

# Sachbericht zum Verwendungsnachweis Teil I & II

**2025**

## Verbundvorhaben

**PIA5**

### PKI in Infrastrukturen für Industrielle Automatisierungstechnik mit 5G

Gefördert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Konsortialführung: <b>ZIEHL-ABEGG</b>	Förderkennzeichen: <b>01MO23005B</b>
Laufzeit des Vorhabens: <b>von: 31.12.2022 bis: 30.06.2025</b>	
Berichtszeitraum: <b>von: 01.01.2023 bis: 30.06.2025</b>	Datum: <b>15.04.2026</b>

Projektpartner:

1. ZIEHL-ABEGG SE
2. Fraunhofer Institut für Integrierte Schaltungen IIS
3. Hochschule Offenburg (HSO)

## Inhalt

<b>1</b>	<b>Aufgabenstellung</b>	<b>6</b>
1.1	Arbeitspaketbeschreibungen	6
1.1.1	Arbeitspaket AP1: Definition Use Cases, Anforderungs- und Architekturanalyse	6
1.1.2	Arbeitspaket AP2: Systemkonzept	11
1.2	Arbeitspaket AP3: Integration Multi Access Edge Computing	19
1.2.1	Auswahl des Multi Access Edge Computing Frameworks	19
1.2.2	Technische Umsetzung & Middleware	21
1.2.3	Integration, Anbindung des MEC-Frameworks an 5G Core	22
1.3	Arbeitspaket AP4: PKI in den Endgeräten	24
1.4	Arbeitspaket AP5: Integration in ein 5G Campus Netzwerk	26
1.4.1	Auswahl eines geeigneten 5G-Kernnetzes	26
1.4.2	Security Framework	28
1.4.3	Integration von EAP-TLS in Open5GS	29
1.5	Arbeitspaket AP6: Vorbereitung der Integration in die Automatisierung und Produktion	29
1.5.1	Integration des Security Frameworks in die Produktionsumgebung von ZIEHL-ABEGG	29
1.6	Arbeitspaket AP7: Durchführung von Funktions- und Resilienztests für ausgewählte Use Cases	30
1.6.1	Use Cases Fraunhofer IIS	30
1.6.2	Use Cases ZIEHL-ABEGG	36
1.7	Arbeitspaket AP8: Dissemination und Dokumentation	40
<b>2</b>	<b>Die wichtigsten Positionen des zahlenmäßigen Nachweises</b>	<b>41</b>
<b>3</b>	<b>Notwendigkeit und Angemessenheit der geleisteten Arbeit</b>	<b>41</b>
<b>4</b>	<b>Voraussichtlicher Nutzen und Verwertbarkeit</b>	<b>42</b>
<b>5</b>	<b>Fortschritt bei anderen Stellen</b>	<b>42</b>
<b>6</b>	<b>Erfolge und geplante Veröffentlichungen</b>	<b>42</b>
<b>7</b>	<b>Literaturverzeichnis</b>	<b>44</b>

# Zusammenfassung

## **Ursprüngliche Aufgabenstellung sowie den wissenschaftlichen und technischen Stand, an den angeknüpft wurde**

Das Vorhaben zielt auf die Entwicklung eines Security Frameworks ab, das die Verbindung von 5G-Netzwerken mit der Automatisierungstechnik in 5G-Campusnetzen absichert. Dafür wird eine einheitliche Sicherheitsarchitektur benötigt, die die Kommunikation in Produktionsumgebungen schützt und die IT-Sicherheit für Industrie 4.0 Use Cases gewährleistet. Eine Public Key Infrastructure (PKI) dient als Grundlage zur Zertifikatsverwaltung, um die Authentizität von Komponenten sicherzustellen und Ende-zu-Ende-Sicherheit zu ermöglichen. Die Architektur berücksichtigt die Anforderungen von IT- und OT-Systemen sowie die Integration von Bestandsanlagen ohne ausreichende IT-Sicherheitsfunktionen. Zudem wird die Sicherheit entlang der gesamten Lieferkette einbezogen. Die Industrieautomatisierung ist eine zentrale Anwendungsdomäne von 5G Campusnetzen und erfordert höchste Dienstgüte, Verfügbarkeit und Zuverlässigkeit. 5G/6G-Netze ermöglichen die nahtlose Integration von Kommunikationskanälen, um diese Anforderungen zu erfüllen. Die Verwaltung mobilfunkspezifischer Schlüssel und Zertifikate erfolgt über die USIM, deren Einsatz in ressourcenbeschränkten Systemen, wie z.B. IoT Geräten, jedoch kostenintensiv und aufwendig ist. Technologien wie eSIM und iSIM bieten hier Kostenvorteile und neue Anwendungsmöglichkeiten. Aufbauend auf dem Projekt FieldPKI wurde die Nutzung einer Public Key Infrastructure (PKI) zur feingranularen Zertifikatsverwaltung auf Anwendungsebene bei Feldbussen untersucht. Für die Anwendungs-Software wurde auf Vorarbeiten des Fraunhofer IIS im Bereich Multi-Access Edge Computing (MEC) zurückgegriffen.

## **Ablauf des Vorhabens**

Die Projektlaufzeit wurde um 6 Monate kostenneutral verlängert. Innerhalb der verlängerten Projektlaufzeit wurden alle Arbeitspakete des Projekts planmäßig im Zeit- und Kostenrahmen durchgeführt.

## **Arbeitspaket AP1: Definition Use Cases, Anforderungs- und Architekturanalyse**

Im Arbeitspaket AP1 wurden Use Cases für die Integration von 5G-Campusnetzen in Produktions- und Automatisierungsumgebungen definiert und analysiert. Daraus wurden Anforderungen an ein Sicherheitsframework abgeleitet, welches die Kommunikation zwischen 5G, IT und OT gegen Cyberangriffe absichert. Zudem wurden Sicherheitsarchitekturen entwickelt und Anforderungen an Security Credentials erarbeitet, sowie Secure Elements für die Schlüsselgenerierung und -speicherung analysiert und bewertet.

## **Arbeitspaket AP2: Systemkonzept**

Aufbauend auf den Ergebnissen von AP1 wurde eine Systemspezifikation erstellt, die Funktionen wie Credential Management, Access Management und die Integration von Secure Elements sowie Automatisierungskomponenten definiert. Ergänzt wurde dies durch eine Bedrohungsanalyse und hierauf basierend einer Sicherheitsarchitektur mit zertifikatsbasierter Authentifizierung und einer PKI-Infrastruktur zur Absicherung der Kommunikation zwischen 5G, OT und IT.

### **Arbeitspaket AP3: Integration Multi Access Edge Computing**

In AP3 erfolgte die Recherche und Auswahl eines geeigneten Multi Access Edge Computing (MEC) Frameworks. Dieses wurde anschließend an das 5G-Campusnetz angebunden. Die Auswahl basierte auf Kriterien wie ETSI-Konformität, Erweiterbarkeit und Open-Source-Implementierung.

### **Arbeitspaket AP4: PKI in den Endgeräten**

Inhalt war die Integration der zertifikatsbasierten Authentifizierung in die Endgeräte. Ein Schwerpunkt waren dabei insbesondere Brownfield-Anlagen. Hierzu wurde ein Security-Gateway auf Basis eines Raspberry Pi mit TPM-Modul entwickelt, welches die, für die Anbindung von Bestandanlagen und die Umsetzung kryptographischer Sicherheitsfunktionen und sichere Schlüsselverwaltung, übernimmt.

### **Arbeitspaket AP5: Integration in ein 5G Campus Netzwerk**

Schwerpunkt war die Umsetzung und Integration des Security Frameworks in das 5G-Campusnetz und die Anbindung der Automatisierungsebene (OT). Nach Evaluierung verschiedener Optionen fiel die Wahl auf ein kommerzielles 5G-Kernnetz um die Anforderungen nach Stabilität und Support für die Testbeds bei Fraunhofer IIS und ZIEHL-ABEGG auch nach Projektende zu sichern.

### **AP6: Vorbereitung der Integration in die Automatisierung und Produktion**

In AP6 wurde das Security Framework erfolgreich in die Produktionsumgebung von ZIEHL-ABEGG integriert. Dies umfasste die Anbindung an das 5G-Campusnetz, die Installation des Security Frameworks auf einem bereitgestellten Server und die Anpassung an die lokale IT-Infrastruktur.

### **AP7: Durchführung von Funktions- und Resilienztests für ausgewählte Use Cases**

In AP7 wurden Funktions-, Resilienz- und Performancetests für die entwickelten Lösungen und Use Cases durchgeführt. Die Tests umfassten die Validierung der zertifikatsbasierten Authentifizierung sowie Sicherheits- und Performancetests. Besondere Schwerpunkte lagen auf der Analyse von Latenz, Schlüsselmanagement und der Absicherung gegen SIM-Karten-Diebstahl.

### **AP8: Dissemination und Dokumentation**

Um den Wissenstransfer innerhalb des Konsortiums und in die Fachöffentlichkeit zu fördern, wurden die Ergebnisse bei zahlreichen Veranstaltungen, wie der IIS-Hausmesse, dem Wireless Congress und dem 5G ACIA Plenum präsentiert. Zudem wurden wissenschaftliche Beiträge der Hochschule Offenburg auf IEEE-Konferenzen veröffentlicht.

### **Wesentlichen Ergebnisse sowie ggf. die Zusammenarbeit mit anderen Forschungseinrichtungen**

Im Rahmen des Projekts wurden folgende Ergebnisse erzielt:

- Entwicklung eines Sicherheitsframeworks für die Absicherung der domänenübergreifenden Kommunikation zwischen 5G, OT und IT. Integration des Sicherheitsframeworks in die Produktionsinfrastruktur von ZIEHL-ABEGG und das Fraunhofer Testbed.

- Erstellung einer PKI zur Verwaltung von Zertifikaten und zur Unterstützung der zertifikatsbasierten Authentifizierung.
- Auswahl, Anpassung und Integration eines MEC-Framework.
- Vorstellung der Projektergebnisse bei Fachmessen, Fachvorträgen und IEEE-Veröffentlichungen

Das Projekt kann einen maßgeblichen Beitrag zu Konzepten zur Verbesserung und Erhöhung der IT-Sicherheit in der industriellen Automatisierung und zur Entwicklung zukunftssicherer Lösungen im Bereich 5G und Industrie 4.0 leisten.

# 1 Aufgabenstellung

Das Projekt zielt darauf ab, eine einheitliche Sicherheitsarchitektur für Lieferketten unter Nutzung von 5G-Infrastruktur zu erforschen. Diese Architektur soll die sichere Verwaltung von Kommunikationsbeziehungen über den gesamten Lebenszyklus von Produkten gewährleisten, beginnend bei der Produktion über die Lieferlogistik bis hin zum Betrieb beim Kunden. Zielsetzung war die Entwicklung einer neuartigen Sicherheitsarchitektur, welche die Kommunikation über verschiedene Schnittstellen absichert, angefangen bei der Produktionsautomatisierung in einem 5G Standalone Campus Netzwerk bis zur Integration in ein öffentliches 5G-Netz für Betrieb und Wartung. Wichtige Aspekte sind die Ende-zu-Ende Security über verschiedene Netzwerkdomänen. Im Produktionsumfeld ist dies die Ende-zu-Ende Sicherheit zwischen 5G-Netz, Operational Technology (OT) Netz und Informationstechnologie (IT) um eine Verschlüsselung der Kommunikation sowie eine zuverlässige, automatisierte Authentifizierung und Autorisierung der beteiligten Komponenten und Stakeholder zu ermöglichen. Die zulässigen Kommunikationsbeziehungen variieren im Lebenszyklus von Inbetriebnahme, Betrieb, Wartung, Update bis hin zum Austausch von Komponenten. Eine (Public) Key Infrastructure wurde als Basis für das neue Sicherheitsframework eingesetzt, um die Verwaltung geeigneter Zertifikate im Kontext von Industrie 4.0 zu unterstützen. 5G bietet darüber hinaus Funktionen und Technologien zur Zertifikatsverwaltung über den gesamten Betriebszyklus einer Automatisierungskomponente. Das Projekt adressiert die unterschiedlichen Sicherheitsanforderungen von Informationstechnologie (IT) und Operational Technology (OT). Während IT-Netze auf Vertraulichkeit, Verfügbarkeit und Integrität fokussiert sind, liegt der Schwerpunkt bei OT-Komponenten auf Zuverlässigkeit, Authentizität und der Einhaltung von Latenzgrenzen. Im Rahmen der Projektdurchführung wurden hierzu **Use Cases** entwickelt, **Sicherheitsanforderungen** definiert, ein **Security Framework** entwickelt, sowie ein **Multi-Access-Edge Computing Framework** ausgewählt und mit eingebunden, welches eine App-basierte Umsetzung der Use Cases ermöglicht.

## 1.1 Arbeitspaketbeschreibungen

Die Bearbeitung erfolgte in sieben aufeinander aufbauenden Arbeitspaketen.

### 1.1.1 Arbeitspaket AP1: Definition Use Cases, Anforderungs- und Architekturanalyse

Im Rahmen dieses Arbeitspakets wurden folgende Themen bearbeitet:

- Erfassung von technisch umzusetzenden Use-Cases im Zusammenspiel zwischen 5G Campusnetzen und Automatisierungstechnik.
- Aufbauend hierauf wurden in einem nächsten Schritt resultierende Anforderungen an ein Sicherheitsframework aus den erfassten Use-Cases abgeleitet. Ziel des Sicherheitsframeworks ist die Absicherung der Kommunikation zwischen 5G, IT und OT gegenüber Cyberangriffen (IT-Sicherheit).

- Basierend auf den gewonnenen Erkenntnissen und Vorgaben folgte die Entwicklung möglicher Sicherheitsarchitekturen und eine Auswahl.
- Ergänzend hierzu wurden Anforderungen an Security Credentials ermittelt, sowie eine erste Bewertung von Secure Elements vorgenommen. Aufgaben des Security Element sind die Generierung qualitativ hochwertiger kryptischer Schlüssel und die Speicherung der privaten Schlüssel.

### 1.1.1.1 Definition von Use Case

Die Entwicklung von Use Cases erfolgte schwerpunktmäßig durch die Projektpartner ZIEHL-ABEGG und Fraunhofer IIS. Das Fraunhofer IIS entwickelte hierzu ein Template zur Use-Case Definition, so dass eine einheitliche Dokumentation und ein gemeinsames Verständnis, sowie eine einheitliche Beschreibung erzielt werden konnten. Dabei wurde Wert daraufgelegt, dass einerseits Synergien genutzt werden konnten, was die spätere Umsetzung von Use Case in den beiden Testbeds der Partner ZIEHL-ABEGG und Fraunhofer IIS anbelangt, andererseits wurden aber auch bewusst unterschiedliche Use Cases generiert, um damit ein breites Spektrum an Anforderungen an die Architektur zu generieren.

### 1.1.1.2 Use Cases bei Fraunhofer IIS

Für die Umsetzung der Use Cases im Testbed des Fraunhofer IIS kam als Repräsentant einer OT-Anlage die Produktionslinie des Fraunhofer IIS am Standort Nürnberg (Abbildung 1) zum Einsatz. Die Produktionslinie besteht aus insgesamt 6 Unterstationen und einer übergeordneten Steuerung (SPS). Die Fertigung eines Endprodukts erfolgt dabei durch Zusammenfügen von Unterteilen, Oberteilen und einem Verbindungsstift. Für die Kommunikation mit der Anlage steht eine OPC UA Schnittstelle zur Verfügung, die die Abfrage von Statusinformationen, Produktionsabläufen und Fehlerzuständen ermöglicht.



Abbildung 1: Produktionslinie am Standort Nürnberg

Für die direkte Ansteuerung der Anlage (Produktauswahl, Starten, usw.) steht zusätzlich ein Web-Interface zur Verfügung. Am Fraunhofer IIS wurden hierzu folgende mögliche Use Cases identifiziert:

- Produktionsdaten live aus der Produktionsanlage
- Alarmmeldungen live aus der Produktionsanlage
- Condition Monitoring
- Produktlagerung mit Ortsinformationen
- Adaptive Produktion

#### **1.1.1.2.1 Produktionsdaten live aus der Produktionsanlage**

Ziel des Use Cases ist es, Informationen gezielt aus der Anlage abzufragen und diese im 5G Campusnetz mittels eines User Equipments (UE) dem Anlagenbediener zu visualisieren. Dazu wird mittels eines 5G tauglichen Smartphones der QR-Code einer Substation erfasst. Auf Basis dieses Codes werden aktuelle Produktionsdaten an der lokalen Steuerung dieser Station ausgelesen und in einer App angezeigt.

#### **1.1.1.2.2 Alarmmeldungen live aus der Produktionsanlage**

Ziel des Use Cases ist es, Alarmmeldungen der Anlage auszulesen und über 5G an ein mobiles UE zu visualisieren. Hierzu werden Fehlerzustände der Produktionsline erfasst, an eine Multi Access Edge Computing (MEC) App gesendet, dort gespeichert und als Alarmmeldung an ein mobiles UE (Tablet oder Smartphone) gesendet und dort angezeigt. Dabei wird zwischen verschiedenen Schweregraden der Alarme unterschieden. Die Auswertung übernimmt eine MEC-App. Ein schwerwiegender Fehler wäre dann erreicht, wenn die Fertigung durch einen Fehler blockiert ist. Folgende Schritte sind hierfür erforderlich:

- Erfassung von Fehlermeldungen und Statusmeldungen.
- Bewertung und Generierung von Alarmmeldungen.
- Übertragung von Alarmmeldungen in Echtzeit an ein Tablet. Mögliche Alarmmeldungen könnten sein: Blockade der Fertigung, Magazinstand leer.
- Speichern der Alarmmeldungen in einem Log für weitere Verarbeitung oder für Nachweis und Fehlerbehandlung.

#### **1.1.1.2.3 Condition Monitoring**

Ziel des Use Cases ist es, dem Anlagenbediener Informationen über den Zustand der Anlage zu informieren. Bei diesem Use Case werden durch eine MEC App Statusinformationen von der Fertigungsstraße erfasst, gespeichert, mit vordefinierten Grenzwerten verglichen und an ein mobiles UE übertragen und angezeigt. Mögliche Daten können sein: Anzahl der gefertigten Produkte, Anzahl von Schaltvorgängen eines Aktors oder die Dauer je Fertigungsschritt. Die Speicherung der Statusinformationen soll in einer MEC-App erfolgen. Die Auswertung erfolgt dann durch die MEC-App, welche die ermittelten Informationen auswertet und direkt Wartungsempfehlungen generiert.

