA ANVÄNDARES GRUPPTILLHÖRIGHETER OCH BEHÖRIGHETER?

För att presentera vilka grupper en användare eller grupp är medlem i så duger vanliga listor bra. När det gäller behörigheter så blir det mer komplext och där bör systemet kunna presentera en överblick i någon form av tvådimensionella matriser.

Figur 17 Ett behörighetshanteringssystem bör kunna visa alla privilegier eller behörigheter en person eller grupp har via någon typ av tvådimensionella behörighetsmatriser.

	Data 1	Data 2	Prog. 1	Prog. 2
Alice	RW		E	
Bob	R	RW	RWE	
Carol		R		E
David	RW	R	E	RWE
Eve		R		RE



Det är också praktiskt om det går att via dessa behörighetsmatriser enkelt sätta och ändra behörigheter för en grupp eller en användare. Ändringar skall idealiskt få genomslag eller gå att välja att synkronisera direkt.

4.8 VAD SKALL MAN KUNNA GÖRA MED EN GRUPP?

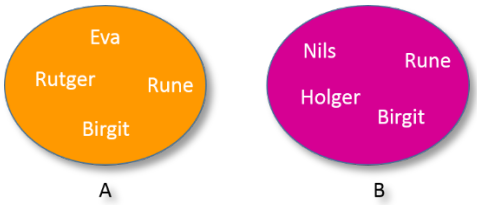
4.8.1.1 Operationer man bör kunna göra på en grupp

Operation:	Beskrivning:
Skapa Grupp	
Ta bort Grupp	
Aktivera/Inaktivera Grupp	Om behov finns att kunna ha inaktiva grupper?
Skapa sammansatt grupp	$A \cup B, A \cap B, A \setminus B$
Ta bort sammansatt grupp	
Lägg till medlemmar i gruppen	Medlemmar kan vara både personer och andra grupper
Ta bort medlemmar ur gruppen	
Byta namn på gruppen	
Flytta gruppen	Flytta gruppen i grupphierarkin
Ändra gruppens privilegier, regler och attribut	I detta ingår många olika funktioner såsom att sätta datum för aktivering/inaktivering av hela gruppen eller enskild medlem i grupp. Regler som triggar olika aktiviteter, vilken access gruppen har till olika system osv….
Sätta gruppadministratör	En gruppadmininstratör kan lägga till och ta bort medlemmar.
Sätta huvudadministratör	Huvudadministratör blir automatiskt den som skapat gruppen men funktionen skall kunna delegeras till annan. En huvudadministratör kan ändra allt och även ta bort gruppen.
Lista direkta medlemmar i gruppen	Lista alla personer och grupper som är medlemmar i gruppen
Lista direkta och indirekta medlemmar	Lista alla personer som finns i huvudgruppen och i alla dess undergrupper
Lista alla grupper som gruppen är medlem i	
Opt in	Personer kan själv välja att bli medlem i gruppen
Opt ut	Medlemmar kan själva välja att gå ur gruppen

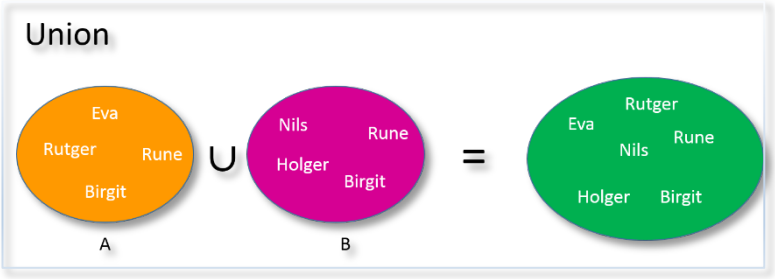
4.8.1.2 Sammansatta grupper

I grupphanteringssammanhang så kan det finnas behov av att exkludera eller inkludera medlemmar i grupper. Ett sätt att göra detta är genom olika gruppoperationer som har sitt ursprung i matematikens mängdlära. Intressanta gruppoperationer är ”union”, ”differens” och ”snitt”. På engelska union, intersection och complement.

Om vi har två grupper, A och B där Rune och Birgit finns i både A och B men övriga i bara en grupp…..

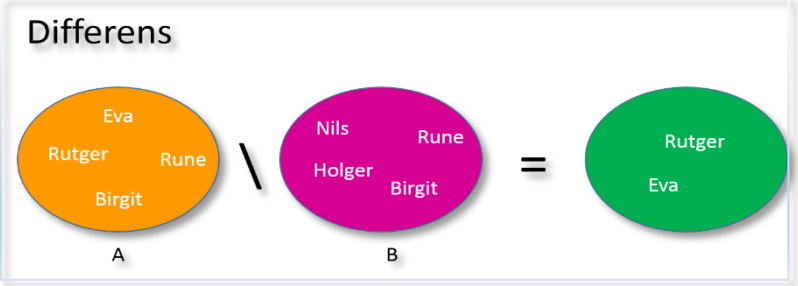


….så blir resultatet följande:

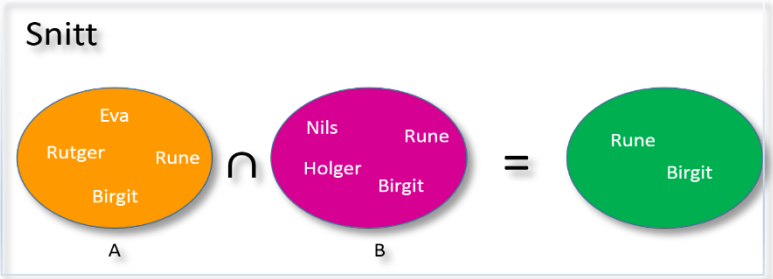


Med union så kan man tänka A + B (A Or B). Man slår ihop grupper. Resultatmängden blir alla som finns i någon av grupperna. Det här är i praktiken samma som när man sätter in flera grupper som medlemmar.

Differens (A AND NOT B) kan man också skriva A - B. Här kommer Rune och Birgit tas bort. Nils och Holger finns inte i grupp A och påverkar inget. Resultatmängden blir Rutger och Eva.



Differens kan exempelvis användas om A innehåller alla studenter och B alla, både studenter och andra, som misskött sig och blivit svartlistade från nätet. Då blir resultatet de studenter som fortfarande har nätaccess.

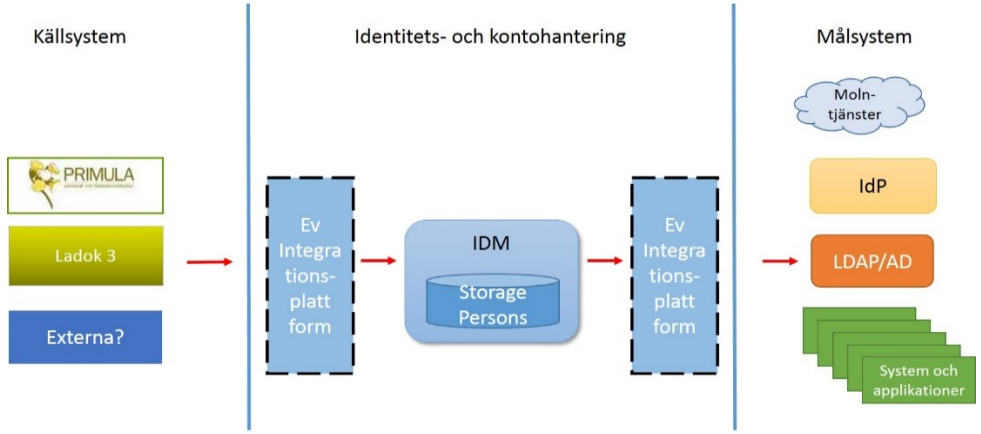


Med snitt (A AND B) plockar man ut de som är medlemmar i båda grupperna. Resultatmängden blir Rune och Birgit.

Ett exempel där du kan använda snitt är om du vill ha en grupp med alla prefekter på en fakultet. Om grupp A är alla på lärosätet med titeln prefekt och grupp B all personal på fakultet X, så ger ett snitt mellan A och B alla prefekter på fakultet X.

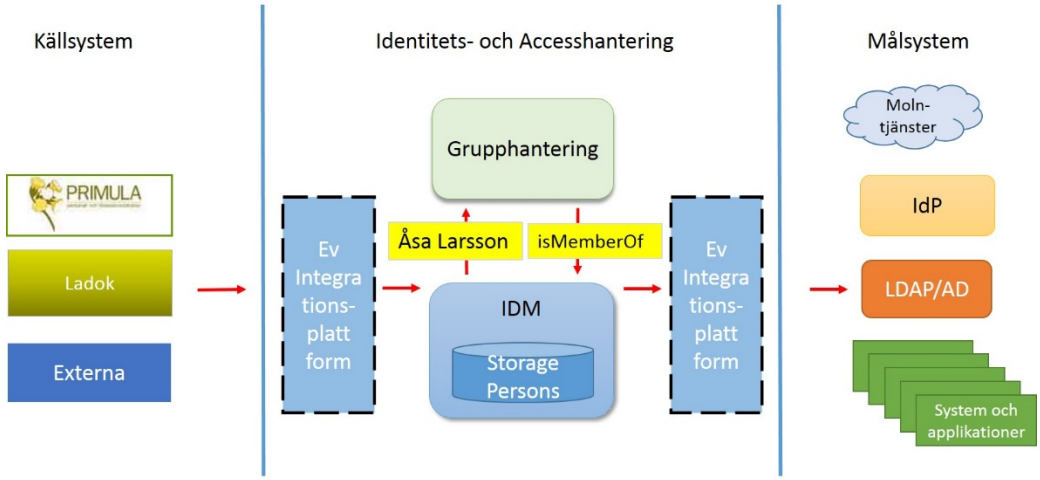
4.9 Hur integrerar vi enklast grupphanteringsverktyget i vår befintliga IT-infrastruktur?

De flesta lärosäten har redan en relativt mogen identitetshantering som är integrerad med många system. Det finns troligen inte två svenska lärosäten med exakt likadan arkitektur men generellt är scenariot att man har Primula och Ladok som källsystem och importerar användare från dessa till en central databas eller ett centralt register. Grupper används till exempel i AD, i ett antal separata system, samt för kursgrupper i lärplattformar. En generell infrastrukturbild för våra lärosäten ser då något förenklad ut såhär:



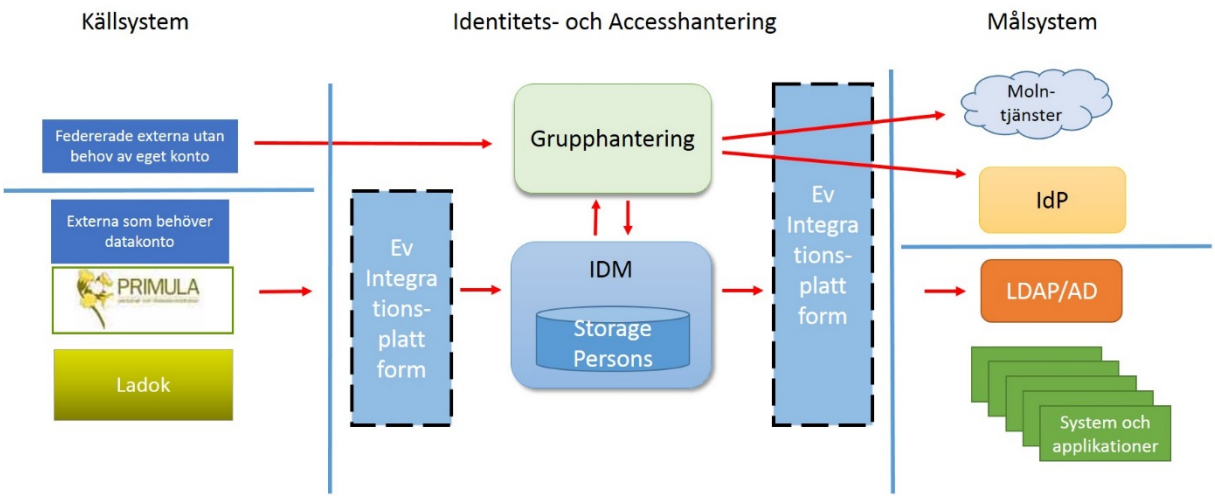
Figur 18 Generell förenklad bild av arkitekturen på våra lärosäten idag

I den centrala databasen finns redan idag normalt ett antal grupper som exporteras ut till olika system. Man har dock oftast inte ett enda system som håller kontroll och överblick över dessa. Ett första steg i integrationen skulle kunna vara att koppla in grupphanteraren mot den centrala databasen/registret för att på det sättet möjliggöra att grupper kan skapas och underhållas och även på ett kontrollerat sätt i viss mån delegeras till icke IT-personal. Övrig integration sker på samma sätt som tidigare, dvs vilka grupper en person är medlem i skrivs tillbaka till den centrala databasen eller registret som synkroniserar grupper med övriga system.



Figur 19 Generell arkitektur med ett grupphanteringsverktyg

Känner man att det blir för stort eller inte tycker sig ha tid eller behov för det just nu kan en annan startstrategi eller en utvidgning vara att låta grupphanteringen hantera externa användare som inte har behov av ett eget datakonto men som idag ofta får det då vi inte kan lösa det på annat sätt. Det är det då också mest praktiskt att låta grupphanteringsverktyget synkronisera ut grupper till IdP:n, eventuellt även till molntjänster? Det skulle då kunna se ut såhär:



Figur 20 Generell arkitekturbild där externa användare importeras direkt till grupphanteringssystemet som synkroniserar ut grupper till system för federerad access och molntjänster.

Hur och vad man väljer att börja med beror förstås både på hur arkitekturen ser ut, vilket behov som är mest intressant, hur mycket resurser man har för att arbeta med det samt vad man vill åstadkomma.

Om man vill uppnå maximal nytta bör ett av huvudmålen med ett införande på sikt vara att ta kontroll över alla användares säkerhetsprivilegier i samtliga system och samtidigt skapa robusta rutiner och en effektiv administration.

4.10 Hur ser vi till att grupphanteringsverktyget inte blir en single point of failure?

Kopplar vi in grupphanteringsverktyget enligt Figur 19 är vi i praktiken inte beroende av att det alltid svarar, dvs vi har inte äventyrat säkerheten. Information som ligger i grupphanteringsverktyget finns även på andra ställen. Grupphanteringsverktyget har bara fått uppgiften att vara den punkt i systemet som skapar och underhåller grupperna. Tittar vi på arkitekturen i Figur 20 kommer enbart möjligheten till filimport av nya externa användare samt möjligheten att skapa nya grupper att påverkas under eventuell nertid. De grupper som redan är synkroniserade ut till sina målsystem ligger kvar och inga förändringar sker med dem.

Utökar man beroendet av grupphanteringsverktyget gäller samma tankar om säkerhet och robusthet som runt IDM-systemet. Det finns dessutom alltid möjlighet att addera en extra grupphanteringsinstans som är read only dit allt data speglas. Att spegla över data till en readonlyinstans kan även vara intressant av prestandaskäl.

4.11 Vilka verktyg finns det och vilka krav bör man ställa?

Det finns ett stort antal företag som erbjuder IAM-lösningar. Vi har inte gjort en inventering av vilka som finns utan hänvisar i det fallet till rapporten från det projekt som föregick detta där man kom fram till att FIM och Grouper var de mest intressanta som verktyg i grupphanteringssammanhang för svenska lärosäten. Det finns företag som erbjuder helhetslösningar antingen med egna produkter såsom Oracle och IBM och andra som bygger ett IAM-system genom ett hopplock av produkter. IAM

erbjuds även as a Service av ett antal företag. Enligt Gartners Magic Quadrant är de ledande företagen inom det området Okta, Ping Identity och Covisint. Onelogin, Centrify, CA Technologies och Lighthouse Security Group ligger också bra till.

För den som är intresserad av utvecklingen på IAM-området rekommenderas att titta på Gartners Identity & Access Management Summit, 2-4 December 2014, och de olika spår man tog upp där [18]. En av huvudsponsorerna av årets upplaga är norska Forgerock som erbjuder en open identity stack och propagerar för IRM. Forgerocks affärsmodell är dock att man skall få sälja utbildning och support så helt open source och gratis är det förstås inte. Att de nämns här beror på att vi bedömde att de har en intressant lösning och infallsvinkel.

Generellt bör du ställa krav på att ett grupphanteringsverktyg stödjer att:

- Sköta all grupphantering från ett ställe
- Skapa ad hoc grupper
- Skapa subgrupper
- Skapa sammansatta grupper
- Distribuera kontroll av grupper
- Delegera administration
- Definiera egna typer av grupper och attribut
- Lista alla direkta och indirekta medlemmar i en grupp
- Enkelt överblicka individuella privilegier inom en grupp
- Vara användarvänligt för normal grupphantering som delegerats till ”vanliga” användare
- Lista alla grupper en användare är medlem i

Fundera även över om systemet stödjer och vilka behov du har av tvåvägsintegration med de målsystem du avser att integrera med.

4.12 Vilka högskolor i Sverige och världen använder FIM och Grouper för grupphantering?

4.12.1 Vilka använder Grouper?

I Sverige är det såvitt vi känner till Uppsala universitet som använder Grouper, om än i begränsad omfattning. Om vi tittar globalt sett så har vi utgått från Groupers wiki där alla användare av Grouper rekommenderas lägga upp information om hur de valt att göra, hur de använder Grouper, till vad och hur de valt att göra sin gruppdesign med mera. Det finns ganska mycket information att tillgå där för den som vill hitta exempel på hur andra gjort. Det som kan vara svårt är att sålla och välja ut det som ger värdefull information.

University of Chicago är nog en av de som använt Grouper längst. De använder Grouper för att administrera access till runt 100 tjänster inklusive trådlösa nätet, LMS, Box.com, Google Apps, 2-faktor autentisering, fildelning, webbaserad fil storage, VPN, LDAP, Shibboleth, SVN, Confluence, VOIP-tjänster, administration av klasser, e-post, routing och studieadministrativa system.

