myIDP - der personalisierte Attribute-Dienst

Web and Business Applications / Betreuer: Prof. Dr. Annett Laube-Rosenpflanzer
Experte: Prof. Dr. Andreas Spichiger

Im Bereich E-Government und allgemein bei Webanwendungen hat sich herausgestellt, dass die redundante Eingabe von Daten in verschiedene Systeme für den Benutzer eine wesentliche Erschwernis darstellt. Durch den Einsatz des myIDP-Dienstes in Kombination mit einer SuisseID, erhält der Benutzer eine persönliche Ablage, in der er seine signierten Daten aufbewahren kann. 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. Eine Ablage dieser Claims zur späteren Wiederverwendung war bis anhin nicht möglich und soll nun mit dem myIDP-Dienst zur Verfügung gestellt werden.

Zielsetzung

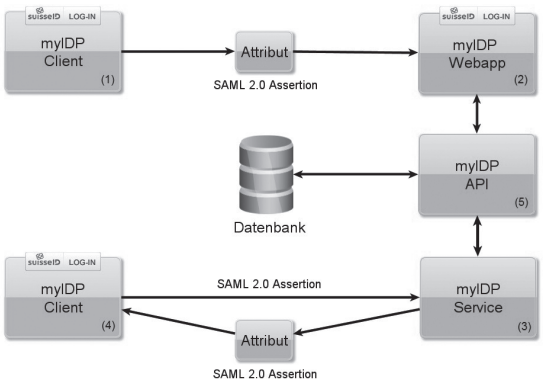
Persönliche Attribute (z. B. Email, Adresse), die auf einem Client mit myIDP-Unterstützung (z. B. von einer Behörde oder einem Webshop) eingetragen wurden, sollen von diesem validiert, zertifiziert und anschliessend als signierte SAML 2.0 Assertion an die myIDP-Webapp versendet werden. Dabei soll es möglich sein, dass derselbe oder ein anderer Client, die zuvor gespeicherten Attribute zu einem späteren Zeitpunkt, als signierte SAML 2.0 Assertion abfragen und weiterverwenden kann. Im Rahmen unserer Bachelor Thesis soll auf Basis der zuvor erstellten Spezifikation ein Prototyp des myIDP-Dienstes implementiert und in eine SuisseID-Testumgebung integriert werden.

Umsetzung

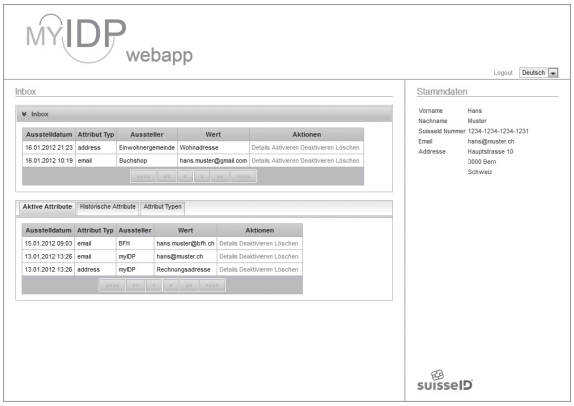
Der Prototyp des myIDP-Dienstes wurde als Java-Applikation implementiert. Zur Umsetzung wurden neuste Technologien wie z. B. Spring, RichFaces und Querydsl verwendet. Die myIDP-Webapp (2) sowie die myIDP-Clients (1) und (4) verlangen die zertifikatbasierte Authentifizierung mittels SuisseID. Nach Erfassung eines Attributes im myIDP-Client (1), wird dieses als signierte SAML 2.0 Assertion an die myIDP-Webapp (2) versendet und dort in der Inbox gespeichert. Dabei sind sowohl Single-value-Attribute (z. B. Email) wie auch Multivalue-Attribute (z. B. Adresse) möglich. Zur Abfrage der Attribute aus der myIDP-Webapp (2) kommt der myIDP-Service (3) zum Tragen. Als Basis für die Webapplikation und den Service dient eine API (5), die als zentrale Komponente alle Services zur Verfügung stellt, um die im myIDP-Dienst anfallenden Daten zu verwalten.

David Ehrler

Ruth Imwinkelried



Systemübersicht myIDP mit Interaktionen zwischen den internen Komponenten



Benutzeroberfläche myIDP-Webapp mit Inbox