arendi

ECC 2017 - Möbelschloss

r&d

arendi

Projektauftrag

Ein Möbelschloss entwickeln, das mit iPhones und Androids geöffnet werden kann.

Anforderungen

- Batteriebetriebenes Möbelschloss
- Nutzung mit Android- und iOS-Smart Devices
- Schloss-Management und Rechtevergabe über Cloud-Anbindung
- Offline-Betrieb
- Optionale Apple HomeKit-Anbindung
- Hoher Schutz gegen Manipulation

arendi

Herausforderungen

Folgenden Punkten mussten wir in diesem Projekt lösen

- Wahl der Technologien
- Austausch und Gültigkeit der Berechtigungen
- Offline-Betrieb
- Security im Allgemeinen
- Sichere Pairing Prozedur
- MFI-Chip
- MFI-Programm

Mehr dazu in den folgenden Minuten

arendi

Wahl der Technologien - Schnittstelle

Wie soll das B-Lock verbunden werden

- NFC (RFID) → nur Android unterstützt
- WLAN → zu hoher Stromverbrauch für Batterien
- LoRa → langsam, schlechte Abdeckung in Gebäuden, keine direkte Smart Phone Verbindung möglich
- ZigBee / Z-Wave → keine direkte Smart Phone Verbindung möglich

→ **Bluetooth LE**

Bluetooth™

arendi

Wahl der Technologien - App

Wie soll die App programmiert werden

- Native Programmierung (Java, Swift)
- Cross Platform

Anforderungen

- Einfaches GUI ohne ausgefallene Feature
- Niedriges Budget
- Entwicklung in der Schweiz → Cross Platform
- Xamarin 2016 von Microsoft übernommen (Tools und Lizenzen vorhanden)

→ **Xamarin Platform**

arendi

Wahl der Technologien - Cloud

Wie und wo sollen die Cloud-Services gehostet werden

- Amazone AWS
- Google Cloud Computing
- Microsoft Azure
- Kostenfrei (OpenSource)

Grundlagen für den Entscheid

- Xamarin 2016 von Microsoft übernommen
- Guter Support von Azure in Xamarin
- Gleiche Tools (Visual Studio) für App- und Cloud-Entwicklung

