OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

LaS³ laboratory for safe and secure systems engineering

ZD.B ZENTRUM DIGITALISIERUNG BAYERN

Energy Safe and Secure System Module ES³M

FuE Cluster-Seminar
13. Dezember 2021

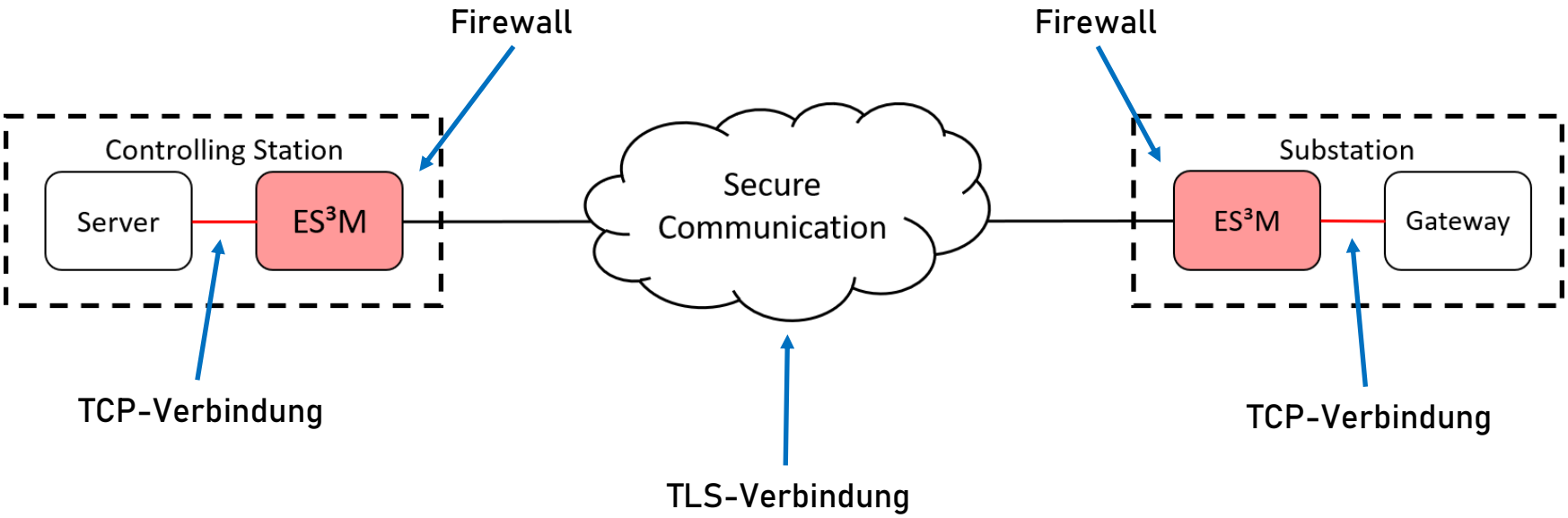
Laboratory for Safe and Secure Systems LaS³

AGENDA

1. Recap: Projektidee
2. Secure Software Update
3. Secure Boot
4. Secure Inter-Controller Communication
5. Zertifikatsmanagement
6. Post-Quantum Kryptografie

1 Recap: Projektidee

Projektansatz

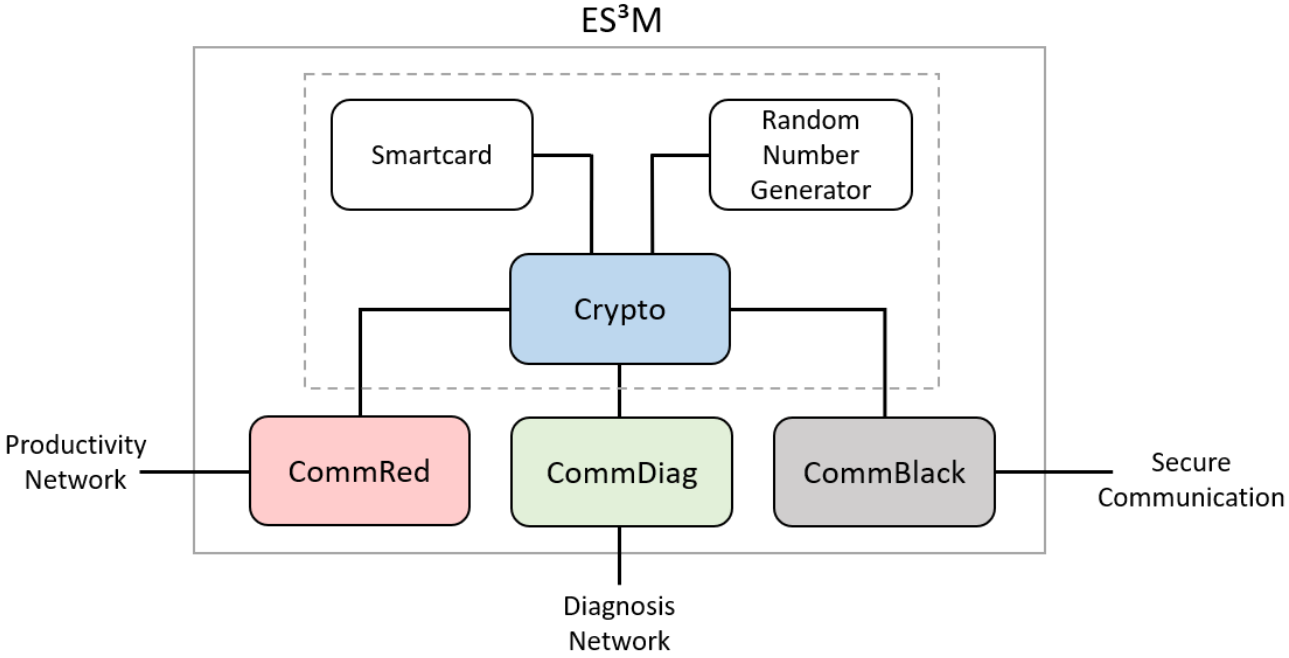


Maßnahmen zur Absicherung

Funktionen des ES³M Gateways:

- → Einsatz von TLS 1.3 für die Absicherung des Kommunikationskanals
- → Firewall-Funktionen zum Schutz vor Denial-of-Service Attacken
- → Generierung eines Audit-Trails inkl. kryptografischer Absicherung auf dem Gateway
- → Überwachung der Funktionalität innerhalb der Haupt-Akteure und durch externe Instanz
- → „Keep it as simple as possible“ (Sowohl bezogen auf Hardware als auch auf Software)
- → Möglichkeit von Software-Updates und teilweisen Hardware-Tausch zur Steigerung der Einsatzdauer
- → Anstreben einer Zertifizierung hinsichtlich Funktionaler Sicherheit und IT-Sicherheit

