Introduktion til automatisk login mod Danmarks Miljøportal

Danmarks Miljøportal overgår i løbet af 2015 til en opgraderet version af den nuværende brugerstyringsløsning baseret på sammenhængende login (føderation), som betyder, at man nu bliver i stand til at opfylde kravene til de fællesoffentlige standarder.

Danmarks Miljøportal har siden midten af 2007 udbudt en løsning, der gør det muligt at udføre automatisk login fra partnerorganisationer. Med automatisk login menes at brugerne udstyret med de korrekte roller og rettigheder, oplever at de får direkte adgang til de ca. 50 applikationer, der p.t. er tilsluttet Danmarks Miljøportal på samme måde, som hvis der var tale om organisationens eget intranet eller lignende.

I dag er 35 ud af 125 partnerorganisationer[[1]](#footnote-1) opkoblet ved hjælp af denne løsning.

Løsningen til automatisk login er baseret på den såkaldte føderationsteknologi, nærmere bestemt WS-Federation protokollen og SAML 1.1 tokens. De fællesoffentlige standarder udsiger imidlertid at man skal anvende SAML 2.x-protokollen og SAML 2.x tokens.

Resten af dette dokument indeholder en beskrivelse af, hvordan en partnerorganisation etablerer automatisk login til den nye føderationsløsning hos Danmarks Miljøportal.

Det er nødvendigt at alle partnerorganisationer har tilendebragt overgangen til den nye føderationsløsning inden d. 15 januar. Er organisationen ikke overgået til den nye løsningen inden den nævnte dato risikerer organisationen at miste det automatiske login til alle applikationer og lokal administration af brugerne, idet Danmarks Miljøportal fra denne dato påbegynder overflytningen af de eksisterende applikationer til den nye føderationsløsning.

Indholdsfortegnelse

[Introduktion til dette dokument 3](#_Toc408899834)

[Design af IdP'en 3](#_Toc408899835)

[De centrale begreber og grundmæssigheder 3](#_Toc408899836)

[Vigtige pointer om designet af føderationsløsningen 3](#_Toc408899837)

[Valg af serverkonfiguration 4](#_Toc408899838)

[Valg af databaseløsning 5](#_Toc408899839)

[Det svære designvalg: Den helt korte version 6](#_Toc408899840)

[Krav 6](#_Toc408899841)

[ADFS 2.0 kan sagtens placeres på en virtuel server.Installation og konfigurering af IdP'en 6](#_Toc408899842)

[Forudsætninger for installationen 7](#_Toc408899843)

[Installation af AD FS 2.0 7](#_Toc408899844)

[Basal konfigurering af AD FS 2.0 13](#_Toc408899845)

[Evt. yderligere tilpasninger 19](#_Toc408899846)

[Validering af IdP'en 20](#_Toc408899847)

[Tilslutning af IdP'en til Danmarks Miljøportal 21](#_Toc408899848)

[Fejlfinding af føderationsløsningen 22](#_Toc408899849)

[Appendiks A: Aktivering af SSO til web services login på organisationens AD FS 2.x server 24](#_Toc408899850)

[Aktivering af endpoint til web services login 25](#_Toc408899851)

[Aktivering af kryptering på udstedte tokens 28](#_Toc408899852)

# Introduktion til dette dokument

Dette dokument beskriver, hvordan en partnerorganisation etablerer automatisk login (som undertiden også kaldes for fødereret login eller føderalt login) til Danmarks Miljøportal. Du kan finde en mere detaljeret beskrivelse af en løsning til automatisk login i notatet "Sammenhængende log-in: SSO til applikationer i et andet sikkerhedsdomæne", der er udarbejdet af IT- og Telestyrelsen.

Da størsteparten af vore partnerorganisationer anvender en it-infrastruktur, der er baseret på Microsoft Active Directory, har vi indsnævret behandlingen af tilkoblingen af Microsofts AD FS 2.x-produkt til dette scenarie. Eftersom føderationsløsningen – fortsat – er baseret på industristandarder, der supporteres bredt, er det naturligvis muligt at tilkoble partnerorganisationer, der anvender føderationsløsninger fra andre leverandører end Microsoft.

# Design af IdP'en

For at en partnerorganisation kan opnå automatisk login skal der opsættes en føderationsløsning lokalt hos denne.

Dette afsnit giver en kort introduktion til de vigtigste begreber og egenskaber ved føderationsløsninger og gennemgår de vigtigste designmæssige valg i relation til føderationsløsninger, der anvender Microsoft AD FS 2.0 eller AD FS 2.1 (Herefter nævnt som AD FS 2.x).

## De centrale begreber og grundmæssigheder

Partnerorganisationens føderationsserver benævnes typisk begrebsmæssigt som IdP'en (Identity Provider) eller CP'en (Claims Provider) eller slet og ret Account Partner'en, altsammen henviser til det faktum at det er partnerorganisationens føderationsserver, som holder styr på brugeridentiteter.

Danmarks Miljøportals føderationsløsning benævnes begrebsmæssigt som SP'en (Service Provider) eller RP'en (Relying Party), hvilket henviser til at det er her, de forskellige (applikations)tjenester bliver udbudt fra.

IdP'er og SP'er omtales under et som STS'er (Security Token Service), hvilket henviser til det faktum at de udsteder og konsumerer tokens.

## Vigtige pointer om designet af føderationsløsningen

Der er en række vigtige pointer omkring designet af partnerorganisationens føderationsløsning:

* Der er kun behov for at IdP'en er tilgængelig fra internettet, såfremt en eller flere af følgende krav er til stede:
  + Hvis brugerne skal kunne udføre login fra internettet (dvs. ikke blot på det interne net).

Dette kan være påkrævet, når hele eller dele af brugerskaren arbejder via internettet eller man blot ønsker at give brugerne adgang til login hele døgnet og ikke råder over VPN-opkoblinger, der kobler dem ind på organisationens interne net.

* + Hvis IdP'en også skal benyttes som SP for eksterne brugere.

Den installerede IDP kan opsættes til også at fungere som SP i relation til organisationens egne internetvendte applikationer.

