GLOBETEAM

Danmarks Miljøportal (DMP)

Vejledning til fagsystemejere omkring tilkobling af .NET4.5baseret web applikation

Version 1.4

-

Indledning

Denne vejledning beskriver hvordan man claims-enabler en .Net 4.5-baseret web applikation til brug med DMP's føderale brugerstyringsløsning ved brug af Microsoft Windows Identity Foundation (WIF) gennem det nu indbyggede System.IdentityModel.

Vejledningen skal læses i konteksten af den overordnede vejledning "Vejledning til fagsystemejere omkring forløbet for tilkobling af en applikation".

Vejledningen forudsætter at Microsoft Windows Identity Foundation (WIF) via .NET4.5 System.IdentityModel benyttes til claims-enabling af web applikationen. Denne vejledning er således ikke brugbar, såfremt man ønsker at anvende et andet API til claims-enabling af web applikationen.

Indhold

Indledning	2
Indhold	3
Forudsætninger for tilkobling af en .NET-baseret web applikation	4
WIF	4
.NET Framework 3.5 SP1	4
Certifikaterne er din største fejlkilde	4
Tilkoblingen af en .NET-baseret web applikation	4
Sådan kobles web applikationen op mod DMP	6
Trin 1: Anskaffelse af de nødvendige certifikater	6
Applikationens krypteringscertifikat	6
Trin 2: Konfiguration af webapplikations web.config-fil	6
Information omkring sikkerhedsrelateret logning	7
Step-by-step eksempel på tilkoblingen af de .NET-baserede samples	8
Appendiks A. Beskrivelse af web applikationens web.config-fil	17
Appendiks B. Brug af ActAs til at kalde en service på vegne af en bruger	18

Forudsætninger for tilkobling af en .NET-baseret web applikation

Såfremt de involverede .NET-udviklere ikke allerede er fortrolige med claims og claims-enabling af web applikationer på .NET-platformen kan det anbefales at studere Microsofts onlinebog "A Guide to Claims–based Identity and Access Control" fra Patterns & Practices-serien (http://msdn.microsoft.com/en-us/library/ff423674.aspx).

WIF

Som nævnt i indledningen er vejledningen bygget på en forudsætning om at claims-enablingen sker ved brug af Windows Identity Foundation (WIF).

WIF er en del af .NET 4.5 frameworket og tager form af System.IdentityModel og System.IdentityModel.Services namespace'ne.

WIF kan afvikles på Windows Server 2012 R2, Windows Server 2008 R2, Windows Server 2008 Service Pack 2, Windows 2003 SP2, Windows 7 og Windows Vista Service Pack 2. WIF til Windows 2008 forudsætter at der allerede er installeret IIS 7.0 og Microsoft .NET Framework 4.5 eller højere på platformen, mens WIF til Windows 2003 forudsætter at der er IIS 6.0 og Microsoft .NET Framework 4.5 eller højere på platformen.

Det er et krav at web applikationen er bygget i .Net 4.5 samt IIS 7.0 eller højere (dog IIS 6.0 ved anvendelse af Windows Server 2003).

ASP.NET 4.0 skal således være registreret i IIS.

Eftersom WIF ikke indeholder støtte af SAML 2.0-protokollen er det forøvrigt en implicit forudsætning at web applikationen benytter WS-Federation (og dermed SAML 1.1-tokens) til kommunikationen med DMP. Dette er dog ikke noget, der er synligt for hverken udvikleren eller brugerne, idet disse teknikaliteter er gemt nede bag WIF, lige bortset fra at enkelte claims ser en smule anderledes ud (det sidste ":" i SAML 2.0 claim'ens navn er erstattet med et "/" for at gøre claim'en kompatibel med SAML 1.1).

.NET Framework 4.5

Det er et krav at anvende mindst .NET Framework 4.5.

Certifikaterne er din største fejlkilde

Når man ser bort fra deciderede kodefejl i selve web applikationen, så er brugen og konfigureringen af certifikater den absolut største kilde til fejl i forbindelse med claims-enabling af en løsning.

