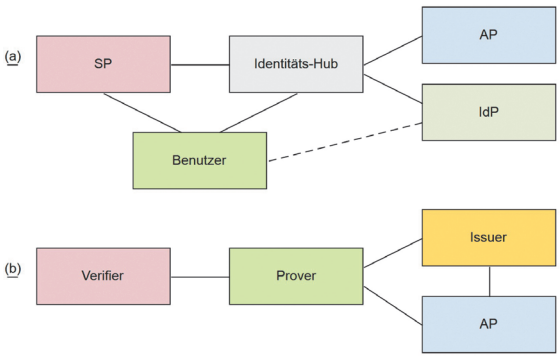
Mehr Privatsphäre durch Authentisierung mit U-Prove

Studiengang: Master of Science in Engineering | Vertiefung: Informations- und Kommunikationstechnologien
Betreuer: Dr. Annett Laube
Experte: Dr. David-Olivier Jaquet-Chiffelle

U-Prove ist eine Technologie zum Schutz der Privatsphäre (Privacy-Enhancing Technology, PET) basierend auf kryptographischen Protokollen. U-Prove wurde in eine bestehende Identity Federation integriert, um die sensiblen Daten der Benutzer zu schützen und ihnen zu erlauben, sich anonym im Internet zu bewegen. Das erarbeitete Konzept, bestehend aus Identitäts-Hub und U-Prove, wurde prototypisch umgesetzt und Auswirkungen auf die Privatsphäre der Benutzer detailliert analysiert.

Ausgangslage

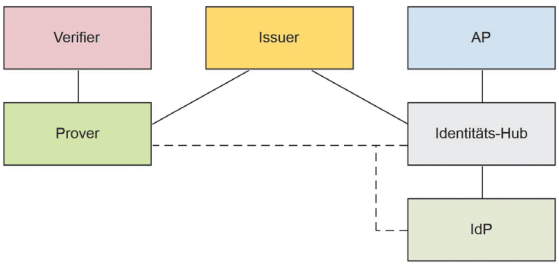
Viele Web-Anwendungen lagern heute die Authentisierung ihrer Benutzer an Identitätsprovider oder Vermittler von Identitätsdiensten aus. Die Vorteile für Anbieter von Web-Anwendungen bringen aber starke Eingriffe in die Privatsphäre der Benutzer mit sich. Jeder Teilnehmer einer solchen Identity Federation kann Daten über die Benutzer sammeln und im Austausch mit anderen sehr umfangreiche Profile über das Verhalten der Benutzer erstellen. Ziel dieser Arbeit ist die Unterbindung dieses Datenaustausches sowie die Erstellung solcher Profile.
Die BFH betreibt eine Identity Federation nach eCH-0168. Abb. 1a zeigt die Ausgangslage der Identity Federation für diese Arbeit. Der Hub ist die zentrale Vermittlungsinstanz zwischen Service Provider (SP) und Identity Provider (IdP) und erhält dadurch alle Benutzerinformationen (Attribute). Mit Hilfe von U-Prove – dessen Konzept in Abb. 1b ersichtlich ist – soll einerseits die Einsicht der Daten minimiert und andererseits Attribute anonymisiert freigegeben werden können.



(a) Identity Federation eCH-0168 (b) U-Prove Konzept

U-Prove

Die Authentisierung erfolgt über sogenannte Tokens mit einem vorgängig berechneten Proof. Die Tokens generieren Issuer und Prover (Benutzer) gemeinsam. Dadurch kennt der Issuer die eindeutige Token ID nicht. Eine Prooferweiterung mit einem SetMembership- oder Range-Proof erlaubt dem Prover, Attribute anonym freizugeben. Der SetMembership-Proof dient dem Beweis, dass das Attribut zu einer vom Verifier (SP) definierten Gruppe gehört. Der Range-Proof verhält sich ähnlich und wird für nummerische Werte verwendet.
Die Prover Attribute für die Tokengenerierung werden bei einem Attribute Provider (AP) bezogen. Die Attribute sind für den Issuer im Klartext ersichtlich. Eine Verblindung der Attribute auf dem AP verhindert, dass Instanzen zwischen AP und Prover die Attribute einsehen können.



Kombinationslösung mit Identitäts-Hub und U-Prove

Schlussfolgerung

Durch die Integration von U-Prove in den Identitäts-Hub – in Abb. 2 – kann die Privatsphäre des Benutzers verbessert werden. Zusatzproofs – wie SetMembership- und Range-Proof – erlauben anonymisierte Attributwerte bei der Freigabe. Durch die Attributverblindung auf dem AP sind die Attribute nur noch für den Prover selber einsehbar. Das beschriebene Konzept zeigt auf, welche Vorteile eine Einbindung von U-Prove bringen kann und welche Grenzen zu beachten sind.

Bojan Leimer