GLOBETEAM

Danmarks Miljøportal (DMP)

Vejledning til fagsystemejere omkring forløbet for tilkobling af en applikation

Version 1.2

Indledning

Denne vejledning beskriver forløbet i relation til tilkobling af en applikation til DMP's føderale brugerstyringsløsning.

Denne vejledning bliver suppleret med en række vejledninger, der er udarbejdet til de mest udbredte afviklingsmiljøer (.NET og Java). For så vidt angår de detaljerede anbefalinger og retningslinjer for udviklingen af applikationerne henvises således til disse vejledninger:

- Vejledning til fagsystemejere omkring tilkobling af .NET 3.5-baseret webapplikation
- Vejledning til fagsystemejere omkring tilkobling af .NET 3.5-baseret web service
- Vejledning til fagsystemejere omkring tilkobling af .NET 4.5-baseret webapplikation
- Vejledning til fagsystemejere omkring tilkobling af .NET 4.5-baseret web service
- Vejledning til fagsystemejere omkring tilkobling af Java Metro-baseret web service

Indhold

Introduktion til DMP's brugerstyringsløsning set fra fagsystemejerens synsvinkel

DMP's føderale brugerstyring er baseret på Safewhere standardprodukt, Identify, og er konfigureret med følgende end points:

- Webapplikationer: WS-Federation (SAML 1.1 tokens) eller SAML 2.0 (SAML 2.0 tokens)
- Web Services: WS-Trust 1.3 med authentication enten via x509 certifikat eller username/password./. Der anvendes udelukkende message-baseret security – dvs al transport sker via HTTP (port 80)

DMP har afgrænset brugen (og supporten) af web services end points til udelukkende at tillade brug af WS-Trust 1.3, da dette er en OASIS-standard. Ligeledes er autentificeringen afgrænset til Username (brugernavn/password) eller x509 klientcertifikat. Der anvendes message security, idet denne både er lettere at konfigurere og fejlfinde på. For uddybende information omkring opsætningen af applikationer til brug med disse henvises der til de underliggende vejledninger.

Det anbefales at løsningerne bygges op omkring de udleverede code samples, idet dette betyder at man er sikker på at løsningen vil fungere korrekt op mod det givne end point. Alternativt er at man skal igennem et trial-and-error forløb, der både er svært og ressourcekrævende for at få en løsning til at fungere korrekt op imod et givet end point, idet de forskellige standarder og applikationsplatforme rummer en lang række muligheder for individuel konfigurering,

Der gøres ligeledes opmærksom på at webapplikationer (dvs. passive requestor-løsninger) **skal** sikre at en evt. WHR-parameter[1] videresendes i http redirect'et til DMPs STS. WHR-parametren finder anvendelse til Home Realm Discovery og sikrer som sådan at det er muligt for brugerne selv at angive hvilken IdP de kommer fra og således undgå at blive spurgt om dette under loginforløbet i STS'ens regi.

Det er i øvrigt muligt at hente federation metadata-filen hos DMP's brugerstyring på https://log-in.miljoeportal.dk/runtime/FederationMetadata/2007-06/FederationMetadata.xml. Den tilsvarende fil for testmiljøet kan hentes på https://log-in.test.miljoeportal.dk/runtime/FederationMetadata/2007-06/FederationMetadata.xml. Hvis du vælger at lave en SAML 2.0 Protokol baseret løsning skal du benytte dig af SAML 2.0 endpoints: https://log-in. miljoeportal.dk/runtime/saml2/metadata.idp og tilsvarende i test: https://log-in.test.miljoeportal.dk/runtime/saml2/metadata.idp

