Identity Management System

IT-Security / Betreuer: Prof. Dr. Eric Dubuis
Experte: Dr. Igor Metz

Eine föderative Zugangslösung für externe Personen soll unter Berücksichtigung realer Gegebenheiten und Anforderungen des Bundes untersucht werden. Dem Stand und Trends im Identity Management folgend wurde ein Lösungskonzept nach dem Vorbild von SWITCHaai gewählt, das technisch auf SAML und Shibboleth basiert. Anhand des Anwendungsfalls «Internetcafé beim VBS» wurde ein architektonischer Durchstich realisiert und dokumentiert. Es konnte gezeigt werden, dass sich mit relativ geringem Aufwand ein organisationsübergreifendes Identity Management aufbauen und flexibel erweitern lässt.

Ausgangslage

In der Studie werden Stand und Trends im Identity Management untersucht, wie die Vision der öffentlichen Hand sowie der Bedarf seitens Wirtschaft und Privatpersonen. Es hat sich gezeigt, dass sich beim Bund noch kein übergreifendes Lösungskonzept abzeichnet. Weiter hat die Analyse ergeben, dass der föderative Ansatz beim Identity Management ein gangbarer Weg sein kann, der sich mit der Föderation SWITCHaai im universitären Umfeld durchgesetzt und gut bewährt hat. Das nähere Studium ihrer organisatorischen und technischen Lösung hat ergeben, dass sich eine Kopie dieser Lösung nach denselben Prinzipien und Standards auch für Bundesämter oder grössere Firmen realisieren liesse.

Anwendungsfall Internetcafé

Im VBS werden ca. 200 Internetcafé Arbeitsplätze in der ganzen Schweiz verteilt betrieben. Ein neuer Bundesratsbeschluss fordert, dass der Internetzugang nur noch mit einer persönlichen Identität gewährt werden darf. Nach dem föderativen Ansatz von SWITCHaai für die organisationsübergreifende Authentifizierung und Autorisierung von Benutzern wird gezeigt, wie ein technisches und organisatorisches Lösungskonzept aussehen könnte, das die neuen Auflagen für Gäste beim Zugang zum Internet erfüllt und bei dem parallel auch der Zugang für interne Mitarbeitende mit Smartcard möglich ist.

Technisches Lösungskonzept

Für die technische Umsetzung des Anwendungsfalls wird eine Lösungsarchitektur vorgeschlagen, die auf SAML und Shibboleth basiert. Mit der Implementierung der einzelnen Komponenten auf einer virtuellen Umgebung wurde das Konzept in den wichtigsten Ausprägungen als «Proof of Concept» realisiert und dessen Tauglichkeit verifiziert.

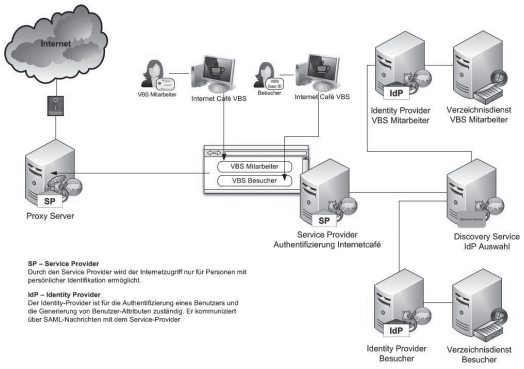
Organisatorisches Lösungskonzept

Die prozessuale, organisatorische Lösung von SWITCHaai basiert auf einem einfachen und klaren Regelwerk über Rechte, Pflichten und Verhalten der Mitglieder in der Föderation, das die Basis für das nötige Vertrauensverhältnis unter allen Parteien bildet. Organisation, Steuerungsgremien und Regelwerk sind im Internet veröffentlicht. Es wird in der Studie dargelegt, wie diese Lösung auf die interne Situation beim VBS übertragen werden könnte.

Ergebnis

Das Ergebnis der Studie gibt einen tragfähigen Rahmen, mit dem das Projekt Internetcafé VBS ohne nennenswerte Risiken umgesetzt werden kann. Die technische Lösungsarchitektur ist im Innern und gegen aussen flexibel erweiterbar. Je stärker sich die organisatorische Umsetzung an die Vorlage von SWITCHaai anlehnt und dies andere ebenso tun, umso leichter lassen sich Föderationsinseln zu grösseren Föderationen zusammenschliessen. Technisch müsste es möglich sein, SuisseID für die Identifikation einzusetzen, wenn sie sich als helvetischen Standard durchsetzt.

Lea Fabienne Dolder



Authentifizierungsplattform für den Anwendungsfall Internetcafé VBS mit föderativem Ansatz