GLOBETEAM

Danmarks Miljøportal (DMP)

Vejledning til fagsystemejere omkring tilkobling af Java Metro-baseret web service

Version 1.2

Indledning

Denne vejledning beskriver, hvordan man tilkobler en Java-baseret web service (WS) til brug med DMP's føderale brugerstyringsløsning ved brug af Sun Metro.

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

Vejledningen forudsætter at Java Metro benyttes til claims-enabling af web service'n. Denne vejledning er således ikke brugbar, såfremt man ønsker at anvende et andet API til claims-enabling af web services.

Indhold

Forudsætninger for tilkobling af en Java-baseret web service og web services klienter

Udviklingen af Java-baserede web services og web services klienter forudsætter et godt kendskab til Java (herunder Java Web). Det må endvidere anbefales at der hersker en god forståelse for Netbeans og evt. Metro/Glassfish.

For mere information om disse teknologier henvises der til:
https://metro.java.net/2.3/
http://download.java.net/glassfish/4.0/release/glassfish-4.0.zip
http://download.netbeans.org/netbeans/8.0/final/bundles/netbeans-8.0-windows.exe
~~https://metro.dev.java.net/2.0.1/~~
~~https://glassfish.dev.java.net/downloads/3.0.1-final.html~~
~~http://netbeans.org/community/releases/69/~~

Field Code Changed

De praktiske krav

Det er valideret at det er muligt at tilkoble en Java-baseret WS med brug af Metro version 2.~~0.1~~3, Glassfish version ~~3.0.1~~4.0 og Netbeans version 8.0~~6.9~~. Erfaringen tilsiger at dette ikke udgør nogen garanti i relation til andre versioner end de nævnte, hvorfor det anbefales at benyttes disse versioner indtil anden information måtte fremkomme.

Bemærk: Hvis du udvikler Java-baserede Web Services klienter er kravet i skrivende stund Metro 2.~~1~~ 3 (dvs. 2.01 vil IKKE virke) i seneste promoted build:
http://java.net/projects/metro/downloads/directory/promoted

Metro 2.~~1~~ 3 leveres automatisk med den seneste promoted version af Glassfish i version ~~3~~4.0~~1~~:
http://dlc.sun.com.edgesuite.net/glassfish/4.0/promoted/
~~http://dlc.sun.com.edgesuite.net/glassfish/3.1/promoted/~~

Der kræves ligeledes, at Java Cryptography Extensions er installeret på serveren eller klienten som anvender services.
http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html

Vejledningen til at koble web services op mod DMP er den samme om man vælger Glassfish ~~3.1~~4.0 og Metro 2.3~~1~~.

Det udviklede Java WS sample er naturligvis baseret på ovennævnte versioner.

Certifikaterne er din største fejlkilde

Når man ser bort fra deciderede kodefejl i selve WS'en og WS-klienten, 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 er meget omhyggelige på denne kant, 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 Java-baseret WS

Sikkerheden for Web Services på DMPs ~~AD FS 2.0~~Idenitfy STS-løsning er baseret på følgende standarder:

- WS-Trust 1.3
- Message-baseret sikkerhed (dvs. HTTP-transport med message-baseret kryptering og signering)
- SAML 1.1 eller SAML 2.0 tokens. Det skal aftales i forvejen med DMP, hvilken type tokens, der anvendes.
- Der anvendes symmetriske nøgler til kryptering
- Key size er 256
- Algorithm suite er Basic256
- Security Header Layout er Lax
- Der kan autentificeres med ~~AD FS~~STS'en med User Name. Brugernavn og adgangskode skal mappe op mod en bruger oprettet i Danmarks Miljøportals administratorløsning
- Der kan autentificeres mod AD FS'en med x509. X509 certifikatet skal udstedes af DMP og mappe op mod en bruger oprettet i Danmarks Miljøportals administratorløsning
- Der anvendes ikke service certificate negotiation mod ~~AD FS 2.0~~Identify STS'en
- Der er frit valg om der anvendes service certificate negotation mod Web Services
- Der er frit valg om der anvendes Secure Conversation mod Web Services. Bemærk dog at for Java er det deaktiveret i samples pga dårlig kompatibilitet mellem .NET og Java, når det kommer til Secure Conversation. Det anbefales således at undgå Secure Conversation indtil videre.

End points for DMP's STS er angivet nedenfor:

User name authentication

- http://log-in.miljoeportal.dk/~~adfs~~runtime/services/trust/~~13~~14/username (produktionsmiljø)
- http://log-in.test.miljoeportal.dk/~~/~~runtime~~adfs~~/services/trust/~~13~~14/username (testmiljø)

Field Code Changed

Field Code Changed

X509 authentication

- http://log-in.miljoeportal.dk/~~adfs~~runtime/services/trust/~~13~~14/certificate (produktionsmiljø)
- http://log-in.test.miljoeportal.dk/~~adfs~~runtime/services/trust/~~13~~14/certificate (testmiljø)

Field Code Changed

Field Code Changed

MEX

- https://log-in.miljoeportal.dk/~~adfs~~runtime/services/trust/mex (produktionsmiljø)
- https://log-in.test.miljoeportal.dk/~~adfs~~runtime/services/trust/mex (testmiljø)

Field Code Changed

Field Code Changed

Bemærk at samples'ne som udgangspunkt er bygget til brug med ~~produktionssystemet~~testsystemet. De vil dog naturligvis kunne tilpasses til at bruge ~~testsystemet~~ produktionssystemet 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 WS'er. De mange opsætningsmuligheder i Java vil ellers hurtigt kunne risikere at gøre det til en uoverskuelig opgave at konfigurere alt det ovenstående i hånden.

Sådan kobles WS'en op mod DMP

Der er kun en enkelt fysisk forudsætning for tilkoblingen af en Java-baseret web service. Der skal foreligge et X.509-certifikat fra en offentlig CA. Dette X.509-certifikat skal benyttes til encryption på WS'en.

Hver enkelt web service, der kobles op mod DMPs ~~AD FS 2.0~~Identify STS skal således være udstyret med et sådant unikt certifikat.

Hvis der benyttes x509 til også at autentificere mod ~~AD FS 2.0~~Identify STS'en kræver det dog tillige at der er udstedt et certifikat fra DMPs egen PKI.

Trin 1: Anskaffelse af det nødvendige certifikat

Der skal erhverves et certifikat til hver WS:

- Et certifikat til kryptering af beskeder mellem DMP og web servicen. 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 servicen kan læse.

Som nævnt i vejledningen: "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 WS'en

Konfigurationen af WS'en til brug op mod DMPs STS er beskrevet i næste afsnit.

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).

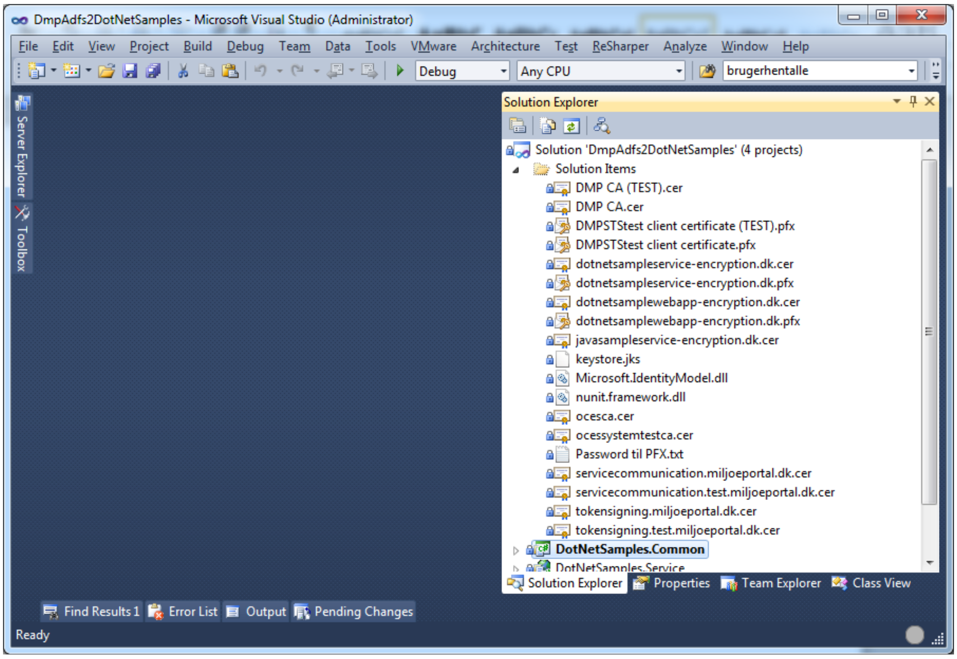
Step-by-step eksempel på tilkoblingen af en Java-baseret WS

Følgende step-by-step guide beskriver, hvordan du opsætter og konfigurerer en Metro-baseret Web Service, der er baseret på Netbeans.

Beskrivelsen tager delvist udgangspunkt i den .Net-baserede solution (~~DmpAdfs2DotNetSamples~~DmpIdentifyDotNetSamples.sln), der er udarbejdet til brug for vejledningen omkring tilkobling af en .Net-baseret web service, i og med at den benytter den .Net-baserede web service-klient fremfor at rumme en Java-baseret WS-klient. Java servicen skal bygges fra bunden i denne step-by-step guide for at garantere at servicen bliver korrekt bagt ind i Glassfish web serveren.

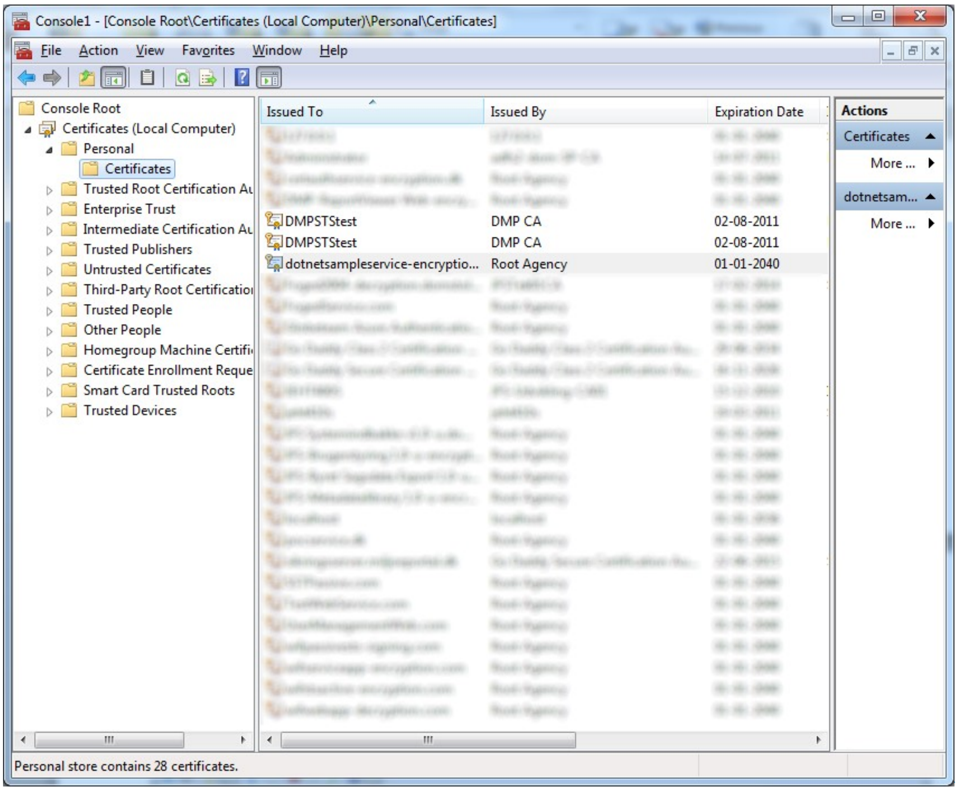
Når disse trin er udført vil du have en kørende Java Metro-baseret Web Service på din egen maskine samt en .NET unit test (dvs. i al praksis en minimal WS-klient), der rekvirerer et token fra DMPs ~~AD FS 2.0~~Identify STS og påhæfter det et kald til Java WS'en.

1. Åbn solution'en i Visual Studio 2010


DmpAdfs2DotNetSamples - Microsoft Visual Studio (Administrator)
File Edit View Project Build Debug Team Data Tools VMware Architecture Test ReSharper Analyze Window Help
Debug
Any CPU
brugerhentalle
Server Explorer
Toolbox
Solution Explorer
Solution Explorer
Properties
Team Explorer
Class View
Find Results 1
Error List
Output
Pending Changes
Ready

Solution 'DmpAdfs2DotNetSamples' (4 projects)
Solution Items
DMP CA (TEST).cer
DMP CA.cer
DMPSTStest client certificate (TEST).pfx
DMPSTStest client certificate.pfx
dotnetsampleservice-encryption.dk.cer
dotnetsampleservice-encryption.dk.pfx
dotnetsamplewebapp-encryption.dk.cer
dotnetsamplewebapp-encryption.dk.pfx
javasampleservice-encryption.dk.cer
keystore.jks
Microsoft.IdentityModel.dll
nunit.framework.dll
ocesca.cer
ocessystemtestca.cer
Password til PFX.txt
servicecommunication.miljoeportal.dk.cer
servicecommunication.test.miljoeportal.dk.cer
tokensigning.miljoeportal.dk.cer
tokensigning.test.miljoeportal.dk.cer
DotNetSamples.Common
DotNetSamples.Service

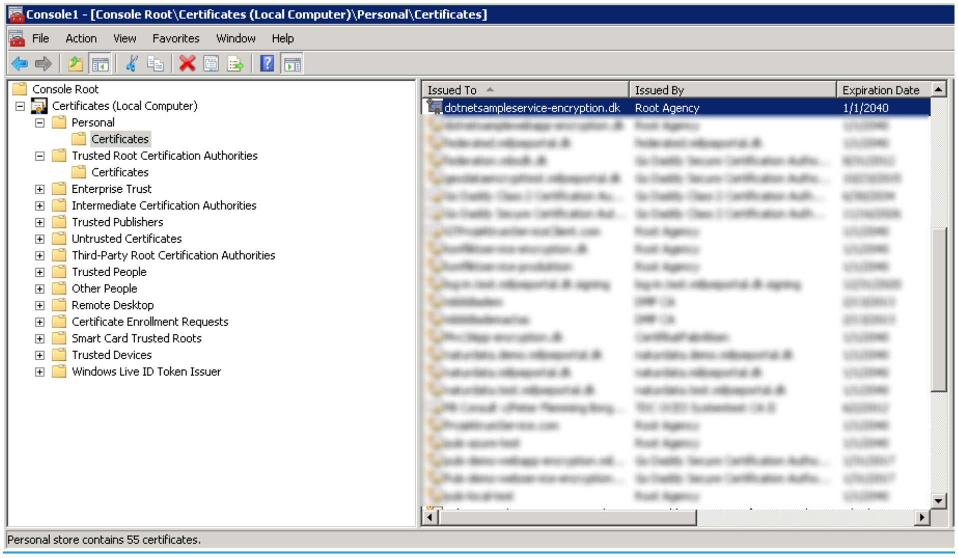
2. Certifikaterne “dotnetsampleservice-encryption.dk.pfx”~~, “DMPSTStest client certificate.pfx”~~ (password: pw) ~~og “DMPSTStest client certificate (TEST).pfx“ (password: pw)~~ installeres i Local Machine -> Personal:



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Other People
Homegroup Machine Certifi
Certificate Enrollment Reque
Smart Card Trusted Roots
Trusted Devices
Actions
Certificates
More ...
dotnetsam...
More ...