Derfor anbefales det på det kraftigste at at udviklere såvel som infrastrukturfolk får "Appendix D: Digital Certificates" (http://msdn.microsoft.com/en-us/library/ff359106.aspx) som pligtlæsning, idet langt størsteparten af de fejl og problemer, der forekommer i relation til claims-enabling, viser sig at udspringe i og omkring certifikaterne.

Tilkoblingen af en .NET 4.5-baseret web applikation

Sikkerheden for Web Applikationer der bruger WS-Federation passive på DMPs Safewhere*Identify STS-løsning er baseret på følgende standarder:

- WS-Federation passive requestor profile

- Kombineret transport- og message-baseret sikkerhed (dvs. HTTPS-transport med message-baseret kryptering og signering af token'et) dvs. tokens er krypteret i http-beskederne.
- SAML 1.1 tokens

End points for DMP's STS er angivet nedenfor:

Passive log-in via WS-Federation passive

- https://log-in.miljoeportal.dk/runtime/ (produktionsmiljø)
- https://log-in.test.miljoeportal.dk/runtime/ (testmiljø)

Bemærk at samples'ne som udgangspunkt er bygget til brug med test miljøet. De vil dog naturligvis kunne tilpasses til at bruge produktionsystemet blot ved at udskifte URL'erne (og evt. certifikater) på end points'ne.

Det anbefales så vidt muligt, at udviklerne tager udgangspunkt i de medfølgende samples, når der oprettes nye web applikationer. De mange opsætningsmuligheder vil ellers hurtigt kunne risikere at gøre det til en uoverskuelig opgave at konfigurere det ovenstående i hånden.

Sådan kobles web applikationen op mod DMP

Der er to fysiske forudsætninger for tilkoblingen af en .NET-baseret web applikation.

1) Der skal foreligge et X.509 SSL-certifikat fra en offentlig CA. Dette X.509-certifikat skal benyttes til transport security på web applikationen (SSL)

2) Der skal foreligge endnu et X.509 SSL-certifikat fra en offentlig CA. Dette X.509-certifikat skal benyttes til kryptering af tokens til på web applikationen

Hver enkelt web applikation, der kobles op mod DMPs Safewhere*Identify STS skal således være udstyret med disse certifikater.

Trin 1: Anskaffelse af de nødvendige certifikater

Der skal erhverves to certifikater til hver web applikation:

- Et SSL certifikat. SSL certifikatet skal være udstedt til common name = applikationens url. Feks. cn=www.koreprovebooking.dk
- Et certifikat til kryptering af beskeder mellem DMP og web applikationen. Dette certifikat er ikke at forveksle med SSL certifikatet, idet certikatet benyttes til at gøre det muligt for STS'en at kryptere beskeder, som kun web applikationen kan læse.

Som nævnt i den overordnede vejledning ("Vejledning til fagsystemejere omkring forløbet for tilkobling af en applikation") skal encryption certifikatet overleveres til DMP uden den private nøgle. Dvs. DMP skal have certifikatets public key-del.

Applikationens krypteringscertifikat

Krypteringscertfikatet skal erhverves hos en offentlig og anerkendt CA. Vi anbefaler især http://www.godaddy.com, da de er godkendte i alle større browsere og er markant billigere end de store spillere såsom Verisign og Thawte. Vi anbefaler tilsvarende at dette erhverves som et almindeligt SSL-certifikat.

Det skal som nævnt ikke bruges til SSL, men SSL-certifikaterne er generelt billigst, og de dækker de behov et certifikat skal opfylde for at kunne benyttes som krypteringscertifikat. Modsat et certifikat der benyttes til SSL-trafik, så skal dette certifikat ikke være udstedt til et bestemt common name. Common name er ligegyldigt for krypteringscertifikatet. Vi anbefaler dog stadig, at der vælges et sigende common name for certifikatet (f.eks. CN=<applikationsnavn>-encryption.<organisationsnavn>.dk).

Trin 2: Konfiguration af webapplikations web.config-fil

Webapplikationens web.config-fil skal tilpasses på nogle få punkter før .NET-applikationen fungerer efter hensigten.

