Kolloquium Masterthesis

im Master-Studiengang Computer Science

Sichere LPWAN-Übertragungen und IoT-Updates am Beispiel eines Smarten Briefkastens

Felix Barz

06.09.2019

Inhalt

1. Einleitung und Ziele der Arbeit
2. Durchführung und Ergebnisse
   a. E2E-Verschlüsselung
   b. Clientseitige Geräte-Aktivierung
   c. Firmware-Updates via LoRaWAN
   d. Sensorik zum Erkennen eines Briefeinwurfs
   e. Entwicklung des Smarten Briefkastens
3. Erkenntnisse und Fazit
4. Demonstration

Einleitung und Ziele der Arbeit

Hauptziele:

- Entwicklung eines Smarten Briefkastens, der mithilfe einer Handy-App über neue Post benachrichtigt
- Sichere, E2E-verschlüsselte Übertragung des Zustands über LoRaWAN
- Verlässliche und authentifizierte Übertragung von Firmware-Updates via LoRaWAN
- Praktische Umsetzung der entwickelten Lösungen

Durchführung und Ergebnisse
E2E-Verschlüsselung

Untersucht wurden:

1. Keine zusätzliche Verschlüsselung
2. Austausch der LoRaWAN-Verschlüsselung
3. Zusätzliche AES-CTR-Verschlüsselung
4. Zusätzliche AES-GCM-Verschlüsselung

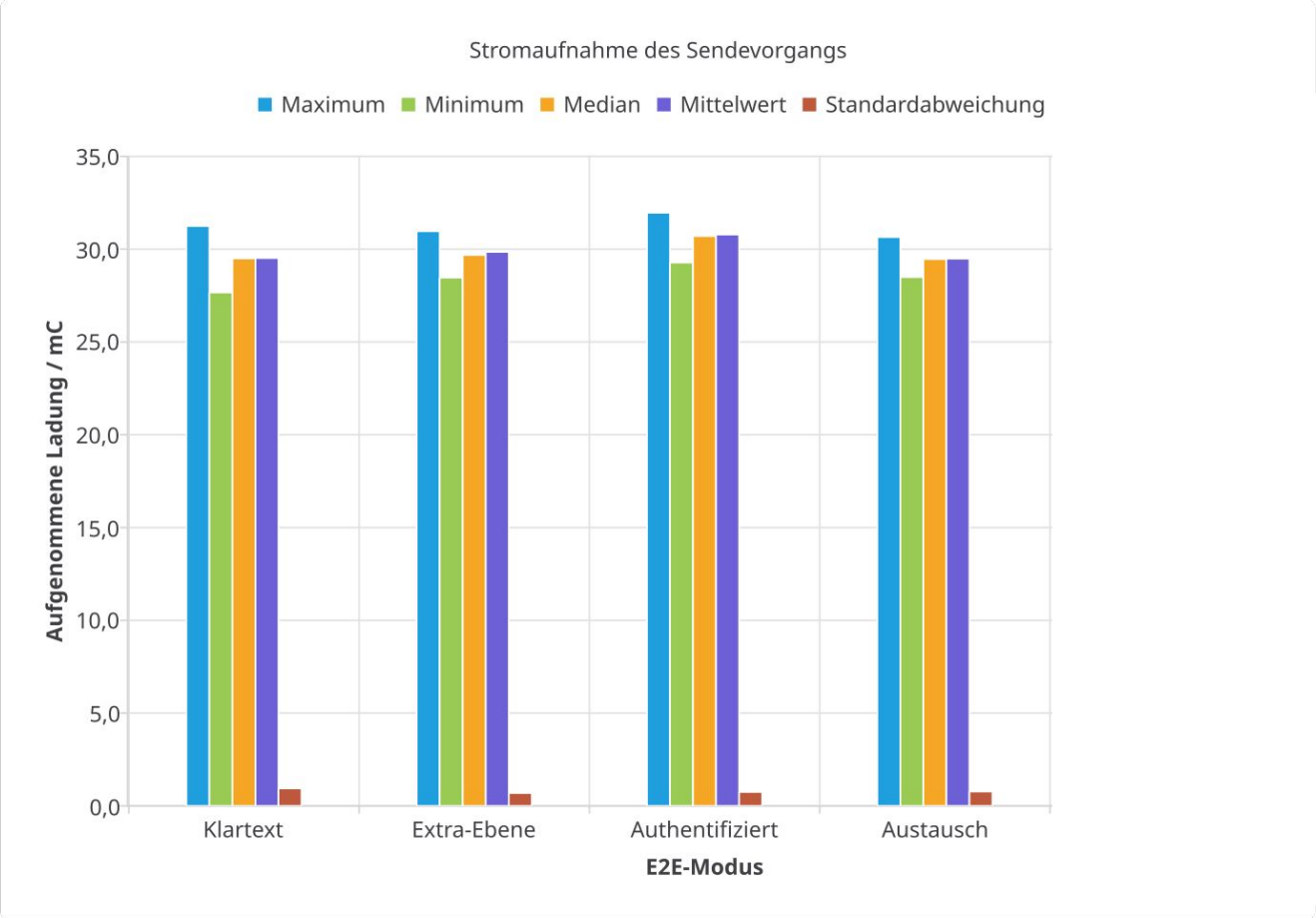
Ziele:

- Untersuchung der Sicherheit
- Untersuchung des Stromverbrauchs

Durchführung und Ergebnisse
E2E-Verschlüsselung

Untersuchung der Sicherheit				
Kriterium	**Unverschlüsselt**	**Austausch**	**AES-CTR**	**AES-GCM**
Vertraulichkeit	nein	ja	ja	ja
Wechselnde IVs	nein	ja	ja	ja
Authentizität	nein	nein	nein	ja

Durchführung und Ergebnisse
E2E-Verschlüsselung



Durchführung und Ergebnisse
E2E-Verschlüsselung

Ergebnisse:

1. Verschlüsselung ist “umsonst”
2. Austausch-Verschlüsselung ist Aufwand ohne Benefit
3. AES-GCM ist am sichersten, benötigt aber mehr Strom

   ➔ Ursache sind die zusätzlichen Bytes

Offene Fragestellungen:

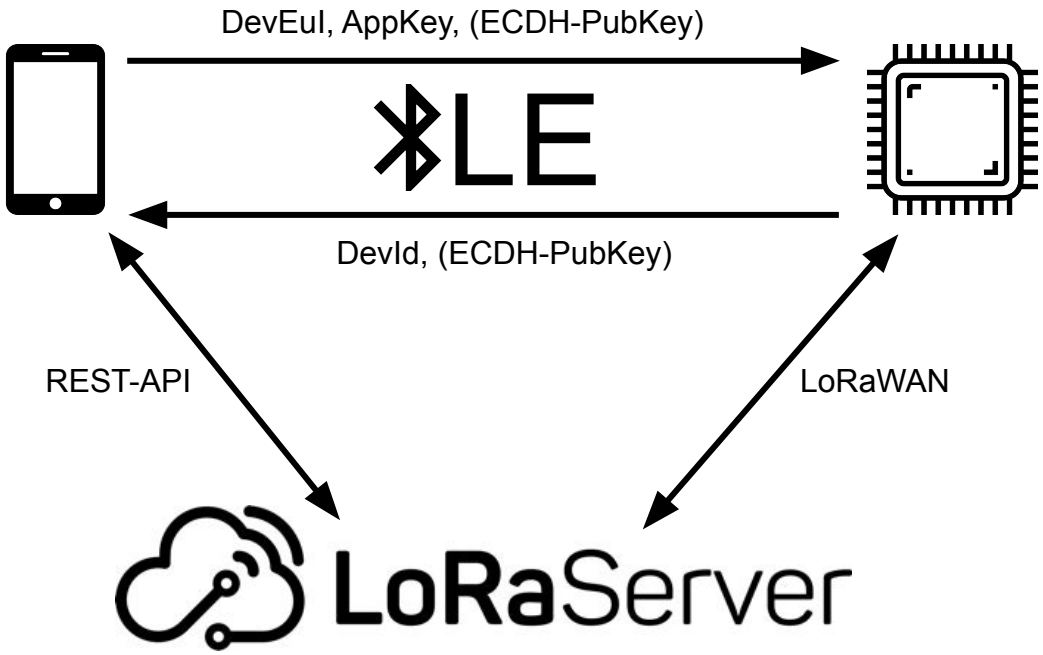
1. Wie lang sollte der GCM-Tag gewählt werden?