* IdP'en og SP'en skal ikke kunne kommunikere direkte med hinanden - hverken under installation og konfiguration eller den efterfølgende drift.
  + IdP'en og SP'en behøver ikke at kunne "se" hinanden, da føderationsprotokollerne er bygget med det sigte, at al kommunikationen sker via den computer, som brugeren anvender. Dvs. det er brugerens computer, der skal have netværksmæssig adgang til IdP'en (samt de bagvedliggende directoryservere, som i vores tilfælde er Active Directory) og SP'en samt naturligvis de webapplikationer og web services, som brugeren ønsker at tilgå.
* IdP'en skal kunne kommunikere direkte med mindst en AD DC fra det domæne, som IdP-serveren er indmeldt i.
* Den føderale sikkerhedsmodel (dvs. IdP'en såvel som SP'en) bygger på udstedelse og brug af billetter (security tokens)[[2]](#footnote-2).

Som udgangspunkt anbefaler vi at man undgår at placere IdP'en på internettet, såfremt det er muligt, idet det kræver væsentligt mere arbejde og stille større krav til sikkerhedsopsætningerne (samt ikke mindst den løbende vedligeholdelse af samme). Det vil med andre ord som regel være markant dyrere i både investering og drift, at placere IdP'en ude på internettet, samtidig med at det naturligvis aldrig vil kunne blive nær så sikkert, som hvis IdP'en er placeret på det interne netværk.

## Valg af serverkonfiguration

Der er fire grundlæggende forskellige serverkonfigurationer, som er relevante i relation til partnerorganisationer, der har behov for at etablere en føderationstilslutning baseret på Microsoft AD FS 2.x op mod Danmarks Miljøportal:

* IdP – Består af en enkelt server med alt hvad det medfører af risiko i relation til nedetid og manglende skaleringsevne.
* Dubleret IdP – Består af to eller flere servere, der optræder som et samlet hele for at opnå det ønskede niveau af oppetid og skalerbarhed.
  + Bemærk at denne løsning forudsætter at der anvendes en eller anden form for load balancing på serverne (eller round robin DNS) således at requests bliver fordelt mellem serverne.
* IdP og proxy-IdP – Består af to (1 IdP og 1 proxy-IdP) servere. Proxy-IdP'en er bygget med henblik på benyttelse på DMZ-netværket og har som sådan en væsentlig reduceret angrebsflade relativt til IdP'en. Proxy-IdP'en er ikke brugbar i sig selv, idet den udelukkende agerer proxy for IdP'en for at opnå det nødvendige sikkerhedsmæssige niveau i løsningen, når IdP'en også skal være tilgængelig ude fra (dvs. fra internettet).
* Dubleret IdP og proxy-IdP – Består af fire (2 IdP'er og 2 proxy-IdP'er) eller flere servere, hvor proxy-IdP'erne og IdP'erne hver optræder som et samlet hele for at opnå det ønskede niveau af oppetid og skalerbarhed.
  + Bemærk at denne løsning forudsætter at der anvendes en eller anden form for load balancing på serverne (eller round robin DNS) således at requests bliver fordelt mellem serverne.

Samme IdP er i stand til at dække en hel Active Directory forest (og andre Active Directory forests, der måtte være tilknyttet ved hjælp af to-vejs Windows forest trusts).

*Bemærk at ovenstående forudsætter at partnerorganisationen ikke har behov for at optræde som en SP for egne applikationer nu eller fremover. Såfremt dette ikke er tilfældet anbefales partnerorganisationen at hente den nødvendige hjælp til designet af løsningskonfigurationen.*

## Valg af databaseløsning

AD FS 2.x giver mulighed for at vælge en af følgende to databasekonfigurationer:

* WID (Windows Integrated Database) – En neddroslet version af SQL Server, som er indbygget i Windows Server 2008 og senere versioner.
* Microsoft SQL Server – Microsofts databaseserver, som findes i et større antal varianter.

WID er klart den nemmeste (og billigste) løsning, da installationen er bygget til at køre fuldautomatisk igennem ved hjælp af nogle håndfulde overskuelige wizard-skærmbilleder.

Til gengæld er WID hæmmet af nogle væsentlige begrænsninger relativt til, hvis man anvender SQL Server:

* Databasen er gemt væk sådan at den ikke umiddelbart er tilgængelig til SQL queries og det kan eksempelvis også være en udfordring at tage backup af databasen.
* Når man vælger at AD FS 2.x skal kunne bestå af mere end en enkelt føderationsserver (den såkaldte farm mode), så bortfalder støtten af SAML token replay detection og SAML artifact resolution.
* Hvis den primære føderationsserver er nede, så vil hele systemet enten være nede (sker hvis AD FS 2.x er konfigureret til at køre i stand-alone mode eller i farm mode med kun en enkelt føderationsserver) eller også ikke det ikke være muligt at udføre nogen ændringer, førend den primære server er "oppe" igen eller en af de andre sekundære servere (farm mode) er blevet sat til at optræde som den primære server. Evt. sekundære føderationsservere (farm mode) vil naturligvis fortsætte med at svare på forespørgsler i hele forløbet.

Med hensyn til SQL Server står valget mellem følgende versioner:

* SQL Express Edition – Kræver ingen licens, men kan til gengæld kun benyttes på den lokale server. Dvs. denne løsning er i al praksis kun relevant, når føderationsløsningen består af en enkelt føderationsserver.
* SQL Standard Edition – Giver adgang til det fulde SQL Server-funktionalitetssæt, herunder flere muligheder for redundans.
* SQL Enterprise Edition – Giver adgang til alt hvad der er i Standard Edition samt en række high-end funktionaliteter, herunder muligheden for at benytte de mest avancerede former for redundans (mirroring).

Så længe føderationsløsningen kun består af en enkelt server kan man således snildt nøjes med SQL Express Edition. Men lige så snart man har behov for redundans i installationen vil det være nødvendigt at skifte op til SQL Standard Edition, medmindre man vælger WID.

## Det svære designvalg: Den helt korte version

Alt det ovenstående kan opsummeres til følgende mønstre:

* Hvis du er *helt* sikker på at du kun får behov for en enkelt IdP, så kan du nøjes med at vælge "Stand-alone federation server" (single instance mode) og du bør ligeledes anvende WID.
* Hvis du har behov for mere end en enkelt IdP (nu eller i fremtiden) på grund af hensynet til oppetid eller skalerbarhed, så skal du *altid* vælge en "Federation server farm" (farm mode).
  + Hvis du ikke har helt ekstreme krav til oppetid, skalerbarhed og SAML 2.x-sikkerhed kan du nøjes med at benytte WID som database.
  + Ellers er du nødt til at anvende SQL Server. Såfremt din installation i første omgang kun består af en enkelt føderationsserver kan du godt nøjes med SQL Server Express Edition, der ikke er licensbehæftet.

