Kombit

Guideline for .Net Sample Web Application

Version 1.0

# kombit-web-net

Sample .Net Web Application using Context Handler

## Introduction

This guide describes how to configure the sample .Net web application using Context Handler for login.

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 guide the terms Brugervendt system andweb application will be used interchangeably.

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

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

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

## Overview Of The Sample .Net Web Application

The .Net 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 how to 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 document from the identity provider with which the sample web application will be used. In this sample, the identity provider is theContext Handler.

In this guide the metadata-file for the KOMBIT Støttesystemer Context Handler in the project environment is used.

## Setup

To use this sample do the following:

1. Either clone the repository <https://github.com/Safewhere/kombit-web-net.git> to C:\kombit-web-net, or unpack the provided zip-file kombit-web-net.zip to C:\kombit-web-net.
2. Open C:\kombit-web-net\Kombit.Samples.CH.WebsiteDemo.sln in Visual Studio, and build the solution.
3. Make sure an SSL certificate that covers the DNS name claimapp.eksterntest-stoettesystemerne.dk is present inLocalMachine\My certificate store.
4. Open the Hosts-file, and map the DNS name claimapp.eksterntest-stoettesystemerne.dk to localhost.
5. Create a new IIS web application:
   1. The Site name should be claimapp.eksterntest-stoettesystemerne.dk
   2. The Physical pathshould be C:\kombit-web-net\Kombit.Samples.CH.WebsiteDemo
   3. The Binding type should be HTTPS
   4. The Host name should be claimapp.eksterntest-stoettesystemerne.dk
   5. Select an appropriate SSL certificate, that matches the host name chosen in the previous step
6. Grant the application pool identity for the web application read and execute permissions to C:\kombit-web-net
7. Import the certificate C:\kombit-web-net\Certificates\saml.claimapp.projekt-stoettesystemerne.dk.p12 toLocalMachine\My.
8. Assign the application pool identity for the web application read permissions to the private key for the certificate imported in the previous step.
9. Open a browser and point it to <https://claimapp.eksterntest-stoettesystemerne.dk>
10. Click the [Go to My Page](https://claimapp.projekt-stoettesystemerne.dk/MyPage.aspx) to login using the Context Handler.