SUNET Inkubator – Verksamhetsplan för 2017

Referenser

[1] https://portal.nordu.net/display/Inkubator/Projekt

Definitioner

ATI	**Arbetsgruppen för Teknisk Integration** är ett Nationellt nätverk inom högre utbildning rörande arkitektur och systemintegrationer
BI	**Business intelligence**, är ett samlingsbegrepp för färdigheter, tekniker, applikationer, processer och metoder för organisationer att bättre förstå sin verksamhet och sin omvärld
IAM	**Identity and Access Management**, disciplin som hanterar elektroniska identiteter och behörighetsstyrning
IoT	**Internet of Things**, är ett nätverk av fysiska enheter t.ex. fordon, byggnader, mätinstrument etc. som är nätverksanslutna och gör det möjligt för dessa enheter att samla in och utbyta data.
IRT	**Incident Responce Team,** funktion som hanterar säkerhetshot mot en organisation
IPS	**Intrusion Prevention System**, monitorerar och detekterar misstänkta aktiviteter i IT system och nätinfrastruktur
Ladok	Lärosätes gemensamma system för att hantera studiedokumentation.
NGFW	**Next generation firewall** – Inspekterar nät-trafiken djupare än traditionella brandväggar för att hitta kända sårbarheter, virus och malware.
NyA	Lärosätesgemensamt antagningssystem
PaaS	**Platform as a Service,** är en typ av molntjänst som tillhandahåller en datorplattform och en uppsättning programvarusystem som en tjänst.
REST	**Representational State Transfer**, kommunikationsmetod som bygger på Hypertext Transfer Protocol
SWAMID	**Swedish Academic Identity Federation**, identitetsfederation som omfattar de flesta lärosäten och övriga myndigheter som är relaterade till svensk forsknings- och utbildningssektor.
U/H	**Universitet och högskolor**

Introduktion

Umeå universitet har i en överenskommelse med SUNET åtagit sig uppdraget att driva e-infrastrukturfrågor i svenska högskolan. Det har tidigare gjorts inom verksamheten SWAMI, som i sin tur startat SWAMID. Från och med 2013 bytte SWAMI namn till ***SUNET Inkubator*** och skiljdes organisatoriskt från SWAMID.

Samarbete mellan lärosäten spelar en viktig roll i utvecklingen av den svenska högskolan genom att

detta stödjer samordning och utveckling av e-infrastrukturen samt hjälper till att fram dokumenterade rekommendationer som är anpassade till svenska förhållanden. SUNET Inkubator skall vara en grund för att kunna utveckla ett effektivt samarbete mellan lärosäten.

Grunden för SUNET Inkubator skall ligga i följande:

- Ge generellt stöd kopplat till samarbete inom e-infrastruktur och IT. Initiera, organisera och driva samarbetsforum inom viktiga e-infrastrukturområden.
- Vara en facilitator och stödja lärosätena i dagliga men viktiga frågor inom e-infrastruktur.
- Hjälpa lärosätena att ta vara på varandras erfarenheter och därmed ge förutsättningar för att skapa bättre lokala lösningar.
- Vara en inkubator när det gäller att utveckla nya idéer och tankar runt e-infrastruktur i den svenska högskolan.
- Driva en samsyn och skapa rekommendationer när det gäller e-infrastrukturfrågor.
- Driva en informations- och kommunikationsverksamhet i viktiga frågor kopplat till e-infrastruktur för svenska lärosäten.
- Driva kompetensutveckling genom att samverka i olika internationella forum och konferenser.

Ersättning för uppdrag inom SUNET Inkubator är 600 kr per timme.

Budget

1. SUNETs föreståndare fastställer budget för Inkubator i budgetprocessen för SUNET.
2. Inkubators styrgrupp, som består av 2 personer från högskolorna, 2 personer från universiteten och en person för SUNET tar fram behov och förslag på de aktiviteter som skall genomföras.
3. Dessa förslag kommuniceras på SUNETs strategidagar.

Process för att hantera projektförslag

Inkubator kan driva ett antal fasta projekt som är en del av årsplanen. Inkommande förslag skall planeras löpande och en ev. omprioritering av pågående projekt kan ske till förmån för aktiviteter som anses vara viktiga. Förslag kan skickas till inkubatorforslag@sunet.se.

Följande aktiviteter sker under året.