#### **1.1.1.2.4 Produktlagerung mit Ortsinformationen**

Eine wesentliche Vereinfachung der Lagerhaltung ist dadurch zu erreichen, dass beim Einlagern von Produkten die genaue Position der Produkte miterfasst und gespeichert wird. Die Position gefertigter Produkte soll über eine 5G Lokalisierung erfolgen. Dazu wird mittels eines Smartphones der QR-Code des Produkts erfasst und eine Verbindung zum MEC-Server aufgebaut. Die Positionserfassung erfolgt über die Ortsinformationen des UEs, welche aus dem 5G Netz bezogen werden (z.B. über den Lokalisierungsservice). Bei der Einlagerung werden die Produktdaten mit diesen Lokalisierungsdaten angereichert und im Lagerhaltungssystem abgespeichert.

#### **1.1.1.2.5 Adaptive Produktion**

Ziel ist das Retrofitting der Anlage durch eine funktionale Erweiterung der Produktionsanlage mittels 5G-fähiger Zusatzkomponenten (HW-Komponenten) und einer MEC-App, die neue Programmabläufe ermöglicht. Da die Anlage selbst nicht in der Lage ist, den Beladungszustand des Transportschlittens zu detektieren, erfolgte eine Erweiterung durch Anbindung einer Lichtschranke. Für die Signalisierung von Betriebszustände wurde eine Signalleuchte in das System integriert. Beide Erweiterungen sind mittels Raspberry Pi und 5G Modem an das 5G Netz angebunden und kommunizieren darüber mit der MEC-Plattform (MEC-App). Mögliche Produktzusammenstellungen, bestehend aus unterschiedliche Farbzusammenstellungen der Unter- und Oberteile und der Verbindungspins, können über ein Smartphone eingegeben werden. Diese Zusammenstellung wird von einer MEC-App verarbeitet. Bei der Produktion wird nun aufgrund von Informationen der Füllstände der Magazine (Leerstand einzelner Magazine) die Produktzusammenstellung dynamisch anpasst. Im originalen Setup kann die Produktionsanlage immer nur ein einziges Produkt fertigen. Der Use-Case steht stellvertretend für Brownfield-Anlagen, die zukünftig in ein 5G Campusnetz eingebunden werden und auch eine Erweiterung der Steuerung erfahren sollen.

#### **1.1.1.3 Use Cases bei ZIEHL-ABEGG**

Bei ZIEHL-ABEGG wurde 5G grundlegend bereits im Jahr 2019 beleuchtet und das Potential für Automation, Kommunikation und Sicherheit erkannt. 5G ist technologischer Teilaspekt in der ZIEHL-ABEGG Innovationsfabrik (InPro in Kupferzell) und soll in der »Fabrik der Zukunft« Anwendung finden. Insbesondere geht es dabei um die Automation von Produktions- und Logistikprozessen, die mit Hilfe einer verschlüsselten End-to-End-Kommunikation kommunizieren sollen. Dazu wurden fachübergreifend verschiedene Use-Cases im Zusammenhang mit 5G definiert. Insbesondere die Möglichkeit einer präzisen Lokalisierung bietet hier großes Potential, die Produktionsprozesse bei ZIEHL-ABEGG noch weiter zu optimieren. Abgeleitet aus diesen Use-Cases wurden für PIA5 in Abstimmung mit den Projektpartnern drei Use-Cases ausgewählt, die technologisch später die Basis für komplexere Anwendungen liefern.

##### **1.1.1.3.1 Lokalisierung von 5G Teilnehmern**

Ziel des Use Cases war es, eine möglichst präzise Lokalisierung von Teilnehmer im ZIEHL-ABEGG Campusnetz zu erreichen. Weiterhin sollten die Lokalisierungsdaten in strukturierter Form vorliegen, sodass sie weiterverarbeitet werden können. Eine weitere Anforderung war die zentrale Speicherung dieser Daten, sowie die Möglichkeit diese über eine API abrufen zu

können, deshalb erfolgte die Umsetzung als MEC-App. So können in der Zukunft beispielsweise Prozesse in der Lagerverwaltung optimiert werden.

#### **1.1.1.3.2 Condition Monitoring**

Auch heute werden die Produktionslagen bei ZIEHL-ABEGG durch eigenentwickelte Schnittstellen überwacht, um z.B. diverse Kennzahlen zu Verfügung zu stellen. Dieser Use-Case soll allgemein gesprochen, die Möglichkeit einer rein 5G basierten Sensordatenübertragung im OT-Umfeld evaluieren, so dass in Zukunft Verkabelung eingespart werden kann. Für die Umsetzung kam hier ein Prototyp der Firma BALLUFF, das CMTK (Condition Monitoring Toolkit) zum Einsatz, welches sowohl mit einem 5G-Modem als auch mit IO-Link Anschlüssen für Sensoren ausgestattet ist und so eine Schnittstelle in die OT schafft. Die softwareseitige Umsetzung erfolgte wieder als MEC-App, so dass die Daten zentral gespeichert und von anderen Teilnehmern ausgewertet werden können.

#### **1.1.1.3.3 5G Retrofitting**

Um den Einsatz von 5G in bestehenden Brownfield-Umgebungen zu testen, war es uns bei ZIEHL-ABEGG wichtig, auch einen Retrofitting Use Case abzubilden, um daraus Rückschlüsse zu ziehen, wie effizient zukünftig 5G als Technologie in den von ZIEHL-ABEGG weltweit betriebenen Produktionsstätten nachgerüstet werden kann. Für PIA5 wurde hierfür unser Produkt, ein Ventilator, 5G-fähig gemacht und Telemetriedaten von diesem ausgelesen und wie bereits in den vorherigen Use Cases mittels einer MEC-App zentral in einer Datenbank gespeichert und anderen Teilnehmern über eine Schnittstelle zur Verfügung gestellt.

#### **1.1.1.4 Use Cases bei der Hochschule Offenburg**

Die Hochschule Offenburg analysierte gemeinsam mit den Projektpartnern die Use-Case-Anforderungen für 5G-Campusnetze. Auf dieser Basis wurde definiert, wie die PKI und das Sicherheits-Setup gestaltet und integriert werden sollen.

Das Sicherheitsframework musste im Universitätslabor implementiert und verifiziert werden. Hierzu wurde ein Demonstrator aufgebaut, der die Authentifizierungslösung umsetzt. Anschließend wurde das erarbeitete Image exportiert und bei den Industriepartnern importiert, wo es in deren eigene Testbed-Umgebungen integriert wurde. Da sich das MEC-System sowie die vollständigen 5G-Testbeds bei Fraunhofer IIS befinden, erfolgte die weitere Validierung dort.

Das Labor umfasste einen PC, einen Router sowie einen Raspberry Pi mit einem Trusted Platform Modul (TPM) sowie einem 5G-Modemmodul. Damit konnte die sichere Kommunikationsabwicklung sowohl in einem 5G-Setup als auch in einem Nicht-5G-Setup demonstriert werden. Ebenso wurde die PKI-Funktionalität erfolgreich gemäß der vorgeschlagenen Lösung getestet.

Die definierten Ergebnisse in Form der erfassten Use Cases sowie der Anforderungen an das Gesamtsystem und an das Teilsystem der PKI-Integration in Endgeräten liegen vor.

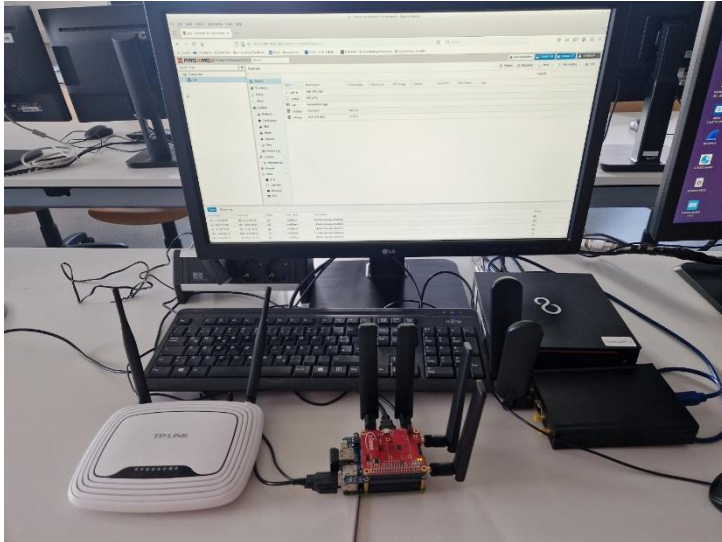


Abbildung 2: Lab Setup & Implementierung

Als Ergebnis der Arbeitspaket lagen Use-Case Beschreibungen und erste Anforderungsdefinitionen an das PIA5 System vor, die als Input für die nachfolgenden Arbeitspakete dienten.

### 1.1.2 Arbeitspaket AP2: Systemkonzept

In Zusammenarbeit mit den Projektpartnern entstand eine gemeinsame Systemspezifikation, die alle Funktionen wie Credential Management, Access Management und die erforderlichen Komponenten wie Secure Elements, User Equipments und genutzte Automatisierungskomponenten berücksichtigt. Weiterhin definiert sie die Verteilung der Funktionalität auf die einzelnen Komponenten und eine Festlegung der benötigten Schnittstellen.

#### 1.1.2.1 Durchführung einer Bedrohungsanalyse

Vorangestellt erfolgte die Durchführung einer Bedrohungsanalyse. Hierzu wurden folgende Schritte umgesetzt:

- Ermittlung des Schutzbedarfs aus den Use-Case Anforderungen
- Durchführung einer selektiven Bedrohungsanalyse (Thread Modeling nach dem STRIDE Model [1])
- Recherche und Analyse ausgewählter BSI-Grundsatzmodule [2] sowie der Technischen Richtlinien TR02102 [3] zu kryptographischen Verfahren, Empfehlungen und Schlüssellängen, sowie die TR 02103 [4] zu X.509 Zertifikaten und der Zertifizierungspfadvalidierung
- Einbeziehen der Anforderungen und Empfehlungen des IT-Grundsatz-Profils zur Absicherung von 5G-Campusnetzen im Eigenbetrieb [5]

Dabei ergaben sich folgende Ergebnisse. Durch die Anbindung der OT-Domäne an ein 5G-Campusnetz zur Unterstützung neuer Anwendungsfälle nimmt die Bedrohungslage der OT potenziell zu, da es zu neuen Angriffsvektoren gegen die OT-Steuerungstechnik kommen kann. Aus der durchgeführten Bedrohungsanalyse zeigten sich folgende Top 3

Bedrohungen, aus denen sich schwerwiegende Risiken ergeben und die Folgeangriffe ermöglichen können:

**Bedrohung 1: Verlust einer SIM-Karte:** Zum Großteil verfügen die Komponenten in der Produktion, wie auch die zu fertigende Produkte und IoT Devices über keine physikalischen Eingabemöglichkeiten (GUI). Deshalb wird die PIN-Eingabe für die Anmeldung am 5G Core hier oftmals deaktiviert. Somit ist der alleinige Besitz einer validen SIM-Karte ausreichend für das Einbuchen im 5G Campusnetz. Erhält ein Angreifer Zugriff auf eine SIM-Karte, besteht das Risiko, dass er sich damit direkt im 5G Netz anmelden kann und dadurch Zugriff auf die angebotenen Geräte erhält. Im IT-Grundschutz-Profil zur Absicherung von 5G-Campusnetzen wird genau dieser Punkt aufgegriffen und ein Management der SIM-Karten (Verwaltung, Ausgabe und sichere Aufbewahrung) als eine wichtige Sicherheitsmaßnahme gefordert. Die Durchführung dieser Maßnahmen gestaltet sich in der Praxis aber schwierig. Herkömmliche SIM-Karten können aus Geräten leicht entwendet werden.

**Bedrohung 2: Unvollständige Implementierung von Sicherheitsfunktionen.** Bei der Recherche nach 5G-Cores für private 5G-Netze und auch beim final eingesetzten Core in den Testbeds zeigte sich, dass hier die Schutzmaßnahmen der ETSI-Standards für 5G Netze, wie z.B. zertifikatsbasierte kryptographische Verfahren, teilweise noch nicht implementiert waren, so dass auch weniger sichere Verfahren zur Authentizitätsprüfung (Login und Passwortabfrage, anstatt zertifikatsbasierte Authentifikation) zum Einsatz kommen und der Datenverkehr zum Teil auch unverschlüsselt erfolgt. Hierdurch können sich potenzielle Angriffsvektoren ergeben.

**Bedrohung 3: Anfällige Software-Implementierung.** Die 5G-Cores für private Netze werden weitgehend "von Grund auf" neu programmiert. Hierdurch muss bereits aufgrund der Komplexität der Software von potenziell nicht erkannten Schwachstellen in der Programmierung ausgegangen werden. Durch eine geringe Verbreitung und aktuelle Marktdurchdringung können diese leicht unerkant bleiben oder erst bei erfolgreichen Cyberangriffen bekannt werden. Das potenzielle Risiko ergibt sich somit dadurch, dass bei neu programmierter Software die Wahrscheinlichkeit unentdeckter Schwachstellen größer ist als bei den Implementierungen im öffentlichen 5G Netz, die einem umfassenden Entwicklungsprozess unterliegen und zudem den Anforderungen der Kritischen Infrastrukturen gerecht werden müssen.

### 1.1.2.2 Sicherheitsarchitektur

Auf Basis der durchgeführten Bedrohungsanalyse wurden nun sicherheitserhöhende Maßnahmen definiert, welche durch das Security Framework realisiert werden sollen, siehe Abbildung 3:

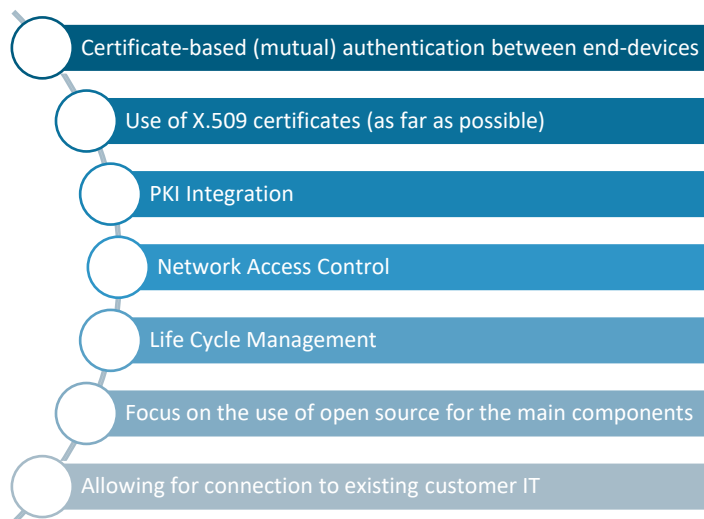


Abbildung 3: Sicherheitsmaßnahmen für das PIA5 System

### 1.1.2.3 Zertifikatsbasierte gegenseitige Authentifikation

Zusätzlich zur primären Authentifizierung, welche bei 5G Campusnetzwerken über 5G AKA erfolgt, wurde entschieden, dass eine sekundäre Authentifizierung basierend auf EAP-TLS erfolgen soll. Gründe für diese Entscheidung waren:

- Abwehrmaßnahme gegen SIM-Karten Diebstahl
- Zukünftige Kompatibilität mit primärer Authentifizierung mittels EAP-TLS, die zukünftig in Campusnetzen unterstützt werden soll.
- Domänenübergreifend; Ende-zu-Ende Sicherheit auch für Komponenten außerhalb des 5G Campusnetzes

Die sekundäre Authentifizierung von Endgeräten erfolgt zertifikatsbasiert, sofern Endgeräte dazu in der Lage sind. Entsprechend dem IEEE-Standard 802.1AR [6] : Secure Device Identity werden zwei Zertifikatstypen definiert (IDeVID Zertifikate und LDeVID Zertifikate, siehe Abbildung 4). Hierbei kommen digitale X.509 Zertifikate nach RFC 5280 [7] zum Einsatz. Die Verwendung anderer Zertifikate als X.509 ist möglich, wird nachfolgend aber nicht weiter betrachtet. Im Projekt erfolgte eine Erweiterung beziehungsweise eine spezifische Verwendung der LDeVID Zertifikate, was laut IEEE-Standard zulässig ist. Daraus resultieren drei Zertifikatstypen:

#### **Herstellerzertifikate – IDeVID Zertifikate**

Herstellerzertifikate dienen dem sicheren Nachweis der Herkunft und der Authentizität von Produkten und der Herstellersoftware. IDeVID Zertifikate werden vom Hersteller einer Komponente aufgebracht und verbleiben über den gesamten Lebenszyklus auf einer Komponente.

#### **Managementzertifikate – LDeVID-MGMT Zertifikate**

Managementzertifikate dienen der Inbesitznahme von Entitäten (Produkten, Anlagen, ...) und autorisieren den Besitzer zum Aufbringen von Anwendungszertifikaten. Durch das Aufbringen eines LDeVID-MGMT Zertifikats ist eine Entität in Besitz genommen, gilt als

vertrauenswürdig eingestuft und erhält initialen Zugriff auf das gesicherte Netzwerk. Zusätzlich kann sich die Entität mittels des LDevID-MGMT Zertifikats gegenüber der Credentialing Entität authentifizieren und so relevante Anwendungszertifikate erhalten. Ein LDevID-MGMT Zertifikat wird beim Besitzwechsel gelöscht und durch ein Entsprechendes des neuen Besitzers ersetzt.

### Anwendungszertifikate – LDevID [Application]

Anwendungszertifikate dienen der (gegenseitigen) Authentifizierung von Endgeräten (auf Anwendungsebene) und somit der Ende-zu-Ende Sicherheit, z.B. zwischen UEs aus dem 5G Netz (Produkt) und Komponenten des Daten-Netzes (Fertigungsanlage oder Datenbank). Anwendungszertifikate können nur vom aktuellen Besitzer einer Komponente aufgebracht, der über das Managementzertifikat authentisiert wird und dazu autorisiert ist (LDevID-MGMT).

In Abbildung 4 erfolgt die beispielhafte Darstellung der Zertifikate, sowie der PKI und Vertrauenskette. Es wird im Beispiel das Zwei-Ebenen Modell, mit einer Root CA und einer Sub CA gezeigt. Die Sub CA ist zugleich die Issuing CA, also die Instanz, welche die Endzertifikate (End-Entity Certificates) erstellt. Für jeden Zertifikatstyp ist eine eigene PKI dargestellt. Je nach gewünschter Ausprägung sind hier aber auch andere Modelle möglich. Die zur Anwendung kommenden X.509 Zertifikate können neben der Prüfung der Authentizität der Endkomponenten grundsätzlich für jeden im RFC 5280 vorgesehenen Einsatzzweck (Authentifikation, Verschlüsselung, Signatur) verwendet werden. Dabei gilt es zu beachten, dass jeweils ein eigenes Zertifikat für jeden Einsatzzweck generiert werden sollte, um Mehrfachverwendung von Zertifikaten zu vermeiden.

