

# Referat Cerebrum-seminar 2019

[usit.uio.no/om/tjenestegrupper/cerebrum/seminar/2019/](https://usit.uio.no/om/tjenestegrupper/cerebrum/seminar/2019/)

Referent: [Andreas Ellewsen](#)

Torsdag 25. april

10:30, Åpning og velkomst, Hans Kristian Fjeld og Joakim Hovlandsvåg

Joakim åpner. Ønsker velkommen. 3 år siden siste seminar. Formålet med seminaret å bli mer kjent, og få prata sammen.

Hans Kristian. UH-IAM får konsekvenser for Cerebrum, derfor en del fokus på det. Tidligste avvikling av Cerebrum 2025. Migrasjonen vil kreve stor innsats. Kort info om hva vi skal få høre om de neste to dagene. Sykdomsfrfall i morgen. Blir byttet ut med info om FS-API-et av Pål Erik Megaard. Presentasjonene vil bli lagt ut i ettertid. Oppfordrer til å stille spørsmål og diskusjon. Kunne stille spørsmål anonymt i nettskjema hvis man ville. Fikk en kort intro av hvem alle er.

10:45, Veikart for Cerebrum. UiO presenterer planer og prioriteringer for de nærmeste årene., Hans Kristian Fjeld, tjenesteeier av Cerebrum på UiO

Prøvd litt forskjellige ting for veikart. Mest fokus på nærmeste tiden. Jobber smidig. Prøvd litt forskjellig. Veikartet finnes på en nettside, men få har sett det. Ting endres for fort til at vi rekker å holde det oppdatert på en god måte. Bruker Jira, men det kan ikke være offentlig tilgjengelig. Prøver å fokusere på høydepunktene.

Deltok i RFI i UH-IAM prosjektet. Var viktig med veikart der også.

Vår 2019:

UiT Cerebrum. UiT migrasjonen skal være ferdig 15.juni.

Passordtjenester for HiØ, UiA og UiT

Ansattautomatikk.

Høst 2019:

Forbedringer i tilgangsstyring (BOTT-ØL). Handler om å klargjøre Cerebrum for integrasjon med tjenester fra BOTT-ØL prosjektet.

Passordtjenester NiH.

Forbedret revisjonslogging. Håper å bli ferdig i løpet av året.

Pybofh. Håper å bli ferdig i løpet av året.

Vår 2020:

Python3. Python2 har end of life i 2019. Dette inkluderer sikkerhetsoppdateringer.

ID-porten. Ikke en veldig stor jobb, men viktig.

BOTT-ØL (DFØ) integrasjon.

Høst 2020:

FS-API. Bruker i dag en databaseintegrasjon, og vi ser det som en nødvendighet å bytte den ut. Har erfaring med det fra Canvas integrasjonen vi fullførte nylig.

Studentautomatikk.

Etter 2020:

For stor usikkerhet til å ha noe mer klart enn disse punktene siden det er store endringer for oss i tiden fremover.

UH-IAM?

UH-IntArk?

BOTT-ØL?

BOTT-SA?

Tidligere hatt fokus på langsiktig investering i Cerebrum. Nå blir ikke det like høyt prioritert siden vi på sikt skal bytte ut Cerebrum.

Ba om innspill til hva som bør tas med i veikartet, og hva som bør være fokuset.

Spørsmål:

Fra salen: Konkrete tiltak visjon policy.

HK: Veldig forskjellig hvordan man praktiserer veikart, gylden middelvei.

Fra salen: Har noen eksempler på gode veikart?

HK: Ikke funnet eksempler man kan kopiere, men tips gjerne om man vet om noen.

11:00, Prosjekt UH-IAM. Prosjekt UH-IAM skal kjøpe inn og innføre en IGA-løsning for Universitetet i Bergen, som deretter skal brukes av hele UH-sektoren. Uninett kommer og forteller om prosjektet og kva konsekvenser det har for oss i UH-sektoren. Prosjektet ønska ha med flere for å kunne svare også på tekniske spørsmål, men grunna nært forestående frister (utsending av RFP) har prosjektet det dessverre altfor travelt til å kunne sende flere., Hildegunn Vada, Uninett

Takket for invitasjon. Leder avdelingen som er ansvarlig for Feide og felles IAM. Veldig interessert i spørsmål om UH-IAM-prosjektet for videre planlegging.

Fortalte om nåsituasjonen per 2017 i BOTT. Mye manuelt arbeid. Liten bruk av rollebasert tilgangsstyring. Liten oversikt over hvem som har tilgang til hva. Revisjon av logger er tidkrevende. ++

Dette fører til noen utfordringer. Sikkerhetsmessige, Juridiske og Operasjonelle.

Man må vite hvem som har tilgang til hva og når de hadde tilgang til det. Enda mer aktuelt nå med tanke på GDPR. Personopplysninger blir lagret flere steder, og det er uklart hvem som har ansvaret for dem.

Gevinster: Bedre samhandling mellom institusjonene. Studentmobilitet (ta fag fra flere institusjoner uten problem). Øke bruken av fellestjenester og dermed oppnå mer standardisering. Økt sikkerhet. ++

Er nå i Fase 2 (Anskaffelse og pilotering) av 3 i prosjektet. UNIT har sagt at sektoren skal være med å bestemme, og dette skjer i Digitaliseringsstyret. De bestemte 28.01.2019 at sektoren skal ha felles IAM. Dette nye IAM-et piloteres av UiB, og Fase2 avsluttes 01.07.2020. Etter dette får man utrulling til resten av sektoren.

Fra salen: Når forventer man at fase 3 er ferdig?

Hildegunn: Forventer en 5-års periode.

Prosjekt mål: Innen 01.07.2020 skal prosjektet anskaffe, pilotere og etablere en felles IAM-løsning for UH-sektoren.

Bergen bruker per i dag et system som heter Zebra. Den nye løsningen vil ikke ta over fullstendig for Zebra til å begynne med. Målet for den nye løsningen er ikke å ta over alle drift fra starten av.

Fortalte om organiseringen av prosjektet.

Felles IAM. Starter med nytt IGA+Feide. Aktuelt å ta inn flere ting etterhvert.

