BFH Identity Hub – Extended Attribute Aggregator

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Dr. Annett Laube-Rosenpflanzer, Gerhard Hassenstein
Experte: Dr. Andreas Spichiger

Identity Hub basierende, föderierte Identitäts-Management Systeme sind heute ein wichtiges Thema im eGovernment und der Schweizer eSociety. Das Ziel dieses Projekts ist die Entwicklung eines erweiterten Attribut-Aggregators, welcher bei externen Attribut-Autoritäten Informationen zu einem Benutzer abfragen kann. Diese Funktionalität wird benötigt, damit die bestehende Shibboleth V3 Identity Provider Software für den Betrieb eines Identity Hubs eingesetzt werden kann.

Ausgangslage

SWITCH als langjähriger Betreiber einer Identity Federation Plattform (SWITCHaai) führt zur Zeit die Swiss edu-ID als übergeordnete Identität im Hochschulumfeld ein. Dieser Wechsel hat auch Änderungen in der Architektur zur Folge, indem neu nur noch ein zentraler Identity Hub als Identity Provider mit einer Vielzahl von Attribut-Autoritäten verwendet werden soll. Momentan sind einige wichtige Funktionserweiterungen auf dem zentralen Identity Hub noch nicht realisiert.

Ziel

Am Beispiel dieser von SWITCH geplanten neuen Infrastruktur wird in dieser Arbeit der Teil des Identity Hubs fokussiert, der die Attribut-Beschaffung und Aufbereitung zur Laufzeit übernimmt. Es soll ein erweiterter Attribut-Aggregator designt und implementiert werden, welcher mittels Backchannel Attribute Queries von den entsprechenden Attribut-Autoritäten die geforderten Attribute holt und diese zu einer Antwort (Attribute Assertion) zusammenfügt. Dieser erweiterte Attribut-Aggregator ist auf Basis des Shibboleth V3 Identity Providers (IdP) und den Standard SAML 2.0 Protokollen zu implementieren.

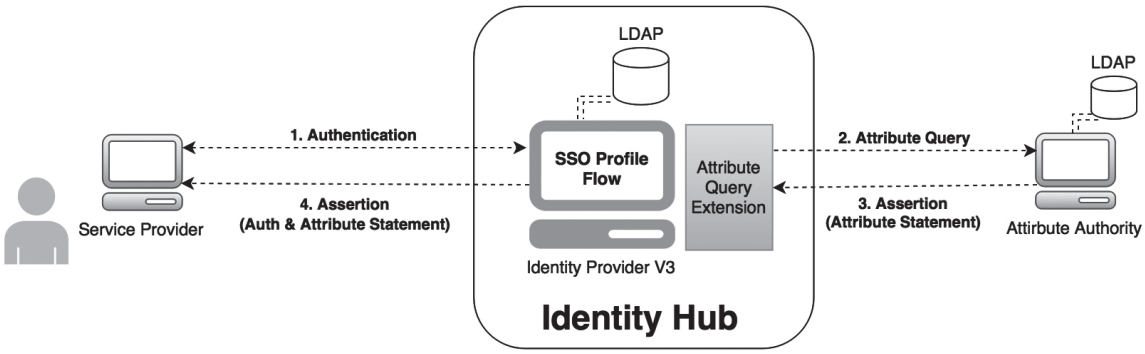
Ergebnisse

In einer ersten Phase wurden die genauen Anforderungen an einen Identity Hub erfasst. Beim Ausarbeiten des Konzepts für einen Shibboleth V3 Identity Provider mit Attribut-Aggregator Erweiterung stellte sich die Frage, wie die neuen Funktionen in die bestehende Spring Web Flow Architektur des Shibboleth V3 IdP zu integrieren sind.
Das Resultat der Arbeit ist eine neu entwickelte «Attribute Query Extension». Diese Extension besteht zum einen aus einem in Java geschriebenen Plugin, welches den Shibboleth V3 IdP um die Attribute Query Funktionalität erweitert und zum anderen aus diversen Anpassungen an den Spring Web Flows und an den Konfigurationen des IdP.

Fazit

Mit der Verwendung von Technologien wie Spring, Java, XML, MySQL, HTML und PHP war die Erweiterung eines Shibboleth V3 IdP zu einem Identity Hub sehr vielseitig.
Es konnte eine Lösung aufgezeigt werden, wie der Shibboleth V3 IdP mit Attribute Query Funktionalitäten erweitert werden kann. Es bedarf noch einiger Punkte, die angepasst und fertiggestellt werden müssen, um die Funktion in einer produktiven Umgebung einsetzen zu können. Aufgrund der Erkenntnisse aus dieser Arbeit kann SWITCH für die Weiterentwicklung des Shibboleth V3 IdP für die Swiss edu-ID wichtige Inputs mitnehmen.

Simon Gfeller
+41 79 795 58 53
simon.gfeller@gmail.com



Single Sign-On Vorgang auf dem Identity Hub mit dem Shibboleth V3 IdP und der Attribute Query Extension