Följande lärosäten finns representerade på Groupers communitysida som användare av Grouper:

Universitet i USA och Canada:

Brown University - Using Grouper with a broad array of applications.
California Polytechnic State University, San Luis Obispo - Browse Cal Poly's Grouper implementation.
Campus Crusade for Christ International - Includes info on the provisioning consumer and on deploying Grouper to multiple environments.
Carnegie Mellon University - Integrating Grouper with Google Apps and more.
Duke University - Read up on Duke's Grouper deployment, including delegated access control in Active Directory..
Lafayette College - Pilot Deployment with VPN use case.
New York University - Grouper deployment at NYU
University of Wisconsin - Madison - Grouper is a component of the Manifest application enabling people to protect apps using a group as well as request campus services for their group.
Northern Arizona University - See how Northern Arizona University integrated Grouper and uPortal
Oregon State University Grouper Pilot, including Grouper with Canvas
Penn State University - Using Grouper with the Central Person Registry.
UCLA - Overview of Grouper use cases and deployment at UCLA
University of Arizona Grouper Pages - a self-service utility allows FERPA-trained faculty and staff members to manage ad-hoc groups
University of California, Berkeley -- Grouper in production with CalMessages email broadcast
University of Chicago - Learn about U. Chicago Grouper, including access management features and VPN delegation.
University of Memphis - Running Grouper API in production
University of Minnesota - Using Grouper to manage access to BPEL workflows, VPN groups and more.
University of Pennsylvania -- Read about Penn's advanced Grouper usage, including handling external users and addressing other permissions use cases.
University of Tulsa - Using Grouper with Shibboleth and Box.com.
University of Utah - A proof-of-concept project within the University of Utah IT department.
University of Washington -- Read about the U-Washington approach to Groups and provisioning
University of Hawaii - See how Grouper is used to augment ListServes and enhance daily termination reports.
Simon Fraser University - Using the Grouper Loader, the Changelog and an ESB connector
University of Montreal - Using Grouper for automatic and delegated group and membership management

Universitet i Europa:

UK:
Newcastle University - A video on how groups are structured, information on access control groups using Talend, managing room booking, wireless access and more.
Cardiff University - Grouper deployment at Cardiff University includes an ESB Interface. (note: last updated in 2011)

Tjeckien:
University of West Bohemia - Look here for several useful items. (note: last update 2009)

Sverige:
Uppsala University in Sweden - View UI screens for adding groups and members.

Frankrike:
Université de Lille1 - Adapting and Frenchify LiteUI / Adaptation et Françisation de LiteUI
GIP RECIA - A public interest group in France uses Grouper with uPortal.

Holland:
SURFnet OpenConext - See how Grouper is used within the OpenConext collaboration platform

Italien:
Consortium GARR - Grouper for a centralize authorization system for multiple virtual organizations.

Tyskland:
Freie Universität Berlin - Unix group management extension to Grouper

4.12.1.1 Interfedererat pilotproject:

LIGO - using Grouper to support multiple authorization scenarios for the an international virtual organization

Läs mer här: https://spaces.internet2.edu/display/Grouper/Community+Contributions

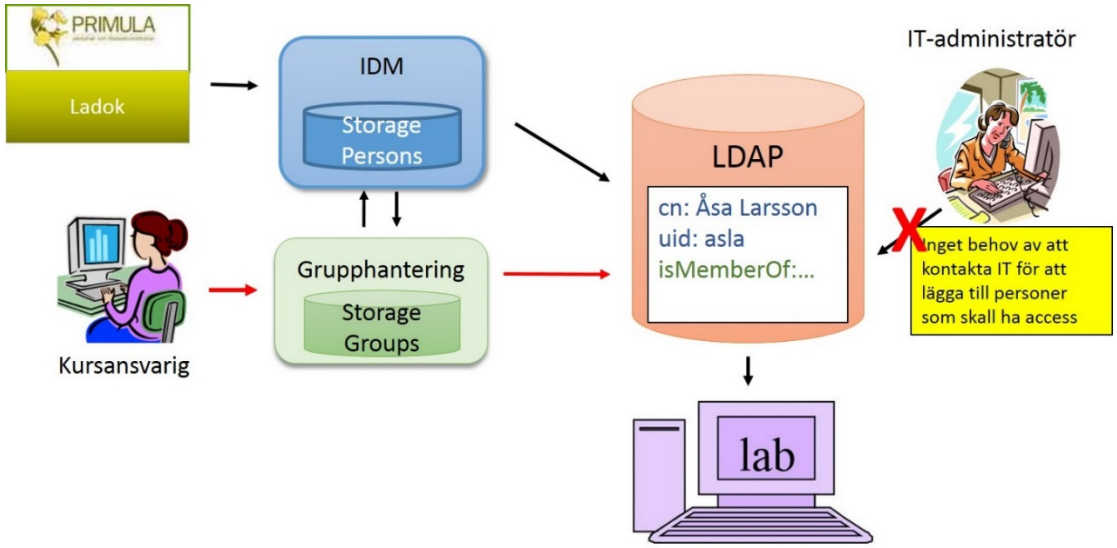
4.12.2 Vilka använder FIM?

Eftersom FIM är en Microsoftprodukt så är det svårare att hitta information om vilka som använder FIM globalt sett. I ett papper om Identity and Access Management for education från Oxford computer Group, en nära samarbetspartner till Microsoft, går att utläsa att Kings College och University West är deras kunder. Det framgår dock inte om de använder FIM och om det är enbart för identitetshantering eller även för grupphantering.

Det finns några svenska lärosäten som använder FIM för identitetshantering. Först ut var SLU. Lund och Malmö har infört FIM relativt nyligen. Högskolan i Väst använder FIM men ej för identitetshantering utan enbart för synkronisering. Ingen använder såvitt vi vet FIM för grupphantering. Linköping och även Umeå har haft funderingar på att införa FIM som grupphanteringsverktyg. Umeå har tills vidare lagt dessa planer på is. Linköping har hunnit planera ganska lång men hade vid vårt senaste samtal inte tagit beslutet att införa det ännu.

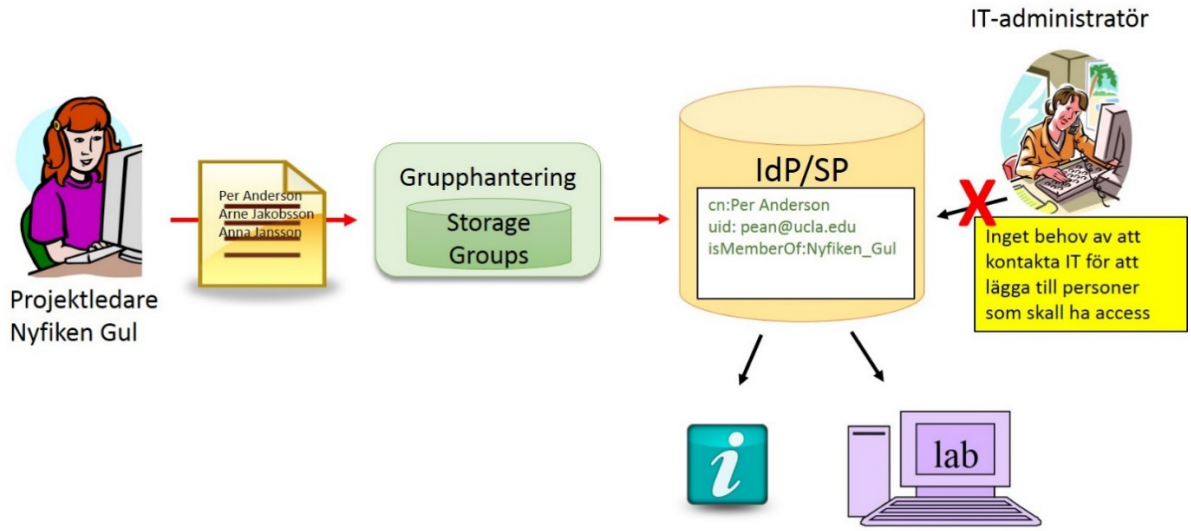
4.13 KAN NI BESKRIVA NÅGRA USE CASE OCH EXEMPEL?

4.13.1 Förenklad och mer effektiv administration genom delegering



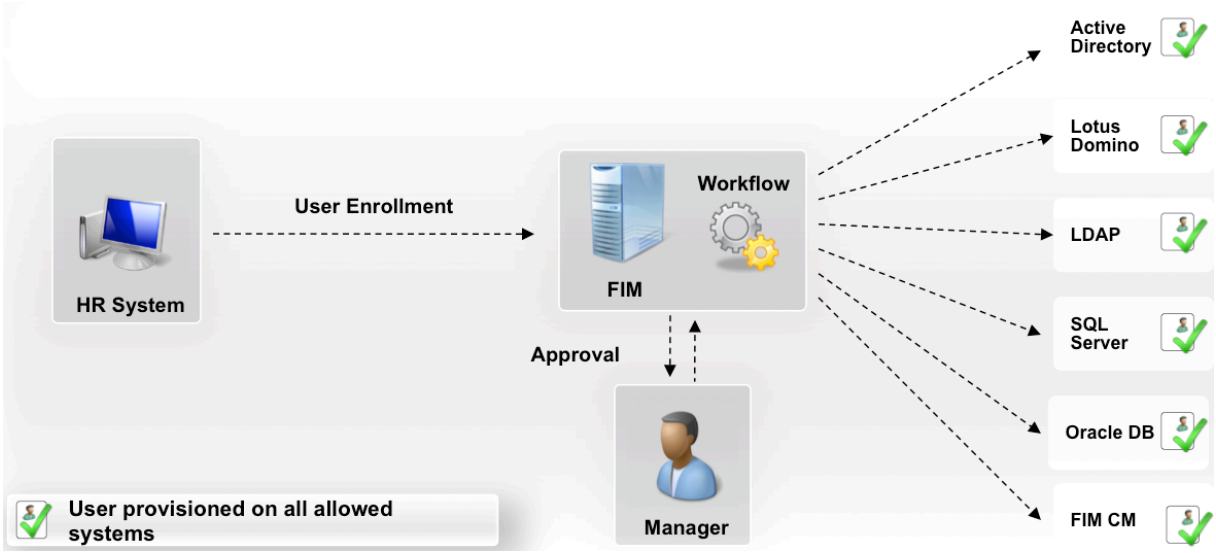
Figur 21 Ge rätten att kontrollera access till den som bäst vet vem som skall ha access

En uppenbar fördel med ett grupphanteringsverktyg är att du kan delegera rätten att besluta vem som skall ha access till en viss resurs till den som bäst vet vem som skall ha access. Det kan gälla för alla möjliga system såsom studentlabb, administration av intrawebben, studieadministrativa system, forskningsresurser, vem som får skicka infobrev etc…

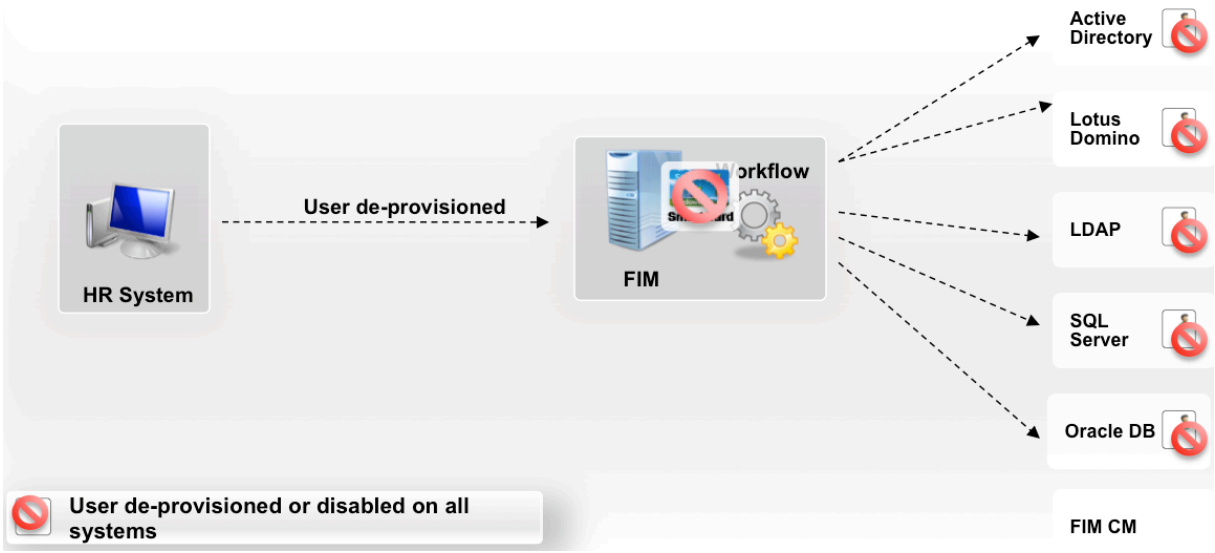


Figur 22 Projektledare kan lägga in federerade användare och ge de access till projektresurser

4.13.2 Ökad säkerhet, överblickbarhet och robusthet kring livscykelprocesser



Figur 23 Automatisk tilldelning av behörigheter för nyanställda, personer som byter organisationstillhörighet och nya studenter



Figur 24 Automatisk återkallning av behörigheter när anställning upphör, en student tar examen eller en externt anslutens tidsbegränsade anknytning till universitetet löper ut.

5 HANDS ON - ERFARENHETER

I inledningen av arbetet med kokboken intervjuades ett antal högskolor och lärosäten i syfte främst att inhämta kunskaper och lärdomar om FIM och Grouper samt hitta bra exempel på egenutvecklad grupphantering. Intressanta att intervjua var främst de som använde FIM eller Grouper samt de som redan hade en egen fungerande lösning för grupphantering. Av de intervjuade har Högskolan i Väst och Luleå Tekniska Universitet implementerat en egen lösning för grupphantering, Uppsala använder Grouper för grupphantering, Malmö och Linköping använder FIM för identitetshantering. Vi pratade även med Mittuniversitetet eftersom de stod i startgroparna för att införa Grouper för att hantera sina federerade användare och hade hunnit fundera lite kring hur de skulle lösa det.

I det här avsnittet presenteras hur de lärosäten vi intervjuade har löst det här med grupphantering samt vilka lärdomar och erfarenheter de har och vill dela med sig av. Vi tittar även på hur FIM och Grouper skulle kunna integreras och användas för grupphantering.

5.1 EGENUTVECKLAD GRUPPHANTERING

5.1.1 Högskolan Väst

Den mest heltäckande egenutvecklade lösningen vi stötte på var hos Högskolan Väst och de använder grupphantering i stor omfattning redan idag. Högskolan Väst har under många år arbetat för att bygga upp en genomtänkt strategi för användares livscykelhantering och en helhetslösning med automatisk synkronisering och integration mot de flesta av sina system. Av runt 53 system synkroniserar man idag mot cirka 40. De påbörjade arbetet med att bygga sitt system för relativt många år sedan och har sedan dess även migrerat det från en annan plattform dock med bibehållet GUI.

Resultatet är ett användbart GUI där användare loggar in i ”Mitt konto”. Användarbehörigheter styr vilka uppgifter användare kan ändra, vilka flikar och vilken information de kan se. En student har ett par flikar medan en IT-administratör har många fler och det är möjligt för alla användare att via GUI:t utföra viss självadministration.

HV har i sitt system definierat ca 250 roller och skapat nio defaultmallar som används för att automatiskt ge olika typer av användare en basbehörighet i olika system när nya konton skapas. De nio mallarna gäller för följande användarkategorier:

1. Anställd
2. Student
3. Gästföreläsare
4. Samarbetspartner
5. Industridoktorand
6. Drivhuset
7. Inhyrd personal
8. Uppdragsutbildning
9. Wifi

Som IT-administratör kan du via GUI:t enkelt överblicka det mesta. Utsökning av en person eller en maskin ger total överblick. Du ser vad en användare har för behörigheter i olika system, vilka datorer

och annan utrustning de har samt vilka grupper de är medlemmar i. Det går även snabbt att ändra en användares behörighet genom att kryssa i en checkbox i en lista för att addera motsvarande behörighet. För att ta bort en behörighet kryssar du ur motsvarande checkbox. För omedelbar synkronisering ut till olika målsystem efter en genomförd ändring finns klickbara knappar i GUI:t.

HV använder som sagt inte något grupphanteringsverktyg utan har en MySQL databas i botten som alltså även håller reda på grupperna. De använder dock FIM, men enbart för att synkronisera ut de grupper som skall ut till AD. För detta ändamål har de hittat en egen lösning som innebär att de skriver direkt till synkroniseringstabellen och därmed inte behöver lagra data i FIM.

Systemet har väldefinierade processer och en genomtänkt livscykelhantering för alla definierade användartyper samt robusta rutiner för on-boarding och off-boarding där användare som slutar automatiskt inaktiveras eller tas bort i alla grupper där de förekommer.

Det är uppenbart att de är nöjda med sitt system och det ser väldigt överskådligt, lättbegripligt och genomtänkt ut. När de får frågan om det är något de skulle vilja förbättra säger de lite skämtsamt att det hade varit ännu bättre om det också hade funnits en enda knapp för att synkronisera till alla system på en gång istället för att trycka på sex eller sju om man omedelbart vill synkronisera ändringar till alla system.

5.1.1.1 Råd och erfarenheter

Deras råd i sammanhanget är att när man börjar planera skall tänka allt, dvs alla system som man kan och bör synkronisera med och även de som man inte tror att man skall kunna synkronisera. Man bör även göra en karta på alla system och synkflöden och tänk igenom alla steg på vägen. Man bör också räkna med att det tar mycket tid med trial and error för att få till bra synkflöden där det bland annat gäller att hitta svar på hur ofta man behöver synkronisera. De har också haft en tät kommunikation och bra dialog med övrig personal på universitetet för att säkerställa att de är medvetna om, att det för att allt skall fungera är viktigt att de matar in bra rådata i systemet.

Sammantaget är enligt HV de frågor man behöver fundera över:

1. Vad ska vi använda grupperna till?
2. Hur bra är rådatan?
3. Tänk allt, även sådant som du inte tror att du skall kunna synkronisera
4. Rita en karta över alla synkflöden och system och gå igenom alla steg
5. Hitta hur fort och ofta ni behöver synka (räkna med mycket trial and error)
6. Larm vid synkfel
7. Skalbarhet?

