MODERNISERINGSSTYRELSEN

Notat – Konceptmodel for SSO

24-05-2016

ØSY/JESBO/TG

FORMÅL

Dette notat beskriver et forslag til koncept for Single Sign On-løsning til Moderniseringsstyrelsens kunderettede systemer. Formålet er at beskrive løsningens grundprincipper, scope og forudsætninger med henblik på at kunne validere løsningskonceptet med relevante interessenter, inden løsningen etableres. Krav til institutioner står til sidst dette dokument.

KONCEPTMODEL FOR SINGLE SIGN ON

Moderniseringsstyrelsen har en række kunderettede systemer, hvor til der efterspørges nemmere adgang for den enkelte bruger. På nuværende tidspunkt skal brugerne logge sig på systemerne med forskellige bruger-id'er og kodeord til hvert system i porteføljen, hvor kodeordet løbende udløber og skal fornyes. Dette opleves som besværligt, og der er stor risiko for, at det store antal brugernavne og kodeord kan få brugerne til at nedskrive bruger-id og kodeord i klar tekst med deraf følgende mulighed for kompromittering af brugerkontoen. Desuden udgør det en gene for brugerne, at de løbende skal bruge tid på at skifte kodeord i mange systemer - samt at de risikerer at glemme kodeord, som ikke benyttes ofte, og derfor skal anmode om nulstilling af disse. Dette kan føre til såvel tabt produktivitet som en suboptimal brugeroplevelse.

Moderniseringsstyrelsen har på den baggrund besluttet at anskaffe en single sign-on-løsning (SSO), som skal være med til at øge brugervenligheden, sikkerhedsniveauet og samtidig give Moderniseringsstyrelsens kunderettede systemportefølje et kvalitetsløft, samt forenkling i forbindelse med brugerhåndtering.

SINGLE SIGN-ON

Moderniseringsstyrelsen har valgt, at den kommende single sign-on-løsning skal være baseret på en fødereret model. SSO-løsingen tager derfor udgangspunkt i principperne for en "hub-and-spoke"-model, hvor Moderniseringsstyrelsens vil anskaffe en føderationsserver, som er koblet til systemerne og til institutionernes databaser med domænebrugere.

I en fødereret SSO-løsning indgår flg. hovedaktører:

1. Føderationsudbyder
2. Identitetsudbyder
3. Serviceudbyder
4. Kunder/Institutioner

Føderationsudbyder (Moderniseringsstyrelsen) varetager en rolle, der kan sammenlignes med et omstillingsbord, når den enkelte bruger skal autentificeres til en webapplikation på baggrund af dennes legitimationsoplysninger. Autentificeringen

sker på baggrund af en forespørgsel, som føderationsudbyder sender til brugerens identitetsudbyder for verificering og efterfølgende til serviceudbyderen. Føderationsudbyderen fastlægger derudover de spilleregler (herunder sikkerhedskrav), der gælder i føderationen.

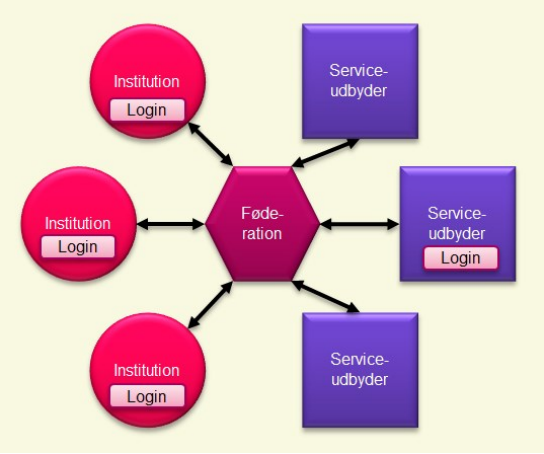
Identitetsudbyderen (institutionernes it-afdeling/-leverandør) står for verificering og autentificering af brugerens legitimationsoplysninger. For at undgå, at tredjepart kan udgive sig for at være en identitetsudbyder, bliver alle tokens sendt fra identitetsudbyderen til føderationsudbyderen signeret med et unikt certifikat, så føderationsudbyder kan verificere identitetsudbyderen og medsendte tokens validitet.

