

Baggrundsbeskrivelse for installation af føderation i partnerorganisationer til Danmarks Miljøportal.

Miljøportalsekretariatet

Ref.: jejn

Den 22. november 2007

Baggrund

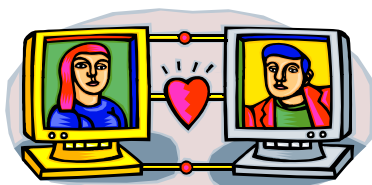
I forbindelse med strukturreformen den 1.1.2007 blev der i styregruppen for projekt "kommunalreform og digital forvaltning" taget beslutning om at sikre de landsdækkende datasamlinger ved hjælp af en brugerstyringsløsning, som bygger på gensidig tillid mellem de tilkoblede partnerorganisationer og Danmarks MiljøPortal (DMP). DMP valgte derfor at udvikle en brugerstyringsløsning, som bygger på begrebet og metoden *føderation*. Føderationsproduktet, som blev valgt, var Microsofts ADFS (Active Directory Federation Services) som er en indbygget komponent i Microsoft Windows 2003 R2 Server.

Valget af Microsoft betyder ikke, at partnerorganisationerne nødvendigvis skal vælge den samme løsning. Partnerorganisationen behøver blot at vælge en løsning, der leverer et token (dvs. en identitetsbeskrivende billet), som overholder WS-federation specifikationen.

Denne baggrundsbeskrivelse er henvendt til den eller de personer i partner-organisationerne, som skal bruge et overblik over føderation samt de dokumenter og komponenter, der skal anvendes i forbindelse med installationen.

Formålet med baggrundsbeskrivelsen er at skabe et overblik over størrelsen på opgaven i forbindelse med implementering af føderation i en partnerorganisation.

1. Hvad er føderation



En **føderation** eller **forbundsstat** er en statsdannelse, som består af en sammenslutning af flere delstater. Her fastlægges en fælles grundlov, hvilke beføjelser det fælles parlament og de nationale parlamenter har. Eksempler på føderationer er Tyskland, Rusland og USA.

I IT termer vil dette kunne oversættes til et partnerskab mellem to uafhængige parter (sikkerhedsdomæner), som bygger på gensidig tillid og ubegrænset godkendelse af hinandens brugere i forhold til de beskyttede applikationer som stilles til rådighed via føderationen.

Føderation virker på den måde, at en partner via en IDP (identity provider/føderations-server) udsteder et token¹ til en bruger i egen organisation/domæne, der kan anvendes til at opnå adgang til udvalgte systemer hos den anden partner i føderationen. Partneren, som leverer fagsystemet i føderationen, kaldes en SP (serviceprovider). SP'eren, som modtager et token, vil herefter give den pågældende bruger de adgange, som de udstedte token beskriver.



Rollefordelingen i Danmarks Miljøportals tilfælde er følgende: De partnerorganisationer som via en føderationsserver anvender DMP's systemer kaldes IDP'ere. Danmarks Miljøportal og fagsystemer kaldes SP'ere.

¹ Et token er et XML-dokument, som via forskellige former for attributter og grupper beskriver brugeren og de rettigheder, som brugeren skal bruge ved tilgangen til den anden partners applikation.

Attributterne i et token er beskrevet, som custom claims og grupperne er beskrevet som groupclaims². Groupclaims er generelt dem, som anvendes til autorisationen i det fagsystem, som brugeren tilgår (med mindre systemet kan "nøjes" med en attribut, der f.eks. beskriver brugerens afdeling).

Denne type applikation findes der meget få eksempler på blandt dem som myndighederne anvender, da der ikke kan differentieres ret meget i forhold til rettighedstildelingen på brugerniveau. Hvis man f.eks. ser på det sociale område, er der her eksempler på systemer, som kræver at rettighedstildelingen er så differentieret, at personale i samme sociale afdeling ikke må have samme rettigheder i samme sagsbehandlingssystem.

2. Fordele ved føderation

Partnerorganisationen

- Brugerne administreres kun internt i organisationens brugerkatalog, hvilket mindsker administrationen drastisk
- Meget lave installationsomkostninger
- Ingen licensomkostninger - kun opgraderingsbeskyttelse.
- Efter opsætning passer ADFS serveren sig selv, administrationen foregår herefter udelukkende i det lokale active directory.
- Ved ansættelse af ny medarbejder skal brugeren kun meldes ind i de normale AD-grupper, som er mappet med de udgående roller.
- Administration af password, herunder skift af password sker kun lokalt.
- Mange konsulenter/leverandører vil levere hjælp til installationen.