Interne Architektur



Interne Architektur

Kommunikations-Controller

Bidirektionale Weiterleitung von Payload-Daten zwischen Netzwerk und interner Kommunikationsschnittstelle

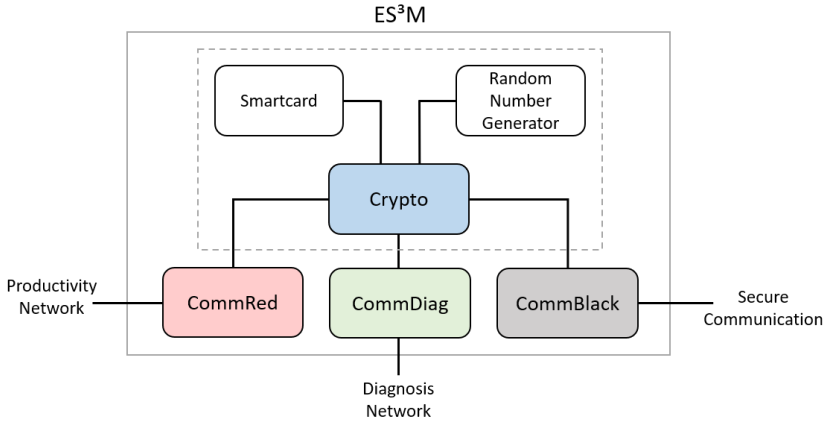
CommDiag

Zusätzliche Überwachung von Crypto, CommRed und CommBlack.

- → Isolation von Netzwerk und Kryptografie
- → Austausch des zentralen Crypto-Moduls
- → Überwachung der primären Controller durch CommDiag

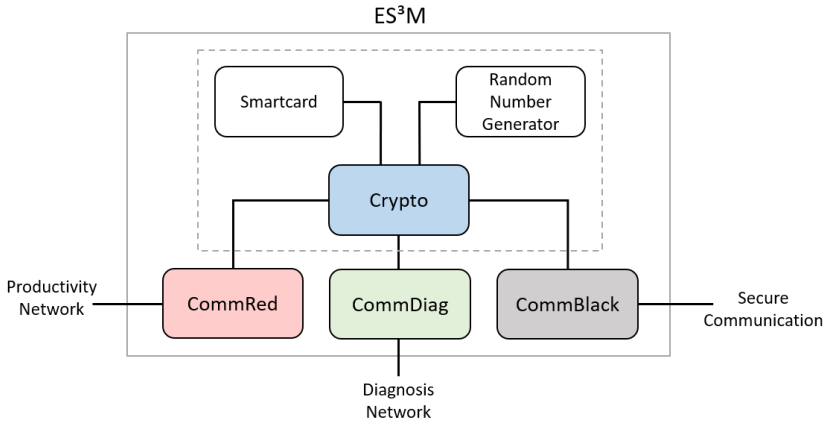
Crypto-Controller

Anwendung des TLS Protokolls auf empfangene Daten inkl. entsprechender Weiterleitung zum Ziel-Interface



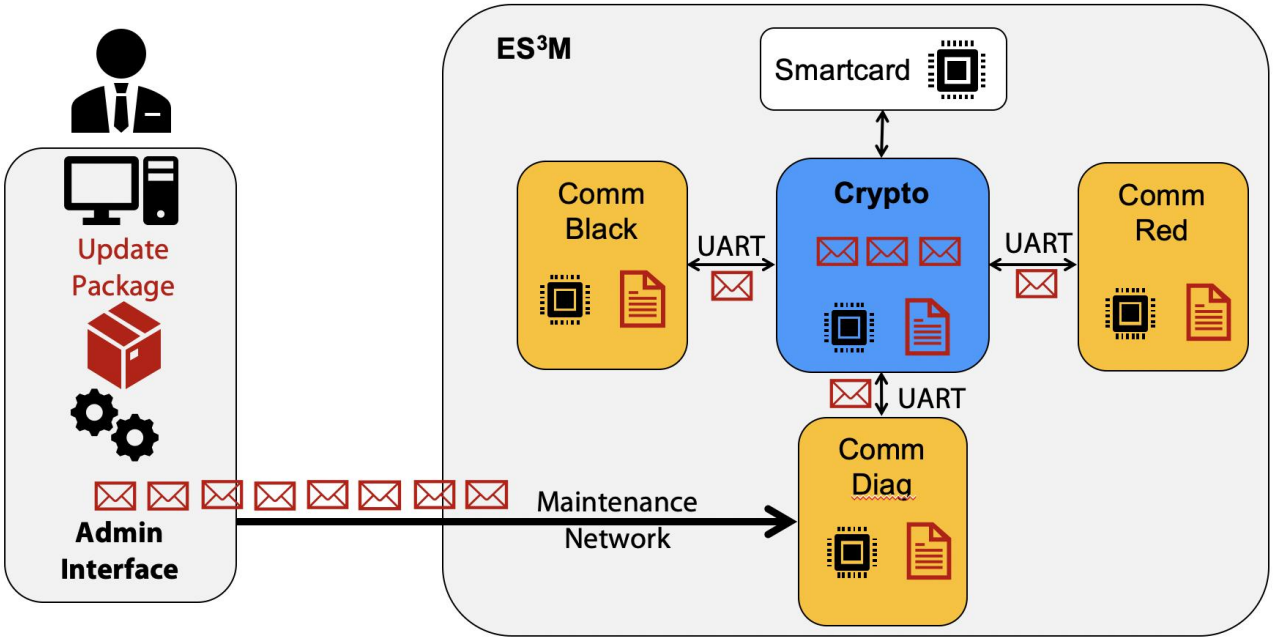
Interne Architektur

- → Einsatz simpler System-on-Chip MCUs (STM32H7 auf Cortex-M7 Basis)
- → Minimales Software-Fundament auf Basis von FreeRTOS und WolfSSL
- → EAL5+ zertifizierte Smartcard zum Speichern von Zertifikaten und privaten Schlüsseln
- → PTG.3 zertifizierter Zufallszahlengenerator für sehr hohe Entropie
- → Interne Kommunikation über SPI und UART zwischen den MCUs

