Kombit

Guideline for .Net Sample Web Application

Version 1.0

**Introduction**

The following document describes how to configure the .Net-based sample web application.

In the KOMBIT Støttesystemer information model, a web application that authenticates users based on an assertion issued by Context Handler (CH) is referred to as a Brugervendt system. In the following document the terms “Brugervendt system” and web application will be used interchangeably.

After completing this guide, the .Net-based sample web application will be configured.

Setting up the .Net-based sample web application in IIS is outside the scope of this document. This is described in the document “All\_guideline\_setup sites IIS.docx”.

It is assumed that the reader is a .Net-developer knowledgeable in the following technologies used to develop this .Net-based sample. This includes:

* C#
* Microsoft.Net framework v4.5
* Microsoft Windows Server Operating System
* Microsoft Internet Information Systems (IIS)
* HTTP
* X509v3 Certificates

# Introduction

The .Net-based sample web application is based on the open source project OIOSAML.Net

The WebsiteDemo in OIOSAML.Net is used to demonstrate how to send a SAML2.0 AuthRequest, how to receive and process a SAML2.0 response containing a SAML2.0 assertion.

This guide explains how to configure the sample web application (websitedemo) based on a SAML2.0 metadata file from an identity provider with which the sample web application will be used.

In this guide the metadata-file for the KOMBIT Støttesystemer Context Handler in the external project test environment is used. Note that this environment is not publically available, and referenced URL’s will therefor NOT be accessible.

Additional information about OIOSAML.Net can be found in the PDF file “Net SAML2 Service Provider Framework.pdf” that is supplied in the Documentations folder, that is included with the project folder in the zip-file containing all the samples.

# Configuring The Sample Web Application

This section describes how to configure the supplied sample web application (Brugervendt system).

Logging is done to the folder c:\temp. This folder must exist for logging to work.

1. Install the token signing certificate (without private key) used by the chosen identity provider in the LocalMachine\TrustedPeople store
   1. The Context Handler in the external project environment uses the certificate “CertificateIdp.p12”. This is supplied with the combined samples in the certificate folder.
2. Install the service provider certificate to be used with the sample web application in the LocalMachine\My store location.
   1. In this guide, the certificate “claimapp.stoettesystemerne.dk.p12” is used. This is supplied with the combined samples in the certificate folder.
3. Grant read-access to the private key for the certificate to be used by the sample web application.
   1. In this guide, Network Service is used as application pool identity, and should be greated read-access to the private key.
4. Store the metadata file for the identity provider to be used, in a folder on disk. In this guideline, we’re using “C:\metadata”
   1. Grant the application pool identity read access to this folder. Here, we’re using Network Service.
5. Modify Web.config of the sample web application. This is located in C:\inetpub\websitedemo\web.config. The following elements must be updated:
   1. Change the value for SigningCertificate to the thumbprint for the certificate “claimapp.stoettesystemerne.dk.p12” that was imported in step 2.
   2. Change server and Id attribute in ServiceProvider section to <https://adgangsstyringeksempler.test-stoettesystemerne.dk/websitedemo>
   3. Modify the <IDPEndPoints>element like below:

<IDPEndPoints metadata="C:\metadata\">  
<add id="<https://saml.adgangsstyringeksempler.test-stoettesystemer.dk/>">  
<CertificateValidation>  
<add type="dk.nita.saml20.Specification.SelfIssuedCertificateSpecification, dk.nita.saml20" />  
</CertificateValidation>  
</add>  
</IDPEndPoints>

# Testing the Web Application

Before the sample web application can be used, it must be configured on the identity provider, the sample web application is used with.

The specific steps for doing this depends on the identity provider being used, and is outside the scope of this document.

For KOMBIT Støttesystemer a web application must configured through the Administration portal.

After the web application has been successfully federated with the identity provider, it is possible to authenticate with the sample web application. To test this, do the following:

1. Browse the URL <https://adgangsstyringeksempler.test-stoettesystemerne.dk/websitedemo>
2. Click the link “Go To MyPage”
3. The browser is redirected to the configured identity provider. You will be required to authenticate by a means supported by the identity provider.
4. The browser is redirected back to the sample web application.
5. MyPage is shown, with a table of the attributes in the issued token.

# Source Code For The Sample Web Application

The source code for the sample web application is located in the following folder

Kombit.Samples.CH.WebsiteDemo

This folder is supplied with the zip-file containing the combined samples.

# Troubleshooting

## Certificate Could Not Be Found certificatenotfound.png

Solution: Check that all thumbprints in web.config are correct.

## Signature Of The Incoming Message Is Invalid

## 2. The signature of the incoming message is invalid signnaturefail.png Solution: Make sure the certificate type in web.config is specified as follows:

<CertificateValidation>  
<add type="dk.nita.saml20.Specification.SelfIssuedCertificateSpecification, dk.nita.saml20" />  
</CertificateValidation>

## Missing claim on IdP to pass OIOSAML.NET validation missingclaim.png

## Solution: Create a claim type "dk:gov:saml:attribute:AssuranceLevel" and set a proper value. For a default configuration of oiosaml.net, that would be>=3.