Arkitektur för identitet och behörighet ur ett lärosätesgemensamt perspektiv (IAM)

Projektplan
November 2016

Innehållsförteckning

Bakgrund och projektidé

Projektdirektivet: Arkitektur för identitet och behörighet ur ett lärosätesgemensamt perspektiv (IAM)

Projektet/utredningen ska utreda hur framtidsvisionerna ser ut kopplat till lärosätenas behov när det gäller gemensam arkitektur runt hantering av elektroniska identiteter och behörigheter (*Identity and Access Management* ***IAM***). Hur ser visionen ut och vilka steg kan genomföras lokalt för att nå detta?

Bakgrund

Hantering av elektroniska identiteter och behörigheter är centralt vid alla lärosäten. Hanteringen har växt fram i olika takt vid olika lärosäten, men i takt med att kraven på lärosäten ökar, framför allt vad gäller kostnadseffektivitet och möjlighet att använda IT-tjänster som ej driftas vid lärosätet, så ökar behoven om samsyn på frågorna kring identitetshantering inom sektorn.
Inom samarbetsorganet ATI har ett behov identifierats att inventera och göra en gemensam kravställning på hur IAM ska kunna komma att hanteras i ett framtidsperspektiv.

Utgångspunkt

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

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

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

- *Federationscentrisk* Den federationscentriska IAM-hanteringen handlar om att världen breddas och att e-identiteterna inte bara hanteras inom en organisation. Det innebär att det måste finnas ett förtroende mellan de olika ingående organisationerna i federationen. Att en organisation litar på tilldelningen av rättigheter som kommer med den hävdade rätten.
  Det är i SWAMID som vi har grunden till den federationscentriska IAM-hanteringen. Det saknas idag samsyn för hur behörighetsstyrning fungerar inom resp lärosäte och vilka krav som är rimliga att ställa där. Några basprocesser finns definierade inom ramen för SWAMIDs tillitsramverk men fokus för federationen är återanvändning av elektroniska identiteter för inloggning. Typexempel på detta område är de IT-tjänster som används genom olika former

av nationella samarbeten, t ex Adobe Connect, Box och kommande version av Ladok (Ladok3). Antagning.se och NyA-webben är också exempel inom området där vissa delar av NyA-webben även har behörighetsstyrning på detta sätt.

- *Användarcentrisk* När e-identiteten sätts i fokus och rättigheter inte längre tilldelas vid den enskilda organisation där e-identiteten ursprungligen hör hemma får vi ett användarcentriskt perspektiv. Tilldelningen flyttas ut ur organisationen till den sammanslutning där organisationen finns.
  För användarcentrisk IAM-hantering finns idag ingenting inom lärosätessverige även om SWAMID utgör en stark utgångspunkt. Som privatperson kommer man i kontakt med denna paradigm t ex genom konceptet att man använda ett Facebook-konto för inloggning i många IT-tjänster. I detta exempel saknas dock behörighetshanteringen.

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

Direktiv

Det projektet/utredningen syftar till att göra tydligt är hur en framtida IAM-hantering kan se ut för ett svensk lärosäte. Förändringar kommer att ske, däremot kanske förändringarna inte kommer att ske i ett steg utan genom en successiv förändring. Den organisationscentriska IAM-hanteringen har byggts upp baserat på krav där vi hanterar IT inom organisationen, mycket av IT kommer att både på kort och medellångt perspektiv att ske inom organisationerna, men hur ser det ut på lång sikt? Hur kan vi redan nu börja planera och skapa en IAM-hantering som är kompatibel med ett användarcentriskt paradigm för IAM och hur kan de olika paradigmen kopplas samman? Lärosätena kommer inom några år möta höjda krav på hanteringen av personuppgifter som också tydligt påverkar området identitetshantering.
De frågeställningar som projektet/utredningen tar sin utgångspunkt i är:

- Tre paradigm för IAM. Vilka delar ur resp. paradigm tillför mest för högskolesektorn?
- Vilka är de grundläggande gemensamma behoven kopplat till identiteter och behörigheter?
- Hur ser e-identiteters livscykel ut i ett framtidsperspektiv?
- Hur ser processen ut för tilldelning av åtkomst till IT-resurser?
- Hur ser en målarkitektur ut och vilka transitionsarkitekturer finns?

Mål

Huvudmålet med projektet/utredningen är att ta fram en vision för en lärosätesgemensam syn på arkitekturen runt IAM-hantering dvs. identiteter och behörigheter. Detta blir ett stöd för hur utvecklingen skall drivas framåt inom respektive lärosäten och vilka gemensamma delar som är nödvändiga.