Durchführung und Ergebnisse
Clientseitige Geräte-Aktivierung

Ziele:

- Nutzung eines zweiten Kanals
- Dynamische Übertragung der JOIN-Parameter auf das Endgerät
- Sichere Aushandlung des Schlüssels für die E2E-Verschlüsselung

Durchführung und Ergebnisse
Clientseitige Geräte-Aktivierung



Durchführung und Ergebnisse
Clientseitige Geräte-Aktivierung

Ergebnisse:

1. Alle Ziele konnten realisiert werden

Offene Fragestellungen:

1. Gibt es geeignetere Zweit-Kanäle (an Stelle von BLE)?
2. Ist die Anwendung bei anderen Architekturen sinnvoll?

Durchführung und Ergebnisse
Firmware-Updates via LoRaWAN

Ziele:

- Sichere (IA) Firmware-Updates via LoRaWAN
- Praxisnaher Ansatz (Multicast)

Module:

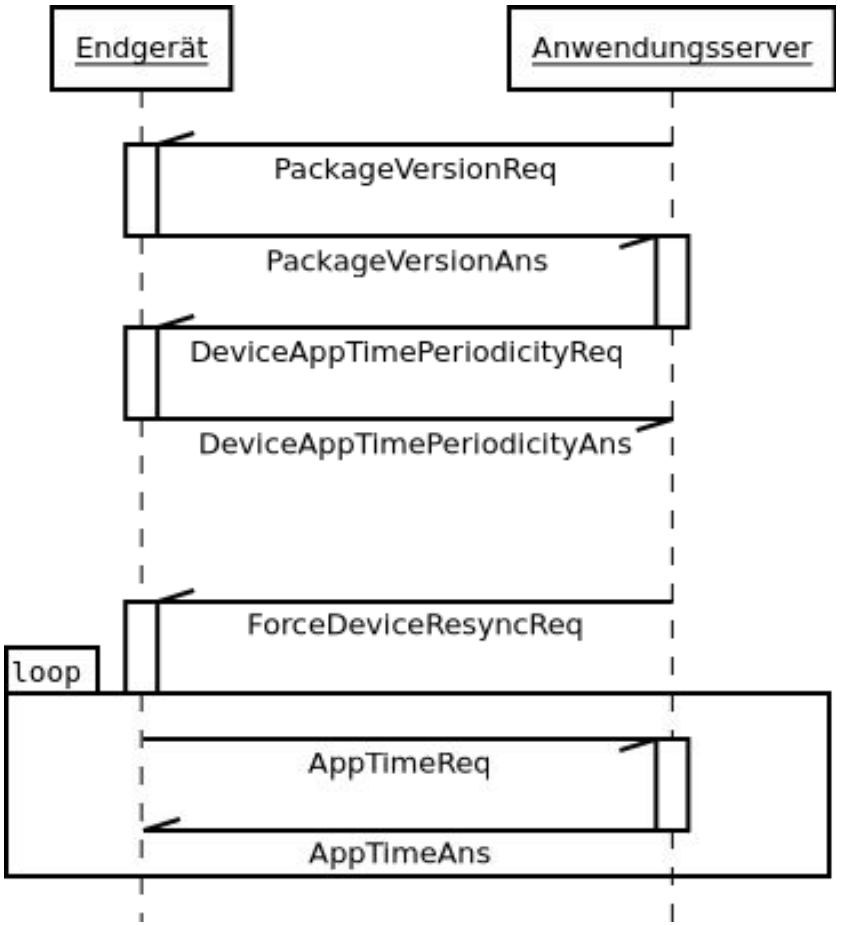
- *Clock Synchronization*
- *Remote Multicast Setup*
- *Fragmented Datablock Transport*
- OTA-Updates

