Generalized Identity Management

Studiengang: BSc in Informatik | Vertiefung: Distributed Systems and IoT
Betreuer: Prof. Dr. Andreas Danuser
Experte: Dr. Igor Metz

Über eine zentrale Plattform werden Identitätsdaten gepflegt, Freigaben verwaltet und Mutationen sicher an die berechtigten Organisationen und Applikationen übertragen. Der Identitätsbesitzer erhält hiermit eine Übersicht und die volle Kontrolle über seine Daten.

Ausgangslage

Bei zahlreichen Organisationen und Softwareanwendungen werden heute Personalien und Attribute (Identität) von Personen (ID-Besitzer) erfasst, verwaltet und an verschiedensten Orten in verschiedenen Applikationen gespeichert. Bei einer Mutation der Daten müssen diese manuell an den verschiedenen Orten angepasst werden und manch ein Ort wird vergessen.

Konzept

Nun wird eine Plattform aufgebaut, auf dieser die Organisationen (Abonnent) die Identität einer Person abonnieren können. Auf dieser Plattform kann der Besitzer seine Identität zentral erfassen, seine Abonnenten granular verwalten und bei Mutationen die Abonnenten automatisch benachrichtigen lassen. Damit die Identität der Person geschützt bleibt, werden die Daten beim Speichern verschlüsselt, bei der Übertragung mit End-to-End-Verschlüsselung geschützt, sowie zur Prüfung der Authentizität zusätzlich signiert.

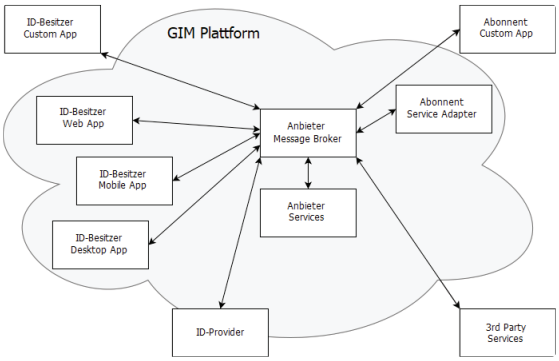
Implementation

Als Resultat wurde eine Plattform mittels Web-Technologien aufgebaut. Dazu gehören eine Web-Applikation (Vue.js), ein Message-Broker (NATS via WebSocket) für die Datenübertragung, diverse Services für Backup und Benutzerverwaltung, sowie eine Demo Implementation von einem Abonnenten.
Die zugrunde liegende Architektur basiert auf Events und auf konfliktfrei replizierbare Datentypen (CRDTs), verpackt in einer wiederverwendbaren Kernkomponente. Die Kernkomponente benutzt das GunDB-SEA Security Modul zur benutzerseitigen Verschlüsselung, Entschlüsselung und Validierung der Daten.

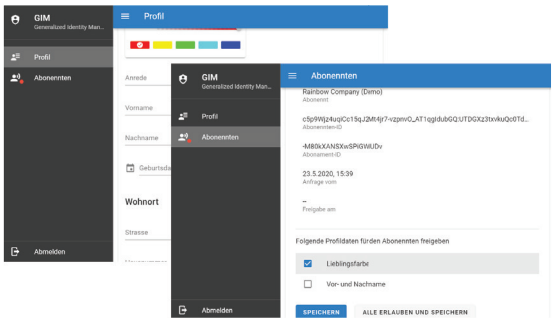
Resultat

Durch die eventbasierte Architektur bietet die Plattform Echtzeit-Eigenschaften, granularen Änderungsverlauf der Identität, Entkopplung für Systemkomponenten, sowie einfache Anbindung an bestehende Systeme. Aufgrund der benutzerseitigen Verschlüsselung hat der Plattformanbieter weder die unverschlüsselten Daten noch das Passwort des Benutzers. Dank dem Message Broker und dem Backup-Service, sind die Applikationen und Services technisch und zeitlich voneinander entkoppelt.

Joel Randy von Allmen
joel.vonallmen@gmx.ch



Gesamtarchitektur mit dem Message Broker als Verbindungspunkt zu allen Applikationen und Services



Vorschau der WebApp mit Profileditor und Freigabeverwaltung von Abonnenten