Danmarks Miljøportal
Data om miljøet i Danmark

Hvad er sammenhængende log-in?

Danmarks Miljøportal
Ref.: jejnb
21. august 2012

Formål

Formålet med beskrivelsen er at skabe et overblik over sammenhængende log-in, som en nem og enkel måde at administrere brugere på.

Denne pjece er henvendt til de partnere af Danmarks Miljøportal, som har brug for viden om sammenhængende log-in. Der vil være information om produktet, fordelene ved at benytte sammenhængende log-in, økonomien i det samt en opsamlende konklusion.

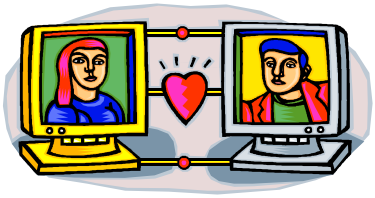
Administration af brugere vha. sammenhængende log-in

Danmarks Miljøportal er indgangen til mange forskellige fagsystemer på miljøområdet. Fagsystemerne benyttes af myndighederne og andre miljømedarbejdere. For at administrere de mange forskellige brugere, benytter Danmarks Miljøportal et brugeradministrationssystem.

Danmarks Miljøportals brugeradministration kaldes sammenhængende log-in og bygger på metoden *føderation*. Den føderation som benyttes er Microsofts ADFS 2 (Active Directory Federation Services), som er en indbygget komponent i Microsoft Windows 2008 R2 Server. Sammenhængende log-in bygger på gensidig tillid mellem de tilmeldte partnere og Danmarks Miljøportal.

Valget af Microsoft betyder ikke, at partnere skal vælge den samme løsning. Eneste krav til partnerne er, at der vælges en løsning, der leverer et token (dvs. en identitets-beskrivende billet), som overholder OIO SAML-specifikationen.

Et partnerskab der bygger på gensidig tillid



En **føderation** eller **forbundsstat** er en statsdannelse, som består af en sammenslutning af flere delstater. Her fastlægger 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 partnere (sikkerhedsdomæner), som bygger på gensidig tillid og ubegrænset godkendelse af hinandens brugere i forhold til de beskyttede fagsystemer, som er omfattet af løsningen.

Fordelene ved sammenhængende log-in

FORDELE FOR PARTNERNE

- Brugerne administreres kun internt i egens organisations brugerkatalog (Active Directory), hvilket mindsker administrationen drastisk
- Administration af password, herunder skift af password, sker kun lokalt
- Ved ansættelse af ny medarbejder, skal brugeren kun meldes ind i de normale AD-grupper, som er mappet med de udgående roller
- Meget lave installationsomkostninger - kan udgøres af en Windows server 2008 R2 SE
- Mange konsulenter/leverandører vil kunne levere hjælp til installationen
- Ingen licensomkostninger - kun opgraderingsbeskyttelse
- Efter opsætning passer ADFS2-serveren sig selv og administrationen foregår herefter udelukkende i det lokale brugerkatalog (Active Directory)
- Løsningen kan anvendes til lignende offentlige installationer

FORDELE FOR BRUGERNE

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

GENERELLE FORDELE

Ved installation af sammenhængende log-in vil en partner kunne spare en mængde administrative udgifter. Både i forhold til normal brugeradministration, men også i forhold til brugernes tidsforbrug på log-in flere gange dagligt. Dertil kommer at ændringer i rollestrukturen mv. vil kunne udføres på meget kort tid eftersom Danmarks Miljøportal har fået udviklet automatiseringsløsninger til partnerne.

Hvad koster det?

For at implementere sammenhængende log-in skal partneren investere i følgende:

1 stk. Windows 2008-server R2 standard edition. Løsningen kan fungere på et virtuelt miljø. Det vurderes, at en server er i stand til at gennemføre 25 logins pr. sekund, hvilket betyder at langt de fleste organisationer kan nøjes med én server.

Partneren kan vælge at foretage installationen selv ud fra installationsvejledninger, som leveres af Danmarks Miljøportal eller der kan anmodes om ekstern konsulentbistand. Det vurderes ud fra tilbud, som Danmarks Miljøportal har modtaget, at konsulentbistand til installationen vil koste maks. 15.000 kr. ekskl. moms, og at selve installationen kan udføres på én arbejdsdag.