Durchführung und Ergebnisse
Firmware-Updates via LoRaWAN

Clock Synchronization:

- Synchronisiert Serverzeit mit dem Endgerät
- Benötigt für Multicast
- Auf Basis der GPS-Zeit

=> Arbeitet korrekt innerhalb eines [0;1) s Intervalls



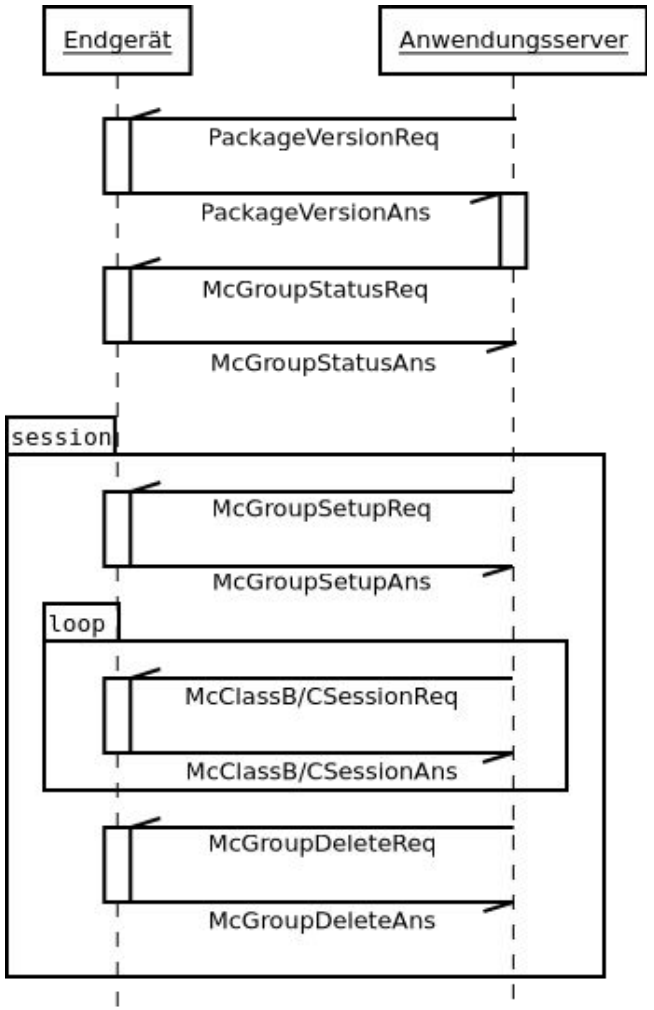
Durchführung und Ergebnisse
Firmware-Updates via LoRaWAN

Remote Multicast Setup:

- Handelt Multicast-Parameter aus
- Legt Zeiträume für Multicast-Transfers fest

=> Viele Probleme mit Class B beim Implementieren

=> Ansonsten korrekte Funktion



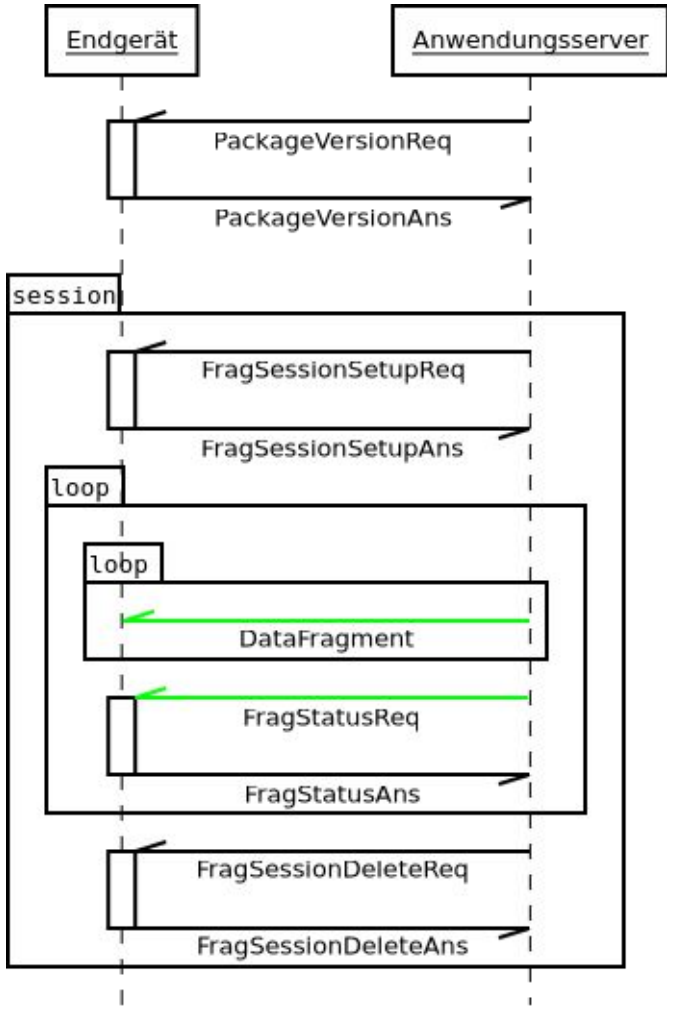
Durchführung und Ergebnisse
Firmware-Updates via LoRaWAN

Fragmented Datablock Transport:

- Fragmentierung des Updates
- Multicast-tauglicher FEC-Code für Paketverluste

=> Transfer mit minimalem Zusatz durch Kontroll- und Korrekturdaten

=> Überträgt Daten verlässlich

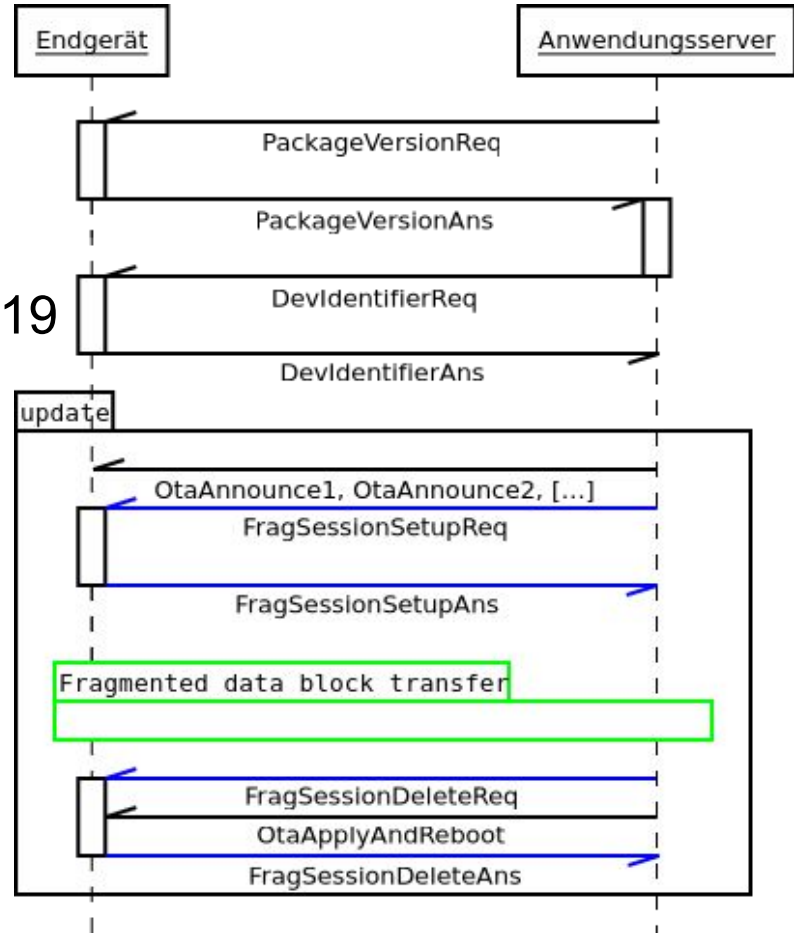


Durchführung und Ergebnisse
Firmware-Updates via LoRaWAN

OTA-Updates:

- Eigenentwickeltes Protokoll
- Authentizitätssicherung: Ed25519
- Integritätssicherung: SHA256
- Integriert mit FDBT

=> Protokoll kann Updates via Uni/Multicast senden



Durchführung und Ergebnisse
Firmware-Updates via LoRaWAN

Ergebnisse:

1. Sichere Firmware-Updates konnten realisiert werden
2. Updates dauern selbst bei optimalen Bedingungen sehr lange
   (3,5 h für ein minimales ESP-Beispiel, 22 h für den Briefkasten)
3. Das Gateway (und Endgerät) werden solange blockiert

Offene Fragestellungen:

1. Kann der Transfer beschleunigt werden
   ➔ z.B. über zusätzliche Gateways oder Delta-Updates

Durchführung und Ergebnisse
Sensorik zum Erkennen eines Briefeinwurfs

Ziele:

- Sensor-Lösung für o. g. Aufgabe finden
- Die Lösung muss energiesparend und verlässlich sein

Untersuchte Technologien:

- *Infrarot Lichtschranke*
- *Infrarot Distanzmessung*
- Ultraschall Distanzmessung
- Kraftmessung
- Klappen-Detektion

Durchführung und Ergebnisse
Sensorik zum Erkennen eines Briefeinwurfs

Kriterium	**Lichtschranke**	**Distanzmessung**
Funktionalität	Ja	Ja
Maximale Reichweite	45 cm	44 cm
Erkennung	>10 cm Sensorabstand Sonnenlicht aktiviert den Sensor	Keine Einschränkung
Abdeckung	Nur innerhalb gerader Linie	Maximal 35°-Winkel linear abnehmende Reichweite
Interferenz	Keine bei Winkeln >30° Keine Reflexion	Interferenz bei mehreren Sensoren Probleme durch Reflexion
Ansteuerung	Einfach	Komplex

Durchführung und Ergebnisse
Sensorik zum Erkennen eines Briefeinwurfs

Ergebnisse:

1. Keine Technologie sticht als bessere Lösung hervor
2. Infrarot Lichtschranke als flexiblere und einfachere Lösung gewählt

Offene Fragestellungen:

1. Sind andere Technologien noch besser geeignet?

   ➔ praktische Untersuchung dieser

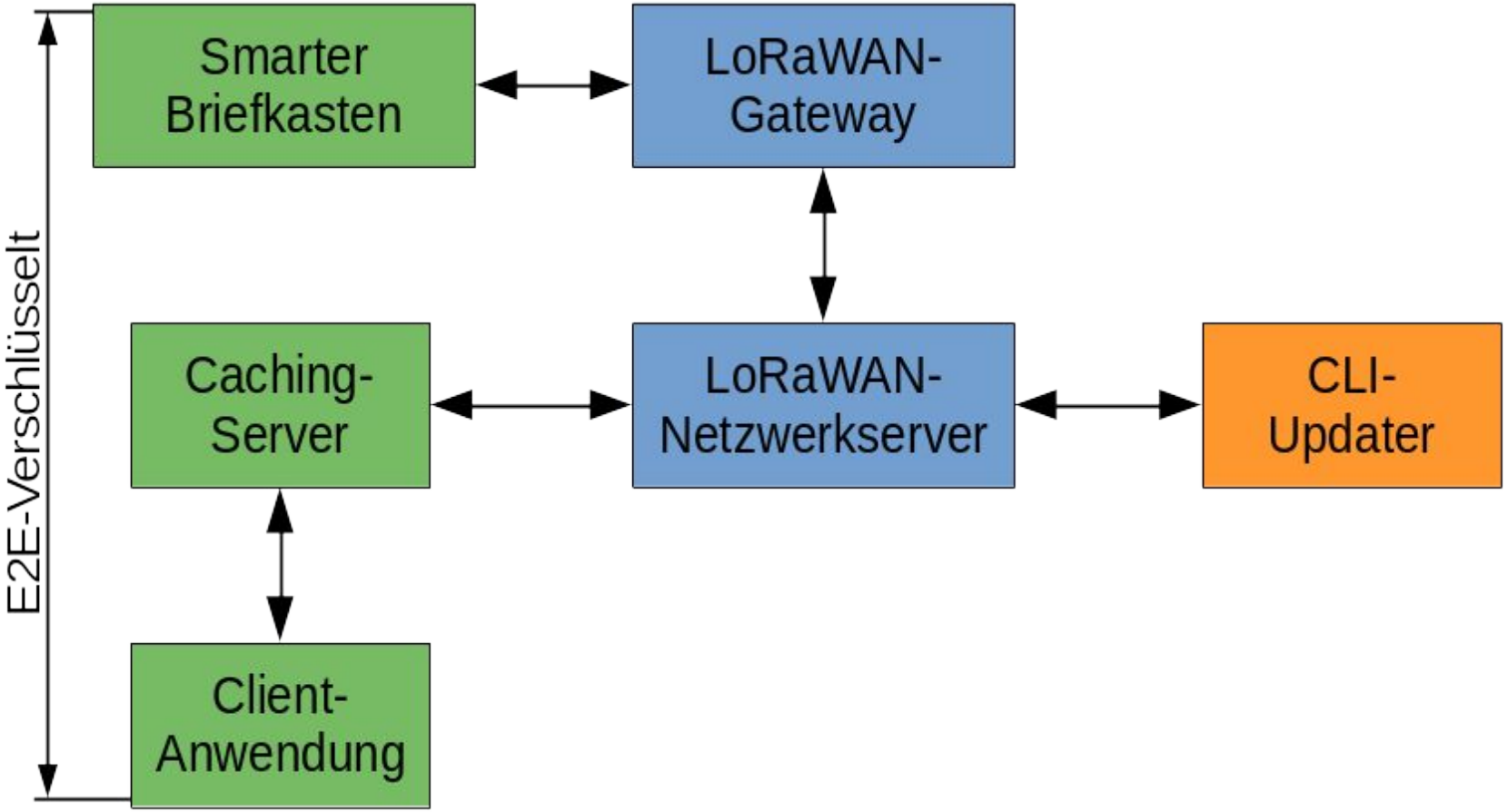
Durchführung und Ergebnisse
Entwicklung des Smarten Briefkastens

Ziele:

- Zusammenführung der vorherigen Ergebnisse
- Erstellung von Anwendungen für Endgeräte, Server und Mobilgeräte
- Übertragung von Post- und Batteriestatus an das Mobilgerät
- Anwendung für Endgerät soll energiesparend sein

Durchführung und Ergebnisse

Entwicklung des Smarten Briefkastens



Durchführung und Ergebnisse
Entwicklung des Smarten Briefkastens

Durchführung und Ergebnisse
Entwicklung des Smarten Briefkastens

Ergebnisse:

1. Entwicklung erfolgreich durchgeführt
2. Funktionierende Demonstration

Mögliche Verbesserungen:

1. Verbesserung des Energieverbrauchs
2. Push-Benachrichtigungen in der App
3. Verbesserung des “Gehäuses”

Erkenntnisse und Fazit

Erkenntnisse:

1. LoRaWAN verwendet kein E2E ⇒ zusätzliche Verschlüsselung
2. Schlüsselaustausch über 2. Kanal erhöht Sicherheit + PFS
3. OTA-Updates über LoRaWAN sind nicht trivial aber möglich
4. Software-Bibliotheken für LoRaWAN sind oft fehlerhaft

Fazit: Projekt konnte erfolgreich realisiert werden, sichere Daten-übertragung und OTA-Updates sind möglich.