Det skal understreges at disse designvalg er vigtige, idet du vil være nødt til at reinstallere føderationsmiljøet fra grunden af, hvis du vælger forkert! Det er således ikke muligt at skifte fra WID til SQL Server eller omvendt samt opgradere fra "Stand-alone federation server" til "Federation server farm".

*Du kan finde en mere detaljeret gennemgang af designvalgene i Microsofts egen AD FS 2.0-dokumentation ("AD FS 2.0 Design Guide"), som p.t. er tilgængelig på http://technet.microsoft.com/en-us/library/dd807036(WS.10).aspx.*

## Krav

AD FS 2.x fungerer med alle versioner af Active Directory. Det er dog vigtigt at du er opmærksom på, at AD FS 2.x ikke er i stand til at mappe AD-grupper af typen domain local groups[[3]](#footnote-3).

AD FS 2.0 kan installeres på Windows Server 2008 og senere versioner af Windows Server. Den er kompatibel med SQL Server 2005 og SQL Server 2008.

AD FS 2.1 kan installeres på Windows Server 2012 og senere versioner af Windows Server. Den er kompatibel med SQL Server 2008 og SQL Server 2012.

Vi vil anbefale at du vælger den nyeste version af styresystemet (Windows Server 2012 R2) og SQL (SQL Server 2012), medmindre du har en god årsag til at gøre noget andet.

Det anbefales at AD FS 2.x placeres på en dedikeret server af sikkerheds- og stabilitetshensyn. Rent driftsmæssigt og kompetencemæssigt kan AD FS 2.x-serveren sidestilles som en webserver med store krav til sikkerheden og oppetiden.

# ADFS 2.0 kan sagtens placeres på en virtuel server.Installation og konfigurering af IdP'en

Dette afsnit gennemgår installationsforløbet for føderationsserveren (dvs. installationen af AD FS 2.0) til stand-alone federation server med WID-databasen.

AD FS 2.0 er som nævnt kompatibel med flere forskellige versioner af Windows Server. Denne installationsvejledning er skrevet ud fra at AD FS 2.0 kører på Windows Server 2008 R2, hvorfor der kan være mindre afvigelser, såfremt du anvender en anden version af Windows Server-styresystemet.

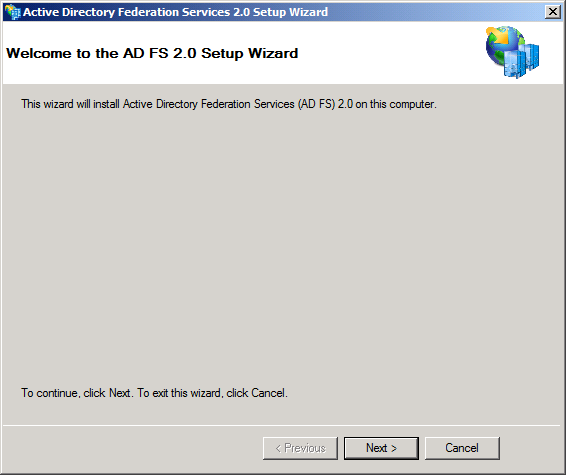
## Forudsætninger for installationen

Installationsvejledningen forudsætter at der allerede er et Active Directory til stede i partnerorganisationen samt at føderationsserveren allerede er installeret med Windows Server 2008 R2 og er join'et til partnerorganisationens Active Directory.

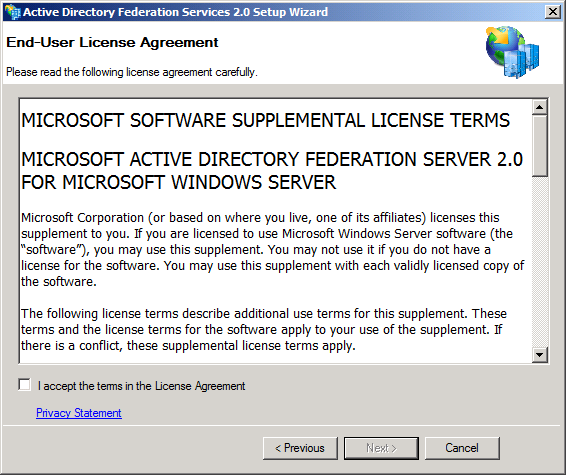
Der skal udstedes et SSL-certifikat[[4]](#footnote-4) til føderationsserveren, som bærer det navn, føderationsserveren er registreret som i DNS (fx login.testkommune.dk). Certifikatet skal naturligvis være accepteret som troværdigt af alle de computere (samt deres web browsere), der skal benytte IdP'en. Af hensyn til sikkerheden anbefales det at SSL-certifikatet anvender en nøglelængde på 4096 bits eller højere.

## Installation af AD FS 2.0

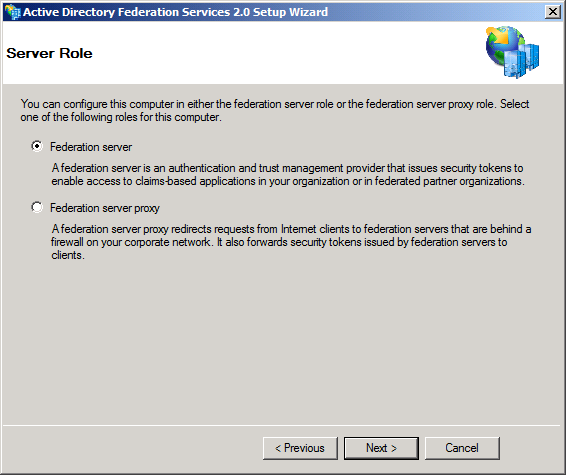
Start AdfsSetup



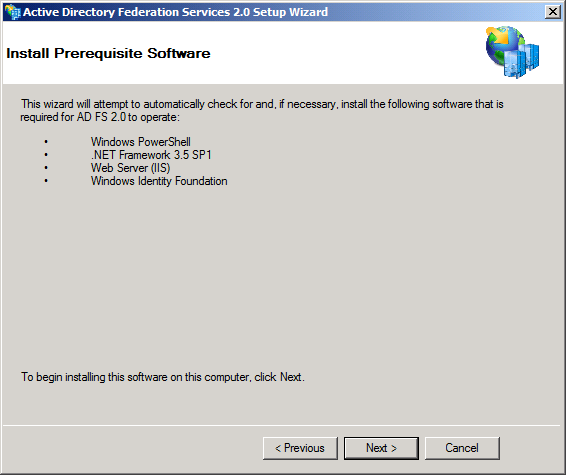
Tryk Next



Afkryds "I accept the terms in the License Agreement" og tryk Next.