5.1.2 LTU

Luleå tekniska universitet använder också grupphantering med ett egenutvecklat GUI. Hjärtat i deras system är LDAP. Deras system har inte hunnit nå samma mognadsnivå som Högskolan Väst men är ändå intressant att titta på eftersom det är integrerat med ett stort antal målsystem. De har också två typer av grupper enligt modellen användargrupper och accessgrupper såsom beskrivs i rapporten. Deras benämning är funktionella grupper och accessgrupper. Funktionella grupper delas upp i manuella och automatiskt genererade. En automatiskt genererad grupp kan inte ändras och om man vill se på en sådan grupp kommer en informationstext upp som säger att den inte går att förändra manuellt men man kan förstås lista gruppens medlemmar. Alla accessgrupper har

tilläggsändelsen –a för att markera att det är en accessgrupp. Accessgrupper används för olika behörighetsnivåer i olika system och kan innehålla flera olika funktionsgrupper samt enskilda användare.

Man har valt en modell där samma accessgrupp kan sätta behörighet i flera olika system. De har en relativt utbyggd synkronisering mot många system där behörighetshantering till de flesta webbapplikationer, portaler och CMS styrs via den centrala grupphanteringen.

De har ett snyggt och lättarbetat GUI och i huvudsak är man nöjd med sitt GUI och de saker man byggt hittills. Förbättringar rör främst policys kring livcykelhantering och löpande administration. Frågeställningar som inte riktigt är besvarade men som man skulle vilja ha tydligare regler och effektivare hantering kring är:

- Vem skall ingå i en grupp och vem har mandat att bestämma det?
- Vem skall förvalta gruppen och hur ser man till att alla grupper alltid har en förvaltare?
- Vilka grupper finns och används de fortfarande?
- Hur kan man enkelt överblicka vilka grupper som har access till vad?
- När kan vi ta bort en grupp?
- Hur sker borttagning av användare som ej längre är anställd eller student?
- Hur får vi garanterat bra beskrivningar av vad gruppen används till?
- Kan vi definiera fler roller som kan ge automatisk tilldelning av behörigheter?
- Hur skall vi hantera externa användare?
- Vi behöver utbilda anställda på LTU, hur ska det ske?

Konsekvensen av att hanteringen av vissa saker inte definierats är bland annat att antalet grupper ständigt växer då grupper på grund av bristande dokumentation sällan återanvänds. Samtidigt behöver man fastställa mer robusta rutiner för bortstädning av grupper som inte används och för att ta bort användare som inte längre är aktiva vid universitetet ur grupper.

LTU:s exempel visar på hur viktigt det är att gå igenom och definiera policys kring en grupps hela livscykelhantering och eventuella strategier och strukturer innan man implementerar grupphantering i stor skala.

5.2 GRUPPHANTERING MED GROUPER OCH FIM

5.2.1 Grupphantering med Grouper

5.2.1.1 Uppsala universitet

Såvitt vi är bekanta med så är Uppsala är det enda lärosäte i Sverige som använder Grouper. Grouper kopplas i deras fall mot medarbetarportalen och visionen var att det skall finnas en plats på universitetet där man skapar, underhåller och avvecklar grupper. Deras erfarenhet av Grouper var att Groupers GUI var lite för dåligt för att kunna användas av gemene man så de har byggt en egen applikation som pratar med Grouper via Groupers API. Vidare hade man önskemål om att automatiskt synkronisera mot LDAP direkt från Grouper men det har man än så länge en annan lösning för.

Uppsala ansåg att startsträckan var rätt lång med Grouper och är därför inte säkra på om de skall bygga ut sin grupphantering med Grouper. Värt att nämna är att de parallellt har en egen modell av grupphantering via tupler av GMAI-objekt som de är nöjda med.

De poängterade dock att från och med version 2 har Grouper ett nytt GUI som är betydligt mer användarvänligt samt att produkten mognat och fått en del adderad funktionalitet.

5.2.1.2 Beskrivning av Grouper

Grouper är ett av de projekt som leds av the Middleware Architecture Committee for Education (MACE). MACE består av en grupp av internationella IT-arkitekter för högre utbildningar. Internet2:s middleware initiativ består av ett antal projekt som adresserar utmaningar inom middleware, bland annat IAM. Internet2 är en sammanslutning av mer än 250 lärosäten i USA, samt lika många forsknings- och industripartners i USA och internationellt. Grouperprojektet föddes ur MACE eftersom man ansåg att det behövdes ett mer flexibelt sätt att hantera grupper än vad funktionerna i LDAP kan erbjuda.

Grouper är open source och första releasen släpptes i december 2004. Utvecklingen av Grouper är finansierad av University of Chicago och University of Bristol med stöd av Internet2 genom NSF Middleware initiativ och the Joint Information Systems Committee (JISC). Eftersom Grouper är utvecklad av och för människor inom universitet och högskolevärlden påstås det vara designat att möta just våra specifika behov.

Grouper är ett system där man kan skapa och hantera grupper i ett centralt repository. Grupperna kan användas för olika syften, till exempel för maillistor eller vem som har tillåtelse att få tillgång till en viss webbapplikation eller delade resurser. Målet är att skapa en grupp en gång men återanvända den i alla de situationer där den har praktisk nytta.

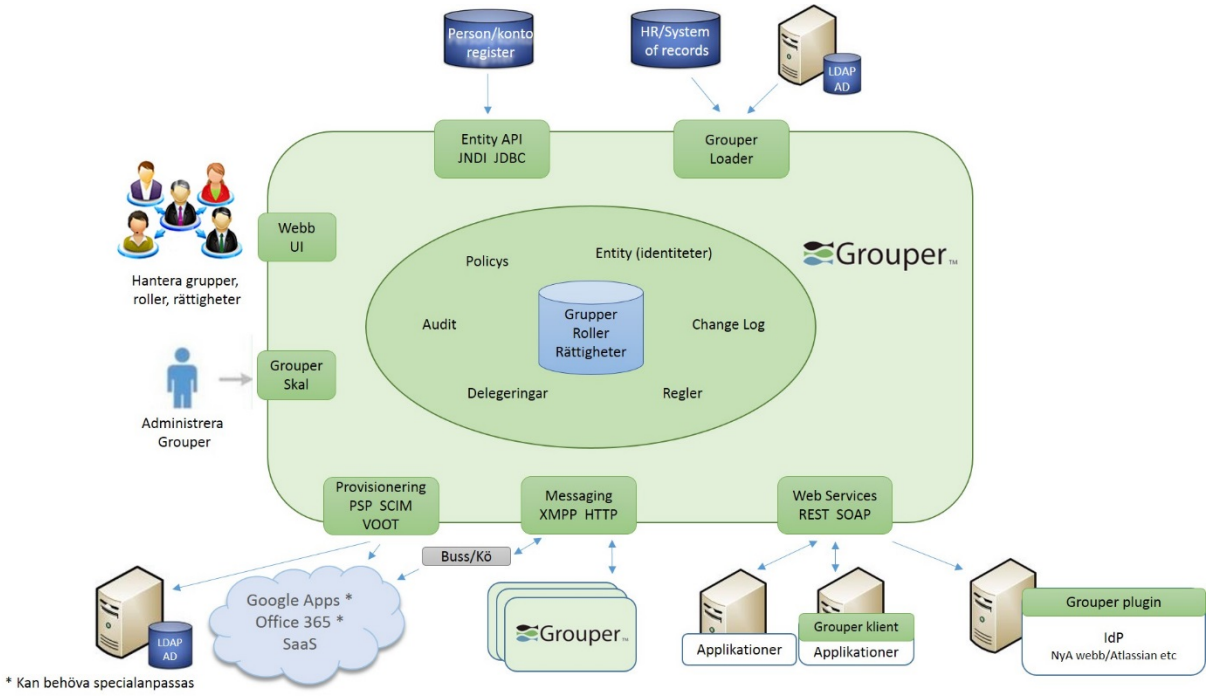
5.2.1.2.1 Information och Demo

Eftersom Grouper är open source finns det väldigt mycket dokumentation i Groupers wiki [19] och även instruktionsvideos kring Grouper för både chefer, arkitekter, utvecklare och administratörer. Det finns även två maillinglistor där man kan posta frågor. Svar kommer relativt fort. Det går även enkelt att ladda ner Grouper Installer v2.2 till sin egen dator och snabbt få en fungerande demo som innehåller Grouper API, UI, WS, loader (daemons), en demodatabas, tomcat och ant. Allt du behöver är en Java 6+ JDK.

För den som är nyfiken på Grouper och vill experimentera lite med det för att lära sig rekommenderar jag att man laddar ner Grouper på sin dator. Det går fort att installera och följer man instruktionsvideon kan man inte misslyckas. Vill man inte det kan man prova Groupers online demo.

Länk till var du kan ladda ner Grouper:
https://spaces.internet2.edu/display/Grouper/Grouper+Downloads
Länk till installationsvideo: http://www.youtube.com/watch?v=XT2deVm3rYc
Länk till Grouper Demo: https://grouperdemo.internet2.edu/

5.2.1.3 Ingående komponenter och arkitektur



Figur 25 Groupers arkitektur

Det finns flera möjligheter att integrera mot Grouper. För import av data så används Grouper loader företrädesvis för att hämta data från SQL, LDAP och AD. För importer som inte kan hanteras av Grouper Loader kan man integrera via Groupers API. För exporter och synkronisering ut till AD, LDAP och Shibboleth används företrädesvis Groupers PSP. För integration mot en ESB används Groupers ESB-connector. För mer detaljer, se Appendix B - Integrationsmöjligheter med Grouper inklusive hänvisningar.

5.2.1.3.1 Användargränssnitt

5.2.1.3.1.1 Admin UI

Groupers ursprunglinga UI är Admin UI. Det exponerar mycket av API:et. Det fungerade bra för administratörer med bra kunskaper om Groupers underliggande koncept men var inte optimalt för andra slutanvändare som enbart skall administrera ett fåtal grupper.

5.2.1.3.1.2 New UI

Med Grouper 2.2 har man byggt ett nytt UI. Det är betydligt mer användarvänligt. Här kommer en användare in och ser på förstasidan tre fält som visar användarens favoriter, de grupper samt de Servicar som den är medlem i eller administrerar. För att skapa grupper och lägga till användare finns tydliga knappar. Se bilder här: https://spaces.internet2.edu/display/Grouper/Grouper+new+UI+v2.2

5.2.1.3.1.3 LITE UI

Från version 1.5 uppdaterades Groupers UI med LITE UI baserat på Ajax. LITE UI var/är en uppsättning sidor för administration av Grouper. Många av funktionerna i LITE UI finns nu i det nya

Grouper UI:t. Det som fortfarande administreras via LITE UI är bland annat attribut, skapa och hantera lokala entiteter (personer eller funktionsidentiteter), externa subjekt.

5.2.1.3.1.4 Groupers skal – GSH

Groupers skal, GSH, är ett kommandoradsbaserat skal som är en del av Grouper API:et. Genom gsh interagerar man alltså med Groupers API. GSH är byggt på Java BeanShell vilket bland annat innebär att man kan skriva in javakod i det. Det finns även ett antal inbyggda kommandon.

Nedanstående gsh-exempel plockar ut alla grupper som en entitet (person) är medlem i.

```
gsh 0% GrouperSession.startRootSession();
gsh 0% subj = findSubject("SD00125")
subject: id='SD00125' type='person' source='kitn-person' name='Barton, Tom'
gsh 1% sess = GrouperSession.start(subj)
edu.internet2.middleware.grouper.GrouperSession: 29c40f97-9fb0-4e45-88bc-a14877a6c9b5,'SD00125','person'
gsh 2% member = MemberFinder.findBySubject(sess, subj)
member: id='SD00125' type='person' source='kitn-person' uuid='d0fa765e-1439-4701-89b1-9b08b4ce9daa'
gsh 3% member.getGroups()
group: name='etc:sysadmingroup' displayName='Grouper Administration:SysAdmin Group' uuid='6f77fb36-b466-481a-84a7-7af609f1ad09'
```

För mer info läs: https://spaces.internet2.edu/display/Grouper/GrouperShell+%28gsh%29

5.2.1.4 Feature Walkthrough

5.2.1.4.1 Groupers nyckelkoncept

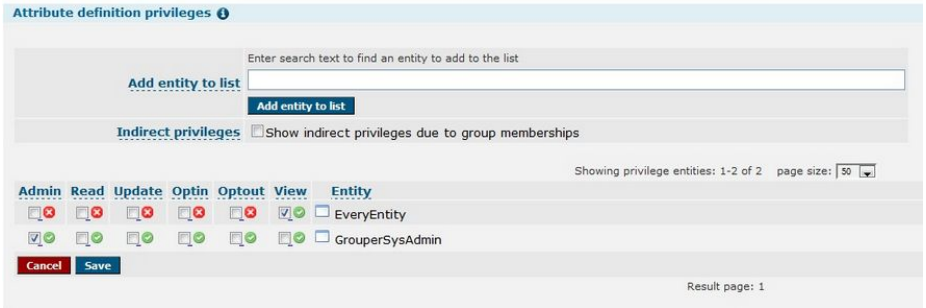
Några termer har ändrats under tiden Grouper har utvecklats. Det kan vara lite förvirrande när du läser i dokumentationen. Du hittar en lista över de termer som har använts tidigare och de som numera används i Grouper här: https://spaces.internet2.edu/display/Grouper/UI+Terminology

5.2.1.4.1.1 Entity

En entity är en abstrahering av de som kan vara medlemmar i en grupp. En entitet kan i dagsläget vara en person eller en grupp. I framtida versioner kan en entitet kanske även vara datorer eller applikationer. Entity hette tidigare Subject och båda benämningarna förekommer i instruktionsvideos och i dokumentationen. Det finns två speciella och förutbestämda lokala entiteter, funktioner eller specialanvändare i Grouper, det är:

- EveryEntity = privilegier som ges denna ärvs/tilldelas alla i en grupp
- GrouperSysAdmin = högsta nivån av administratör i Grouper

Så som privilegierna är satta nedan kommer alltså alla att få se att attributdefinitionen finns (view) men enbart de som är GrouperSysAdmins kommer att kunna administrera.



5.2.1.4.1.2 Group

En grupp representerar en samling entities. Entiteterna är medlemmar i gruppen. Om du anger att grupp B skall vara en medlem av grupp A innebär det således att alla medlemmar i grupp B också är medlemmar av grupp A.

5.2.1.4.1.2.1 Roles

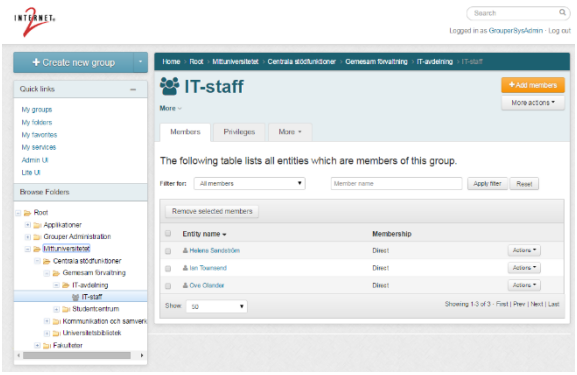
Roller i Grouper är RBAC-objekt vilket egentligen är en speciell typ av grupp. Du behöver använda en roll närhelst du tilldelar gruppen behörighet att accessa något. Du kan tilldela en roll (alltså en grupp av typen roll) rättigheter vilket i praktiken betyder att den rollen (gruppen) kommer att ha dessa rättigheter. Rollens medlemmar kan vara både enskilda personer och andra grupper.

Enklast är kanske att tänka på roller som bryggan mellan användare och rättigheter i system. Så som vi har tänkt design av grupper i den här rapporten kommer förmodligen samtliga accessgrupper att vara grupper av typen roll i Grouper [20].

Figur 26 välja typ på en grupp i Grouper

5.2.1.4.1.3 Folder

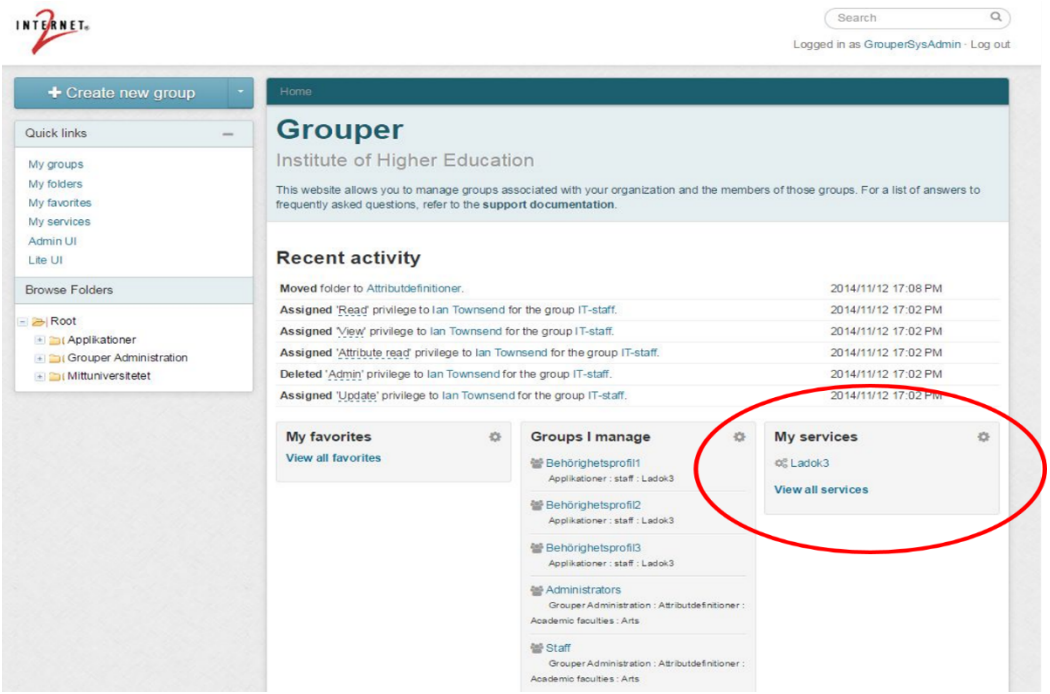
En folder är en mapp och mappar kan ordnas hierarkiskt. I en mapp kan man skapa nya mappar, grupper och undergrupper. Mappar används för att ordna relaterade grupper. Gruppnamn bör vara globalt unika och folderstrukturen bör förutom att logiskt ordna grupperna ha funktionen av att skapa ett globalt unikt namespace som motsvaras av sökvägen till en viss grupp.