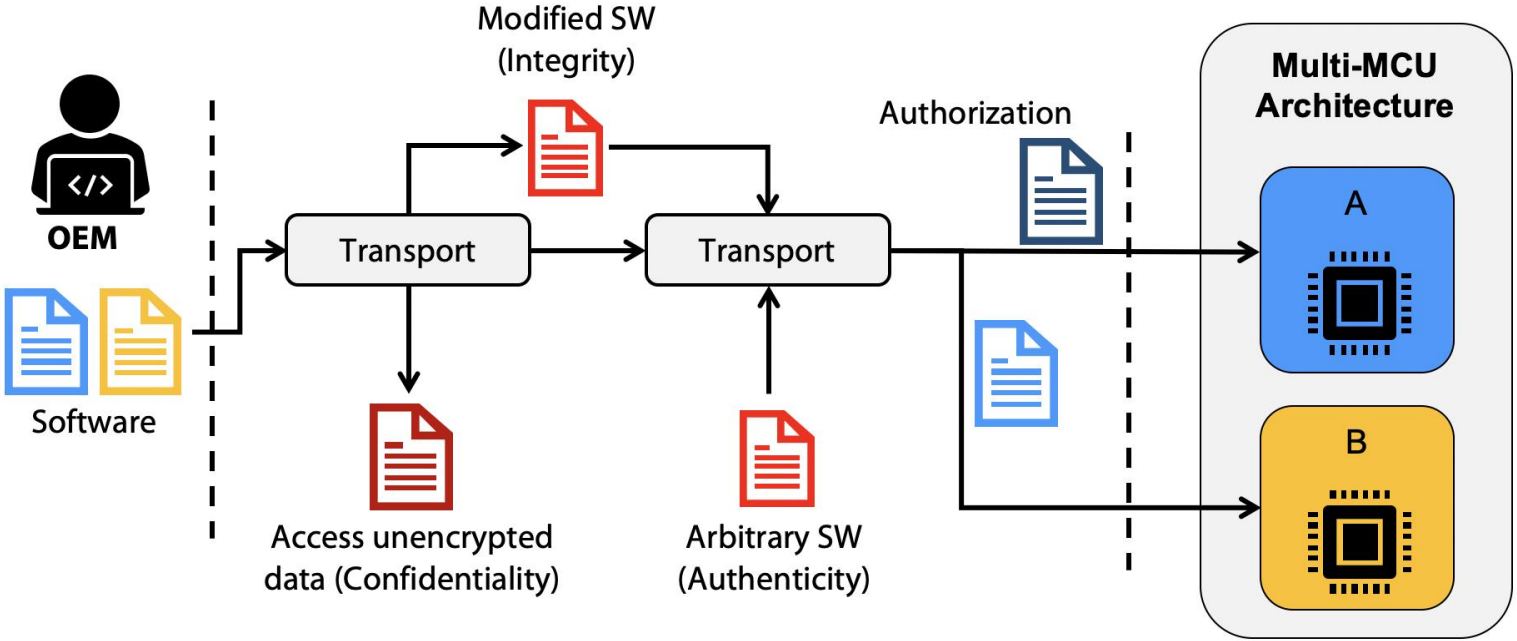


2 Secure Software Update

SWU: Overview



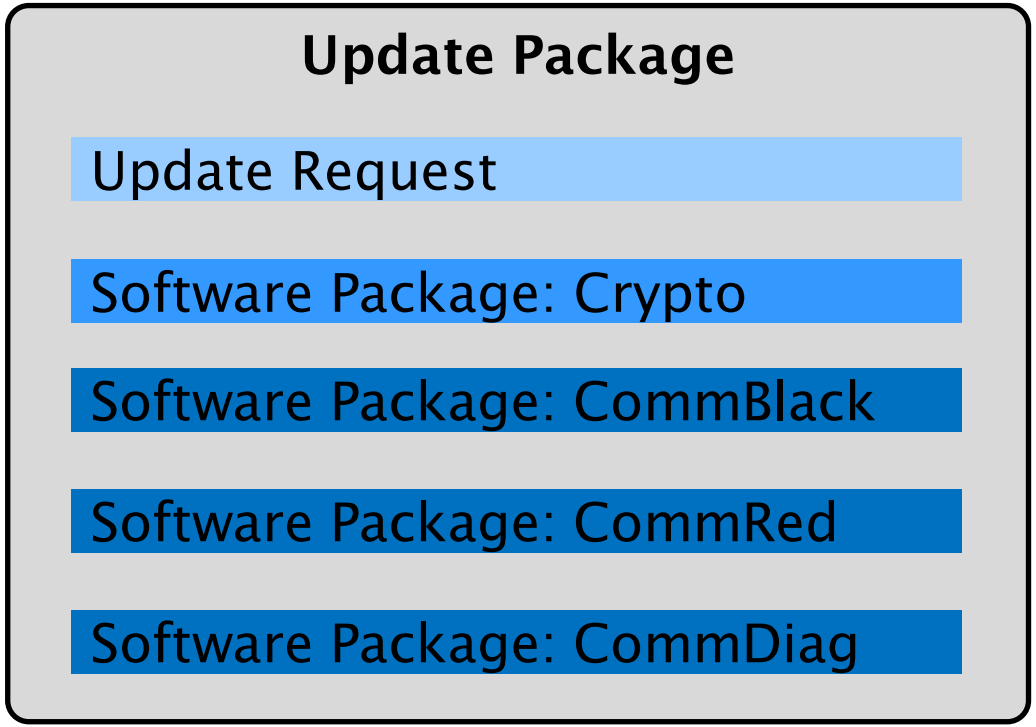
Threats


Modified SW
(Integrity)
Authorization
Multi-MCU
Architecture
OEM
Transport
Transport
A
B
Software
Access unencrypted
data (Confidentiality)
Arbitrary SW
(Authenticity)

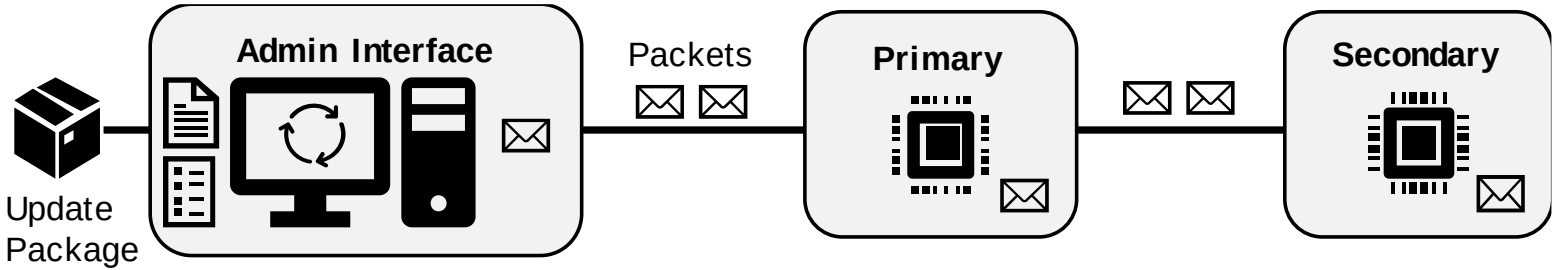
SWU Principles

Cryptography	**Authenticity, Integrity & Confidentiality** Secure Communication Channel (TLS) Digital Signatures
Security-relevant Information	Version number Target ID … Timestamp
Fail-Safe Update: Redundant Software	Keep old software as fallback option