Markedsundersøkelse: Mange leverandører svarte. Erfaring med offentlig sektor. Prismodellene er ganske like. Vært opptatt av at man kan få tak i et godt produkt utenfor sektoren, og man ser ikke et strategisk behov/verdi for at sektoren skal lage dette selv.

Fortalte om hva som er spesielt med UH-sektoren, og hva slags løsning man er på jakt etter. Legger vekt på brukervennlighet, automatisering, analyse og rapportering.

Stor risiko i prosjektet.

Man ønsker også å komme inn på den samme DFØ-løsningen.

Info om hvordan Felles IAM vil påvirke oss. Være forberedt på at dette kommer til å skje. Skal lære av UiB-piloten. Tempo og rekkefølge er ikke klar. Ta gjerne kontakt om man har ønsker.

Utvikling av Feide fremover: Nesten 300 tjenesteleverandører med 600 tjenester. Feide 2.0 (Dataporten+gamle Feide) kom i høst. Deling av data i en API-Gatekeeper. Ny grafisk profil og nettside. Nytt avtaleverk. Går over til godkjenning av bruksvilkår. Ny innlogging i løpet av sommeren. Jobber med innloggingsmetoder for internasjonale brukere. Innlogging med Europeisk eID fungerer. eduGain. Innlogging med ID-Porten, Facebook, LinkedIn. Ser på Orchid.

Skal gå fra halvårlig release til CI/CD. 2-faktor identifikasjon.

Fornyelse av kundeportalen.

Spørsmål:

Fra salen: Vil domenet til dataporten endre seg?

Hildegunn: Ikke planlagt så langt. Skal kommuniseres godt om det blir tilfellet.

Fra salen: Har man tenkt noe på Feide og dette nye IGA systemet?

H: Feide og nytt IGA må spille godt sammen.

Fra salen: Du sa tidligere at Cerebrum ble valgt bort, fordi det var mange andre gode produkter. Kan man ikke da ende opp med en dårligere løsning enn Cerebrum? Hvorfor ble det da gjort på denne måten (at Cerebrum ikke lenger er med i vurderingen)?

H: Konkurranselovgivning. Hvis UiO skulle kunne svart på tilbudet ville det vært med noen lover.

11:30, UH-IAM - konsekvens for Cerebrum. UiO presenterer hvordan de forholder seg til UH-IAM, og sine tanker om vegen videre., Hans Kristian Fjeld

Ikke enig i beslutningen til UH-IAM-prosjektet. Tror Cerebrum ville vært en billigere og bedre løsning enn det vi nå vil få på sikt. Men forholder oss selvfølgelig til den beslutningen som ble tatt og jobber videre ut ifra det.

Forholder seg til tidslinjen:

2019 RFP 2020 Pilot UiB 2021 Utrulling BOTT 2022 Utrulling resten av sektor 2025.

Hentet fra handlingsplan or digitaliseringsstrategien i UH sektoren.

Cerebrum For UH: normal operasjon 2022 Transisjonsløsning 2025

Cerebrum BOTT: Normal operasjon 2021 Transisjonsløsning 2023

Tenker at man vil måtte kjøre Cerebrum til og med 2025.

Tidslinjer:

BOTT-ØL (DFØ) 2019 UiO og UiB 2021 NTNU og UiT 2022

UH: IAM 2019 RFP 2020 Pilot UiB 2021 Utrulling Bott 2022 Utrulling resten av sektor 2025

Risiko å integrere mot ett nytt IGA som fortsatt er i pilot.

Tett kobling mellom HR-data i DFØ tjenester og IGA. Begge inngår i IAM. Starter onboarding i DFØ sine tjenester.

Har ikke fått til roller i tilgangsstyring tidligere. Må jobbe med IAM-prosesser i BOTT-ØL prosjektet.

IGA og HR-systemer er viktige. Viste hvordan de store prosjektene henger sammen med IAM og tilgangsstyring. Målet er å få masse roller i SAP som er brukbar til tilgangsstyring. Roller i bred forstand.

Vi bruker en del slik rolledata, men det har ikke vært godt nok, og dermed har tilgangsstyring skjedd i sluttbrukersystemet. Har dermed løst autentisering, men ikke autorisasjon.

Roller propagerer inn i IGA, men roller er ikke i seg selv en tilgang, men vi bruker det til å autorisere tilgang. IGA-et er autorativt for tilganger.

Beste praksis innen IAM.

Eksempel på hvorfor:

Har en person som jobber og er ansatt og har tilgang til et økonomisystem, og har rollen direktør. Har tilgang til diverse med det. Gjør noe som ikke er bra. Vil så låse ut denne personen. Men vi vil ikke nødvendigvis endre på rollen hans (han er fortsatt direktør). Det er altså ikke et en til en forhold mellom roller og tilganger.

Kort info om hva vi vet:

Ser for oss at migrasjonen blir en stor jobb.

De to første årene videre er viet til nødvendige sikkerhetsoppdateringer og kobling med DFØ.

Stor respekt for prosjektmedlemmene i IAM prosjektet, men synes de har fått feil mandat. Tenker ikke at gevinstene ligger i å innføre nytt IGA.

Få av punktene fra forprosjektet er videreført til UH-IAM. Legger vekt på at felles IGA er punkt nr. 18. på listen over ting man bør ta tak i. Prosesser lenge før.

Oppsummering:

Fokus på stabilitet og sikkerhet.

Lite endring neste to år.

Cerebrum er IGA for BOTT-ØL.

Begynne å klargjøre for avvikling mot 2025. Må begynne å planlegges lang tid i forveien.

Økt bemanning i migrasjonsperioden.

Avvente anskaffelse og UiB pilot (Kostnad, Gevinst)

13:00, FKS-konsortiet sin tilnærming til UH-IAM. FKS-samarbeidet forvalter ei IGA-løysing for mange i UH-sektoren. De forteller om korleis de forholder seg til UH-IAM., Odd Kristian Lundby, Høgskolen i Innlandet

Konsortiet startet i 2005. Består av USN, UIS, HINN, HVO, UNIS.

Parallelt løp med fokus på å videreutvikle dagens løsning. Må løse dagens utfordringer i dag. Startet Livssyklusprosjektet. Den mentale forberedelsen.

Søkt å få direkte medvirkning i UH-IAM prosjektet.

Med videreutvikling av dagens løsning har vi fått ny supportleverandør/konsulentavtale.