Utredningen kommer att leverera följande leverabler

- Sammanställning av de processer som bör finnas dokumenterade vid resp lärosäte samt exempel på implementationer av processerna. Dessa processer inkluderar både de processerna som krävs för att uppfylla SWAMIDs tillitsramverk och övriga processerna anknutna till identitetshanteringen och innefattar bl a
    - Livscykelhantering av konto för olika kategorier av användare (anställda, studenter, övriga verksamma)
    - Identifieringsmetoder (hur säkerställer vi att individen är den den utger sig för att vara)
- Sammanställning av vilken ingående funktionalitet som är naturlig att implementera inom ramen för identitets- och behörighetshanteringen vid resp lärosäte. Sammanställning ska också tydliggöra vilka behov resp funktionalitet förväntas möta
- Sammanställning av vilken funktionalitet som är naturlig att implementera via gemensamma IT-tjänster för högskolesektor i Sverige inom ramen för SWAMID och vilka behov denna funktionalitet förväntas möta.
- Sammanställning av högskolesektorns krav på Svensk e-legitimation och vilket förhållande högskolesektorn kommer att ha till eIDAS för tydlig kanalisation via SWAMID
- Dokumenterade processer för hur behörighetsstyrning bör fungera inom resp. lärosäte och hur behörighetstilldelning för användare utanför lärosätet bör fungera

Sammantaget innebär detta att utredningen kommer att leverera en gemensam vision för identitets- och behörighetshantering, både för lokalt för resp. lärosäte och gemensamt för högskolesektorn genom samarbetet via SWAMID. Utredningen kommer också leverera en generell plan som kan användas för resp. lärosäte att hitta lämpliga sätt att ta sig till visionen.

Organisation

Projektledare
Fresia Pérez, Kungliga tekniska högskolan KTH, fresia@kth.se

Styrgrupp
Valter Nordh, Sveriges universitetsnät SUNET, valter@sunet.se
Stefan Edholm, Sveriges lantbruksuniversitet SLU, stefan.edholm@slu.se
Fredrik Nilsson, Riksidrottsuniversitetet GIH, fredrik.nilsson@gih.se
Johan Nordgren, Blekinge Tekniska Högskola BTH, johan.nordgren@bth.se
Ann Öhrn, Örebro universitet ORU, ann.ohrn@oru.se
Otto Ramirez, Försvarshögskolan FHS, otto.ramirez@fhs.se (reserv)

Uppdragsgivare
Per Hörnblad, projektkoordinator SUNET Inkubator, per.hornblad@umu.se

Arbetsgrupp
Markus Jardemalm, Uppsala universitet, markus.jardemalm@uadm.uu.se
Ola Ljungkrona, Chalmers, ola.ljungkrona@chalmers.se
Eskil Swahn, Lunds universitet, eskil.swahn@ldc.lu.se

Referensgrupp
Daniel Blomberg, Mälardalens högskola MDH, daniel.blomberg@mdh.se
Fredrik Jönsson, Kungliga tekniska högskolan KTH, fjo@kth.se
Johan Peterson, Linköpings universitet LIU, johan.peterson@liu.se
Mats Törnblom, Stockholms universitet SU, mats.tornblom@su.se

Projektet använder personer från ATI-gruppen som referens till arkitekturfrågor. Vid behov formas ytterligare referensgrupp.

Projektmetod

Projektets huvudmål är att ta fram en vision och en arkitektur över tjänster och processer.

Ett första utkast av vision och karta kommer att produceras av projektets arbetsgrupp via workshops. Utkastet kommer sedan presenteras för och diskuteras med olika intressenter och i olika fora.

Intressenter kommer att kartläggas genom en intressentanalys.

Intervjuer, både strukturerade och ostrukturerade, kommer att hållas för att samla in data. Datat kommer sedan analyseras och kommer slutligen ligga till grund för eventuella ändringar och kompletteringar.

Kommunikation och information

Projektets tidsplan och status kommer att kontinuerligt uppdateras och presenteras på webben under https://portal.nordu.net/display/Inkubator/IAM.

Kontinuerliga statusrapporter kommer att skickas till styrgrupp och uppdragsgivare.

Projektet och dess status kommer att presenteras under SUNET-dagarna 2017.

Budget

IAM projektet har en budget på 400 000 kr för 2017 men har kunnat påbörja projektet redan 2016 med mindre del av det årets Inkubatorbudget, 60 000 kr.
Budgeten ska framförallt täcka projektledningskostnader, därefter arbetsgruppens/expertgruppens kostnader. Ersättningen är 600 kr per timme.

Grov fördelning
Projektledning 200 000 kr
Expertgrupp: 130 000 kr
Resor: 70 000 kr

SUNET Inkubator
Arkitektur för identitet och behörighet ur ett lärosätesgemensamt perspektiv - Projektplan

Projektplan

IAM

14 okt 2016 - 31 dec 2017

projectplace