arendi

# ECC 2017 - Möbelschloss

r&d

# 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
- Hoher Schutz gegen Manipulation
- Optionale Apple HomeKit-Anbindung

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**

# 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**

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**

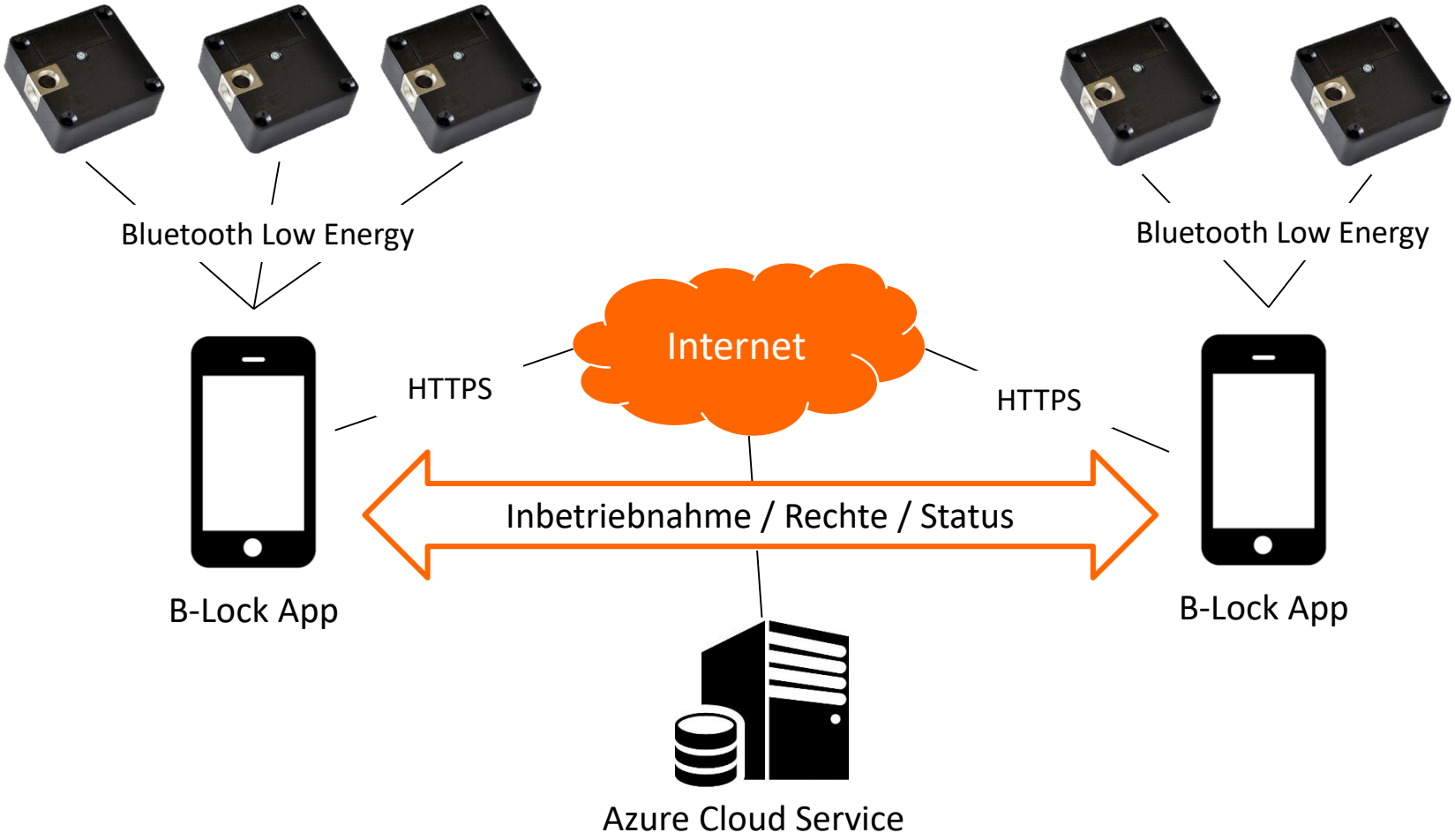
arendi

# 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)

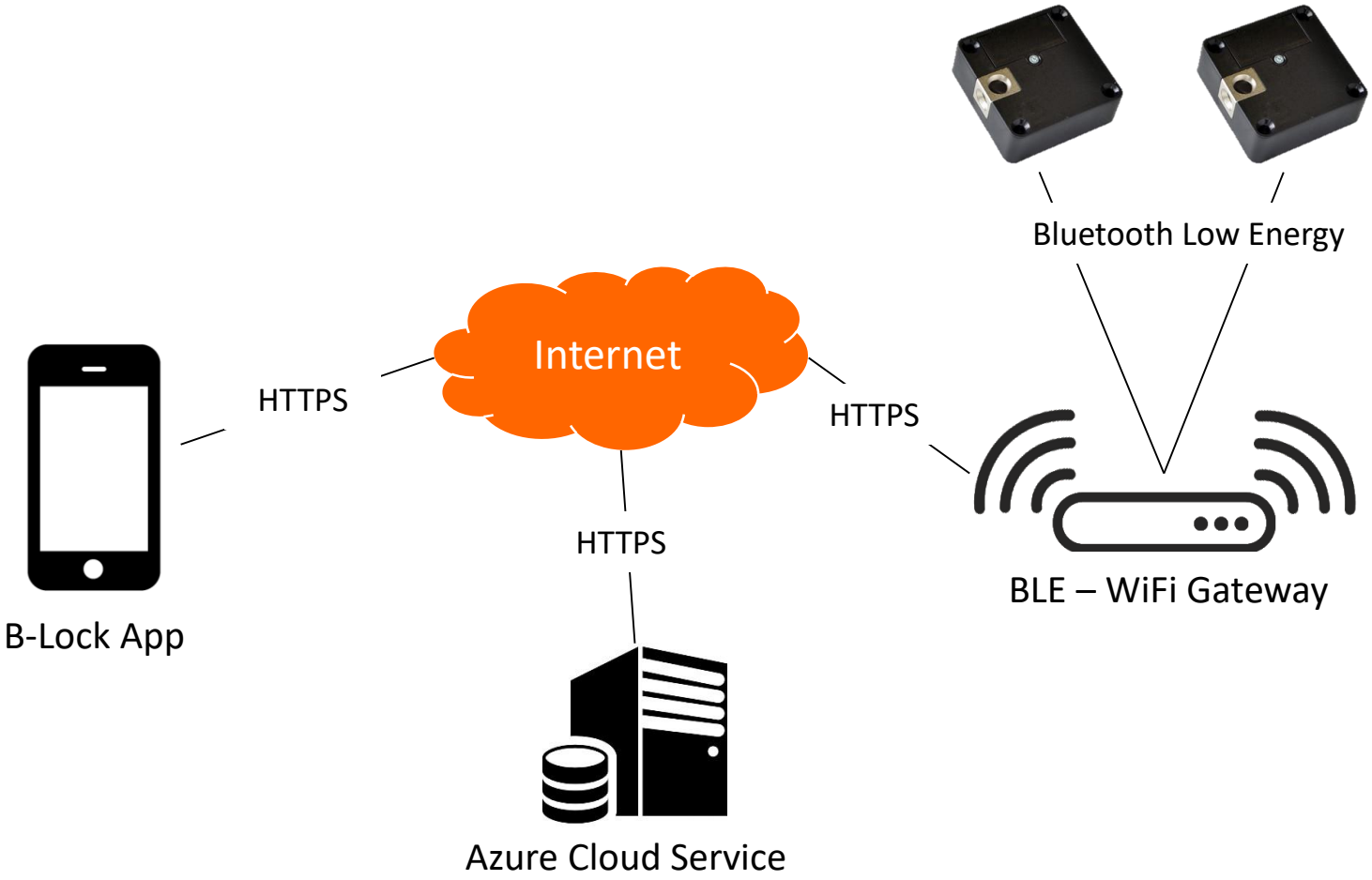
# Topologien – Cloud-Lösung

- Für Organisationen und Shops



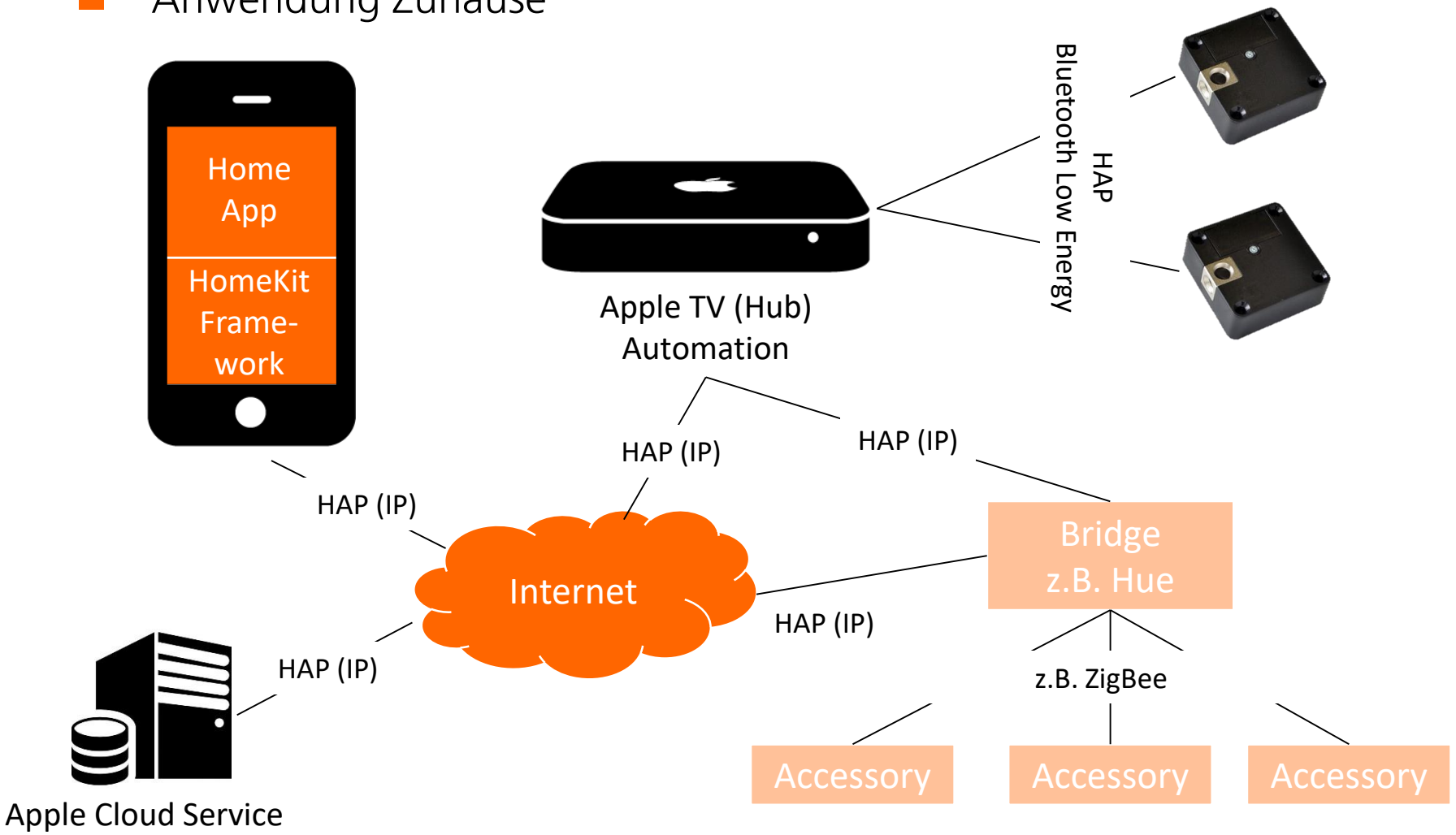