Jobber i 2019 med GDPR. Må gjøre en del ting med vår ID løsning. tar vare på for mye informasjon, for lenge. Håper å kunne få en løsning som gir de mulighet til å gi folk all informasjon de har lagret om dem.

Jobber også med FS-API-et samt opprydding i koden sin.

FS-API:

2 institusjoner bruker FS-WS SOAP. Sliter med denne til tider.

2 institusjoner bruker FS-WS REST. Har gått over pga. problemer med SOAP versjonen.

Skal lage ny konektor til nytt FS-API.

Planen å gå over til det til høsten.

Svalbard bruker ikke FS.

Livssyklusprosjektet:

- Slitt med at onboardingprosessen er dysfunksjonell. Folk kommer ikke inn eller ut av systemet på riktig tidspunkt. Spesielt perifere ansatte.
- Prosjektet skal være teknologi agnostisk. Inkluderer IT, HR og studie.
- OsloMet, Nord, HVL, HiMolde.
- Stort fokus på prosessbiten.

UH: IAM medvirkning:

Har i FKS konsortiet en løsning med god funksjonalitet og vil ikke ha noe dårligere. Forberedt på at det blir annerledes, men må være like bra eller bedre enn dagens løsning. Vil ha bedre rapportering enn de har i dag.

Har en representant i styringsgruppa.

Spørsmål:

Hans Kristian: Vet vi noe om hvem som vil levere på anbudet?

OK: Sannsynligvis konsulenter og partnere som gjør det for dem. De store selskapene leverer vanligvis ikke slikt selv, men gjennom partnere.

Hans Kristian: Livssyklusprosjektet. Sa du noe om hvor langt dere har kommet eller når det er ferdig?

OK: Nei. Trår litt vannet for øyeblikket. En del rammevilkår å ta hensyn til. Kommer litt an på om det blir kjørt i gang noe felles. Vi jobber, men vi har ingen konkrete milepæler på det. Uklart siden det er uklart hva som skjer i resten av sektoren.

Hildegunn: Hører hva dere sier, og ser hvor nyttig diskusjonene med BOTT er nå. Enig i at man ikke kan tro at man bare kan kjøpe inn en IAM-løsning og at dette løser alle problemer. Opplever at de har et godt samarbeid med BOTT-ØL.

OK: En annen bekymring vi har sett er at det fokuserer mindre på HR biten og mer på lønn og økonomi. Ender man opp med et tredje system?

(ref.anm: Folk snakker fort så det mangler en del her)

13:15, Paneldebatt om UH-IAM. Prosjekt UH-IAM er sentralt for alle på seminaret, og vi veit at mange har spørsmål. Prosjektet er positive til en god dialog om prosjektet. Vi prøver ha det som en paneldebatt. Panelet vert UH-IAM-prosjektet, UiO, og andre, som svarer på spørsmål fra salen. Send inn spørsmål til panelet. Du kan være anonym om du vil det., Hildegunn Vada, Uninett, Hans Kristian Fjeld, UiO, Odd Kristian Lundby, FKS-samarbeidet, Joakim Hovlandsvåg er ordstyrer

Hvordan ser dere helst for dere at arbeidet for å standardisere arbeidet i sektoren bør gjøres? Ideelt sett. Hvem, hvordan og når?

HK: Var inne på det. Ønsker meg at burde vært del av UH-IAM-prosjektet. Burde hatt tette forbindelser til Økonomi og lønn (BOTT-ØL).

Hildegunn: Var innoem det i sted. Erfaringen er at det er vanskelig å få alle til å gå i samme retning. Det er godt samarbeid i sektoren, men denne typen prosesser tar typisk lang tid.

OK: Eneste realistiske mulighet er at det blir styrt sentralt.

HK: Planen var å opprette et IAM-program som skulle jobbe med dette. Håper det skjer der hvis ikke UH-IAM tar det. Forvaltningsorganiseringen bør være iterativ.

H: Trenger innspill. Sektoren trenger at vi prøver å samarbeide.

Hvordan løses migrasjon fra gammelt til nytt IGA ved hver virksomhet?

H: I Bergen tenker man at det nye IGA-et skal koble til to kildesystemer (Ny SAP og FS) og dette skal sluses inn i Zebra. Kanskje Noen målsystemer som kobles løs fra Zebra og på det nye IGA-et. Ikke bruke mye tid på kobling i starten og heller få i gang rapportering tidlig.

Fra salen: Egentlig trenger man ikke bruke den gamle IGA-en. Det bør ikke være noe problem å bytte ut en IGA. Man skal bare ha det samme inn og omtrent det samme ut.

H: I praksis er ikke dette så enkelt.

HK: Som leverandør av Cerebrum er vår tilnærming på dette er at vi har et eget migrasjonsprosjekt fra starten til slutten.

H: Vi må også bruke en leverandør som skal hjelpe oss med dette.

HK: Men det blir opp til hver virksomhet hvor mye?

Fra salen: Nevnt at i forbindelse med migrasjon må man øke bemanning. Får derfor en kostnad. Får vi mer penger for å få gjort dette eller må hver institusjon styre dette selv?

H: Hver institusjon må regne med å få en høyere kostnad i en innføringsperiode ja.

OK: Må planlegge forretningslogikk osv. Stor variasjon mellom institusjoner. Stort antall målsystemer. Vil få en alvorlig jobb å tilpasse ting. Kan fort ende opp med to parallelle systemer i lang tid. Må sentralisere ting for at dette skal være hensiktsmessig.

HK: Kommentar på noe litt annet. Man har et forslag til en finansieringsmodell. UNIT vil ha et fond. Fondet finansierer prosjektet, men fondet fylles på ved at man betaler når man kobler seg på. Sektoren selv skal altså finansiere dette.

H: Fondet skal finansiere større felles løft på sikt. Mitt inntrykk er at vi har god IAM-kompetanse i sektoren, men vi må bygge opp en sektorkompetanse-pool for å være robuste. Trenger starthjelp utenfra, men viktig at vi får god kompetanse selv.

OK: I Norge har dette vært litt underprioritert, og man merker det godt.

HK: Generelt lite forståelse oppover hva et IGA koster.

H: Var i kontakt med universitet i København, som inkluderte å unngå GDPR-bot som en realisert gevinst, som var veldig positivt for budsjettet.