Issued To	Issued By	Expiration Date
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
DMPSTStest	DMP CA	02-08-2011
DMPSTStest	DMP CA	02-08-2011
dotnetsampleservice-encryptio...	Root Agency	01-01-2040
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Personal store contains 28 certificates.

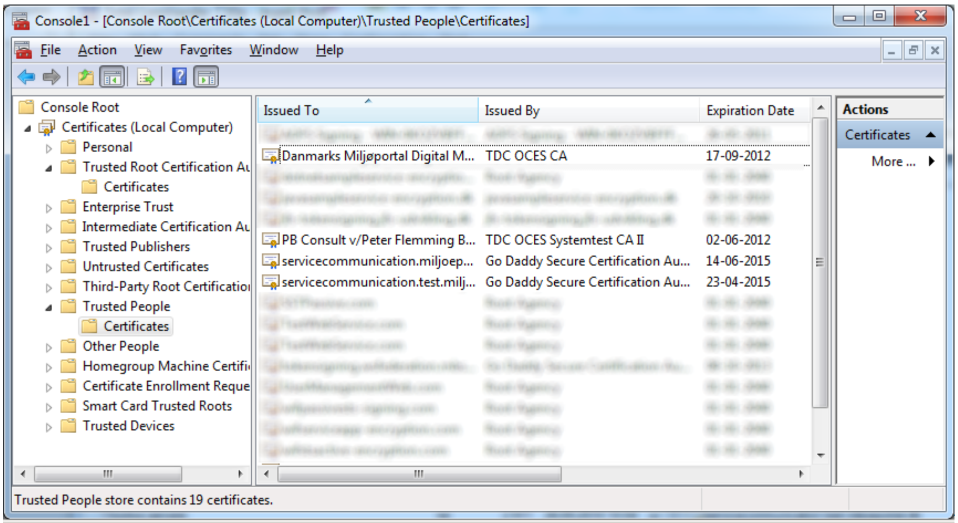

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Other People
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - Trusted Devices
    - Windows Live ID Token Issuer

Issued To	Issued By	Expiration Date
dotnetsampleservice-encryption.dk	Root Agency	1/1/2040

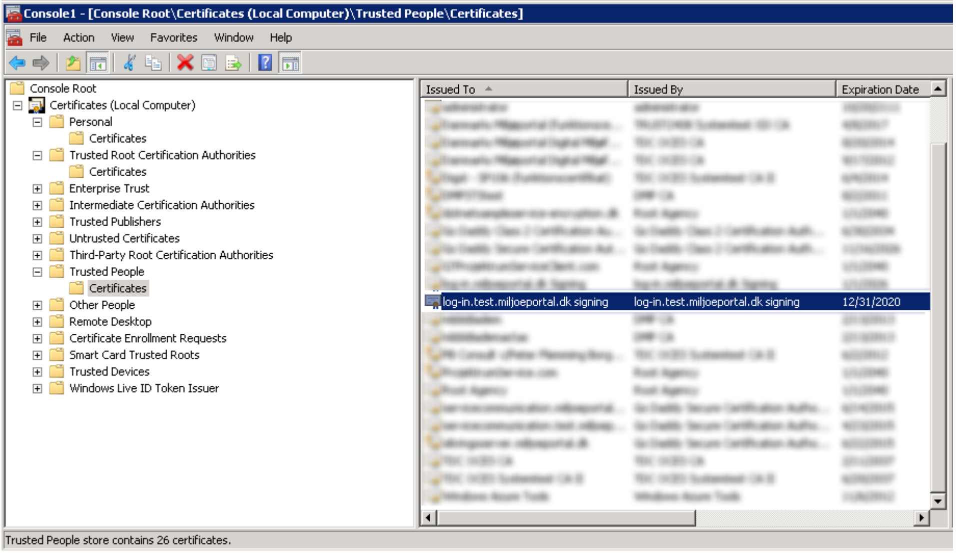
Personal store contains 55 certificates.

3. Certifikaterne: "~~servicecommunication.miljoeportal.dk.cer~~log-in.test.miljoeportal.dk signing.cer"~~, "tokensigning.miljoeportal.dk.cer", "servicecommunication .test.miljoeportal.dk.cer" og "tokensigning.test.miljoeportal.dk.cer" ~~ installeres i Local Machine -> Trusted People


Console1 - [Console Root\Certificates (Local Computer)\Trusted People\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Certificates
Other People
Homegroup Machine Certifi
Certificate Enrollment Reque
Smart Card Trusted Roots
Trusted Devices
Actions
Certificates
More ...

Issued To	Issued By	Expiration Date
Danmarks Miljøportal Digital M...	TDC OCES CA	17-09-2012
PB Consult v/Peter Flemming B...	TDC OCES Systemtest CA II	02-06-2012
servicecommunication.miljoep...	Go Daddy Secure Certification Au...	14-06-2015
servicecommunication.test.milj...	Go Daddy Secure Certification Au...	23-04-2015

Trusted People store contains 19 certificates.


Console1 - [Console Root\Certificates (Local Computer)\Trusted People\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificates
Other People
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer

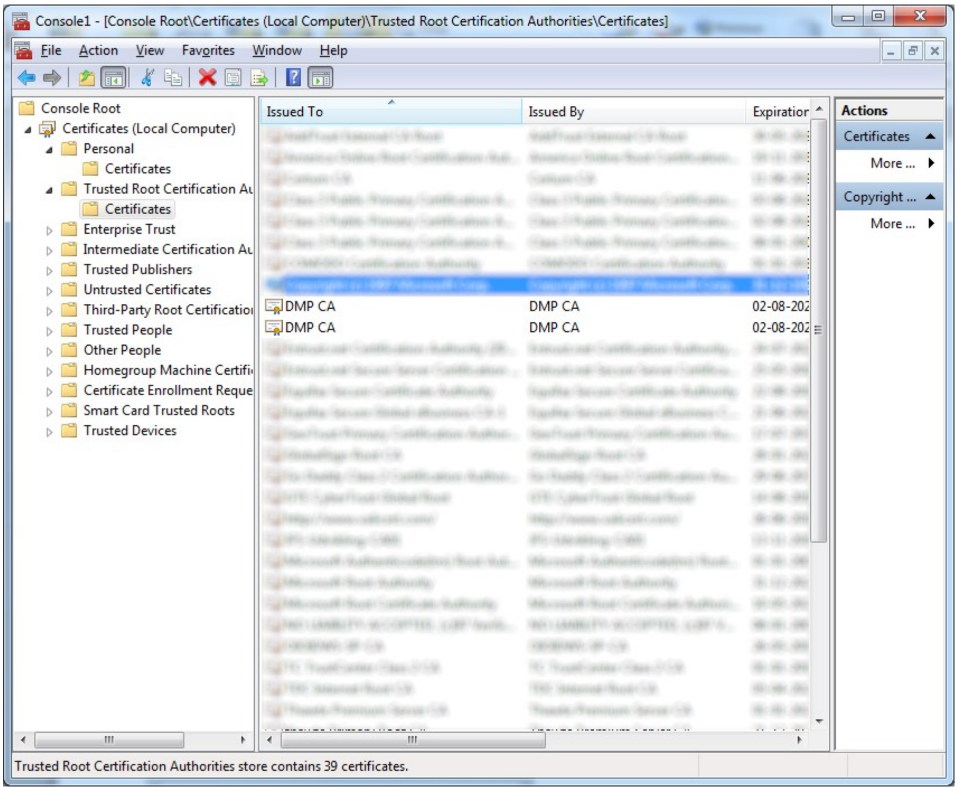
Issued To	Issued By	Expiration Date
log-in.test.miljoeportal.dk signing	log-in.test.miljoeportal.dk signing	12/31/2020

Trusted People store contains 26 certificates.

Formatted: Danish

4. Certifikaterne ”DMP CA.cer~~” og ”DMP CA (TEST).cer”~~ ” installeres i Local Computer -> Trusted Root Certification Authorities:

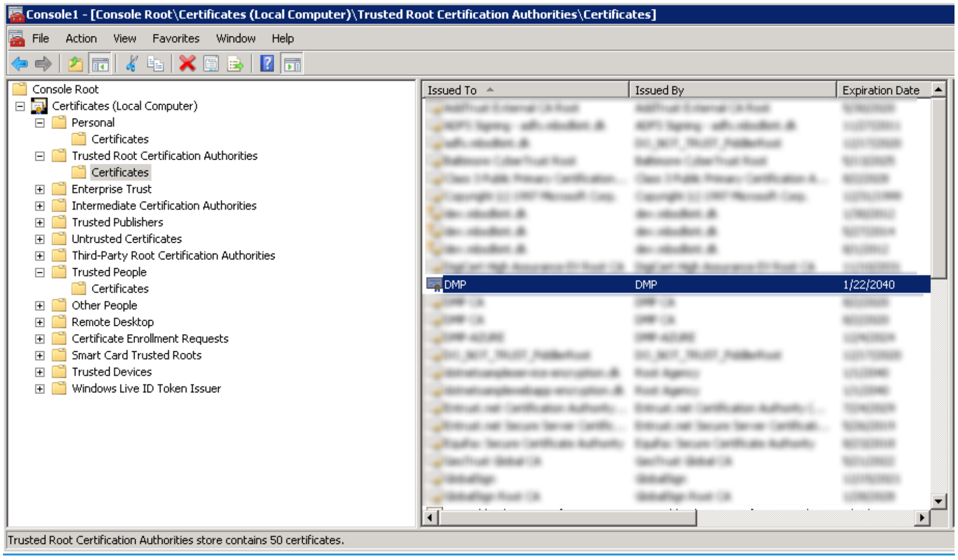
Formatted: English (United States)



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Other People
Homegroup Machine Certifi
Certificate Enrollment Reque
Smart Card Trusted Roots
Trusted Devices
Actions
Certificates
More ...
Copyright ...
More ...

Issued To	Issued By	Expiration
DMP CA	DMP CA	02-08-202
DMP CA	DMP CA	02-08-202

Trusted Root Certification Authorities store contains 39 certificates.

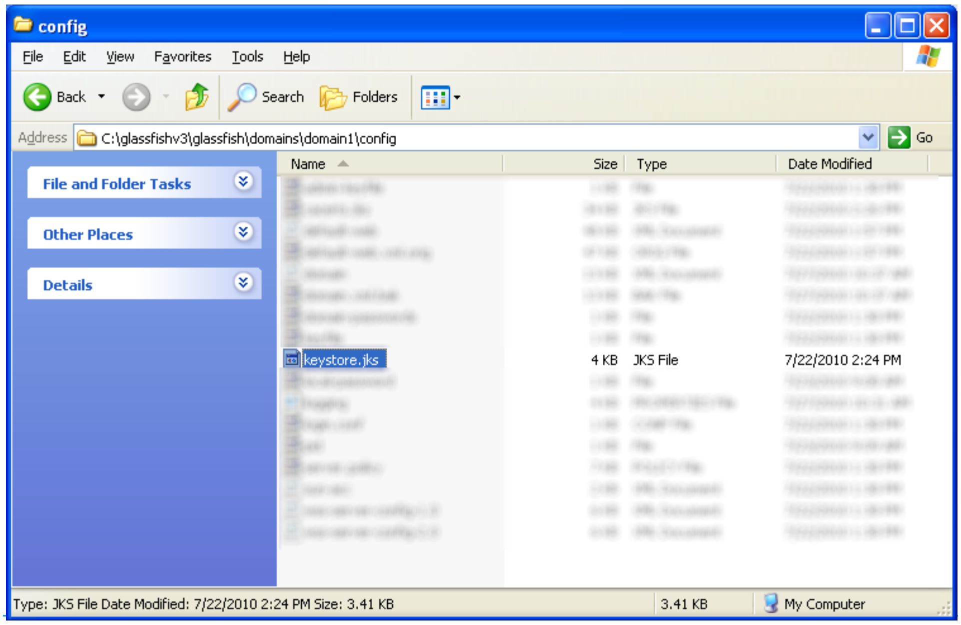

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
      - Certificates
    - Other People
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - Trusted Devices
    - Windows Live ID Token Issuer

Issued To	Issued By	Expiration Date
[redacted]	[redacted]	[redacted]
DMP	DMP	1/22/2040
[redacted]	[redacted]	[redacted]

Trusted Root Certification Authorities store contains 50 certificates.

5. sample~~K~~keystore.jks-filen kopieres til default domænet i Glassfish. I dette eksempel bruger vi ”domain1”. Denne fil indeholder det certifikat med private key som web servicen skal bruge.