- Löpande:
    - Kommunikation med olika forum och epostlistor för att uppmana till att projektförslag kommer in.
    - Styrgruppen
        - Kallas samma för löpande prioritering av inkomna förslag.
        - Planerar löpande in prioriterade miniprojekt/tester som ryms inom budget.
        - Väger löpande pågående projekt mot inkomna projekt om det är något som skall prioriteras högre och man får pausa ett pågående projekt.
- Q1: Start av planerade större projekt
- Q2: Kommunicera/förankra omprioriteringar på vårens strategidagar.

- Q3:
  - Styrgruppen planerar in större projekt inför ett budgetår samt avsätter en summa för miniprojekt/tester.
  - Förankra större projekt på höstens strategidagar.
- Q4 :
  - Planering av kommande projekt
  - Ev. start av projekt inför nästa år om det ryms i budget.
  - Avslut av planerade projekt

Sammanfattning av 2016

SUNET Inkubator har under 2016 drivit projekten Gemensamma integrationsplattformar iPaas, Administration av mobiler och datorer med Microsofts verktyg i molnet samt Stadsplan för lärosäten. Projekten har jobbat med refererensgrupper med representanter från ett antal lärosäten. Resultaten från projekten kommer att presenteras i separata slutrapporter/wikisidor för respektive projekt se ref. [1].

SUNET Inkubator har under 2016 fortsatt att driva aktiviteter för Arbetsgruppen för Teknisk Integration som består av deltagare från ett antal lärosäten. Samarbetet är nu väl etablerat och har lyft sektorn när det gäller IT-arkitektur och integrationsfrågor. ATI Task Force med representanter från 7 lärosäten jobbar konkret med olika frågor inom området. Under året har gruppen jobbat intensivt med Ladok3 integrationer där mindre arbetsgrupper har jobbar med användningsfall för integration. Detta användningsfall har används av Ladok3 projektet för att beskriva hur de åstadkoms med befintliga REST tjänster. Andra områden som gruppen har jobbat med är erfarenhetsutbyte, säkerhet i arkitektur, integrationskatalog, arkitektur bedömningar, masterdata samt IAM-området. Fyra fysiska möten och ett antal online möten har anordnats kopplat till ATI. Samarbetet med motsvarande gruppering för universitet i Finland har vidareutvecklats och ett gemensamt möte kommer att hålls i slutet av 2016.

Samarbetet rörande deloyment och Windowsplattformen har fortsatt under 2016. Två möten kopplade till samarbetet skall genomföras under 2016 med inbjudna experter där även lärosäten delat med sig av sina erfarenheter kopplat till SCCM, Windows 10 och Molnet. Ytterligare ett möte med fokus på molnet och Azure har genomförts strax före sommaren.

Under 2016 har två konferenser arrangerats (i samarbete med Ladokkonsortiet) under SUNET-dagarna i Kristianstad respektive Borås.

Aktiviteter och projekt 2017

Verksamhetsdelen kan delas upp i basverksamhet och projektverksamhet. Basverksamheten består av övergripande ledning, koordinering och kommunikationsverksamhet samt drivande av samarbetsforum och samverkan.

- Samarbetsforum

- Driva olika typer av samarbete mellan lärosäten samt vara en facilitator för samarbete och därmed effektivisera arbetet inom e-infrastruktur.
- Driva Ladok-Inkubatordagar i samband med SUNET-dagar.
- Windowssamarbete: Under 2017 fortsätter Windowssamarbetet som en del i projektet samarbetsprojektet *Molnlösningar för U/H*.
- IT-arkitektur och teknisk integration: Under 2017 fortsätter samarbetsaktiviteter inom området IT-arkitektur och teknisk integration. Detta innebär ett fortsatt samarbete med ATI – som är ett nationellt nätverk för arkitektur och teknisk integration. Här pågår ett arbete med att ta fram en samsyn inom arkitekturområdet samt att arbeta med gemensamma riktlinjer och rekommendationer. Ett antal workshops anordnas. Den interna gruppen ATI Task Force som jobbar konkret med olika delar i den gemensamma referensarkitekturen understöds samt integration med nya Ladok är ett fortsatt fokusområde. En specifik plan tas fram för ATI men några exempel på aktiviteter listas nedan:
  - Fortsatta leveranser kring integrationsarkitekturen i Ladok3
  - Säkerhetsarbete inom arkitektur
  - Erfarenhetsutbyte inom aktuella områden
  - Masterdatahantering
  - Informationsmodeller
  - Fortsatta leveranser kopplat till referensarkitekturen
  - Arkitekturgranskningar på lokala lärosäten
  - Workshops inom nätverket kopplat till dokumentation och modeller av lokal arkitektur.
  - Ta fram gemensamma rekommendationer att jobba med arkitektur lokalt.
  - Vidareutveckla samarbetet med peers (Finland)