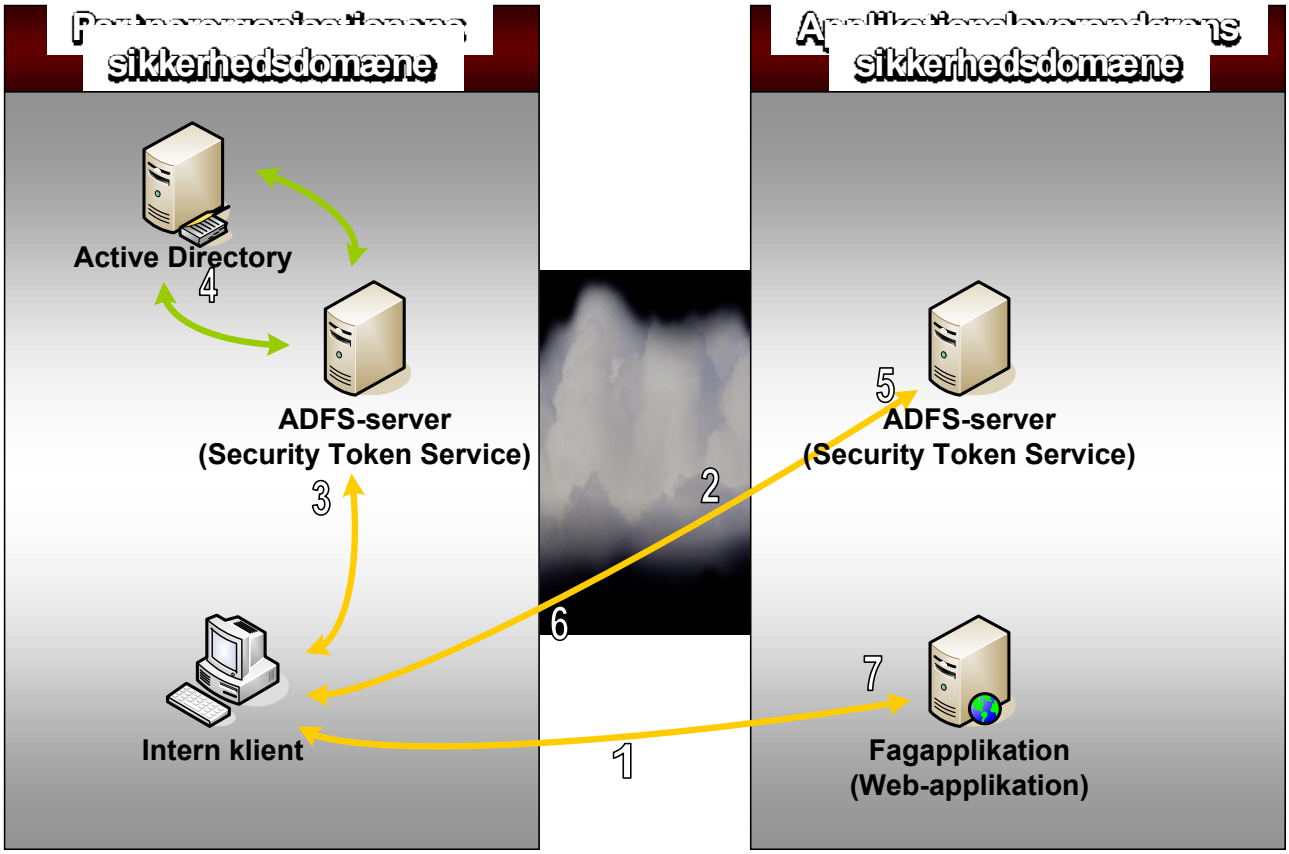
Claims-baserede applikationer

I føderale applikationer skal applikationen ikke længere selv logge brugeren ind. Dvs. i en føderal løsning sker login'et mod applikationen centralt – altså udenfor applikationens rækkevidde – og applikationen "fodres" blot med en liste af claims, der beskriver brugerens roller og egenskaber. Af samme årsag betegnes føderale applikationer ofte slet og ret som claims-baserede applikationer.

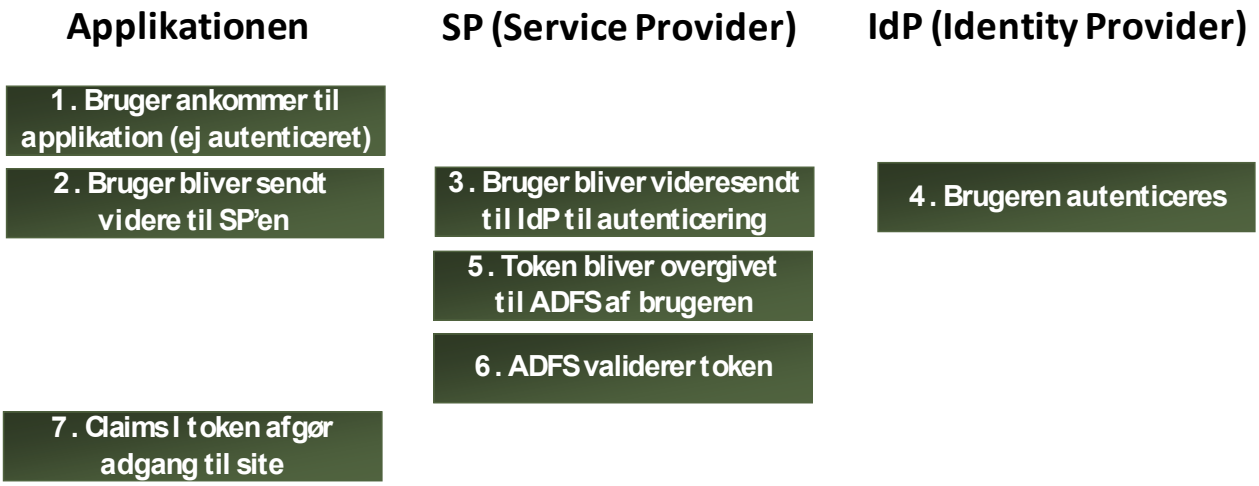
Der er med andre ord aldrig en adgangskode eller et brugernavn/adgangskode-check involveret hos selve applikationen. Applikationsudvikleren vil som sådan udelukkende komme til at arbejde med claims og sparer dermed også en hel masse arbejde relativt til de tidligere metodikker for autentificering og autorisation!

