Authentifizierung für das generische Zugriffskontrollsystem KeyRing

Studiengang: Master of Science in Engineering | Vertiefung: Information and Communications Technologies
Betreuer: Prof. Dr. Annett Laube
Experte: Prof. Dr. Andreas Spichiger (Bundeskanzlei, Bereich Digitale Transformation und IKT-Lenkung)

Shared Economy ist ein Begriff, der uns immer häufiger begleitet. KeyRing bietet dabei eine Lösung, die ein breites Spektrum von Anwendungsfällen abdeckt. Der vorhandene KeyRing-Prototyp hatte jedoch sicherheitstechnische Lücken. In dieser Thesis wurden Konzepte und die Implementierung von KeyRing analysiert und mit sicheren Authentifizierungsverfahren sowie weiteren Sicherheitsmechanismen ergänzt, ohne die Benutzerfreundlichkeit zu beeinträchtigen.

Ausgangslage

Das generische Zugriffskontrollsystem KeyRing ermöglicht verschiedene Anwendungsfälle wie die Vermietung von Ferienhäusern oder den Zugang zu physischen Systemen. Die vorhandene Implementation realisiert dabei nur das Grundgerüst, welches zur Ausstellung, Verteilung und Verwendung von KeyRing-Token notwendig ist. Ziel dieser Arbeit ist es, Konzepte und die Implementation zu analysieren und dort, wo es als sinnvoll und notwendig erachtet wird, zusätzliche Sicherheitsmechanismen, wie Authentifizierungsverfahren, einzusetzen.

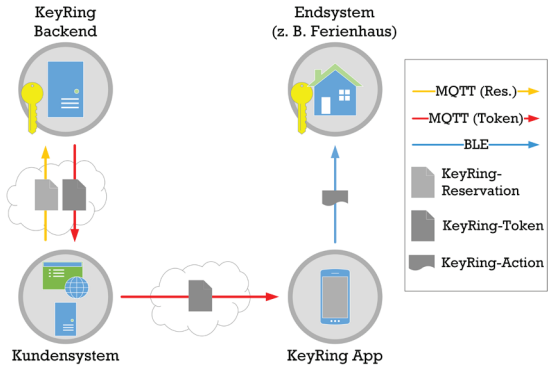
Analyse

Die Analyse fokussierte sich dabei auf drei Hauptbereiche, welche im KeyRing-Netzwerk entscheidend sind. Dabei handelt es sich um die MQTT-Kommunikation für die Übertragung der KeyRing-Tokens, die BLE-Kommunikation als Übertragungsweg zwischen der Smartphone-KeyRing-App und dem Endsystem sowie die Authentifizierung des KeyRing-Benutzers. Anhand dieser Analyse wurde ein neues Authentisierungsverfahren, genannt SMOKER, für die MQTT-Kommunikation eingesetzt, welches auf einem Zero-Knowledge-Verfahren beruht. Dieses Verfahren benötigt dabei keine benutzerspezifischen Daten. Einzig ein öffentlicher Schlüssel für die Zuordnung zu einer Smartphone-App muss bekannt sein. Dieser Schlüssel wird auf einem zentralen Server (Backend) abgelegt, womit der KeyRing-Benutzer von einer Reservationsplattform (Kundensystem) das Smartphone als Empfänger von Tokens auswählen kann. Für die Abfrage dieser Daten wird für die Authentisierung und Autorisierung das «OpenID Connect»-Protokoll eingesetzt. Der zentrale Server (Backend) kann am Beispiel eines Google-Kontos den Benutzer erfolgreich authentifizieren.

Fabian Fischer

Implementation

Anhand der Ergebnisse der Analyse wurde der vorhandene Prototyp weiterentwickelt, so dass der sichere Austausch von Tokens zwischen dem KeyRing-Backend und der Smartphone-KeyRing-App ermöglicht wird. Der KeyRing-Benutzer kann bei einer Reservationsplattform KeyRing-Tokens bestellen, wodurch diese an das gewählte Smartphone übertragen werden. Das Smartphone ist dabei authentifiziert und der Übertragungsweg verschlüsselt. Diese Tokens werden anschliessend durch den Benutzer bei einem Endsystem, wie z. B. bei einem Ferienhaus, genutzt, um Zutritt zu erhalten (siehe Abbildung). Dabei wird eine KeyRing-Action übertragen, welche symmetrisch verschlüsselt ist und nur durch das KeyRing-Backend und das dazugehörige Endsystem entschlüsselt werden kann.



Nachrichtenfluss im KeyRing-Netzwerk

Fazit

Der entwickelte Prototyp erfüllt die geforderten Ziele, so dass verschiedene Anwendungsfälle zu Demonstrationszwecken vorgeführt werden können. Die Tokens werden jederzeit sicher übertragen und die App weist eine einfache Bedienung auf.