- Samverkan
  - SUNET Inkubator verkar i ett internationellt sammanhang där utbyte av erfarenheter är nödvändigt för att minska dubbelarbete. Vi är inte ensamma om de problem och möjligheter som finns och vi bör vara en god aktör i samarbetet med andra organisationer. Exempel på organisationer och nätverk som SUNET Inkubator kan verka inom är t.ex. TERENA, Gartner etc. Det kan även handla om nätverk inom arkitekturområdet som t.ex. SWEAN, eller konferenser inom arkitekturområdet som t.ex. EAC. För windowssamarbetet kan det även handla om konferenser som t.ex. Microsoft Ignite.
- Projekt
  - Arkitektur för identitet och behörighet ur ett lärosätesgemensamt perspektiv (IAM)
  - Säkerhet - utökat skydd
  - Platform as a Service/Intelligent Cloud - Molnlösningar för U/H

Ambitionen är att de projekt som genomförs i SUNET Inkubator skall ha tillgång till en expertgrupp med medlemmar från olika lärosäten inom de områden som projekten verkar.

Nedan beskrivs projekten för 2017.

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

Sammanfattning

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 att ta sig till visionen.

Organisation

En projektledare utses som ansvarar för att ta fram en projektplan och att strukturera upp arbetet. En referensgrupp skapas som ger input till projektet.

Utredningen bör få en bred samsyn kring frågeställningarna och representanter för följande intressenter bör finnas som aktiva deltagare:

- Lärosätesrepresentanter
- SWAMID
- UHR

Säkerhet - utökat skydd

Sammanfattning

Projekt utreder möjligheten till att öka skyddet på lärosäten genom att använda sig av *Nästa generations brandväggar (Next Generation FireWall)* och *System för intrångsskydd (Intrusion Prevention System).*

Bakgrund

Säkerhetsfrågor inom IT-området har blivit allt viktigare för svenska lärosäten då dataintrången ökar kraftigt. Idag ser vi betydligt mer av sofistikerade attacker och avancerade hot mot våra informationstillgångar vilket i sin tur gör det svårt eller omöjligt att hantera detta med traditionell teknik. Idag finns det ett starkt behov av sofistikerade och automatiserade tekniska lösningar för att möta hoten. Kostnaden för traditionella metoder att bemöta dessa hot är kraftigt ökande vilket är ett starkt incitament för att ett bättre stöd måste implementeras.

Direktiv

Projektet utreder två delar inom säkerhetsområdet d.v.s. *Nästa generations brandväggar* samt *System för intrångsskydd.*

Allmäna frågeställningar

- Vad sparar vi budgetmässigt på att införa ovanstående lösningar?
- Vilka aktuella produkter finns på marknaden som kan vara lämpliga att använda?
- Hur ser produkternas uppdateringar ut? Det krävs att produkterna får sin information om skadlig kod och säkerhetshot från de flesta tidszoner för att fungera tillfredställande.

Nästa generation brandväggar

- Vad ger *nästa generations brandväggar* för effektivitets vinster?
- Att börja i liten skala och sedan expandera, vad ska man tänka på och ta i hänsyn vid ett sådant införande?
- Redundans?
- Kompabilitet mot nätinfrastruktur?
- Inom vilka områden ser man administrativa vinster?
- Ökning av administrativa/löpande kostnader?

- Administrationsgränssnitt och behörighetsnivåer (Nät, IRT, Support)

System för intrångsskydd

- Äldre IPS krävde mycket administration och underhåll, hur ser det ut idag?
- Hur kan man koppla ISP funktioner mot befintlig infrastruktur (övervakning, loggning mm.)
- Hur ser ett rekommenderat införande ut?
- Redundans?

Mål

Huvudmålet med projektet är att ta fram rekommendationer kring *Nästa generations brandväggar* samt *System för intrångsskydd*. Här är det viktigt att projektet kan visa på de vinster och extra kostnader det medför att implementera någon av dessa lösningar. Projektet skall även visa på skillnaden och likheter mellan dessa tekniska lösningar.

Projektet utvärderar olika produkter som implementerar de olika teknisk lösningarna och gör en jämförelse och rekommendation kopplat till dom olika produkterna.

Organisation

Projektledare utses som ansvarar för att ta fram en projektplan.

En referensgrupp skapas som kan ge input till projektet.