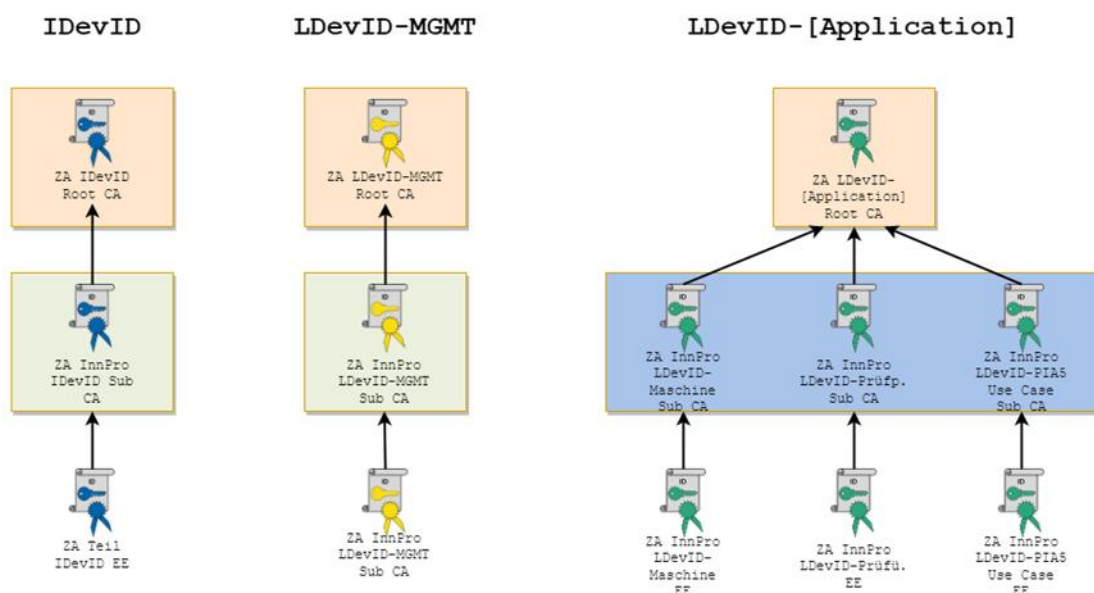


Abbildung 4 Zertifikatstypen und CA-Infrastruktur

Die Auswahl der CA-Implementierungen wird nicht vorgegeben. D.h. es wird ein generischer Ansatz verfolgt. Sowohl der Einsatz kommerzieller Implementierungen als auch freie Implementierungen sind somit möglich. Die Auswahl unterliegt dem Betreiber (Unternehmen) und

kann somit durch betriebsinterne Richtlinien festgelegt werden. Ebenso wenig schränkt das Konzept die Verwendung der Enrollment- und Management Protokolle, für das Ausrollen und das Lebenszyklusmanagement (Update, Revokation, usw.) von Zertifikaten, ein.

Besonders bei den Komponenten der Produktion, sowohl die Anlagen als auch die zu fertigten Komponenten betreffend, ist jedoch davon auszugehen, dass aufgrund von Ressourcenlimitierung eine Einschränkung bei der Auswahl der möglichen Managementprotokolle besteht. Die im Konzept vorgesehene Credentialing Entity (CE) schließt hier mögliche Lücken. Die CE agiert als Vermittler zwischen CA und Endgerät. Bei Bedarf kann sie eine Transformation der Enrollmentprotokolle zwischen CA und Endgerät vornehmen. Die Zertifikatsanforderung (CSR) und das Zertifikat selbst bleiben von den Transformationen jedoch unbeeinflusst. Die CE ist Bestandteil des PIA5 Security Frameworks.

Ein primäres Ziel bei der Entwicklung der Architektur war es, eine möglichst flexible Integration in existierende IT-Infrastruktur zu ermöglichen.

Daher orientiert sich die PIA5 Sicherheitsarchitektur an bestehenden Systemen zur Absicherung von Firmennetzen. Das Gesamtsystem soll aus den folgenden Hauptkomponenten bestehen:

- Firewall
- Network Access Control (NAC)
- Authentication und Authorization Service (AA)
- Credential Management, bestehend aus einer Credentialing Authority und der Credentialing Entity (CA & CE)
- Multi-Access Edge Computing Gateway (MEC)

Abbildung 5 zeigt den Aufbau der Software auf dem zentralen Server. Die Anordnung der Sicherheitskomponenten bezieht sich dabei auf den umgesetzten Demonstrator und soll keine strikte Vorgabe darstellen, wie die bezüglichen Softwarekomponenten in einem realen Einsatzfall verteilt sein müssen. Dies ist abhängig von der bestehenden IT-Infrastruktur in einem Unternehmen. Die Farben zeigen an, wie sicherheitskritisch die einzelnen Komponenten sind (hell → nicht kritisch zu dunkel → kritisch). Die Bestandteile des PIA5 Sicherheitsframeworks werden durch den Einsatz von separaten VMs vom MEC-Framework getrennt.

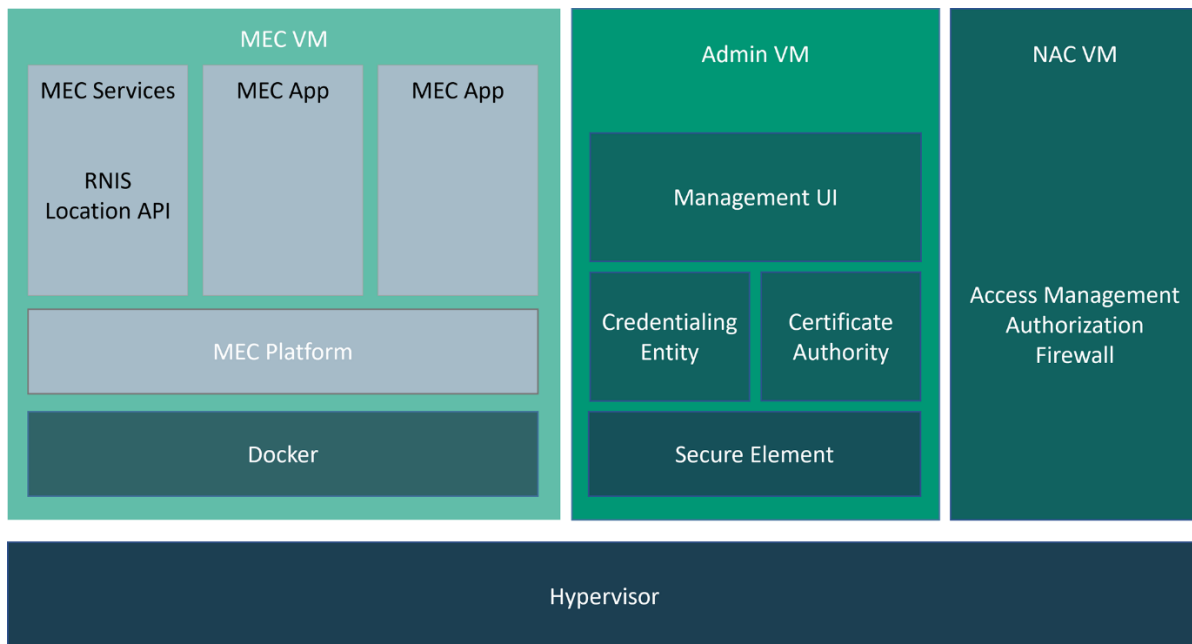


Abbildung 5: Sicherheitsarchitektur des PIA 5 Security Frameworks

#### 1.1.2.4 Multi-Access-Edge Computing mit Anbindung

Das MEC ist unabhängig vom eigentlichen Sicherheitsframework und wird analog zu Netzsegmenten in der IT und OT-Domäne als eigenes Segment betrachtet. Dies soll an dieser Stelle nur der Vollständigkeit halber erwähnt sein. Eine detaillierte Beschreibung erfolgt in Arbeitspaket 3.

Die **Network Access Control** Komponente dient als Einstiegspunkt in ein geschütztes Netz. Sie implementiert Protokolle, um einen Authentifizierungsvorgang mit verschiedenen Endgeräten anzustoßen und verwaltet, welche Endgeräte Zugriff auf welche Netzsegmente erhalten. Es existiert ein breites Angebot an sowohl kommerziellen als auch Open Source NAC Lösungen, die von Firmen eventuell bereits für ihre firmeninternen Netze eingesetzt werden. Der Funktionsumfang diverser NAC-Systeme variiert stark. Häufig sind ein Authentication and Authorization Server (AA) und eine Firewall integriert oder zumindest werden Zugriffspunkte für solche definiert. Konzeptionell wird für den präsentierten Prototypen davon ausgegangen, dass das NAC sich um die initiale Authentifizierung eines Endgeräts kümmert. Um sich an die Gegebenheiten bei Industriekunden anpassen zu können, ist das Security Framework so konzipiert, dass es parallel zu bereits existierenden NAC-Systemen eingesetzt werden kann. Für den Einsatz im Fraunhofer Testbed wird ein Open-Source NAC installiert.

Die **Firewall** arbeitet mit einer Whitelist, alle Verbindungen müssen explizit zugelassen werden. Die Whitelist wird von der **NAC-Komponente** verwaltet, oder kann manuell durch den Administrator konfiguriert werden, z.B. um Ende-zu-Ende verschlüsselte Kommunikation zwischen Bestandssystemen zuzulassen.

Die **Admin VM** kapselt Softwarekomponenten, die kritische Funktionen der PKI-Infrastruktur zur Verfügung stellen und somit sicherheitskritisch sind. Die Admin VM enthält die Credentialing Entity<sup>1</sup> und das dazugehörige Administratoreninterface, das eine Übersicht über alle verwalteten Identitäten sowie das Zertifikatsbasierte Rechtemanagement enthält. Falls eine eigene CA oder Sub-CA für die Automatisierungsdomäne genutzt werden soll, so wird diese ebenfalls in der Admin VM installiert. Der Admin VM kann Zugriff auf sicherheitsrelevante Hardwareressourcen wie z.B. ein Secure Element gewährt werden.

Die **Certificate Authority** signiert Zertifikate für Endgeräte. Die Signatur der CA auf dem Zertifikat einer Endkomponente ist, was diese Endkomponente als vertrauenswürdig ausweist. CAs sind ein zentraler Bestandteil von PKI-Systemen und wurden als solches bereits vielfach implementiert.

Die **Credentialing Entity** übernimmt ein zentrales Management von Zertifikaten der OT und 5G Domänen. Sie übernimmt eine Vermittlerfunktion zwischen Endgeräten und CAs und ermöglicht dabei für ressourcenbeschränkten Endgeräten in der OT-Domäne die Verwendung und das Management von Zertifikaten. Die CE setzt Verfahren zum Einbringen, Sperren und Löschen von Zertifikaten um. Zum Einsatz kommen die zu Beginn des Abschnitts „Zertifikatsbasierte gegenseitige Authentifikation“, beschriebenen Zertifikate.

Das **Secure Element** dient der Erzeugung qualitativ hochwertiger kryptographischer Schlüssel und zur sicheren Speicherung dieser. Damit wird eine Schlüsselextraktion durch Angriffe deutlich erschwert. Zudem bieten Secure Elements Unterstützung von kryptographischen Verfahren zur Verschlüsselung und Signatur von Daten.

Nach sorgfältiger Analyse möglicher Optionen wurde entschieden, das Security Framework an der Schnittstelle N6<sup>2</sup> und somit am Übergang zwischen 5G Campus Netz und dem Daten Netz (DN) zu positionieren (siehe Abbildung 6). Die Positionierung des Security Frameworks an der N6-Schnittstelle ist eine strategische Entscheidung, die sowohl die Sicherheit als auch die Flexibilität und Effizienz der MEC-Anwendungen maximiert. Die N6-Schnittstelle stellt einen zentralen Punkt für die Sicherheit dar. Sie ermöglicht die zentrale Überwachung und Verwaltung des domänenübergreifenden Zugriffs (der Kommunikation) zwischen 5G, IT und OT. Dies geschieht ohne direkten Eingriff in die einzelnen Domänen, was Sicherheitsrisiken minimiert. Eine zentrale Stelle für das Zertifikatsmanagement stärkt die Sicherheit und vereinfacht die Verwaltung von Zugriffsrechten. Die Positionierung an der N6-Schnittstelle ermöglicht zudem eine flexible Integration des Security Frameworks in verschiedene 5G Core-Architekturen, ohne dass tiefgreifende Modifikationen am Core selbst erforderlich sind. Dies ist besonders wichtig bei Open-Source-Implementierungen, wo Dokumentationsmängel und

---

<sup>1</sup> Die Credentialing Entity ist eine Zertifikats-Management-Einheit, welche die Nutzung unterschiedlicher Certificate Authority (CA) Zertifikats-Management Protokoller ermöglicht und zusätzliche Managementfunktionen übernimmt.

<sup>2</sup> Die N6-Schnittstelle ist eine der standardisierten Schnittstellen in der 5G-Architektur. Sie verbindet das User Plane Function (UPF) mit externen Datennetzen, wie dem Internet, Unternehmensnetzwerken oder Content Delivery Networks (CDNs).

mögliche lizenzrechtliche Probleme (wie „Copy-left“ Probleme) auftreten können. Bei kommerziellen 5G Cores könnte die Unterstützung durch Hersteller zusätzliche Kosten verursachen. Die N6-Schnittstelle hilft, diese Abhängigkeiten zu minimieren.

Für das MEC-Framework bietet die Anbindung an die N6-Schnittstelle des 5G Cores die Möglichkeit einer vollständigen direkte Erreichbarkeit aus allen Domänen. Um den vollen Funktionsumfang eines MEC nutzen zu können, benötigt das MEC zusätzlich zur Anbindung an die Data Plane eine Anbindung an die Control Plane des 5G Cores. Ein Anschluss an die Control Plane ist laut ETSI-Standard [8] über die NEF-Funktion vorgesehen, dies ist jedoch an den kommerziellen Cores, die in den beiden Testbeds eingesetzt werden, nicht möglich, da die Cores noch keine NEF enthalten. Eine alternative Einbindung des MECs als Application Function (AF) in den 5G Core ist ebenfalls nicht möglich, so dass hier andere Wege beschritten werden mussten. Diese sind je nach ausgewähltem 5G unterschiedlich. Details zur Umsetzung erfolgen in der Beschreibung in Arbeitspaket 3.

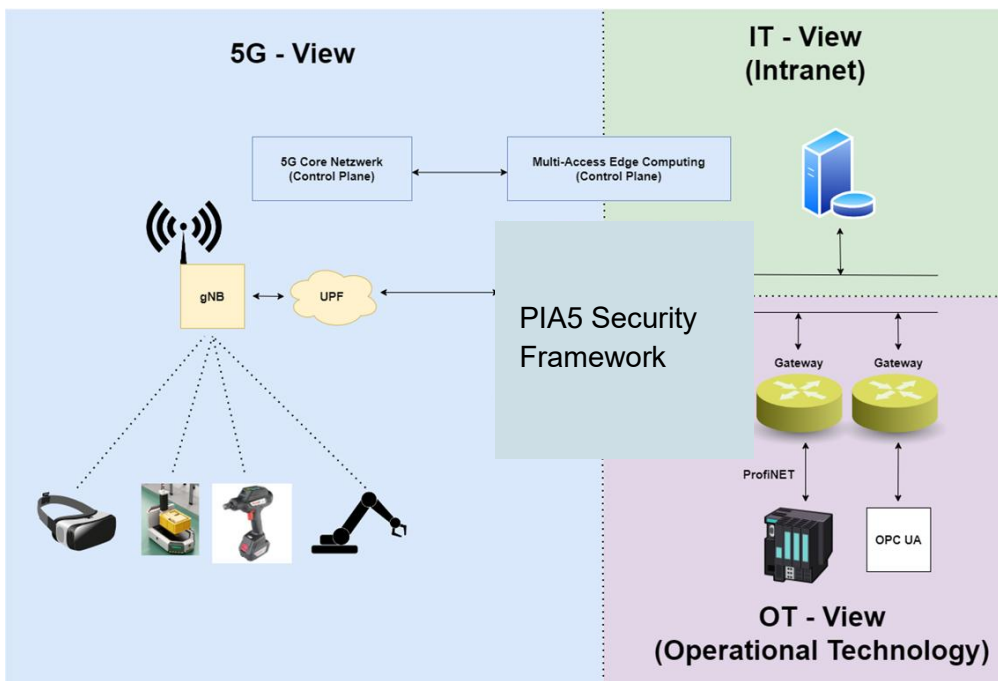


Abbildung 6 Einbindung des PIA5 Security Frameworks in die 5G, OT und IT-Infrastruktur

### 1.1.2.5 Recherche und Auswahl des Secure Element

Die Hochschule Offenburg führte mit Unterstützung des Fraunhofer IIS eine umfangreiche Recherche zu Secure Elements durch. Secure Elements (SE) sind manipulationsresistente Hardwarekomponenten, die dazu entwickelt wurden, kryptographisches Material sicher zu speichern und sicherheitskritische Operationen auszuführen. Sie stellen eine hardwarebasierte Root of Trust dar und werden zunehmend in 5G-Campusnetzwerken eingesetzt, um die Geräteauthentifizierung und das Anmeldedaten-Management zu stärken.

Die Hauptfunktion eines SE besteht darin, sicherzustellen, dass private Schlüssel und andere vertrauliche Anmeldedaten innerhalb der Hardwaregrenze verbleiben. Intern generierte und gespeicherte Schlüssel können nicht extrahiert werden, was im Vergleich zur rein softwarebasierten Schlüsselspeicherung eine zusätzliche Schutzschicht bietet. Darüber hinaus

ermöglichen Secure Elements eine Multi-Faktor-Authentifizierung, da der Zugriff auf das geschützte Material sowohl die physische Anwesenheit der Hardware als auch einen Autorisierungsfaktor, wie beispielsweise eine PIN, erfordert.

Innerhalb einer PKI-basierten Sicherheitsarchitektur bilden Secure Elements die Grundlage für das Lebenszyklusmanagement von Zertifikaten. Geräteidentitäten können über Zertifikate fest an die Hardware gebunden werden, wobei die zugehörigen privaten Schlüssel niemals das SE verlassen. Über standardisierte Schnittstellen wie PKCS#11 oder OpenSSL-Engines lassen sich SEs nahtlos in etablierte Protokolle integrieren. Dies ermöglicht eine sichere Zertifikatserstellung z. B. über Enrollment Over Secure Transport Protokoll (EST) sowie eine starke Authentifizierung mittels EAP-TLS. Auf diese Weise wird sichergestellt, dass Geräte im industriellen Umfeld von 5G-Campusnetzen während ihres gesamten Lebenszyklus eine überprüfbare und vertrauenswürdige Identität behalten.