Slutbrugerne

- Brugere skal kun logge på lokalt. Herefter har brugere ægte SSO(single sign on) på alle systemer, som de har rettigheder til.
- Brugere skal kun huske deres lokale brugernavn og password. Således skal det kun resettes ét sted i tilfælde af, at brugeren har glemt det.

3. Løsningsdokumenterne og IDP Automatiserings komponenten

Der er udgivet følgende dokumenter til brug for partnerorganisationen. Der gøres opmærksom på, at dokument versionerne er de nuværende, som kan opdateres over tid:

1. *Supplerende noter og retningslinjer til konfiguration af ADFS i et Active Directory-miljø*
2. *Installation og konfiguration af ADFS i partnerorganisationer*
3. *ADFS-vejledning til ADFS-importapplikation*
4. *Konfiguration af WS-Federation i partnerorganisationer*
5. *Attributliste til Miljøportalen*
6. *Rollebeskrivelse*

² Groupclaims i forbindelse med føderation er roller, som indeholder en eller flere rettigheder i et system.

7. *Brugervejledning for slutbruger_føderation*
8. *Partnerautomatisering_pw_123.zip*
9. *DefaultADPropertyMapping.xml*
10. *partnerorg_xxxxx.xml*

Ad. 1. Dokumentet beskriver de overvejelser og tiltag IT-afdelingen skal foretage inden installationen af ADFS komponenten.

Ad. 2. Denne vejledning bruges af IT-afdelingen til at installere ADFS på en windows 2003 R2 server, som er koblet på domænet. Den skal anvendes af personer, som har en IT-infrastruktur-mæssig baggrund, og kender til domæner og DNS.

Ad. 3. Vejledningen beskriver hvordan IT-afdelingen anvender automatiseringskomponenten til at mappe grupperne i AD til udgående roller i ADFS serveren. Komponentens betydning er, at IT-afdelingen, efter anvendelsen kun skal tildele de nyoprettede grupper i AD'et brugere. Samt evt. udvide brugen af Active Directory-attributter. Hvorefter brugerne har adgang til partnerens systemer.

Ad. 4. Vejledningen beskriver hvilke forholdsregler og specifikationer en føderationspartner, som benytter et andet WS-federation³-baseret produkt end ADFS skal forholde sig til ved føderation med en ADFS baseret partner, f.eks. DMP.

Ad. 5. Dokumentet beskriver hvilke grundlæggende attributter partneren anvender. Attributterne ligger klar til automatisk overførsel ved hjælp af automatiserings modulet og filen under ad. 9.

Ad. 6. Beskrivelse af de roller som anvendes af DMP og hvem de skal og kan tildeles.

Ad. 7. Brugervejledning for slutbrugeren. Denne skal anvendes i forbindelse med, at fagsystemerne og partnerorganisationerne overgår til føderation.

Ad. 8. ZIP-filen indeholder automatiseringsmodulet, som skal installeres på de ADFS servere, som partnerorganisationen anvender.