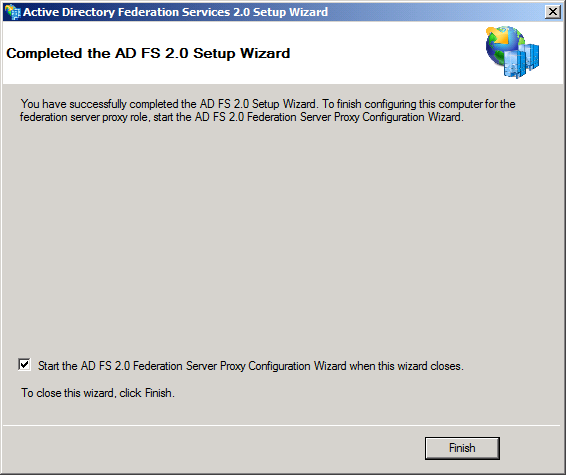
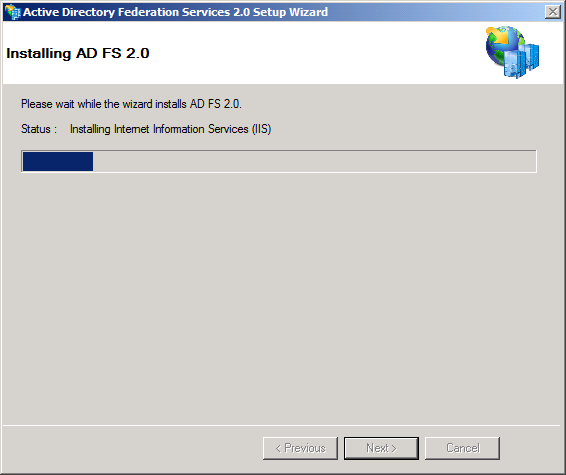


Tryk Next



Tryk Next

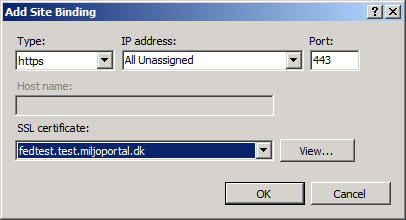
Afvent installationen gennemføres



Tryk Finish.

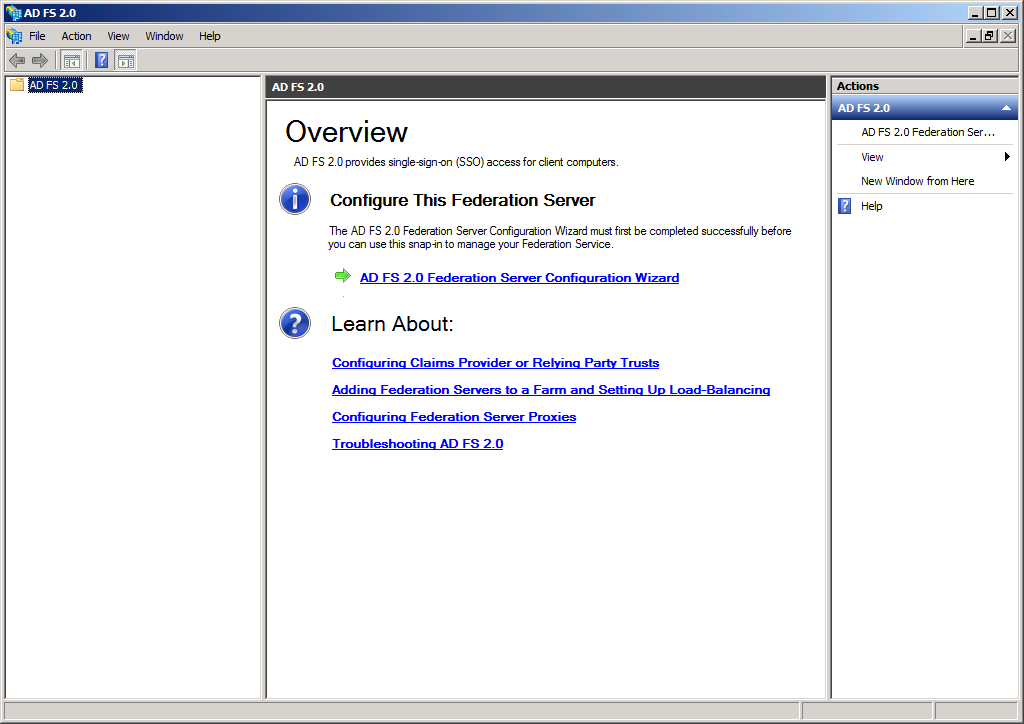
## Basal konfigurering af AD FS 2.0

Default Web Site på IIS konfigureres med SSL-certifikatet, som bærer det navn, føderationsserveren er registreret som i DNS (fx login.testkommune.dk). Dette sker ved at starte IIS Manager og vælge Default Web Site, trykke på Bindings.., trykke på Add.. og udfylde Add Site Binding på følgende vis (dog med navnet på det ønskede certifikat fremfor fedtest.test.miljoportal.dk).

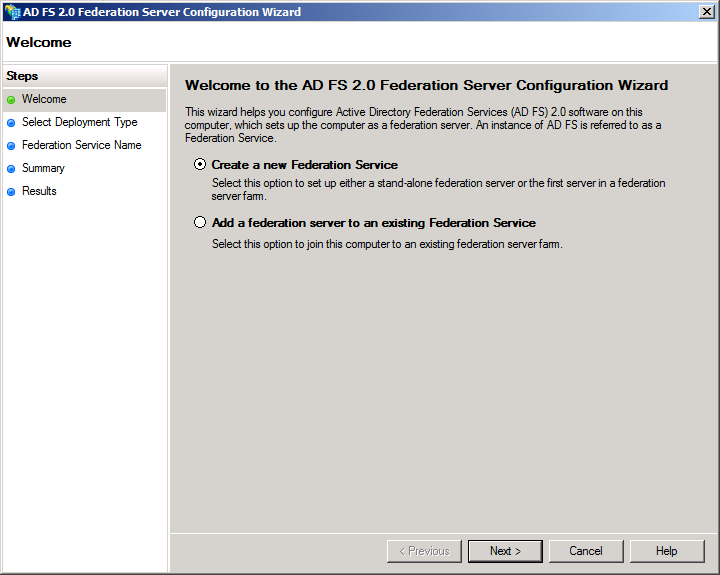


Tryk OK indtil ændringen er registreret og afslut IIS Manager.