# Topologien – Cloud-Lösung mit Gateway

- Für Remote Zugriff / IoT



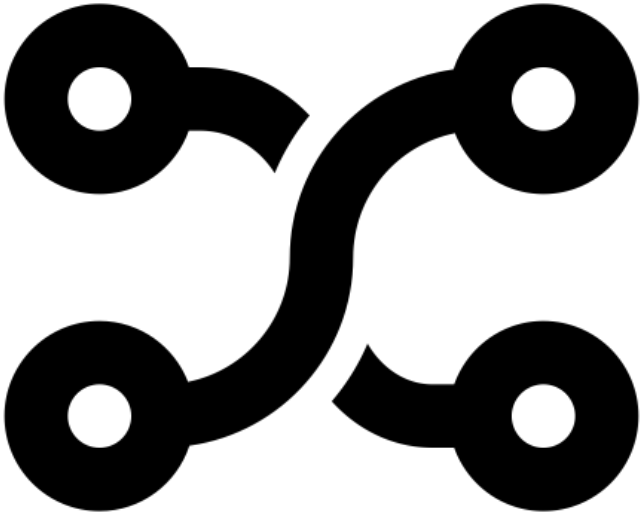
# Topologien – HomeKit

- Anwendung Zuhause



arendi

# Gleich geht’s weiter…



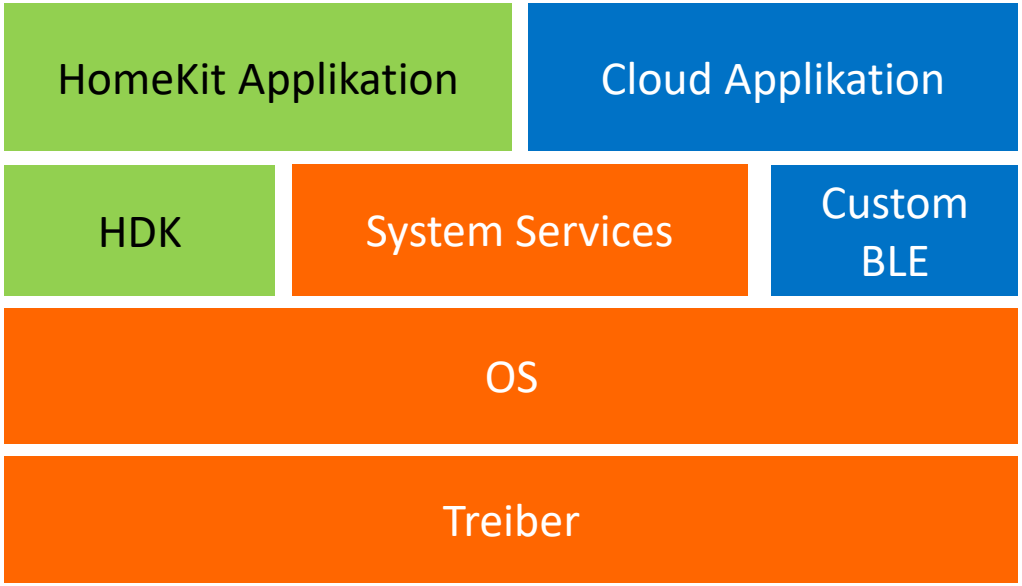
# Firmware

## 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»

- Erlaubt 3rd Party proprietäre Apple-Schnittstellen zu verwenden
- Marketing
- Teilnahme für HomeKit zwingend
  → Zugriff auf Dokumentation
  → Zugang zu MFI-Chip Samples
- Lizenzierter Manufacturing-Partner nötig
- Produktplan wird von diesem eingereicht
- Bezug MFI-Chips in Produktionsmengen