Unter den verfügbaren Typen von Secure Elements ist das Trusted Platform Module (TPM) besonders für kleine eingebettete Geräte geeignet. Allerdings ist die Lieferkette für TPM-Module eingeschränkt, da nur wenige Hersteller zertifizierte Produkte anbieten. In dieser Arbeit wurde ein TPM-Modul von Infineon ausgewählt, da es verfügbar war und den erforderlichen Standards entspricht.

Betrachtete Secure Elements	Auswahlkriterien
<ul style="list-style-type: none"><li>•UICC</li><li>•USIM</li><li>•ESIM</li><li>•EUICC</li><li>•HSM</li><li>•TPM</li><li>•vTPM</li><li>•iSIM</li></ul>	<ul style="list-style-type: none"><li>•Öffentlich bekannte und gut definierte Schnittstellen</li><li>•Öffentlich verfügbare Treiber</li><li>•Kompatibilität mit Linux</li><li>•Unterstützung der geforderten kryptographischen Verfahren</li><li>•Formfaktor</li><li>•Für Embedded Systems geeignet</li></ul>

## 1.2 Arbeitspaket AP3: Integration Multi Access Edge Computing

Ziel des Arbeitspaketes war die Auswahl eines Multi Access Edge Computing Frameworks (MEC) und die Integration beziehungsweise Anbindung an das 5G Campusnetz. Das MEC dient dabei einerseits dazu, mittels spezifischer und autorisierter Services Informationen aus dem 5G Core zu beziehen und sie MEC-Anwendungen (APPs) zur Verfügung zu stellen und auch dazu, mittels der MEC APPs die Use Cases umzusetzen.

### 1.2.1 Auswahl des Multi Access Edge Computing Frameworks

Folgende Anforderungen wurde im Projekt erarbeitet. MEC-Lösungen mussten diese erfüllen, um für zukünftigen Einsatz in die engere Wahl zu gelangen:

- ETSI Compliance
- In aktiver Entwicklung

- Keine reinen Emulationen
- Dokumentation muss „relativ“ gut sein
- Entsprechung des eigenen in PIA5 vorgegebenem und geforderten Funktionsumfang
- Erweiterbarkeit
- Anbieter aus vertrauenswürdigen Staaten<sup>3</sup>
- Open Source Implementierung

Anhand der gestellten Anforderungen erfolgten eine umfangreiche Recherche und Bewertung von MEC-Implementierungen. Gestartet wurde mit einer Sichtung der ETSI konformen MEC-Implementierungen<sup>4</sup>, welche die ETSI auf ihren Webseiten nennt. Tabelle 1 zeigt die seitens der ETSI genannten MEC-Frameworks und die Benennung der Ausschlusskriterien, weshalb das Framework für PIA5 ungeeignet war.

Produkt	Ausschlusskriterium	In der näheren Auswahl
AdvantEDGE	Reine Emulation	
Akraino	Chinesische Entwicklung; Keine sinnvollen Services für unsere Use Cases	
Edge Galery	Chinesische Entwicklung	X
Eurocom/OpenAirInterface MEC		X
Italtel	Proprietäre APIs; Implementierung konnte nicht mehr gefunden werden	
LightEdge	Älteres Forschungsprojekt, scheint nicht maintained zu werden	X
Location API Simulator	Simulator, keine relevanten APIs	
Simus5G	Simulator basiert	

Tabelle 1 Auf Eignung untersuchte ETSI-konforme MEC-Frameworks

Dabei zeigte sich, dass nach eingehender Prüfung nur wenige Kandidaten es in die engere Auswahl schafften. Am Ende fiel die Wahl auf das MEC von OpenAirInterface.

Begründet werden kann dies mit der vergleichsweise guten Dokumentation, eine gute Einsatzmöglichkeit des implementierten MEC-Service (RNIS) für die ausgewählten Use Cases und aufgrund der Eignung als Template für die Implementierung weiterer MEC-Services.

<sup>3</sup> Auch wenn die Vorgabe der Bundesregierung derzeit nur für öffentlich 5G Kernnetze gilt, wurde im Projekt entschieden, keine Komponenten von chinesischen Herstellern zu nutzen. BMI: „In 5G-Kernnetzen dürfen bis spätestens Ende 2026 keine Komponenten von Huawei und ZTE mehr eingesetzt werden“. <https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2024/07/5g.html>

<sup>4</sup> [https://mecwiki.etsi.org/index.php?title=MEC\\_Ecosystem](https://mecwiki.etsi.org/index.php?title=MEC_Ecosystem)

Die Verwendung des Open Source Kong Gateways als zentrale Komponente des MEC sorgt außerdem dafür, dass das MEC leicht mit zusätzlichen Sicherheitsfeatures erweitert werden kann. Für das Kong Gateway gibt es eine große Menge an Addons, die für die Unterstützung diverser Sicherheitsprotokolle (z.B. OAuth2) sorgen. Leider sind nicht alle dieser Addons frei verfügbar.

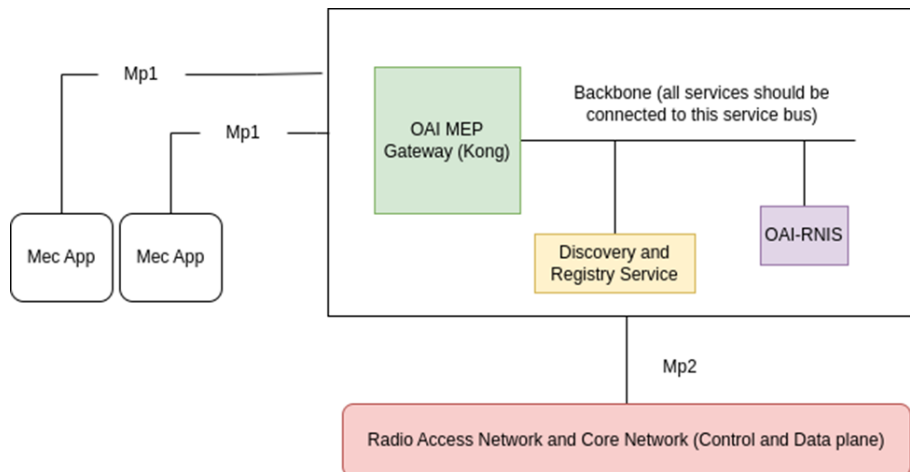


Abbildung 7 OAI MEC [Quelle : <https://gitlab.eurecom.fr/oai/orchestration/oai-mec/oai-mep>]

Wie in Abbildung 7 zu sehen ist, bietet das OAI (OpenAirInterface) MEC alle Schnittstellen, die zur Anbindung an den eingesetzten kommerziellen 5G Core und zur Umsetzung der geplanten Use Cases nötig sind (siehe unten). Die in der Abbildung mit Mp2 bezeichnete Schnittstelle entspricht der bereits erwähnten N6 Schnittstelle. Der Discovery and Registry Service stellt Endnutzern eine zentrale Liste aller verfügbaren Dienste unter einer bekannten Adresse zur Verfügung. Die einzelnen Services werden als Microservices implementiert und müssen sich lediglich bei der Registry anmelden, um für Nutzer verfügbar gemacht zu werden. Dadurch lässt sich das MEC leicht um zusätzliche Dienste ergänzen. Alle Dienste können ausschließlich über das Kong Gateway erreicht werden, das als zentraler Sicherheitsendpoint darstellt.

## 1.2.2 Technische Umsetzung & Middleware

Alle betrachteten Open Source MEC Plattformen sind für die Ausführung mit Docker konzipiert. Die MEC-Plattform selbst wird in einem Docker Container ausgeführt und MEC-Apps laufen ebenfalls in Containern. Je nach MEC-Lösung wird zusätzlich Kubernetes zum Managen der Container eingesetzt.

Beim Einsatz von Docker müssen die BSI Grundsatzbausteine SYS 1.5 Virtualisierung [9] und SYS 1.6 Containerisierung [10] beachtet werden. Insbesondere wird darauf hingewiesen, dass Anforderungen an Isolation und Kapselung der Anwendungen beachtet werden müssen. Der Zugriff von Virtuellen Systemen auf Schnittstellen des Host Systems ist einzuschränken. Im PIA5 Projekt betrifft dies insbesondere den Zugriff auf das Secure Element. Teile der PIA5 App, die direkt auf das Secure Element zugreifen müssen, daher wird z.B. der AA-Service nicht in Containern ausgeführt.

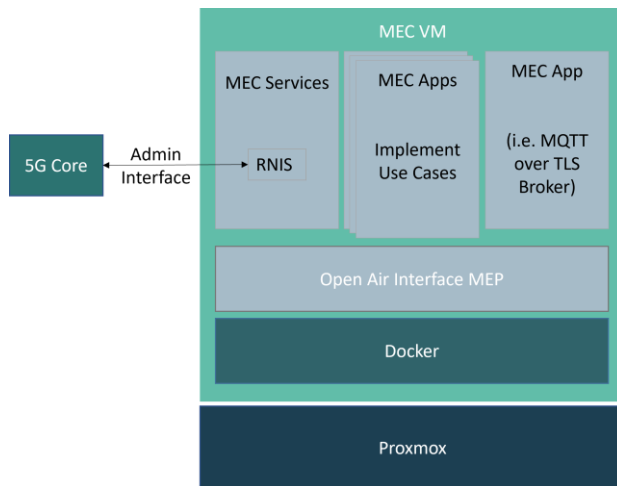


Abbildung 8 MEC-Software

Die MEC-Plattform ist in der Lage, zwei unterschiedliche Arten von Diensten zu hosten. Zum einen sind dies die MEC-Services und zum anderen die MEC-Apps (Anwendungen). Die MEC-Services bieten grundsätzlich Dienste für die MEC-Apps an. Sie sind Teil des MEC-Systems und können Daten aus dem 5G Core abfragen. Hierzu müssen sie über eine Anbindung an die Control Plane des 5G Cores verfügen. Damit unterliegen sie in aller Regel höheren Sicherheitsanforderungen als die MEC-Apps, zumindest aus Sicht der Stabilität des 5G Systems. Entgegen dem ETSI-Standard verfügt der 5G Core im PIA5 Projekt nicht über die Network Exposure Function (NEF) Schnittstelle. Der Zugriff auf interne Daten des 5G Cores erfolgte über ein vom Hersteller zur Verfügung gestelltes Admin Interface. Im PIA5 Projekt waren dies Lokalisierungsinformationen (beschränkt auf die aktuelle Cell ID, in dem sich ein UE befindet) und Kennwerte zu verbundenen 5G Geräten, z.B. IP-Adresse und Anbindungsstatus.

Die MEC-Apps sind Anwendungsprogramme, die für die Umsetzung der Use Cases erstellt wurden.

#### MEC-Services

- Abfrage, verwalten und verarbeiten von Informationsdaten aus dem 5G Core, oder anderen Daten-Quellen (Multi Access)
- Sind über die Control Plane an den 5G Core angeschlossen (NEF bzw. Admin-Interface)
- stellen Daten für MEC-Apps bereit

#### MEC-Apps

- MEC-Apps implementieren Use Cases
- sind über die Data Plane erreichbar

### 1.2.3 Integration, Anbindung des MEC-Frameworks an 5G Core

Eine zentrale Aufgabe des Arbeitspakets war die Anbindung an bzw. Integration des MEC-Frameworks in den 5G Core. Eine Integration in den 5G Core wurde aus zwei Gründen nicht umgesetzt. Die Integration wäre nur mit intensiver Unterstützung des Core Herstellers

möglich gewesen, was im Projekt nicht umsetzbar war. Außerdem sah das entwickelte Sicherheitskonzept in PIA5 vor, das MEC-Framework an den Domänenübergängen zu positionieren, was durch das Konzept einer Anbindung realisiert wurde. Eine weniger enge Kopplung an dieser Stelle bringt auch den Vorteil, dass eine Anbindung an andere 5G Core Implementierungen, oder eine spätere Anbindung über die NEF, falls diese verfügbar wird, mit deutlich weniger Aufwand verbunden wäre.

Für die Umsetzung der Use-Cases war folgender Informationsaustausch zwischen MEC-Framework und dem 5G Core erforderlich:

- Abfrage von Informationen über Endgeräteverfügbarkeit und (grobe) Lokalisierung
- Bereitstellen der Daten über die ETSI RNIS API

Die Anbindung des OIA MEC Frameworks an den 5G Core erforderte Anpassungsarbeiten. Das Schichtenmodell für das OAI MEC Framework zeigt Abbildung 9.

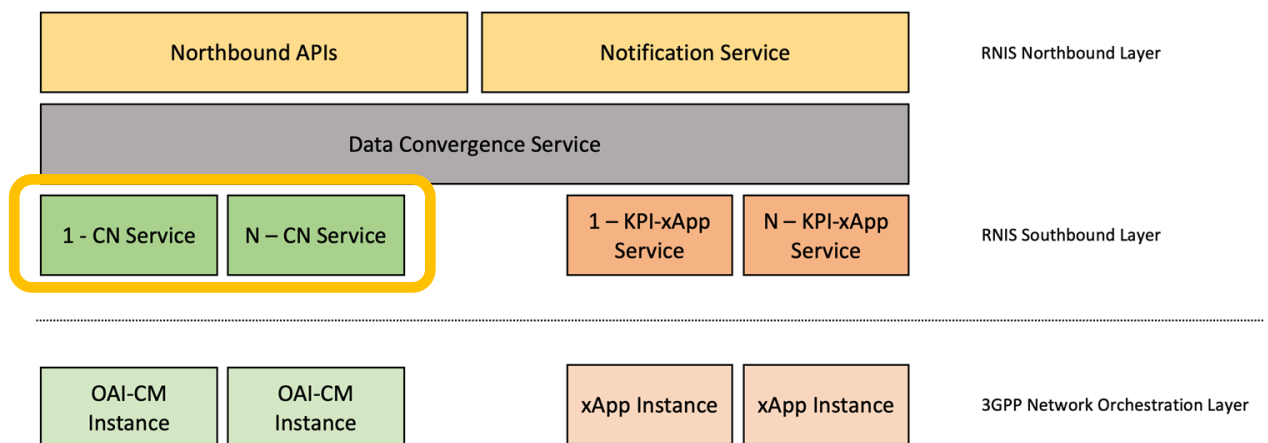


Abbildung 9 Schichtenmodell des OpenAirInterface(OAI) MEC Frameworks

Anders als ursprünglich erwartet, verfügt der genutzte 5G Core über keine NEF, so stand keine standardisierte API zur Abfrage der benötigten Daten zur Verfügung. Auch der OpenAirInterface Core, für den das verwendete MEC konzipiert wurde, verfügt zum Zeitpunkt der Arbeiten über keine NEF und die Abfrage der benötigten Informationen aus dem 5G Core erfolgt über eine nicht standardisierte REST API.

Um das MEC an den für den im PIA5 Testbed verwendeten 5G Core anzupassen, waren zusätzliche Arbeiten notwendig. Zum einen mussten die Core Network Services, die für den Verbindungsaufbau und Datenaustausch mit dem 5G Core verantwortlich sind, umgeschrieben werden. Dafür wurden API-Calls, die das OpenAir MEC an den OpenAir Interface Core schickt, durch äquivalente Abfragen an den eingesetzten 5G Core ersetzt.

Zum anderen musste die Logik des Data Convergence Services, der die Datenspeicherung und -verarbeitung des MEC übernimmt, angepasst werden. Dies war erforderlich, da das OAI MEC auf andere Datenformate und Hardwarekonfigurationen (z. B. Anordnung und Anzahl der Zellen pro Basisstation) ausgelegt war als die im Testbed des IIS gegebenen.

Abbildung 10 zeigt die Hardware, auf der das Security Framework und der MEC-Server ausgeführt wurden. Dabei handelt es sich um einen handelsüblichen 19“ Servereinschub (24 Intel Xeon CPUs, E5-2620).

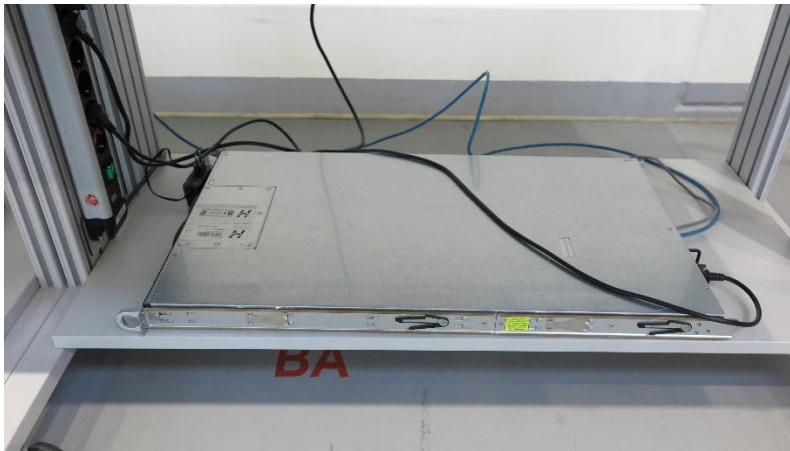


Abbildung 10 Server Hardware

### 1.3 Arbeitspaket AP4: PKI in den Endgeräten

Ziel des Arbeitspakets ist es, die zertifikatsbasierte Authentifikation und den PKI-Ansatz bis in die Endgeräte zu bringen. Speziell bei Brownfield-Anlagen bedarf es spezifischer Erweiterungen, damit eine zertifikatsbasierte Absicherung überhaupt erst umsetzbar ist. Die Befähigung der zertifikatsbasierten Authentifikation und weiterer kryptographischer Verfahren zum Schutz der Integrität und Vertraulichkeit von Daten bedarf bei Bestandsanlagen sowohl einer Hardware- als auch Softwareerweiterung. Im Projekt wurde diese durch ein Security Gateway erreicht, welches als Erweiterung der Bestandsanlage des Fraunhofer IIS vorgeschaltet wurde. Die Umsetzung erfolgte prototypisch mittels eines Raspberry Pi (Model 4B) mit dem Betriebssystem Raspian OS. Das Security-Gateway hat die Aufgabe, die sekundäre Authentifikation basierend auf EAP-TLS zu übernehmen. Für die Kommunikationsanbindung an das 5G Netz kam ein 5G Modem der Firma Quectel zum Einsatz [11]. Die Erzeugung und manipulationsgeschützte Speicherung der kryptographischen Schlüssel für die sekundäre Authentifikation wurde durch das in Arbeitspaket 1 bereits ausgewählte TPM erreicht.

Die Anbindung des TPM erfolgte durch die Hochschule Offenburg. Um die für das TPM verwendete Hierarchie zu realisieren, wurde auf die von der Trusted Computing Group definierten Hierarchien zurückgegriffen. Diese umfassen die Plattform-Hierarchie, die Endorsement-Hierarchie sowie die Storage-Hierarchie (auch Owner-Hierarchie genannt). In unserer Implementierung wurde die Storage-Hierarchie verwendet, bei der der Storage Root Key (SRK) als Anker dient. Diese Hierarchie ist für allgemeine Zwecke vorgesehen und ermöglicht es Systembesitzern und Administratoren, Schlüssel für Anwendungen – in unserem Fall auf dem Raspberry Pi – zu erzeugen und zu verwalten.