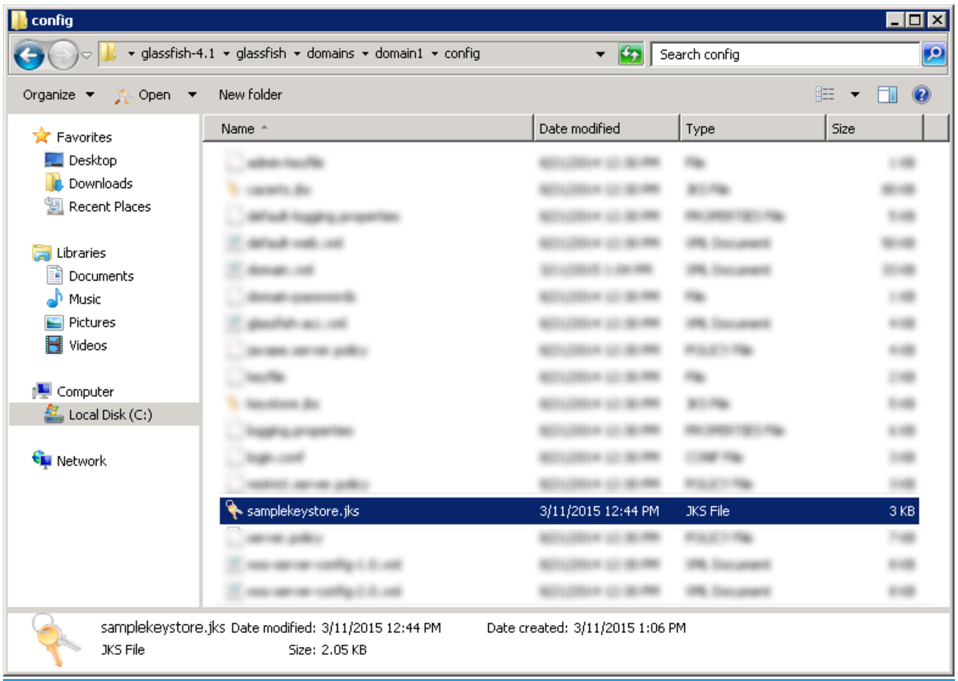


C:\glassfishv3\glassfish\domains\domain1\config

Name	Size	Type	Date Modified
keystore.jks	4 KB	JKS File	7/22/2010 2:24 PM

Type: JKS File Date Modified: 7/22/2010 2:24 PM Size: 3.41 KB 3.41 KB My Computer

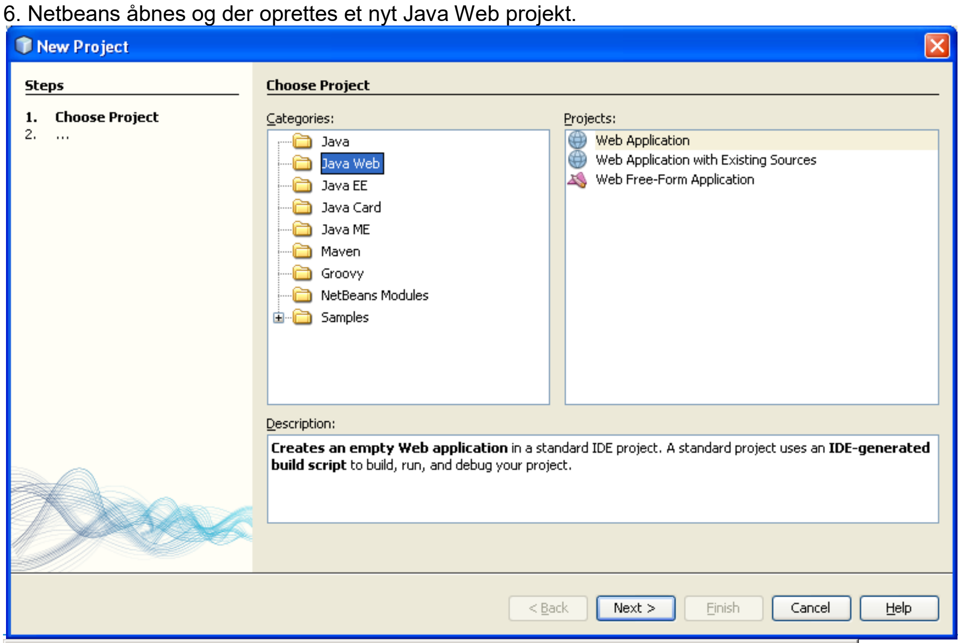
Formatted: Danish



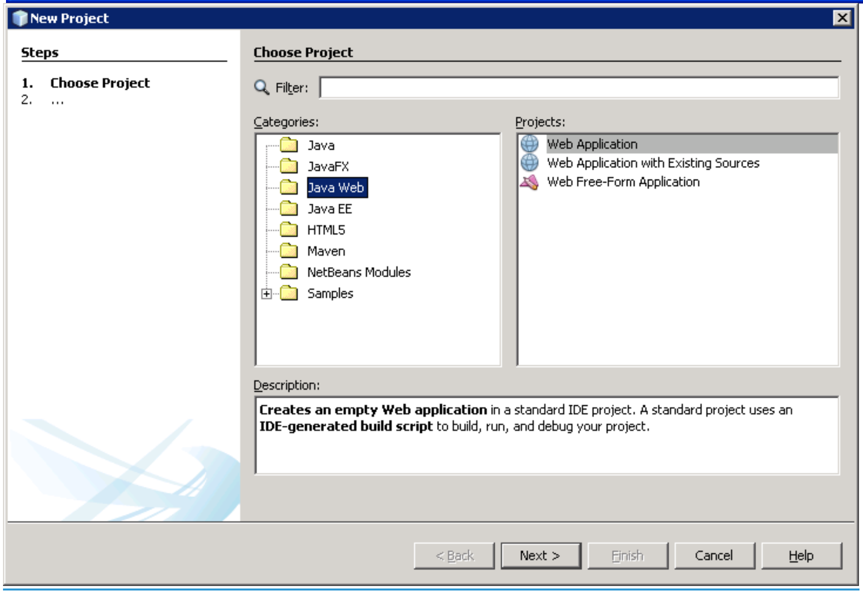
Name	Date modified	Type	Size
[redacted]	[redacted]	[redacted]	[redacted]
samplekeystore.jks	3/11/2015 12:44 PM	JKS File	3 KB
[redacted]	[redacted]	[redacted]	[redacted]

samplekeystore.jks Date modified: 3/11/2015 12:44 PM Date created: 3/11/2015 1:06 PM
JKS File Size: 2.05 KB

6. Netbeans åbnes og der oprettes et nyt Java Web projekt.

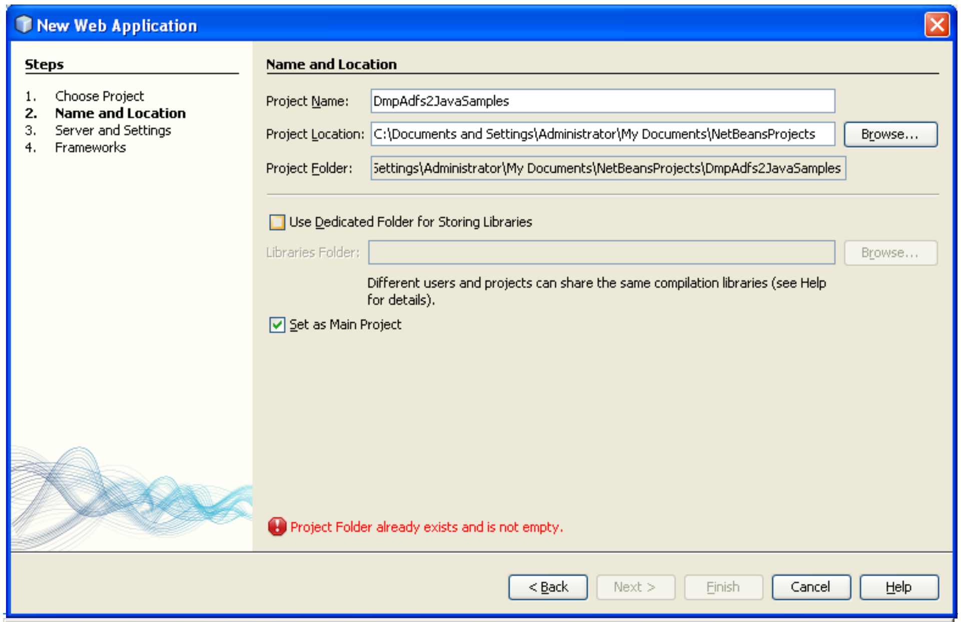


Creates an empty Web application in a standard IDE project. A standard project uses an **IDE-generated build script** to build, run, and debug your project.



Creates an empty Web application in a standard IDE project. A standard project uses an **IDE-generated build script** to build, run, and debug your project.

7. Tryk Next.



New Web Application

Steps

1. Choose Project
2. **Name and Location**
3. Server and Settings
4. Frameworks

Name and Location

Project Name: DmpAdfs2JavaSamples

Project Location: C:\Documents and Settings\Administrator\My Documents\NetBeansProjects

Project Folder: Settings\Administrator\My Documents\NetBeansProjects\DmpAdfs2JavaSamples

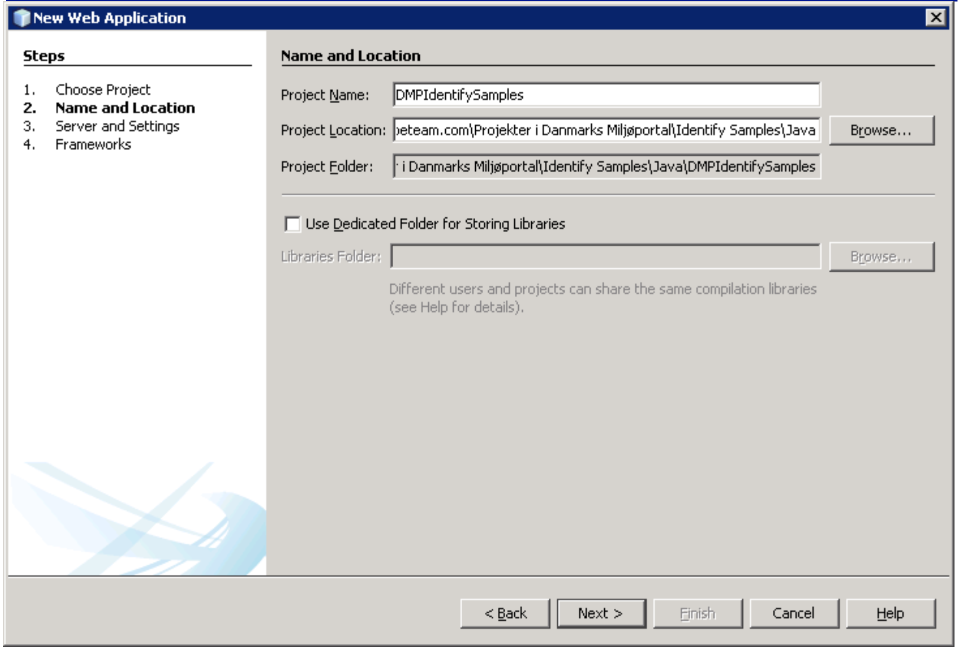
☐ Use Dedicated Folder for Storing Libraries

Libraries Folder:

Different users and projects can share the same compilation libraries (see Help for details).

☑ Set as Main Project

Project Folder already exists and is not empty.



New Web Application

Steps

1. Choose Project
2. **Name and Location**
3. Server and Settings
4. Frameworks

Name and Location

Project Name: DMPIdentifySamples

Project Location: eteam.com\Projekter i Danmarks Miljøportal\Identify Samples\Java

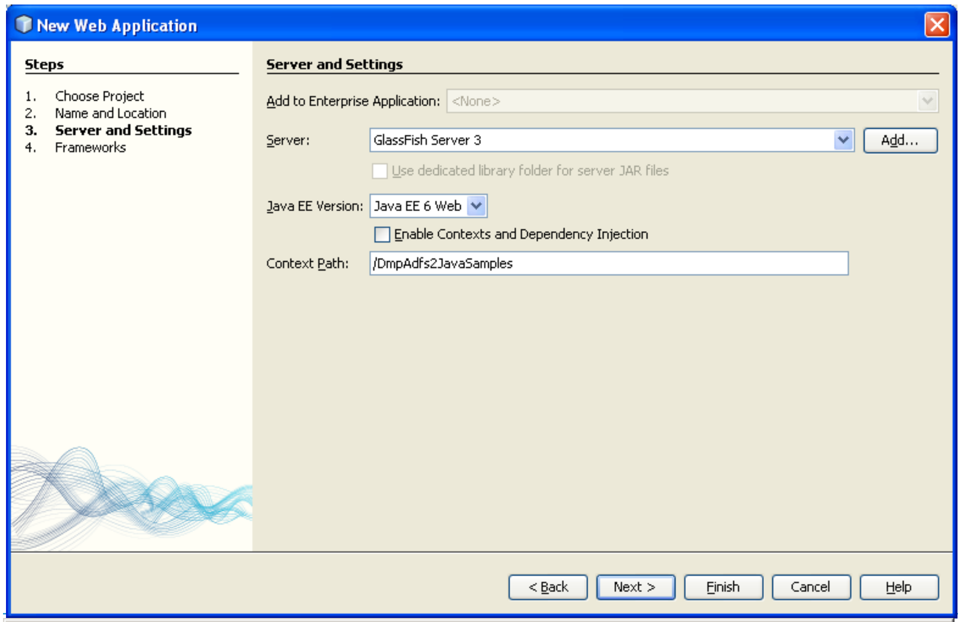
Project Folder: i Danmarks Miljøportal\Identify Samples\Java\DMPIdentifySamples

☐ Use Dedicated Folder for Storing Libraries

Libraries Folder:

Different users and projects can share the same compilation libraries (see Help for details).