[1] WHR-parametren er beskrevet i vejledningen "Introduktion til automatisk login mod Danmarks Miljøportal".

Følgende illustration viser et loginforløb mod en claims-enablet webapplikation:



Loginforløbet på figuren er angivet nedenfor:



Det er altså i trin 7, at brugerens claims overleveres til applikationen i form af et SAML-formatteret token.

Claims
Safewhere*Identify er ligesom dets modstykke, AD FS 2.0 og (ADFSv1), som DMP's oprindelige brugerstyring var baseret på, baseret på claims. Claims-paradigmet er på vej til at vinde bredt indpas som den dominerende måde at udføre identitetsstyring på. Metodikken er dog stadig ny for de fleste, hvorfor vi vil indlede med en opsummering af, hvad det handler om.

Claims er et sæt af name-value parametre, der beskriver en bruger af systemet. Eksempler på claims:

- En applikationsrolle.
- En brugeregenskab (feks. et CVR-nummer, en e-mail adresse eller måske personens fødselstidspunkt).

En claims består essentielt af et name, der identificerer Claim'en, samt en value.

Name skal være unik. Name består af en unik udsteder og et unikt navn (fx "http://www.miljoeportal.dk/telephoneNumber" eller "dk:gov:saml:attribute:PidNumberIdentifier"), mens value angiver indholdet af den pågældende attribut. Den fuldstændige liste over de claims, der anvendes i DMP's løsning, kan findes i dokumentet "DMP - Claims".

I claims-baserede applikationer bliver claims anvendt som den centrale identifikation af brugeren. Applikationens del af arbejdet med styring af brugere og rettigheder er således begrænset til at evaluere claims for den aktive bruger og på baggrund af deres indhold bestemme, hvilken adgang brugeren har, samt hente evt. relevante informationer omkring samme.Dette sker på basis af rollebaseret sikkerhed, som tager udgangspunkt i, hvilke roller, der er udtrykt i brugerens claims. Har brugeren eksempelvis tilknyttet 3 rolle claims, så er det det samme som at sige at brugeren er medlem af de 3 roller.

Det er muligt at finde yderligere detaljer omkring claims i følgende Microsoft-artikel:

http://msdn.microsoft.com/en-us/magazine/cc163366.aspx. Det kan evt. også anbefales at lynlæse de første kapitler af Microsofts onlinebog "A Guide to Claims–based Identity and Access Control" fra Patterns & Practices-serien (http://msdn.microsoft.com/en-us/library/ff423674.aspx).

SAML 1.1 og SAML 2.0 tokens
DMPs STS er bygget til brug med SAML 2.0 tokens, da dette er den vedtagne fællesoffentlige standard. Det er således et krav at alle IdP'er, der tilkobles DMP anvender SAML 2.0 tokens.

Af hensyn til kompatibiliteten tilbydes der dog brug af både SAML 1.1 tokens og SAML 2.0 tokens på applikationssiden. For Web Services har man frit valg mellem SAML 1.1 og SAML 2.0 tokens. Webapplikationer, der er baseret på WS-Federation protokollen anvender altid SAML 1.1 tokens, mens web applikationer, der anvender SAML 2.0-protokollen pr. definition anvender SAML 2.0 tokens.

Der er en lille (men afgørende) forskel mellem SAML 1.1 og SAML 2.0 i relation til syntaksen af claims. SAML 1.1 tokens tillader kun brug af "/" til at separere udstederens navn og claim'ens navn i claim'ens Name-del, hvorimod SAML 2.0 tokens tillader brug af fx ":" som separator. Claims, der er en del af OIOSAML-standarden, anvender ":" som separator.

Ved opsætningen af claims i applikationen er det således nødvendigt at være opmærksom på, hvorvidt der anvendes SAML 1.1- eller SAML 2.0-tokens.