Folder hette tidigare Stem och benämns så ibland i instruktionsvideos och dokumentation. Man kan välja att inte visa den folder (stem) som är rot i folderstrukturen i GUI:t. Man kan även välja att lägga till ett prefix före alla gruppnamn för att kunna minska djupet i hierarkin. Vidare kan undermappar ärva egenskaper från sina föräldrar.

5.2.1.4.1.3.1 Services

Grouper har som tidigare nämnts en hierarkisk struktur i vilken man kan organisera Groups, Roles, and Permissions. Från och med version 2.2 så finns även möjlighet att tagga huvudfoldern till en applikation som en service. Det blir då lättare att hitta servicen i Grouper registret samt att administratörer av den servicen får upp den under My Services på sin sida. Se nedan.



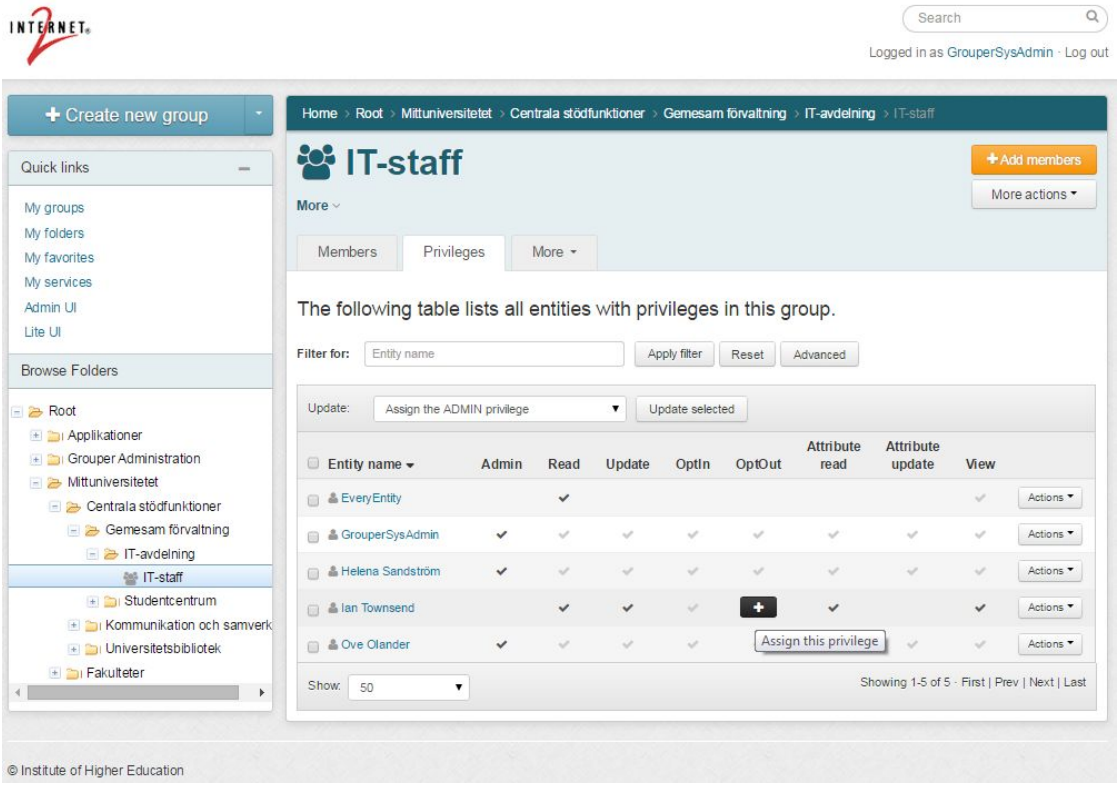
Strukturellt så borde varje applikation eller system som man vill styra behörighet till representeras av en mapp som taggats med typen Service. I en Service definieras sen ett antal grupper av typen roll, en roll för varje behörighetstyp. I var och en av dessa rollgrupper lägger man in de användargrupper som skall ha den behörighet som specificeras av just den rollgruppen [21].

5.2.1.4.1.4 Privileges

Grouper tillhandahåller kontroll över vem som kan skapa mappar och grupper, vem som kan ändra medlemmar i gruppen, samt vem som kan dela ut privilegier för specifika mappar och grupper till andra. Om du ger privilegier till en entitet som är en grupp så ger du dessa privilegier till alla medlemmar i gruppen. Ger du privilegier till en entitet som är en person så får just den personen dessa privilegier.

Privilegier för en mapp:

Create Group	Entitet kan skapa grupper i denna mapp
Create Folder	Entitet kan skapa undermappar i denna mapp



Figur 27 Lista över privilegier för gruppen IT-staff

Privilegier för en grupp:

Admin	Entitet kan lägga till och ta bort medlemmar, ta bort gruppen och ändra privilegier för gruppen
Update	Entitet kan lägga till och ta bort medlemmar i gruppen
Optin	Entitet kan välja att gå med i gruppen
Optout	Entitet kan välja att gå ur gruppen
View	Entitet kan se att gruppen existerar
Read	Entitet kan se vilka som är medlemmar i gruppen
Attribute read	Entitet kan se gruppens attribut
Attribute update	Entitet kan uppdatera gruppens attribut

I Figur 27 ser vi att specialanvändarna/funktionerna EveryEntity och GrouperSysAdmin finns med i listan. EveryEntity = alla medlemmar i den här gruppen får alltså Read-rättigheter, dvs de kan se vilka som är medlemmar i gruppen. GrouperSysAdmin får administrera trots att den specialanvändaren inte själv är medlem i gruppen. Privilegier ändras lätt genom att man klickar i listan vilken rättighet som skall läggas till (svarta plusset i bilden) respektive tas bort (syns inte i bild men visas med ett kryss).

5.2.1.5 Access Management

Grouper har ett antal olika sätt att hantera access till interna/externa resurser och tjänster.

5.2.1.5.1 Groupers Attribut

Groupers attribute framework används för att attacha metadata till olika objekt. Du kan skapa egna attribut och tilldela dessa till grupper, medlemskap, medlemmar, mappar, andra attribut och attribute assignments (en nivå ner). Attribut hanteras fortfarande via Gropuers Lite UI [22].

Grouper har också inbyggt sex attribut (strängar) som används för globalt id, namngivning och sökning.

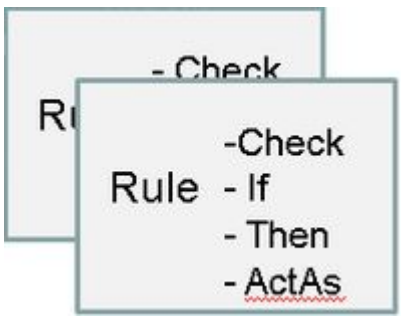
- id = global unik identifierare
- extension = relativt namn på gruppen eller foldern
- name = används för att söka grupp på namn och innehåller <förälder> <extension>
- displayExtension = Namn på gruppen
- displayName =<Förälderns displayname><displayExtension>
- description = en beskrivning av gruppen

En grupp i Grouper har oftast ett namn som är läsbart och förståeligt och ett annat som kan vara uppbyggt av bara förkortningar.

5.2.1.5.1.1 Privileges

Privilegierna är kopplade till vad en användare får göra med en mapp eller en grupp i Grouper. Privilegierna bestäms när du skapar en ny mapp, en ny grupp eller lägger till medlemmar i gruppen. Som tidigare nämnts går det att bestämma vem som får administrera, uppdatera (lägga till och ta bort medlemmar), läsa, se, själv begära in och utträde i gruppen samt se eller uppdatera gruppens attribut.

5.2.1.5.1.2 Rules



Regler triggas när en viss händelse inträffar i Grouper. Du kan till exempel använda en regel om du vill att en student skall få ett slutdatum på medlemskap i gruppen som har access till kursens wiki när studenten tagits bort från den grupp som motsvarar kursens klasslista. Grouper har drygt ett 20-tal regler som följer med version 2.0. Bland annat att du kan få en notifiering via email när du närmar dig det slutdatum som är satt är satt för medlemskap i en grupp. Regler är konfigurerbara deklarativa script. Funktionen påminner om JBoss drools och kräver ingen ändring av en konfigfil för att aktiveras. Regler konfigurerars via Groupers Attribute Framework.

5.2.1.5.1.3 Permission Limit

Permission Limit är en runtime-begränsning på permissions. Dessa kan inte ärvas och kan bara sättas direkt på en roll (dvs grupp av typen roll) eller på en entitet/medlem som finns i en roll. Begränsningen kan vara att användare i en viss roll bara kan logga in i ett system under kontorstid eller att en enskild användare bara får godkänna betalningar på maximalt ett visst belopp i systemet.

5.2.1.5.1.4 Allow/disallow

Allow och disallow kan till exempel användas när permissions för en grupp ärvs av en förälder och man behöver förändra detta för en av grupperna eller för någon medlem i en grupp. Allow för att utöka rättigheter och disallow för att smalna av ytterligare. Det kan till exempel gälla om man inte vill att en användare som jobbar med löneutbetalningar skall ha rätt att se sina närmaste medarbetares löneuppgifter.

5.2.1.5.1.5 Enabled/disabled dates

Enabled och disabled används för att aktivera respektive inaktivera medlemskap i en grupp vid en fastställd tidpunkt i framtiden.

5.2.1.5.2 Notifieringar

Grouper kan integrera med eller provisionera data till externa system i realtid när förändringar sker. Det görs via notifieringar baserade på Groupers change Log och kan ske via:

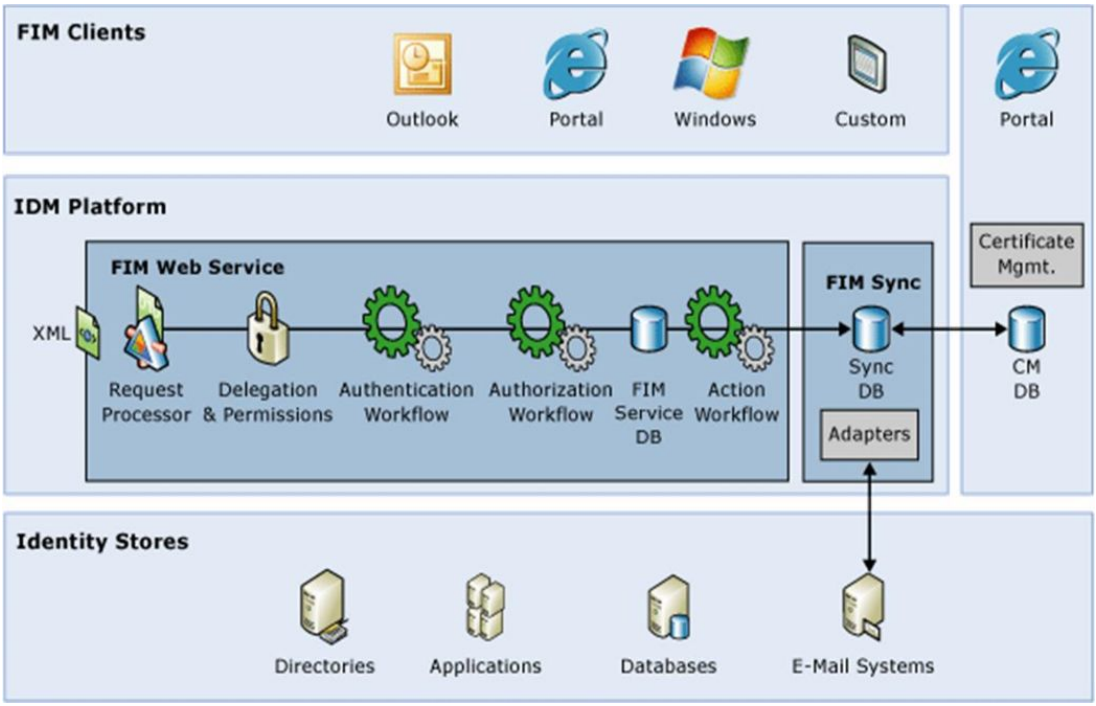
- PSP till LDAP, AD eller via SPML
- Grouper ESB connector eller XMPP
- Genom att implementera sin egen change log consumer i Java

5.2.2 Grupphantering med FIM

FIM är en state-baserad IDM produkt designad att hantera användares identiteter, deras personliga attribut samt grupper. FIM integrerar bland annat med AD för identitetssynkronisering. FIM är inte open source så tillgången på information är inte lika omfattande och vi har heller ingen som använder grupphantering med FIM i Sverige. De som kommit längst i planeringen av att använda FIM för grupphantering är Linköping. Vi har även intervjuat Malmö och pratat lite med Lund som idag använder FIM för sin identitetshantering. När det gäller FIM har det varit lite svårare att tränga in i detaljerna eftersom vi inte har haft någon programvara att testa på så det här avsnittet kommer inte bli lika uttömmande som i Groupers fall.

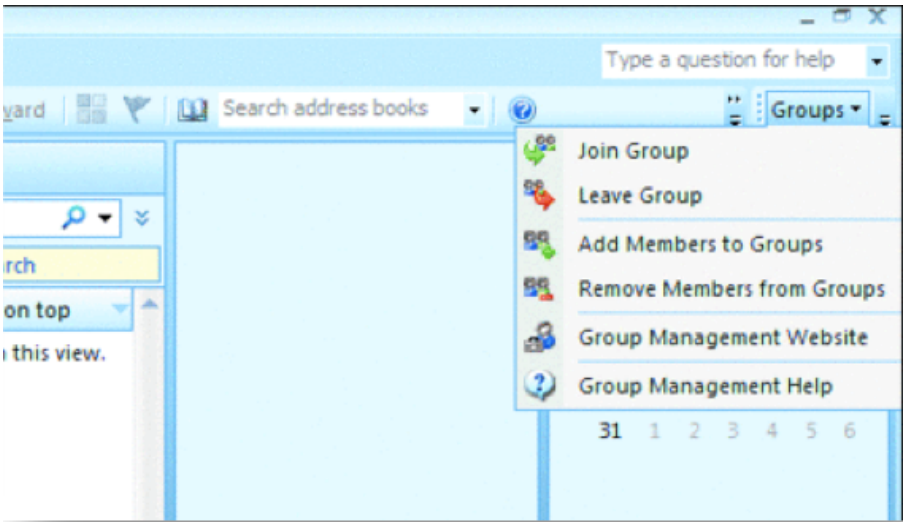
Från genomförda intervjuer så är den sammantagna bilden att FIM fungerar för identitetshantering. Den är dock väldigt noga om att få in rätt data och man behöver hantera scenariot som uppstår om FIM inte får svar från källsystemet så att den inte raderar alla användare och all information på grund av att den tror att källsystemet är tomt. Malmö hade inte hittat en bra lösning för att hantera sina externa användare i FIM då den hade svårigheter att hantera flera containers i AD på ett bra sätt. För Malmö har det också krånglat en del innan man hittade en lösning eftersom FIM hade en strikt prioritetsordning i hur den plockar in data från källsystem. Lösningen blev att man adderade data inkrementellt från olika system för att få in allt data på ett korrekt sätt i FIM. Både Lund och Malmö har varit beroende av konsulthjälp. De har haft kontakt med Kent Nordström från Konab konsult AB. FIM har fått kritik för sin hantering av priviligierade konton. FIM kommer under 2015 ersättas av Microsoft Identity Manager där man bland annat förbättrat den hanteringen så det torde vara den produkten man skall titta på om man är nyfiken på FIM [28].

5.2.2.1 Ingående komponenter och arkitektur



Figur 28 FIMs arkitektur

Bland FIM:s klienter hittar vi en add-in till Outlook som gör att användare kan begära inträde och utträde ur grupper via Outlook och att personer som äger grupper lika enkelt kan bekräfta eller avböja en begäran via Outlook. Det går även koppla in Exchange 2007 eller 2010 som klient. FIM:s portal går via SharePoint. När det gäller egenutvecklad integration med FIM så måste alla kodade anpassingar ske via Visual Studio 2008 och man kodar i .NET. Det finns även möjlighet att använda Microsoft PowerShell, till exempel för att exportera policy Rules eller andra objekttyper från FIM Service databas.



Figur 29 FIM Add-in för Outlook

FIM:s IDM-plattform utgöras av FIM Service och FIM Synchronization Service. FIM Service har ansvar för att hantera WS requests och evaluera dessa samt att hålla reda på alla workflows. Det finns tre typer av workflows: autentisering, auktorisation samt action. FIM Synchronization Service är den centrala komponenten som synkroniserar data mellan multipla datakällor. Synchronization servicen aggregerar information om identiteter in till metaversen och tillhandahåller en agentlös metod för att kommunicera med varje datakälla och sköter provisionering. Båda FIM servicarna använder Microsoft SQL Server som databas.

Kommunikation hanteras i FIM av Management Agents. Extensible Management Agents kan byggas i .Net. Via Web Services kan man utöka FIM vilket gör att det är möjligt att koppla ihop den med Sharepoint. Rapporter kan fås via WMI-anrop eller via tredjepartslösningar.

Figur 30 Sharepoint-baserad Mangement Console

5.2.2.2 Feature Walkthrough

Det som främst verkar skilja FIM mot Grouper är att FIM inte stödjer en hierarkisk struktur med kataloger eller grupper i grupper. En grupp är i FIM ett objekt och du kan själv planera ”up front” hur olika gruppobjekt skall designas. Allt i FIM är representerat som objekt. De primära objekttyper som skeppas med FIM är requests, groups, users, sets, management policy rules, workflow processes, workflow activities, syncronization rules, functions, och search scopes.

5.2.2.2.1 Set och Management Policy Rules

FIM har något som de kallar för set. Medlemmar i ett set kan läggas till för hand eller läggas till automatiskt utifrån en given regel. På ett set kan du koppla två olika typer av management policy rules.

5.2.2.2.2 Management Policy Rules

Det finns två typer av Managment policy rules, Requester Management Policy Rule, RMPR, samt Transition-base Management Policy Rule. TMPR. En RMPR kan användas för att utvärdera om en request skall godkännas eller inte samt i nästa steg, om requesten blir godkänd och ett state ändras så träder TMPR in och bestämmer vilken operation som följer av att ett state har ändrats. Till exempel kan man i första steget begära att lägga till någon som just har blivit anställd och om det blir godkänt enligt den första policyregeln så har ett state ändrats. Då träder nästa policyregel in vilket till exempel triggar operationen att ge personen access till intranätet.