Hvordan vil man håndtere institusjonsspesifikke krav og prosesser, og infrastruktur? Må alle institusjoner følge UiBs verdensbilde?

H: Ser at vi trenger stor fleksibilitet rundt integrasjoner slik at hver institusjon kan lage egne integrasjoner. Man må dermed rette seg til sektorens verdensbilde, ikke UiB sitt. Ser ikke for oss at hele sektoren skal ha alt likt. Urealistisk. Ikke på lang sikt heller.

OK: Prosessbiten. UiB er pilot. All prosess blir da formet etter hvordan UiB har det. Ønsker at man holder øye med ting slik at man ikke får UiB-spesifikke løsninger.

H: Dette har vi snakket med Bergen om.



HK: Veldig godt spørsmål. Ønsker å standardisere sektorens behov.

Fra salen: Standardisere prosesser. Vil det bli satt gjennom BOTT? HR, IAM?

HK: Ikke lett å realisere i praksis. IAM-prosesser spenner over HR og IGA. Vanskelig, men veldig viktig. Påpekt mange ganger.

H: Helt enig. Skal støtte opp om disse prosjektene.

Vil kildekode lisens og muligheten for sektoren å selv videreutvikle løsningen uten å måtte leie inn dyre konsulenter være med som et krav i anbudsprosessen?

OK: Vi tenker at vi skal eie og kunne videreutvikle dette selv.

H: Har også krav om at datafunksjonalitet skal være tilgjengelig gjennom API-et

OK: Skal eie kildekode og gjøre tilpasninger selv.

HK: Tenker IntArk. Hvis leverandøren følger dette får vi et fleksibelt verktøy, vi kan snakke med via API-er.

OK: Må likevel gjøre tilpasninger.

H: Dette er vi veldig bevisst på.

HK: Varierende grad i kvaliteten på API-ene

Hvilken rolle vil Unit, Uninett, UH-IAM-prosjektet ta i innføringen? Hvor førende har prosjektet tenkt å være?

H: Vil ha god styring og god kontroll. Går inn på en kontraktsmodell der man kjøper gjennom Uninett for å kunne få mest mulig standardisert løsning. Samarbeid med leverandøren. Uninett har koordinerende rolle.

Joakim: Vil det være sentral styring av innføringen hos hver enkelt institusjon under prosjektet?

H: På noe ja, hovedsakelig det som er felles. Ikke noe spesifikt. Institusjoner må være forberedt på tilpasninger.

14:15, Cerebrum siden sist. Kjapp gjennomgang og smakebiter av kva som har skjedd med Cerebrum siden forrige seminar. Spør om du vil ha mer detaljer om det du fant interessant! Fredrik Larsen, Tech lead for Cerebrum utvikling

Hva har skjedd etter 2016?

Sist seminar snakket jeg om fokus fremover.

- IntArk
- Scheduler,
- Rest-API. Jobbet en god del videre med og er i bruk på flere instanser.

- Snakket ikke om SAP-import sist. Skjer nå i henhold til IntArk.
- Jobbet mye med Canvas-integrasjon, som vi får høre om senere.

Fokus på Devops. Få på plass varsling, logging og statistikk. Har nå overvåkning av Cerebrum gjennom Zabbix og Sentry. Alle loggene våre samles i ELK (ElasticSearch, Logstash, Kibana). Samler statistikk i statsd (Graphite, Statsd, Grafana)

Hadde stort fokus på brukeropplevelse i 2016. Snakket om å jobbe med passordbytteopplevelsen. Har ført til bedre, sikrere, og enklere passordregler. Fått nye passordtjenester som er tatt i bruk av noen instanser.

Snakket også sist om veikartet. Bruker mye tid på å lage felles funksjonalitet.

Skulle ta grep rundt teknisk gjeld. Har skrevet om hele Cerebrum slik at det nå internt bruker Unicode, og et viktig steg for å gå over til python3. Står på planen.

Siste ting vi snakket om sist i veikart var tilgangskontroll. Ville automatisere grupper. Dette har vi implementert nå. Kun brukt av UiO og UiT per i dag. Mange grupper bygges i dag automatisk.

Annet nytt:

- GDPR- Fått på plass en del opprydding i gammel personinformasjon.
- Lagd en modul for samtykke og reservasjoner. Originalt for Office365. Nå også for Gsuite. Kun i bruk på UiO per i dag. Ta kontakt om andre ønsker ta i bruk.
- Lager for tiden ny audit-logg. Ikke fornøyd med den gamle.
- Pybofh.

Tok en titt i Jira og vi har.

- Løst 1157 issues
- Laget 1259 nye issues.

14:45, UiT-Cerebrum migreres til UiO - skrekk eller fryd? UiT Norges arktiske universitet flytter drifta av Cerebrum over til UiO. Migrasjonen skjer siste uken i juni. Vi forteller om erfaringene og konsekvensene med dette., Kenneth A. Johansen, UiT og Joakim Hovlandsvåg, UiO

Jobber mye med dette på UiO for tiden.

K: Tilnærmer oss dette med litt skrekkblandet fryd. Skal bli veldig spennende. Hovedfokuset er å frigjøre interne ressurser.

J: Vi frigjør Kenneth og gjør det mer kostnadseffektivt. UiT har 13 år med instansspesifikk kode. Ca 700.000 kroner i arbeidsinnsats fra UiO. Skal bli ferdig til 15.juni. Har ca 1.5 uke fra 15.juni til alle tar ferie.

K: Har siden 2002 utviklet egne rutiner for mye. Koden divergerte for over 10 år siden. Vært vant med å ha full kontroll. Drifter og utvikler samtidig. Vet hva som kjører, og ser alle logger. Det mister vi nå. Lang liste med ting vi mister. Blir en del endringer i hva vi får tilgang til å følge med på. Blir mye nytt, men

håper vi blir fornøyde. Blir en del dobbeltarbeid. Blir rutineendringer siden vi har ting som er avhengig av manuelle kjøring av script. Hva skjer med responstid? Minutter, eller dager? Mange positive ting. Blir et klart skille mellom drift og utvikling. Blir enklere å ta i bruk funksjonalitet laget av andre. Opprydding i kode og scripts. Kenneth og Karen får gjort andre ting. Slipper periodevis konvergering med UiO-kode. Slipper å drifte Cerebrum.