Nedenstående skema viser en *estimeret pris* på implementeringsudgifterne i forbindelse med indgåelse af sammenhængende log-in med Danmarks Miljøportal.

Emne	Estimeret pris
1 stk. Windows 2008-server R2 Standard edition	Kr. 5.000 ekskl. moms
1 stk. Hardware-server	Kr. 25.000 ekskl. moms
Opsætning (kan udelades)	Kr. 15.000 ekskl. moms
I alt	**Kr. 45.000 ekskl. moms**

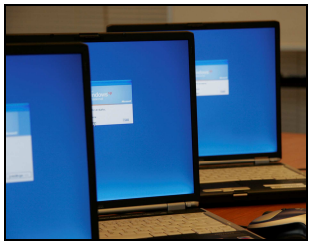
Hvis der anvendes en virtuel server, minimeres udgifterne til hardwaren.

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

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

Føderation med partnere der ikke anvender ADFS 2

Det er, som tidligere beskrevet, muligt at anvende en anden føderationsserver end ADFS-serveren. Partnerne skal blot levere et OIO SAML-token ud fra de specifikationer, som er udgivet af Digitaliseringsstyrelsen.



Sammenhængende log-in i teknisk forstand

Sammenhængende log-in virker på den måde, at en partner via en CP (Claim provider/føderationsserver) udsteder et token[1] til en bruger i egen organisation/domæne. Det udstedte token kan anvendes som adgangsbillet til udvalgte fagsystemer hos den anden partner i føderationen. Denne partner leverer fagsystemerne og kaldes en SP (serviceprovider). Når tokenet er modtaget af serviceprovideren, vil den pågældende bruger have netop den adgang, som det udstedte token foreskriver.

I tilfældet Danmarks Miljøportals er CP'erne partnere, der via en føderationsserver anvender DMPs fagsystemer. Danmarks Miljøportal og dets fagsystemer er SP'ere.

Attributterne og grupperne er i et token beskrevet som claims[2]. Claims anvendes til autorisation i det fagsystem, som brugeren benytter.

Vejledninger til brug for partnerens installation

Der er udgivet en række vejledninger til til brug for partnernes installation herunder vedr. IDP-Automatiseringskomponenten. De kan rekvireres ved at kontakte Danmarks Miljøportal på miljoeportal@miljoeportal.dk

Kontaktinformation

Kontakt Danmarks Miljøportal på telefon 72 54 54 54 eller skriv til miljoeportal@miljoeportal.dk