8. Tryk Next



New Web Application

Steps

1. Choose Project
2. Name and Location
3. **Server and Settings**
4. Frameworks

Server and Settings

Add to Enterprise Application: <None>

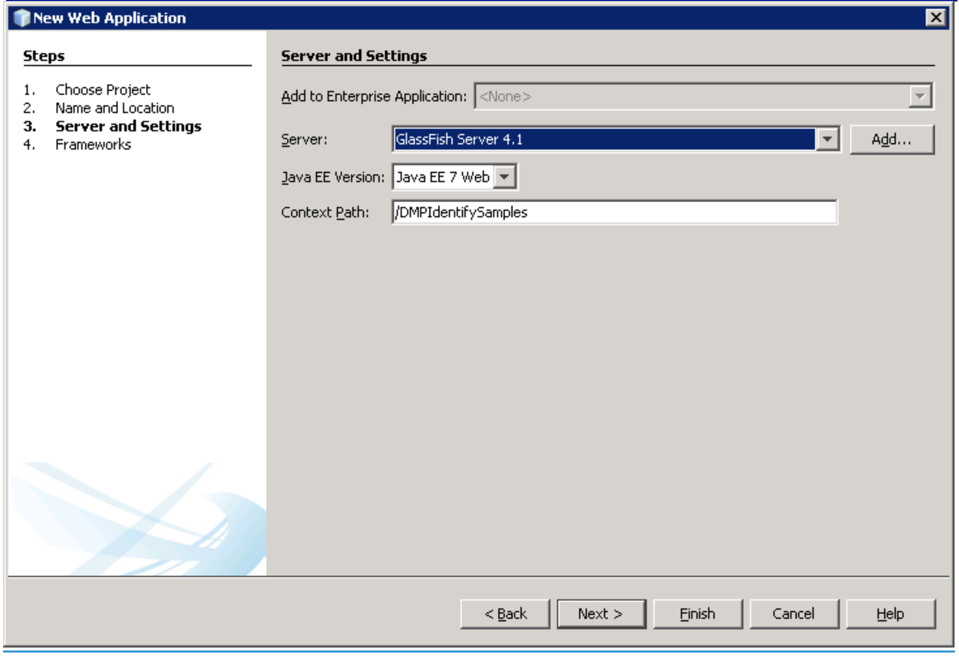
Server: GlassFish Server 3

□ Use dedicated library folder for server JAR files

Java EE Version: Java EE 6 Web

□ Enable Contexts and Dependency Injection

Context Path: /DmpAdfs2JavaSamples



New Web Application

Steps

1. Choose Project
2. Name and Location
3. **Server and Settings**
4. Frameworks

Server and Settings

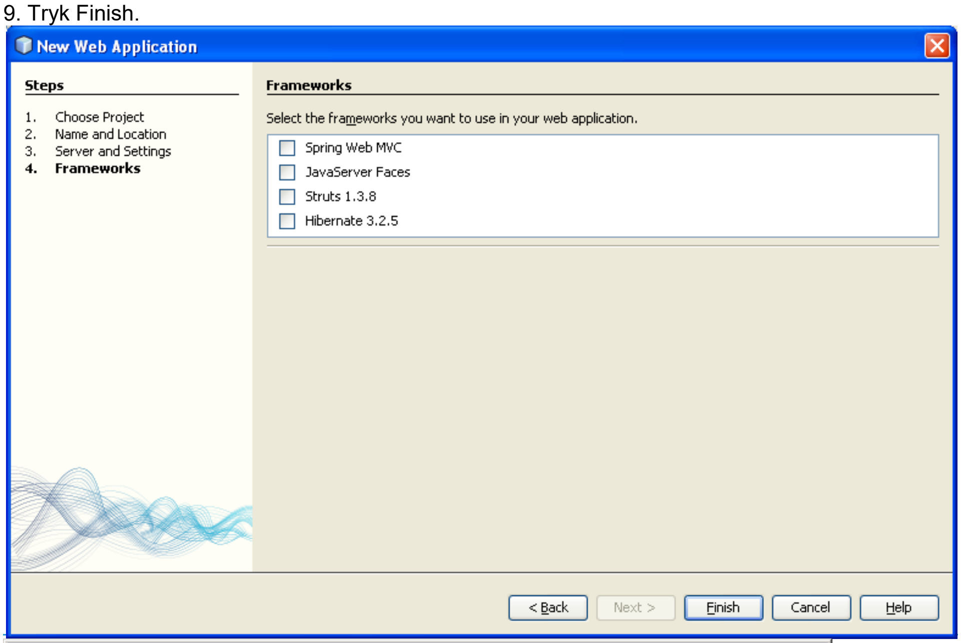
Add to Enterprise Application: <None>

Server: GlassFish Server 4.1

Java EE Version: Java EE 7 Web

Context Path: /DMPIdentifySamples

9. Tryk Finish.



New Web Application

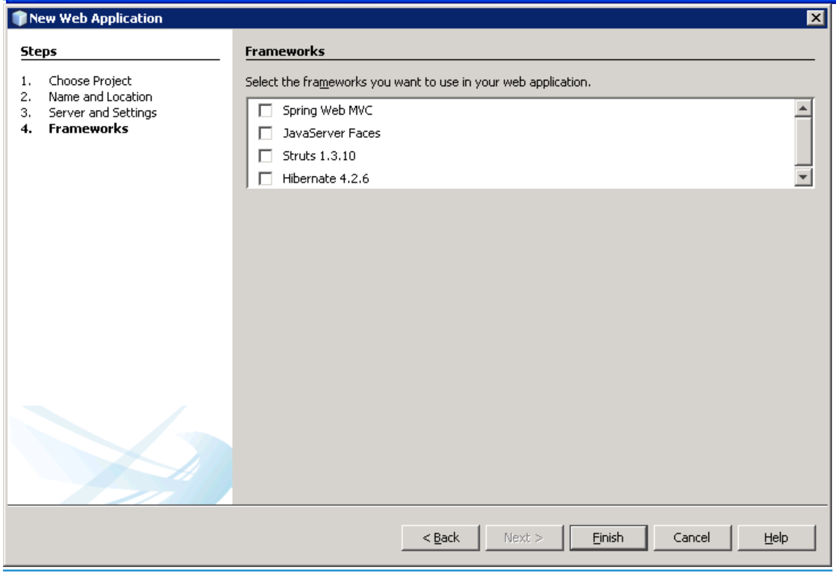
Steps

1. Choose Project
2. Name and Location
3. Server and Settings
4. **Frameworks**

Frameworks

Select the frameworks you want to use in your web application.

□ Spring Web MVC
□ JavaServer Faces
□ Struts 1.3.8
□ Hibernate 3.2.5



New Web Application

Steps

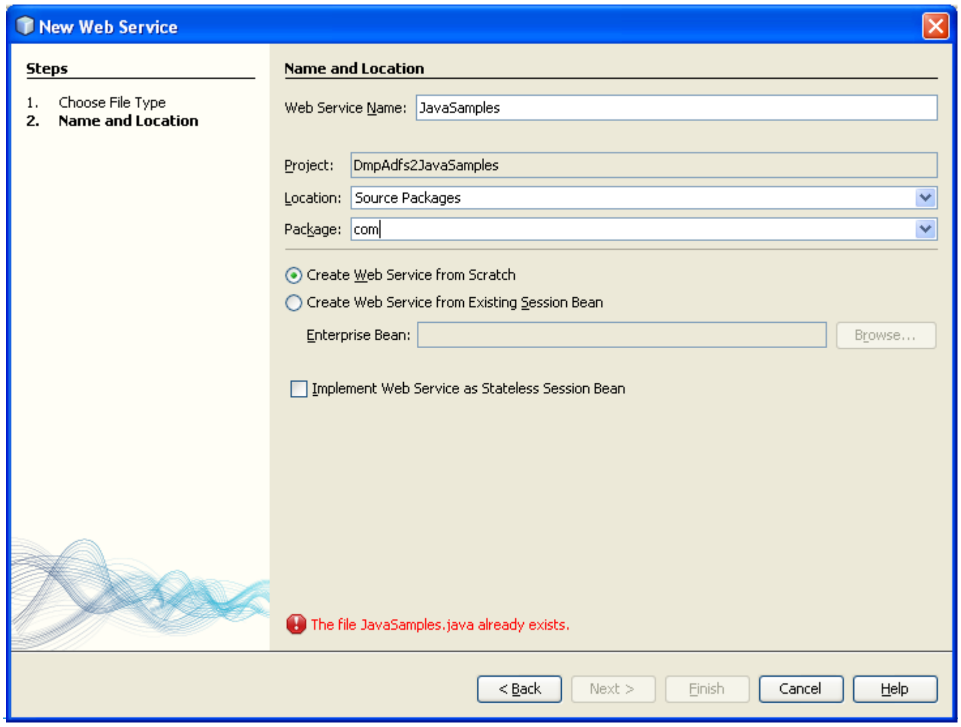
1. Choose Project
2. Name and Location
3. Server and Settings
4. **Frameworks**

Frameworks

Select the frameworks you want to use in your web application.

□ Spring Web MVC
□ JavaServer Faces
□ Struts 1.3.10
□ Hibernate 4.2.6

10. Højreklik på projektet, vælg New Web Service… og tryk Finish.



Web Service Name: JavaSamples

Project: DmpAdfs2JavaSamples

Location: Source Packages

Package: com

● Create Web Service from Scratch

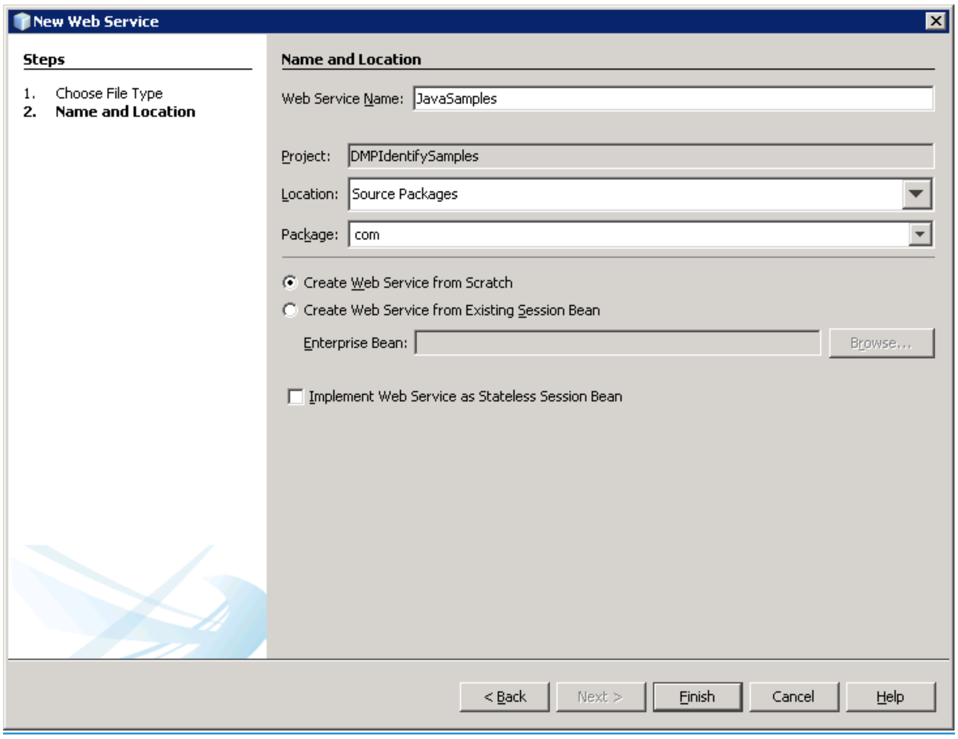
○ Create Web Service from Existing Session Bean

Enterprise Bean:

□ Implement Web Service as Stateless Session Bean

The file JavaSamples.java already exists.

Formatted: Danish



Web Service Name: JavaSamples

Project: DMPIdentifySamples

Location: Source Packages

Package: com

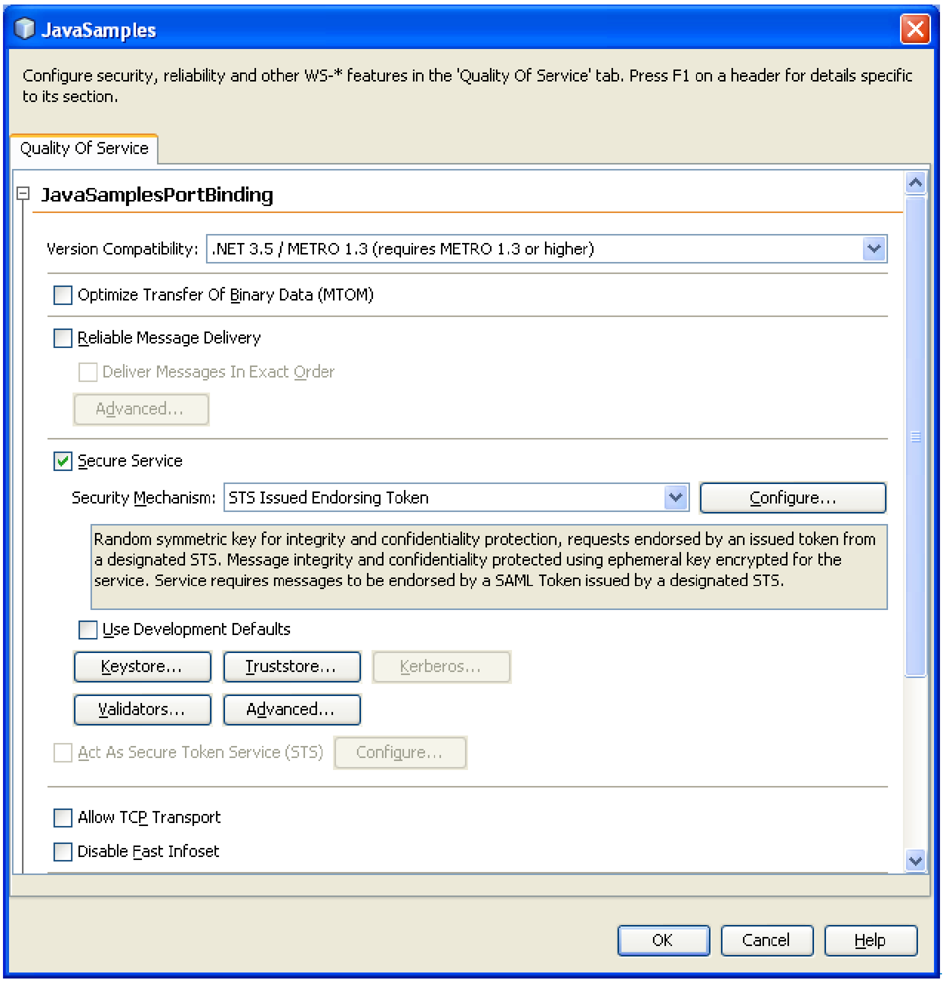
● Create Web Service from Scratch

○ Create Web Service from Existing Session Bean

Enterprise Bean:

□ Implement Web Service as Stateless Session Bean

11. Højreklik på Web Servicen ”JavaSamples”, vælg Edit Web Service Attributes... og
    - Sæt “Version Compatibility” til “.NET 3.5 / Metro 1.3 (requires METRO 1.3 or higher)”
    - Sæt vinge i “Secure Service”
    - Vælg “STS Issued Endorsing Token” i “Security Mechanism”



Configure security, reliability and other WS-* features in the 'Quality Of Service' tab. Press F1 on a header for details specific to its section.

JavaSamplesPortBinding

Version Compatibility: .NET 3.5 / METRO 1.3 (requires METRO 1.3 or higher)

□ Optimize Transfer Of Binary Data (MTOM)

□ Reliable Message Delivery

□ Deliver Messages In Exact Order

☑ Secure Service

Security Mechanism: STS Issued Endorsing Token

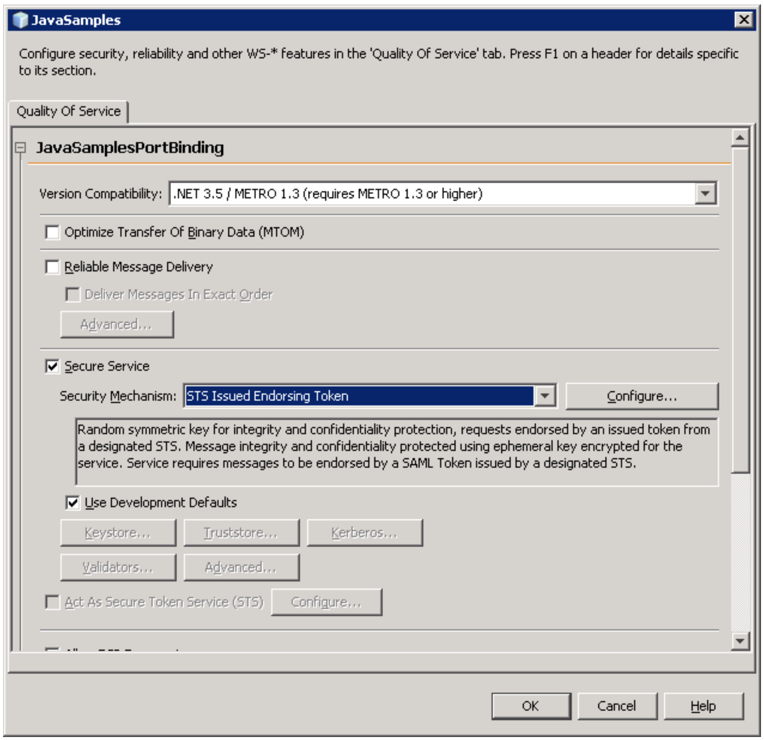
Random symmetric key for integrity and confidentiality protection, requests endorsed by an issued token from a designated STS. Message integrity and confidentiality protected using ephemeral key encrypted for the service. Service requires messages to be endorsed by a SAML Token issued by a designated STS.

□ Use Development Defaults

□ Act As Secure Token Service (STS)

□ Allow TCP Transport

□ Disable Fast Infoset



JavaSamples

Configure security, reliability and other WS-* features in the 'Quality Of Service' tab. Press F1 on a header for details specific to its section.