Serviceudbyderen (systemejer) har en service, der tilbydes et kundesegment. Oftest er denne service en webapplikation, hvor brugeren skal anvende en webbrowser for at få adgang til servicen. Brugerens egen institution skal have indgået kontrakt med serviceudbyder og der skal være oprettet forbindelse til en føderationsudbyder, hvis der ønskes, at anvendes single sign-on til den ønskede service.

Kunder/institutioner leverer brugere til den samlede føderation. Kunder/institutioner kan påtage sig ekstra rolle/-r i forbindelse med en SSO-løsning, men det afhænger af dog af valget for SSO-model. Kunden/institutionen kan agere identitetsudbyder, da disse ofte selv har en brugerdatabase (fx et AD), som bliver anvendt i forbindelse med autentificering af den enkelte brugers adgang til institutionens domæne. Det er med nogle SSO-modeller muligt at anvende institutionens brugerdatabase, hvorfra den enkelte bruger bliver verificeret og autentificeret af føderationsudbyderen.

Det vurderes, at en SSO-løsning baseret principperne fra "Hub-and-Spoke med decentralt login" vil kunne opfylde de opstillede behov på en kost-effektiv og langtidsholdbar måde.

Løsningsarkitekturens logiske komponenter, er illustreret på nedenstående figur:



Figur 1 SSO-løsning konceptmodel baseret på Hub-and-Spoke med decentralt login

Det essentielle i denne model består i, at den enkelte institution selv er identitetsudbyder for egne medarbejdere. Dette betyder konkret, at hver institution skal

etablere en såkaldt Identitetsudbyder komponent, som udstiller en standardiseret servicegrænseflade til håndtering af brugerlog-in.

Moderniseringsstyrelsen etablerer en central føderationsserver, der på den ene side integreres med institutionernes brugerregister, og på den anden side integreres med Moderniseringsstyrelsens portefølje af systemer. Herved bliver institutionerne afkoblet fra de tekniske detaljer i systemerne og kan koncentrere sig om autentifikation af egne medarbejdere.

Denne model indebærer en lang række fordele:

- Brugerne kan genbruge deres lokale domænelog-in, som de kender og formentlig benytter hver dag. Alle øvrige brugernavne og kodeord til Moderniseringsstyrelsens systemer forsvinder og dermed den tilhørende administration og gener ved udløb eller når de glemmes.
- Brugerne oplever single sign-on, hvilket resulterer i smidigere arbejdsgange og øget produktivitet.
- Der opnås en højere sikkerhed i og med, at domæne-logins typisk er underlagt mere kontrollerede processer end login til eksterne systemer for den enkelte institution. Eksempelvis vil en institution forventes at lukke en domænekonto, når medarbejderne stopper, mens man måske ikke altid er opmærksom på de eksterne brugerkonti den enkelte bruger har adgang til gennem webapplikationer.

Modellen indebærer, at institutionerne teknisk og sikkerhedsmæssigt tager et ansvar for autentifikationen af egne medarbejdere i og med, at autentificering baseres på institutionernes domænelog-in. SSO-løsninger er baseret på gensidig tillid og klar ansvarsfordeling. I den forbindelse forventes det, at Moderniseringsstyrelsen udarbejder en føderationsaftale, som indgås ved tilslutning af en institution. Føderationsaftalen aftale fastlægger relevante minimumskrav, der blandt andet vedrører sikkerhedspolitik, logning, processer samt tekniske kontroller.

I tilfælde af en sikkerhedsbrist, der vedrører SSO-løsningen vil denne principielt højst kunne berøre brugerkonti for institutionens egne medarbejdere. Da en institution rent teknisk ikke kan autentificere andre institutioners medarbejdere. En brist skalerer derfor ikke til andre institutioner i forbindelse autentificering af brugeren til de respektive systemer.

SSO-løsningen kan i sagens natur ikke garantere, at en bruger kan udnytte en systemfejl i andre systemer for at opnå uretmæssig adgang til andre institutioners data. Korrekt adskillelse mellem de forskellige institutioner i en applikation (*herunder multi tenancy*) skal derfor håndteres af det enkelte system.

For små institutioner, der ikke har etableret et domæne, vil løsningen omfatte en central brugerdatabase som erstatning, men dette er en undtagelse fra den generelle model, som kun tænkes anvendt i meget begrænset omfang. Denne kan endvidere bruges til brugere, der ikke er tilknyttet nogen institution.