Das TPM stellt standardisierte Schnittstellen und Engines bereit, über die Anwendungen kryptographische Operationen durchführen können. Zu den unterstützten Engines gehören die PKCS#11-Engine sowie die OpenSSL-Engine. Anwendungen, die OpenSSL für TLS-Kryptographie nutzen, können TPM-geschützte Schlüssel ohne Änderungen verwenden. Für

unsere Lösung griffen wir in erster Linie auf die OpenSSL-Engine zurück. Allerdings traten hierbei Kompatibilitätsprobleme mit der aktuellen OpenSSL-Version (v3.x) auf. Nach Eröffnung eines Support-Tickets bestätigte der Hersteller das Problem, sodass wir als Work-around die ältere Version OpenSSL v1.1.1v kompilierten und einsetzten.

Darüber hinaus wurde die Nutzung der PKCS#11-Schnittstelle untersucht. Auf dem Endgerät, das Zugang zum 5G-Netzwerk erhält, erfolgte die Integration über wpa\_supplicant, der als primärer Network Manager auf dem Raspberry Pi fungiert. Die PKCS#11-Engine ermöglicht dabei ein Zwei-Faktor-Authentifizierungskonzept: Die erste Authentifizierung erfolgt über PacketFence mittels RADIUS EAP-TLS, während die zweite Authentifizierung auf Anwendungsebene (z. B. mit cURL) durchgeführt wird.

Die Realisierung der Ende-zu-Ende-Konnektivität erforderte eine enge Verzahnung von Softwaremodulen und unterstützenden Bibliotheken. Insbesondere mussten die eingesetzten Anwendungen sowohl die Funktionalitäten der PKCS#11-Engine als auch die OpenSSL-Kryptographiebibliothek unterstützen.

Für die PKI-Infrastruktur nutzten wir OpenSSL, um eine Proof-of-Concept-Umgebung mit einer Root-Zertifizierungsstelle, einer Sub-CA sowie End-Entity-Zertifikaten aufzubauen. Dieses Setup diente als Nachweis für die Integration einer PKI in unser Systemdesign.

Abbildung 11 zeigt das Sicherheits-Gateway mit der TPM-Erweiterung (Infineon SLB 9672 TPM2.0). Es ermöglicht die Anbindung einer Feldbuskomponente oder eine OT-Anlage an das 5G Campus Netz, aber auch an ein WLAN. Auf der Feldbusseite erfolgt eine Unterstützung des OPC-UA Protokolls und ermöglicht damit die Anbindung an die OPC-UA Schnittstelle der Produktionsstraße.

Bei kommerziell verfügbaren UEs kommen die dort bereits verfügbaren Komponenten für das Schlüsselmanagement zum Einsatz (Smartphone, usw.).

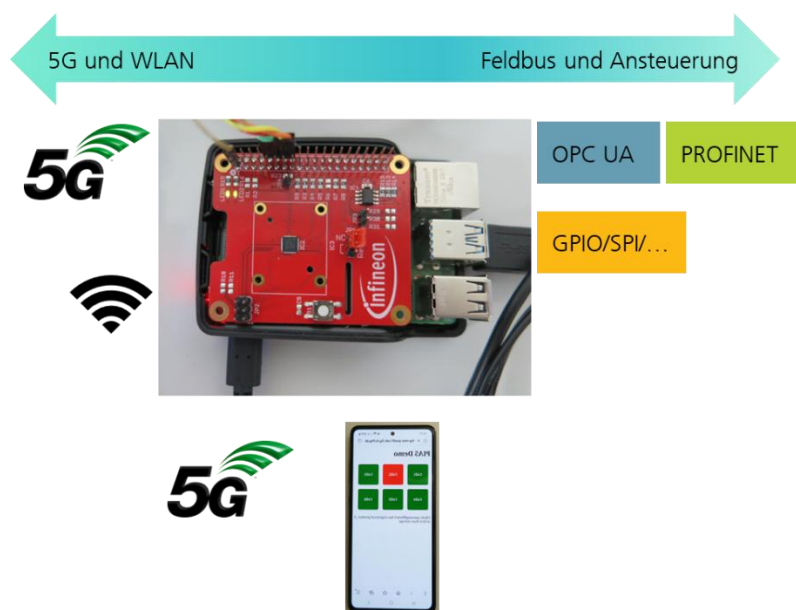


Abbildung 11: Raspberry Pi mit TPM-Erweiterung

Der Raspberry Pi dient dabei als Gateway zu WLAN und 5G Netzen (mit einem angebundenes 5G Modem) und als „Vorschaltgerät“ für das Retrofitting von Bestandsanlagen. In den implementierten Use Cases wurde er zur intelligenten Feldbuskomponente ausgebaut und erhielt weitere Zusatzkomponenten (Lichtschranke, Signalleuchte und Softwareerweiterung zur Anlagensteuerung. In Abbildung 11 sieht man das TPM (Secure Element des Herstellers Infineon) als aufgesteckte Hardwareerweiterung).

Das Smartphone dient als mobiles Bediengerät und verfügt über eine eigenständige 5G Netzanbindung. Für die zertifikatsbasierte Authentifikation, sowie die kryptographische Verschlüsselung der Kommunikation wurden Anwendungszertifikate genutzt. Verwendet wurden die vom Android Betriebssystem zur Verfügung gestellten Mechanismen für die Installation von Anwenderzertifikaten und CA-Zertifikaten.

## 1.4 Arbeitspaket AP5: Integration in ein 5G Campus Netzwerk

Ziel des Arbeitspakets war die Integration in bzw. Anbindung des Sicherheitsframeworks an das 5G Campusnetz und die Anbindung der Automatisierungsebene (OT). Die Arbeiten hierzu erfolgten zum Großteil beim Fraunhofer IIS. Die Integration und erste Funktionstests erfolgten am 5G Kernnetz am Fraunhofer Standort und waren Vorbereitung für die Integrationsarbeiten bei ZIEHL-ABEGG.

### 1.4.1 Auswahl eines geeigneten 5G-Kernnetzes

Im Rahmen des Projekts wurde die Auswahl eines geeigneten 5G-Kernnetzes als zentrale Aufgabe identifiziert, um die geplanten Testbeds erfolgreich umzusetzen. Dabei wurden sowohl Open Source als auch kommerzielle Lösungen evaluiert, um eine optimale Balance zwischen Funktionalität, Kompatibilität und Budgetanforderungen zu gewährleisten.

Es wurden verschiedene Open Source 5G-Kernnetze näher untersucht, darunter die Kernnetze **Open Air Interface** und **Open5GS**. Die Open Source Lösungen bieten grundsätzlich eine vielversprechende Grundlage für die Implementierung eines 5G-Kernnetzes. Allerdings traten im Verlauf der Evaluierung mehrere Probleme auf, die eine Nutzung im Projektkontext erschwerten. Für den Einsatz einer der im Rahmen der Open Source Implementierungen ausgetesteten und empfohlenen Basisstation wären zusätzliche Investitionen erforderlich gewesen. Dies war aufgrund von fehlendem Budget nicht möglich. Ein weiteres grundlegendes Problem ist die oftmals bei Open Source Projekten fehlende oder unvollständige Dokumentation, so dass der Aufbau eines 5G Campusnetzes zum eigenen Forschungsthema geworden wäre. Dies zeigte sich aber erst nach der eingehenden Recherche. Für das PIA5 Projekt war es zielführender, ein hinsichtlich Stabilität und Funktionalität stabileres 5G Kernnetz auszuwählen und einzusetzen, welches einen regulären Betrieb im Produktionsumfeld ermöglicht. Dies war nur durch den Einsatz eines kommerziellen 5G Kernnetzes im Rahmen der Projektlaufzeit zu erreichen.

Deshalb fiel die Entscheidung für den Einsatz in den beiden Testbeds bei ZIEHL-ABEGG und Fraunhofer zugunsten des 5G Kernnetzes **Druid-Core (Private Core Network (PCN))** des Herstellers Raemis [12].

Bei ZIEHL-ABEGG wurde in einem Auswahlverfahren der Druid-Core ausgewählt und am Fraunhofer IIS gab es hierzu bereits eine Installation. Die Vorteile sind Stabilität, garantierte Funktionalität und die Unterstützung durch einen Systemintegrator, der das 5G Campusnetz installiert und wartet und bei Fragen die Verbindung herstellen kann. Der Hersteller Remis arbeitet für den Druid-Core an der EAP-TLS Implementierung für die primäre Authentifikation, die während der Projektlaufzeit allerdings leider noch nicht zur Verfügung stand.

Bereits vor dem Projekt konnte ZIEHL-ABEGG erste Erfahrungen mit einem mobilen 5G Netz von Nokia sammeln. Im Rahmen von PIA5 wurde dann zusammen mit einem Implementierungspartner ein professionelles 5G Campusnetz in der Produktionsstätte Kupferzell BT4 installiert. Dies besteht aus vier Radio Units der Firma ASOCS, wobei drei der Radio Units den Innovationsbereich „InPro“ mit ca. 40 m x 40 m abdecken und die erste Zelle bilden, in der auch präzise Lokalisierung möglich ist. Die vierte Radio Unit deckt den Rest der Halle ab und bildet die zweite Zelle, so dass auch Übergänge zwischen diesen getestet werden konnten. Die Radio Units sind über Glasfaser an das ca. 300 m entfernte Data Center angeschlossen. Der Druid-Core von Remis wird auf einem DELL R750 Server betrieben. Im Laufe des Projekts wurden sowohl an Hard- und Software mehrere größere Optimierungen an dem Netz durch ASOCS, unseren Implementierungspartner und Kollegen des Fraunhofer Instituts vorgenommen. So wurde beispielsweise die Halle speziell vermessen, um die Reflexionen durch die vorhandene Umgebung berücksichtigen zu können, was wiederum wichtig für eine präzise Lokalisierung ist.

Durch die gemeinsamen Erfahrungen von ZIEHL-ABEGG und Fraunhofer IIS mit dem Druid-Core konnte so ein unkomplizierter Transfer und eine konsistente Integration des entwickelten Sicherheitsframeworks gewährleistet werden.

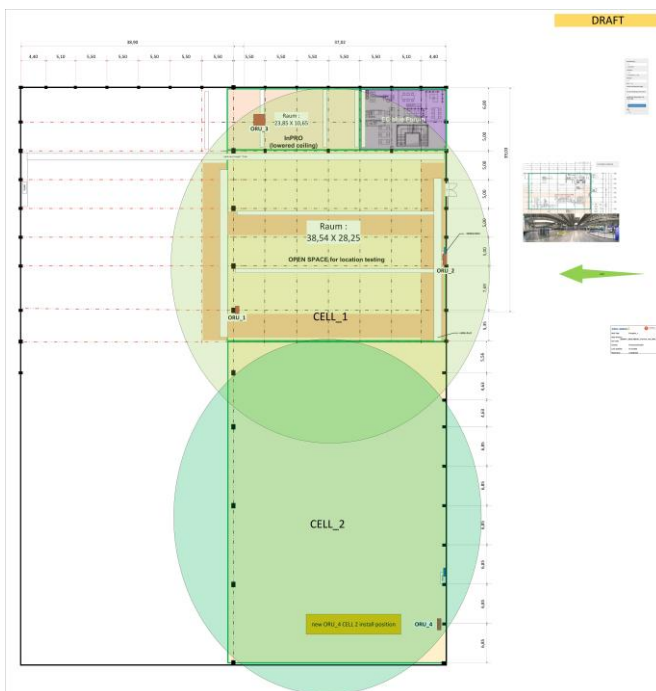


Abbildung 12: 5G Campusnetz von ZIEHL-ABEGG in Kupferzell

Die Auswahl eines geeigneten 5G-Kernnetzes stellte eine zentrale Herausforderung im Projekt dar. Während Open Source Lösungen wie Open5GS und Open Air Interface vielversprechend erschienen, verhinderten technische und budgetäre Einschränkungen deren Einsatz. Die Entscheidung für das kommerzielle 5G-Kernnetz Druid-Core ermöglichte eine stabile und zuverlässige Umsetzung der Testbeds. Gleichzeitig konnte durch die Integration von EAP-TLS in Open5GS durch die HSO ein wertvoller Beitrag zur Weiterentwicklung von Open Source Technologien geleistet werden.

## 1.4.2 Security Framework

Im Rahmen des Arbeitspakets wurde das in Arbeitspaket 1 erarbeitete Security Framework Konzept implementiert, das speziell auf die Anforderungen eines 5G-Kernnetzes abgestimmt ist. Ziel war es, die Sicherheit der Kommunikationsinfrastruktur zu gewährleisten und gleichzeitig die Integration mit dem 5G-Kernnetz und der Multi-Access Edge Computing (MEC)-Plattform zu ermöglichen. Die Umsetzung erfolgte gemäß der erstellten Systemspezifikation. Die Entwicklung und Integration des 5G-relevanten Security Frameworks war ein zentraler Bestandteil des Projekts. Trotz technischer Herausforderungen, wie der fehlenden Unterstützung von RADIUS über 5G, konnte eine sichere und funktionale Lösung implementiert werden. Das Radius Protokoll war geplant für die sekundäre Authentifikation im 5G Core nach ETSI TS 133 501, so dass Geräte zusätzlich zur SIM-Karte, deren Diebstahl einen zentralen Angriffsvektor darstellt, ein weiteres Credential benötigen, um Zugriff zu sicherheitskritischen Netzwerkabschnitten zu erhalten. Trotz intensiver Abstimmung mit dem Druid-Core Hersteller war die Nutzung des Radius Protokolls mit dem 5G Kernnetz nicht umsetzbar. Stattdessen wurde die Radiusimplementierung im Security Framework durch Anbindung an eine WLAN-Anbindung umgesetzt und funktional getestet. Die Netzsegmentierung stellt sicher, dass sensible Daten und Kommunikationsströme zusätzlich geschützt sind.

Wie bereits in AP3 beschrieben wurde das Security Framework an der N6-Schnittstelle integriert, wodurch die Sicherheit durch eine strikte Netzsegmentierung ergänzt wird.

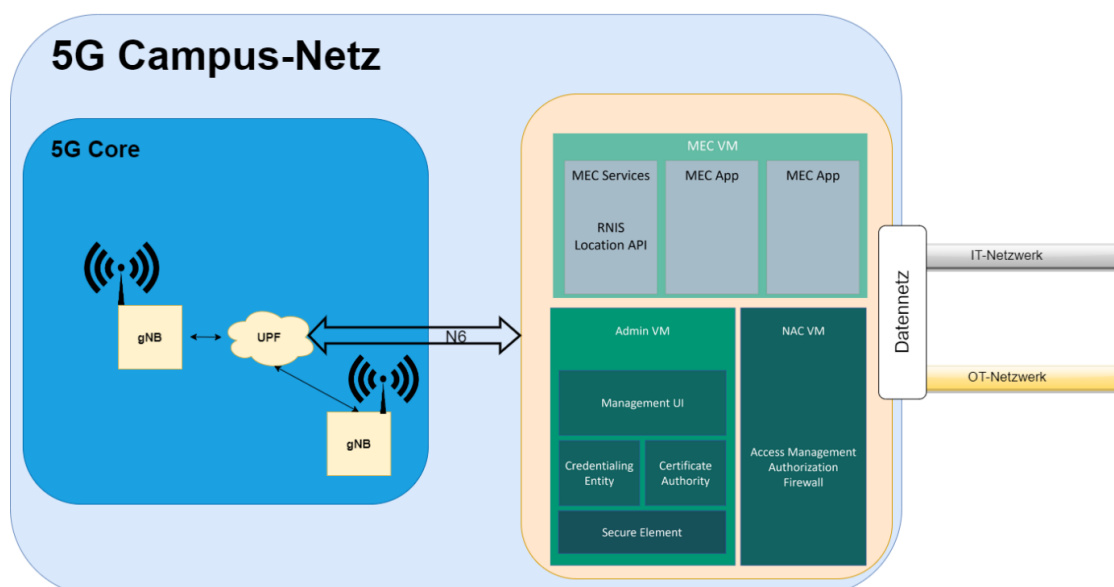


Abbildung 13: Anbindung des Security Framework und MEC-Framework an die N6 Schnittstelle des 5G Cores

### **1.4.3 Integration von EAP-TLS in Open5GS**

Trotz der Entscheidung für den Druid-Core wurde parallel eine Integration von EAP-TLS in das Open Source Kernnetz Open5GS durch den Projektpartner Hochschule Offenburg durchgeführt. Diese Arbeit stellt einen wichtigen Beitrag zur Weiterentwicklung von Open Source 5G-Kernetzen dar. Für die Integration von EAP-TLS in das 5G-Kernnetz wurde zunächst eine Literaturrecherche durchgeführt. Gemäß dem 3GPP-Standard sieht das Authentifizierungsframework zwei Ebenen der Authentifizierung vor: die primäre und die sekundäre Authentifizierung. In der Analyse wurden EAP-TLS und EAP-AKA miteinander verglichen, da beide Verfahren auf dem EAP-Framework basieren.

Im Anschluss wurde die Implementierung des Open5GS-Core und UE-RANSIM untersucht. Die Software wurde installiert und mit Wireshark-Traces analysiert. Dabei konnten zwar mehrere Interaktionen zwischen den Netzelementen beobachtet werden, jedoch waren nicht alle erforderlichen Kommunikationsaustausche in den Traces sichtbar. Eine anschließende Codeanalyse ergab, dass Open5GS derzeit ausschließlich 5G-AKA als Authentifizierungsmethode unterstützt. Zusätzlich wurde das Rohde & Schwarz CMX500-System auf die Unterstützung von EAP-AKA überprüft, wobei sich herausstellte, dass auch dort keine Implementierung vorliegt.

Gemäß den 3GPP-Spezifikationen ist die Ableitung mehrerer Sicherheitsschlüssel erforderlich, die in einer komplexen Hierarchie des 5G-Netzes eingebettet ist. Die Umsetzung von EAP-TLS erwies sich daher als herausfordernd, da Kommunikationsaustausche über verschiedene Schnittstellen hinweg notwendig sind. Darüber hinaus wurden Änderungen identifiziert, die in Open5GS umgesetzt werden müssten, einschließlich Erweiterungen der Open-API-Modellierungssprache.

## **1.5 Arbeitspaket AP6: Vorbereitung der Integration in die Automatisierung und Produktion**

Ziel des Arbeitspakets war die Vorbereitung und Abstimmung mit ZIEHL-ABEGG hinsichtlich der Integration des Security Frameworks in die Produktionsinfrastruktur.