5.2.2.2.3 Gruppadministration

Grupper skapas/administreras i FIM på ett av tre sätt:

- Manuellt
- Administreras av gruppägaren/gruppägarna
- Automatiskt utifrån kriterier

Det är endast för manuellt administrerade grupper som en person själv kan begära inträde. För övriga två kommer begäran om inträde i en grupp att avböjas automatiskt. Automatiska grupper kan skapas utifrån i förväg bestämda kriterier. När det gäller begäran om inträde går det att bestämma om det krävs godkännande från mer än en gruppägare för att en begäran om inträde i en grupp skall bekräftas. Det går även att sätta slutdatum på grupper.

Det finns även stöd i GUI:t för självadministration, såsom att sätta om lösenord och uppdatera din användarprofil. Det är dock delar som hör till identitetshantering och skall inte blandas ihop med grupphanteringsfunktioner.

5.2.2.2.4 Metaverse och MA:s

Hjärtat av FIM är en metaverse som är omringad av MA:s, dvs management agents som hanterar all import och export till metaversen. Objekt som är lagrade i metaversen kan inte editeras direkt utan ändras via flöden. Allt i FIM är representerat som objekt.

5.2.2.2.5 Filter attribute

För filtrering används XPath och filterattributet finns på flera av de primära objekttyperna. Specifikt bör nämnas groups, sets, och search scopes.

5.2.2.2.6 Requests

Varje requestobjekt har tre komponenter: requestor, operation och Target. Target anger vilken resurs man begär, operation vad man vill göra i resursen och requestor är förstås vem som ställer frågan, vem som begär nämnda resurs.

Nedan visas Linköpings planerade design av ett kursgruppsobjekt. Då det saknas ett naturligt sätt att göra grupper av grupper i FIM så kan ni notera att man har ett attribut som heter SystemContext där man kan ange om detta är en labbgrupp i en kurs eller om det är ”main”-gruppen. Det blir lite som att göra en egen dubbellänkad lista.

5.2.2.2.7 Exempel på planerat kursobjekt från Linköping

Attribute	**Value**
Id	*A unique id for the group (LIU:Student: institution:Program:year:Kurs:Q3:Labbgrupp1)*
Name	*The official name of the group (Kurs:Labbgrupp 1)*
Description	*A textual description of the group*
Mall	*Gruppens context:* • University • Institution • Department • Program • Course • SubGroup
Creator/System	*The id of the creator of the (manual) group*
Members	*A list of users/groups that are members of the group*
Filter/Scope	*One or more groups/attributes that are limiting the search for members in the group. If a member falls out of scope of the filter, the member should be removed.*
MinSize	*Minimum number of (manual) members of the group. Used to validate that the group´s purpose is fulfilled. Only valid for manual GM groups. The group will be disabled (Enabled = false) until MinSize is reached.*
MaxSize	*Maximum number of (manual) members of the group. Only valid for manual GM groups.*
StartDate	*The date when the group starts to apply. The group will be disabled (Enabled = false) until the Start Date occurs.*
EndDate	*The date when the group ends to apply. The group will be disabled (Enabled = false) after the End Date occurs.*
Source	*The source system that are responsible for the members. It is only the source system that can change the population of the group.*
System	*The system that created the group. Can be used to group/filter group objects.*
SystemContext	*One or more attributes describing the context of the group in scope for the system, ex:* • *CourseCode* • *Main (if several systemScopes are used this could point out the main group of them)* • *Students* • *Labgroup X* • *Labgroup Y*
Target systems	*Systems that subscribes to the group. Some features are close connected to target systems and if they are enabled the target system will automatically end up here. Ex:* • *Ad.liu.se* • *Sesam*

Group Managers	*A list of persons/group(s) that are allowed to make changes to the group (Description/Filter/Size/Etc) Ex: TDDB28-Teachers*
Group Member Managers	*A lits of persons/group(s) that only are allowed to make changes to the membership*
Membership Approval	*Determines who can join/leave the group.* • *Open (anyone can join/leave)* • *Closed (Only Group Member Managers can add/remove members)* • *Aproval (Group Member Managers will ge an approval mail where they can Accept/Reject the join* • *Auto (Use Scope as a filter)*
Enabled features	*A feature could be* • *E-mail enabled* • *Connected to SharePoint Room* • *Connected to Integra Zone*
Enabled	*The status of the group. Values true/false. If the value I false the group´s members won´t replicate outside GM and if the API is used to query for membership the API will return error or false*

5.3 GRUPPHANTERING OCH LADOK 3

En tillämpning på grupphanteringen som redan idag är vanligt förekommande på Sveriges lärosäten är hantering av kursgrupper där information om kursgrupperna erhålls utifrån kursregistreringarna i Ladok och dessa kursgrupper används sedan till bland annat e-postlistor och behörigheter i lärplattformar. När övergången från Ladok till Ladok 3 sker kommer det att krävas anpassningar av den befintliga gruppprovisioneringen, där grupperna idag provisioneras utifrån integration via ODBC-koppling mot Ladokdatabasen. Detta avsnitt syftar till att ge en vägledning till Ladok3 ur ett grupphanteringsperspektiv.

Generellt så gäller för Ladok 3 att man kommunicerar via ett REST-api samt att man använder federerad inloggning via SWAMID. Ladok 3 är också eventbaserat vilken innebär att man kan prenumerera på händelser.

Från ett grupphanteringsverktyg vill man till Ladok kommunicera vilka användare som har behörighet att göra vad. Till grupphanteringsverktyget vill man från Ladok ha information om vilka studenter som har registrerat sig på vilken kurs och använda den informationen för att kunna generera motsvarande grupper automatiskt.

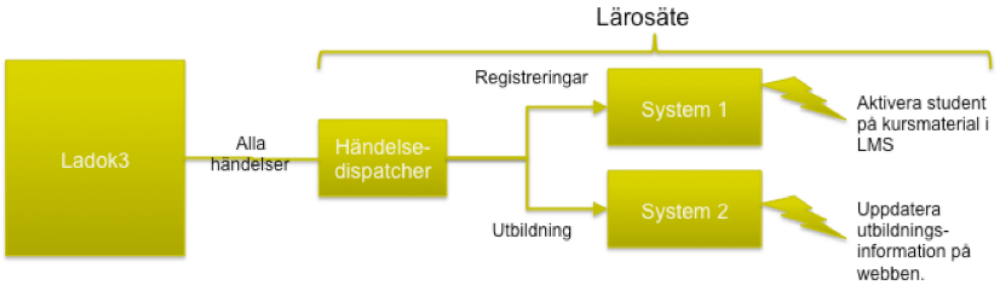
5.3.1 Ladok3 som källsystem för grupper

Idag använder många lärosäten Ladok för att generera kursgrupper till användning i andra system såsom lärplattformar och e-postlistor. Med ett grupphanteringssystem skulle en ny student som registrerat sig på en kurs eller ett program automatiskt kunna få de behörigheter de normalt behöver i olika system. Informationen hämtas idag genom att SQL uttag och förändringar erhålls genom jämförelser mot tidigare uttag. När Ladok ersätts av Ladok3 blir det inte längre möjligt att ta del av informationen via SQL. Istället kommer integrationen att ske via det händelsebaserade gränssnittet (atomfeeds) och/eller REST gränssnittet som Ladok3 tillhandahåller. Det händelsebaserade

gränssnittet kommer sannolikt att kunna erbjuda större möjlighet till finkornighet än dagens lösning. Ladok 3 är uppbyggt i flera domäner och för kursgrupper är de intressanta domänerna studieinformation, som innehåller information om utbildningstillfällen samt domänen för studiedeltagande.

5.3.1.1 Integrationsmönster

Ladok3 rekommenderar att en lokal händelsedispatcher tar emot händelser ifrån Ladok3 och ser till att informationen når de system som har behov av den, se Figur 31. Integrationen med Ladok3 kommer således att vara indirekt för grupphanteringsverktyget, men det ställer krav på att den lokala händelsedispatchern hanterar de händelser som är intressanta för grupphanteringsverktyget.

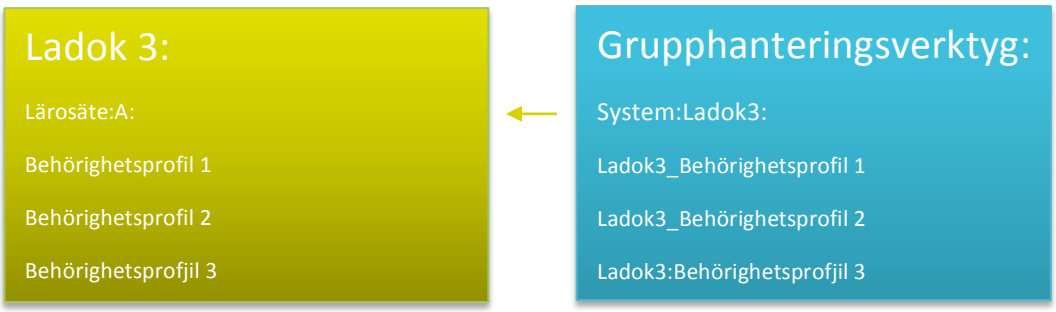


Figur 31: källa Ladok 3 Wiki [23]

Ett uppenbart Use Case i sammanhanget är att man vill hämta alla studenter som anmält sig på en viss kurs från Ladok och utifrån den informationen automatiskt generera motsvarande kursgrupp i grupphanteringssystemet. En ny kursgrupp i grupphanteringssystemet bör sedan medföra att det automatiskt skapas ett kursrum i lärplattform, att studenter ges får access till eventuella labblokaler, att kursdeltagare läggs till på kursens maillista osv…

5.3.2 Integration för att sätta behörigheter

Ladok 3 arbetar med en behörighetsmodell där en kombination av en användares behörighetsprofil och en användares organisatoriska tillhörighet avgör vilken behörighet personen får i systemet. Ett lärosätes olika behörighetsprofiler i Ladok 3 borde alltså representeras av motsvarande grupp i grupphanteringsverktyget.



API:et för Ladok 3 är dock inte slutgiltigt definierat så hur den här integrationen praktiskt kommer att ske på bästa sätt kan vi inte svara på. De två alternativ som huvudsakligen är möjliga är anrop via REST-api:et alternativt via affiliations på liknande sätt som i NyA:s anställdawebb. I dagsläget finns det REST-anrop men däremot inte stöd för affiliations då det behovet inte är klarlagt ännu.

5.4 SUMMERING

Efter arbetet med den här kokboken och de insikter och lärdomar vi gjort på vägen är känslan att de flesta universitet och högskolor skulle tjäna på att införa ett grupphanteringssystem. Det långsiktiga målet i sammanhanget skulle förstås vara att skaffa sig fullständig kontroll över alla användares behörigheter samt säkerställa en robust och konsekvent livscykelhantering. I vårt dagliga arbete ser vi många aktuella användningsfall där vi skulle ha stor nytta av ett etablerat grupphanteringssystem. Det skulle underlätta och ofta medföra stora vinster både i effektivitet och säkerhet, speciellt kring aktiviteter i samband med on-boarding och off-boarding. Andra tydliga fördelar gäller scenarion där man vill kunna producera tillförlitliga rapporter och överblicka vem som har rättighet att göra vad.

När det gäller valet av verktyg så känns Grouper mer generell och FIM lite mer specifik. Den stora skillnaden mellan verktygen är att Grouper är ett renodlat grupphanteringsverktyg medan FIM är en Identity Manager i första hand och ett grupphanteringssystem i andra hand. En bedömning är därför att Grouper är lättare att koppla till befintlig IT-infrastruktur utan att man inledningsvis behöver bygga om sin identitetshantering. Vill man ha både ett identitetshanteringssystem och ett grupphanteringssystem kan det däremot var värt att titta på FIM.

Enligt en artikel i Computer World från 2011 är den höga kostnaden den största nackdelen med FIM. Enligt artikeln behöver man en serverlicens för varje server som en FIM-komponent är installerad på. En annan negativ aspekt var att produkten inte var väl dokumenterad. Där fanns dock en relativt stor FIM community och konsulthjälp var lätt att finna [27]. Aktuella licenskostnader presenteras under avsnitt 6.1.2.4.1 Införandekostnader.

En annan skillnad mellan verktygen är att Grouper har stöd för att både visuellt och organisatoriskt ordna sina grupper hierarkiskt med både mappar i mappar, grupper i mappar och grupper i grupper. FIM jobbar istället objektorienterat där en typ av grupp är ett objekt och man får bygga sin hierarki själv med dubbellänkar från föräldraobjekt till barn och tvärtom.

En reflektion i sammanhanget, vilket Luleå nämnde men vi även hört från andra, är att det för stora inköpta systemen som till exempel Agresso varit väldigt svårt att vinna gehör för de önskemål man haft för att hitta en bra integrationslösning mot ett centralt behörighetssystem. Om det är ett gemensamt problem för många är det något som vi gemensamt borde driva via SUNET Inkubator. Vidare borde vi vid framtida uppköp och design av nya system ifrån Sveriges universitet och högskolor gemensamt kravställa integrationslösningar som fungerar med central grupp- och behörighetshantering.

6 INFÖRANDE OCH FÖRVALTNING

Införandet av ett grupphanteringsverktyg kan vara huvudmålet med ett IT-infrastrukturprojekt eller så ingår grupphanteringsverktyget i ett större införandeprojekt kring Identity- och Accessmanagement, IAM. Eftersom kokboken i första hand är avsedd att handla om grupphantering avgränsas följande avsnitt till att beskriva införandet av grupphantering. Samma argument bör dock kunna användas även i ett större sammanhang där fler delar av IAM införs.

6.1 BEHOVSANALYS OCH BESLUTSUNDERLAG

Vem som har mandat att fatta beslut om att införa IT-infrastrukturella tjänster på lärosätet styrs av delegationsordningen och av lärosätets projektstyrningsmodell. IT-chefen är troligen alltid inblandad i beslutet men vilka som är inblandade i övrigt varierar sannolikt mellan olika lärosäten. Oavsett vem som fattar beslutet om ett införande, ger ett bra underlag en ökad chans att få införandeprojektet beviljat. För att komma fram till ett beslut om att prioritera ett IT-infrastrukturellt införandeprojekt, bland alla andra typer av satsningar, behöver effekten och nyttan kunna beskrivas på ett begripligt sätt även för icke-tekniker.

I jämförelse med verksamhetsnära projekt kan nyttan med ett infrastrukturellt projekt vara svårare att motivera då den ofta är indirekt. Det är först i integrationen med andra system som man kan dra nytta av att det finns ett gott infrastrukturellt stöd. Det kan också vara svårt att påvisa lönsamhet för en infrastrukturell satsning omedelbart, istället blir lönsamheten tydlig först när många system är anslutna till lösningen. Utifrån att projekt bedrivs i syfte att uppnå ett projektmål kan det vara svårt att i ett projekt för införande av verksamhetsspecifikt systemstöd, motivera ett införande av en generell central lösning som kommer andra system tillgodo.

> Exempel: I projektet för ett nytt intranät vid Umeå universitet fanns kravet på stöd för manuell administration av behörighetsgrupper för de samarbetsytor som skulle lanseras samtidigt som behörighetsgrupper utifrån organisatorisk tillhörighet var önskvärda utifrån att institutionsspecifika samarbetsytor skulle skapas. Den valda intranätsplattformen har ett inbyggt stöd för hantering av behörighetsgrupper. Detta medförde att nyttan av att implementera ett generellt grupphanterings-verktyg inte låg inom ramen för projektets mål varvid en intranätsspecifik lösning för den manuella administration av grupperna implementerades där de organisatoriska grupperna lästes in från Active Directory. Hade däremot en generell grupphanteringsplattform redan funnits hade kostnaden att ansluta till den varit mindre och kunna motiverats av nyttan av ett vidare användningsområde för grupperna.

Ett fullständigt beslutsunderlag innehåller

- Beskrivning av projektet
- Lönsamhetsberäkning
- Förutsättningar
- Riskanalys

6.1.1 Beskrivning av projektet

Beskrivningen av projektet omfattar bakgrund, syften och mål. Dessa delar styrs till stor del av hur frågan om införandet av grupphantering väckts i organisationen. Omfattningen av projektet bör också beskrivas.

6.1.1.1 Omfattning

Precis som det beskrivs i avsnitt 4.3 Hur börjar man? finns två generella återkommande rekommendationer när det gäller planering och införande av grupphantering.

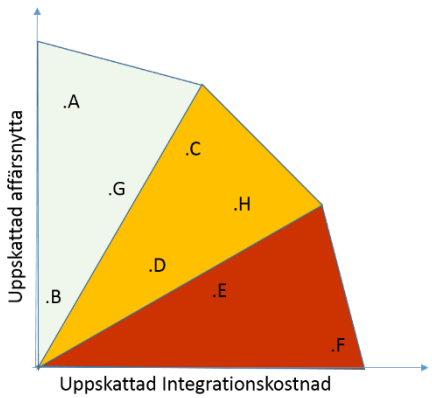
6.1.1.1.1 Tänk allt

Det inledande grundarbetet och analysen bör omfatta en målbild med ett fullt utbyggt stöd för grupphantering där all accesshantering i alla system hanteras direkt eller indirekt mot grupphanteringssystemet. Analysen bör också ge svar på vilka system och tillämpningsområden som undantas till följd av orimlig overhead för en central administration.

Bygg alltså ett grupphanteringssystem som är skalbart och designat att klara av att sköta accesshanteringen för allt. Även system som idag av olika skäl inte är försvarbara att integrera kan på sikt bytas ut och det kan då bli aktuellt att överväga att integrera. ”Tänk allt” innebär också att det skall fungera i interfederationssammanhang samt för molntjänster.

6.1.1.1.2 Bygg ut stegvis

Genom att dela in arbetet i etapper skapas förutsättningar för justeringar och förbättringar allt eftersom projektet fortskrider.