Tilkobling af en applikation

Tilkoblingen af en applikation til DMP's føderale brugerstyringsløsning består af følgende trin:

1. Tilpasning af applikationen til konsumering af claims.
2. Tilkobling af applikationen til DMP's testmiljø.
3. Aftestning af applikationen mod DMP's testmiljø.
4. Tilkobling af applikationen til DMP's produktionsmiljø.
5. Slutaftestning af applikationen mod DMP's produktionsmiljø.
6. Frigivelse af applikationen til drift.

Denne vejledning giver en overordnet beskrivelse af, hvordan man gennemfører de ovennævnte trin.

Tilpasning af applikationen til konsumering af claims

Applikationen skal være claims-aware for at den kan fungere med DMP's brugerstyring. Claims-aware betyder at applikationen anvender det SAML token, som bliver genereret af DMP's føderale brugerstyring, til autentificering og autorisering.

Applikationen skal med andre ord være bygget til at konsumere SAML tokens med det format (dvs. de claims), som finder anvendelse i DMP's føderale brugerstyring. Formatet er beskrevet i dokumentet "DMP – Claims v2.1".

En claims-aware applikation skal pr. definition være i stand til at håndtere brugeren, når han eller hun rammer applikationen i form af en token.

Det er som sådan en forudsætning at applikationen – såfremt man gemmer yderligere informationer i relation til brugeren – sikrer sig at der vitterlig er tale om præcis den samme bruger ved næste login. Til dette formål bør applikationen som absolut minimum gøre brug af uniqueAccountKey claim'en. Denne kan evt. suppleres med whenCreated og objectGUID.

Bemærk i øvrigt at indholdet af claims er præcis det samme uanset om applikationen anvender SAML 1.1 tokens (WS-Federation) eller SAML 2.0 tokens (SAML 2.0-protokollen). Der vil dog være forskel i syntaksen på OIOSAML-baserede claims jvf tidligere.

Tilkobling af applikationen til DMP's testmiljø

DMP har behov for et antal informationer for at kunne tilkoble en applikation. I første omgang vil tilkoblingen ske til testmiljøet.

Følgende informationer er nødvendige for at tilkoble en webapplikation:

- Applikationsnavn – Navnet på applikationen.
- Unikke URL'er – Applikationens URL'er (http-adresser). Her benyttes den URL, som applikationen bliver tilgået på.
- Et x509 certifikat uden private key – Applikationens certifikat, som bruges til at kryptere og dekryptere de SAML-tokens, som DMP's brugerstyring udsteder til applikationen. Certifikatet skal overleveres til DMP uden den private nøgle. Dvs. DMP skal kun have adgang til certifikatets public key-del.
- Optionelt Token signing-certifikat – Dette er som typisk ikke relevant for applikationer, idet det udelukkende finder anvendelse ved brug af andre STS'er eller når man anvender SAML

2.0-protokollen på applikationssiden. Dette er dog naturligvis relevant, såfremt applikationen er "gemt" bag ved en lokal STS.
- End point(s) – Angiver applikationens end point(s). Dette tager form af en eller flere URL'er (applikationens https-adresse) samt en angivelse af, hvilken protokol, der anvendes (SAML 2.0 eller WS-Federation).
- Secure hash algorithm – Kan p.t. enten være SHA-1 eller SHA-256. Det anbefales at der anvendes SHA-256, hvis muligt, idet dette giver en bedre sikkerhed.
- Claims – Fagsystemejeren vil skulle informere DMP om, hvilke claims applikationen er i stand til at konsumere. Dette sker lettest ved at oprette en ekstra kolonne i Excel-arket "DMP - Claims v2.0" og fremsende dette til DMP. Fagsystemejeren skal samtidig informere DMP om, hvorvidt applikationen er bygget til SAML 1.1 eller SAML 2.0 tokens (dvs. om der anvendes WS-Federation passive protokol eller SAML 2.0 passive protokol).