SWU Data Structure



SWU Process


Admin Interface
Packets
Primary
Secondary
Update Package

3 Secure Boot

Ausgangssituation

→ Gefahr: Manipulation der Firmware (Schreibzugriff auf Flash)

→ Muss nicht zwingend über Update-Prozess erfolgen

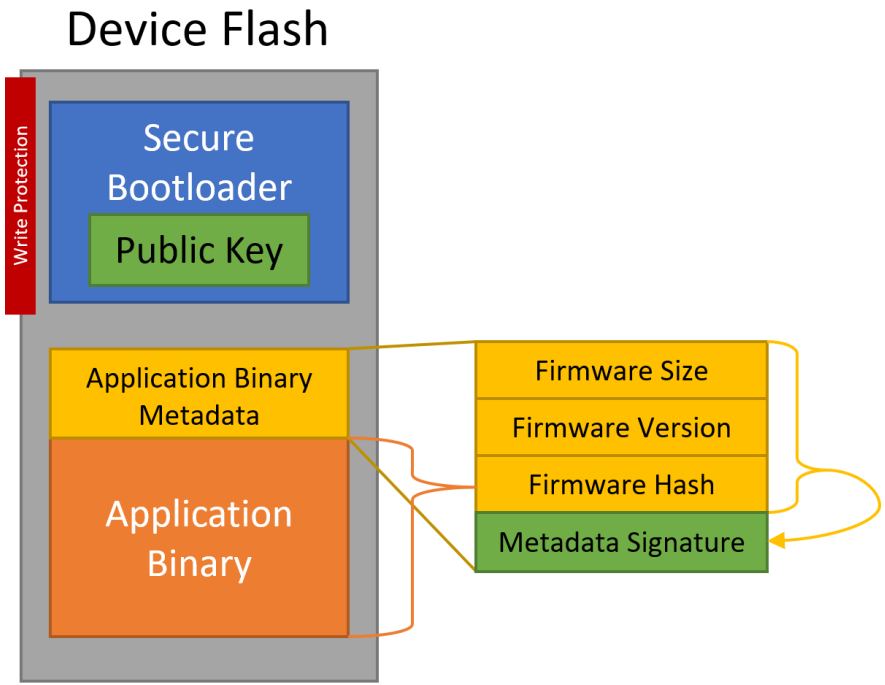
Secure Boot:

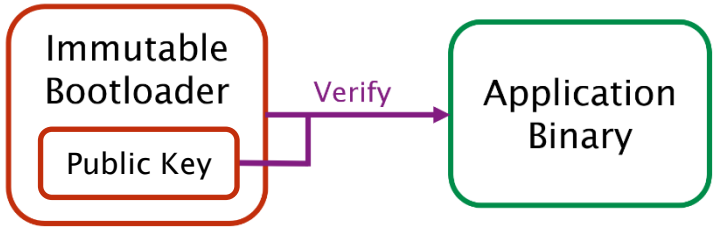
→ Verifikation von Integrität und Authentizität der Firmware beim Start

  → Verhindern der Ausführung von manipulierter Firmware

→ Optimal: Verifikation der Firmware-Version (Rollback-Protection, Zusammenpassende Versionen auf den Controllern)