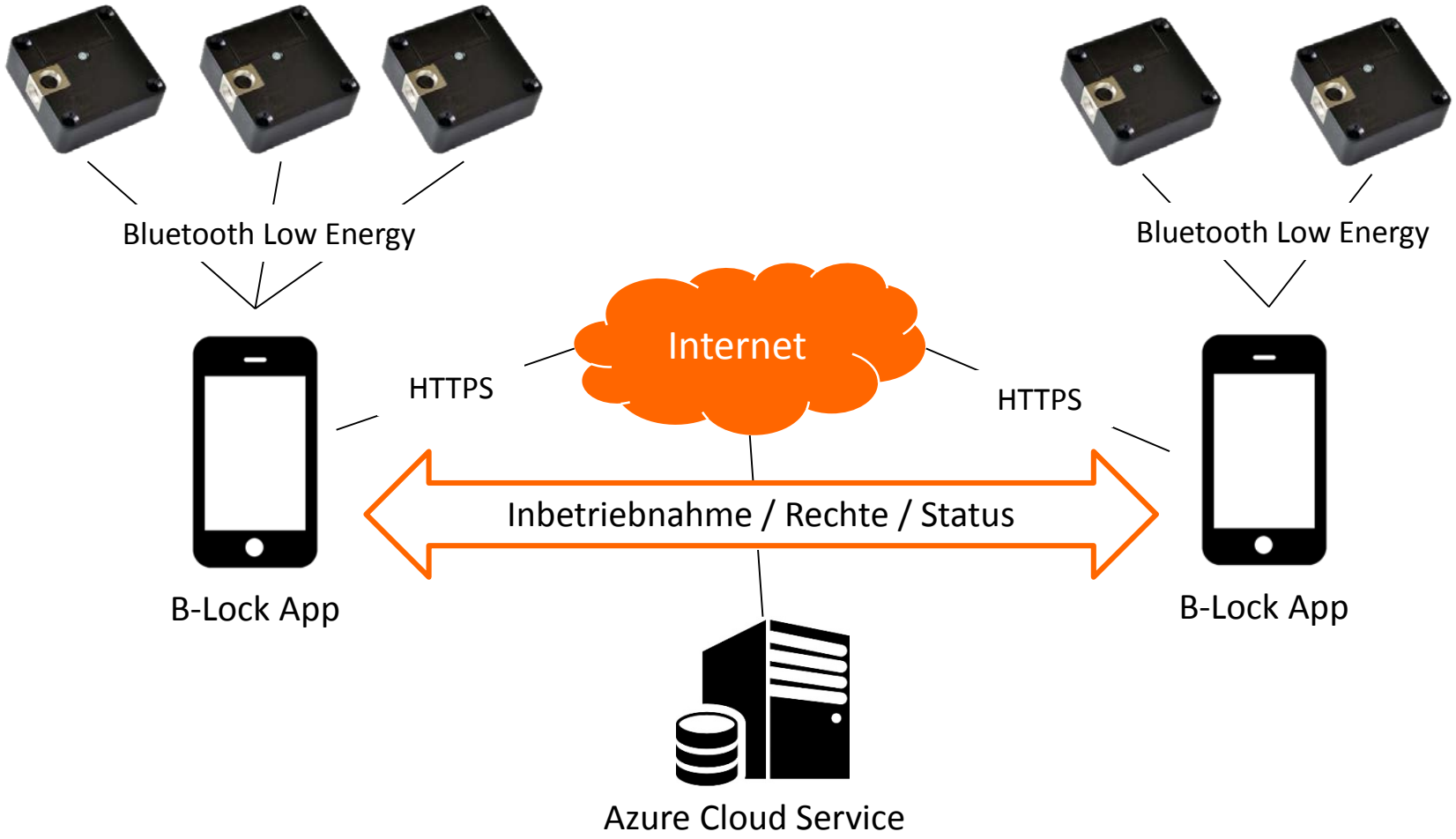
Azure Cloud-Computing-Plattform

Hardware

- Bestehende Mechanik von RFID-Lesern
- Platz für Elektronik beschränkt
- Speisung durch Lithium Batterie vorgegeben
- BLE-Chip Nordic nRF52 im Flat-Design integriert
- Aufwendiges Antennen-Design (Metalle)