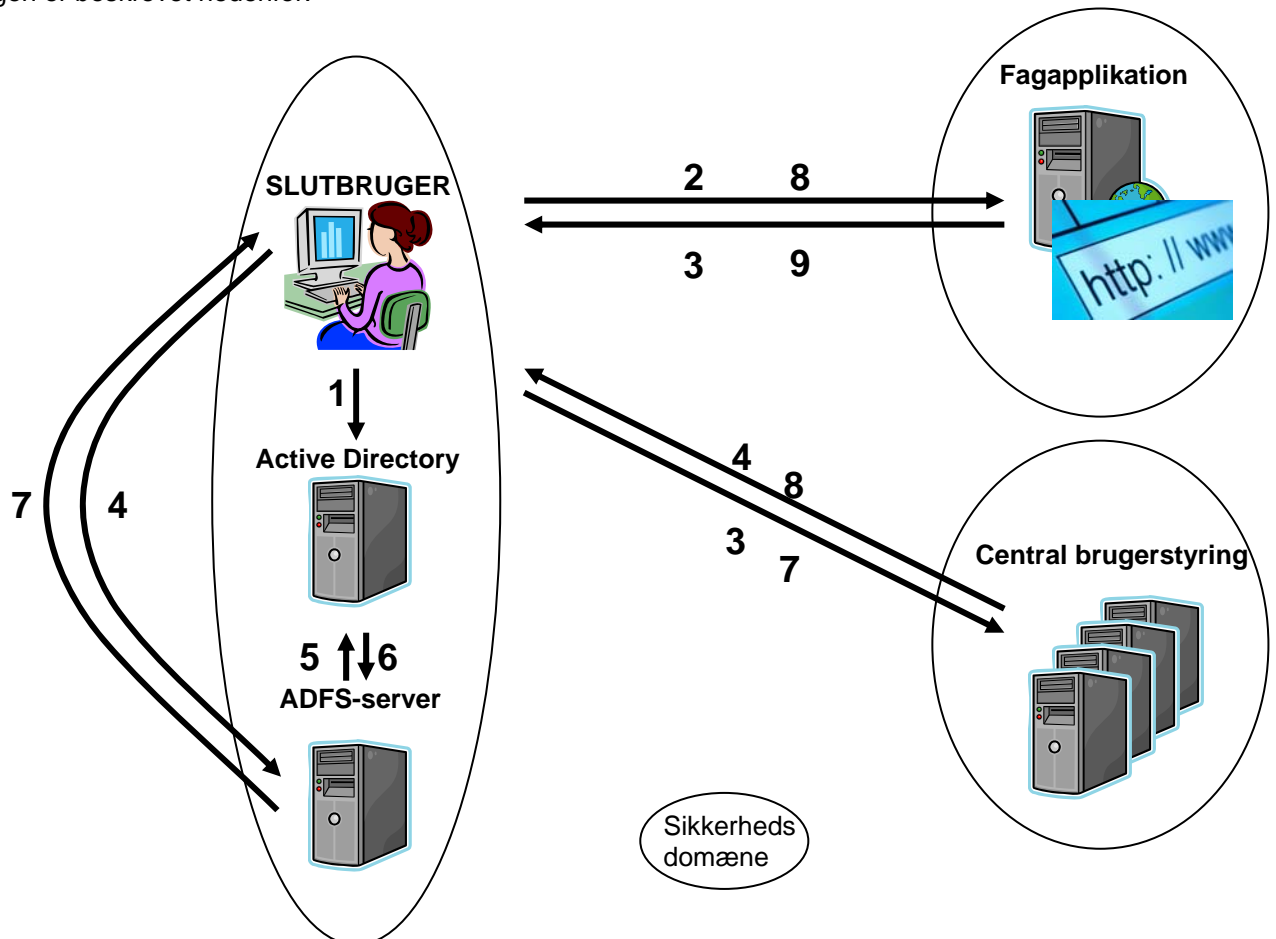
Ad. 9. XML fil som indeholder de faste attributter, som skal anvendes som outgoing custom claims. Man kan foretage individuel mapning fra egne attributter i active directory til de faste attributter.

Ad. 10. XML fil indeholdende de roller, der skal anvendes af organisationen som outgoing claims.

³ WS-Federation er specifikationen af det token, som sendes mellem 2 føderationspartnere. Samt sikkerheden omkring det sendte token.

4. Autentificeringen og autorisationen fra partnerorganisation til fagsystem.

I det følgende beskrives, hvordan en bruger tilgår en fagapplikation via føderation mellem en IDP og en SP. I forbindelse med føderationen foregår kommunikationen via brugerens browser. Nummereringen er beskrevet nedenfor.



Figur 4.1

Ad. 1. Brugeren logger på sit eget netværk, som normalt ved arbejdsdagens start, hvor denne bliver autentificeret af sit lokale Active Directory.

Ad. 2. Brugeren tilgår en applikation ved at tilgå den pågældende URL via f.eks. link.

Ad. 3. Applikationen anmoder brugeren om at få et token, der indeholder de nødvendige attributter og roller. Hvis brugerens browser ikke kan præstere en sådan omstilles brugeren til Centralbrugerstyring.

