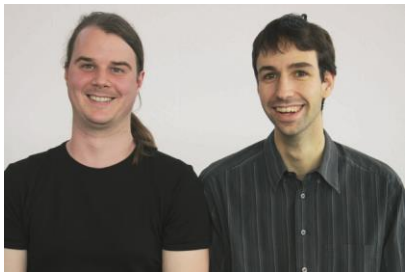
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

Federated Identity Management



Diplomierende
Pirmin Felber
Michael Petri

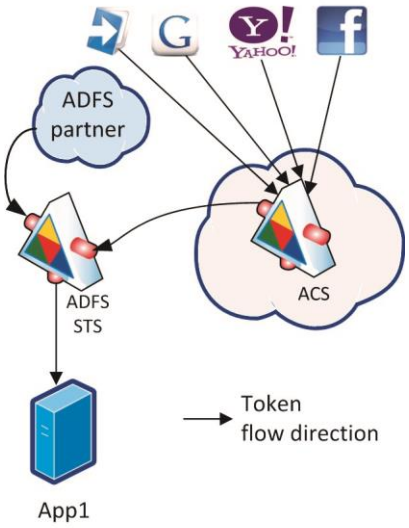
Dozent
Eduard Mumprecht

Nahezu jede geschäftsrelevante Web-Applikation authentifiziert Benutzer und autorisiert diese. Gehören Benutzer und Betreiber einer Applikation unterschiedlichen Organisationen an, entstehen neue Probleme im Identity Management und der Sicherheit. Das Konzept der claims based Identity fanden wir in unserer Projektarbeit als mögliche Lösung. Kernidee dieses Konzepts ist die Aufteilung von Authentifizierung und Autorisierung auf zwei Parteien. Der Claims Provider übernimmt die Authentifizierung der Benutzer und bildet deren Eigenschaften als Claims in sogenannten Tokens ab. Die Relying Party konsumiert Tokens und autorisiert (erteilt Berechtigungen) aufgrund der darin enthaltenen Claims. Vertreter beider Parteien tauschen Tokens nur innerhalb einer Federation aus. Bindeglied zwischen Claims Provider und Relying Party ist ein gegenseitiger federated trust.

In dieser Bachelorarbeit geht es um die Endpunkte der Federation – also das Zusammenspiel von Claims Provider und Relying Party. Wir untersuchen die Handhabung der Tokens und die korrekte Interpretation der gehandelten Informationen über die Benutzer. Ferner zeigen wir das Zusammenwirken der verschiedenen Systemteile anhand eines konkreten Prototyps.

Wir verschafften uns mit umfassendem Literaturstudium einen guten Überblick über verschiedene Modelle und Ansätze. Mit Microsoft ADFS 2.0 und WIF liegen konkrete Komponenten vor, mit denen sich das Konzept der claims-based Identity in einem Microsoft Umfeld realisieren lässt. Anhand einer realen Situation erarbeiteten wir sowohl mit der Bison IT Service AG als auch mit der fenaco Informatik sinnvolle Prototypen.

Die vertiefte Auseinandersetzung mit den Endpunkten der Federation und der Bau eines Prototyps führten zu konkreten Empfehlungen für den Betrieb einer ADFS Infrastruktur. Wir zeigen, dass sich mit ADFS 2.0 und WIF das Konzept der claims based Identity zuverlässig und kostengünstig umsetzen lässt. Eine Herausforderung nach dieser Arbeit bleibt die Erstellung und Verwaltung von Autorisierungsregeln. Hier empfehlen wir weitere Nachforschungen.



Mittels Föderationen können sowohl Identitäten öffentlicher Claims Provider (LiveId, Google, Facebook etc.) als auch nicht öffentlicher Claims Providern über Organisationsgrenzen hinweg genutzt werden.