myIdP Extension

IT-Security / Betreuerin: Dr. Annett Laube-Rosenpflanzer
Experte: Dr. Andreas Spichiger

Im Bereich E-Government und allgemein bei Webanwendungen hat sich herausgestellt, dass die redundante Dateneingabe in verschiedene Systeme für den Benutzer ein wesentliches Erschwernis darstellt. Durch die Realisierung des myIdP Prototyps im SuisseID Umfeld, steht dem Benutzer nun eine persönliche Ablage, in der er seine signierten Daten aufbewahren kann, zur Verfügung. Nachdem er seine Daten erstmals eingegeben hat, stehen diese nach seiner Freigabe in allen Applikationen mit myIdP-Unterstützung zur Verfügung. Eine wiederholte Eingabe der Daten bleibt ihm nun dank dem myIdP Dienst erspart.

Ausgangslage

Die SuisseID ist der erste standardisierte elektronische Identitätsnachweis der Schweiz und garantiert mit ihrem relativ aufwendigen Validierungsprozess, dass die elektronische Identität eindeutig einer natürlichen Person zugeordnet wird. Durch die Einbindung sogenannter Claims können Daten eines Benutzers bestätigt und beglaubigt werden. Ein Prototyp, welcher die Ablage und spätere Wiederverwendung dieser Claims ermöglicht, wurde in einer früheren Bachelor-Thesis erarbeitet und vorgestellt. Mit diesem steht nun eine anpassungsfähige Lösung bereit, welche von den Service Providern genutzt werden kann.

Persönliche Attribute (z. B. Adresse), die auf einem Client mit myIdP-Unterstützung eingetragen werden, können von diesem validiert, zertifiziert und anschliessend als signierte SAML 2.0 Assertion an die myIdP Webapp versendet werden. Dabei ist es möglich, dass ein Client die zuvor gespeicherten Attribute zu einem späteren Zeitpunkt als SAML 2.0 Assertion abfragen und weiterverwenden kann.

Zielsetzung

Die aktuelle Implementierung soll durch einige weitere Funktionalitäten erweitert werden. Es stehen momentan nur zwei Attributtypen für die Abfrage bereit, weitere sollen flexibel, in Form von XML Schema Definitionen, via Import integriert werden können. Dafür soll eine neue Komponente «myIdP Admin» erstellt werden.

Im Gegensatz zur SuisseID Core Infrastruktur und deren Attributtypen besteht zum myIdP kein definiertes Vertrauensverhältnis, deshalb soll ein Qualitätsmodell implementiert werden, damit Service Provider die Vertrauenswürdigkeit der erhaltenen Claims überprüfen können. Zusätzlich bietet eine neue Claim-Proxy Variante dem Service Provider die Möglichkeit, die Qualität selbst zu berechnen. Dazu werden ihm vom myIdP Dienst alle benötigten Informationen geliefert.

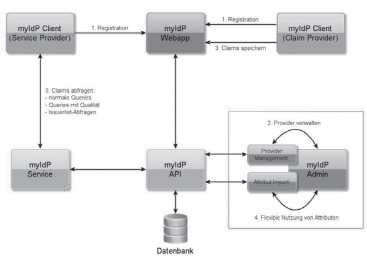
Des Weiteren soll man im myIdP Dienst einstellen können, dass nur Requests von registrierten Service Providern bearbeitet werden. Dasselbe gilt auch für Claim Provider. Ein Registrationsportal (für die Provider) und eine Verwaltung (für den myIdP Administrator) soll realisiert werden.

Marcel Bühlmann

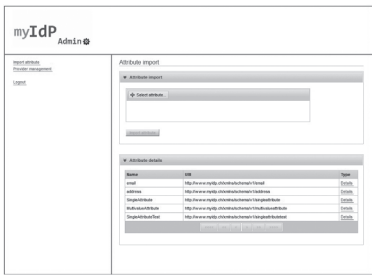
Umsetzung

Der Prototyp des myIdP Dienstes wurde als Java-Applikation implementiert. Zur Umsetzung wurden neuste Technologien wie z. B. Spring, RichFaces und Querydsl verwendet. Im myIdP Service und Client wurde ein Qualitätsmodul eingebaut, welches einfach erweitert und abgeändert werden kann. Die neue myIdP Admin Komponente stellt das User Interface für die Verwaltung der Attributtypen und der Provider zur Verfügung. In dieser können flexibel neue Attributtypen importiert werden. Bestimmte Provider können zugelassen oder gesperrt werden. Dem Administrator stehen deren Zertifikat sowie die Metadaten zum Download bereit. Alle umgesetzten Anpassungen sind abwärtskompatibel. Die Registration kann ein- und ausgeschaltet werden. Die Berechnung der Qualität erfolgt nur auf Anfrage des Service Providers. Um diese im SAML Response mitzuschicken wurde das SuisseID Schema erweitert.

Matthias Jeker



myIdP Systemübersicht mit Interaktionen zwischen den einzelnen Komponenten



Benutzeroberfläche des myIdP-Admin Dienstes (Attributtyp-Verwaltung)