Verbetering bruikbaarheid ADFS login scherm ten behoeve van Mobiele gebruikers

Auteur: Martin van Es

Datum: 20-11-2012

Versie: 0.3

Inleiding

Steeds meer diensten voor hoger onderwijs en onderzoek gebruiken SURFconext als authenticatiemechanisme. Een aantal van deze diensten is geschikt voor gebruik op mobile devices. Helaas is een groot deel van de Identity Providers slecht of niet te gebruiken op mobile devices. Dit belemmert het gebruik van deze diensten.

Het document "Bruikbaarheidsrichtlijnen voor authenticatieschermen" bevat serveronafhankelijke richtlijnen voor het “mobielvriendelijk” maken van authenticatieschermen.

In dit document vindt u een praktische uitwerking van deze richtlijnen in een ADFS 2.0-omgeving. Er zijn voorbeeldbestanden beschikbaar die u met behulp van dit document kunt aanpassen aan uw eigen wensen en eisen.

Over authenticatie via ADFS 2.0

In een ADFS-omgeving spelen meestal twee servers een rol: de ADFS 2.0-server die de authenticatie voor toegang tot de federeatie tegen het domain afhandelt en de ADFS-proxy die de scheiding tussen het domain en de buitenwereld verzorgt en zich meestal in de DMZ bevindt.

Gebruikers van buiten het domain krijgen via de proxy een form based authentication request te zien. Dit form is het onderwerp van deze beschrijving.

Als een gebruiker zich aangemeld heeft op het domain en naar de ADFS-server gaat, wordt hij zonder loginscherm geauthenticeerd (Single Sign On). Indien niet aangemeld, dan krijgt de gebruiker een basic authentication request.

Let op: als er geen gebruik gemaakt wordt van een proxy moet mogelijk aan de ADFS-server gemeld worden dat de gebruiker geen basic authentication request maar het form based authentication request te zien krijgt. De aanpassingen in dit document betreffen in dat geval de ADFS-server. Let op dat op de ADFS-server integrated authentication (Kerberos SSO) en Forms-based authentication niet gecombineerd kunnen worden!

Bronbestanden

Alle ADFS2.0 form-bestanden bevinden zich onder c:/inetpub/adfs/ls. Het bestand ls.zip bevat alle benodigde bestanden om het form volgens de richtlijnen "Mobiel vriendelijker" te maken. Pak dit zip-bestand uit in de directory c:/inetpub/adfs of in een tijdelijke directory en kopieer de bestanden in de ls directory met de hand naar c:/inetpub/adfs/ls.

De uitgepakte inhoud van het ls.zip bestand ziet er als volgt uit:

```
ls
├── icon_error.png
├── logo.png
├── App_GlobalResources
│   ├── MobileResources.de.resx
│   ├── MobileResources.nl.resx
│   └── MobileResources.resx
├── MasterPages
│   ├── css
│   │   ├── style_320.css
│   │   ├── style_480.css
│   │   └── style.css
│   └── MobileMasterPage.master
└── MobileForm.aspx
```

De dikgedrukte bestanden en folders zijn nieuw ten opzichte van de bestaande structuur na installatie van de ADFS-proxy.

Aanpassingen

web.config

Eindpunt van de aanpassingen ten opzichte van een default install is het bestaande bestand web.config in de c:/inetpub/adfs/ls directory. In dit bestand is gedefinieerd welk aspx-document gebruikt moet worden voor de form based authenticatie. Maak voor je aanpassingen gaat doen in dit bestand een kopie zodat er teruggevallen kan worden op de originele situatie.

De regel die aangepast moet worden is als volgt te herkennen (gebruik eventueel de zoekfunctie van de editor).

```
<localAuthenticationTypes>
  <add name="Forms" page="FormsSignIn.aspx" />
```

Om de nieuwe layout te gebruiken moet deze laatste regel aangepast worden naar:

```
  <add name="Forms" page="MobileForm.aspx" />
```

De nieuwe pagina is hierna zonder herstart van ADFS beschikbaar.