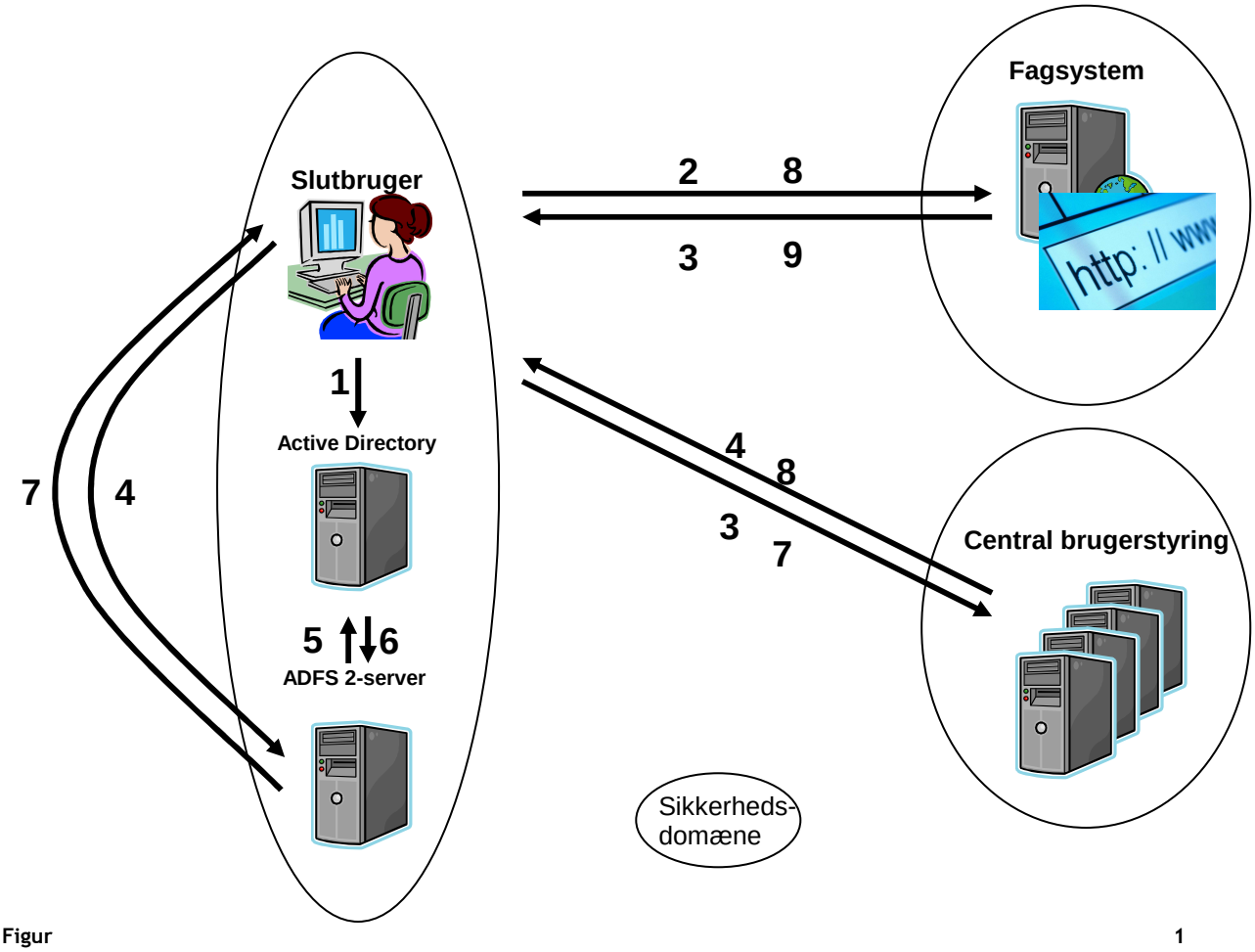
1 Et token er et krypteret XML- dokument, som via forskellige former for attributter og grupper beskriver brugeren og de rettigheder, som brugeren har ved tilgangen til den anden partners fagsystem.

2 Claims af typen 'DMP Roles' er roller, som indeholder en eller flere rettigheder i et system.

Bilag 1

Hvordan får en bruger adgang til fagsystemer med sammenhængende log-in? – teknisk beskrivelse

I det følgende beskrives, hvordan en bruger får adgang til fagsystemer mellem en CP[3] og en SP[4] Autentificeringen og autorisationen mellem partnere forløber. Kommunikationen foregår via brugerens browser som beskrevet neden for.



Figur 1

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

Ad. 2. Brugeren åbner et fagsystem ved at tilgå den pågældende URL via fx link.

Ad. 3. Fagsystemet 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 Central brugerstyring.

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, sende brugeren til ADFS 2-serveren i brugerens eget hjemmedomæne. I de tilfælde hvor den centrale brugerstyring ikke finder den pågældende cookie, bliver brugeren bedt om at angive homerealm (domæne) ud fra en dropdownmenu. Herefter sendes brugeren til den valgte ADFS 2-server.

Ad. 5. ADFS 2-serveren anmoder brugerkataloget (Active Directory) om de nødvendige informationer om brugerens rolle og attributforhold.

3 CP er en claim provider/føderationsserver

4 SP er en serviceprovider

Ad. 6. Brugerkataloget (Active Directory) leverer de ønskede informationer om brugeren - og ADFS2-serveren sammensætter på basis heraf et token.

Ad. 7. ADFS 2-serveren leverer det ønskede token til brugerens browser, og sender brugeren videre 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 dé roller, som fagsystemet skal anvende, der kommer med i fagsystemet. Evt. sker der nødvendige konverteringer til roller og data som fagsystemet forstår. Når dette er gjort, viderestilles brugerens browser til fagsystemet.

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