### **1.5.1 Integration des Security Frameworks in die Produktionsumgebung von ZIEHL-ABEGG**

Die Integration des Security Frameworks in die Produktionsumgebung von ZIEHL-ABEGG war ein wichtiger Meilenstein im Projekt. Durch die enge Zusammenarbeit mit der IT-Abteilung von ZIEHL-ABEGG konnte eine erfolgreiche Integration in das 5G-Campusnetzwerk am Standort Kupferzell realisiert werden. Ziel war es, die Sicherheitsanforderungen in der Kommunikationsinfrastruktur von ZA zu erfüllen und exemplarisch die Anbindung eines Produkts an das 5G-Campusnetzwerk und das Security Framework zu demonstrieren.

Hierzu war ein intensiver Austausch mit der IT-Abteilung von ZA erforderlich, um die Integration des Gateways, bestehend aus einem Server mit der in AP2 dargestellten Softwareinstallation in die bestehenden Kommunikationsnetze zu ermöglichen. Dazu wurde ein Kommunikationskonzept erstellt, das die Anforderungen und technischen Details der Integration definierte. Das Konzept wurde der IT-Abteilung von ZA vorgestellt und gemeinsam abgestimmt, um eine reibungslose Umsetzung sicherzustellen. Eine Besonderheit, auf die während der

Vorbereitung Rücksicht genommen werden musste, war, dass bei ZIEHL-ABEGG die logische Architektur des 5G-Netzes von der von Fraunhofer IIS abwich, da die für den Betrieb des Kernnetzes essenziellen Komponenten, wie z.B. der Druid-Core bei ZIEHL-ABEGG in einem eigenen, von den Teilnehmern separiertem Netz betrieben werden. Da das Security Framework aber sowohl die Schnittstellen des Druid-Cores, als auch die Benutzer des 5G-Netzes erreichen muss, musste sichergestellt werden, dass der Server in beiden Netzen erreichbar ist.

Für die praktische Umsetzung stellte ZA einen Server zur Verfügung, auf dem vom Fraunhofer IIS das Security Framework installiert und ausgiebig getestet wurde. Diese Tests dienten dazu, die Funktionalität und Kompatibilität des Frameworks mit der bestehenden IT-Infrastruktur zu validieren. Das Arbeitspaket endete mit der erfolgreichen Integration des Security Frameworks und der Anbindung des MEC an die vor Ort gegebene Infrastruktur. Es wurde eine technische Einführung durchgeführt, um die IT-Abteilung von ZA mit der Nutzung und Verwaltung des Frameworks vertraut zu machen. Zusätzlich wurde eine technische Dokumentation erstellt, die alle relevanten Details zur Installation, Konfiguration und Nutzung des Frameworks enthält.

Die exemplarische Anbindung eines Ventilators und die Entwicklung eines Retrofitting-Moduls bei ZIEHL-ABEGG demonstrierten die praktische Anwendbarkeit und Flexibilität des Frameworks. Die durchgeführten Tests und die technische Dokumentation stellen sicher, dass das Framework langfristig in der Produktionsumgebung von ZA genutzt und weiterentwickelt werden kann. Die Integration war die Voraussetzung für die Umsetzung der Use-Cases in den beiden Testbeds.

Im Rahmen des Projekts wurden durch die Hochschule Offenburg die theoretischen Konzepte sowie empfohlene Vorgehensweisen des Industriepartners ZIEHL-ABEGG und dem Fraunhofer-Institut in mehreren Sitzungen mit dem IT-Team und weiteren relevanten Stakeholdern vorgestellt und diskutiert. Ziel dieser Treffen war es, den angemessenen Einsatz der Konzepte in der Produktionsinfrastruktur zu bewerten und vorzubereiten. Der Wissenstransfer konnte insbesondere dadurch effektiv gestaltet werden, weil ein Großteil der entwickelten Lösungen auf Open-Source-Bibliotheken basiert. Das erworbene Wissen wird von ZIEHL-ABEGG für die Übertragung in produktionsnahe Umgebungen genutzt.

## **1.6 Arbeitspaket AP7: Durchführung von Funktions- und Resilienztests für ausgewählte Use Cases**

### **1.6.1 Use Cases Fraunhofer IIS**

Im Rahmen des Projekts wurden bereits während der Entwicklung und der Integration in die Testbeds sukzessive immer wieder Tests durchgeführt, um die Funktionalität, Sicherheit und Performance der entwickelten Lösungen zu validieren. In diesem Arbeitspaket erfolgte nun eine spezifische und umfassende Testdurchführung mit dem Ziel einer möglichst hohen Testabdeckung. Dies umfasste funktionale Prüfungen, Sicherheitsanalysen und Performance-tests. Ziel war es, die Praxistauglichkeit der Lösungen zu bewerten und potenzielle Schwachstellen zu identifizieren. Gemeinsam mit den Projektpartnern wurden verschiedene

Testabläufe geplant, um die spezifischen Anforderungen der jeweiligen Testbeds zu berücksichtigen. Die Schwerpunkte des Fraunhofer IIS lagen auf den Tests der eigenen Use Cases im IIS-Testbed, insbesondere auf funktionalen Tests. Ein besonderer Fokus lag auf der Validierung der Sicherheitsfunktionen, wie dem Zertifikatsmanagement und dem Berechtigungsmanagement. ZIEHL-ABEGG konzentrierte sich auf die Tests der eigenen Use Cases im ZA-Testbed, um die Integration in die Produktionsumgebung zu evaluieren.

Die durchgeführten Funktionstests und Resilienztests haben die Praxistauglichkeit der entwickelten Lösungen bestätigt. Die Integration der verschiedenen Komponenten in das IIS-Testbed ermöglichte eine umfassende Validierung der Funktionalität und Interoperabilität.

Die Sicherheitsanalyse und Literaturrecherchen zeigten, dass die größte Angriffsfläche im Entwerfen der SIM-Karte liegt, was durch gezielte Sicherheitsmaßnahmen adressiert wurde. Die Performancetests lieferten wertvolle Erkenntnisse über die Auswirkungen des Sicherheitsframeworks auf die Anwendungen, insbesondere in Bezug auf Latenz und Schlüsselmanagement.

Die Ergebnisse der Tests bilden eine solide Grundlage für den weiteren Einsatz und die Optimierung der entwickelten Lösungen.

Im Rahmen der Sicherheitsauswertung lag der Fokus abweichend vom ursprünglichen Plan auf theoretischen Analysen, insbesondere auf der Sichtung von bekannten Schwachstellen, die in den Datenbanken CVE (Common Vulnerabilities and Exposures) und CWE (Common Weakness Enumeration) erfasst sind. Der Grund für diese Herangehensweise war der Einsatz von Open Source Software, für die Schwachstellen bereits anderweitig dokumentiert und analysiert wurden und zusätzliche Penetrationstests auf die Open Source Software keinen weiteren tiefgreifenden Nutzen erwarten ließen und das Testen von Open Software nicht im Fokus des Projekts lag.

Die Performancetests zielten darauf ab, die praktischen Auswirkungen des eingesetzten Sicherheitsframeworks auf die Anwendungen zu untersuchen. Dabei wurden folgende Aspekte analysiert:

- Dauer der Erstellung und Verteilung von Zertifikaten: Es wurde geprüft, wie lange dieser Prozess benötigt, um die Effizienz des Frameworks zu bewerten.
- Schlüsselgenerierung mit und ohne TPM (Trusted Platform Module): Ein Vergleich wurde durchgeführt, um die Unterschiede in der Performance zu ermitteln.
- Latenz durch Verschlüsselung und Zertifikate: Die Auswirkungen der Verschlüsselung und Zertifikatsnutzung auf die Latenz zwischen 5G und OT (Operational Technology) wurden untersucht.
- Die Performance des 5G-Netzwerks selbst wurde nicht getestet, da hierzu bereits Ergebnisse vorliegen, die jedoch der Geheimhaltung unterliegen.

Zusammenfassend wurde festgestellt, dass bei HTTPS mit beidseitiger Nutzung von Zertifikaten im Vergleich zu HTTPS ohne zertifikatsbasierte Authentifikation es zu keinen signifikanten Unterschieden in der Performance kam. Bei der Nutzung des TPM-Moduls in HTTPS wurde im Testaufbau eine signifikante Verschlechterung der Performance um Faktor 14 ermittelt. Die Ursachen für dieses Verhalten konnten im Rahmen der Tests nicht ermittelt werden. Die Anbindung des TPM zeigte sich generell als nicht trivial und erforderte ohnehin

Support durch der Hersteller Infineon. Für weiterführende Untersuchungen waren im Projekt keine Mittel verfügbar. Dies hatte generell Auswirkungen auf die Qualität der der Performanceanalyse.

Die Hochschule Offenburg konzentrierte sich bei der Testdurchführung auf Funktionstests der PKI-basierten Authentifizierung mit PacketFence als RADIUS-Server in einer Proxmox-VM unter Verwendung von TPM-gestützten Schlüsseln. Diese Tests hatten das Ziel, die sichere Umsetzung der EAP-TLS-Authentifizierung zu prüfen. Die Testumgebung bestand aus einer Proxmox-VM mit PacketFence, einem Supplicant mit TPM 2.0 sowie einer Zertifizierungsstelle (CA). Der private Schlüssel blieb dabei über PKCS#11 im TPM geschützt, während PacketFence mit dem CA-Trust-Anchor für die Zertifikatsprüfung konfiguriert war.

Mit `tpm2_ptool` wurde ein Token erstellt und ein Schlüssel generiert. Daraus entstand eine Certificate Signing Request (CSR), die von der CA signiert zurückgegeben wurde. Der Supplicant wurde mit der PKCS#11-URI des Schlüssels in `wpa_supplicant.conf` konfiguriert, und die Protokolle bestätigten das fehlerfreie Laden der Zertifikatskette.

Im positiven Testfall verlief die EAP-TLS-Authentifizierung erfolgreich, und PacketFence validierte das Zertifikat korrekt. Im negativen Testfall wurde ein ungültiges Zertifikat erwartungsgemäß abgelehnt. Während der Tests traten keine Leistungs- oder Stabilitätsprobleme auf.

Zusammenfassend zeigen die Tests, dass PKI-basierte EAP-TLS-Authentifizierung mit TPM-gestützten Schlüsseln in einer PacketFence-RADIUS-Umgebung unter Proxmox zuverlässig funktioniert und die Sicherheitsanforderungen für zertifikatsbasierte Authentifizierung erfüllt.

Bezüglich der technischen Umsetzung und den weiteren Tests wurden vom Fraunhofer IIS aus den im Arbeitspaket 1 erarbeiteten Use Cases zwei ausgewählt und hier näher beschrieben:

- Adaptive Produktion und
- Produktlagerung mit Ortsinformationen

#### **1.6.1.1 Umsetzung und Test: Use Case Adaptive Produktion**

Die Umsetzung des Use Cases erfolgte unter Einbeziehung der am Standort Nürnberg vorhandenen Produktionsstraße. Abbildung 14 zeigt die einzelnen Substationen. Die Produktionsstraße erlaubt, ohne die PIA5 Erweiterung, die Konfiguration einer Produktzusammenstellung aus Unterteilen (Station 1 schwarz, Station 2 weiß), Oberteilen (Station 3 schwarz, Station 4 weiß) und einem Verbindungsstift (Station 5 Kunststoff, Station 6 Metall). Es kann ein Werkstück gefertigt werden, danach muss dieses vom Transportschlitten (sichtbar bei Station 6, Start) entnommen werden. Die Anlage verfügt über keine Sicherheitsmaßnahmen, wenn das Werkstück nicht entnommen wird, und es kommt bei einem Neustart zu einer Kollision, wenn der Schlitten bereits mit dem vorherigen Werkstück beladen ist.

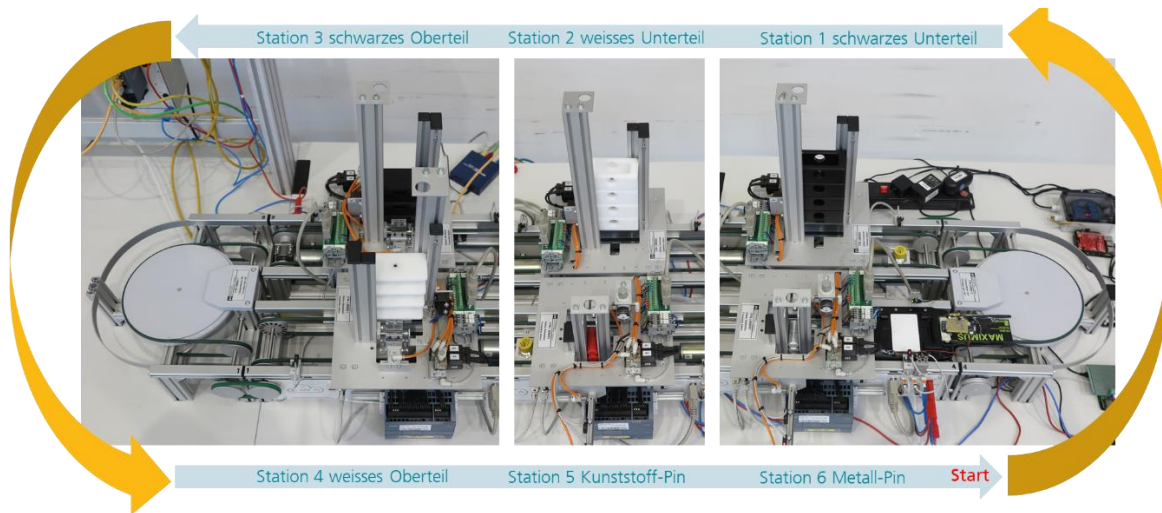


Abbildung 14: Produktionsstraße

Gegenstand des Use Cases war nur mittels Software- und Hardwareerweiterungen, welche im 5G Campusnetz eingebunden sind, mittels Retrofitting einer Bestandsanlage eine funktionale Erweiterung der Grundfunktionen exemplarisch zu zeigen. Der Use Case wurde so ausgeführt, dass er im 5G Campusnetz bei ZIEHL-ABEGG für weitere Retrofitting-Anwendungen ebenfalls eingesetzt werden kann. In der Produktionsstraße erfolgte das Anbringen einer Lichtschranke am Startpunkt, welche den Beladungszustand des Transportschlittens überprüft und einen Neustart nur dann freigibt, wenn dieser unbeladen ist. Weiterhin erfolgte das Anbringen einer Signalleuchte, welche je nach Status grün oder rot leuchtet. Die Kommunikationsanbindung erfolgte jeweils über 5G Modems und einen Raspberry Pi. Auf diesen 5G Endknoten sind die Sicherheitsmechanismen aus AP 5 implementiert, d.h. zertifikatsbasierte Authentifikation mittels X.509 Zertifikaten und Verschlüsselung der Kommunikation. Die Generierung der kryptographischen Schlüssel und die sichere Verwahrung der privaten Schlüssel erfolgt im Secure Element (TPM). Abbildung 15 zeigt die Erweiterungskomponenten. Die Erweiterungskomponenten kommunizieren direkt mit einer MEC-App, welche auf der MEC-Plattform gehostet wird.

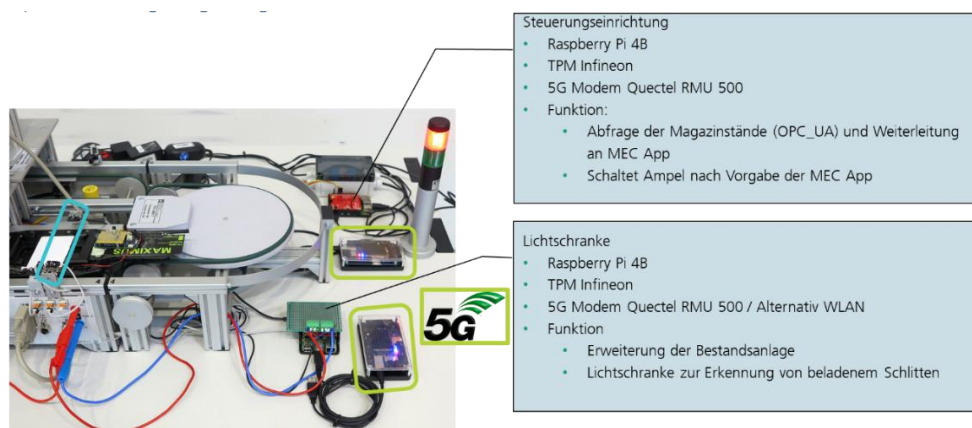


Abbildung 15: PIA5 Erweiterungen

Vorrangiges Ziel des Use Cases ist es, exemplarisch zu zeigen, dass durch die Erweiterung eine Anbindung von Bestandsanlagen an ein 5G Campusnetz mit zusätzlichen Sicherheitsmaßnahmen, der sekundären Authentifikation, möglich ist und eine Ende-zu-Ende Sicherheit damit realisierbar wird. Funktional wurde die Anlage dahingehend erweitert, dass in ein Auftragssystem, welches im vorliegenden Use Case durch eine MEC-App realisiert wird, mehrere Aufträge eingegeben werden können und bei einem Leerlaufen eines Magazins (Unterteil, Oberteil, Verbindungspin) auf einen gemäß der Konfiguration nachfolgenden Auftrag gewechselt wird. In Abbildung 16 werden alle am Use Case beteiligten Komponenten und die Funktionsabläufe dargestellt.