J: En del av fokuset er Cerebrum oppleves som en sort boks. Mange ønsker mer innsyn. Vi er nervøse for belastningen på drift, men vi tar mange grep. Blir flere å dele kostnaden for felles funksjonalitet på. Blir enklere å migrere til nye UH-IAM-løsning hvis man migrerer på forhånd.

Vil få bofh-kommandoer for job\_runner (Cerebrum sin motor for å kjøre importere, eksporter og annen automatikk), som kanskje er interessant for de andre institusjonene. Skal kunne få ut status på jobb, detaljer om jobbene, og å kunne kjøre jobber. Kanskje andre kunne tenkt seg dette etter UiT får det? Ikke utvikla ennå, så detaljer ikke klare.

Splitter ut konfigurasjon for alle instanser. Gjør det mulig for andre å også få ut sitt oppsett av Cerebrum.

På sikt: Mer selvbetjening. Sammenslåing av personer skjer 2-3 ganger i uken hos UiT så dette må vi få ordnet.

Fra salen: Hvor mange ressurser har dere brukt på UiT?

K: Brukt flere år på det vi har gjort hittil.

15:15, Integrasjon mellom TP og Exchange. Prosjekt Kalenderdata jobber med IntArk-integrasjon mellom TP, Exchange og Canvas, og fortell kort om kva de har lærd til no., Jo Sama

TP = Timeplanlegging

Ønsker å samle kalenderdata for personer på ett sted. Vil gjøre det enklere å samarbeide. Vil provisjonere det automatisk. Skal være synlig i Exchange.

Dagens tilstand er at det finnes en løsning fra UiT som ikke følger IntArk. Lager ny. To faser. Først kalendertjenesten og TP + Exchange. Fase2 canvas + lokale tilpasninger.

Løsningen følger mikrotjeneste arkitektur slik at den følger IntArk. Åpner for mange muligheter (se figur fra presentasjon).

Er en del begrensninger. Kan se at vi har en sentral tjeneste for å håndtere data (avvik fra IntArk). Exchange som visningsflate setter rammer for hva vi kan gjøre. Får ikke bestemt fargene på kalenderhendelser vi oppretter selv, og man kan flytte møter man blir invitert til. Legger til en varslingstekst i hendelsene for å advare mot dette.

Fra salen: Vi har undervisningsrom som reserveres av sykehuset. Kunne tenkt meg å koble sykehuset til dette.

J: Har tenkt på dette og det er vanskelig. Møterom i Exchange lages ved add room og sender. Tar litt tid før det blir akseptert. Her sendes det litt eposter i bakgrunnen som vi ikke ser, som vi må styre med for å få det til å virke.

Fra salen: Støttes online versjonen av Exchange?

J: Ja.

15:45, Pybofh. Vi går gjennom den nye Bofh-klienten, korleis bruke den, og kva som gjenstår., Simeon Simeonov

Forskjellen mellom Pybofh og jbofh (standardklienten): Utvikles aktivt. Skrevet i python2, men liten endring for å gå til python3. Moderne dokumentasjon som oppdateres kontinuerlig. Alt jeg snakker om nå kan finnes i dokumentasjonen. Enklere å debugge og utvide. Og den kan brukes som en/et modul/bibliotek for å skripte opp enkle ting mot bofhd-serveren. Den er ikke bundlet for øyeblikket pga. sertifikatproblematikk.

Hvordan man installerer og setter det opp: Se slide.

Viste noen enkle eksempler på hva man kan gjøre: Hent ut alle medlemmer av en gruppe (group list) og slå deretter opp hvilke affiliations hver enkelt av medlemmene har (person info).

Fra salen: Noe ekstra å sette det opp?

S: Nei

Dag Løvlie: Kan man installere dette på Windows? Har du testet? Er ønskelig at UiO tester det før vi bruker tid på det.

S: Har ikke testet. windows Tror ikke det.

Jonas Braathen: pybofh bruker et bibliotek for input som ikke fungerer på windows, så det må vi bytte ut først.

Fra salen: Vil man distribuere det?

S: ER noen utfordringer. Fungerer bedre enn jbofh. Enklere å teste ting med det, men må da fikse at det kjører på Windows for eksempel.

Hans Kristian: Pybofh er på veikartet for høst 2019.

## Fredag 26. april

09:00, UH: IntArk. Prosjekt UH: IntArk er nylig fullført, og forteller om vedtatt arkitektur for UH-sektoren, kva den gir oss, og infrastrukturen som trengs for å støtte denne., Einar Jerpseth, prosjektleder UH: IntArk

Utgikk grunnet sykdom.

09:15, FS-API, Pål Erik Megaard

Var opprinnelig bestiller av FS-API-et.

Gikk gjennom API-et, og hvilke meldinger som genereres. Se presentasjon.

Kom ny versjon av FS-API-et i går, se e-post.

Er noen mangler før Cerebrum kan gå over til å bruke FS-API. Ønsker å gå bort fra gammel db-tilkobling (sql). Har andre tjenester vi også ønsker å koble på FS-API.

La også ved noen lenker i siste foil, for de som er interessert i mer detaljer.

09:15, IntArk: Canvas. UiO har utvikla en hendingsbasert integrasjon mellom Canvas, FS, Cerebrum og SAP. Utviklerne forteller om korleis den fungerer, og erfaringer vi har fått., Jonas Braathen, utvikler

UiO laget ny integrasjon mot Canvas. Er utviklet for å kunne være fleksibel, og prøvd å være gjenbrukbar.

Bruker rom-mal i FS for å styre hvordan aktiviteter skal se ut i Canvas.

(ref.anm: Referent tror begge dager starter på samme tidspunkt og ankommer ved starten av spørsmålsrunden her for å være «tidlig ute».)

Spørsmål:

Fra salen: Hvorfor bruker dere ikke FS sin egen Canvas-integrasjon?

J: Vi vil få til IntArk slik at det oppdateres kontinuerlig, slik at man slipper å vente på nattlige kjøringar.

Fra salen: Hos oss går det hver time.

Pål Erik: Vår jobb rakk ikke å bli ferdig på en time så jobben ble aldri ferdig.