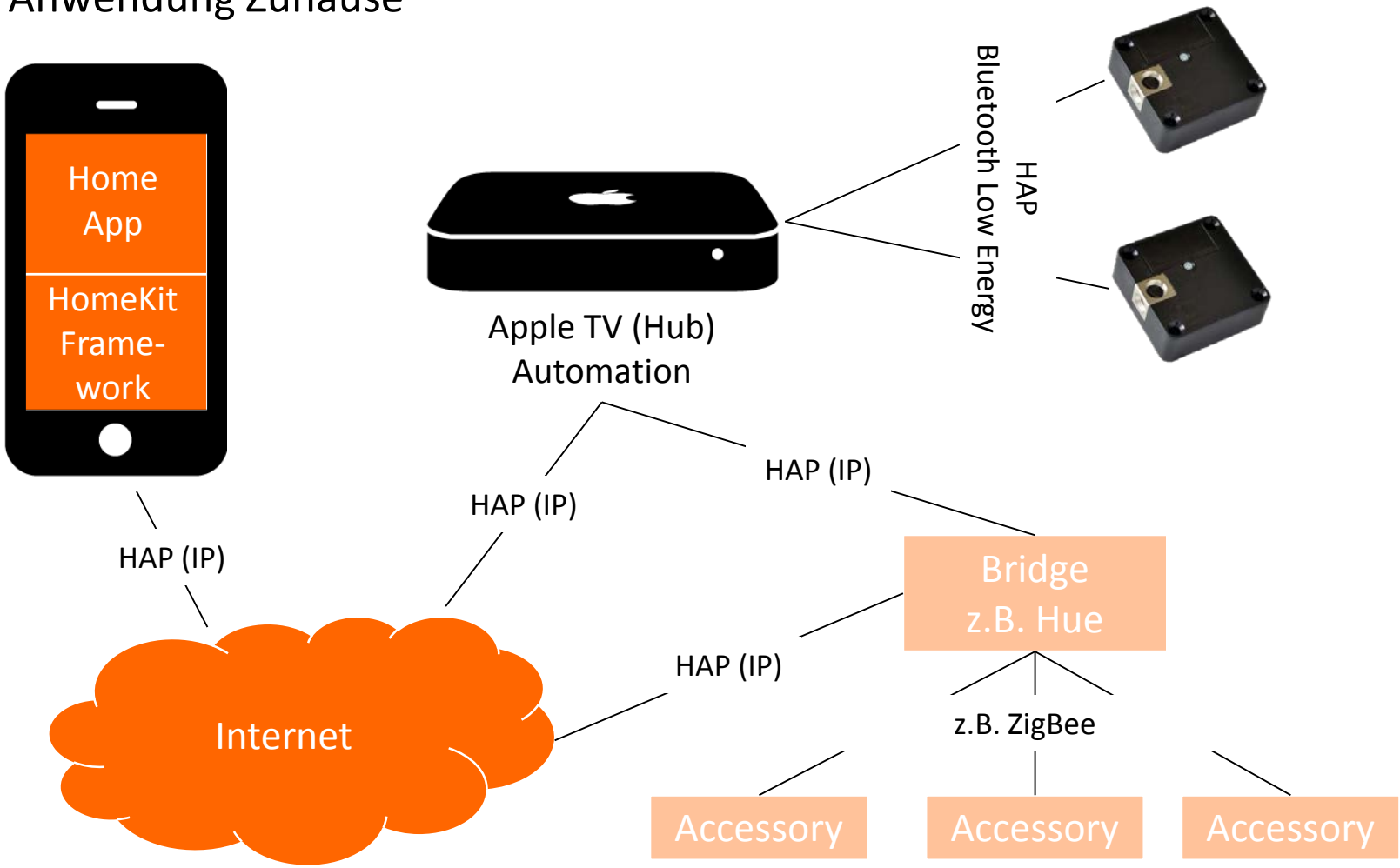
Topologien – Cloud-Lösung

- Für Organisationen und Shops



Topologien – HomeKit

- Anwendung Zuhause



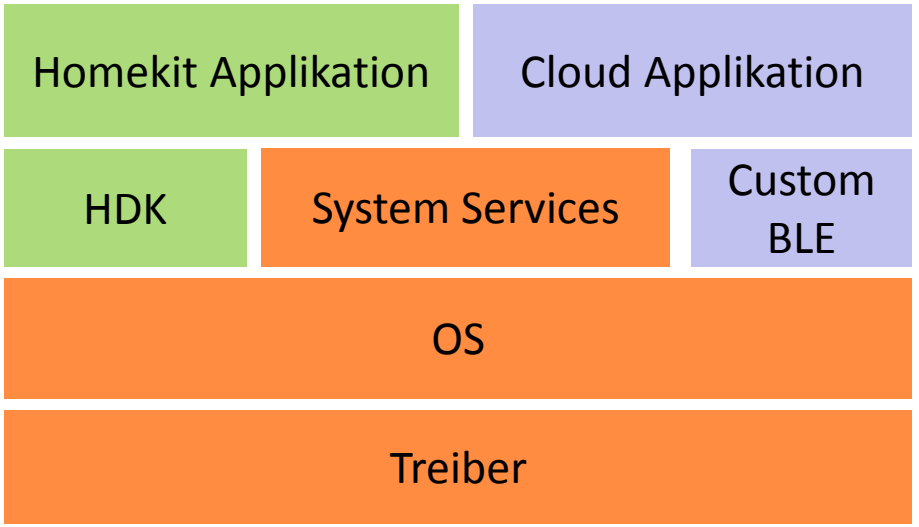
Firmware

Plattformgedanke

- Arendi BLE Plattform
- Treiberschicht: Gemeinsame Basis für Homekit + Cloud-Lösung
- Nordic Homekit Development Kit (HDK)

BLE-Services

- Proprietäre-Services für Cloud-Lösung
- Homekit-definierte Services



Homekit – MFI – «Made for iPhone/iPod»

MFI-Chip benötigt

- Kosten abhängig vom Produktplan
- Hält Zertifikat «Accessory Certificate»
- Stromverbrauch Grössenordnung 80uA(!)
- Chip nur für «Pair-Setup» benötigt

Homekit – MFI – «Made for iPhone/iPod»

MFI-Programm

- Teilnahme zwingend
  → Zugriff auf Dokumentation
  → Zugang zu MFI-Chip Samples
- Lizenzkosten für Nicht-Homekit MFI
- Unterscheidung Development-Partner / Manufacturing-Partner

Homekit – MFI – «Made for iPhone/iPod»

Produktion von MFI-Produkten

- Lizenzierter Manufacturing-Partner nötig
- Produktplan wird von diesem eingereicht
- Bestellung MFI-Chips in Produktionsmengen

arendi

Homekit Application Protocol

VERTRAULICH

arendi

Homekit Security

VERTRAULICH

Cloud-Lösung: Security

- Angelehnt an Homekit
- Erstinbetriebnahme von Lock mit modifiziertem SRP-6a
- Generierung von symmetrischen Long-Term-Keys
- Cloud-Speicherung der LTKs.
- Dauer ca. 10s

- Verschlüsselung mittels 128-bit AES-EAX AEAD-Verfahren
- Nutzung der AES-Hardwarebeschleunigung des nRF52
- Weniger Rechenintensiv, schneller Verbindungsaufbau

Wir sind Ihre Lösung.

Arendi AG
Eichtalstrasse 55
8634 Hombrechtikon
Schweiz

www.arendi.ch