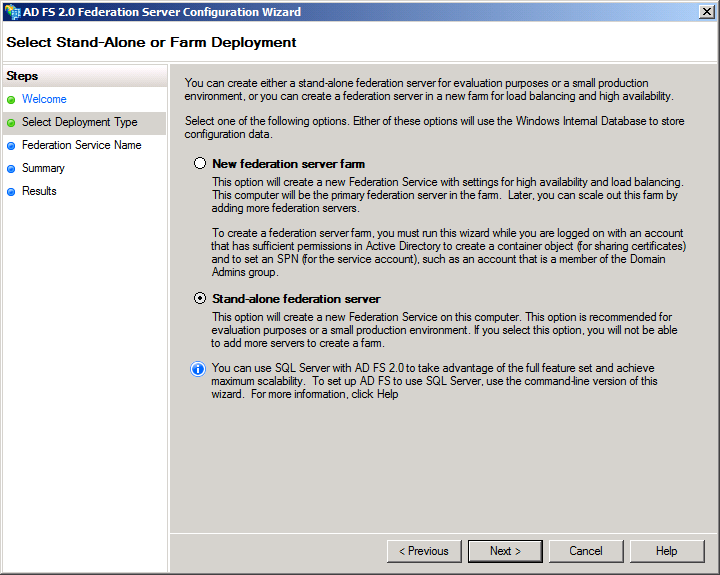
Start MMC-konsollen "AD FS 2.0 Management" (Administrative Tools).



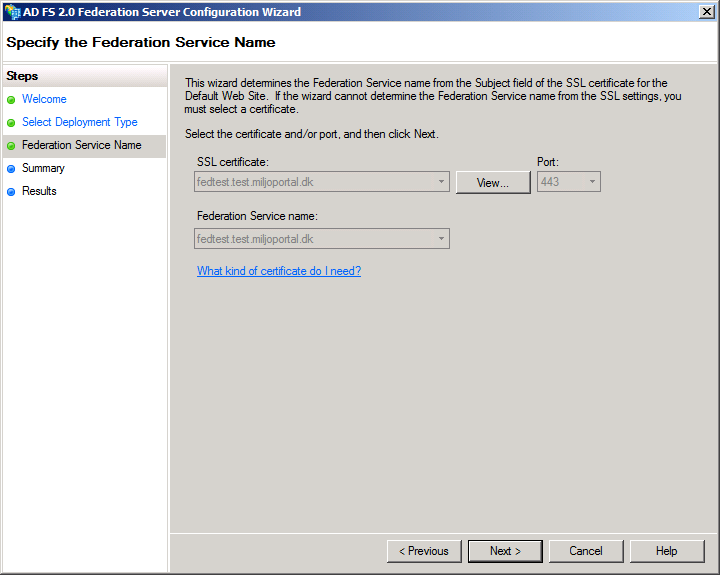
Tryk på "AD FS 2.0 Federation Server Configuration Wizard".



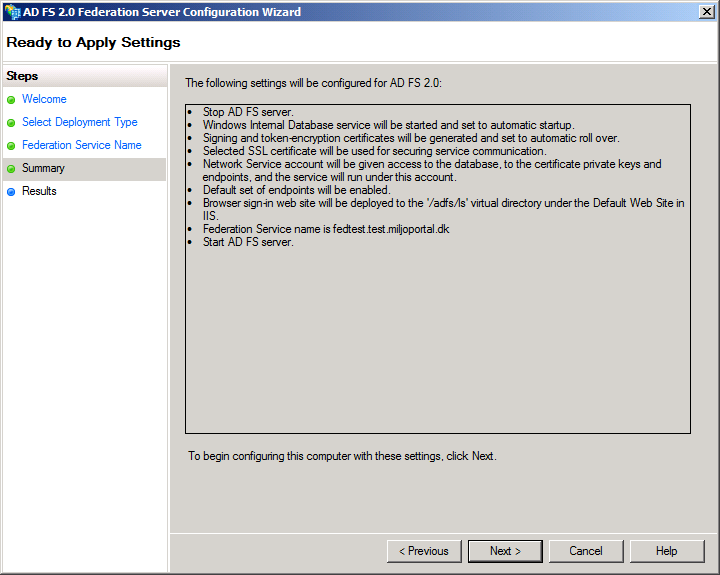
Tryk Next



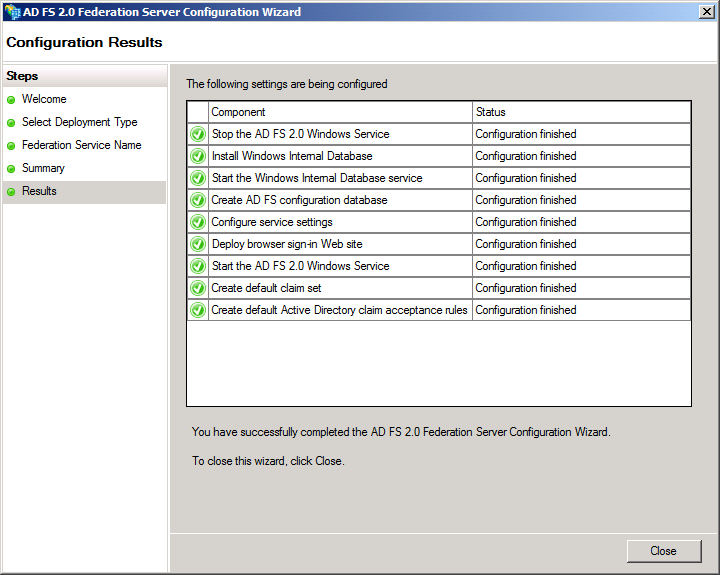
Vælg "Stand-alone federation server" og tryk Next



Tryk Next



Tryk Next



Tryk Close

## Evt. yderligere tilpasninger

Du bør slå Security Event Logging til:

* Vælg "Edit Federation Service Properties..." på roden i MMC-konsollen, vælg Events-fanebladet og sørg for at alle fem event typer er afkrydsede (dvs. tilføj afkrydsning ud for "Success audits" og "Failure audits").
* Husk ligeledes at checke at "Audit object access" er slået til i computerens Audit Policy. Ellers bliver der nemlig ikke logget noget i Security Event Log.

Det anbefales ligeledes at du udfylder organisationsinformationen:

* Vælg "Edit Federation Service Properties..." på roden i MMC-konsollen, vælg Organization-fanebladet, afkryds "Publish organization information in federation metadata" og udfyld de ønskede felter.

