

Registration Authority as a Service

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Gerhard Hassenstein
Experte: Prof. Dr. Andreas Spichiger (BFH)

Das Eidg. Justiz- und Polizeidepartement betreibt an weltweit verteilten Standorten Infrastrukturkomponenten zur Registrierung und Verifikation von biometrischen Ausweisdokumenten. Das Projekt Registration Authority as a Service (RaaS) automatisiert das Lifecycle Management von Zertifikaten für entsprechende Biometrie-Systeme. Zu den zentralen Funktionen gehört das initiale Ausstellen von Private-Key-Containern sowie das Erneuern und Revozieren von Zertifikaten.

1

Ausgangslage

Die Biometrie-Infrastruktur des Eidg. Justiz- und Polizeidepartements umfasst dezentrale Systeme, die sich an kantonalen Aussenstellen, Botschaften oder Konsulaten befinden. Diese Systeme benötigen zur Bereitstellung von unterschiedlichen kryptographischen Funktionalitäten Zertifikate. Sie werden unter anderem eingesetzt, um die Kommunikation zwischen den Aussenstandorten und der lokalen Biometrie-Infrastruktur in Bern zu verschlüsseln bzw. Requests zu signieren. Mit der bisherigen Lösung mussten Zertifikate nach deren Ablaufdatum über einen manuellen Prozess erneuert und verteilt werden. Im Rahmen einer Architektur Anpassung werden Erfassungsgeräte neu über eine Webanwendung gesteuert, was zu erhöhten Anforderungen bezüglich Ausstellung und Erneuerung von Zertifikaten führt.

Ziel

Registration Authority as a Service stellt dezentralen Biometrie-Systemen einen sicheren Webservice für ein automatisiertes Management von Zertifikaten bereit. Die Systeme an den Aussenstandorten sollen Zertifikate selbstständig erneuern oder revozieren. Darüber hinaus umfasst die Lösung eine Webapplikation für administrative Tätigkeiten. Dazu zählen das ini-

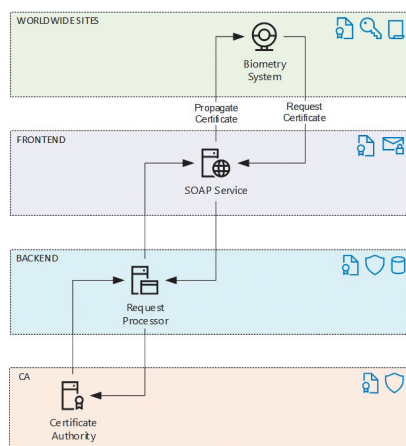
tiale Ausstellen von Private-Key-Containern, die Verwaltung von Entitäten und Request-Policies, sowie die Definition von Approval- und Alarmierungsmechanismen. Schwerpunkte dieser Bachelorthesis liegen in der Implementierung der einzelnen Komponenten und deren Schnittstellen. Aufgrund sensibler Daten, die mit Zertifikaten des Systems verschlüsselt werden, resultieren hohe Anforderungen an die Sicherheit der Gesamtlösung. Im Rahmen dieser Arbeit werden Softwarekomponenten für einen produktiven Betrieb entwickelt und die Infrastruktur für eine Aufnahme des Betriebs bereitgestellt. Nach dem Rollout sollen ca. 700 Biometrie-Erfassungsstationen weltweit Zertifikate der Lösung verwenden, um sicherheitskritische Aufgaben wie «Ausweisdokumente ausstellen», «Visa erteilen» oder «biometrische Daten verifizieren» auszuführen.



Othmar Kesseli

Realisierung

Die RaaS-Infrastruktur umfasst eine Vielzahl von Komponenten, um den Lebenszyklus von Zertifikaten zu steuern. Biometrie-Systeme an verteilten Standorten kommunizieren durch signierte SOAP-Requests mit einem WCF-Frontend-Service. Dieser interagiert über eine RESTful-API mit einer Backend-Komponente, welche entsprechende Methoden zur Verwaltung von Zertifikaten bereitstellt. Dieses Backend-System verwaltet die zentrale Datenbank und steuert über weitere Schnittstellen die Kommunikation zur Certificate Authority und einer Password-Management-Applikation, um Private-Key-Container-Passwörter zu persistieren. Eine Administrationsoberfläche in Form einer Webapplikation erlaubt die Verwaltung von Entitäten und bietet weitere Funktionalitäten um Requests zu steuern und nachzuvollziehen. Das System wurde mit den Microsoft Technologien Windows Communication Framework (Frontend-Service), ASP.NET Web-API (Backend-Service) und ASP.NET MVC (Administration-GUI) entwickelt.



Systemübersicht