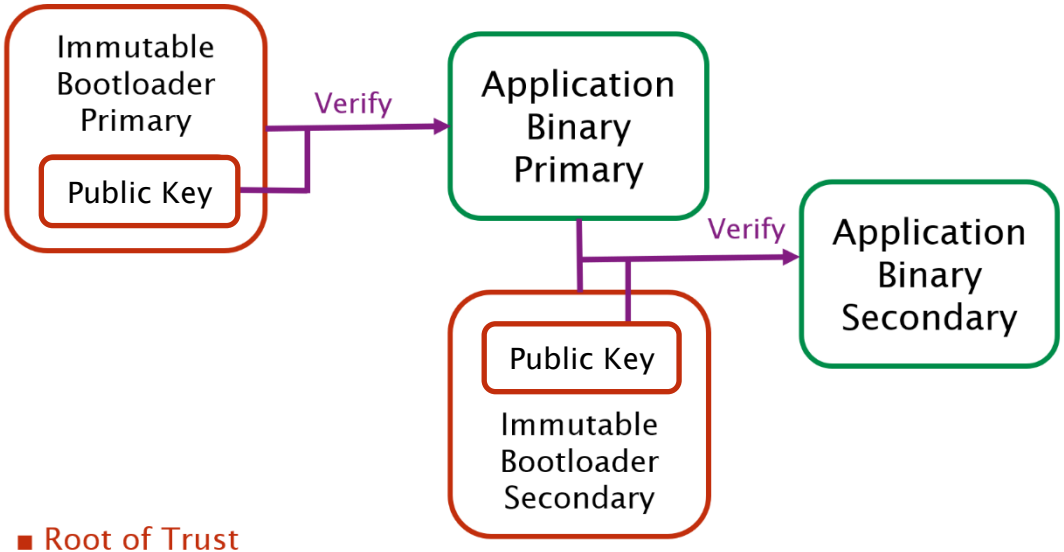
ES³M Secure Boot





- Root of Trust
- Trusted due to Chain of Trust

ES³M Secure Boot

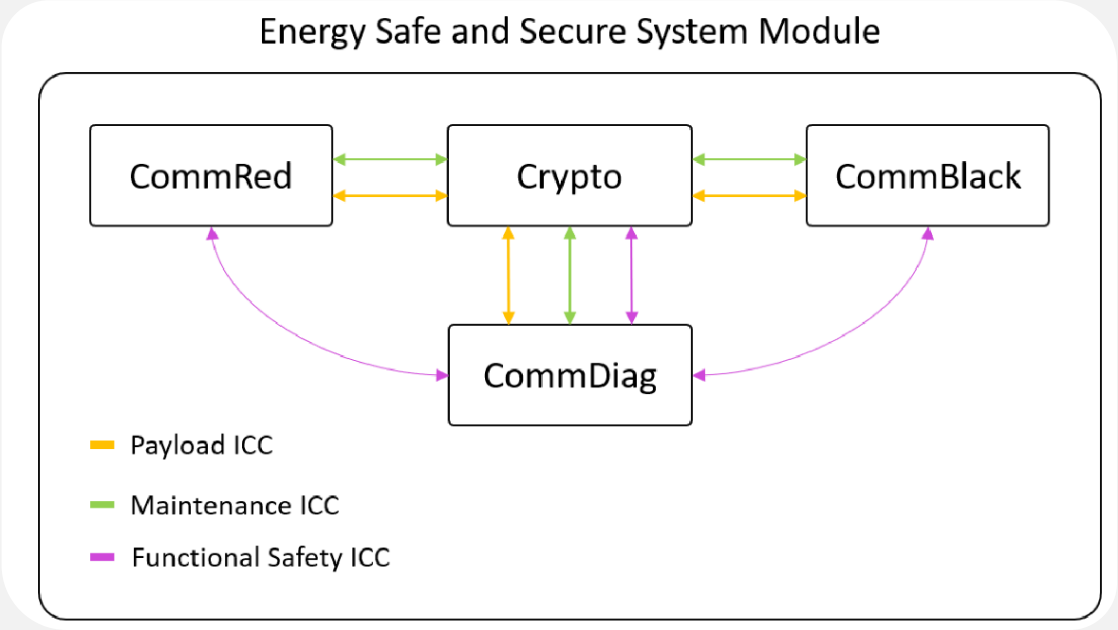


- Root of Trust
- Trusted due to Chain of Trust

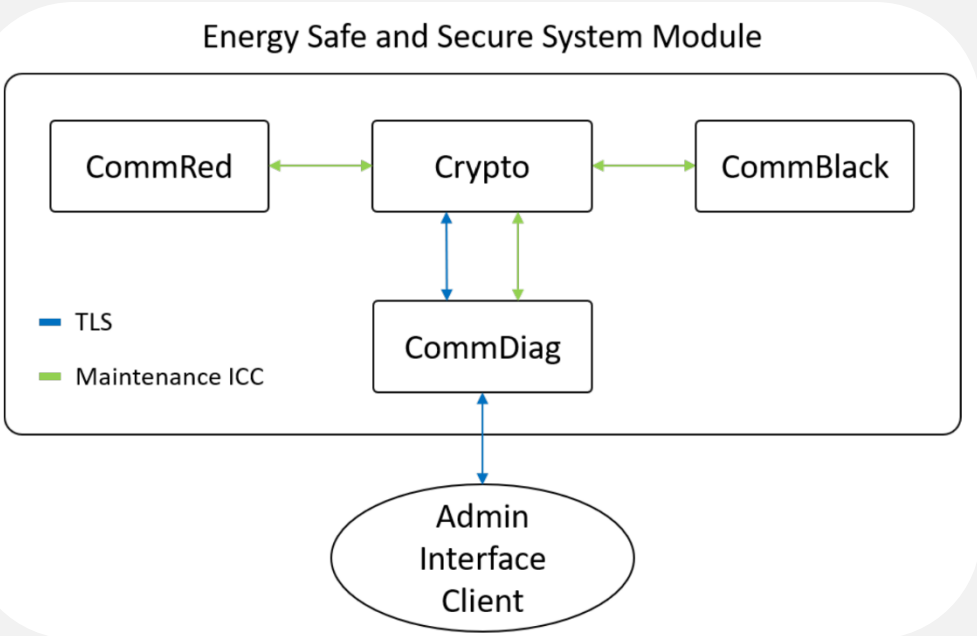
4 Secure Inter-Controller Communication