Det anbefales at web.config-filen tilpasses manuelt, som beskrevet i Appendiks A. Alternativt kan Microsofts FedUtil-værktøj benyttes, hvilket bliver beskrevet i Appendix C.

Trin 3: Tilpasning af global.asax

Det er endvidere påkrævet at udføre en lille ændring af global.asax-filen i relation til protected void Application_Start(object sender, EventArgs e).

Sektionen med protected void Application_Start(object sender, EventArgs e) skal helt præcist ændres til nedenstående i global.asax.cs-filen før applikationen kompileres:

protected void Application_Start(object sender, EventArgs e)

FederatedAuthentication.WSFederationAuthenticationModule.RedirectingToldentityProvider += new

EventHandler<RedirectingToldentityProviderEventArgs>(WSFederationAuthenticationModule_Red irectingToldentityProvider);

}
void WSFederationAuthenticationModule_RedirectingToldentityProvider(object sender,
RedirectingToldentityProviderEventArgs e)

```
{
    e.SignInRequestMessage.HomeRealm = Request.QueryString["whr"];
}
```

Tilretningen medfører at WIF altid videresender en evt. WHR-parameter til DMPs STS, hvilket betyder at brugerne har mulighed for at angive hvilken IdP de kommer fra og således sikre at de altid bliver redirect'et til denne.

Information omkring sikkerhedsrelateret logning

Claims er konsistente og valide repræsentationer af brugeren, der er logget ind via STS'en, som i vort tilfælde er DMP's føderale brugerstyring. Claims overføres til applikationen ved hjælp af sikre offentlige standarder, der garanterer for at overleveringen af claims til applikationen er sikker og pålidelig.

Hvis applikationen benytter sig af sikkerhedsrelateret logning kan brugerens claims således fint benyttes i denne sammenhæng. Der er med andre ord ikke nogen forskel på logning i et føderalt scenarie relativt til et traditionelt brugerlogin. Det er dog naturligvis vitalt at man tilsikrer at logningen som minimum indbefatter de claims, der sikrer at der kan ske en entydig identifikation af brugeren til et hvilke som helst senerekommende tidspunkt (dvs. logningen skal indbefatte en unik identifier såvel som de nødvendige informationer, der gør det muligt at finde tilbage til hvem denne unikke bruger var).

Step-by-step eksempel på tilkoblingen af de .NET-baserede samples

Følgende step-by-step guide tager udgangspunkt i de medfølgende samples i solution'en "DmpldentifyDotNetSamples.sln" og beskriver, hvordan du får sample .NET web applikationen op at køre lokalt og får logget ind i web applikationen.

Når disse trin er udført vil du have en kørende .NET-baseret web applikation), der rekvirerer et token fra DMPs Safewhere*Identify STS og logger ind og viser token'ets indhold i en webside.

1. Åbn solution'en i Visual Studio 2013.