Development Partner

Manufacturing Partner

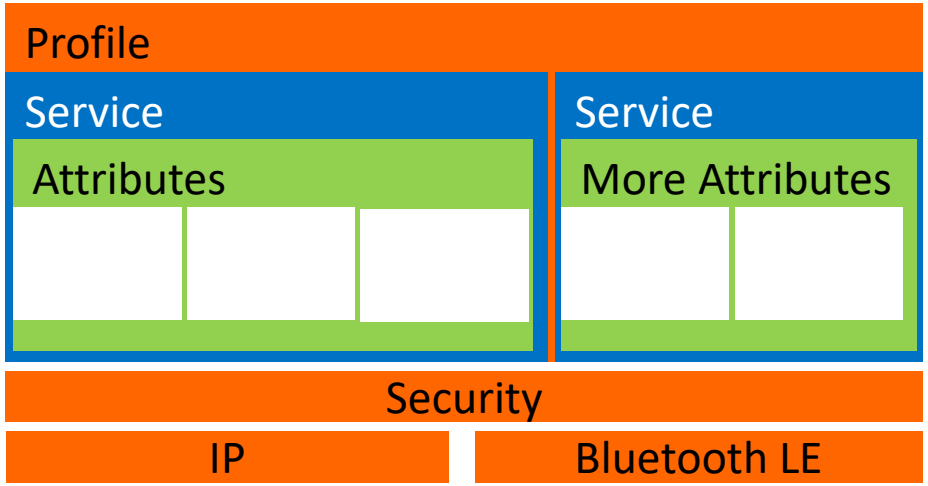
Made for iPod iPhone iPad

# HomeKit – MFI – «Made for iPhone/iPod»

- Authentication Co-Processor
- Hält *«Accessory Certificate»* → Apple-Autorisierung von Accessory
- Challenge / Response
- Kommunikation über $I^2C$
- Ruhestrom: ~30uA
- HomeKit: Chip nur für *«Pair-Setup»* benötigt
  → Kann im regulären Betrieb deaktiviert werden
- Kosten abhängig vom Produktplan…

# HAP – HomeKit Accessory Protocol

- Konzept ähnlich BLE GATT
  → vordefinierte Attribute, Services, (Profile)



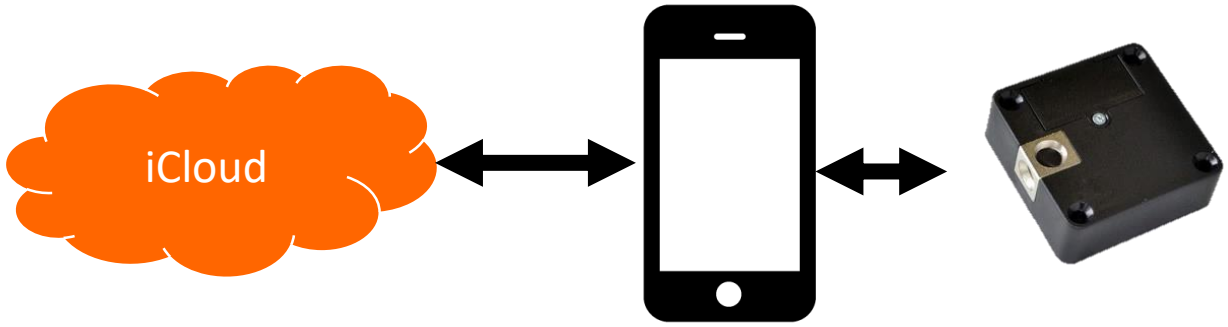

- Serielles TLV-kodiertes Paketformat
- Viele Metadaten → generische Verwendung?
- BLE-Advertising
  →identifiziert Accessory
  →signalisiert Kommunikationsbedarf