Ad. 4. Central brugerstyring undersøger brugerens cookies for at finde en persistent cookie, som indeholder brugerens homerealm forhold, dvs. angivelse af hvilket domæne, som brugeren kommer fra. Såfremt den centrale brugerstyring finder den pågældende information vil den centrale brugerstyring, for at få udstedt et token, redirecte brugeren til ADFS serveren i brugerens eget hjemmedomæne. Såfremt den centrale brugerstyring ikke finder den pågældende cookie, bliver brugeren bedt om at angive homerealm(domæne) ud fra en dropdownmenu. Herefter redirectes brugeren til den valgte ADFS server.

Ad. 5. ADFS serveren anmoder Active Directory om de nødvendige informationer om brugerens rolle og attributforhold.

Ad. 6. Active Directory leverer de ønskede informationer om brugeren -og ADFS serveren sammen-sætter på basis heraf et token.

Ad. 7. ADFS serveren leverer det ønskede token til brugerens browser og redirecter brugeren til Central brugerstyring.

Ad. 8. Den centrale brugerstyring modtager brugerens udstedte token og gennemgår det for at kontrollere, om brugerens token indeholder rettigheder, som er i overensstemmelse med partnerorganisationens rettigheder til det pågældende fagsystem. Den centrale brugerstyring mapper og tilskærer desuden det udformede token, således at det kun er de roller, som fagsystemet skal anvende, der kommer med i fagsystemet. Samt der evt. sker de nødvendige konverteringer til roller som og data som fagsystemet forstår. Når dette er gjort, viderestilles brugerens browser til fagsystemet.

Ad. 9. Fagsystemet modtager tokenen og tildeler brugeren rettigheder i overensstemmelse med de rettigheder, som er beskrevet i det modtagne token. Herefter åbner fagsystemet for en autentificeret og autoriseret session.

5. Føderation med partnerorganisationer som ikke anvender ADFS

Det er, som tidligere beskrevet, muligt at anvende en anden føderationsserver end ADFS-serveren. Partnerorganisationen skal blot levere et WS-føderationstoken ud for de specifikationer, som er angivet af Microsoft samt i dokumentet: ” *Konfigurering af WS-Federation i partnerorganisationer*”. Herefter vil den pågældende partner kunne tilgå en ADFS -baseret SP på lige fod med de resterende organisationer.

6. Økonomi

Partnerorganisationen skal investere i følgende:

1 stk. Windows 2003 server R2 enterprice edition samt hardware.

Derudover kan partnerorganisationen vælge at foretage installationen selv ud fra vejledningen som leveres af DMP eller anmode om ekstern hjælp.

Det vurderes ud fra tilbud, som DMP har modtaget, at dette bør kunne gøres inden for ca. 15.000 kr. ekskl. moms.

Vurderet vil installationen tage ca. 1 arbejdsdag.

Nedenstående skema viser en estimeret pris på anlægsudgifterne i forbindelse med føderation i mod DMP.

Emne	Pris
1 stk. Windows 2003 server R2 enterprice edition	Kr. 15.000 ekskl. Moms
1 stk. Hardware server	Kr. 25.000 ekskl. Moms
Opsætning	Kr. 15.000 ekskl. Moms
I alt	Kr. 55.000 ekskl. Moms

Årlige driftsomkostninger vil derfor kun udgøre en standard serverdrifts udgift, samt en eventuel opgraderingsbeskyttelse af softwaren.

Forudsætningerne for ovenstående estimat er at partnerorganisationen anvender Microsoft Active Directory, som brugerkatalog.

7. Konklusion

Ved installation af føderation vil en partnerorganisation kunne spare en mængde administrative udgifter. Både i forhold til normal brugeradministration, men også i forhold til brugernes daglige tidsforbrug på login flere gange dagligt.

Derudover vil løsningen kunne anvendes imod andre offentlige lignende installationer.

Med de automatiseringer, som DMP har fået udviklet til partnerorganisationerne, vil ændringer i roller-strukturerne m.v. kunne udføres på meget kort tid.

Løsningen vurderes derfor, som en nødvendig installation der vil gavne partnerorganisationen meget.

8. Kontaktinfo vedrørende føderation med DMP

Jens Jakob Nørtved Bork

Projektleder.

Danmarks Miljøportalssekretariat

c/o By og Landskabsstyrelsen

Haraldsgade 53

2100 København Ø

☎ +45 7254 6910 - ✉ jejnb@miljoportal.dk

☎ +45 2270 5673

☎ 7254 5454 - ✉ miljoportal@miljoportal.dk

www.miljoportal.dk

Eannr.: 5798000871007

CVR: 29776938