2. Certifikatet "dotnetsamplewebapp-encryption.dk.pfx" (password: pw) installeres i Local Machine -> Personal.

🔚 Console1 - [Console Root\Certificates (Loca	l Computer)\Personal\Certificates]					
🚟 File Action View Favorites Window H	elp					_ 8 ×
Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friendly Name	Actions
🖃 🔂 Certificates (Local Computer)	and the state of t	100 11	and the second second	Descripting file lights.	- Thereit	Certificates
Personal	And a second sec	1000-10	10000000	free particular for the second	100000	Mara Astions
Certificates	and the second s	1000 (1)		the opposite the local	-	More Actions
Enterprise Trust	×		1110010		- Contraction	*.demo.miljoeportal.dk 🔺
Intermediate Certification Authorities	dotnetsamplewebapp-encryption.dk	Root Agency	1/1/2040	<aii></aii>	<none></none>	More Actions
🗉 🧮 Trusted Publishers	and the second s	Contraction Contraction of the		The second second	-	
Untrusted Certificates	and the second se	to ball, from loth and halfs	- and the second second	income the state of the state o		
Third-Party Root Certification Authorities	the light fam - build also be	the limited from a function state.		- 10-	And Designation of the	
Irusted People	and inside factors the Managers and	to hadde they in the Manter walk.	1111000		- Manager	
Bemote Deskton	and the again parties and last one	Nucl Agence	1111000		- Manual -	
Certificate Enrollment Requests	starting or our strengthered	Total Agency	1111000		- Manual -	
🗉 🧮 Smart Card Trusted Roots	second second second	That Approx	1111000		- Manager -	
🕀 🚞 Trusted Devices	property and addressed at the special	tagets that officialized in significant	1010100	100	Table to the set	
📧 🚞 Windows Live ID Token Issuer	and the second se		101000	the spinster of the		
	A CONTRACTOR OF A CONTRACTOR	1000 10		the opposite the locate.		
	And the second second second second	Contraction of the second				
	and the second s	and the second sec		-		
	and the second se	and the set of the set of				
	and south division framework from	the second parameters (so if			- Marcal	
	Character and a con-	Num manual	11111000		- Marcallo	
	Constant operation in the local diversity of	Number of Statements	10100000		- Hannes	
	search dates without more place of	to have been interested and	10100001	ter-e-indiana.	and descent	
	while does relies the storage	to half faces tellistic talls	12423801	ter-e-turberticale.	The second second	
	Second Country and	Fuel Agenci	111120000	100	- dependent	
	Provide and requiring the characteristic	to half these settlements.	1274220001	term totatement.	10010-0001-0001	
		to faile texas terminates rates		the on the second second	<u> </u>	
]•]					
Personal store contains 55 certificates.						

3. Certifikatet: "log-in.miljoeportal.dk signing.cer" og "log-in.test.miljoeportal.dk signing.cer" installeres i Local Machine -> Trusted People.

🚟 Console1 - [Console Root\Certificates (Loca	al Computer)\Trusted People\Certifi	icates]				
\overline Eile Action View Favorites Window H	elp					_ 8 >
Console Root	Issued To A	Issued By	Expiration Date	Intended Purposes	Friendly Name	Actions
🖃 🔜 Certificates (Local Computer)	grant ingen all studen it	are spin, all studen &		100	(Barney)	Certificates
Personal	derring all studen &	and there are students		-	(Base)	Maria Askinga
Invised Root Certification Authorities Foterprice Truct	- Margare - surveyor - the	all's couldres of	111000			More Actions
Intermediate Certification Authorities	The support of the second	and the second s		the plant of the		
Trusted Publishers	Property and the second second	ACCOUNT OF A COMPANY OF A				
🗉 🧮 Untrusted Certificates	A construction of the second s			ter a sufferingen .		
Third-Party Root Certification Authorities	Come and in the second second	the same and same and the same		and the second second	the state of	
Trusted People	Constructioned	1000-10	and the second s	Record States	- damage	
Certificates	Contract and the owner of the second	Total Institute	1111100000		- Manager	
Other People Remote Deskton	and half fam. I will also be	the least frage if the blocks had	our feature of		termater fam.	
Certificate Enrollment Requests	and the second territory and	to half fan i treffinger naft.	111100		- Manager	
	CONTRACTOR AND AND AND AND AND	Number of States	1111110		- Manager	
🛨 🧮 Trusted Devices	🔄 log-in.miljoeportal.dk Signing	log-in.miljoeportal.dk Signing	1/1/2026	<all></all>	<none></none>	
🗉 📔 Windows Live ID Token Issuer	🛱 log-in.test.miljoeportal.dk signing	log-in.test.miljoeportal.dk signing	12/31/2020	<all></all>	<none></none>	
	No. of the Association	100 (1)		period and approximate the	1000000	
	and the second s			constraints and stores.		
	And room there are been and	the state operation of the				
		the second se				
		In large large large large large		The second second		
	and the second second second second	in light from lastinger halfs	-	large automaticate		
	Contractor on otherspectral di	in light bear indicates halfs	- and the second second	ine or mathematicale		
	and the second second	New contents on	121112	- 180	- Marrier	
	where reside the second second	the cold transmission in th	10000000		The second same	
	and the second s	Wellow Australia	100000000		- Manager	
	<u> </u> • [Þ	
Trusted People store contains 26 certificates.						