JavaSamplesPortBinding

Version Compatibility: .NET 3.5 / METRO 1.3 (requires METRO 1.3 or higher)

□ Optimize Transfer Of Binary Data (MTOM)

□ Reliable Message Delivery

□ Deliver Messages In Exact Order

☑ Secure Service

Security Mechanism: STS Issued Endorsing Token

Random symmetric key for integrity and confidentiality protection, requests endorsed by an issued token from a designated STS. Message integrity and confidentiality protected using ephemeral key encrypted for the service. Service requires messages to be endorsed by a SAML Token issued by a designated STS.

☑ Use Development Defaults

□ Act As Secure Token Service (STS)

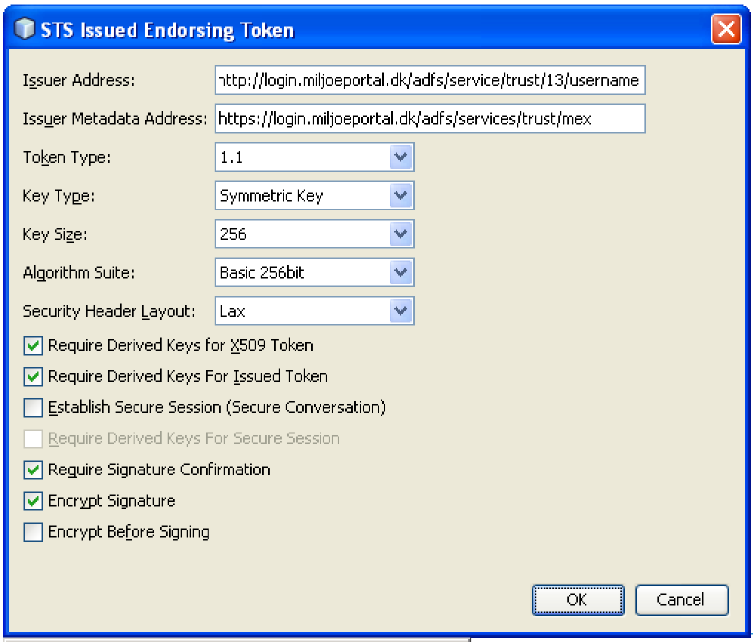
12. Tryk på Configure... og

- Indtast http://log-in.test.miljoeportal.dk/~~adfs~~runtime/services/trust/~~13~~14/username i “Issuer Address” (bemærk, at her skal URL’en til det tilsvarende end point i testmiljøet anvendes, såfremt løsningen skal benyttes op mod dette)
- Indtast https://log-in.test.miljoeportal.dk/runtime~~adfs~~/services/trust/mex i “Issuer Metadata Address” (bemærk at her skal URL’en i givet fald udskiftes til det tilsvarende end point i testmiljøet)
- Vælg 1.1 i “Token Type”
- Vælg Symmetric Key i “Key Type”
- Vælg 256 i “Key Size”
- Vælg Basic 256bit i “Algorithm Suite”
- Vælg Lax i “Security HeaderLayout”
- Sæt vinge i “Require Derived Keys for x509 Token”, “Require Derived Keys for Issued Token”, “Require Signature Confirmation” og “Encrypt Signature”

Field Code Changed

Field Code Changed

og tryk OK



STS Issued Endorsing Token

Issuer Address: http://login.miljoeportal.dk/adfs/service/trust/13/username

Issuer Metadata Address: https://login.miljoeportal.dk/adfs/services/trust/mex

Token Type: 1.1

Key Type: Symmetric Key

Key Size: 256

Algorithm Suite: Basic 256bit

Security Header Layout: Lax

☑ Require Derived Keys for X509 Token

☑ Require Derived Keys For Issued Token

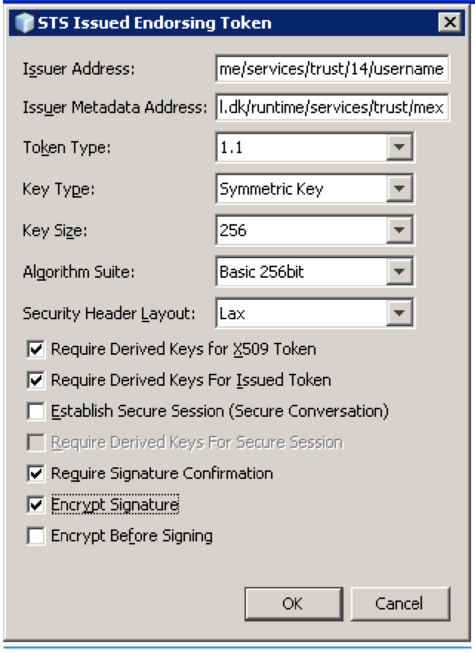
□ Establish Secure Session (Secure Conversation)

□ Require Derived Keys For Secure Session

☑ Require Signature Confirmation

☑ Encrypt Signature

□ Encrypt Before Signing



STS Issued Endorsing Token

Issuer Address: me/services/trust/14/username

Issuer Metadata Address: l.dk/runtime/services/trust/mex

Token Type: 1.1

Key Type: Symmetric Key

Key Size: 256

Algorithm Suite: Basic 256bit

Security Header Layout: Lax

☑ Require Derived Keys for X509 Token

☑ Require Derived Keys For Issued Token

□ Establish Secure Session (Secure Conversation)

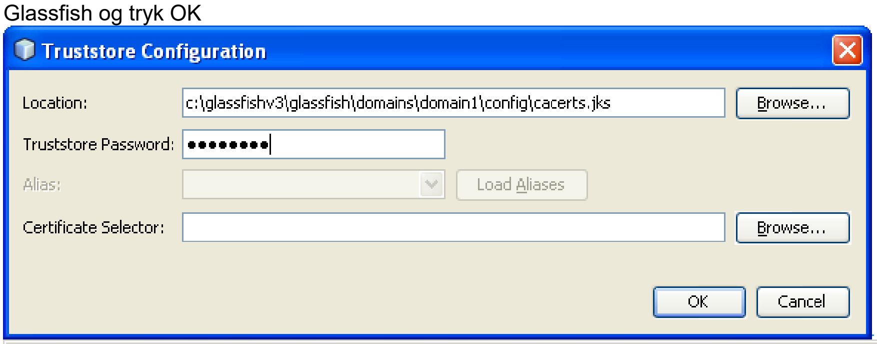
□ Require Derived Keys For Secure Session

☑ Require Signature Confirmation

☑ Encrypt Signature

□ Encrypt Before Signing

13. Tryk på Truststore, verificer at truststore peger ned på ”cacerts.jks” under default domain for Glassfish og tryk OK



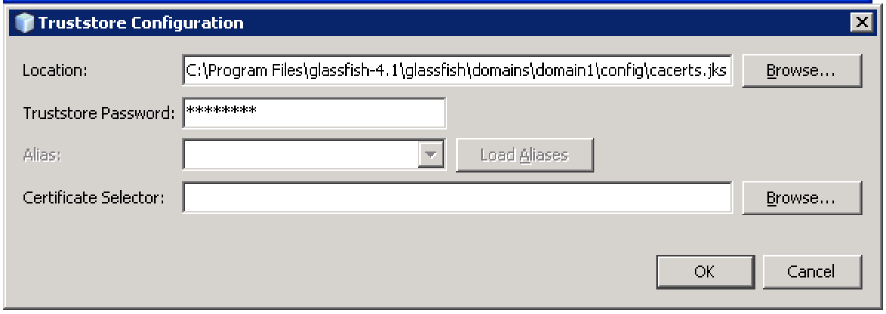
Truststore Configuration

Location: c:\glassfishv3\glassfish\domains\domain1\config\cacerts.jks

Truststore Password: ●●●●●●●●

Alias:

Certificate Selector:



Truststore Configuration

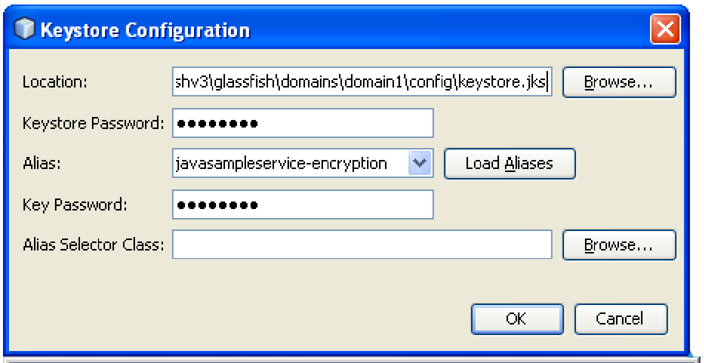
Location: C:\Program Files\glassfish-4.1\glassfish\domains\domain1\config\cacerts.jks

Truststore Password: ********

Alias:

Certificate Selector:

14. Tryk på Keystore..., verificer at keystore peger ned på ”keystore.jks” under default domain for Glassfish (åassword til både keystore og key password er i denne sample: ”changeit”), vælg ”javasampleservice-encryption” under Alias og tryk OK



Keystore Configuration

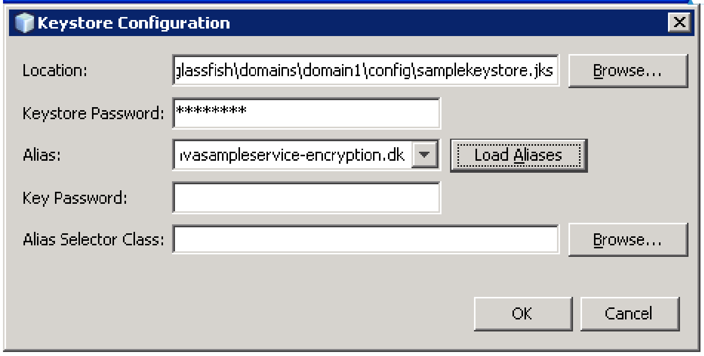
Location: shv3\glassfish\domains\domain1\config\keystore.jks

Keystore Password: ●●●●●●●●

Alias: javasampleservice-encryption

Key Password: ●●●●●●●●

Alias Selector Class:



Keystore Configuration

Location: glassfish\domains\domain1\config\samplekeystore.jks

Keystore Password: *********

Alias: ıvasampleservice-encryption.dk

Key Password:

Alias Selector Class:

Formatted: Danish

15. Dobbelklik på sevicen ”JavaSamples” og indsæt følgende kodestump. Bemærk i highlight, at der skal bruges SOAP 1.2 på servicen:

```
package com;

import javax.jws.WebMethod;
import javax.jws.WebService;
import javax.xml.ws.BindingType;

/**
 *
 * @author Administrator
 */
@WebService()
@BindingType(value="http://java.sun.com/xml/ns/jaxws/2003/05/soap/bindings/HTTP/")
public class JavaSamples {

    @WebMethod
    public String HelloWorld()
```

```
        {
            return "Hello world!";
        }
    }
```

Formatted: English (United States)

16. Der skal nu importeres certifikater certifikater til cacerts.jks-filen under default domain på Glassfish.

I denne sample tager vi udgangspunkt i at Glassfish er installeret i C:\Program Files\glassfish-4.1~~C:\glassfishv3~~ og default domain derfor bor i C:\Program Files\glassfish-4.1\glassfish~~C:\glassfishv3\glassfish~~\domains\domain1. Alle certifikaterne der skal importeres ligger i den medfølgende Visual Studio 2010 solution under ”External References”. Vi bruger Java keytool (en del af Java SDK’en) til at importere certifikaterne:

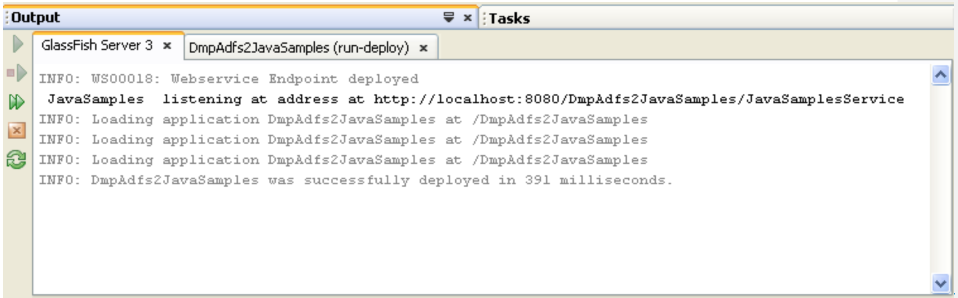
- DMP ~~AD FS 2.0~~Identify Signing certifikat (~~PRODUKTION~~TEST):
  keytool -import -alias dmp-~~adfs2~~identify-signing -file ~~tokensigning~~log-in.test.miljoeportal.dk.cer -keystore C:\~~glassfishv3~~glassfishv4\glassfish\domains\domain1\config\cacerts.jks
- ~~DMP AD FS 2.0 Signing certifikat (TEST):~~
  ~~keytool -import -alias dmp-adfs2-signing-test -file tokensigning.test.miljoeportal.dk.cer -keystore C:\glassfishv3\glassfish\domains\domain1\config\cacerts.jks~~
- ~~TDC OCES CA certifikat:~~
  ~~keytool -import -alias ocesca -file ocesca.cer -keystore C:\glassfishv3\glassfish\domains\domain1\config\cacerts.jks~~
- ~~TDC OCES Systemtest II CA certifikat:~~
  ~~keytool -import -alias tdcocessystemtestii -file ocessystemtestca.cer -keystore C:\glassfishv3\glassfish\domains\domain1\config\cacerts.jks~~

Formatted: English (United States)

Formatted: English (United States)

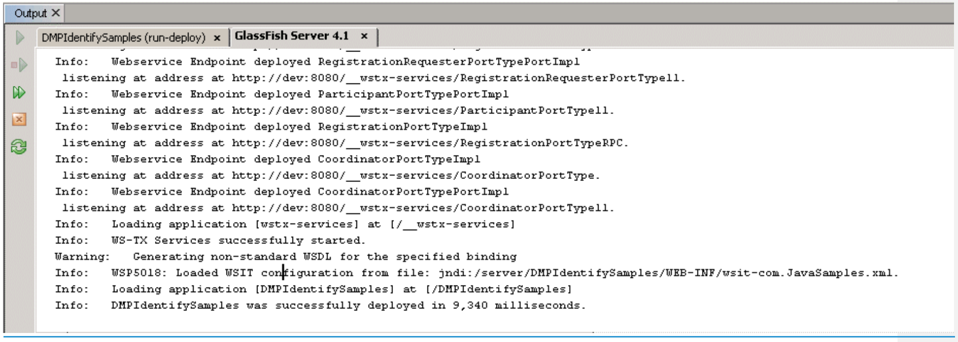
17. Projektet kompileres og deployes

Glassfish svarer i sin log, at servicen er deployeret. Bemærk, at URL’en skal være præcis som angivet her før at der kan udstedes tokens til servicen. Hvis du følger guiden slavisk vil servicen komme ud på følgende adresse:



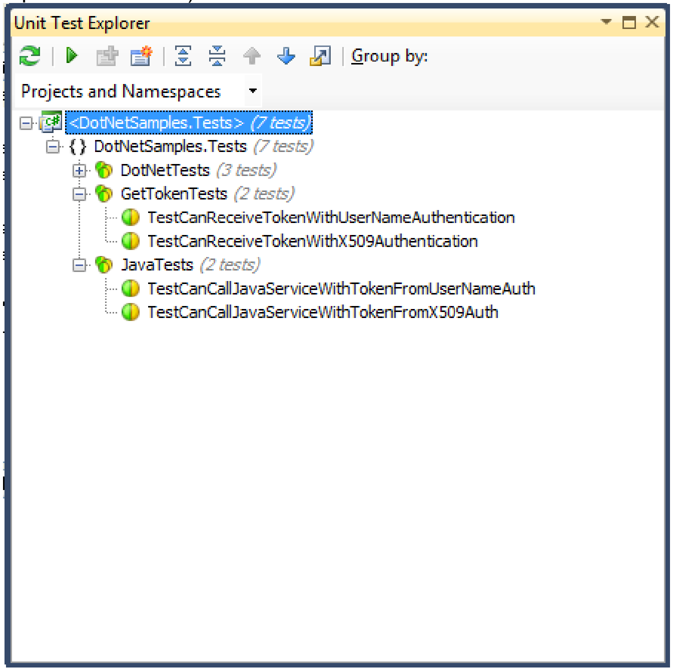
```
INFO: WS00018: Webservice Endpoint deployed
 JavaSamples  listening at address at http://localhost:8080/DmpAdfs2JavaSamples/JavaSamplesService
INFO: Loading application DmpAdfs2JavaSamples at /DmpAdfs2JavaSamples
INFO: Loading application DmpAdfs2JavaSamples at /DmpAdfs2JavaSamples
INFO: Loading application DmpAdfs2JavaSamples at /DmpAdfs2JavaSamples
INFO: DmpAdfs2JavaSamples was successfully deployed in 391 milliseconds.
```

Formatted: Danish



```
Info:   Webservice Endpoint deployed RegistrationRequesterPortTypePortImpl
 listening at address at http://dev:8080/__wstx-services/RegistrationRequesterPortTypell.
Info:   Webservice Endpoint deployed ParticipantPortTypePortImpl
 listening at address at http://dev:8080/__wstx-services/ParticipantPortTypell.
Info:   Webservice Endpoint deployed RegistrationPortTypeImpl
 listening at address at http://dev:8080/__wstx-services/RegistrationPortTypeRPC.
Info:   Webservice Endpoint deployed CoordinatorPortTypeImpl
 listening at address at http://dev:8080/__wstx-services/CoordinatorPortType.
Info:   Webservice Endpoint deployed CoordinatorPortTypePortImpl
 listening at address at http://dev:8080/__wstx-services/CoordinatorPortTypell.
Info:   Loading application [wstx-services] at [/__wstx-services]
Info:   WS-TX Services successfully started.
Warning:   Generating non-standard WSDL for the specified binding
Info:   WSP5018: Loaded WSIT configuration from file: jndi:/server/DMPIdentifySamples/WEB-INF/wsit-com.JavaSamples.xml.
Info:   Loading application [DMPIdentifySamples] at [/DMPIdentifySamples]
Info:   DMPIdentifySamples was successfully deployed in 9,340 milliseconds.
```

18. Gå over i .NET solution'en og kør unit tests'ne for Java servicen (bemærk, unit tests for Java er foldet ud på skærmbilledet)



```
<DotNetSamples.Tests> (7 tests)
  { } DotNetSamples.Tests (7 tests)
    DotNetTests (3 tests)
    GetTokenTests (2 tests)
      TestCanReceiveTokenWithUserNameAuthentication
      TestCanReceiveTokenWithX509Authentication
    JavaTests (2 tests)
      TestCanCallJavaServiceWithTokenFromUserNameAuth
      TestCanCallJavaServiceWithTokenFromX509Auth
```

Sådan kobles Web Services klienter op mod Web Services der anvender DMP

Forudsætningerne for at koble en Java-baseret Web Services klient op mod en Service under DMPs AD FS 2.0 er følgende.

1) Du er blevet udleveret public key certifikatet for servicens krypteringscertifikat
2) Du er blevet udleveret med en WSDL-adresse for den service du kobler en klient op mod
3) Du er i besiddelse af de medfølgende .NET samples til fagsystemejere som indeholder de nødvendige certifikater til DMP's AD FS 2.0-løsning

Som nævnt i forudsætninger for tilkobling øverst i dokumentet er kravene for at sætte en Java-baseret klient i luften mod en service under DMP, at der anvendes Glassfish 3.1 og Metro 2.1 i seneste promoted builds.

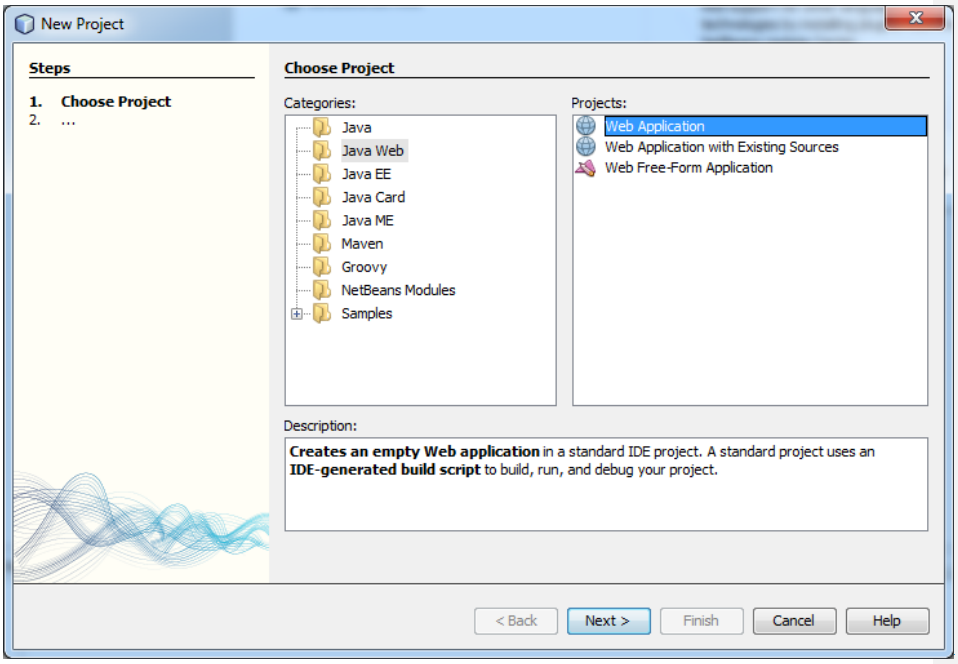
Step-by-step eksempel på tilkoblingen af en Java-baseret web services klient

Følgende step-by-step guide beskriver, hvordan du opsætter og konfigurerer en Java-baseret Web Services klient, der er baseret på Netbeans.

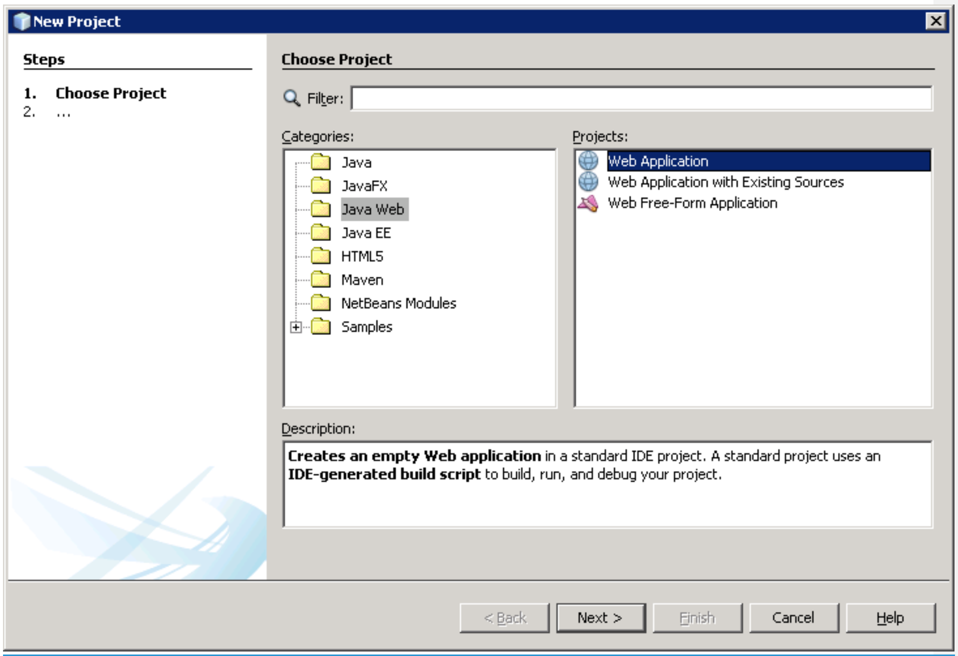
Beskrivelsen tager delvist udgangspunkt i den .Net-baserede solution (DmpAdfs2DotNetSamples.sln), der er udarbejdet til brug for vejledningen omkring tilkobling af en .Net-baseret web service, i og med at den benytter certifikaterne der følger med i samples'ne.

Når disse trin er udført vil du have en kørende Java-baseret Web Services klient på din egen maskine, der rekvirerer et token fra DMPs AD FS 2.0 og påhæfter det et kald til Web Service under DMP.

1. Åbn Netbeans og vælg New Project
2. Vælg Java Web -> Web Application:

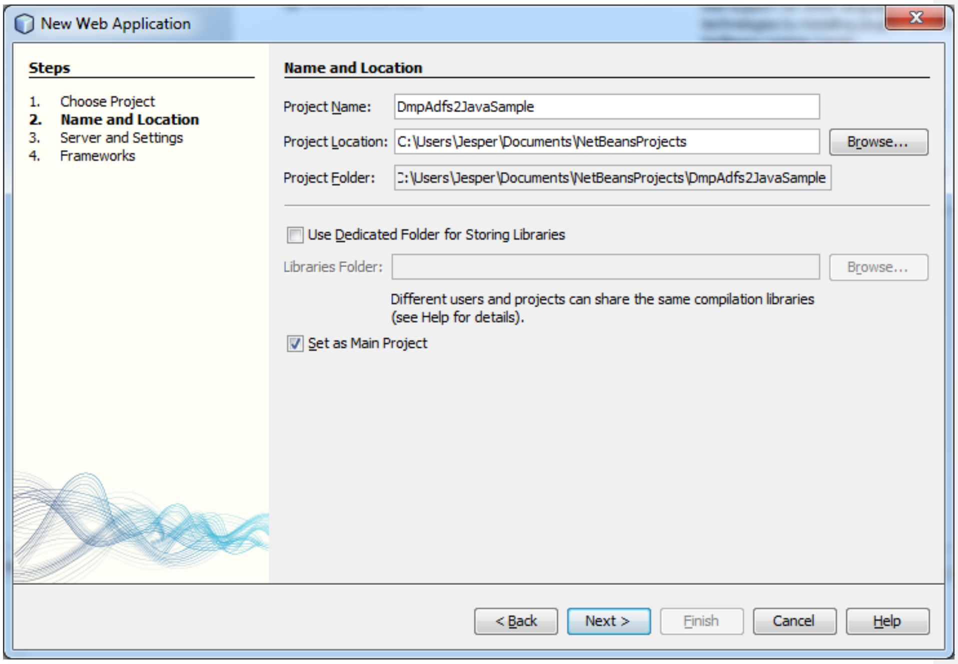


Creates an empty Web application in a standard IDE project. A standard project uses an **IDE-generated build script** to build, run, and debug your project.



Creates an empty Web application in a standard IDE project. A standard project uses an **IDE-generated build script** to build, run, and debug your project.

3. Navngiv projektet



Steps

1. Choose Project
2. **Name and Location**
3. Server and Settings
4. Frameworks

Name and Location

Project Name: DmpAdfs2JavaSample

Project Location: C:\Users\Jesper\Documents\NetBeansProjects

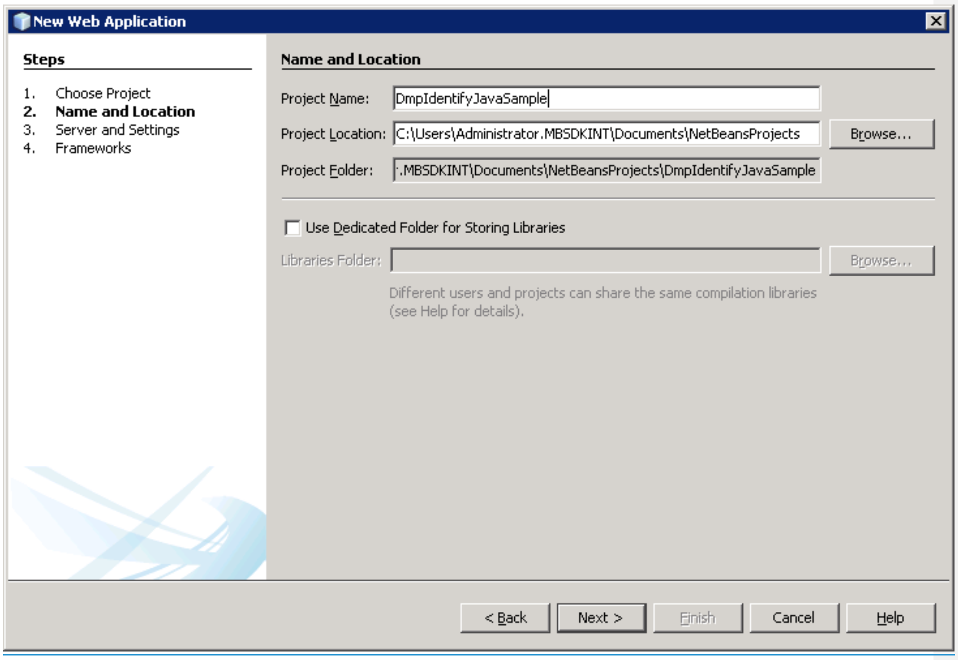
Project Folder: :\Users\Jesper\Documents\NetBeansProjects\DmpAdfs2JavaSample

□ Use Dedicated Folder for Storing Libraries

Libraries Folder:

Different users and projects can share the same compilation libraries (see Help for details).