Ausgangssituation

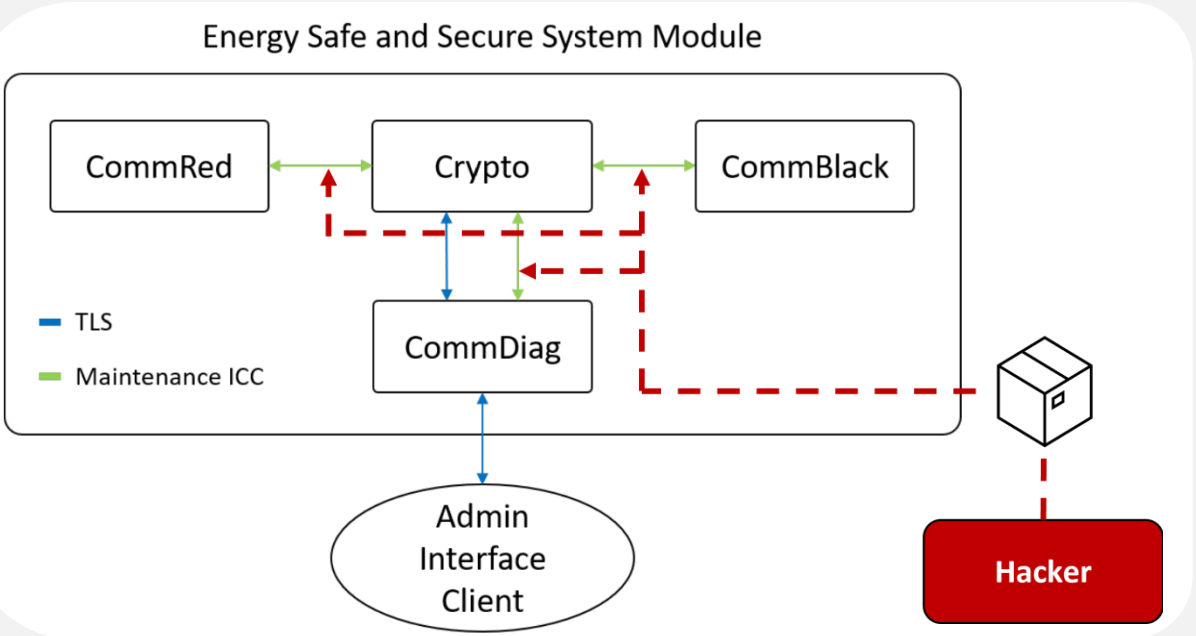
Inter-Controller Communication



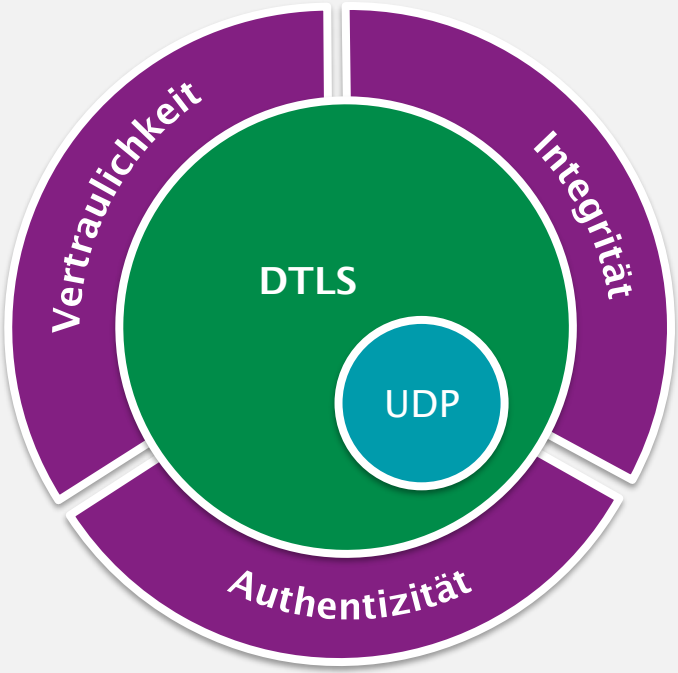
Bedrohungsszenario



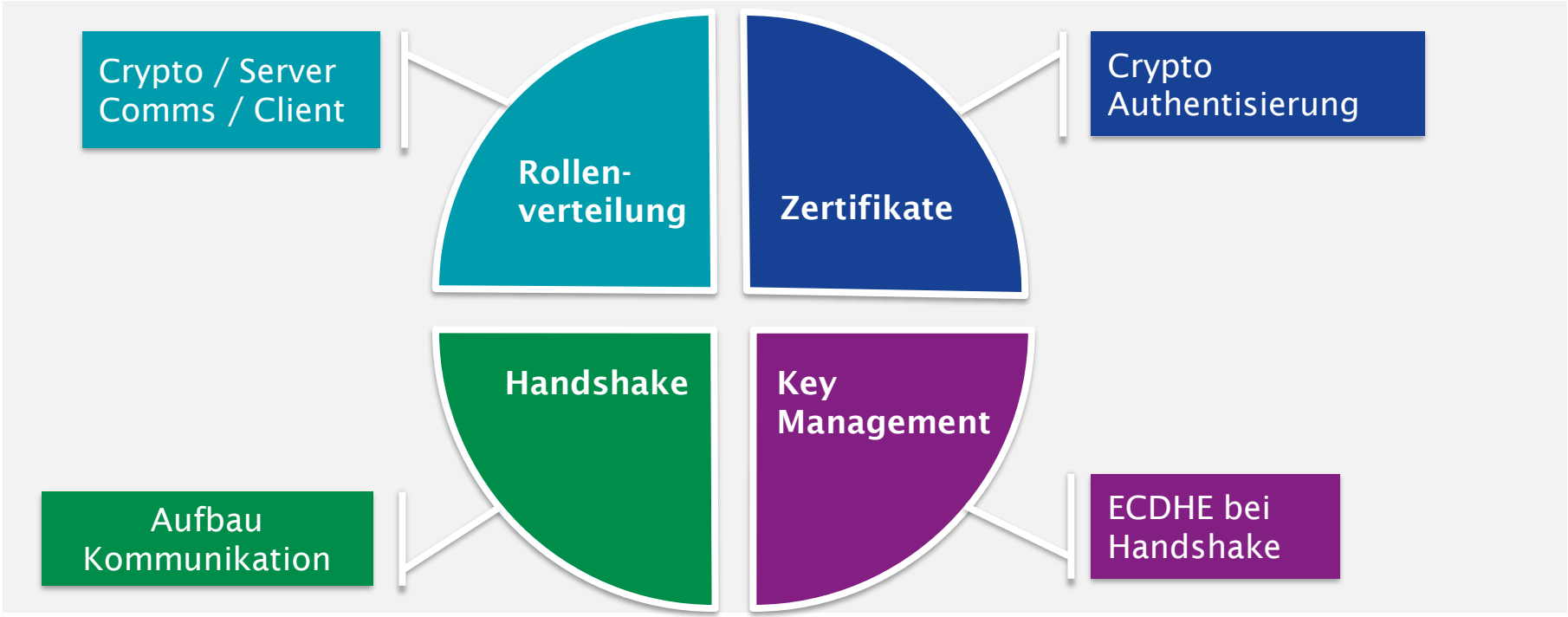
Bedrohungsszenario



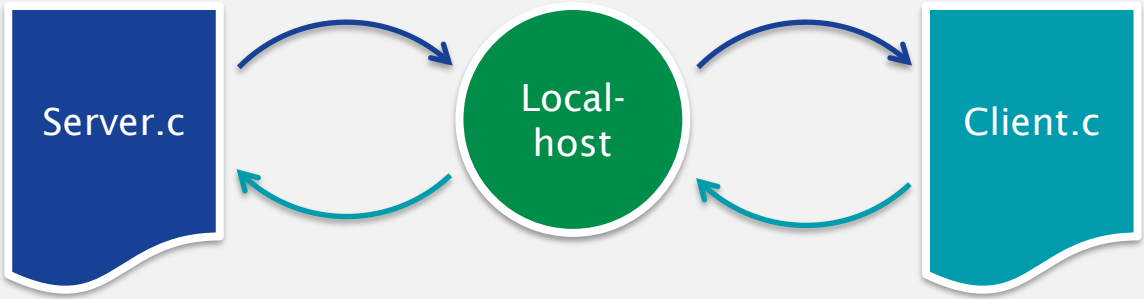
Datagram Transport Layer Security (DTLS)