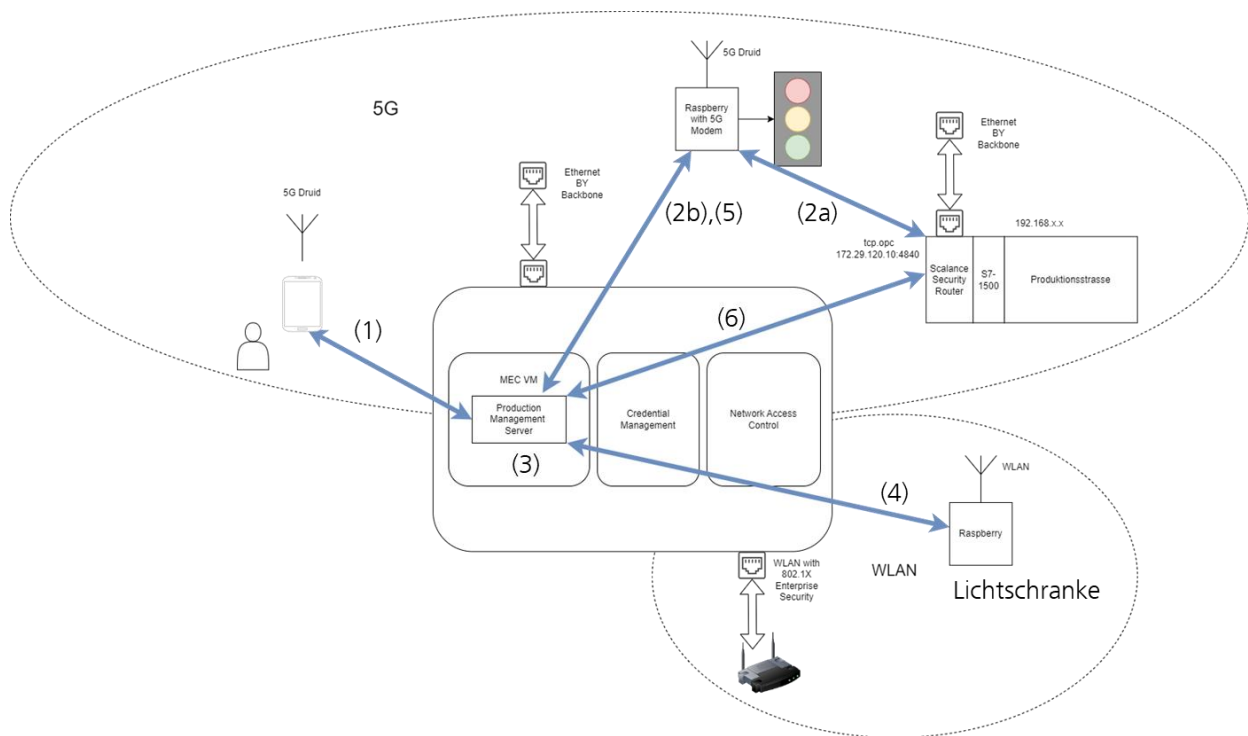


Abbildung 16 PIA 5 Gesamtsystem für Use Case Adaptive Produktion

Funktionaler Ablauf:

- Schritt (1): Der Nutzer gibt eine Liste der gewünschten Produkte in ein Endgerät (Smartphone oder Laptop) ein und übermittelt diese an die MEC-App (Produktion Management Server)
- Schritt (2a, 2b) Es erfolgt eine Abfrage der Magazinstände durch die MEC-App. Der Raspberry PI dient hierbei als Security Gateway, der nur Anfragen von Geräten mit entsprechenden Anwenderzertifikaten akzeptiert. Er ermöglicht außerdem die physikalische Anbindung der Produktionsstraße, die nur Ethernet und das OPC UA Protokoll unterstützt, an das 5G Campusnetz und das HTTPS-Protokoll.
- Schritt (3): Die MEC-App berechnet, welche Produktvariante auf Basis der Magazinstände aktuell gefertigt werden kann.

- Schritt (4): Die MEC-App überprüft mittels Abfrage der Lichtschranke den Status des Transportschlittens. Die Anbindung der Lichtschranke erfolgte im Testbed über 5G und alternativ über WLAN. Über die WLAN-Anbindung wurde die Möglichkeit gezeigt, auch weitere Funkstandards zu bedienen und es konnte die – im 5G Kernnetz nicht verfügbare – Radius Anbindung getestet werden.
- Schritt (5): Die MEC-App übermittelt den (Schalt-)Zustand an die Signalleuchte. Grün: die Produktion kann gestartet werden. Rot: es gibt einen oder mehrere Fehler.
- Schritt (6): Start der Produktion, wenn keine Fehler vorliegen. Die tatsächliche Kommunikation zwischen MEC-App und Produktionsstraße erfolgte wie bei Schritt 2a und 2b über das Security Gateway.

Die Schritte 2a, 2b, 3, 4, 5 und 6 erfolgen zyklisch, bis eine Anpassung der Produktkonfiguration entsprechend der Magazinstände vorgenommen wird, keine vorgegebene Konfiguration mehr gefertigt werden kann oder die Aufträge abgearbeitet sind.

### 1.6.1.2 Umsetzung und Test: Produktlagerung mit Ortsinformationen

Zielsetzung des Use Cases ist es, zu zeigen, dass Daten im Lagersystem durch Ortsdaten, welche aus dem 5G Kernnetz bezogen werden, ergänzt werden können, wodurch sich die Positionsbestimmung von Lagerware vereinfacht. Der Use Case steht stellvertretend für jegliche Arten von Lokalisierung im 5G Campusnetz. Da beim eingesetzten 5G Kernnetz des Fraunhofer IIS sich die Positionsbestimmung aktuell nur auf die Zellinformation bezieht, kann hier leider keine genauere Information geliefert werden. Im Testbed von ZIEHL-ABEGG waren hier wesentlich genauere Lokalisierungsdaten verfügbar. Für die Umsetzung kam das Security Gateway und die MEC-Plattform zur Anwendung, wie diese in Abbildung 16 bereits gezeigt wird. Für den Use Case wurden ein Smartphone genutzt, ein QR-Code, der das Produkt beschreibt, und eine URL zum Einspeichern der Lokalisierungsdaten des einzulagernden Produkts (aus dem vorherigen Use Case (siehe Abbildung 17)).



Abbildung 17: Komponenten des Use Cases Produktlagerung mit Ortsinformationen

Durch Einscannen des QR-Codes mittels Smartphone erfolgt eine verschlüsselte Verbindung vom Smartphone, welches im 5G Campusnetz eingebucht ist und darüber zur MEC-App

kommuniziert. Das Smartphone erhält von der MEC-App die aktuellen Lokalisierungsinformationen seines Standorts. Der Bezug der Informationen erfolgt über den MEC Service RNIS, der die Informationen über das Admin Interface des 5G Kernnetzes bezieht und an die autorisierte MEC-App weiterleitet, siehe Abbildung 18. Die Lokalisierungsinformation werden dann im Lagerhaltungssystem abgespeichert.

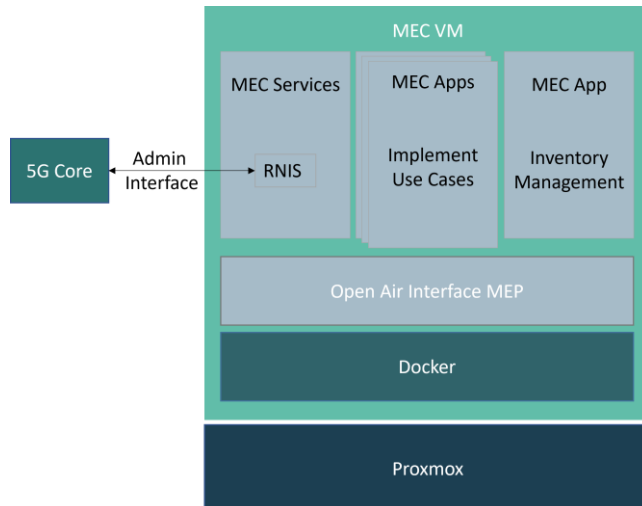


Abbildung 18: Verbindung RNIS MEC-Service und 5G Kernnetz

### 1.6.1.3 Fazit

Die durchgeführten Funktionstests und Resilienztests haben die Praxistauglichkeit der entwickelten Lösungen bestätigt. Die Integration der verschiedenen Komponenten in das IIS-Testbed ermöglichte eine umfassende Validierung der Funktionalität und Interoperabilität.

Die Sicherheitsanalyse zeigte, dass die größte Angriffsfläche im Entwenden der SIM-Karte liegt, was durch gezielte Sicherheitsmaßnahmen adressiert wurde. Die Performancetests lieferten wertvolle Erkenntnisse über die Auswirkungen des Sicherheitsframeworks auf die Anwendungen, insbesondere in Bezug auf Latenz und Schlüsselmanagement.

Die Ergebnisse der Tests bilden eine solide Grundlage für den weiteren Einsatz und die Optimierung der entwickelten Lösungen. Das funktionale Testen der Use Cases zeigte, dass die Umsetzung von Use-Cases mit einer domänenübergreifenden Kommunikation erfolgreich umgesetzt werden konnte, sofern das 5G selbst stabil funktioniert.

## 1.6.2 Use Cases ZIEHL-ABEGG

### 1.6.2.1 MEC App Architektur

Alle drei Use Cases von ZIEHL-ABEGG wurde in einer MEC-App zusammengefasst, welche in der entsprechenden VM auf dem bereits erwähnten Server läuft, der sowohl Zugriff auf das Kernnetz als auch das Usernetz hat. Zentraler Bestandteil der MEC-App ist eine ASP.NET Core REST API, welche die nötigen Schnittstellen zur Datenverarbeitung bereitstellt. Die Datenhaltung erfolgt auf einer SQL-Datenbank, die ebenfalls auf der VM installiert wurde. Den Kern des Backends bilden drei Backgroundjobs, die jeweils pro Use Case die Daten abholen und in die Datenbank schreiben. Der zweite wesentliche Bestandteil ist die Bereitstellung von Endpunkten, über die von anderen Teilnehmern die gesammelten Daten abgerufen werden können. Zur Visualisierung der Daten und Administration der

Autorisierungsrollen wurde ein Frontend in React entwickelt, welches die Methoden der API implementiert.

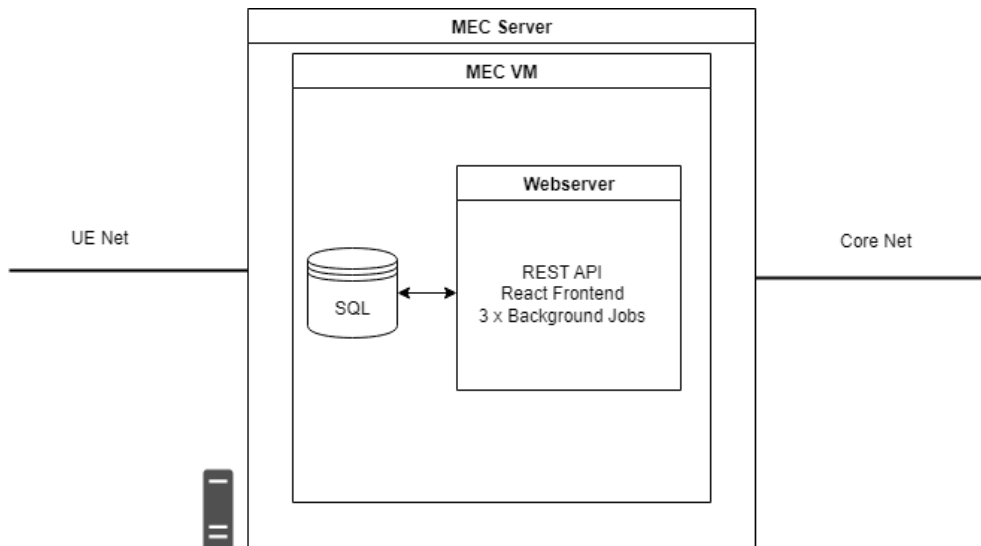


Abbildung 19: MEC-App Architektur

### 1.6.2.2 MEC App Authentifizierung und Autorisierung

Zur Erstellung der PKI wurde zuerst auf der OpenSSL CA, welche Teil der CE ist, eine Root Zertifikat erstellt. Damit wurden dann weitere Zertifikate erstellt bzw. signiert, u.a. für die Konsumenten der MEC-API, sowie für die API selbst. Hier waren unterschiedliche Einstellung zu setzen, da die Zertifikate nicht nur zum Aufbau einer verschlüsselten Verbindung mit TLS, sondern auch zur Client Authentifizierung genutzt wurden. Informationen zum Anwender/Gerät wurden im Common Name (CN) bzw. Subject Alternative Name (SAN) des Zertifikats hinterlegt. Jeder Teilnehmer bzw. Server muss sein entsprechendes Client- bzw. Serverzertifikat und das Root Zertifikat installiert haben. Für die Clientauthentifizierung wird in der API sowohl die Signatur des Zertifikats anhand des Root Zertifikats, sowie weitere Angaben im CN und SAN geprüft.

Zusätzlich zur Authentifizierung wurde ein Rollenkonzept zur Autorisierung implementiert. Hierfür wurden verschiedene Rollen zum Lesen und Schreiben der einzelnen API-Endpunkte angelegt. In der SQL-Datenbank sind diese Rollen den verschiedenen Benutzern der API anhand der Zertifikate zugeordnet. Dieses Konzept lässt sich einfach erweitern und anpassen und bietet eine zusätzliche Sicherheitsschicht im Gegensatz zu dem alternativen Modell, welches die Autorisierungsinformationen direkt im Zertifikat hinterlegt, da bei einer Kompromittierung des Zertifikats keine zusätzliche Prüfung auf Server bzw. Datenbankebene erfolgen würde. Die Rollenzuordnungen können über das UI der MEC-App mit entsprechenden Rechten gepflegt werden.

Die Sicherheit der Authentifizierung und Autorisierung wurde ausgiebig getestet und bestätigt.

MEC API User							
ID	Common Name	Display Name	Description	Cert Valid From	Cert Valid To	Is Active	
1	DEKUN-SFT044086	Christoph Rauh	Rechner von Christoph Rauh	26.6.2025	21.6.2025	<input checked="" type="checkbox"/>	
2	DEKUN-PF3SK8L4	Uwe Richter	Rechner von Uwe Richter	2.7.2025	27.6.2025	<input checked="" type="checkbox"/>	
3	INPRO-RASPB14	INPRO-RASPB14	INPRO-RASPB14 mit IP 10.13.103.4	26.6.2025	21.6.2025	<input checked="" type="checkbox"/>	

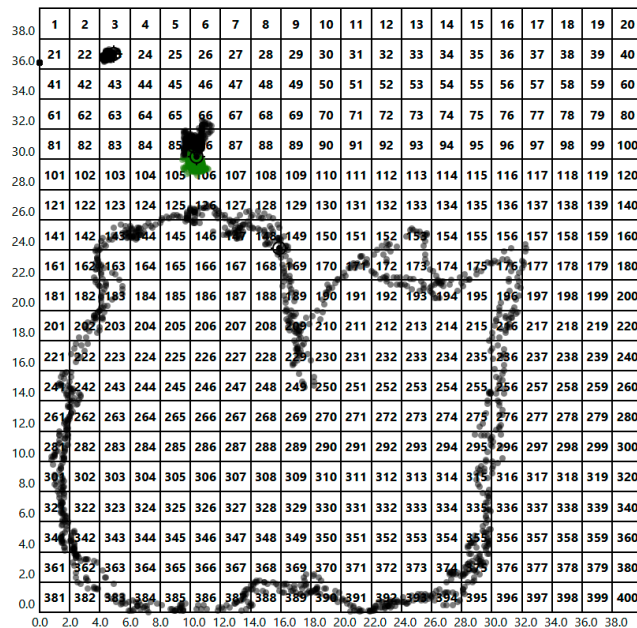
  

MEC API Roles					
RoleId	UserRoleId	Name	Description	Is Active	
3	32	ReadVentData	Rolle zum Lesen der MEC API Ventilatorenendpunkte	<input checked="" type="checkbox"/>	
4	29	ReadPosData	Rolle zum Lesen der MEC API Lokalisierungsendpunkte	<input checked="" type="checkbox"/>	
5	33	ReadCMTKData	Rolle zum Lesen der MEC API CMTKendpunkte	<input checked="" type="checkbox"/>	
6	34	ReadUserData	Rolle zum Lesen der MEC API User- und Rollenendpunkte	<input checked="" type="checkbox"/>	
7		WriteUserData	Rolle zum Bearbeiten der MEC API User- und Rollenendpunkte	<input type="checkbox"/>	

Abbildung 20: Autorisierung MEC-App

### 1.6.2.3 Umsetzung und Test: Lokalisierung von 5G Teilnehmern

Für die Lokalisierung wurde auf eine API von ASOCS, dem Radio Unit Hersteller bei ZIEHL-ABEGG zurückgegriffen und für unsere Zwecke angepasst. Aus der MEC-App werden die Lokalisierungsinformationen periodisch abgerufen und mit Daten angereichert in der SQL-Datenbank gespeichert. Im Frontend der MEC-Applikation wurde eine Darstellung entwickelt, die den Lokalisierungsbereich in ein flexibles Raster einteilt, um so zukünftige Automatisieren, wie etwa Lagerbuchungen simulieren zu können. Im Raster werden die verschiedenen Positionen der Teilnehmer, sowie ihre bisherigen Laufwege zur Laufzeit angezeigt. Durch umfangreiche Tests hat sich gezeigt, dass die Genauigkeit der Lokalisierung zurzeit bei ca. 1 Meter liegt.



**Settings**

Sektoren X Achse: 20    Sektoren Y Achse: 20    Intervall [ms]: 250    Modus: ZA 5G Campus

---

**Letzte Positionsmeldung**

16:40:03 UE 10.13.103.4 (X:10.23, Y:30.86) UE 10.13.103.5 (X:4.90, Y:37.00) UE 10.13.103.1 (X:10.39, Y:30.19) UE 10.13.103.16 (X:15.90, Y:24.10)

Aktuelle Session hat 1235 Einträge

---

**Protokoll**

- 16:40:03: UE 10.13.103.16 betritt Sektor 148
- 16:40:03: UE 10.13.103.1 betritt Sektor 86, UE 10.13.103.16 betritt Sektor 168
- 16:40:02: UE 10.13.103.1 betritt Sektor 85, UE 10.13.103.16 betritt Sektor 149
- 16:40:02: UE 10.13.103.1 betritt Sektor 86
- 16:40:01: UE 10.13.103.1 betritt Sektor 106
- 16:40:01: UE 10.13.103.1 betritt Sektor 86
- 16:39:59: UE 10.13.103.16 betritt Sektor 148
- 16:39:57: UE 10.13.103.1 betritt Sektor 106
- 16:39:57: UE 10.13.103.1 betritt Sektor 86
- 16:39:56: UE 10.13.103.16 betritt Sektor 147
- 16:39:56: UE 10.13.103.1 betritt Sektor 106
- 16:39:55: UE 10.13.103.1 betritt Sektor 86, UE 10.13.103.16 betritt Sektor 146
- 16:39:55: UE 10.13.103.16 betritt Sektor 145
- 16:39:54: UE 10.13.103.16 betritt Sektor 125

Abbildung 21: Lokalisierung von 5G Teilnehmern – UI der MEC-App

### 1.6.2.4 Umsetzung und Test: Condition Monitoring

Für die Umsetzung dieses Use Cases kam das CMTK (Condition Monitoring Toolkit) von BALLUFF zum Einsatz, ein Prototyp, der diverse Soft- und Hardwareschnittstellen bietet, sowie ein integriertes 5G Modem enthält. Über die vorhandenen IO-Link Anschlüsse gelingt die Verbindung zu OT-Geräten, wie z.B. in unserem Fall Temperatur- und Vibrationssensoren. Teil des CMTK ist weiterhin ein Linux basiertes System, über welches weitere Einstellungen, wie z.B. die Datenübertragung gesteuert werden kann. Bei der Implementierung haben wir uns hier aus Performancegründen für MQTT als Übertragungsprotokoll entschieden. D.h. zusammengefasst werden Sensordaten, welche aus den am CMTK angeschlossenen Sensoren stammen über MQTT und 5G an die API übertragen, wobei das CMTK als MQTT-Broker und die API als MQTT-Client agiert. Die API wiederum speichert die eingehenden Daten in der SQL-Datenbank und bietet REST-Methoden, um diese Daten anderen Konsumenten über HTTPS und 5G zur Verfügung zu stellen. Im UI der MEC-App findet man eine Visualisierung der Daten des ausgewählten MQTT-Topics.