For den bedst mulige sikkerhed anbefales det at partnerorganisationen udsteder separate certifikater til service communications, token decrypting og token signing[[5]](#footnote-5). Du udskifter certifikaterne på følgende vis:

* Start PowerShell med Administrator-privilegier og skriv:
  + Add-PSSnapin Microsoft.Adfs.PowerShell (Ikke nødvendigt på AD FS 2.1)
  + Set-ADFSProperties -AutoCertificateRollover $false
* I AD FS 2.0 Management MMC-konsollen gøres følgende under AD FS 2.0|Service|Certificates:
* Udskiftning af Service Communications-certifikat – Tryk på "Set Service Communications Certificate" og vælg det nye certifikat.
* Udskiftning af Token Decrypting-certifikat – Tryk på "Add Token-Decrypting Certificate" og vælg det nye certifikat, sæt det nye certifikat til det primære certifikat ("Set as Primary") og slet det autooprettede certifikat ("Delete").
* Udskiftning af Token Signing-certifikat – Tryk på "Add Token-Signing Certificate" og vælg det nye certifikat, sæt det nye certifikat til det primære certifikat ("Set as Primary") og slet det autooprettede certifikat ("Delete").

Såfremt du ønsker at være helt compliant med OIOSAML-specifikationen skal du endvidere konfigurere en common domain cookie-funktionaliteten, hvilket håndtere ved at udfylde commonDomainCookie-elementet[[6]](#footnote-6) nede i web.config-filen.

## Validering af IdP'en

Du bør afslutningsvis gøre følgende for at validere at din AD FS 2.0-installation fungerer efter hensigten:

1. Check at AD FS 2.0-tjenesten er kørende – Start Services og check at "AD FS 2.0 Windows Services" har status "Started".
2. Check AD FS 2.0's Event Log – Start Event Viewer og check at indholdet i "AD FS 2.0 Eventing" (der er placeret under "Applications and Services Logs") ser nogenlunde fornuftigt ud. Dvs. at der ikke er nogen errors samt en Event ID 100, som fortæller at AD FS 2.0-tjenesten er startet korrekt op.
3. Check at du kan få et svar fra AD FS 20 – Start en web browser på en klient, der kan nå IdP'en og gå til webadressen https://<*serverens DNS-navn*>/adfs/fs/federationserverservice.asmx. Såfremt AD FS 2.0 fungerer korrekt vil du få et XML-dokument retur, som angiver IdP'ens opsætninger.
   1. Bemærk at dette skal gøres på en anden maskine end IdP'en. Det vil nemlig som regel **ikke** virke efter hensigten, hvis du benytter IdP'ens egen web-browser!

# Tilslutning af IdP'en til Danmarks Miljøportal

Tilslutningen af IdP'en til Danmarks Miljøportals SP sker på følgende måde:

1. Start en web browser på en klient, der kan nå IdP'en, gå ind på følgende webadresse https://<IdP'ens DNS-navn>/FederationMetadata/2007-06/FederationMetadata.xml og gem den resulterende XML-fil på disken. XML-filen sender du til din kontaktperson hos Danmarks MIljøportal.
2. Når Danmarks Miljøportal har oprettet din organisation på SP'en vil vi kvittere med importapplikationen og de nødvendige importfiler til samme samt en brugervejledning for dette.
3. *I perioden mellem den 1/1 2015 og frem til Danmarks Miljøportal har udfaset den gamle føderationsinstallation (hvilket forventes at ske pr. 1/4 2014) vil der skulle afvikles to forskellige importapplikationer, idet både Danmarks Miljøportals eksisterende ADFS 2.0-baserede SP og den fremtidige Safewhere\*Identify-baserede SP skal være oprettet på partnerorganisationens AD FS 2.0 IdP for at sikre at partnerorganisationen har adgang til automatisk login mod alle applikationerne.*

Når du har kørt importapplikationen jf. brugervejledningen vil dine brugere være i stand til at udføre automatisk login til alle de applikationer, der er tilknyttet Danmarks Miljøportal.

Du kan validere at dette er tilfældet – samt at du får overført alle de nødvendige informationer – ved at pege din web-browser hen på ClaimApp-testapplikationen som er placeret på webadressen https://administration.miljoeportal.dk/claimappweb/. Såfremt alt fungerer korrekt vil du få følgende skærmbillede tone frem på skærmen med de informationer, som IdP'en har overført for den pågældende bruger til Danmarks Miljøportal.

# Fejlfinding af føderationsløsningen

Såfremt du har fulgt anvisningerne i installationsvejledningen til punkt og prikke, så bør du stå med en fuldt funktionel AD FS 2.0-installation. Såfremt der er noget, der giver problemer på din IdP, så er det overvældende sandsynligt at det har noget med certifikaterne at gøre.

Erfaringen fra føderationsinstallationer tilsiger således at mere end 80% af alle fejl er relateret til certifikaterne. Procenttallet bør kun blive endnu mere overvældende i "certifikaternes favør" i vort tilfælde, hvor fejlmulighederne for installationen jo må siges at være rimeligt overskuelig.

De fleste problemer opstår dog ikke på føderationsserveren, men derimod i klientens brug af IdP'en. I den sammenhæng er de gængse problemer:

1. Klienten stoler ikke på SSL-certifikatet, der er installeret på IdP'en, SP'en (dvs. Danmarks Miljøportal) eller på applikationen – I Danmarks Miljøportals tilfælde anvender SP og applikationerne certifikater fra CA'er, der er accepterede af de gængse web-browsere og styresystemer, hvorfor du roligt kan gå ud fra at der er en fejlkonfigurering på klienten, hvis web-browseren melder om certifikatfejl i relation til disse.
2. Web-browseren udfører ikke automatisk login til IdP'en – Hvis du anvender en web-browser, der ikke automatisk er i stand til at overføre klientens Kerberos token til IdP'en vil du blive konfronteret med en logindialog hos IdP'en.
   1. Den eneste web-browser, der p.t. er i stand til at overføre et Kerberos token uden yderligere konfigurering, er Internet Explorer.
   2. Såfremt du har problemer med at få Internet Explorer til at udføre automatisk login skyldes det som regel at IdP'en ikke bliver opfattet som værende en del af ”Lokalt intranet”/”Local Intranet”. Det kan dog også skyldes at der er udført en anderledes konfigurering af zonernes sikkerhedsopsætninger for så vidt angår evnen til at udføre automatisk login.
3. Klienten nægter at overføre tokens til SP'en eller applikationen – Såfremt klienten ikke udfører automatisk login til applikationen, men der i stedet opstår en fejl, når web-browseren tilgår enten SP'en eller på applikationen, så vil det normalt skyldes at der går noget galt med hensyn til overførslen af cookies. Cookies bliver brugt ved overførsel af det token, IdP'en har udstedt, til SP'en og igen ved overførsel af det token, SP'en har udstedt, til applikationen.
   1. Såfremt du har problemer med at få Internet Explorer til at udføre automatisk login mod SP'en og/eller applikationen skyldes det som regel at de bliver opfattet som værende usikre (dvs. at de ikke er en del af ”Websteder, du har tillid til”/”Trusted Sites" eller en zone, der tillægges større tillid og dermed giver adgang til flere funktionalitet). Det kan dog også skyldes, at der er udført en anderledes konfigurering af cookie-opsætningerne eller zonernes sikkerhedsopsætninger på web-browseren.

