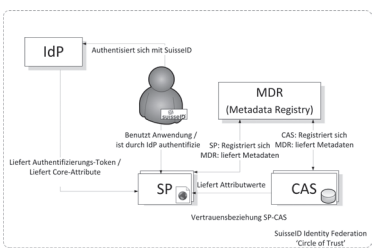
«Circle of Trust» SuisseID SP-CAS

IT-Security / Betreuer: Gerhard Hassenstein
Experte: Prof. Dr. Torsten Braun

Aufgabe dieser Bachelor Thesis war es, eine Lösung zu finden, wie innerhalb der SuisseID Umgebung eine Vertrauensbeziehung zwischen Service Providern und Claim Assertion Services hergestellt werden kann. Unsere Lösung sieht vor, dass die Komponenten über eine Verwaltungsstelle Metadaten austauschen und so eine Vertrauensbeziehung herstellen können. Das Konzept wurde anschliessend in einer Pilotumgebung realisiert.

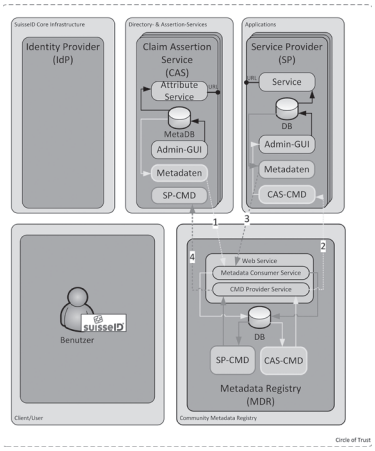
Mit der SuisseID wurde im Mai 2010 ein standardisierter elektronischer Identitätsnachweis eingeführt, welcher die Möglichkeit zur sicheren, vertrauenswürdigen Authentifikation bietet.
Da für viele Prozesse bei einem Service Provider (SP) ein Identitätsnachweis alleine nicht genügt, ist es notwendig, dass weitere Eigenschaften vertrauenswürdig überprüft werden können. Solche Eigenschaften können beispielsweise der Beruf (Notar, Arzt, Apotheker) oder die Mitgliedschaft bei einem Verein sein. Diese Eigenschaften nennt man zusammenfassend Funktionsnachweise. Damit ein SP solche Funktionsnachweise anfordern kann, beschreibt der SuisseID Standard dazu eine offene Infrastruktur, die sogenannte Claim Assertion Infrastructure (CAI). Diese besteht aus dem Identity Provider (IdP), der personenbezogene Informationen liefert und die Authentifizierung vornimmt.
Da der IdP aber nur eine beschränkte Auswahl an Core Attributen liefern kann (die Daten, die auch im Pass vorhanden sind) sind für Funktionsnachweise, die darüber hinausgehen, zusätzliche Funktionsregister (Claim Assertion Services – CAS) notwendig.



Übersicht Circle of Trust

Motivation

Da die CAS externer Anbieter nicht Teil der Core Infrastructure sind, besteht zwischen SP und CAS kein gegebenes Vertrauensverhältnis. Diese Vertrauensbeziehung ist aber in vielen Fällen die Grundlage dafür, dass ein solcher Dienst überhaupt angeboten, beziehungsweise in Anspruch genommen werden kann.
Bei einer kleinen Anzahl von CAS und SP ist es möglich, Vertrauensbeziehungen zwischen den Komponenten bilateral zu regeln. Wird die Infrastruktur aber grösser, skaliert diese Methode unzureichend. Der organisatorische und technisch administrative Aufwand wäre zu gross.



Workflow Metadaten Austausch

Idee

Die Claim Assertion Infrastructure basiert technisch auf dem offenen Standard SAML 2.0 des OASIS Konsortiums. Dieser Standard sieht vor, den Aufbau von Vertrauensbeziehungen durch den Austausch von Metadaten zu realisieren. Im Software Development Kit der SuisseID-Projekt, welches Referenzcharakter besitzt, ist die Verwendung von Metadaten noch nicht vorgesehen.
Das Konzept sieht vor für den Aufbau von Vertrauensbeziehungen zwischen CAS und SP SAML Metadaten zu benutzen, die über eine zusätzliche Komponente, der Metadata Registry (MDR), ausgetauscht werden. Dazu ist vorgesehen, dass CAS und SP ihre Metadaten an den gemeinsamen Vertrauensanker senden können und sich damit bei einer Vertrauens-Community anmelden. Für die Vertrauensgemeinschaft, im Konzept «Circle of Trust» genannt, müssen bestimmte Regeln gelten. Diese Regeln werden bei der Registrierung bei der MDR manuell überprüft. Durch die Delegation der Überprüfung und der Verteilung der Metadaten, skaliert der «Circle of Trust» auch bei einer wachsenden Anzahl von Mitgliedern gut. Innerhalb des «Circle of Trust» vertraut jede Komponente jeder anderen, sofern sie ihr nicht explizit das Vertrauen abspricht.»

Sandro Leoni

Tobias Merz

Kevin Schneider