4. Oprettelse af en application pool i IIS 7 ved navn "DMP Identify Samples".

Add Application Pool	? ×
<u>N</u> ame:	
DMP Identify Samples	
.NET Framework version:	
.NET Framework v4.0.30319	
Managed pipeline mode:	
Integrated 💌	
Start application pool immediately	
OK Cano	el

5. Application pool'ens bruger ændres til Network Service og Load User Profile sættes til True.

.NET Frame		
Enable 32-B	work Version	¥4.0
LINDUG JZ-L	Bit Applications	False
Managed Pi	ipeline Mode	Integrated
Name		DMP Identify Samples
Queue Leng	gth	1000
Start Auton	natically	True
3 CPU		
Limit		0
Limit Action		NoAction
Limit Interv	al (minutes)	5
Processor A	Affinity Enabled	False -
Processor A	Affinity Mask	4294967295
E Process M	lodel	
Identity		NetworkService
Idle Time-o	ut (minutes)	20
Load User P	Profile	True 🗾
Maximum W	/orker Processes	1
Ping Enable	d	True
Ping Maxim	um Response Time (seconc	90
Ping Period	(seconds)	30
Shutdown 1	Fime Limit (seconds)	90
Startun Tim	e Limit (seconds)	90

6. Der oprettes en applikation i IIS 7 ved navn "dotnetsamplewebapp". Denne skal pege ned på mappen "DotNetSamples.WebApp" i de medfølgende samples. Applikationen tildeles den nyoprettede application pool "DMP Identify Samples".

Add Application		? ×
Site name: Default Web Site		
Path: /		
<u>A</u> lias:	Application pool:	
dotnetsamplewebapp	DMP Identify Samples	S <u>e</u> lect
Example: sales		
Physical path:		
entiry Sample Apps(.ivet4.5(Dotive	Comples.webApp	
Pass-through authentication		
<u>C</u> onnect as Test Settings		
	ОК	Cancel

7. Network Service tildeles Read-rettighed til private key på dotnetsamplewebapp-encryption.dkcertifikatet (højreklik på certifikatet under Local Machine -> Personal og vælg All Tasks -> Manage Private Keys...).

Permissions for dotnetsamp	lewebapp-encry	yption.dk pr Þ
Security		
Group or user names:		
SYSTEM		
ANETWORK SERVICE		
Administrators (DEV\Adminis	trators)	
@3-1-3-3-0-130631		
	A <u>d</u> d	<u>R</u> emove
Permissions for NETWORK	· · ·	
SERVICE	Allow	Deny
Full control		
Read Special permissions		
Special permissions		
click Advanced.	ea seangs,	Ad <u>v</u> anced
Learn about access control and r	ermissions	
ОК	Cancel	Apply

8. Verificer, at der kører SSL (HTTPS) på web sitet ved at højreklikke på web sitet og vælge Edit bindings...:

ite Bindir	ngs				? >
Type	Host Name	Port	IP Address	Binding	<u>A</u> dd
https	localhost	443	*		Edit,
					<u>R</u> emove
					Browse
•				►	
					⊆lose

Såfremt der ikke kører SSL på web sitet kan du installere et testcertifikat via følgende guide: http://weblogs.asp.net/scottgu/archive/2007/04/06/tip-trick-enabling-ssl-on-iis7-using-self-signedcertificates.aspx

9. Kompiler løsningen og åbn din browser på https://localhost/dotnetsamplewebapp/. Du vil blive redirected til loginbilledet:

og-in.test.miljoeportal.dk/runtime/ldap/formsbas	edlogin.idp?ici_ci=k¥UE¥IDQcv48	j0PjUOO - Windows Internet E	plorer	
Me https://log-in.test.miljoeportal.dk/runtime/ldap/form	sbasedlogin.idp?ici_ci=kVUEVIDQcv48j0	PjUOOM7DKX67mI92% 🔎 🗾 🔒	🖹 🔄 🗙 🧯 miljoeportal.dk	×
Danmarks Miljøportal Data om miljøet i Danmark			Sådan logge	er du ind
	Indtast dit brugernavn Brugernavn Adgangskode Har du glemt din adgar	og adgangskode herunder. vnTest ••••••••••••••••••••••••••••••••••••		
KAN DU IKKE LOGGE IND? Det kan skyldes:			VEJLEDNINGER Generelle vejledninger	
 Din konto er blevet låst Du skal kontakte din lokale 			Læs om Brugeradministration	