*Bemærk at ovenstående observationer kan variere med styresystemets og web browserens opsætninger og/eller version. I forbindelse med Internet Explorer har det erfaringsmæssigt vist sig, at web-browserens opsætninger kan variere endog temmelig meget for at det automatiske login fungerer som ønsket. Så der er desværre ikke andet at sige end at du kan risikere at skulle forsøge dig lidt frem med hensyn til valg af internet-zone og evt. cookie-opsætning.*

Bemærk i øvrigt at det er "by design" at brugeren bliver spurgt om, hvilken IdP han eller hun kommer fra ved første login mod Danmarks Miljøportal. Såfremt klienten fungerer korrekt vil brugeren ikke blive stillet dette spørgsmål igen forløbig ved brug af samme pc, idet informationerne gemmes i en persistent cookie på pc'en.

Såfremt man ønsker at undgå at brugeren skal angive hvilken IdP han eller hun kommer fra er det muligt at angive en ekstra parameter ved kald til de fødererede applikationer. For at undgå at brugerne skal angive hvilken partnerorganisation, de kommer fra, skal følgende link benyttes for hver fødereret applikation:

*https://<applikationens URL>/?whr=<partnerorganisationens identifier[[7]](#footnote-7)>*

Fx: https://admin.mbsdk.dk/claimapp?whr=http://federation.naestvedkommune.dk/adfs/services/trust

Denne parameter kan således indbygges i links, der gøres tilgængelige for brugerne via favoritter eller genveje.

# Appendiks A: Aktivering af SSO til web services login på organisationens AD FS 2.x server

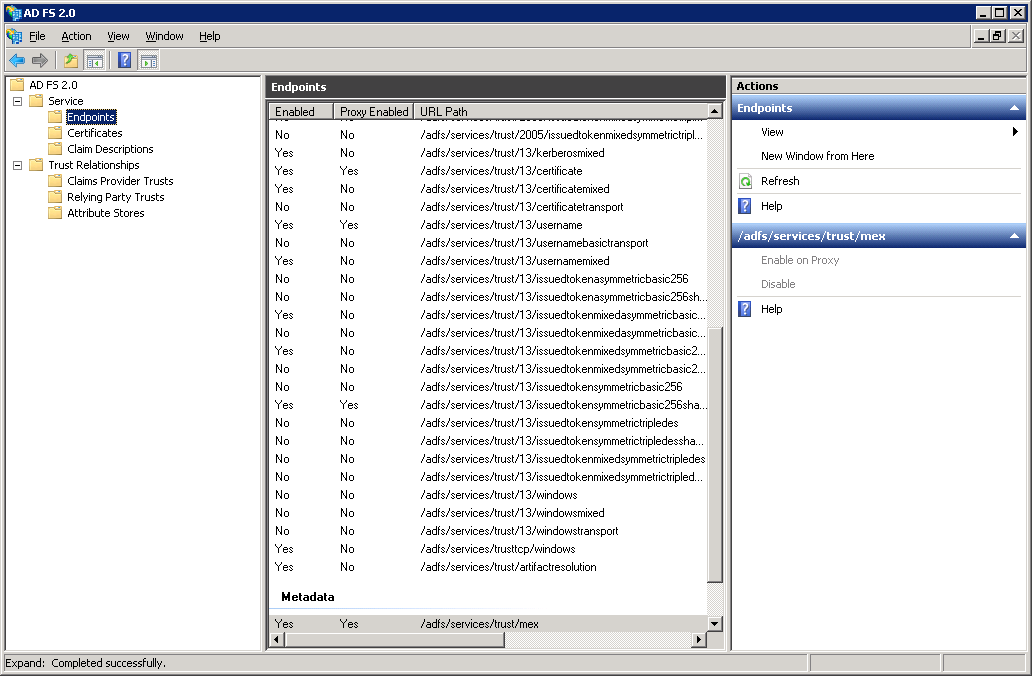
Brugen af SSO til web services kræver to ting på organisationens føderationsserver.

1. Aktivering af et konkret endpoint til web services login
2. Aktivering af kryptering på udstedte tokens

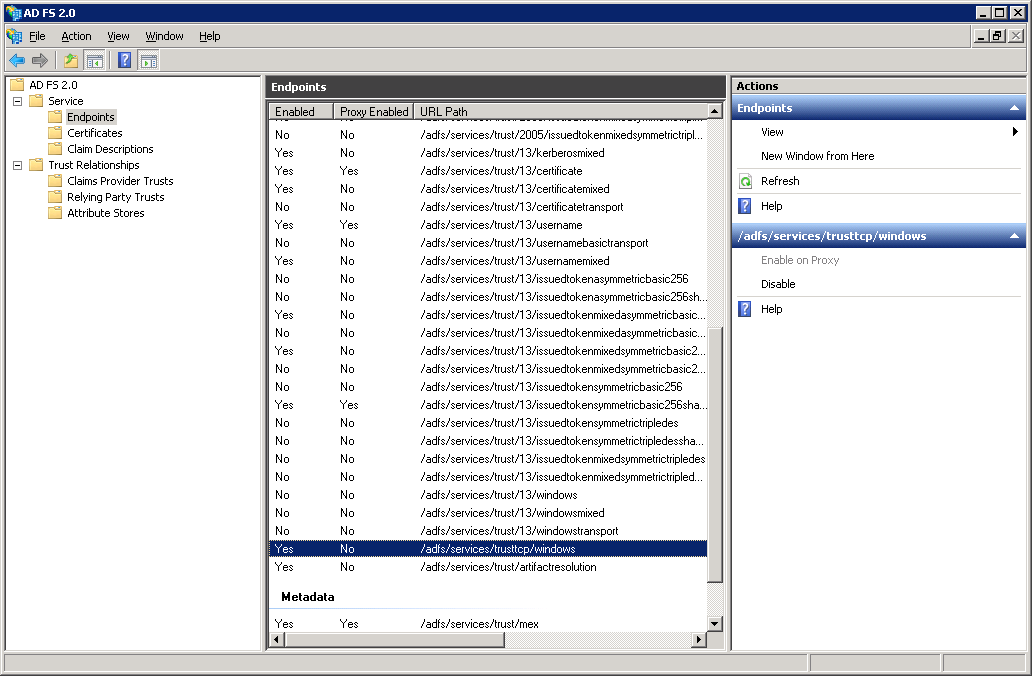
De følgende afsnit beskriver disse punkter i detaljer.