Figur 32 Uppskattningsgraf

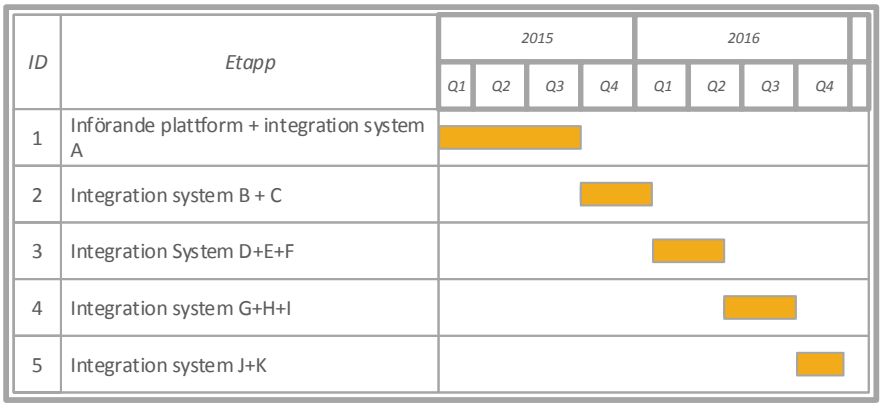
I syfte att redan tidigt leverera nytta så rekommenderas att inledningsvis införa grupphantering i något sammanhang där det genererar tydlig affärsnytta och får stor effekt. Ett sätt att kartlägga det är att göra en skattning och presentera resultaten grafiskt.

Enlig Figur 32 skulle System A och G i den övre gröna triangeln vara mest intressanta att börja med eftersom de ger mest affärsnytta i förhållande till vad det kostar att implementera. Valet kan falla på ett annat system som ger stor affärsnytta om integrationskostnaden går att räkna hem på grund av att man kommer kunna återanvända integrationslösningen mot käll- och/eller målsystem i andra sammanhang.

Införandet av ett centralt grupphanteringsverktyg kräver integrationer till andra system för att det skall vara möjligt att påvisa en positiv lönsamhetskalkyl. Samtidigt kommer det troligen att vara en förhållandevis utdragen process att koppla alla system som skulle kunna dra nytta av central grupphantering till det verktyg som införs. Införandeprojektet kan därför delas in i etapper eller delprojekt där ett antal system kopplas in i varje delprojekt. Alternativt begränsas målet med införandeprojektet till att endast omfatta de högst prioriterade systemen. Detta alternativ bygger

dock på ett antagande om nyttan för resterande system är så stor så att en anslutning i ett senare skede går att motivera.

Vilka systemintegrationer som skall ingå i införandeprojektet bör ingå i beslutsunderlaget. Ett överskådligt sätt att visa vad som ingår i det övergripande projektet och vad som ligger utanför är att visualisera en roadmap för flera år.



Redan i beslutsunderlaget för införandeprojektet bör också grupphanteringsverktygets plats i den övriga IT-infrastrukturen beskrivas.

6.1.2 Lönsamhetsberäkning

Finns en etablerad modell för lönsamhetsberäkning på lärosätet används denna för lönsamhetskalkylen. Ekonomistyrningsverket har en vägledning för hur man räknar på lönsamhet som steg för steg beskriver hur en lönsamhetskalkyl framställs
http://www.esv.se/PageFiles/2864/rakna-pa-lonsamheten.pdf

Oavsett vilken beräkningsmodell som används behöver lönsamhetsberäkningen sannolikt innehålla en nulägesbeskrivning, en beskrivning av det önskade läget och vilka nytta det medför samt vilka kostnader som är förenade med införandet.

I sin enklaste form är lönsamhetsberäkningen resultatet av

$$Nyttovärdet\ av\ projektet - kostnaden\ för\ projektet$$

Ett positivt resultat innebär att projektet är lönsamt.

6.1.2.1 Bakgrund och nuläge

För att kunna relatera nyttan med införandet av ett grupphanteringsverktyg till något behöver bakgrunden och nuläget beskrivas. Beskrivningen bör omfatta vilka behov som finns av grupphantering på lärosätet i nuläget och hur väl dessa behov uppfylls idag, samt vilka system som redan idag använder sig av grupphantering i någon form. Vilka kostnader är förenade med dagens lösning och vad kostar bristerna?

Exempel på frågeställningar att ta upp:

- Saknas det stöd för att administrera vissa typer av grupper?
- Finns det manuellt arbete förenat med administrationen av grupper som skulle kunna automatiseras?

- Finns det grupper som idag administreras i flera system?
- Skapas grupper i onödan för att överblicken över vilka grupper som redan finns är dålig?
- Hur väl uppfylls regler och riktlinjer idag? T ex. utifrån Informationssäkerhet och designprinciper

6.1.2.2 Börlägesanalys

Börlägesanalysen presenterar de alternativa lösningar som finns och redogör för- och nackdelerna med dessa. För att reducera mängden arbete med att ta fram börlägesanalysen bör arbetet läggas upp så att så många alternativ som möjligt kan uteslutas så tidigt som möjligt.

I börlägesanalysen beskrivs syftet med införandet av ett grupphanteringsverktyg och vilka de huvudsakliga skälen till införandet är. Ur ett ekonomiskt perspektiv kan dessa grovt kategoriseras till

- Reducera kostnader
- Öka produktiviteten
- Öka vinsten

Syftet med införandet av ett grupphanteringsverktyg hamnar troligen inom ramarna för de två första kategorierna.

- En ökad automation av grupphanteringen reducerar kostnaderna då antalet arbetsuppgifter som behöver hanteras av personal minskar
- En reduktion av väntetider i verksamhetsprocesserna ökar produktiviteten, till exempel genom att väntetiden för processen att lägga till en medlem i en grupp minskar. Detta kan ske som en följd av ökad automation men också genom och den manuella gruppadministrationen kan delegeras ut till den del av organisationen som har kännedom om hur gruppen skall vara uppbyggd.

Ibland är syftet med ett projekt att lärosätet skall leva upp till externa krav s.k. åligganden. Det kan handla om lag- och regelkrav eller förändrade förutsättningar. Även dessa krav går att översätta i ovanstående ekonomiska kategorisering i en lönsamhetskalkyl. Kostnaden för nuläget beskrivs då som kostnader förenade med att kravet inte uppfylls, eventuella vitesbelopp, skadeståndskrav, förlorade intäkter etc. Den kan också beskrivas som kostnader förenade med att uppfylla kraven utifrån de förutsättningar som ges i dagsläget, även om arbetet i praktiken inte utförs idag.

En förändrad förutsättning för lärosäten som kommer att ske inom de närmsta åren är införande av Ladok3. Den grupphantering som implementerats på flest lärosäten idag är automatisk generering av kursgrupper med studenter som läser på ett visst kurstillfälle för användning t.ex. i lärplattformar. Eftersom Ladok3 kommer att kräva en förändring av den automatiska genereringen av kursgrupper kommer nulägeskostnaden omfatta kostnaderna för att den automatiska kursgruppsgenereringen saknas. Börläget kan däremot se olika ut beroende på i vilket sammanhang lönsamhetskalkylen tas fram. Genomförs lönsamhetskalkylen i det lokala Ladok3-införande projektet handlar det kanske bara om kostnaden för att anpassa nuvarande lösning till ladok3 som källsystem. Är syftet med lönsamhetskalkylen istället att motivera ett införande av ett (nytt) centralt grupphanteringsverktyg skall börläget återspegla kostnaderna för att implementera den automatiska grupphanteringen i det centrala grupphanteringsverktyget

Ett skäl som framhävs i många infrastrukturella satsningar är en ökad säkerhet, som i IT-system ofta handlar om informationssäkerhet. Informationssäkerhetshöjande åtgärder kan betraktas som tvingande systemanpassningar.

Vilken nivå på informationssäkerhet som skall gälla för ett system beror på vilken informationsklassning som finns för den information som systemet behandlar. I informationsklassning bedöms kraven på

- Tillgänglighet, att information finns tillgänglig när den behövs
- Konfidentialitet, att informationen är åtkomlig endast för dem den berör
- Tillförlitlighet, att informationen är korrekt

Audit eller möjlighet till uppföljning av vilka som tagit del av/ändrat informationen räknas ibland också in som ett informationssäkerhetskrav. Det är främst när det gäller kraven på tillgänglighet, konfidentialitet och audit som ett centralt grupphanteringsverktyg kan bidra med stöd till de applikationer som är anslutna till systemet.

I valet mellan en systemspecifik grupphantering eller ett centralt system erbjuder den första ofta en finkornigare lösning för accesskontroll. Denna typ av argument emot en central hantering måste kunna mötas t.ex. genom att påvisa ökade administrativa kostnader ur ett holistiskt perspektiv på lärosätesnivå.

6.1.2.3 Nyttohemtagning

Förutom att beskriva hur nyttan skall realiseras bör det även beskrivas vem som är ansvarig för att säkerställa att nyttan uppnås.

	2015	2016	2017	2018	2019
Minskad administration					
Effektiviserad behörighetsgivning					
Central översikt av behörigheter					
Automatiserade användargrupper					
…					
Totalt					

6.1.2.4 Kostnader

Kostnaderna förenade med att genomföra de förändringar som införandet innebär både i själva projektet men även långsiktigt när systemet gått in i förvaltning redogörs.

Kostnaderna bör redovisas per år fram till dess att en stabil nivå för förvaltningen av systemet uppnås och redovisningen bör också synkroniseras med nyttoberäkningarna.

	2015	2016	2017	2018	2019
Införandekostnader					
Kostnader för anskaffning					
Licenskostnader					
Projektkostnader					
Förvaltningskostnader					
-Systemförvaltning					
-Ändringshantering					
-Användarstöd					
-Licensavgift					
-support och underhållsavtal					
-Drift och övervakning					

6.1.2.4.1 Införandekostnader

Oavsett valet av teknisk lösning för grupphantering behöver ett införandeprojekt inledas med ett arbete med att bestämma vad grupperna skall användas till och hur administrationen av grupperna skall hanteras. Räkna med minst ett halvårs kalendertid med en utredare på någonstans mellan 25-50% arbetstid plus tid för workshops med berörda verksamhetsområden om en bred förankring skall kunna uppnås.

En analys av möjligheterna i potentiella källsystem att integrera för att skapa användargrupper behöver genomföras.

- Vilka tekniska förutsättningar finns för en integration?
- Vilken information behövs för att kunna generera grupper?

Svaret på dessa frågor kan kräva kontakter med leverantörer och diskussioner med informationsägaren för källsystemet och en uppskattning är det krävs minst en veckas analys per källsystem som skall integreras för att ta fram ett lösningsförslag.

På samma sätt måste integrationsmöjligheterna analyseras i system till vilka accessgrupper från grupphanteraren skall distribueras. Även här krävs minst en veckas analys per system.

- Vilka tekniska förutsättningar finns för en integration?
- Vilka accessgrupper skall finnas?
- Hur ska dessa accessgrupper administreras? Manuellt/automatiskt?

Om införandet av en central grupphanterare innebär nya arbetssätt behöver tid också läggas på att ställa om organisationen till ett det nya sättet att arbeta.

Är valet att bygga ett grupphanteringsverktyg från grunden tillkommer implementationskostnaderna till införandeprojektet utifrån att kraven i avsnitt 4.11 skall realiseras.

Faller valet istället på en befintlig grupphanterare behöver installations- och konfigureringskostnader tas med i beräkningarna samt eventuella utbildningskostnader för teknikerna som sedan skall implementera och förvalta systemet.

För FIM tillkommer dessutom licenskostnader för produkten om det inte är så att produkten redan används för identitetshantering på lärosätet. Räkna med följande att följande licenser krävs:

- En serverlicens per server 10 000 -15 000 tkr
- SQLserver licenser för att lagra informationen om grupperna
- En CAL per användare man lagrar information om. Ca 14 kr/användare

Detta motsvarar för Linköpings universitet med knappt 3400 användare drygt 160 tkr/år.

Oavsett val av grupphanterare behöver tid läggas på att implementera de grupper och integrationer som identifierats under analysfasen.

6.1.2.4.2 Förvaltningskostnader

Omfattar kostnader för att hålla systemet i drift, här ingår till exempel kostnader för licenser, support och underhållsavtal, drift och övervakning av systemet samt tid för att bedriva systemförvaltning, se vidare specifikation i avsnitt 6.3

6.1.3 Förutsättningar

Grupphantering utgör sannolikt inte den första komponenten inom identitets- och accesshantering som införs utan behovet av stöd för grupphantering kommer förmodligen inte in i bilden förrän lärosätet uppnått en utökad mognadsnivå enligt Figur 11. Det är också viktigt att redogöra för vilka beroenden som finns till övrig infrastruktur och sätta in lösningen i sitt sammanhang.

Förutom att de infrastrukturella förutsättningarna behöver vara uppfyllda bör tidpunkten för införandet också bedömas.

- När är det sannolikt att de resurser som krävs för ett lyckat införande finns tillgängliga?
- Finns det andra högt prioriterade arbetsuppgifter som riskerar att ta fokus ifrån projektet?
- Finns det en mottagande förvaltningsorganisation som kan ta hand om resultatet efter införandet?

6.1.4 Risker

Identifiera vilka risker som finns med den lösning som föreslås och vilka åtgärder som skall vidtas för att minimera dessa risker. En bedömning av vilken sårbarhet som finns för att upprätthålla kompetensen för en teknisk förvaltning av lösningen långsiktigt bör ingå.

För en egenutvecklad lösning krävs sannolikt ett större långsiktigt åtagande lokalt på lärosätet och fler än en resurs med kompetens för lösningen för att undvika ett nyckelpersonsberoende.

Även en lösning baserad på Grouper kräver ett upprätthållande av lokal kompetens under lång tid även om stöd finns att hämta i Groupers aktiva community och kompetensen som behöver upprätthållas kan begränsas till den lokala tillämpningen av Grouper.

För FIM är det möjligt att själv implementera grupphanteringen men det finns också möjlighet att köpa in konsultstöd för implementationen. Om det senare alternativet är aktuellt blir det viktigt att vidtaga åtgärder för att undvika inlåsningseffekter i form av ett konsultberoende för den lärosätesspecifika lösningen.

6.1.4.1 Molntjänst

Kommer lösningen på något sätt att omfatta en molntjänst krävs också att en risk- och sårbarhetsanalys utifrån ett informationssäkerhetsperspektiv eftersom grupphanteringsverktyget kommer att hantera personuppgifter.

6.2 INFÖRANDEPROJEKT

Beslutet om att ett införande av ett grupphanteringsverktyg har fattats. Mycket av det material som använts i beslutsunderlag bör kunna återanvändas när projektplanen för projektet skrivs.

6.2.1 Organisation

Beställaren av projektet tillhör rimligtvis ledningen i IT-organisationen vid lärosätet då grupphantering är en IT-infrastrukturell tjänst. Med i styrgruppen bör även de verksamhetsområden som blir berörda vara representerade. Nedan listas övriga intressenter som kan vara rimliga att ha i åtanke vid besättandet av rollerna i ett införandeprojekt för ett grupphanteringssystem.

6.2.1.1 Framtida förvaltningsorganisation

Att redan i införandeprojektet av grupphanteringssystemet ta med representanter från den framtida förvaltningsorganisationen underlättar övergången från projekt till förvaltningen. Det innebär också att det finns en mottagare att diskutera krav kring förvaltningsbarhet och leverablerna från projektet

6.2.1.2 Informationsägare i källsystemen

För de grupper som skall genereras automatiskt krävs någon form av integration med ett källsystem. Oavsett om denna integration är direkt med källsystemet eller via en integrationsplattform eller IdM, är det ursprungliga källsystemet informationsägare. Detta medför att informationsägaren i källsystemet måste godkänna användningen av informationen i grupphanteringssystemet och vara medveten om användningsområdet.

6.2.1.3 Målsystemens förvaltning

För system som direkt eller indirekt integreras med grupphanteringshanteringsverktyget, ingår förvaltningsorganisationerna för dessa i listan över intressenter. Förutom att kravställa hur de specifika grupperna skall sättas upp behöver integrationsmetoder beslutas i samråd med denna.

6.2.2 Leverabler

De produkter som ett införandeprojekt för ett grupphanteringsverktyg bör leverera beskrivs nedan:

6.2.2.1 Teknisk plattform för grupphantering

Den tekniska plattformen för grupphanteringsverktyget med tillhörande systemdokumentation.

6.2.2.2 Gränssnitt för integration mot grupphanteringssystemet

Förutom att definiera och implementera de tekniska integrationsgränssnitten mot grupphanteringssystemet bör även rutiner för att hantera en nya integration etableras. Om det är en egenutvecklad plattform kommer det mesta arbetet bestå i att ta fram gränssnittet, om en befintlig grupphanteringsplattform istället anskaffas bör arbetet bestå i att ta fram ett proxygränssnitt för att minimera påverkan på integrerande system vid framtida systemuppdateringar.

6.2.2.3 Användargränssnitt

Då administrationen av manuella grupper kommer vara decentraliserad i hög utsträckning är det viktigt att det är självinstruerande, tydligt och enkelt. Att gränssnittet inte innehåller mer information än vad som är relevant för användaren kan vara ett angreppssätt för detta. Detsamma gäller om användargränssnitt utvecklas för gruppmedlemmar själva skall kunna gå in och se vilka grupper de tillhör eller vilka behörigheter de har.

6.2.2.4 Gruppolicy

Gruppolicyn bör omfatta vilka användningsområden grupphanteringsverktyget är avsett för samt vilka krav som ställs på hur en grupp hanteras i systemet i fråga om namnstandard, attribut på gruppen, livscykelhantering etc. Beroende på val av grupphanterare kan det vara så att vissa delar av policyn också går att lägga in som regler i verktyget.

6.2.2.5 Användardokumentation

För användarna av grupphanteringsverktyget behöver självstudiematerial kring hur verktyget används tas fram. För att underlätta förvaltningen av utbildningsmaterialet kan små korta instruktioner i exempelvis en wiki eller korta instruktionsvideos vara att föredra framför en fullständig instruktionsbok. På så sätt att det är enkelt att byta ut en inaktuell del i samband med en systemuppgradering.

Om valet av grupphanterare blir ett standardsystem är det möjligt att det finns befintliga instruktioner till hur systemet skall användas som tillhandahålls av leverantören eller motsvarande. En bedömning bör dock göras vilket material som är lämpligt att använda och hur det behöver kompletteras för att passa den lokala tillämpningen.

6.2.2.6 Förvaltningsplan

Oavsett om förvaltningen av grupphanteringsverktyget initialt sker i projektets regi eller överlämnas till förvaltningsorganisationen redan vid första leveransen erbjuder förvaltningsplanen ett gott stöd för för att hålla ordning på den löpande driften. Förvaltningsplanen bör gälla från och med det att system tagits i drift.