Indtast brugernavn: vnTest og password: HejPANDAtest123! og tryk enter

10.Du bliver redirected tilbage til webapplikationen:

Attps://localhost/dotnetsamplewebapp/default.aspx - Windows Internet Ex	plorer 📃 🗋 🔀
C C F K https://localhost/dotnetsamplewebapp/default.aspx	P ▼ S Certificate error B 49 × G localhost × 10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
SAML 1.1 uid claim'en	
vnTest	
Alle claims	
ClaimType	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vnTest
http://schemas.microsoft.com/ws/2008/06/identity/authenticationme	thod http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password
http://schemas.microsoft.com/ws/2008/06/identity/authenticationins	tant 03-17-2015 06:41:55
urn:oid/0.9.2342.19200300.100.1.1	vnTest
http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Brugere
http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Offentlig
http://schemas.microsoft.com/ws/2008/06/identity/claims/role	00000001
http://schemas.microsoft.com/ws/2008/06/identity/claims/role	miljoe_natur_konsulent_kom
http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Domain Users

Appendiks A. Beskrivelse af webapplikationens web.config-fil

Dette appendix indeholder en uddybning af indholdet af web applikationens web.config-fil.

Bemærk at sektioner der ikke skal ændres for at bygge en ny webapplikation er udeladt af hensyn til overblikket.

```
<?xml version="1.0"?>
<configuration>
                                                                          Der angives webapplikationens
  <configSections>
    <section name="system.identityModel"</pre>
                                                                          præcise URL i audienceUris og
type="System.IdentityModel.Configuration.SystemIdentityModelSec
                                                                          under realm.
tion, System.IdentityModel, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=B77A5C561934E089" />
    <section name="system.identityModel.services"</pre>
type="System.IdentityModel.Services.Configuration.SystemIdentit
yModelServicesSection, System.IdentityModel.Services,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089" />
  </configSections>
  <system.identityModel>
    <identityConfiguration saveBootstrapContext="true">
      <audienceUris>
        <add value="https://localhost/dotnetsamplewebapp/" />
      </audienceUris>
      <issuerNameRegistry type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry,
System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089">
        <trustedIssuers>
          <!--log-in.test.miljoeportal.dk.cer-->
          <add thumbprint="<mark>c3ab04c6d018029443d90127290b48e0f021eef2</mark>" name="<mark>CN=log-in.test.miljoeportal.dk</mark>
signing" />
        </trustedIssuers>
      </issuerNameRegistry>
      </identityConfiguration>
  </system.identityModel>
  <system.identityModel.services>
    <federationConfiguration>
      <!--centraladmin-administration.test.miljoeportal.dk (Self Signed)-->
      <serviceCertificate>
        <certificateReference x509FindType="FindBySubjectName" findValue="dotnetsamplewebapp-encryption.dk"</pre>
storeLocation="LocalMachine" storeName="My"/>
      </serviceCertificate>
      <wsFederation passiveRedirectEnabled="true" issuer="https://log-</pre>
in.test.miljoeportal.dk/runtime/WSFederation/WSFederation.idp" realm="https://localhost/dotnetsamplewebapp/"
1>
      <cookieHandler requireSsl="true">
      </cookieHandler>
    </federationConfiguration>
  </system.identityModel.services>
```

</configuration>

Appendiks B. Brug af ActAs til at kalde en service på vegne af en bruger

Der henvises til vejledningen "DMP - Vejledning til fagsystemejere omkring tilkobling af .NETbaseret web service" for hvordan token et sendt til en web applikation bruges til kald til bagvedliggende services via ActAs.