BEHOV SOM LØSNINGEN SKAL ADRESSERE

For at kunne gennemføre et kvalitetsløft for adgangen til Moderniseringsstyrelsens kunderettede systemportefølje skal følgende behov løftes i løsningen:

- Det skal være muligt for brugeren at anvende sit lokale domænelogin ved adgang til Moderniseringsstyrelsens kunderettede systemportefølje. Eksisterende brugernavne i systemerne vil blive knyttet til domænekonti, mens kodeord til specifikke systemer skal udfases. Efter brugeren er logget på eget domæne bør al login til Moderniseringsstyrelsens kunderettede systemportefølje kunne ske uden yderligere brugerinteraktion via Single Sign-On.
- Der er en stigende efterspørgsel for at kunne tilgå nogle af Moderniseringsstyrelsens kunderettede systemer gennem mobile enheder, eksempelvis smartphones og tablets. Anvendelse af mobile enheder er tiltænkt systemer, hvor der skal foretage momentære interaktioner med et system, eksempel registrering af et rejsebilag eller faktura, når brugeren ikke har mulighed for fuld kontorfunktionalitet via en computer o. lign., hvorfor et behov for en fuldt understøttet arbejdsgang ikke er nødvendigt. Behovet gælder både såkaldte HTML5-applikationer samt 'native' mobile apps designet til et specifikt, mobilt operativsystem. Applikationerne må ikke stille yderligere krav til institutionernes egne infrastruktur, der ikke vurderes som et generelt krav for den samlede SSO-løsning. Applikationerne skal være standardprodukter og automatisk kunne opdateres og hentes fra en anerkendt kilde for det pågældende styresystem for den mobile enhed, eksempelvis fra AppStore, Google Play og lign.
- For PC'er og bærbare computere er det centralt, at føderationsløsningen ikke sætter nogen væsentlige begrænsninger eller forudsætninger for infrastruktur, som institutionerne etablerer til egne formål, men kan genanvende denne via nogle veldefinerede standardiserede grænseflader. Dette betyder blandt andet, at der ikke skal installeres software, der sikre at SSO-løsningen kan anvendes af den almindelige bruger. Det skal bemærkes, at krav om opsætning af en identitetsudbyder er nødvendig – men at dette relatere til it-afdelingen og almindelig tekniskdrift.
- Der opleves et stigende fokus på IT-sikkerhed for Moderniseringsstyrelsens kunderettede systemer, herunder hvorvidt systemerne er tilstrækkeligt beskyttet mod udefrakommende trusler. Den kommende SSO-løsning skal derfor give mulighed for at begrænse angrebsfladen, hvorfor uautoriseret adgang bliver vanskeligere at opnå.
- Systemerne, der skal tilgås gennem SSO-løsningen, har ikke nødvendigvis alle det samme behov for sikringsniveau ved autentificering. Baseret på en kommende løsning kan der være mulighed for, at håndtere differentiering af sikkerhedsniveauer – men det afhænger dog af udfaldet for udbuddet.
- Løsningen skal understøtte brug af yderligere autentifikation til særligt følsomme systemer. Dette kan eksempelvis være NemID til erhverv, en-gangskodeord via mail eller SMS etc. Af samfundsøkonomiske incitamenter er der fokus på at genanvende eksisterende to-faktor løsninger (etableret af institutionerne selv[1] eller NemID) frem for at føderationsløsningen skal tilbyde en selv.

[1] De fleste større institutioner forventes at have en lokal løsning til to-faktor autentifikation, som fx benyttes til hjemmearbejdspladser, VPN etc.

BRUGSSCENARIER SOM LØSNINGEN SKAL ADRESSERE

SSO-løsningen skal kunne understøtte den daglige arbejdsgang for alle tilkoblede institutioner – men for at højne sikkerheden for adgang til Moderniseringsstyrelsens systemportefølje er der lagt hovedfokus på, at kunne understøtte 3 brugsscenarier:

1. Login fra domæneregistreret arbejdsplads
2. Login fra mobile enheder
3. Login for brugere uden domæneidentitet.

LOG-IN FRA DOMÆNEREGISTRERET ARBEJDSPLADS

Det forventes, at de fleste brugere anvender Moderniseringsstyrelsens systemer fra en domæneregistreret arbejdsplads. Ved domæneregistreret arbejdsplads menes, at brugeren har adgang til institutionens domæne i form af en forbindelse til lokalnettet, hvor der kan anvendes domænelogin eller ved brug af et Virtuelt Private Network (VPN). Ved anvendelse af VPN til domænet, bliver der skabt en sikker forbindelse mellem bruger og domænet, når brugeren er fysisk placeret uden for det. En VPN-forbindelse opfattes som en del af netværksdomænet i brugerens institution og kan eksempelvis anvendes i forbindelse med en hjemmearbejdsplads, hvor der er behov for adgang til domænet.