HK: Et viktig prinsipp i IntArk er at data skal hentes i kildesystemet. Med FS sin filintegrasjon får man all data fra FS. For UiO har enkelte data Cerebrum og SAP som kildesystem, som da vil gå via FS, og det strider mot beste praksis.

J: Denne konfigurerbare strukturen var også noe som studieadministrasjonen var interessert i. Fantes ikke i filintegrasjonen.

09:45, IntArk: SAP og Lenel Onguard. UiO har utvikla ny integrasjon mellom SAP og universitetets adgangskortsystem (UA). Utviklerne går gjennom korleis integrasjonen fungerer., Sten Solli og Ulf Jarre Jerpseth

Kan ikke bruke SAP-dataene direkte i Onguard. Tilgjengelig via VMI. Må lage noe mellom Onguard sin VMI og de andre IntArk elementene. I dette tilfellet SAP.

Første vi må gjøre er å ha en meldingskø mellom kildesystemet og vårt. Lytter på køen. Bruker Python. Tenkte først å bruke PowerShell, men viser seg å være mye enklere å bruke Python.

API-et sender en melding med info om hvilken url dataene er tilgjengelig på hvis dette er en melding man bryr seg om. Lager en funksjon som henter ut informasjonen i url-ene fra de meldingene man er interessert i. (Veldig enkelt å skrive koden, se slidene.) Får svar i JSON-format.

Dette kan vi da bruke til å oppdatere info i Onguard og endre kortholder info for personene.

Potensielt automatisk oppdatering av kortilgang fra roller i SAP. Kan begrense papirarbeid betraktelig.

Bibsys vil gjerne vite når folk får nye adgangskort.

Koden vår beskjed fra adgangskortsystemet. Lager en liten melding om at dette er skjedd og sender det til meldingskøen. Denne meldingen kan da hentes ut av en annen integrasjon som oppdaterer sitt system med dette.

Eneste problemet så langt er at det er mange meldinger.

Spørsmål:

Fra salen: Var det sånn at man ikke får JSON som default fra SAP?

Jarre: Må be om json for å få det, hvis ikke får man xml.

Fra salen: Krever det conduit-lisensen til Onguard?

Sten: Ja, men bruker bare en. Microservice snakker med den, men trengs ikke flere.

10:00, Overvåking av Cerebrum. Drifterne går gjennom korleis UiO overvaker Cerebrum, og deres syn på forbedringer., Kai Vaade, drifter

Var tidligere 3 personer. Er nå 2. Har vakt på dagtid innenfor kjernetiden. Følger også med hvis man jobber tidligere eller senere enn dette, men ikke et krav.

Er proaktive for å oppdage feil så fort som mulig for å begrense konsekvenser. Utfordring at det er mange integrasjoner og mye automatikk som ikke er lett å teste.

Mest sårbare når vi legger ut ny kode. Endring av konfigurasjon skjer hovedsakelig av drift, mens utviklerne som regel utfører kodeendringer. Mulig å legge til tester av ny kode, men vanskelig å sjekke at alt går bra.

Overvåker produksjon med:

RT – Får som regel inn meldinger fra folk hvis det skjer ting.

Mattermost – Lynmeldinger mellom IT ansatte ved UiO.

Zabbix - Monitoreringssystemet. Gjør en del tester på disk, cpu, load osv. Men kan også sette opp alarmer på nesten hva som helst. Det systemet som gir oss mest muligheter. Ble nylig oppgradert. Følger med på bofhd, job\_runner, antall filer i job\_runner dir, og antall filer eldre enn 2 år. Har noen UiO spesifikke ting også som kan gjøres for andre om det er ønskelig også.

Sentry – Samler opp feil for oss slik at vi slipper å sende ut masse eposter.

ELK – Elasticsearch Logstash og Kibana. Bruker det kanskje i for liten grad.

Kom gjerne med forslag til forbedringer.

Eksempel på avvik:

Kodeendring som medførte at Cerebrum fjernet fødselsnummer. Ble satt i produksjon en fredag. Ble ikke oppdaget før på kvelden, av HiØ. For å unngå dette i fremtiden har vi fått opp lynmeldingstjeneste, jobber med å revidere prodsettingsrutinene og rutiner for varsling. Kom gjerne med innspill for hva man ønsker alarmer om. Skal også forbedre logging etter hvert. Vi forbedrer oss litt hele tiden. Ikke sikkert om vi hadde oppdaget feilen raskere i dag.

10:45, BOTT-ØL i et IAM-perspektiv. BOTT-ØL (Økonomi og Lønn) sitt delprosjekt IPAS ser på implementasjonen av ny ERP-løsning i BOTT, og spesielt tilgangsstyringa. Kva har dette å si for et IGA? Johnny Hansen, UiT, prosjektleder IPAS

BOTT-ØL har gått over en tid. IPAS er bare en del av det. Skal fortelle om begge, og tilgangstyring.

Jobber ved UiT. 80% BOTT, altså egentlig bare BOTT. Jobbet i 2 år som koordinator. Før det seksjonsleder for Karen og Kenneth i *Prosesstøtte og integrasjon*. Jobbet med sykehus. Før det elsykler i 3 år.

Er nå i gjennomføringsfasen av prosjektet. Resultatmål er at det skal utvikles, standardiseres, og innføres.

Stor prosjektorganisasjon (se slide for detaljer). Hadde kick-off i februar med 110 deltakere.

7 faser. En fase per halvår. Går 2019 til 2022. Utviklingen stater til sommeren eller etter ferien. Testing starter tidlig 2020. Har konsekvenser i forhold til IntArk. Bør ha IntArk klart før testing starter. Vil ikke teste uten å vite at IntArk er robust. Viktig at BOTT har implementert IntArk. Oppfordrer andre enn UiO til å også prøve seg på å implementere det.

Skal komme **hele** UH til gode. Bruker BOTT som eksempel her.

Viste produktnedbrytingsstrukturen. Mye som skal gjøres. De fleste produktene er godt i gang.

Tidsplan. Inneholder 12-1300 aktiviteter. Har planen i MS Project.

Våren 2019:

Oppstart alle teamene. Kartlegging. Begynt på funksjonelle design.

Strategisk avtale med DFØ.

Hva får vi?