Platform as a Service/Intelligent Cloud - Molnlösningar för U/H

Sammanfattning

Projektet samordnar erfarenhetsutbyte mellan lärosäten inom området molnbaserade lösningar samt tittar djupare på för U/H intressanta lösningar som erbjuds genom Plattform as a service (PaaS) från de tre stora leverantörerna Microsoft, Amazon och Google. Hybridlösningar och Intelligent Cloud bl.a. kopplat till forskningsstöd ligger i fokus.

Bakgrund

Många lärosäten tittar i dag på olika möjliga molnlösningar och det finns lösningar från flera lärosäten som är driftsatta i Microsoft Azure. Microsoft och andra molnleverantörer levererar många PaaS tjänster som är intressanta för U/H. Hybridscenarion d.v.s. lokala tekniklösningar som integreras med PaaS lösningar i molnet blir allt mer intressanta eftersom många kommer att leva med lokala lösningen inom överskådlig tid. Genom ett hybridsenario så kan lokala lösningar effektiviseras samt det underlättar en senare övergång till en molnlösning. Inom *Identity Management - IdM* området så kan ett exempel på hybridscenario vara användandet av Microsoft Azure AD Connect som möjliggör ett lokalt AD men ger ändå tillgång till att utnyttja kraftfulla funktioner i Azure AD som MultiFactor Authentication MFA, Advanced Threath Protecton etc.

Förutom *IdM* området så finns en mängd andra intressanta PaaS tjänster för att hantera t.ex. cachning , process automation, notifikationer, köer , ServiceBus, Service Fabrics, IoT, BI, Machine Learning, Data Lakes, Recovery och mycket mer. I detta finns delar som är speciellt intressanta kopplat till forskningsstöd som t.ex. BI och Machine Learning etc.

Direktiv

Projektet skall visa på de möjligheter som olika typer av PaaS ger samt främja erfarenhetsutbyte inom området mellan lärosäten. Projektets referensgrupp riktar in projektet på de delar som är mest intressanta ur ett U/H perspektiv. Projektet berör även lösningar som är intressanta ur ett forskarstödsperspektiv t.ex. BI och Machine Learning (kan bl.a. användas för olika typer av adaptiva system).

Projektet inventerar även de befintliga lösningar som finns inom U/H och jobbar med webinarier, enkäter och intervjuer för att sprida information samt för att främja erfarenhetsutbyte.

Mål

Huvudmålet med projektet är att främja erfarenhetsutbyte inom U/H inom området molntjänster/PaaS och visa på möjliga lösningar och effektiviseringar som kan göras genom att utnyttja denna typen av tjänster. Vidare skall projektet peka på för U/H intressanta PaaS tjänster och hur dessa kan användas ur ett lärosäterperspektiv. Tjänster för forskningsstöd är av speciellt intresse.

Organisation

Projektledare utses som ansvarar för att ta fram en projektplan.

En referensgrupp skapas som kan ge input till projektet vilka delar som är mest intressantast att utreda.

Budget

Område	Aktiviteter	Budget (kr)
Ledning, kommunikation och information.	Övergripande projektledning och koordinering, hantering av projektförslag, uppstart av projekt, resurssättning, Inkubator presentationer, Ladok-Inkubatordagar, koordinering workshops etc. Budget för resor etc. inkl. viss reserv för projekten.	300 000
Samarbetsforum	Windows samarbete (säkerhet, deployment, etc). Samarbetet blir detta år en del av projektet *Molnlösningar för U/H.* Budget för eventuella aktiviteter tas från projektbudgeten.	
Arkitektur och Teknisk Integration	Budget till gemensamma möten och föreläsare. Budget för vidare arbete inom ATI Task Force som fördelas på 7 inblandade lärosäten. Under året genomförs ett antal prioriterade aktiviteter som ryms inom budget.	350 000
Samverkan	Div. forum och konferenser	40 000
Oplanerade projekt och tester		50 000

Arkitektur för identitet och behörighet ur ett lärosätesgemensamt perspektiv (IAM)	Se projektbeskrivning.	400 000
Säkerhet - utökat skydd	Se projektbeskrivning.	370 000
Molnlösningar för U/H	Se projektbeskrivning. *En minimal version av projektet utförs då budgeten är begränsad.* Fokus på informationsspridning och erfarenhetsutbyte mellan lärosäten.	90 000
Summa		**1 600 000**

Fakturering till SUNET sker kvartalsvis.

Fastställd av SUNET, oktober 2016

Valter Nordh