Secure Inter-Controller Communication



Aufbau Proof-of-Concept



Zusammenfassung und weitere Forschung

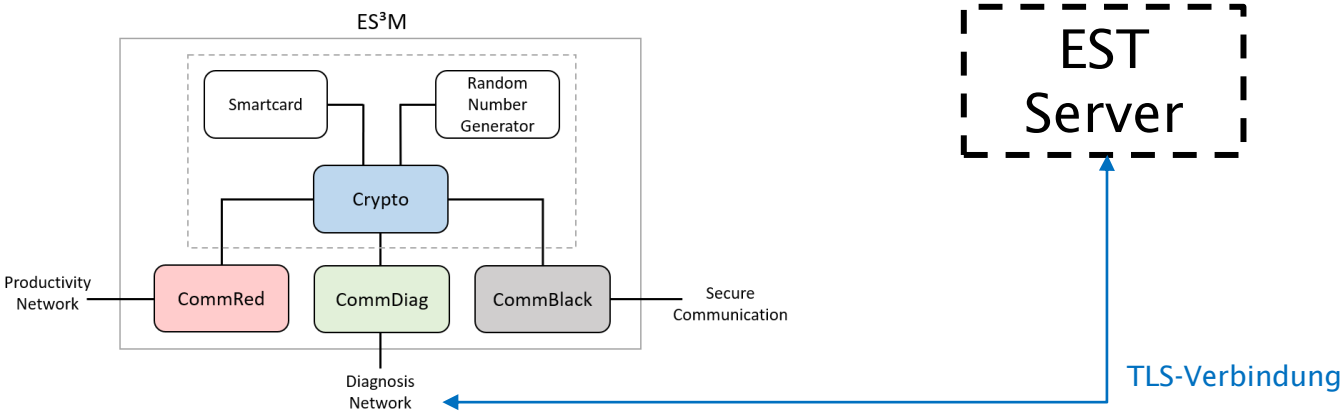
- Sicherstellen der Schutzziele mithilfe von DTLS
- Proof-of-Concept Setup und Test auf lokalem System
- Implementierung auf dem ES³M
- Überprüfen der Anwendbarkeit und Performance

5 Zertifikatsmanagement

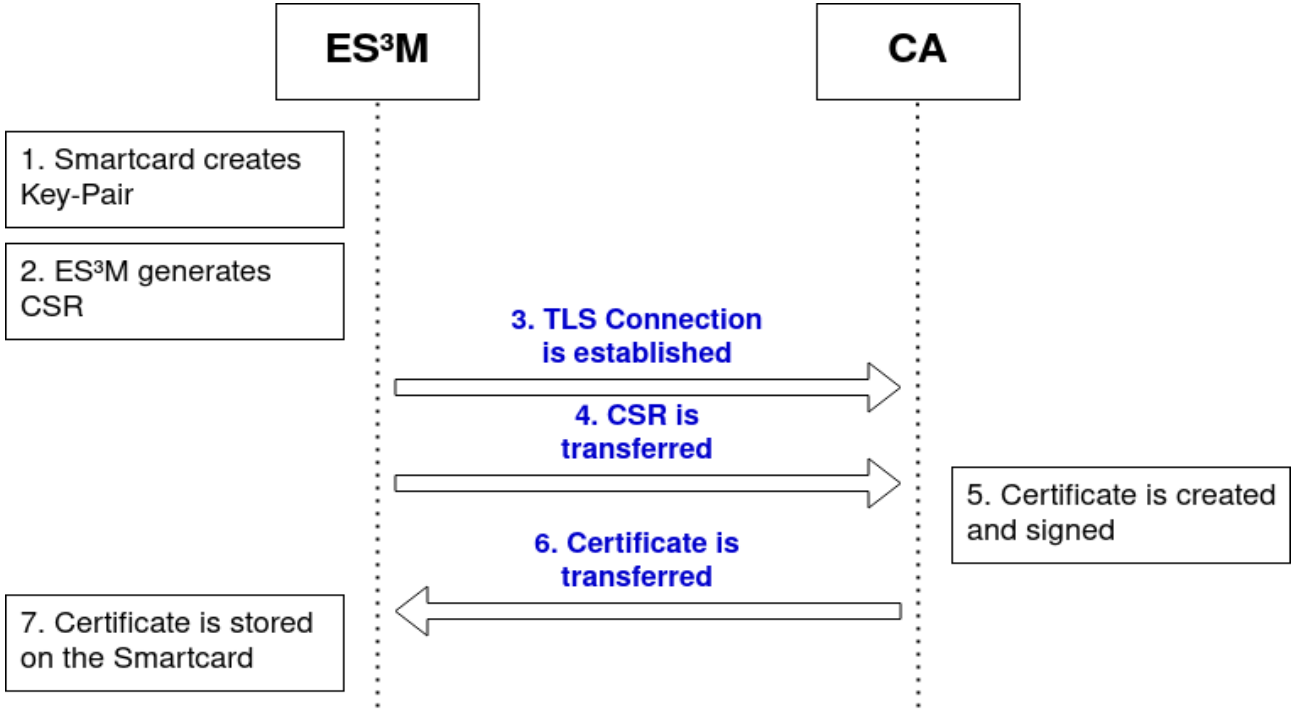
Einbringen von neuen Zertifikaten

→ Enrollment over Secure Transport (EST)

→ Anfrage vom ES³M an einen EST Server zur Beantragung eines neuen Zertifikats (Automatisierung der Beantragung eines Zertifikats)



EST-Ablauf

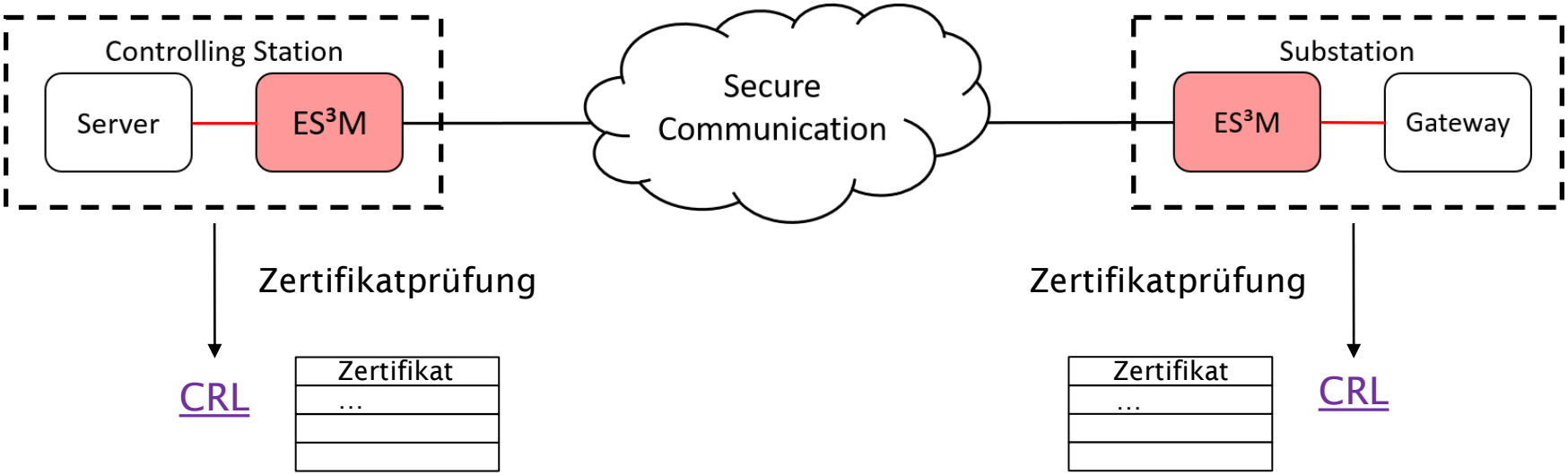

ES³M
CA
1. Smartcard creates Key-Pair
2. ES³M generates CSR
3. TLS Connection is established
4. CSR is transferred
5. Certificate is created and signed
6. Certificate is transferred
7. Certificate is stored on the Smartcard