☑ Set as Main Project



New Web Application

Steps

1. Choose Project
2. **Name and Location**
3. Server and Settings
4. Frameworks

Name and Location

Project Name: DmpIdentifyJavaSample

Project Location: C:\Users\Administrator.MBSDKINT\Documents\NetBeansProjects

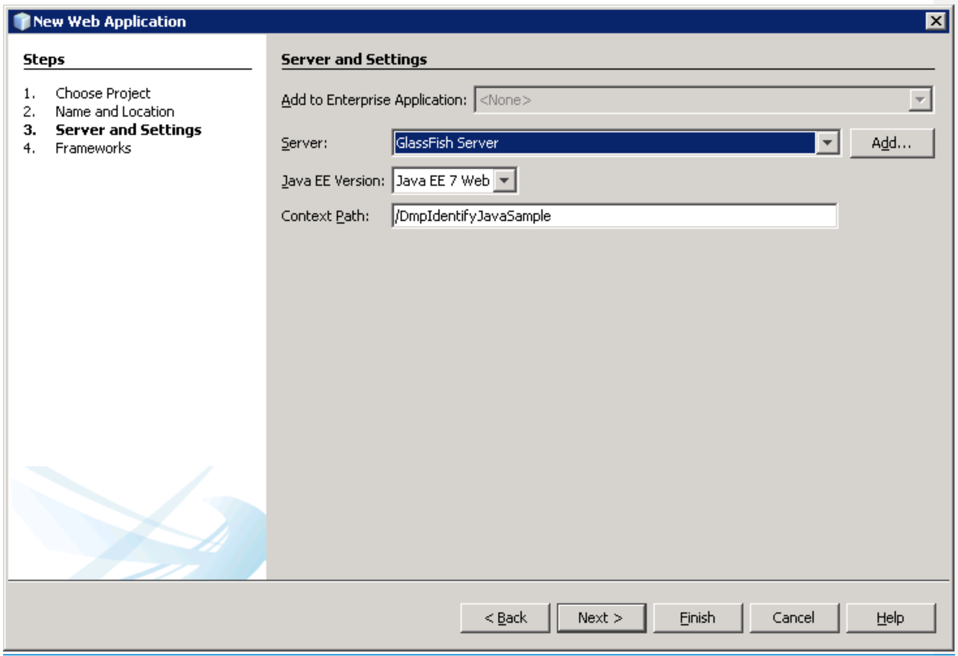
Project Folder: :.MBSDKINT\Documents\NetBeansProjects\DmpIdentifyJavaSample

□ Use Dedicated Folder for Storing Libraries

Libraries Folder:

Different users and projects can share the same compilation libraries (see Help for details).

4. Vælg Glassfish ~~3.1 s~~Serveren hvor web applikationen der huser klienten skal hostes på



New Web Application

Steps

1. Choose Project
2. Name and Location
3. **Server and Settings**
4. Frameworks

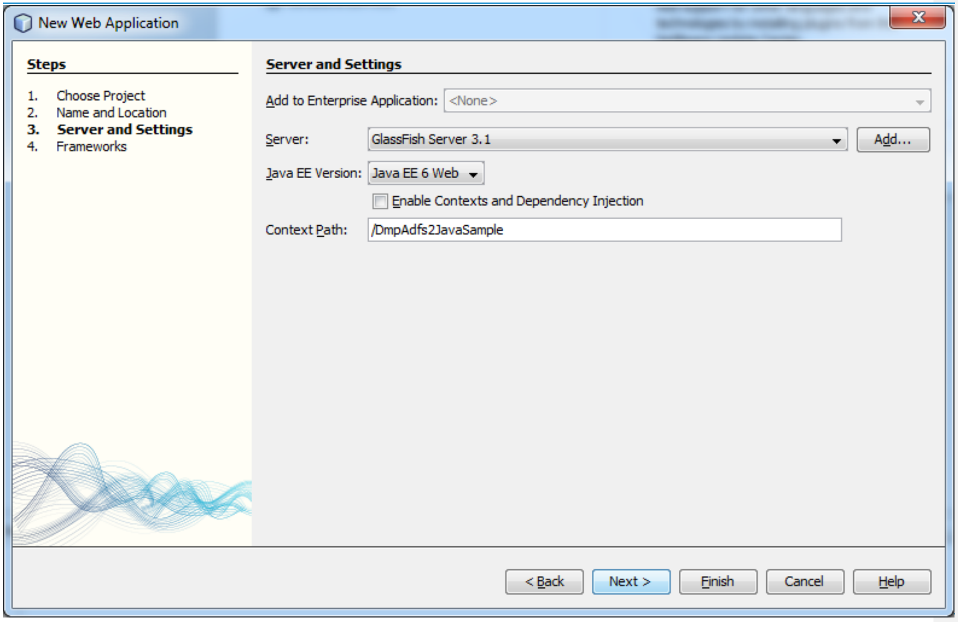
Server and Settings

Add to Enterprise Application: <None>

Server: GlassFish Server

Java EE Version: Java EE 7 Web

Context Path: /DmpIdentifyJavaSample



New Web Application

Steps

1. Choose Project
2. Name and Location
3. **Server and Settings**
4. Frameworks

Server and Settings

Add to Enterprise Application: <None>

Server: GlassFish Server 3.1

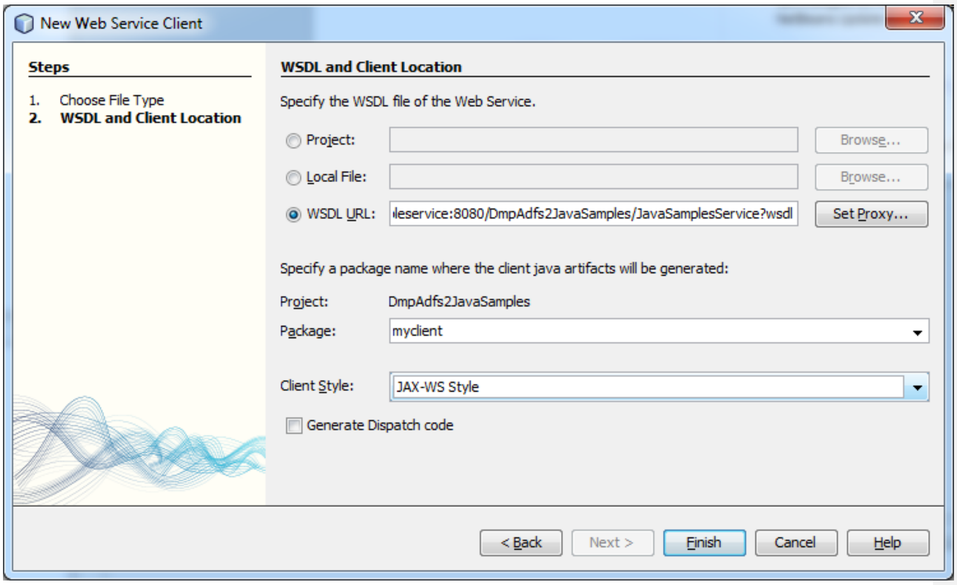
Java EE Version: Java EE 6 Web

□ Enable Contexts and Dependency Injection

Context Path: /DmpAdfs2JavaSample

5. Klik Finish

6. Højreklik på projektet og vælg New Web Service Client. Indtast her et evt. package navn for klienten og WSDL-adressen til servicen



New Web Service Client

Steps

1. Choose File Type
2. **WSDL and Client Location**

WSDL and Client Location

Specify the WSDL file of the Web Service.

○ Project: Browse...

○ Local File: Browse...

● WSDL URL: ıleservice:8080/DmpAdfs2JavaSamples/JavaSamplesService?wsdl Set Proxy...

Specify a package name where the client java artifacts will be generated:

Project: DmpAdfs2JavaSamples

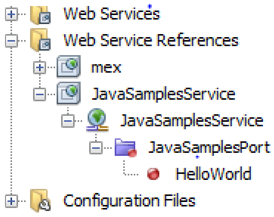
Package: myclient

Client Style: JAX-WS Style

□ Generate Dispatch code

< Back | Next > | Finish | Cancel | Help

7. Klik Finish og Netbeans vil generere en klient til servicen

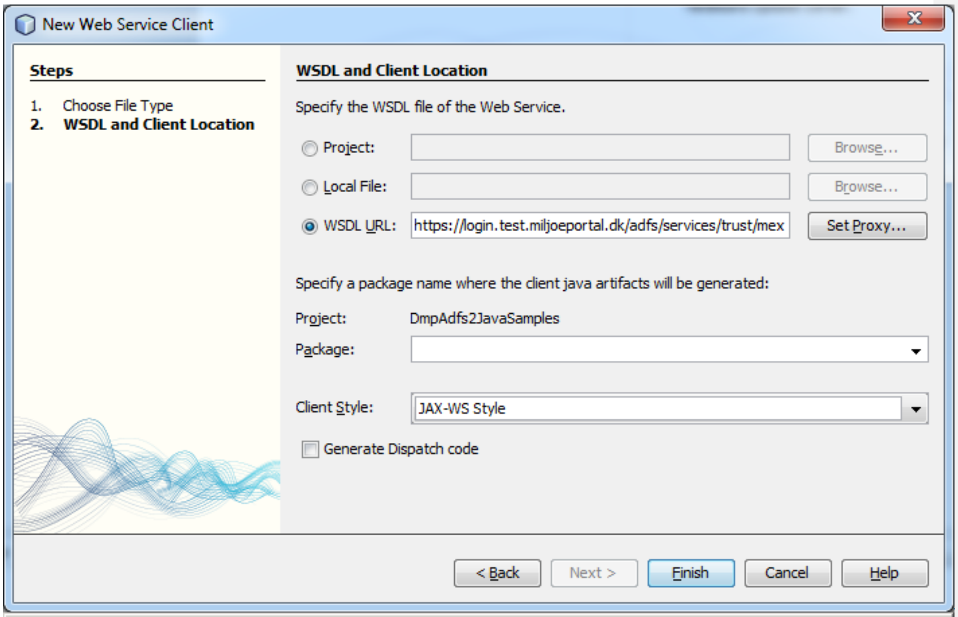


```
⊞ Web Services
⊟ Web Service References
    ⊞ mex
    ⊟ JavaSamplesService
        ⊟ JavaSamplesService
            ⊟ JavaSamplesPort
                HelloWorld
⊞ Configuration Files
```

8. Højreklik nu igen på projektet og vælg New Web Service Client. Indtast WSDL-url'en til enten DMPs produktions- eller testmiljø. Bemærk, der skal IKKE tastes noget i package name, da dette kan give name clashes.
    - TEST: https://log-in.test.miljoeportal.dk/~~adfs~~runtime/services/trust/mex
    - Produktion: https://log-in.miljoeportal.dk/~~adfs~~runtime/services/trust/mex

Field Code Changed

Field Code Changed



Steps

1. Choose File Type
2. **WSDL and Client Location**

WSDL and Client Location

Specify the WSDL file of the Web Service.

○ Project:

○ Local File:

● WSDL URL: https://login.test.miljoeportal.dk/adfs/services/trust/mex

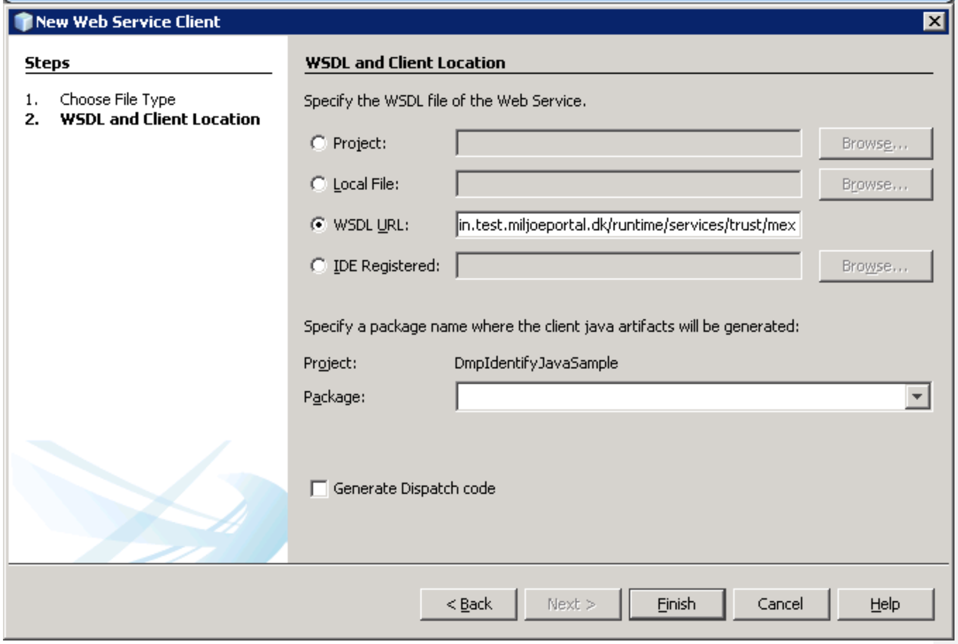
Specify a package name where the client java artifacts will be generated:

Project: DmpAdfs2JavaSamples

Package:

Client Style: JAX-WS Style

□ Generate Dispatch code



Steps

1. Choose File Type
2. **WSDL and Client Location**

WSDL and Client Location

Specify the WSDL file of the Web Service.

○ Project:

○ Local File:

● WSDL URL: in.test.miljoeportal.dk/runtime/services/trust/mex

○ IDE Registered:

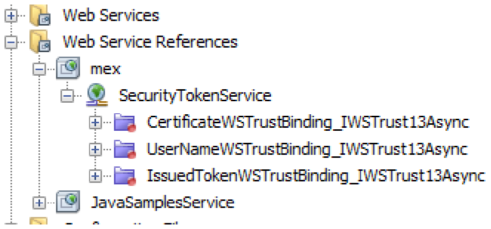
Specify a package name where the client java artifacts will be generated:

Project: DmpIdentifyJavaSample

Package:

□ Generate Dispatch code

9. Klik Finish og Netbeans vil generere en klient til AD FS 2.0'en

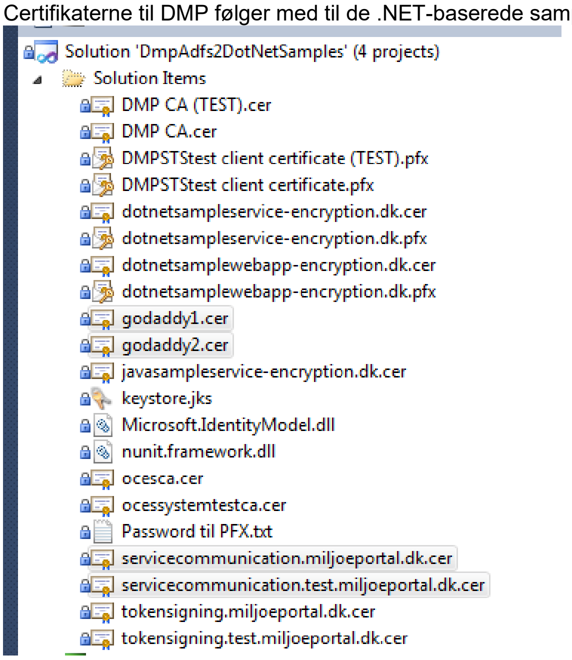


- Web Services
- Web Service References
  - mex
    - SecurityTokenService
      - CertificateWSTrustBinding_IWSTrust13Async
      - UserNameWSTrustBinding_IWSTrust13Async
      - IssuedTokenWSTrustBinding_IWSTrust13Async
  - JavaSamplesService

10. Det er nu tid til at importere certifikater i trust stores på klienten. Der skal importeres følgende to certifikater inklusive chains:
    - Public key af krypteringscertifikatet til DMPs AD FS 2.0
    - Public key af krypteringscertifikatet til servicen