6.2.2.7 Kontinuitetsplan

Vilka konsekvenser som ett längre driftsavbrott för grupphanteringsverktyget medför bör kartläggas och vilka alternativa rutiner som då skall gälla bör dokumenteras i kontinuitetsplanen för systemet. I planen skall det också framgå vilken ansvarsfördelning som gäller vid ett avbrott. I samband att kontinuitetsplanen etableras bör också systemets prioritetsordning i förhållande till andra system fastställas för den händelse att ett driftsavbrott drabbar många system.

Implementationen av grupphanteringsverktyget påverkar innehållet i kontinuitetsplanen. Är den enda effekten av ett driftsavbrott att det inte går att skapa ny grupper påverkar det verksamheten

mindre än om konstant tillgänglighet av grupphanteringsverktyget är avgörande för tillgången till accessgrupper i andra system.

Kontinuitetsplanen överlämnas till förvaltningsorganisationen i samband med etableringen av förvaltningen.

6.2.3 Aktiviteter

De övergripande aktiviteterna i ett införandeprojekt av central grupphantering faller inom ramen för följande aktiviteter:

- Fastställa gruppolicy
- Etablera teknisk plattform för grupphanteraren
- Skapa integrationer emot källsystem
- Skapa integrationer till mottagande system
- Etablera förvaltningsorganisation

6.2.4 Etapper

Indelningen av projektet i etapper bör ha sin utgångspunkt i att varje etapp skall kunna definiera nytta och att det finns ett uttalat mål för etappen. Utifrån utgångspunkten tänk helhet men implementera stegvis kan en lämplig indelning vara utifrån de användningsfall som identifierats. Den första etappen skulle då innehålla minst ett användningsfall förutom aktiviteter för grundläggande uppsättning av systemet. Kommande etapper bygger vidare med fler användningsfall och eventuella anpassningar till grundstrukturen som dessa kräver. Revideringar av grundstrukturen bör bli mindre och mindre för varje etapp

1. Etapp 1: grundläggande etablering
    a. Fastställa gruppolicy
    b. Etablera teknisk plattform för grupphanteraren
    c. Implementera första användningsfallet
    d. Etablera förvaltningsorganisation
2. Etapp 2 och vidare etapper
    a. Revision av gruppolicy
    b. Tillägg och anpassningar av den tekniska plattformen
    c. Tillägg och anpassningar till integrationerna emot grupphanteringsverktyget

6.2.5 Kommunikationsplan

Förutom intern kommunikation i projektet bör kommunikationsplanen även omfatta aktiviteter som beskriver hur man når ut till andra, hur man når framtida användare och målgrupper i organisationen.

Om en etapp exempelvis omfattar implementation av grupphantering i syfte att skapa e-postlistor, ingår kanske en e-postlista för antagna studenter. Samma generiska funktionalitet i grupphanteringsverktyget skulle också kunna användas för att skapa en e-postlista till alla studenter som läst 2 år på lärosätet. Ur projektets perspektiv har nyttan med denna lista inte identifieras, men programansvariga för Mastersprogrammen som inte är inblandade i projektet skulle kunna vara intresserade av detta.

6.2.6 Utbildning

En stor del av grupphanteringssystemet skall baseras på automatiskt genererade grupper utifrån input ifrån andra system och jobbet genomförs utan mänsklig inblandning. Denna del kräver därför inte någon utbildning av slutanvändare. Administrationen av manuella grupper däremot bör ske decentraliserat och det är mot denna användargrupp som utbildningsinsatserna bör vara riktade. Den decentraliserade hanteringen medför att det är relativt många som kommer att vara administratörer av manuella grupper och det är rimligt att räkna med minst en administratör per institution/avdelning. Till följd av mängden administratörer, samtidigt som gruppen kommer att vara relativt heterogen både vad gäller IT-kompetens och befattning, är traditionell ”klassrums”-utbildning olämplig och fokus bör ligga på självstudier.

6.3 SYSTEMFÖRVALTNING

Grupphanteringsverktyget behöver förvaltas enligt de processer som tillämpas vid lärosätet. En av de vanligast förekommande systemförvaltningsmodellerna i på svenska lärosäten är PM3 och rapporten har därför utgått ifrån denna i beskrivningen av systemförvaltning. Modellen förespråkar en paketering av system i objekt. Grupphanteringsverktyget bör paketeras som tjänsteerbjudanden tillsammans med övriga IAM tjänster på lärosätet.

6.3.1 Förvaltningsprodukter

Till förvaltningen av ett grupphanteringsverktyg bör följande förvaltningsprodukter tas i beaktande:

6.3.2 Grupphanteringsverktyget

Utgör IT-systemet som förvaltas. Förutom lagring av information kring grupperna, innehåller verktyget regler samt användargränssnitt för gruppmedlemmar och gruppadministratörer.

6.3.2.1 Gruppolicy

Gruppolicyn bör omfatta vilka användningsområden grupphanteringsverktyget är avsett för samt vilka krav som ställs på en grupp som hanteras i systemet i fråga om namnstandard, attribut på gruppen, livscykelhantering etc. Beroende på val av grupphanterare kan det vara så att vissa delar av policyn också går att lägga in som regler i verktyget.

6.3.2.2 Användardokumentation

Se beskrivning i avsnitt 6.2.2 Leverabler

6.3.2.3 Adaptrar till grupphanteringsverktyget

En integration innebär att minst två system kommunicerar med varandra. Tillhör dessa olika system olika förvaltningsobjekt blir det viktigt att fastställa hur ansvarsfördelningen mellan dessa två förvaltningsobjekt ser ut. Ingår integrationen som en del av källsystemets eller det mottagande systemets förvaltning eller en kombination av båda dessa? Finns det en integrationsplattform bör det huvudsakliga ansvaret ligga i förvaltningen av denna, medan ansvaret för respektive systemadapter bör ligga i respektive förvaltningsobjekt.

6.3.3 Förvaltningsorganisation

Grupphanteraren bör sannolikt inte förvaltas i en egen förvaltningsorganisation utan ingå i ett förvaltningsobjekt kopplat till IT-infrastrukturen på lärosätet så som identitetshantering och katalogtjänst. Uppsala universitet har valt att lägga systemförvaltningen av sin grupphanterare i

objektet Gemensam IT. På Umeå universitet skulle den sannolikt hamna i objektet för Teknisk plattform.

	Verksamhetsnära	*IT-nära*	*Denna nivå skapar basen i*
Budget	Objektägare	IT-systemägare	Styrgrupp
Beslut	Objektansvarig	IT-systemansvarig	Förvaltningsgrupp
Operativ	Objektspecialist	Driftsansvarig Applikationsansvarig	

Tabell 1: Förvaltningsorganisation enligt PM3

Som i all förvaltning av IT-infrastruktur ligger utmaningen i att fånga slutanvändarnas önskemål och synpunkter då förvaltningsobjektet ofta berör många olika verksamhetsprocesser. Påverkan är dessutom ofta indirekt genom integrationer med andra förvaltningsobjekt. Det är rimligt att tro att även ett grupphanteringsverktyg skulle stå inför samma utmaningar.

Ett sätt att hantera detta är att säkerställa att det finns en dialog mellan förvaltningen av grupphanteringsverktyget och de förvaltningsobjekt som integrerar emot grupphanteringsverktyget på beslutsnivå. Ett annat sätt kan vara att knyta referensgrupper till förvaltningsorganisationen.

6.3.4 Förvaltningsaktiviteter

6.3.4.1 Systemförvaltning

Ett grupphanteringsverktyg kräver i likhet med annat IT-infrastrukturellt stöd sannolikt samverkan med omkringliggande systemförvaltningsobjekt.

6.3.4.2 Marknadsföring

Hur går man vidare för att öka användningen efter införandeprojektet är till ända? Att sälja in ett bra erbjudande kan vara mer effektivt än att påtvinga organisationen en lösning. Beroende på hur många system som anslöts i införandet av grupphanteringsverktyget finns eventuellt fler system som skulle kunna dra nytta av central grupphantering. För dessa systems ägare är det viktigt att fortsätta dialogen och peka på fördelarna. Det kan också finnas användningsområden som inte förutspåddes vid införandet som ytterligare ökar nyttan. Att aktivt berätta om vad som redan är infört i olika forum, kanske i form av ”success stories” kan bidra till att fler användningsområden identifieras.

6.3.4.3 Användarstöd

Användarstödet riktar sig i huvudsak mot administratörer av manuella grupper. Förutom att besvara frågor ifrån användarna bör användarstödet fokusera på att säkerställa att dokumentation och utbildningsmaterial hålls uppdaterat.

Beroende på hur stor grad av självservice som implementerats eller regler kring åtkomsten av informationen i grupphanteringssystemet, kan det vara så att vissa funktioner inte är tillgängliga för alla användare, utan kräver att centrala administratörer tar ut information ifrån systemet. Exempel på sådana uttag kan vara statistiskt underlag till verksamhetsberättelsen kring åldersfördelningen för en viss grupp av användare. Underlaget med vilka användare som ingår i gruppen erhålls kan behöva tillhandahållas av en central administratör.

6.3.4.4 Ändringshantering

Finns en etablerad ändringsprocess vid lärosätet bör denna tillämpas även när det kommer till ändringar i grupphanteringsverktyget.

Då en relativt stor andel av informationen i grupphanteringssystemet är information som härstammar ifrån andra källsystem, samtidigt som informationen från grupphanteringsverktyget används i andra system är det viktigt med en bred förankring när en ändring skall ske. Användning av referensgrupper med olika fokusområden bör övervägas som stöd till beslut kring ändringshantering.

Informationskontrakt

En modell som Linköpings universitet infört för att underlätta dialogen mellan parterna i en integration är informationskontrakt som godkänns av informationsägaren för källsystemet innan en integration får ske. Ett informationskontrakt upprättas för varje integration och innehåller uppgifter om vilken information som sprids mellan käll- och målsystemen. Informationskontraktet underlättar även för informationsägaren i händelse av en informationssäkerhetsrevision. Kopplat till ett grupphanteringsverktyg skulle det finnas ett informationskontrakt för varje källsystem och varje ny integration som innebär en spridning av den informationen till ett annat system skulle kräva ytterligare ett informationskontrakt.

6.3.5 Daglig drift och underhåll

Inom ramen för daglig drift och underhåll faller aktiviteter för att hålla systemet i drift. Förutom övervakning av själva grupphanteringssystemet blir det viktigt att hålla koll på att integrationerna till och från systemet fungerar.

6.3.5.1 Registervård

Även om målsättningen är att hanteringen av grupperna skall vara så automatiserad som möjligt och decentraliserad i hög utsträckning, är det rimligt att tro att det kommer att finns händelser som kräver registervård. Effekterna av en omorganisation skulle t ex kunna få effekter på strukturen av manuella grupper.

Rutiner för genomgång av inaktiva och tomma grupper bör också falla inom ramen för registervård. Det dagliga arbete som läggs ned av gruppadministratörerna för att hålla enskilda grupper uppdaterade med rätt medlemmar bör däremot kunna anses tillhöra ordinarie användning av systemet.

6.4 SUMMERING

Införandet av ett grupphanteringssystem kräver omfattande analyser och förberedelser och dessa är oberoende av vilken systemlösning som grupphanteringen implementeras med hjälp av. I valet mellan egenutvecklat systemstöd eller anskaffning av ett befintligt systemstöd bör både kostnaderna för ett införande och riskanalysen för de olika alternativen ligga till grund för beslutet.

Grupphanteringsverktyget bör förvaltas tillsammans med övrig identitetsinfrastruktur på lärosätet. Förväntningen finns att systemet skall kräva lite användarsupport trots spridda användningsområden och relativt många användare i systemet. För att kunna uppfylla denna förväntan är det viktigt att rutiner och riktlinjer kring systemet är framtagna och kommunicerade.

TERMER OCH FÖRKORTNINGAR

ABAC	Attribute Based Access Control. Attributbaserad accesskontroll innebär att access garanteras om ett eller flera attribut har rätt värde. Om attribut som testas mot en viss regel ger utfallet sant så ges access. Attributen kan vara användarattribut, mijlöattribut, tidsattribut, etc..
	
	Om du behöver vara en anställd fakultetsperson som har rätt att godkänna utbetalningar i EkonomisystemX men bara mellan 7.00 och 17.00 så skulle en regel kunna se ut typ :
	
	`If (`
	
	`(eduPersonAffiliation == staff) && (eduPersonPrimaryAffiliation == Faculty) &&`
	
	`(17.00 < CurrentTime > 07.00) &&`
	`(Memberof(EconomySystemX:Sign))) {`
	
	`Access = True;`
	
	`}`
	
	Regler kan till exempel skrivas I XACML. Axiomatics [24] är ett exempel på produkt som tillhandahåller detta.

CIFER	Community Identity Framework for Education and Research. CIFER vill samla open source initiativ inom identity management som är orienterade mot högre utbildningar och forskning.
Comanage	Collaborative Organization Management. Ett projekt inom Internet2 Middleware Initiative som syftar till att utveckla applikationer som ingående medlemmar, Cos, kan använda. Exempel på applikationer är wikis, kalendrar och konferensapplikationer.
eduGAIN	eduGAIN har som intention att möjliggöra ett pålitligt utbyte av information relaterade till identiteter, autentisering och auktorisation mellan GEANT parters federationer. Detta sker genom att eduGAIN koordinerar vissa tekniska element i federationens infrastruktur samt framtagande av policys. Målet är att möjliggöra Web-SSO till tjänster som tillhandahålls av ingående och samarbetande parter.
e-Science	e-Science refererar till vetenskap och forskning som i ökande grad kommer att utföras genom ett globalt och distribuerat samarbete som är möjligt genom internet. Alla relevanta resurser inom ett forskningsområde integreras och nödvändiga verktyg ställs till förfogande. Denna infrastruktur organiserar bland annat fördelningen av tunga databeräkningar, stödjer samarbetsprocesser samt tillhandahåller en plattform för publicering av forskningsresultat som i sin tur kan vara en källa till vidare forskning.
FIM	Microsoft Forefront Identity Manager 2010 R2. En state-baserad identitetshanteringsprodukt som är designad att hantera ett företags eller en organisations användares digitala identiteter, persondata och grupper.
GÈANT	GÉANT är det pan-Europeiska forsknings och utbildningsnät som kopplar samman Europas nationella forsknings och utbildningsnät (NRENs).

	Tillsammans kopplar man ihop mer än 50 miljoner användare. GÉANT är ett av de mest avancerade forskningsnäten i världen. GÈANT når även 65 länder utanför Europa.
Grouper	Ett access management system utvecklat av Internet2, designat för den vitt administrativt distribuerade och den heterogena tekniska miljö som är vanlig inom universitet och högskolor. Det möjliggör att man kan hantera access både centralt och distribuerat och med delegerad administration. En open source programvara.
Horizon2020	Eus största forsknings och innovationsprogram någonsin med nära 80 billioner Euro i finansiering fördelat över 7 år (2014-2020). Tillsammans med de privata investeringar dessa pengar kommer att attrahera förväntar man sig att det skall generera nya genombrott, upptäckter och världsledande idéer som också kan tas från forskningslabbet till marknaden.
InCommon	InCommon skapar och underhåller ramverket för gemensamt förtroende när det gäller identiteter och access inom utbildning och forskning i USA. ”InCommon Federation” är USAs forsknings- och utbildningsfederation.
Internet2	Internet2 är en icke vinstdrivande datornätskonsortsium som bland annat levererar nät till ca 250 av USA:s lärosäten inom högre utbildning, dvs de är en av USA:s NREN. Internet2 började som ett universitetsprojekt för avancerad utveckling av internet 1997 i form av UCAID. Idag har Internet2 ett registrerat varumärke och har ca 500 medlemmar varav ca hälften är lärosäten. Övriga medlemmar kommer bland annat från industrin, övriga forskningsvärlden, statliga myndigheter, är andra nätverk eller samarbetspartners. Internet2 utvecklar fortfarande framtidens nätverkstekniker. Där ingår bland annat identitets- och accesshanteringsverktyg.
NRENS	National Research and Education Networks. SUNET är ett exempel på ett sådant.
RBAC	Role Based Access Control. Rollbaserad access. Rättigheter är tilldelat en viss roll. Har man den rollen så får man dessa rättigheter. En person kan ha flera roller. En roll kan ha flera rättigheter. Roller kan även vara hierarkiskt ordnade så att roller ärver rättigheter från sina föräldrar.
REFEDS	En grupp som representerar krav från forsknings- och utbildningsvärlden inom det stadigt växande området access- och identitetshantering. Man samarbetar med organisationer som Kantara, OIX och Identity Commons. REFEDS medlemmar delar ett intresse i att utveckla teknologier inom identitets- och behörighetshantering samt gemensamma policys och processer. Medlemmarna har olika bakgrund men många representerar nationella identitetsfederationer och av dessa kommer många från NRENS.
SICS	The Swedish Institute of Computer Science. Sveriges ledande forskningsinstitut inom tillämpad Informations- och kommunikationsteknologi.
SIEM	Security Information and event management. En term för mjukvara som kombinerar SIM och SEM. Security Information Management och Security Event Management. System som i realtid samlar ihop data, analyserar loggar utifrån ett säkerhetsperspektiv och notifierar om eventuella konstigheter samt presenterar.
SWAMID	Sorterar under SUNET och är Sveriges identitetsfederation som omfattar de

	flesta universitet, högskolor och övriga myndigheter som är relaterade till forsknings- och utbildningssektorn.
TIER	TIER står för Trust and Identity in Education and Research. Det är tänkt att fungera som en koordinator av de olika initiativ inom Internet2-samarbetet som på olika sätt arbetar för att supporta access, samarbete och interoperabilitet mellan identitetsinfrastrukturer inom högre utbildningar i USA. Det omfattar allt från open source mjukvara i form av bland annat Grouper till policys, scheman, Shibboleth, MACE register, LDAP-scheman, applikationer, federationen, multifaktorautentisering och certifikat.
Vetenskapsakademien	En svensk oberoende organisation grundad 1739. Uppgiften är att främja vetenskaperna och stärka dess inflytande. Akademin utgörs av dess ledamöter som idag är ca 450 varav 175 är utländska. Akademin tar av hävd särskilt ansvar för naturvetenskap och matematik och strävar efter att sprida kunskap om aktuell forskning, delta i samhällsdebatten kring utbildning och har nära kontakt med internationella vetenskapliga organisationer. De delar också ut priser, belöningar och stipendier. De mest kända är Nobelpriset i Fysik och Kemi.
Vetenskapsrådet	Vetenskapsrådet är den svenska myndighet under utbildningsdepartementet som har som uppgift att utveckla svensk forskning och därmed bidra till samhällets utveckling. De arbetar bland annat med att fördela medel till forskning, analysera och ta fram strategier, fungera som rådgivare till regeringen i forskningspolitiska frågor, hantera etik och genusfrågor inom forskning, sprida kunskap om nya forskningsresultat och göra de tillgängliga och se till att de når områden i samhället där de kan komma till nytta, samt att öka förståelsen för grundforskningens betydelse i samhället. Vetenskapsrådet har också som uppdrag att främja mång- och tvärvetenskaplig forskning samt att sträva efter ökat nationellt och internationellt samarbete.
VINNOVA	VINNOVA är en statlig myndighet under Näringsdepartementet och är också nationell kontakmyndighet för EU:s ramprogram för forskning och utveckling. De är vår innovationsmyndighet med uppgift att främja hållbar tillväxt genom att förbättra förutsättningarna för innovation och de finansierar även forskning. Varje år investerar VINNOVA ca 2.7 miljarder i forskning. Medel som skall medfinansieras från andra aktörer med lika mycket så totalt ger det 5.4 miljarder till innovativ forskning i Sverige varje år.