# HomeKit – Security

- Vollständig Proprietäre Protokoll-Security
- Verwendet für IP- oder BLE-basierte Accessories.
- BLE-eigene Security Features ungeeignet
  → Bindung an einzelnes Gerät (statt «Cloud»)

**Bluetooth LE Pairing/Bonding**

**HomeKit**



# HomeKit – Security

- End-zu-End-Verschlüsselung und Authentifizierung
  → ChaCha20 Streamcipher (256-bit)
  → Muss in Software gerechnet werden

- *«Pair-Setup»* nach Factory-Reset:
  → Secure Remote Password Protocol (SRP)
  → 8-stelliger Setup code dient als «Passwort»
  → Verhindert Man-in-the-Middle
  → Überprüfung des MFI-Zertifikats eingebunden
  → Sicherer Austausch von Long-Term-Keys

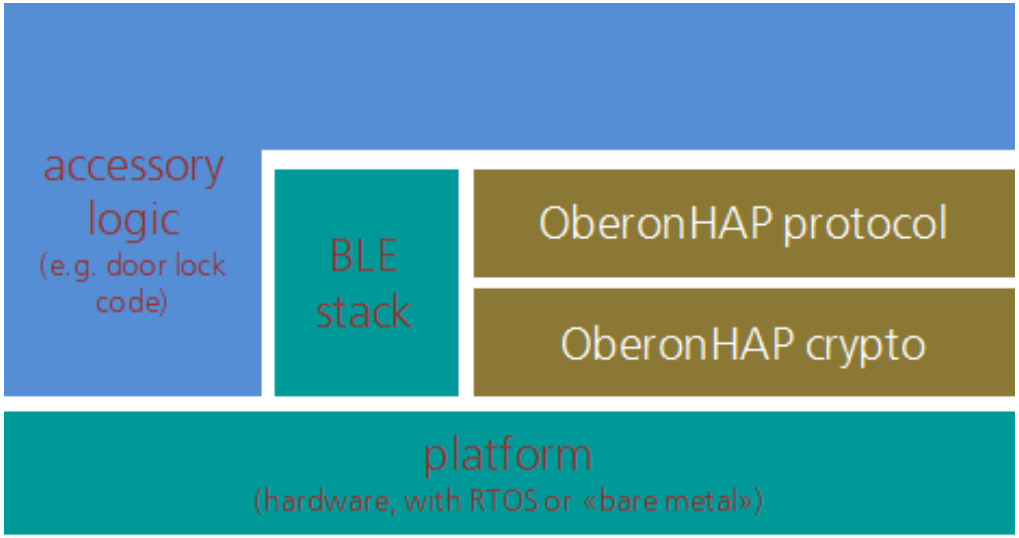
- *«Pair-Verify»* bei jedem Verbindungsaufbau
  → Curve25519 Public Key Exchange
  → Authentisiert mit Long Term Keys und SRP Proof

XXX-XX-XXX

arendi

# HomeKit – Nordic HomeKit SDK

- Zugänglich für MFI-Programm Teilnehmer
- Basierend auf Oberon HAP, Nordic Softdevice
- Proprietäre Umsetzung von HAP, Security
  → Optimiert auf Cortex M-Cores.
  → v.a. rechenintensive Krypto




NORDIC SEMICONDUCTOR

arendi

# Cloud-Lösung – Security

- Angelehnt an HomeKit → Re-use von Crypto
- Erstinbetriebnahme von Lock mit 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 als HomeKit-Variante

# Demo

Beide Lösungen demonstrieren wir am Stand.

arendi

# Wir sind Ihre Lösung.

**Arendi AG**
Eichtalstrasse 55
8634 Hombrechtikon
Schweiz

**www.arendi.ch**

r&d