Appendix C. Konfiguration af webapplikations web.config-fil ved hjælp af FedUtil

Webapplikationens web.config-fil skal som nævnt tidligere i dette dokument tilpasses på nogle få punkter før .NET-applikationen fungerer efter hensigten.

Det er som nævnt vores anbefaling at man gennemfører opgaven manuelt, da dette er en forholdsvis hurtig og nem operation (se Appendix A).

Alternativt kan man anvende værktøjet FedUtil, der er udviklet af Microsoft til formålet. FedUtil genererer imidlertid nogle meget store og komplekse web.config-filer, hvilket nedsætter læseligheden af web.config-filen ganske dramatisk.

For komplethedens skyld gennemgår vi dog brugen af FedUtil i dette appendix.

Konfigurering med FedUtil

WIF SDK'et (http://www.microsoft.com/downloads/details.aspx?FamilyID=c148b2df-c7af-46bb-9162-2c9422208504&displaylang=en) indeholder et værktøj ved navn FedUtil, som har til hensigt at gøre det lidt nemmere at gennemføre tilpasningen af web.config-filen end hvis man arbejder direkte i filen.

På første skærmbillede vælges web.config-filen og applikationens navn, hvis ikke det allerede fremgår af web.config-filen:

Welcome to the Federation	Utility wizard	
his wizard helps you to establish a trust r oken Service (STS).	relationship between a claims-aware application and a Security	y [
Application configuration location		
C:\inetpub\claimapp\Web.config	Brov	vse
(Example: c:\inetpub\wwwroot\applicat	tion 1\web.config)	
Application LIDI		
Application URI	app/	
Application URI https://admin.test.miljoeportal.dk/claima (Example: https://www.contoso.com/ap	app/ pplication1/)	<u>•</u>
Application URI https://admin.test.miljoeportal.dk/claima (Example: https://www.contoso.com/ap	app/ pplication1/)	×
Application URI https://admin.test.miljoeportal.dk/claima (Example: https://www.contoso.com/ap	app/ pplication1/)	<u>*</u>
Application URI https://admin.test.miljoeportal.dk/claima (Example: https://www.contoso.com/ap	app/ pplication1/)	

På andet skærmbillede vælges STS'en (dvs. DMP's føderale brugerstyring) og der angives dennes federation metadatafil (enten direkte eller indirekte ved hjælp af dets webadresse):

Select a Security Token Service (STS) ontion			
solder a sociality reven solvice (or sy option.			
⊂ No STS			
Enables claims programming model for the selected Service.	application. This op	tion does not req	uire a Security Token
C Create a new STS project in the current solution A new STS project will be added to the current solu- modified to frust and accept claims issued by this S'	tion. The selected a TS. This option is on	pplication's confi ly available throu	guration will be igh the 'Add STS
reference"menu item in Visual Studio.			
eference'menu item in Visual Studio. Use an existing STS			
 reference * menu item in Visual Studio. Use an existing STS The selected application's configuration will be mod STS. Specify the WS-Federation metadata docume 	ified to trust and acc nt location for the ex	cept the claims is visting STS.	sued by an existing
 reference*menu item in Visual Studio. Use an existing STS The selected application's configuration will be mod STS. Specify the WS-Federation metadata docume STS WS-Federation metadata document location 	ified to trust and acc nt location for the ex	cept the claims is kisting STS.	sued by an existing
 reference*menu item in Visual Studio. Use an existing STS The selected application's configuration will be mod STS. Specify the WS-Federation metadata docume STS WS-Federation metadata document location https://login.test.miljoepbrtal.dk./federationmetadata/ 	ified to trust and acc nt location for the ex 2007-01 B	cept the claims is kisting STS.	sued by an existing Test location
reference*menu item in Visual Studio. Use an existing STS The selected application's configuration will be mod STS. Specify the WS-Federation metadata docume STS WS-Federation metadata document location [https://login.test.miljoepbrtal.dk./federationmetadata/ (Example: https://fabrikam.com/FederationMetadata	ified to trust and acc nt location for the ex 2007-01 B /2007-06/Federatio	cept the claims is disting STS. rowse	sued by an existing Test location
reference*menu item in Visual Studio. © Use an existing STS The selected application's configuration will be mod STS. Specify the WS-Federation metadata document STS WS-Federation metadata document location STS WS-Federation metadata document location [https://login.test.miljoepbrtal.dk./federationmetadata/ (Example: https://fabrikam.com/FederationMetadata	ified to trust and acc nt location for the ex 2007-01 B /2007-06/Federatio	cept the claims is disting STS. rowse	sued by an existing Test location