MobileForm.aspx

MobileForm.aspx bevat het formulier, dwz de gebruikersnaam veld, het wachtwoordveld en de eventuele foutmeldingen en is onderdeel van een MasterPage die in de kop van MobileForm.aspx gedefinieerd is:

```
<%@ Page Language="C#" MasterPageFile="~/MasterPages/MobileMasterPage.master" ...
```

MobileMasterPage.master

MobileMasterPage.master is een aangepaste versie van de originele MasterPage.master. Dat is te zien aan de header van deze pagina, waarin nog

steeds verwezen wordt naar de originele MasterPage.master.cs CodeFile:

```
<%@ Master Language="C#" AutoEventWireup="true" CodeFile="MasterPage.master.cs" ...
```

MobileMasterPage.master bevat de basispagina (template) voor het mobiele login form, met verwijzingen naar de verschillende (mobiele) stylesheets, de viewportr en de javascript voor het activeren van het username veld in de header en wat afsluitende tips in de footer.

De regels hieronder zijn uiteindelijk verantwoordelijk voor het includeren van de form content zoals beschreven in MobileForm.aspx

```
<form id="MainForm" runat="server">
<asp:ContentPlaceHolder ID="ContentPlaceHolder1" runat="server">
</asp:ContentPlaceHolder>
</form>
```

De inhoud van deze file spreekt verder voor zich. Eventuele aanpassingen in logo en opmaak zullen hier plaatsvinden. Verdere aanpassingen van de kleuren kunnen doorgevoerd worden in de respectievelijke stylesheets zoals vermeld in de header van dit bestand.

Taalbestanden

De voorbeeldpagina bevat een loginscherm voor Engels-, Nederlands- en Duitstalige gebruikers. ADFS heeft geen mogelijkheid de taal door de gebruiker te laten kiezen, maar kijkt naar de Accept-Language header die de browser meestuurt.

Alle tekstvelden in het loginscherm zijn vervangen door variabelen en voor de aanpassingen in deze layout zijn vier nieuwe waarden toegevoegd. Deze variabelen zijn terug te vinden in de respectievelijke files in de directory App_GlobalResources en staan in de MobileResources.xx.resx bestanden. Omdat Engels default is, staan de originele Engelse teksten in de het bestand MobileResources.resx (zonder lokaliteits aanduiding 'nl' of 'de').

De vier nieuwe velden zijn:

- **WelcomeHeader**: dit is de aanhef van het loginscherm
- **WelcomeText**: dit is de welkomtekst onder de aanhef
- **HelpHeader**: de kop voor de helptekst onder de loginvelden
- **HelpText**: de helptekst onder de loginvelden

Taalkeuze

Helaas is er geen mogelijkheid de eindgebruiker een taalkeuzemogelijkheid aan te bieden. Het is wel mogelijk terug te vallen op een standaard taal als de meegestuurde taal van de gebruiker niet beschikbaar is in het nieuwe interface.

Hiervoor moet in web.config een kleine aanpassing gemaakt worden:

Voeg in de <appSettings> sectie, onder het <add key="logo" element de volgende twee regels toe:

```
<add key="DefaultLanguage" value="en-us"/>
<add key="AvailableLanguage" value="nl, en-us" />
```

In bovenstaand voorbeeld is Engels (Amerikaanse variant) de standaard taal en worden zowel Nederlands (nl) als Engels (Amerikaanse variant) geaccepteerd. Voor het gemak is een web.config.new met deze aanpassing toegevoegd. Let op dat deze file alleen deze aanpassingen bevat en niet naar MobileForm.aspx wijst, zoals hierboven beschreven.

De benodigde aanpassingen in Global.asax.cs zijn bijgevoegd in Global.asax.cs.new. Maak eerst een kopie van de Global.asax.cs file voor deze te overschrijven met de inhoud van Global.asax.cs.new.

Let op:

De MobileResources-bestanden moeten in UTF-8-formaat opgeslagen worden!

De ADFS (Proxy) server is heel kritisch over welke labels en textboxen gebruikt worden en of deze ook voorkomen in de respectievelijke bestanden. Dit is de reden dat bijvoorbeeld.

<!--<asp:Label ID="PageTitleLabel" runat="server"></asp:Label>--> en

<!--<asp:Label ID="STSLabel" runat="server"></asp:Label>-->

tussen commentaartags zijn toegevoegd aan het bestand MobileMasterPage.master. Zonder deze regels stopt de form based authenticatie en wordt een foutmelding gegeven. Het is dus zaak deze te allen tijd te laten staan.