Mer en erstatning av flere systemer i BOTT med ett standardisert system. Positivt å bruke felles løsning. Vil kunne håndtere prosjektøkonomi. Støtte for søknadsfasen for forskningsprosjekter. Tilsetting og arbeidskontrakt. Selvbetjeningsapp for å føre fravær, reise, osv. Blir tilrettelagt for sanntids flyt av data mellom disse løsningene.

IPAS:

Integrasjonsplattform, arkitektur, sikkerhets + integrasjon.

34 integrasjoner inn/ut av DF. Har 10 interne løsninger. Nye. Virksomhestspesifikke.

Delprosjekt Utvikling tar seg av funksjonell design.

Er en del avhengigheter. BOTT Masterdata, UNIT Masterdata? BOTT-ØL, UH-IAM, UH:IntArk.

Viktig at UH:IntArk er på plass..

BOTT Masterdata: Må komme i gang. Etterlyser litt mer fart på dette.

UNIT Masterdata: Vet ikke om det er noe fart her.

Tilgangsstyrings og brukeradministrasjon:

Vi er ikke ferdig. Har produktbeskrivelse og designdokument skal være godkjent ved utgangen av mai. Hensikten med produktet er å gi BOTT brukere de tilganger og rettigheter de skal ha.

En del gap fra forarbeidene. Se slidene for mer info. Dette vi prøver å få dekket opp med vårt produkt.

Info om hvordan man ser for seg DFØ sine løsninger. Følger IntArk. Se slidene.

Ser for seg at man har roller definert i SAP og HR. Dette er da masterdata. Må fungere med den både nye UH-IAM-løsningen og Cerebrum. Ønskelig å gjøre det så likt som mulig så det ikke har stor betydning hvilken IGA som kjører. Må også kunne integrere med DFØ-IAM da de har sin egen løsning. DFØ er skeptiske til at vi skal styre alt. Har ikke helt landet på hvordan man vil ha det med roller. Må gå noen runder til. Roller er kompliserte saker. Må finne et kompromiss som passer for alle.

Har et møte på Skype om noen uker for å få mer klarhet i det. Inviterte Hans Kristian til å være med på det.

Problemstilling man bør tenke på. Vil ha cerebrum i en god stund fremover. Når dette blir byttet ut flytter man IGA biten til UH-IAM, men Cerebrum er mer enn dette for mange i dag. Dette blir per i dag distribuert ut til andre systemer. Hva skjer med denne delen av Cerebrum? Blir en stor jobb.



Spørsmål:

Hans Kristian: Cerebrum brukes til my annet enn IGA. En av disse i tingene er integrasjoner. Derfor vi har laget UH:IntArk. For å få dette ut av Cerebrum. Er fortsatt en jobb som må gjøres.

Johnny Hansen: Når man bytter Cerebrum til UH-IAM: Grunnlaget blir da borte slik at man ikke kan flytte dataene. Må da kjøre ting parallelt. Blir problematisk for Tromsø. Må tenkes gjennom. Kanskje man må kjøpe tjeneste fra USIT for det.

11:25, «Alt vi har». Vi suser gjennom Cerebrum og gir en kort intro til alt som rører seg av automatikk. Merk at flere av punkta som taklast opp vil kreve tilpassinger før de kan brukast av alle instanser. Formålet med lyntalen er mer å starte en dialog om behov og løsinger., Fredrik Larsen, Tech lead for Cerebrum utvikling.

Alle har Bofh. Omtrent halvparten har fått API. De som vil ha kan si fra så setter vi opp det, da det settes opp etter behov. Samme gjelder for event Publisher. Event Publisher publiserer meldinger man kan lytte på. Alle har også job\_runner som passer på at alle eksporter kjører på riktig tidspunkt osv.

Gikk gjennom job\_runner og fant ut at det er mange jobber som kjører på alle instansene. UiO har over 200 jobber. Mer enn 3 ganger mer enn neste.

HK: Hvor mange jobber er det på UiT.

F: Usikkert. Gikk ikke gjennom deres konfigurasjon.

Forskjeller mellom databasene til de forskjellige instansene. Se slides for detaljer.

Vil bli kvitt DNS. Har et prosjekt for å flytte det ut.

Vi burde sette opp gpg-modulen for alle, men er kun satt opp hos UiO. Tillater kryptering av data. Gjør at vi ikke trenger klartekstpassord i Cerebrum fordi vi integrerer med AD, som krever klartekstpassord.

Fra salen: UiT har 72 jobber.

Feide\_service for to-faktor brukes kun av UiO og UiA.

Note har kun UiA. Nyttig for å lagre et kort notat på en entitet.

Dag Løvlie: Note brukes i liten grad.

Virtuelle grupper. Brukere er automatisk medlem i gruppen hvis de oppfyller visse krav.

Ansattautomatikk: Alle som har DFØ-SAP har samme opplegg. UiO har eget SAP opplegg.

Gruppeautomatikk: Batch jobb som oppdaterer store grupper. UiO lager en gruppe med det. UiA har to grupper. En for vitenskapelige, og en for teknisk/admin.

Tenker å gå over til virtuelle grupper på sikt.

Har noen fronter-grupper som man ikke vet helt hva brukes til. Er noe tilgangskontroll for kurs knyttet til dem. Vil bli kvitt de.

Varsler: De fleste bruker velkomst SMS, passordbyttepost og passordbytte-SMS.

Vedlikehold: Mange bruker remove-person-info for å rydde opp i persondata.

LDAP: Alle har Feideeksport. Litt varierende ellers.

AD: Alle har brukere, grupper og passord. Litt ekstra rundt omkring.

Eksporter: Kan få ting fra SAP til FS hvis det er ønskelig.

Rapporter: Lager et hav av rapporter. Se gjerne gjennom og si fra hvis noe er interessant. Vet generelt lite om hva som finnes om hva det brukes til.

Hvis noen savner noe må de gjerne si fra.

12:45, [Passordtjenester - veien videre](#). Nye Passordtjenester er tatt i bruk av mange - til dømes [passord.uio.no](#), [passord.nmh.no](#), [passord.hiof.no](#) og [passord.uit.no](#) - UiO forteller om visjonen for tjenesten, og veien videre., Hans Kristian Fjeld, tjenesteeier for Cerebrum på UiO

Tror passord er en veldig god kandidat for standardisering. Vi har like behov for passord, regler, og metoder rundt de. Koster å være god på passord. Beste praksis endrer seg. Før ville man bytte passord ofte. Det fører til dårlige passord, eller at folk skriver det ned. Må følge med på disse endringene for å ha en god passordtjeneste. Med en felles tjeneste er vi bedre rustet til å respondere på endringer.