Prüfung der Zertifikatsgültigkeit

→ Revocation: nachträgliches Zurückziehen eines Zertifikats durch die PKI

→ Certificate Revocation List: Liste aller zurückgezogener Zertifikate

→ Speicherung lokal auf dem Gerät

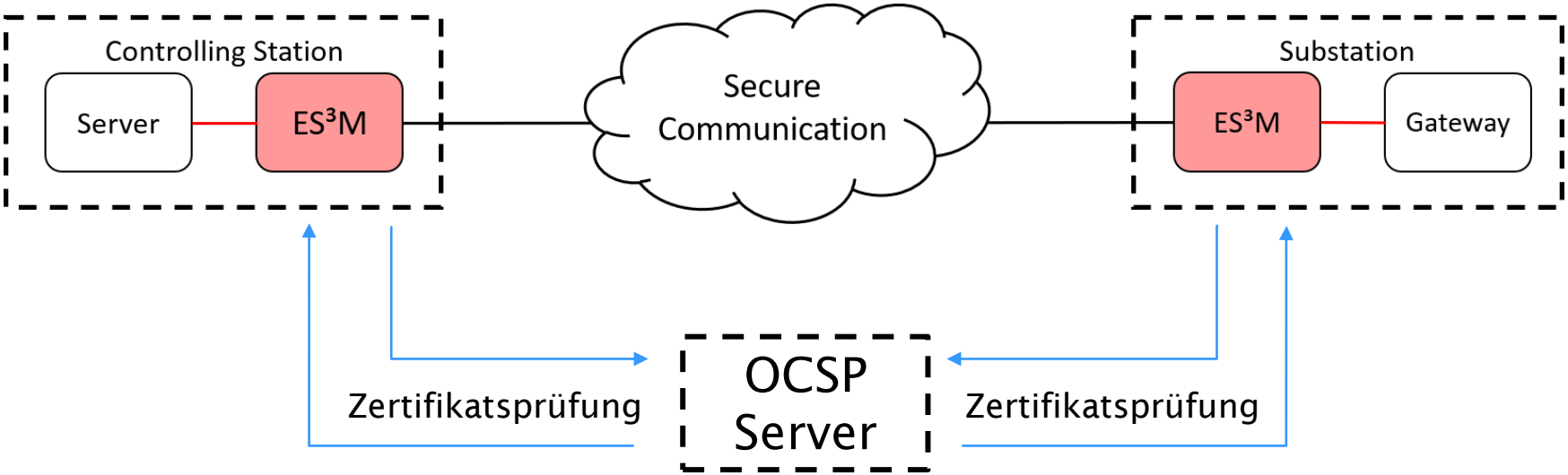


Prüfung der Zertifikatsgültigkeit

→ Online Certificate Status Protocol (OCSP)

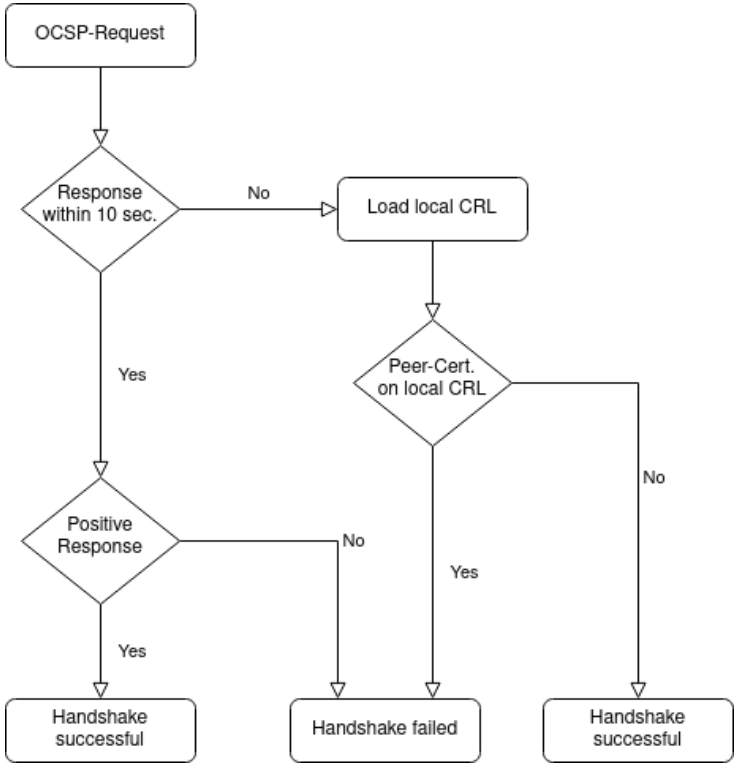
→ Anfrage beim OCSP Server der PKI während des Verbindungsaufbaus

→ Zusätzliche Netzwerkverbindung zur PKI



Ablauf der Verifikation im ES³M

- → Versenden eines OCSP-Request
- → Timeout überwacht die Antwortzeit des OCSP-Responders
- → Wird nach Ablauf des Timeouts keine OCSP-Response empfangen, wird die lokale CRL geladen
- → Keine Abhängigkeit von einer zusätzlichen Netzwerkverbindung



5 Post-Quantum Kryptografie

Erprobung von PQC-Algorithmen

- → Integration von PQC-Algorithmen in TLS
- → Verbindung mit bestehenden Komponenten: Hashprozessor, Zufallszahlengenerator
- → Vergleich der Algorithmen hinsichtlich Performanz und Ressourcenverbrauch
- → Librarys: PQClean und PQM4 in WolfSSL
- → Vorstellung einer Endlösung bestehend aus den besten Algorithmen

Kontakt

Tobias Frauenschläger
Laboratory for Safe and Secure Systems LaS³
OTH Regensburg
www.las3.de

tobias.frauenschlaeger@oth-regensburg.de

Prof. Dr. Jürgen Mottok
Laboratory for Safe and Secure Systems LaS³
OTH Regensburg
www.las3.de

juergen.mottok@oth-regensburg.de