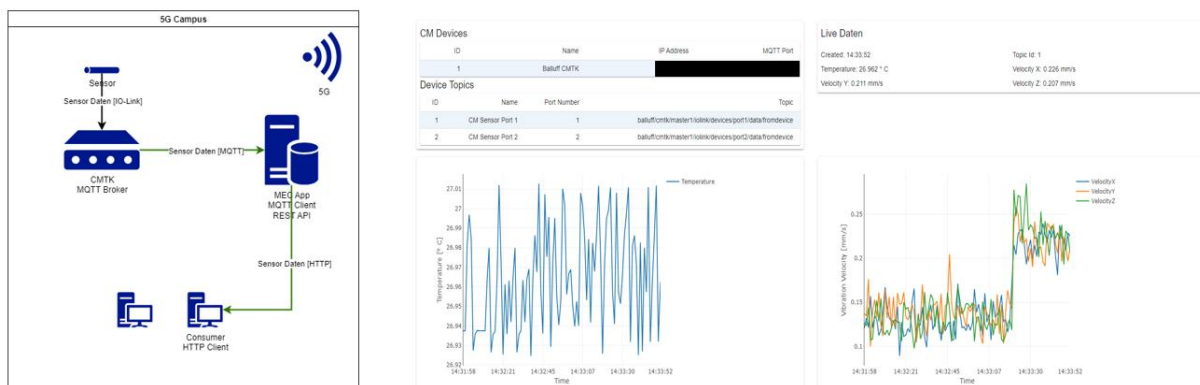


Abbildung 22: Condition Monitoring - Architektur und UI der MEC-App

### 1.6.2.5 Umsetzung und Test: 5G Retrofitting

Da aktuell 5G Modems noch nicht klein bzw. kostengünstig genug sind, um sie direkt in einem Ventilator zu verbauen, aber der Use Case viel Potential bietet, wurde beschlossen, einen Ventilator mittels Retrofitting 5G-fähig zu machen. Dazu wurde dieser über bestehende Modbus-Schnittstellen mit einem PC verbunden. Der PC wiederum wurde über eine 5G-Modem in das Campusnetz integriert und kommuniziert mit der API. Dafür wurde ein HTTP-Server entwickelt, der auf dem PC läuft und ebenfalls mit eigenen Zertifikaten für die Clientauthentifizierung, abgeleitet aus dem Root-Zertifikat, ausgestattet wurde. So kann die API, mit dem korrekten Client Zertifikat regelmäßig Telemetriedaten von dem PC bzw. dem Ventilator abrufen und diese dann wie bei den anderen Use Cases strukturiert in der Datenbank speichern und über eigene Endpunkte anderen Teilnehmern zur Verfügung stellen. Im UI befindet sich wieder eine Übersicht der angeschlossenen Ventilatoren und eine Visualisierung der Daten.

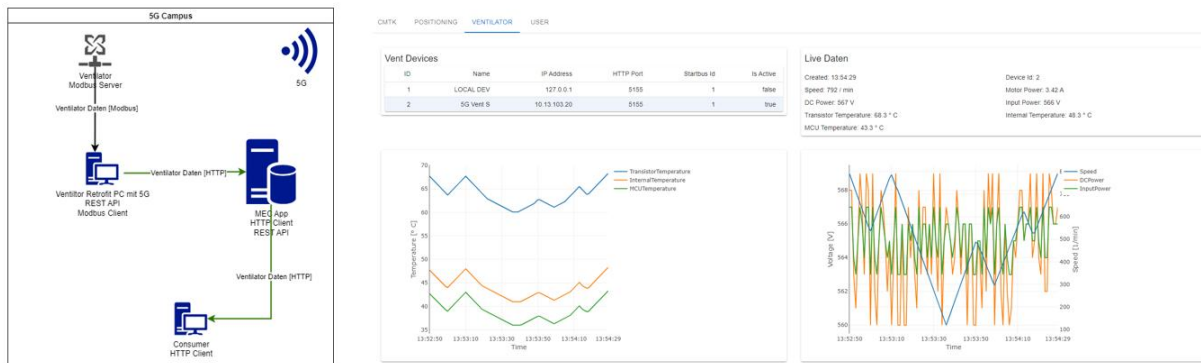


Abbildung 23: 5G Retrofitting - Architektur und UI der MEC-App

## 1.7 Arbeitspaket AP8: Dissemination und Dokumentation

Die Dissemination und Dokumentation spielten eine zentrale Rolle im Projekt, um die Ergebnisse strukturiert festzuhalten und den Wissenstransfer zwischen den Projektpartnern sowie nach außen zu gewährleisten. Im Rahmen der Projektdurchführung wurden umfangreiche Dokumentationen erstellt, die alle relevanten Aspekte des Projekts abdecken – von der Anforderungserhebung bis hin zu den Testergebnissen und dem Abschlussbericht.

Dokumentation im Rahmen der Projektdurchführung

- Use Case Beschreibung:
  - Für die im Projekt definierten Use Cases wurden detaillierte Beschreibungen erstellt, die die Anforderungen, Ziele und geplanten Umsetzungen der jeweiligen Anwendungsfälle dokumentieren.
- Anforderungserhebung:
  - Die Anforderungen an die verschiedenen Systemkomponenten und Prozesse wurden systematisch erhoben und dokumentiert. Dies bildete die Grundlage für die Entwicklung und Implementierung der Lösungen.
- Systemkonzept und Spezifikationen:
  - Basierend auf den erhobenen Anforderungen wurde ein umfassendes Systemkonzept entwickelt.
  - Die Spezifikationen der einzelnen Komponenten und Schnittstellen wurden detailliert beschrieben, um eine reibungslose Implementierung und Integration zu ermöglichen.
- Testspezifikation und Ergebnisdokumentation:
  - Für die durchgeführten Tests wurden spezifische Testpläne erstellt, die die Testziele, Abläufe und erwarteten Ergebnisse definierten.
  - Die Testergebnisse wurden dokumentiert, um die Funktionalität und Resilienz der entwickelten Lösungen nachzuweisen.
- Quartalsberichte:
  - Im Verlauf des Projekts wurden regelmäßige Quartalsberichte erstellt, die den Fortschritt, Herausforderungen und erreichten Meilensteine dokumentierten. Diese Berichte dienten der internen Abstimmung und der Information der Projektpartner.

- Abschlussbericht:
  - Der Abschlussbericht fasst die Ergebnisse des gesamten Projekts zusammen und dient als zentrale Referenz für die erzielten Fortschritte und Erkenntnisse.

Die umfassende Dokumentation im Rahmen der Projektdurchführung war ein wesentlicher Bestandteil des Projekts. Sie gewährleistete Transparenz, Nachvollziehbarkeit und eine strukturierte Aufbereitung der Ergebnisse. Die erstellten Dokumente – von der Use Case Beschreibung bis hin zum Abschlussbericht – bilden eine solide Grundlage für die Weiterentwicklung der im Projekt erarbeiteten Lösungen und den Wissenstransfer in zukünftige Projekte.

Die Dissemination der Ergebnisse ermöglicht es den Projektpartnern, die gewonnenen Erkenntnisse effektiv zu nutzen und in ihren jeweiligen Anwendungsbereichen weiterzuentwickeln.

Die Dissemination der Projektergebnisse war ein wesentlicher Bestandteil des Vorhabens, um die gewonnenen Erkenntnisse sowohl innerhalb des Projektkonsortiums als auch in der Fachöffentlichkeit zu verbreiten. Im Rahmen des Projekts wurden verschiedene Maßnahmen ergriffen, um die Ergebnisse zu kommunizieren und den Wissenstransfer zu fördern. Eine ausführliche Darstellung erfolgt im Abschnitt „Erfolgte und geplante Veröffentlichungen“.

## 2 Die wichtigsten Positionen des zahlenmäßigen Nachweises

Bei allen drei Projektpartnern entstanden folgende Kosten gemäß des Verwendungsnachweises:

- Personalkosten: Es wurden Mitarbeitende beschäftigt, um die wissenschaftlich-technischen Arbeiten durchzuführen.
- Reisekosten: Für Projekttreffen, die Vorbereitung und Integration des Security Frameworks im Testbed von ZIEHL-ABEGG und Reisen zu Konferenzen und anderen Öffentlichkeits-Aktivitäten wurden Reisekosten benötigt.

Zusätzlich dazu entstanden bei der Hochschule Offenburg folgenden Kosten:

- Verbrauchsmaterial: Für die Umsetzung der wissenschaftlich-technischen Arbeiten wurden TPM-Module, Raspberry Pis mit entsprechendem Zubehör, sowie 5G-Modems beschafft.

## 3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die durchgeführten Arbeiten im Projekt waren notwendig und angemessen. Die formulierten Aufgaben, sowie der Arbeitsplan wurden der Vorhabensbeschreibung entsprechend erfolgreich bearbeitet. Trotz der umfangreichen Arbeiten und des hierfür relativ kurzen Bearbeitungszeitraums wurden an Demonstratoren an zwei Standorten in den 5G Testbeds aufgebaut und es konnte die Funktion der Entwicklungen nachgewiesen und dem Fachpublikum

präsentiert werden. Zudem gab es umfangreiche wissenschaftliche Präsentationen und Veröffentlichungen, sowie Fachvorträge.

## 4 Voraussichtlicher Nutzen und Verwertbarkeit

Die zunehmende Anzahl an Cyberangriffen auf Unternehmen erfordert zusätzliche Absicherung und Härtung der Kommunikationsinfrastruktur der Unternehmen. Auch der Einsatz von digitalen Identitäten im industriellen Umfeld nimmt zu. Daher wird das an den BSI-Grundschutz angelehnte Architekturkonzept mit verschiedenen Anwendungsfällen – einschließlich Campusnetzen – weiter konkretisiert. Dazu gehören zunehmend auch 5G Campusnetze, die in der Produktion zum Einsatz kommen. Der Know-How-Aufbau und die im Projekt entwickelten Konzepte, sowie die entwickelten prototypischen Komponenten und Demonstratoren eröffnen den Projektpartnern weitere Forschungs- und Entwicklungsmöglichkeiten im Umfeld der Absicherung von Campusnetzen für die Produktion aber auch in anderen Einsatzbereichen der 5G Campusnetze wie z.B. in Krankenhäusern.

Mit der Implementierung eines eigenen Campusnetz, sowie der Verwendung der im Projekt entwickelten Sicherheitsarchitektur in der Innovationsfabrik von ZIEHL-ABEGG wurde der erste wichtige Schritt getan, um 5G und die zu berücksichtigenden Sicherheitsaspekte weiter zu evaluieren. Mit den daraus gewonnenen Erkenntnissen kann ZIEHL-ABEGG anschließend diese Technologien ggf. in Teilbereichen anderer Produktionsstätte über Retrofitting implementieren bzw. die hier gewonnen Ergebnisse in die Planung von neuen Werken oder Produktionsanlagen einfließen lassen.

## 5 Fortschritt bei anderen Stellen

Während der Projektdurchführung erfolgte eine ständige Beobachtung der Änderungen hinsichtlich regulatorischer Vorgaben und Empfehlungen (BSI), der 3GPP Standardisierung zu Security in 5G Netzen, sowie Maßnahmen und Standardisierung von Absicherung der OT-Netze z. B. für PROFINET und OPC UA. Im Rahmen der Bedrohungsanalyse sowie während der Konzeptphase wurde insbesondere das „IT-Grundschutz-Profil zur Absicherung von 5G-Campusnetzen im Eigenbetrieb“ des BSI berücksichtigt und aktiv eingebunden.

## 6 Erfolgte und geplante Veröffentlichungen

Das Fraunhofer IIS hat die Arbeiten an verschiedenen Veranstaltungen, Kongressen und Fachgremien vorgestellt

- Präsentation der Projektergebnisse und des Demonstrators auf der IIS-Hausmesse "5G Connect Advanced", Nürnberg, Deutschland, 2024.
- P. Heusinger, A. Oeder, I. Rausch – „PKI in Infrastructures for Industrial Automation-Technology with 5G“, 2024, Wireless Congress, München, Deutschland, 2024.
- Vorstellung der PIA5 Projektergebnisse und des Demonstrators im Rahmen des 5G ACIA Plenums, Nürnberg, Deutschland, 2024.

- A. Oeder, P. Heusinger, „*PKI in Infrastrukturen für die industrielle Automatisierungstechnik mit 5G*“, Vorstellung der PIA5-Ergebnisse auf dem Treffen des Arbeitskreis "Industrielle Sicherheit" des VDMA, Frankfurt am Main, Mai 2025.
- P.Heusinger, A. Oeder, I. Rausch: Vorstellung des Konzeptes im Rahmen eines Vortrags zum Thema „*Security in 5G Campus Networks*“ beim Wireless Congress 2026, München, Deutschland (geplant).

Die Hochschule Offenburg – ivESK-Arbeitsgruppe hat vier wissenschaftliche Beiträge auf IEEE-Konferenzen veröffentlicht, die sich mit dem Einsatz von PKI für OT- und IIoT-Geräte in industriellen Anwendungsfeldern befassen:

- A. Shukla, F. Sowieja, J. S. E and A. Sikora, "*Certificate Based Primary Authentication for 5G Networks*," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 1223-1229, doi: 10.1109/IDAACS58523.2023.10348771.
- J. Göppert and A. Sikora, "*Evaluation of the Secure PROFINET Application Relation Establishment Performance*," 2024 IEEE 22nd International Conference on Industrial Informatics (INDIN), Beijing, China, 2024, pp. 1-6, doi: 10.1109/INDIN58382.2024.10774374.
- J. Göppert and A. Sikora, "*Credential Management for CANopen FD: A Life Cycle Oriented Concept and Implementation*," 2024 IEEE 22nd International Conference on Industrial Informatics (INDIN), Beijing, China, 2024, pp. 1-6, doi: 10.1109/INDIN58382.2024.10774305.
- A. Shubbar, J. Göppert, K. Naik and A. Sikora, "*PKI-Based Security for Industrial Automation Systems Using 5G Campus Networks*," 2025 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Nice, France, 2025, pp. 1-6, doi: 10.1109/MeditCom64437.2025.11104431.

Präsentation der Umsetzung und Ergebnisse in Fachgremien:

- Vorstellung in relevanten Organisationen wie der PROFIBUS/PROFINET Nutzerorganisation (PNO) und CAN in Automation (CiA), einschließlich einer Präsentation am **8. Oktober 2024** im Rahmen des **CiA IG06 SIG02 HLP Cybersecurity Meetings**.

## 7 Literaturverzeichnis

- [1] Microsoft (2002): STRIDE Threat Model. Microsoft Security Development Lifecycle (SDL). Online verfügbar unter <https://learn.microsoft.com/de-de/azure/security/develop/threat-modeling-tool-threats>, zuletzt geprüft am 01.04.2025.
- [2] BSI (2023): IT-Grundschutz-Bausteine (Edition 2023). Online verfügbar unter [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine\\_Download\\_Edition\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html), zuletzt geprüft am 05.09.2024.
- [3] BSI (2023): Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102-1). Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?\\_\\_blob=publicationFile&v=13](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=13), zuletzt geprüft am 10.10.2024.
- [4] BSI (2023): X.509: X.509 Zertifikate und Zertifizierungspfadvalidierung (BSI TR-02103). Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02103/BSI-TR-02103.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02103/BSI-TR-02103.pdf?__blob=publicationFile&v=2), zuletzt geprüft am 10.10.2024.
- [5] BSI (2024): IT-Grundschutz-Profil zur Absicherung von 5G-Campusnetzen im Eigenbetrieb. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/5G-Campusnetze/IT-GS-Profil\\_5G\\_Campusnetze\\_im\\_Eigenbetrieb.pdf?\\_\\_blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/5G-Campusnetze/IT-GS-Profil_5G_Campusnetze_im_Eigenbetrieb.pdf?__blob=publicationFile&v=5), zuletzt geprüft am 02.04.2025.
- [6] IEEE (2018): IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity (IEEE 802.1AR-2018). Institute of Electrical and Electronics Engineers. Online verfügbar unter [https://standards.ieee.org/standard/802\\_1AR-2018.html](https://standards.ieee.org/standard/802_1AR-2018.html), zuletzt geprüft am 17.10.2024
- [7] Internet Engineering Task Force (IETF) (2008): RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Online verfügbar unter <https://datatracker.ietf.org/doc/html/rfc5280>, zuletzt geprüft am 17.10.2024.
- [8] ETSI (2023): TS 123.5023 - Procedures for the 5G System (5GS), Version 18.3.0. European Telecommunications Standards Institute. Online verfügbar unter [https://www.etsi.org/deliver/etsi\\_ts/123500\\_123599/123502/18.05.00\\_60/ts\\_123502v180500p.pdf](https://www.etsi.org/deliver/etsi_ts/123500_123599/123502/18.05.00_60/ts_123502v180500p.pdf), zuletzt geprüft am 02.04.2025.
- [9] BSI (2023): IT-Grundschutz-Baustein SYS.1.5 Virtualisierung. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium\\_Einzel\\_PDFs\\_2023/07\\_SYS\\_IT\\_Systeme/SYS\\_1\\_5\\_Virtualisierung\\_Edition\\_2023.pdf?\\_\\_blob=publicationFile&v=3#download=1](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/07_SYS_IT_Systeme/SYS_1_5_Virtualisierung_Edition_2023.pdf?__blob=publicationFile&v=3#download=1), zuletzt geprüft am 02.04.2025.

- [10] BSI (2023): IT-Grundschutz-Baustein SYS.1.6 Containerisierung. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar [https://www.bsi.bund.de/Shared-Docs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium\\_Einzel\\_PDFs\\_2022/07\\_SYS\\_IT\\_Systeme/SYS\\_1\\_6\\_Containerisierung\\_Edition\\_2022.pdf?\\_\\_blob=publicationFile&v=3](https://www.bsi.bund.de/Shared-Docs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/07_SYS_IT_Systeme/SYS_1_6_Containerisierung_Edition_2022.pdf?__blob=publicationFile&v=3), zuletzt geprüft am 02.04.2025
- [11] Quectel (o. J.): 5G RMU500 EVB Kit. Online verfügbar unter <https://www.quectel.com/product/5g-rmu500-evb-kit/>
- [12] Druidsoft (o. J.): 5G Core Übersicht. Online verfügbar unter <https://druidsoftware.com/raemis-cellular-network-technology/>