SuisseID ‹CAS as a VM›

IT-Security / Betreuer: Prof. Gerhard Hassenstein
Experte: Prof. Dr. Andreas Spichiger

Der ‹CAS as a VM› ist eine als virtuelle Maschine konzipierte und lizenzfreie Implementation des Claim Assertion Services. Dieses System bildet in der SuisseID-Welt eine Art Auskunftsdienst für beliebig konfigurierbare Informationen aus verschiedenen internen LDAP- und MySQL-Datenquellen über einen auf dem CAS registrierten Benutzer. Diese Informationen lassen sich, ausschliesslich mit der aktiven Zustimmung des jeweiligen Benutzers, von jedem SP (Service Provider) signiert und somit beglaubigt abrufen.

Ausgangslage

Mit der SuisseID existiert seit dem Frühling 2010, lanciert durch das Staatssekretariat für Wirtschaft (SECO), die erste standardisierte Methode, um eine Person elektronisch sicher zu authentifizieren. Weiter lassen sich damit eine kleine Anzahl von Informationen, welche klassischerweise auch in einem Pass abgedruckt sind, über dieses System abrufen. Diese sogenannten Core-Attribute werden von der Basis-Infrastruktur, den IdPs (Identity Provider), in signierter und somit beglaubigter Form dem Benutzer zur Verfügung gestellt.
Damit der SuisseID-Welt zusätzliche, zu den durch die IdPs gelieferten begrenzten, Informationen zugänglich gemacht werden können, wurde der CAS als Konzept durch die Arbeitsgruppe der SuisseID ausgearbeitet.

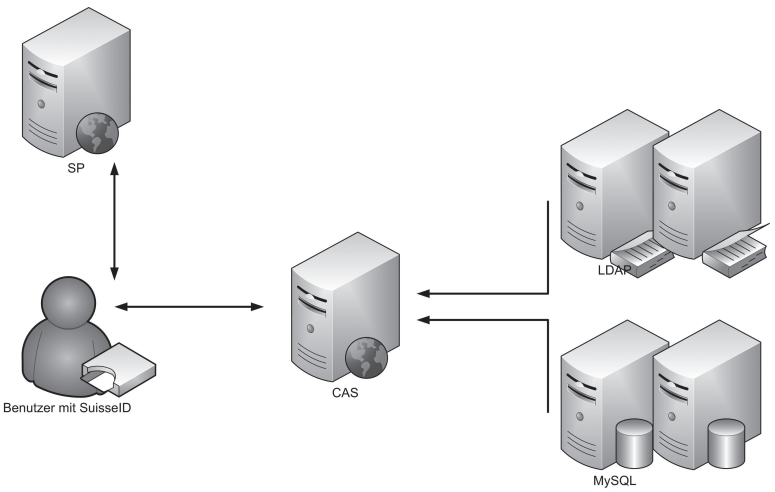
Zielsetzung

Damit die einzelnen Firmen und Verbände, welche Informationen über Benutzer anbieten wollen, einen CAS kostengünstig und einfach bei sich einbinden können, soll mit diesem Projekt ein lizenzfreier und durch den jeweiligen Administrator parametrierbarer CAS entwickelt werden. Der CAS soll zudem direkt als vollständig lauffähige virtuelle Maschine zum kostenlosen Download angeboten werden, damit das ganze System direkt in die bestehende Umgebung eingebunden und konfiguriert werden kann.

Umsetzung

Um das Konzept als kostenloses System umzusetzen wurden als Betriebssystem CentOS und als Applikationsserver GlassFish gewählt. Aufbauend auf diese Grundlage wurde der CAS gemäss Spezifikation und Konzept als Webanwendung implementiert. Zusammen mit der Administrationsanwendung, ist es dem Administrator des Systems möglich, eine beliebige Anzahl an Datenquellen (zurzeit LDAP-Verzeichnisdienste und MySQL-Datenbanken) an den CAS anzubinden. Basierend auf diesem Datenbestand kann er einzelne Attribute dieser Datenquellen unter einem eindeutigen Namen der SuisseID-Welt zum Abrufen anbieten. Optional lassen sich die Ausgabewerte der Attribute anhand von Übersetzungsregeln vor der Ausgabe abändern.
Um den Dienst nutzen zu können, muss der Benutzer zuerst mit seiner SuisseID-Nummer und internem Benutzernamen vom Administrator auf dem CAS registriert werden. Zudem muss jeder dieser Einträge vom jeweiligen Benutzer zusammen mit seiner SuisseID und seinem internen Passwort validiert werden. Damit ist sichergestellt, dass jegliche Daten nur an den eigentlichen Benutzer ausgegeben werden.

Florian Bänziger
suisseid@sysdev.info



Interaktion des Benutzers mit dem SP und dem CAS mit dessen unterstützten Datenquellen