    Begge certifikater inklusive chains skal importeres til cacerts.jks'en i det glassfish domain løsningen er hosted i. I dette eksempel vælges default domain i en Glassfish installeret under C:\Glassfish3, altså bliver stien til cacerts.jks:
    c:\glassfish3\glassfish\domains\domain1\config\cacerts.jks

    Certifikaterne til DMP følger med til de .NET-baserede samples, og er markeret her:

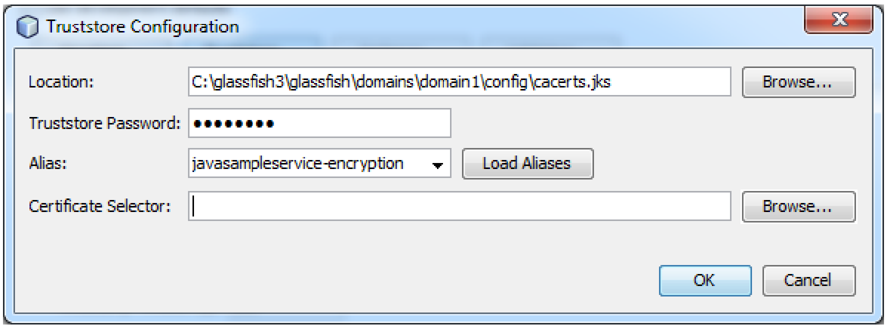


```
Solution 'DmpAdfs2DotNetSamples' (4 projects)
  Solution Items
    DMP CA (TEST).cer
    DMP CA.cer
    DMPSTStest client certificate (TEST).pfx
    DMPSTStest client certificate.pfx
    dotnetsampleservice-encryption.dk.cer
    dotnetsampleservice-encryption.dk.pfx
    dotnetsamplewebapp-encryption.dk.cer
    dotnetsamplewebapp-encryption.dk.pfx
    godaddy1.cer
    godaddy2.cer
    javasampleservice-encryption.dk.cer
    keystore.jks
    Microsoft.IdentityModel.dll
    nunit.framework.dll
    ocesca.cer
    ocessystemtestca.cer
    Password til PFX.txt
    servicecommunication.miljoeportal.dk.cer
    servicecommunication.test.miljoeportal.dk.cer
    tokensigning.miljoeportal.dk.cer
    tokensigning.test.miljoeportal.dk.cer
```

Alle fire certifikater importeres til cacerts.jks evt. via KeyStore explorer -> Tools -> Imported Trusted Certificate.

Certifikatet til servicen importeres på samme måde, men verificer at hele kæden til certifikatet kommer med ind i keystore't.

11. Det er nu tid til at konfigurere Web Services klienten samt klienten til AD FS 2.0'en. Højreklik på Web Services klienten og vælg Edit Web Service Attributes. Under Security vælges Truststore... og alias'et for servicens public key certifikat vælges:



Truststore Configuration

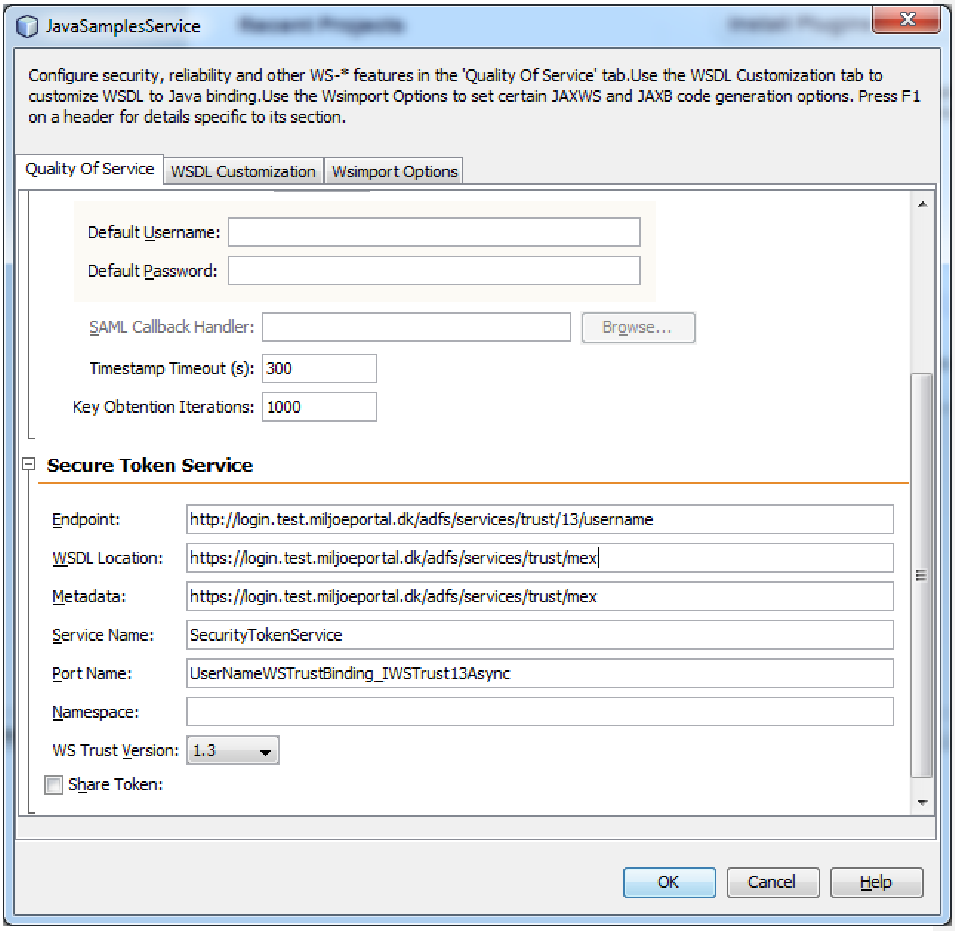
Location: C:\glassfish3\glassfish\domains\domain1\config\cacerts.jks

Truststore Password: ••••••••

Alias: javasampleservice-encryption

Certificate Selector:

12. Klik OK. Fold nu Secure Token Service noden ud og fyld ind som anvist.



JavaSamplesService

Configure security, reliability and other WS-* features in the 'Quality Of Service' tab.Use the WSDL Customization tab to customize WSDL to Java binding.Use the Wsimport Options to set certain JAXWS and JAXB code generation options. Press F1 on a header for details specific to its section.

Default Username:

Default Password:

SAML Callback Handler:

Timestamp Timeout (s): 300

Key Obtention Iterations: 1000

Secure Token Service

Endpoint: http://login.test.miljoeportal.dk/adfs/services/trust/13/username

WSDL Location: https://login.test.miljoeportal.dk/adfs/services/trust/mex

Metadata: https://login.test.miljoeportal.dk/adfs/services/trust/mex

Service Name: SecurityTokenService

Port Name: UserNameWSTrustBinding_IWSTrust13Async

Namespace:

WS Trust Version: 1.3

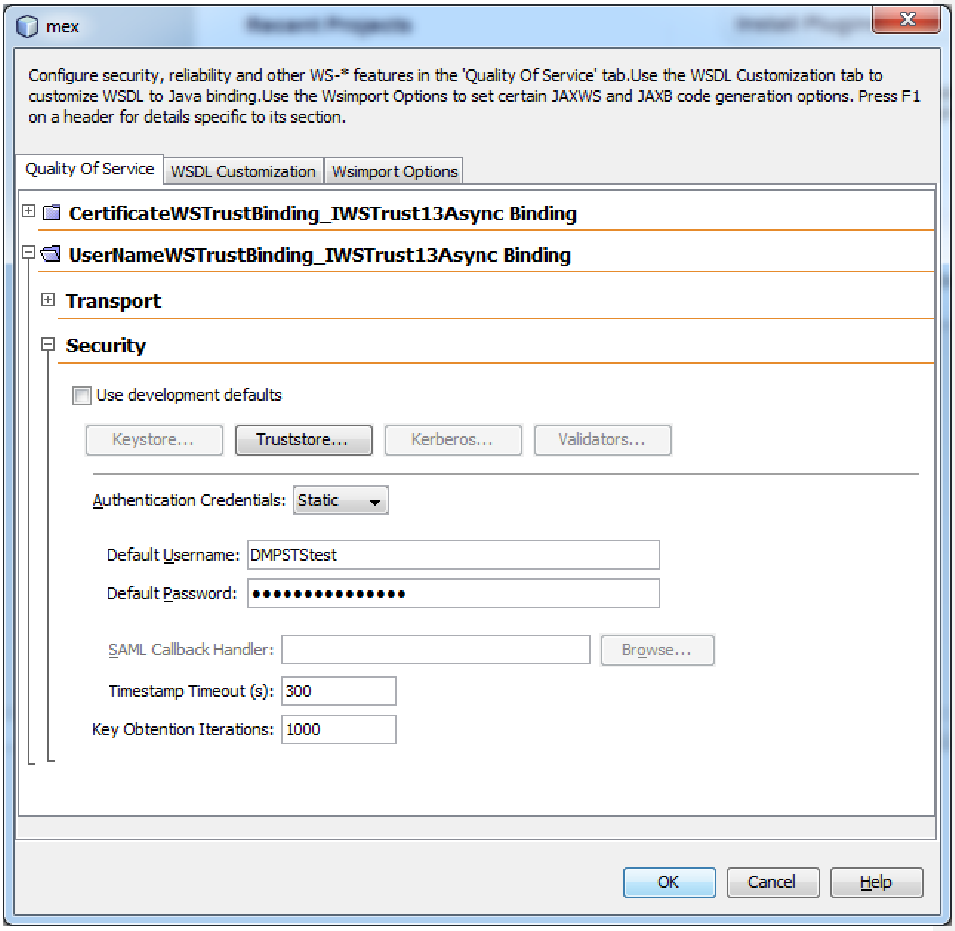
□ Share Token:

Bemærk, såfremt det er produktionsmiljøet der anvendes bruges adresserne:

- http://login.miljoeportal.dk/adfs/services/trust/13/username
- https://login.miljoeportal.dk/adfs/services/trust/mex

13. Klik OK. Web Services klienten er nu konfigureret.

14. Højreklik på klienten til AD FS 2.0'en (mex) og vælg Edit Web Service Attributes. Fold noden "UserNameWSTrustBinding_IWSTrust13Async" og indtast brugernavn og adgangskode til DMP i felterne:



mex

Configure security, reliability and other WS-* features in the 'Quality Of Service' tab.Use the WSDL Customization tab to customize WSDL to Java binding.Use the Wsimport Options to set certain JAXWS and JAXB code generation options. Press F1 on a header for details specific to its section.

⊞ CertificateWSTrustBinding_IWSTrust13Async Binding

⊟ UserNameWSTrustBinding_IWSTrust13Async Binding

⊞ Transport

⊟ Security

☐ Use development defaults

Authentication Credentials: Static

Default Username: DMPSTStest

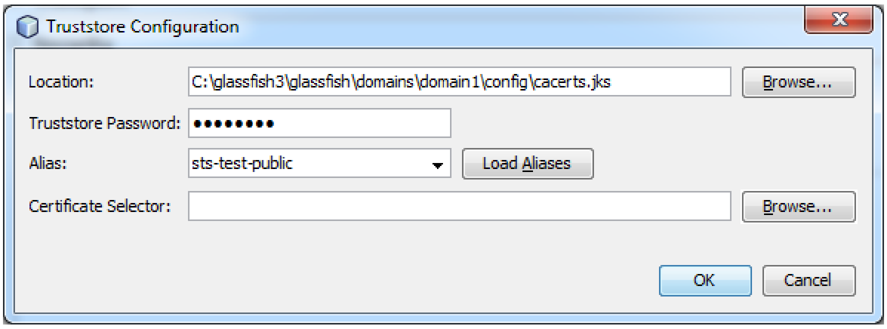
Default Password: •••••••••••••••

SAML Callback Handler:

Timestamp Timeout (s): 300

Key Obtention Iterations: 1000

15. Klik på Truststore... og vælg public key af AD FS 2.0'ens servicecertifikatet – altså enten:
servicecommunication.miljoeportal.dk.cer (produktion)
eller
servicecommunication.test.miljoeportal.dk.cer (test)



Truststore Configuration

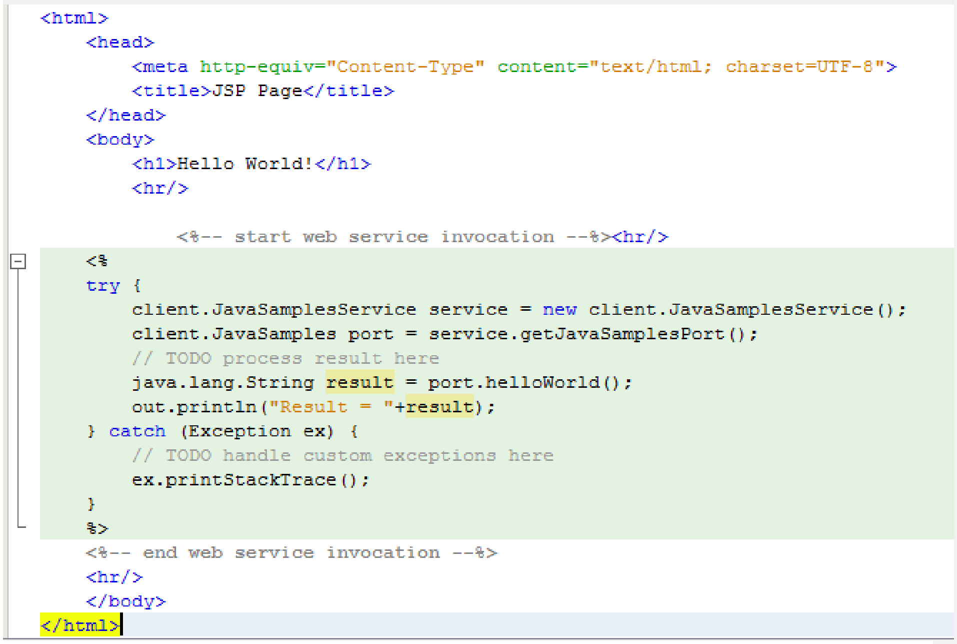
Location: C:\glassfish3\glassfish\domains\domain1\config\cacerts.jks

Truststore Password: ●●●●●●●●

Alias: sts-test-public

Certificate Selector:

16. Klik OK. Klienten til AD FS 2.0'en er nu færdigkonfigureret
17. For at teste klienten kan man evt. dragge en serviceoperation ind i den medfølgende index.jsp i web applikationen i Netbeans som her:



```
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
        <title>JSP Page</title>
    </head>
    <body>
        <h1>Hello World!</h1>
        <hr/>

            <%-- start web service invocation --%><hr/>
    <%
    try {
        client.JavaSamplesService service = new client.JavaSamplesService();
        client.JavaSamples port = service.getJavaSamplesPort();
        // TODO process result here
        java.lang.String result = port.helloWorld();
        out.println("Result = "+result);
    } catch (Exception ex) {
        // TODO handle custom exceptions here
        ex.printStackTrace();
    }
    %>
    <%-- end web service invocation --%>
    <hr/>
    </body>
</html>
```