Følgende informationer er nødvendige for at tilkoble en Web Service:
- Applikationsnavn – Navnet på applikationen.
- Unikke identifier(s) – Applikationens URL'er (http-adresser). Her benyttes den URL, som applikationen bliver tilgået på[2].
- Et x509 certifikat uden private key – Applikationens certifikat, som bruges til at kryptere og dekryptere de SAML-tokens, som DMP's brugerstyring udsteder til applikationen. Certifikatet skal overleveres til DMP uden den private nøgle. Dvs. DMP skal kun have adgang til certifikatets public key-del.
- Optionelt Token signing-certifikat – Dette er som typisk ikke relevant for applikationer, idet det udelukkende finder anvendelse ved brug af andre STS'er. Dette er dog naturligvis relevant, såfremt applikationen er "gemt" bag ved en lokal STS.
- Secure hash algorithm – Kan p.t. enten være SHA-1 eller SHA-256. Det anbefales at der anvendes SHA-256, hvis muligt, idet dette giver en bedre sikkerhed.
- Claims – Fagsystemejeren vil skulle informere DMP om hvilke claims applikationen er i stand til at konsumere. Dette sker lettest ved at oprette en ekstra kolonne i Excel-arket "DMP - Claims v2.0" og fremsende dette til DMP. Fagsystemejeren skal samtidig informere DMP om, hvorvidt applikationen er bygget til SAML 1.1 eller SAML 2.0 tokens.
- STS Endpoint(s) – Angiver hvilke(n) af DMP's endpoints applikationen benytter (SAML tokens, Username (brugernavn/password) eller x509 klientcertifikat).

Fagsystemejeren vil desuden skulle informere DMP om hvorvidt man ønsker at få oprettet en testbruger på testmiljøet (samt hvad ønskerne til dettes navn er) samt om fagsystemejeren ønsker at kunne udføre føderalt login.

Såfremt fagsystemejeren ønsker at kunne teste føderalt login op mod applikationen vil det være nødvendigt at de tager initiativ til at få tilknyttet en IdP til testmiljøet. Til dette formål kan beskrivelserne for etablering af føderationsserver ("Introduktion til automatisk login mod Danmarks Miljøportal") anvendes. Den eneste afvigelse er at alle navne, der slutter med "miljoportal.dk" skal ændres til "test.miljoportal.dk".

DMP vil informere fagsystemejeren, når applikationen er oprettet på DMP's testmiljø.

[2] Såfremt der er behov for det er det dog også muligt at anvende URN'er, som den unikke id i forbindelse med web services.

Aftestning af applikationen mod DMP's testmiljø
Når applikationen er oprettet på DMP's testmiljø vil det være muligt for fagsystemejeren og evt. andre interessenter, der er tilknyttet testmiljøet, at afteste login mod denne.

I denne sammenhæng bør man sikre at der sker en aftestning af alle de primære loginscenarier for applikationen:

- Login via IdP i partnerorganisation.
- Login via IdP i partnerorganisation med angivelse af WHR-parameter.
- Direkte login i DMP.
- Direkte login i DMP med angivelse af WHR-parameter.

samt at man checker at alle de informationer (dvs. roller og attributter) bliver overført i claims – og behandlet og benyttet på korrekt vis – af applikationen.

Såfremt der er tale om en web service bør man endvidere tilsikre at der sker en aftestning med hvert af de end points, der skal kunne anvendes.

Tilkobling af applikationen til DMP's produktionsmiljø
DMP skal kontaktes, når fagsystemejeren finder tiden moden til at etablere applikationen i produktionsmiljøet.

Det er fagsystemejerens valg om applikationen skal overflyttes fra test til produktion (hvilket i givet fald betyder at DMP genbruger informationerne fra opkoblingen til testmiljøet og sletter applikationen fra testmiljøet) eller om fagsystemejeren får oprettet en ny version af applikationen i produktion. Det er DMP's anbefaling at fagsystemejeren har en version af applikationen tilkoblet DMP's testmiljø og produktionsmiljø, idet dette vil betyde at man har mulighed for at afteste applikationsopdateringer uden at brugerne vil opleve nedetid.

Såfremt fagsystemejeren opererer med en testversion og en produktionsversion af applikationen skal fagsystemejeren fremsende de tilsvarende informationer til DMP for produktionsversionen af applikationen (se afsnittet "Tilkobling af applikationen til DMP's testmiljø").

DMP vil informere fagsystemejeren, når applikationen er oprettet på DMP's produktionsmiljø.

Slutaftestning af applikationen mod DMP's produktionsmiljø
Når applikationen er oprettet på DMP's testmiljø vil det være muligt for fagsystemejeren og evt. andre interessenter, der er tilknyttet produktionsmiljøet, at afteste login mod denne.

I dette tilfælde bør man gennemløbe de samme testscenarier, som blev defineret til aftestningen af applikationen i testmiljøet.

Frigivelse af applikationen til drift
DMP skal informeres, når fagsystemejeren mener at tiden er moden til at sætte applikationen i drift.

Ift. servicevinduer og drift henvises til DMP's WSLA som ligger på
http://wiki.miljoeportal.dk/display/itarkitektur/Web+service+level+agreement