På det tredje skærmbillede angives krypteringscertifikatet:

Security tokens issued by an STS can be	e encrypted. Select a security token	encryption option for your	14
application.			وا فيوا
C No encryption			
Security tokens issued by the STS will	I not be encrypted.		
Enable encryption			
Security tokens issued by the STS will Note: Make sure that the private key o which the application runs (example: N	I be encrypted by the selected certifi of this encryption certificate is acces Network Service).	cate. sible by the Windows identity	y under
Encryption Certificate			
C Generate a default certificate			
Select an existing certificate from state	ore		
CN-claimann test milioenostal dk		Select Certificat	e
Jerra-craimapp rest, miljoeportar.uk			
jerredamappitestimijoeportatur.			

På det fjerde skærmbillede fremvises de claims, som STS'en oplyser er til rådighed via dets federation metadata-fil (det er desværre ikke muligt at angive hvilke af disse claims, der skal benyttes af applikationen; dette kan kun ske ved at redigere i web.config-filen):

Following are the claims offered by the Security Token	Service.		
	4		
Claim Name	∠ Claim Type		
AD FS 1 x E-Mail Address	http://schemas.xmlsoap.org/claims/EmailAddress		
AD FS 1x UPN	http://schemas.xmlsoap.org/claims/UPN		
Authentication method	http://schemas.microsoft.com/ws/2008/06/identity/		
Authentication time stamp	http://schemas.microsoft.com/ws/2008/06/identity/		
Common Name	http://schemas.xmlsoap.org/claims/CommonName		
Deny only group SID	http://schemas.xmlsoap.org/ws/2005/05/identity/cl		
Deny only primary group SID	http://schemas.microsoft.com/ws/2008/06/identity/		
Deny only primary SID	http://schemas.microsoft.com/ws/2008/06/identity/		
E-Mail Address	http://schemas.xmlsoap.org/ws/2005/05/identity/cl		
By default, only name and role claims will be requested file to add/update your claims requirement.	by the application. Update your application's configuration		

På det femte skærmbillede opsummeres opsætningerne og der er mulighed for at tilvælge opsætningen af et job, der automatisk checker for evt. ændringer af STS'ens federation metadat-fil en gang i døgnet således at et evt. skift af token signing-certifikat også bliver automatisk ændret i applikationens web.config-fil:

Su	mmary			A
Revi your	ew the summary information below. Acce selection.	ept the settings by clicking	Finish", or click "Back" t	o modify
Арр	lication Information:	AV alation and a second		2
App	plication URI: https://admin.test.miljoepo	ntal.dk/claimapp/		
App	plication type: 'ASP NET web application	ntion"		
Sel	ected application certificate: 'CN=claiman	pp.test.miljoeportal.dk'		
Issu will n	uer name registry changes: Your applicati not modify your IssuerNameRegistry	ion is already configured wit	th a custom IssuerNam	eRegistry, FedUtil
Sec STS	S option: "Use an existing STS"			
Tru	s WS-Federation metadata document loc ust management	ration: https://lonin.teet.mil	inenntal dk (tederation	metadata/2007
Г	Schedule a task to perform daily WS-Fe	ederation metadata updates		
	If selected, FedUtil will create a task in metadata document every day at 12:00 are changes detected in the metadata	the Task Scheduler to silen) AM. This task will update document, such as signing	tly query the STS's W the application's config certificate changes.	S-Federation guration if there
e,				
		< Back	Finish	Cancel
		- DOON		