REFERENSER

[1] European Commission, Directorate-General for Reserach and Innovation, ”Innovation union - A pocket guide on a Europe 2020 initiative,” 2013.

[2] TIER, Internet2, [Online]. Available: http://www.internet2.edu/products-services/trust-identity-middleware/. [Använd Oktober 2014].

[3] InCommon, Internet2, [Online]. Available: https://www.incommon.org/.

[4] Shibboleth. [Online]. Available: https://shibboleth.net/.

[5] Shibboleth, Internet2, [Online]. Available: http://www.internet2.edu/products-services/trust-identity-middleware/shibboleth/.

[6] COmanage, Internet2, [Online]. Available: http://www.internet2.edu/products-services/trust-identity-middleware/comanage/.

[7] eduGAIN, GÉANT, [Online]. Available: http://www.geant.net/service/eduGAIN/Pages/home.aspx.

[8] HORIZON2020, European Commission, [Online]. Available: http://ec.europa.eu/programmes/horizon2020/.

[9] Carl-Fredrik Sorensen, Bård Henry Moum Jakobsen, Geri Vangen, Jan Erik Garshol, Arild Halsetronning, ”Samarbeid om IKT-arkitektur for statlige universiteter och hyskoler,” UNINETT, 2011.

[10] CIFER IAM Testbed, Internet2, 27 Mars 2014. [Online]. Available: https://spaces.internet2.edu/display/cifer/IAM+Testbed.

[11] InCommon Collaborate Pilot with eduGAIN, Internet2, 3 September 2014. [Online]. Available: https://spaces.internet2.edu/display/InCCollaborate/2014/09/03/InCommon+Expands+Support+for+International+Research+Through+Pilot+With+University+of+Wisconsin-Milwaukee.

[12] ”Category R&S, Research and Scholarship,” InCommon, [Online]. Available: https://spaces.internet2.edu/display/InCFederation/Research+and+Scholarship+Category.

[13] REFEDS, Terena, Code of Conduct, [Online]. Available: https://refeds.terena.org/index.php/Introduction_to_Code_of_Conduct.

[14] FEIDE, UNINETT , Kunnskapsdepartementet i Norge, [Online]. Available: https://www.feide.no/.

[15] SWAMID, SUNET, [Online]. Available: http://www.swamid.se/.

[16] eduID, SUNET, [Online]. Available: http://www.sunet.se/Tjanster/SUNETs-tjanster-/eduID.html.

[17] eduID. [Online]. Available: https://www.eduid.se/.

[18] Gartner, ”Identity & Access Management Summit,” 2-4 december 2014. [Online]. Available: http://www.gartner.com/technology/summits/na/identity-access/.

[19] ”Grouper Wiki,” Internet2, [Online]. Available: https://spaces.internet2.edu/display/Grouper/Grouper+Wiki+Home.

[20] ”Grupper av typen Roll,” Internet2, [Online]. Available: https://spaces.internet2.edu/display/Grouper/Grouper+Role+and+Permission+Management.

[21] ”Folder taggad som Service,” [Online]. Available: https://spaces.internet2.edu/display/Grouper/Organizing+services+in+Grouper.

[22] ”Grouper Attribute framework,” [Online]. Available: https://spaces.internet2.edu/display/Grouper/Grouper+attribute+framework.

[23] ”Ladok 3 Wiki,” [Online]. Available: https://confluence.its.umu.se/confluence/pages/viewpage.action?pageId=62295273.

[24] Axiomatics. [Online]. Available: http://www.axiomatics.com/why-axiomatics.html.

[25] Grouper, ”rules use cases,” [Online]. Available: https://spaces.internet2.edu/display/Grouper/Grouper+rules+use+cases.

[26] Carl-Fredrik Sörensen, NTNU; Bård Henry Moum Jakobsen, UiO; Geir Vangen, UiO; Jan Erik Garshol, BIBSYS; Arild Halsetrönning, UNINETT, ”SAMARBEID OM IKT-ARKITEKTUR FOR STATLIGE UNIVERSITETER OG HØYSKOLER,” UNINETT på uppdrag av Kunnskapsdepartementet, 17 mars 2011.

[27] Computerworld, ”Hands on with Microsoft Forefron Identity Manager 2010” [Online]. Available: http://www.computerworld.com/article/2510600/infrastructure-management/hands-on-with-microsoft-forefront-identity-manager-2010.html?page=2

[28] Technet Blog, ”Microsoft Identity Manager Preview Release” [Online]. Available: http://blogs.technet.com/b/ad/archive/2014/11/18/microsoft-identity-manager-preview-release-1-is-now-available.aspx

APPENDIX

APPENDIX A – UNDERLAG TILL STANDARDISERAT GRUPP-API I PSEUDO-JAVA

Metod	Beskrivning:
createGroup(String parent, String groupName, int type)	Returnerar gruppens unika ID. Om det finns olika typer av grupper behöver vi ange vilken typ av grupp vi vill skapa. Parent kan vara en mapp eller en grupp.
deleteGroup(String groupName)	Gruppen ”groupName” tas bort. Operationen innebär att gruppen även tas bort ur alla grupper den är medlem i.
getGroupID(String groupName)	
Medlemsoperationer	
addGroupMember(String name , String groupName)	Gruppen “namn” blir medlem I gruppen “groupName”
addMember(String name, String groupName)	Personen “name” blir medlem I gruppen “groupName”
addMembers(List<String> groups, List<String> persons, String groupName)	Personer och grupper i listorna groups och persons blir medlemmar i gruppen “groupName”
isEmpty()	Returnerar true om gruppen saknar medlemmar
isMember(String groupName, String memberID)	Returnerar true om medlemmen finns I gruppen.
deleteMember(String groupName, String memberID)	Tar bort medlemmen memberID från groupName
getMembers(String groupName)	Returnerar lista med namn på alla direkta medlemmar (grupper och personer)
getAllMembers(String groupName)	Returnerar lista med namn på gruppens alla direkta och indirekta medlemmar (personer)

getMemberShips(String subjectID, String groupName)	Returnerar vilka grupper en grupp eller en person är medlem i
Administration av gruppen	
setGroupAdmin(String groupName, String subjectID)	GroupAdmin kan lägga till och ta bort medlemmar.
hasGroupAdmin(String groupName)	Returnerar true eller false
getGroupAdmin(String groupName)	Returnerar lista på gruppadmin
setGroupOwner(String groupName, String subjectID)	Ägaren av gruppen är huvudadmin och kan ändra allt som går att ändra samt ta bort gruppen.
hasGroupOwner(String groupName)	Returnerar true eller false
getGroupOwner(String groupName)	Returnerar lista på gruppägare (om systemet tillåter fler än en annars gruppägaren
Ändringar av grupp och medlemsprivilegier	
resetDeactivationDate(Date date, String groupName)	Sätter om gruppens inaktiveringsdatum
deactivateGroup(String groupName)	Sätter inaktiveringsdatum till idag alternativ sätter gruppens status till inaktiv om det är möjligt.
enablePrivilegeForAll(Privilege privilege)	Privilegier innebär här vad en medlem kan se och göra i gruppen. Privilege är tänkt som en Enum anpassat efter vad som går att sätta i grupphanteringsverktyget typ: Public enum Privilege { READ, WRITE, VIEW, OPT_IN osv ….}
disablePrivilegeForAll(Privilege privilege)	
enablePrivilegeForMember(String memberID, Privilege privilege)	
disablePrivilegeForMember(String memberID, Privilege privilege)	
Ändringar av gruppen och medlemmarnas egenskaper och regler	
setAttributeForGroup(Map<key,value>)	Den här biten kommer att behöva vara flexibel och designas utifrån aktuella behov och underliggande system och de möjligheter som finns. Det kan vara allt från finkorniga attribut och regler för ABAC till enklare enstaka attribut. Det specificeras därför inte vidare här.
setAttributeForMember(String memberID, Map<key, value>)	
deleteAttributeForGroup(Map<key,value>)	
deleteAttributeForMember(String memberID, Map<key,value>)	

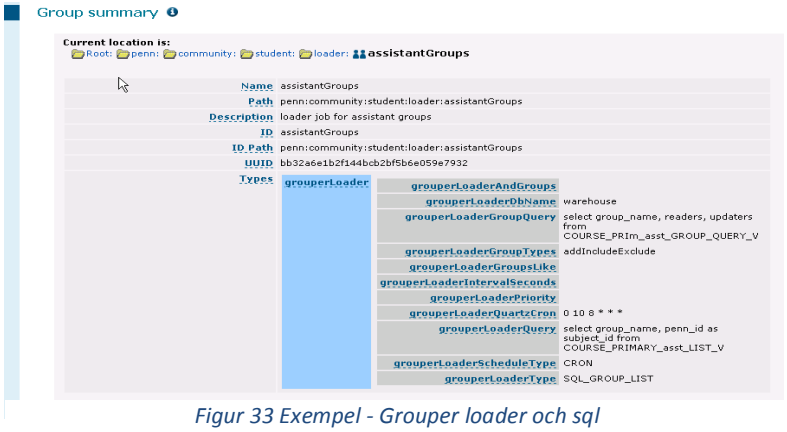
getAttributeForMember(String memberID)	Funktionen bör dock finnas.
getAttributeForGroup(String groupName)	
setRuleForGroup(Map<key,value>)	
setRuleForMember(String memberID ,Map<key,value>)	
deleteRuleForGroup(Map<key,value>)	
deleteRuleForMember(String memberID, Map<key,value>)	
Sammansatta Grupper	
createUnionGroup(String parentID, String nameOfUnionGroup, String nameOfFirstGroup, String nameOfSecondGroup)	Typ: If FirstGroup **OR** SecondGroup then newGroup
createIntersectionGroup(String parentID, String nameOfIntersectionGroup, String nameOfFirstGroup, String nameOfSecondGroup)	Typ: If FirstGroup **AND** SecondGroup then newGroup
createComplementGroup(String parentID, String nameOfComplementGroup, String nameOfFirstGroup, String nameOfSecondGroup)	Typ: if FirstGroup **AND NOT** SecondGroup then newGroup
deleteCompositeGroup(String groupName)	Tar bort alla typer av sammansatta grupper.
Administrativa Funktioner	
getGroupTypes()	
getAttributeTypes()	
getRules()	
getUser(userID)	
getUser(String name)	

APPENDIX B - INTEGRATIONSMÖJLIGHETER MED GROUPER INKLUSIVE HÄNVISNINGAR

Från SQL, LDAP eller AD till Grouper

Från SQL, LDAP och AD kan man använda Grouper Loader. Det finns även stöd för det via GUI:t.

Det kommer behövas konfiguration i till exempel sources.xml och grouper-loader.base.properties.



Figur 33 Exempel - Grouper loader och sql

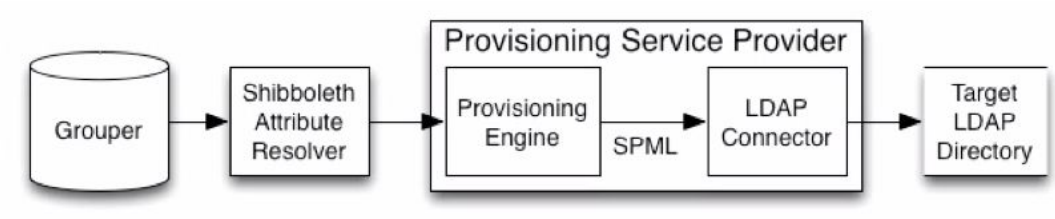
För mer info läs: https://spaces.internet2.edu/display/Grouper/Grouper+-+Loader+LDAP
Med gsh: https://spaces.internet2.edu/display/Grouper/Grouper+LDAP+GSH+example

Grouper API

Groupers API fungerar också att använda för integrationer från olika system. Förutom de installationsanvisningar och videoinstruktioner som finns på Groupers wiki hittar ni en som är lätt att följa här: https://iam.alaska.edu/grouper/wiki/GrouperInstall

Grouper till LDAP eller AD

Till LDAP används företrädesvis Groupers PSP som fungerar enligt nedan. Den använder alltså Shibboleths attribute resolver för att hämta data från Grouper till PSP:n.



Intressanta filer att konfigurera i sammanhanget är psp-services.xml eller psp-resolver.xml. För mer info läs: https://spaces.internet2.edu/display/Grouper/Grouper+Provisioning

Grouper till Shibboleth

Från och med Grouper version 2.1 så tillhandahåller Groupers Shibboleth Attribute resolver extensions för Data Connections och attributdefinitioner. Denna funktionalitet låg tidigare i Grouper API:t (från version 1.5). För integrationer med Shibboleth så rekommenderas man dock gå via PSP:n om man inte har väldigt speciella användningsfall.

För mer info läs: https://spaces.internet2.edu/display/Grouper/Grouper+Shibboleth+Integration

Grouper till WS-applikationer

WS-applikationer kan prata med Grouper direkt via WS-gränssnittet.

För mer info läs: https://spaces.internet2.edu/display/Grouper/Grouper+Web+Services

Grouper via VOOT och SCIM

VOOT är ett enkelt protokoll för att kunna få tillgång till att läsa information om en användares gruppmedlemsskap mellan domäner. Groupers VOOT connector är en jar-plugin för Groupers WS. Grouper har även stöd för att sända gruppinformation till SCIM-endpoints. Det är dock inte ett alternativ till Grouper Web Service och för närvarande behöver användarid:t i målsystemet matcha det ID subjektet eller entiteten har i Grouper för att det skall fungera.

För mer info läs: https://spaces.internet2.edu/display/Grouper/Grouper+SCIM+Integration
och https://spaces.internet2.edu/display/Grouper/Grouper+Voot+Connector

Grouper till ESB

Grouper har en ESB connector. Den är Groupers interface mot en ESB och skickar och tar emot händelser när förändringar sker. All konfiguration för ESB finns i grouper-loader.properties. Man kan ha multipla instanser av consumers och listeners förutsatt att portar och användarnamn etc är unika.

ESB connectorn introducerades i Grouper 1.6 och används idag i produktion men har ännu inte använts i så stor skala att de vill kalla den stabil. Den jackar in i changelog consumern. Den är medvetet designad som lightweight. För funktionalitet som saknas hänvisas man att använda web service istället. I Grouper version 2.2.1 som släpptes i november 2014 har man bland annat lagt till kryptering för ESB-meddelanden och stöd för SNS/SQS och AWS messaging.

För mer info läs: https://spaces.internet2.edu/display/Grouper/Grouper+ESB+Connector

Notifieringar

Grouper kan integrera med eller provisionera data till externa system i realtid när förändringar sker. Det görs via notifieringar baserade på Groupers change Log och kan ske via:

- PSP till LDAP, AD eller via SPML
- Grouper ESB connector eller XMPP
- Genom att implementera sin egen change log consumer i Java

Här följer ett exempel på konfig I grouper-loader för händelsedriven change notification

```
# grouper-loader.properties

changeLog.consumer.httpTestGroup.class =
edu.internet2.middleware.grouper.changeLog.esb.consumer.EsbConsumer
changeLog.consumer.httpTestGroup.publisher.class =
edu.internet2.middleware.grouper.changeLog.esb.consumer.EsbHttpPublisher
changeLog.consumer.httpTestGroup.publisher.url = http://server.utulsa.edu:4499/
changeLog.consumer.httpTestGroup.quartzCron = 48 * * * * ?
```

För mer info läs: https://spaces.internet2.edu/display/Grouper/Notifications+(change+log)

Grouper för nybörjare:

Presentation från University of Utah som går igenom hur du installerar och sätter upp Grouper och använder Grouper Loader för att hämta kursdeltagare och provisionera till AD samt lite specialgrejjer för just Grouper.

- Presentations-pdf: https://spaces.internet2.edu/download/attachments/14517786/Grouper-For-Beginners-BryanWooten-Apereo-June2014.pdf?version=1&modificationDate=1402062238953
- Video där du hör vad presentatören säger: http://www.youtube.com/watch?v=bGsi631WdFE
- Det finns massor med vidoes att följa för den som är ny till Grouper se: https://spaces.internet2.edu/display/groupertrain/Grouper+Training

Groupers Attribut

Groupers attribute framework används för att attacha metadata till olika objekt. Attribut kan tilldelas grupper, medlemskap, medlemmar, mappar, andra attribut och attribute assignments (en nivå ner). Attribut hanteras fortfarande via Gropuers Lite UI.

Du kan läsa mer om attribut här:
https://spaces.internet2.edu/display/Grouper/Grouper+attribute+framework

Bra Groupersidor:

Grouper: http://www.internet2.edu/products-services/trust-identity-middleware/grouper/
Grouper Training videos: https://spaces.internet2.edu/display/groupertrain/Grouper+Training
Grouper group and folder design ideas:
https://spaces.internet2.edu/display/Grouper/Group+and+folder+design+ideas