## Aktivering af endpoint til web services login

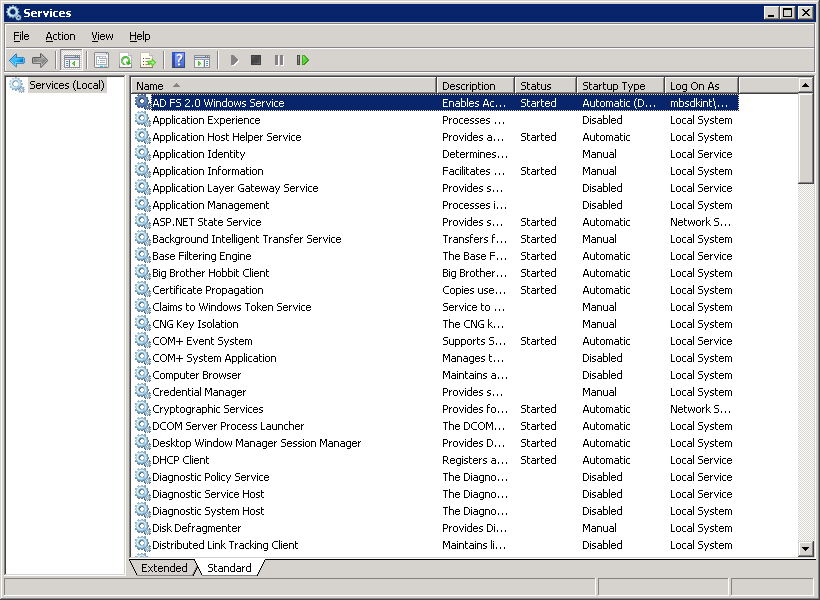
1. Fra AD FS 2.0 MMC’en markeres endpoints



1. Endpointet ”/adfs/services/trust/13/windows” findes i listen

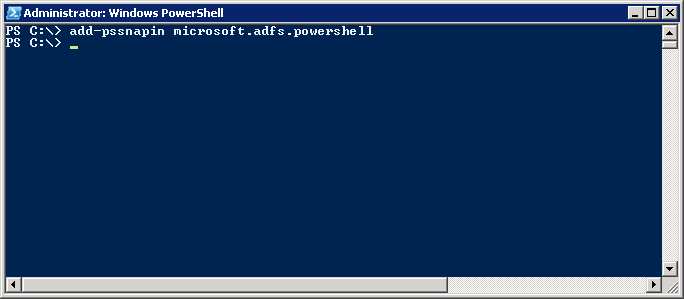


1. Endpointet skal stå til “Enabled”: Yes og “Proxy Enabled”: No. Dette ændres ved at højreklikke på endpointet og vælge Enable.
2. Genstart AD FS 2.x servicen



## Aktivering af kryptering på udstedte tokens

1. Åbn en powershell kommandoboks som administrator på serveren
2. Skriv følgende kommando “add-pssnapin microsoft.adfs.powershell” (Ikke nødvendigt på AD FS 2.1)



1. Skriv følgende kommandoer hver efterfulgt af enter.

set-adfsrelyingpartytrust -targetidentifier: ”https://log-in.test.miljoeportal.dk/runtime/” -EncryptClaims:$true

set-adfsrelyingpartytrust -targetidentifier: ” https://log-in.miljoeportal.dk/runtime/” -EncryptClaims:$true

1. En partnerorganisation er en organisation som via en underskrevet brugeradministrationsaftale har retten til at administrere organisationens brugeres adgang til systemerne som er koblet på brugerstyringen. [↑](#footnote-ref-1)
2. Billetten er et XML-dokument, som indeholder de informationer i og omkring brugeren, som anses for at være nødvendige og relevante for løsningen. Billetter sikres med brug af digitale certifikater (både signering og kryptering). De har i øvrigt en begrænset levetid. Levetiden bestemmes af udstederen. [↑](#footnote-ref-2)
3. Den tekniske årsag til denne begrænsning er, at Active Directory ikke er i stand til at slå domain local groups korrekt op, hvis de henhører til andre domæner og forests. [↑](#footnote-ref-3)
4. Windows Server er p.t. hæmmet af en bug i relation til styringen af adgangsrettigheder til private key-delen af certifikater på de nye CNG CSP'er, hvilket skyldes at private keys til denne CSP bliver gemt et andet sted i filsystemet end de "gamle" CryptoAPI-baserede certifikater. Indtil denne mangel bliver elimineret er I nødt til at undgå at benytte CNG CSP'en i forbindelse med certifikater til brug for AD FS 2.0. [↑](#footnote-ref-4)
5. Som absolut minimum bør du udskifte certifikaterne til token signing og token decrypting, idet disse certifikater – som bliver genereret pr. automatik under installationen af AD FS 2.0 – kun holder i et år fra installationsdatoen. Vi har desværre set rigtig mange timer blive spildt på troubleshooting af den type fejl gennem de seneste år, hvorfor vi anbefaler at disse certifikater udskiftes med nogen af længere varighed (som ideelt sét også har en eller anden alarmfunktion tilknyttet). [↑](#footnote-ref-5)
6. Se også http://msdn.microsoft.com/en-us/library/ee895366.aspx. [↑](#footnote-ref-6)
7. Medmindre du har ændret på standardopsætningen af Federation Service Properties, så vil partnerorganisationens identifier være "http://" efterfulgt af det DNS-navn, der er angivet i IdP'ens SSL-certifikat og afsluttet med "/adfs/services/trust". Hvis DNS-navnet er federation.naestvedkommune.dk vil identier'en således være "http://federation.naestvedkommune.dk/adfs/services/trust". [↑](#footnote-ref-7)