Er der medarbejdere, der ikke anvender VPN fra en hjemmearbejdsplads for at udføre deres arbejdsopgaver, har disse ikke adgang til Moderniseringsstyrelsens systemer efter institutionen er koblet til SSO-løsningen. Det anbefales, at institutionerne undersøger medarbejdernes behov for VPN fra hjemmearbejdspladser i forhold til adgang til Moderniseringsstyrelsens systemportefølje.

LOG-IN FRA MOBILE ENHEDER

For mobile enheder findes to typer af applikationer, der skal understøttes:

a) Browser-baserede applikationer (programmeret i HTML5)
b) Native Applikationer

En mobil browser fungerer principielt som en browser på en pc, og derfor kan autentifikationsforløbet som beskrevet for en domæneregistreret arbejdsplads teknisk understøttes. Den største udfordring er her, at mange mobile enheder enten ikke kan etablere en VPN forbindelse til domænet eller at det i brugssituationen vil blive opfattet som for besværligt (fx oprettelse af rejseudlæg på farten). Til håndtering af mobile enheder, som ikke er forbundet direkte til institutionens domæne, foreslås, at institutionen etablerer en særlig Identitetsudbyder til mobile enheder, som kan nås via internettet. Denne Identitetsudbyder vil dog kun give adgang til systemer, der er tiltænkt adgang fra mobile enheder. Derved sikrer man, at adgangen fra internettet ikke åbner en generel angrebsflade men kun påvirker de ønskede mobilapplikationer og kun for de institutioner, som ønsker mobiladgang.

For native applikationer er det udbredt praksis, at man straks efter installationen af den pågældende App på sin enhed skal foretage en form for indrullering og personalisering af App'en. Dette kan foretages ved, at App'en starter en browser,

hvor brugeren logger på via forløbet beskrevet for mobile webapplikationer, og hvor resultatet efter autentifikation er, at App'en modtager en brugerspecifik nøgle, som lagres i App'en, og som bruges ved efterfølgende servicekald mod applikationens back-end. Ved at benytte denne tilgang, behøver man således ikke at etablere særlig funktionalitet i føderationsløsningen til håndtering af Native Apps.

I forbindelse med udrulning af applikationer til mobile enheder, kan det være at systemerne, som en ekstra sikkerhedsforanstaltning, har valgt at initiale indrullering af brugeren kun må ske på domænet, eller om indrullering også tillades via en internetvendt Identitetsudbyder. Dermed vil der være behov for, at Institutionerne også etablere en internetvendt identitetsudbyder. En internetvendt identitetsudbyder tillader, at man direkte fra internettet kan autentificere og autorisere den enkelte brugere – der vil derfor ikke være tilknyttede særlige certifikater og anden sikkerhed til denne type identitetsudbyder.

LOGIN FOR BRUGERE UDEN DOMÆNEIDENTITET

For at kunne anvende SSO-løsningen og dermed opnå adgang til Moderniseringsstyrelsens systemportefølje, skal den enkelte bruger være oprettet hos en identitetsudbyder. Dette kan give udfordringer for de institutioner, der ikke har muligheden for at etablere en identitetsudbyder.

SSO-løsningen skal derfor kunne danne rammerne for, at disse institutioner kan oprettes hos en identitetsudbyder – der udstilles af SSO-løsningen, der vil bestå af en central brugerdatabase. Administrationen af brugerne vil være institutionens ansvar og være institutionsopdelt, så administratorer ikke kan se og oprette brugere på tværs af institutioner. Her skal det sikres, at en brugerinstitution kan administrere egne brugere, hvorfor der skal kunne differentieres mellem brugernes rettigheder til SSO-løsning. SSO-løsningen skal etablere et login-modul for disse (få) brugere, der kan håndtere verificering og autentificering af legitimationsoplysninger.

BRUGEROPLEVELSEN

Brugerne vil ikke opleve ændringer i brugerfladen, før deres institution er overgået til føderationslog-in. Når dette sker, vil de evt. modtage en ny URL / startside, som de herefter skal anvende – formentlig som led i en informationskampagne fra institutionen.