Utgangspunktet for prosjektet var at vi hadde mange henvendelser rundt på passord. Hadde tungt fokus på brukeropplevelsen. Fikk god hjelp fra både UX og Sikkerhet. Vi fikk en mer brukervennlig tjeneste og vi får nå også sikrere passord.

Har fått mange innspill som har ført til små justeringer som i sum har gjort ting veldig bra.

Fikk oss en god latter da vi fikk se de gamle passordreglene. Folk gruet seg til å bytte passord. Nå har vi inntrykk av at folk synes det er ganske enkelt.

Bruker en variant av Stanford Password Policy. Bruk en vanlig setning. Man får da bedre entropi gjennom lengde i stedet for gjennom flere mulige tegn. De fleste forsøk på å knekke passord i dag er Brute force og da er lengden det viktigste.

Forhindrer gjenbruk av passord ved å kreve lange passord. Erfaring viser også at det er enklere å huske. Enklere å taste på mobiltelefoner.

Løst koblet til Cerebrum gjennom Cerebrum WS. Skrevet i Python3 og bruker Flask/Gunicorn og JSON Web Tokens i backend. Frontend bruker React og Redux.

Veikart:

Vår 2019: UiA, UiT

Høst 2019: NiH

Vår 2020: ID-Porten

Høst 2020: Brukerundersøkelse

Etterspurt å kunne autentisere seg inn i passordtjenesten gjennom ID-Porten. Glemt passordtjenesten benytter SMS. Fått en del innspill fra brukerundersøkelser tidligere. Tenker å kjøre en ny en i 2020 for å se om det er noen endringer vi bør ta hensyn til.

Tenker at det er bedre at vi gjør felles endringer enn at vi alle gjør små endringer hver for oss. Billigere hvis det er likt.

13:00, Cerebrum REST API. Etter alt snakket om UH: IntArk og RESTfulle integrasjoner, går vi gjennom Cerebrum sitt integrasjonspunkt, og korleis en kan integrere mot dette., Jonas Braathen, utvikler

I mai 2016 laget vi noen enkle endepunkter for å hente ut informasjon. Var ment for en AD integrasjon. Ikke klar per i dag. HiØ ville ha litt gruppefunksjonalitet. Passordtjenesten trengte litt mer informasjon. Cert ville ha info om karantener.

Autentiserer med et token. Får tilgang til alt eller ingenting. Egner seg best for integrasjon mellom systemer. API Manager kan låse ned til enkeltendepunkter.

Satt opp for 5 institusjoner. Har snakket om de fleste systemene som bruker det. Vil gjerne ha innspill til diverse skript man har behov for.

Dokumentasjon: <https://api.uio.no> og <https://int.usit.uio.no/cerebrum/>

Tok en liten tur gjennom API Manager. De fleste endepunktene er modellert etter hva vi kan gjøre med de interner Apene. Så på hvordan man kan liste ut personer, kontoer, grupper, tilknytninger osv. Mye forskjellig man kan gjøre. Se dokumentasjonen og vær kreativ.

Fra salen: Nå er det Cerebrum som svarer. Kunne man fått Cerebrum til å spørre FS.

Jonas: Da bør man heller snakke med FS sitt API.

Anbefaler å se i dokumentasjonen for å finne ut mer.

Spørsmål:

Fra salen: Kan man bruke Cerebrum APIet som en UH standard slik at endepunktene er klar ved nytt IGA?

Jonas: Det er jo et RESTFUL API og det baserer seg på Cerebrum måten å lagre ting på. Ikke nødvendigvis hensiktsmessig for et annet IGA å lagre slik. Det nærmeste vi har kommet å finne en standard for hvordan dette bør være er noe so heter SCIM, men den oppfyller ikke alle våre behov.

Johnny Hansen: Oppfordrer UiO til å se på standard for API-et til Cerebrum, for å gjøre det enklere å bytte ut.

Jonas: Har noen prøvd å bruke det?

HiØ: Trond gjorde noe, men usikkert hva det innebar

UiA: Bruker det til noe telefon-greier.

13:40, Nye eValgProsjekt Videreutvikling av eValg nærmer seg ferdig med ei heilt ny eValg-løysing. Vi går gjennom en valgprosess, for å gi et innblikk i korleis den fungerer. Du kan også teste ut nye eValg-løysinga selv (tilgjengelig bare fra UH-nett)., Joakim Hovlandsvåg, prosjektleder, og Håkon Møller, utvikler av eValg3

Joakim forteller først.

Bakgrunnen for ny eValg er at dagens løysing er lite intuitiv. Simeon må dermed hjelpe alle med å opprette og kjøre valg. Man må få den til å bli mer selvbetjent.

Alt gammelt ut. Fått hjelp av UX for å gjøre valgprosessen enklere for spesielt valgadministratorer. Opptelling flyttes inn på nettsiden.

Prosjektet har gått på en stund. Blir ferdig for UiO i år. Tilpassinger for andre skjer etter 2019.

Håkon viser frem hvordan man setter opp et valg.

Bruker Styreorgan som eksempel. Med eValg 2 må man opprette flere valg for dette. Nå kan man styre dette som et valg med 3 «undervalg». Blir geleidet til neste steg når man lagrer. Flyten er forenklet betraktelig.

Fra salen: Er det mulig å lage egne valgtyper selv med egne regler?

Håkon + Joakim: Det skal vi ordne. Må se på det etter vi er ferdig med å lage de mest vanlige valgene først.

Fra salen: Er det alltid kjønnskvoltering?

Håkon, Joakim, Sivert: På som standard, men kan skrus av om man vil. Vektingen styres i bakgrunnen og skal være konfigurierbar.

Joakim: Er meningen å skjule mest mulig vanskelige detaljer for valgadministrator, for å gjøre det enkelt og intuitivt.

14:00, Oppsummering og avslutting, Hans Kristian Fjeld og Joakim Hovlandsvåg

Joakim og Hans Kristian takker for oppmøtet og to hyggelige dager. Fint med feedback på det vi gjør.