FMH Single Sign-On auf Basis des Identity Server 3

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Marcel Pfahrer
Experte: Prof. Dr. Andreas Spichiger
Industriepartner: FMH, Bern

Die verschiedenen Anwendungen der FMH (Verbindung der Schweizer Ärztinnen und Ärzte) sind über einen zentralen Identity Provider verbunden. Dieser basiert auf ASP.Net Web Forms und Windows Identity Foundation 3.5. Dabei können die rund 35 000 Benutzer zwischen verschiedenen Authentisierungsvarianten wählen. Im Rahmen der Arbeit wurde die Lösung durch ASP.Net MVC 5 und Identity Server 3 modernisiert. Zudem wurden zwei bestehende Anwendungen an die neue Lösung angepasst werden.

Identity Server 3

Was ist Identity Server?

Dahinter steckt ein .Net/Katana basiertes Framework, welches die Umsetzung von «Single Sign-On»/»Single Sign-Out» und Zugangskontrollen ermöglicht, in dem Prokolle wie OpenID Connect und OAtuh2 verwendet werden. Ausserdem wird eine Vielzahl von Clients unterstützt.
Der Identity Server 3 dient als neuer Identity Provider und authentisiert als zentrale Stelle alle Benutzer.
Die Benutzer werden danach von den Clients anhand einer eindeutigen ID autorisiert. Die ID wird mit den restlichen vom Client abgefragten Werten in einem JSON Web Token gespeichert und an den Client zurückgegeben.

Clients

Der Client muss auf dem Identity Server registriert sein um mit diesem interagieren zu können. Er nutzt den Server um User zu authentisieren, damit sich der Client dessen Identität sicher sein kann.

Users

Ein User oder Benutzer ist ein Mensch, welcher einen registrierten Client verwendet, um auf seine Daten Zugriff zu erhalten.

Scopes

Scopes identifizieren Ressourcen, auf welche der Client zugreifen will. Die eindeutigen Kennzeichnungen der Scopes werden während der Authentisierung an den Identity Provider gesendet und dieser prüft, ob der Client die Berechtigung hat um darauf zu zugreifen.

Umsetzung

Datenbank Vom Identity Provider der FMH wird bereits eine Datenbankstruktur vorgegeben. Diese wird so auch weiterhin verwendet. Alle Clients, Scopes und User sind ebenfalls in der Datenbank erfasst. Für die Kommunikation zwischen Server und Datenbank wurde EntityFramework verwendet.

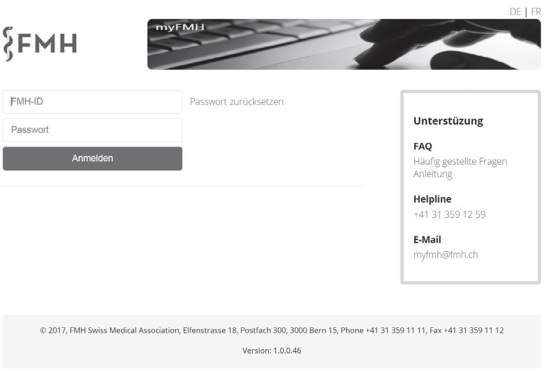
Design

Der Benutzer soll von der Umstellung auf Identity Server möglichst wenig Veränderungen erfahren. Darum wurde Wert auf den Erhalt des bestehenden Designs gelegt.

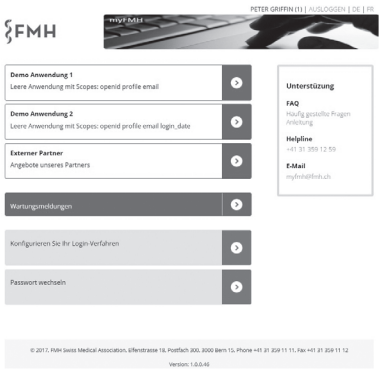
Sicherheit

- Die Kommunikation zwischen den Clients und dem Identity Server basiert auf SSL
- Die Tokens von Identity Server, sind mit einem pfx Zertifikat signiert
- Die Passwörter werden «gehashed» und «gesaltet» auf einer Datenbank abgelegt
- Passwort Zurücksetzungen sind nur mit gültigen Tokens per E-Mail möglich.

Daniel Hirt



Login Ansicht des Identity Servers



Übersichtsseite des neuen ASP.Net MVC 5 Clients