Første gang brugerne logger på en applikation efter institutionen er overgået til føderation, vil de blive bedt om at logge på med det eksisterende, applikationsspecifikke brugernavn og kodeord. Herefter "forsvinder" behovet for at skulle bruge dette igen (permanent), og brugeren får automatisk adgang til den ønskede applikation.

Endvidere vil brugerne første gang blive bedt om at vælge deres institution, hvorefter valget huskes i en browser cookie. Hvis brugeren skifter browser eller sletter sine cookies, vil institutionen skulle vælges igen i loginforløbet.

Efter den initiale førstegangslog-in vil brugeren opleve at få direkte adgang til applikationerne uden at skulle logge på, hvis de sidder på institutionens domæne.

Tilgår brugeren applikationen fra en mobil enhed uden forbindelse til domænet, vil de dog blive afkrævet brugernavn og kodeord til domænet for at kunne logge på (men applikationsspecifikke kodeord er som sagt udryddet).

KRAV TIL INSTITUTIONER

Institutionerne skal teknisk etablere en eller flere Identitetsudbydere – antallet afhænger af institutionens eget behov. Identitetsudbyderen skal udstille en føderationsprotokol baseret snitflade til brugerlog-in baseret på SAML2.0, for at kunne deltage i føderation. Derudover stilles der ingen tekniske krav til netværk eller arkitektur. Afhængigt af udbuddets resultat, kan andre føderationsprotokoller komme på tale.

I forbindelse med implementering af SSO-løsningen vil der blive etableret en identitetsudbyder for institutioner med brugerdatabase hos Statens IT. Moderniseringsstyrelsen og Statens IT koordinerer etableringen af denne identitetsudbyder, som vil blive vedligeholdt, driftet og supporteret af Statens IT.

For institutioner med et Active Directory er det relativt enkelt at etablere en Identitetsudbyder, som kan opfylde de tekniske krav. Microsoft har inkluderet softwareproduktet Active Directory Federation Services (ADFS) i Windows serverløsninger, som kan etablere en Identitetsudbyder oven på et AD, dvs. etableringsomkostningen er begrænset til en Windows server og konfigurationsarbejdet. For institutioner med behov for højere oppetid og driftsstabilitet, kan man etablere et dubleret setup med lidt flere servere på 2-4 arbejdsdage. Selvom arbejdet således er begrænset, er erfaringen fra andre føderationer dog, at føderationskonceptet er nyt for mange og kræver en vis tilvænning og indlæring.

Der findes en lang række andre Identitetsudbyder løsninger (både open source og kommercielle) for institutioner, som måtte køre andre med andre former af brugerdatabaser end Microsoft AD.

Erfaringer fra bl.a. Danmarks Miljøportal viser, at en erfaren konsulent kan konfigurere en simpel ADFS opsætning på 1-2 arbejdsdage, og der findes detaljerede trin-for-trin vejledninger udarbejdet til andre føderationer (WAYF, KOMBIT, Danmarks Miljøportal), man kan tage udgangspunkt i.

Normalt vil man starte med at etablere en Identitetsudbyder, som er placeret på institutionens interne domæne, og som understøtter domænebrugere fra deres almindelige pc-arbejdsplads. Har institutionen et ønske om at understøtte SSO for mobile enheder, kan det som tidligere beskrevet være relevant for institutionen at etablere en ekstra Identitetsudbyder, som er internetvendt.

Da sikkerheden i føderationen i stort omfang vil afhænge af sikkerheden af de lokale domænelog-ins, skal institutionerne leve op til sikkerhedskrav oplistet i den føderationsaftale, der vil blive etableret. Føderationsaftalen kan fx stille krav til brugeroprettelsesprocesser, nedlæggelse af brugere, politik for kodeordskvalitet på

domænet etc. For institutioner med lav sikkerhedsmæssig modenhed, kan dette indebære organisatoriske og tekniske tiltag.

For små institutioner uden eget domæne vil der blive stillet krav til, at der kan anvendes en central institutionsadskilt identitetsudbyder, som er tilknyttet føderationsløsningen. Disse institutioner skal udpege en institutionsadministrator, der skal stå for den daglige administration af institutionens brugerdatabase, eksempelvis oprette og deaktivere brugere.