Bundesanstalt
für den Digitalfunk der Behörden und
Organisationen mit Sicherheitsaufgaben

# Schlussbericht zum Teilvorhaben

Highspeed Anbindung mobiler Leitstellen mit LEO-Satelliten und 5G (HiLeit) - Sichere und Robuste Zugangsknoten

Hochschule Bonn-Rhein-Sieg
16BEC0041
01.10.2024 - 31.07.2026

Gefördert durch:

Bundesministerium
des Innern

aufgrund eines Beschlusses
des Deutschen Bundestages

**Inhaltsverzeichnis**


| | | |
|---|---|---|
| **I.** | **Kurzdarstellung** | 3 |
| | **1. Problemstellung** | 3 |
| | **2. Voraussetzungen, unter denen das Vorhaben durchgeführt wurde** | 3 |
| | **3. Planung und Ablauf des Vorhabens** | 4 |
| | **4. Wissenschaftlicher und technischer Stand** | 4 |
| | **5. Kurzdarstellung der wichtigsten Vorhabenergebnisse** | 4 |
| | **6. Nutzen und zukünftige Anwendungsmöglichkeiten der Vorhabenergebnisse** | 5 |
| **II.** | **Eingehende Darstellung** | 6 |
| | **1. Erzielte Ergebnisse im Einzelnen** | 6 |
| | **1.1 AP1.2 - Dissemination, Transfer von Know-How** | 6 |
| | **1.2 AP2.2 - Evaluierungsszenarien für Demonstrator** | 6 |
| | **1.3 AP3.1 - Sicherheitskonzept** | 7 |
| | **1.4 AP3.2 - Zugang und Backhaul** | 8 |
| | **1.5 AP4.1 - Sicherheit und Vertraulichkeit** | 8 |
| | **1.6 AP4.2 - Einbindung** | 9 |
| | **1.7 AP4.3 - Parametrisierung** | 10 |
| | **1.8 AP5.2 - Multi-Gateway / Load-Balancing / Failover** | 11 |
| | **1.9 AP5.3 - Föderation und Kommunikationssicherheit** | 11 |
| | **1.10 AP6 - Feldtest, Evaluation, Bewertung** | 11 |
| | **2. Beitrag zu den Zielen der Fördermaßnahme, voraussichtlicher Nutzen und Verwertbarkeit** | 13 |
| | **2.1 Wirtschaftliche Erfolgsaussichten nach Vorhabenende** | 14 |
| | **2.2 Wissenschaftliche und/oder technische Erfolgsaussichten nach Vorhabenende** | 15 |
| | **2.3 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit** | 15 |
| **III.** | **Anlagen** | 16 |
| | **1. Wichtige Positionen des zahlenmäßigen Nachweises** | 16 |
| | **2. Zusammenarbeit und Projektmanagement** | 16 |
| | **2.1 Zusammenarbeit mit dem Konsortium** | 16 |
| | **2.2 Zusammenarbeit mit der BDBOS und VDI/VDE** | 17 |
| | **3. Übersicht der Maßnahmen der Öffentlichkeitsarbeit** | 18 |
| | **4. Übersicht der Schutzrechtsanmeldungen** | 18 |

# I. Kurzdarstellung

## 1. Problemstellung

Bei Großschadenslagen, wie dem Hochwasser an Ahr und Erft im Jahr 2021, versagen reguläre Kommunikationsinfrastrukturen regelmäßig: Mobilfunkmasten fallen aus, Festnetzverbindungen werden physisch zerstört, und der TETRA-Digitalfunk bietet aufgrund seiner begrenzten Bandbreite keinen vollwertigen Ersatz für breitbandige Datenkommunikation. Für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) ergibt sich daraus eine kritische Lücke: Einsatzkräfte sind auf breitbandige Datenkommunikation angewiesen, um Führungssoftware zu betreiben, Lagebilder zu übertragen, Telemedizin zu nutzen und die Einsatzkoordination sicherzustellen. Das Forschungsvorhaben HiLeit (Highspeed Anbindung mobiler Leitstellen mit LEO-Satelliten und 5G) adressiert diese Problematik durch die Entwicklung einer autarken, ausfallsicheren Breitband-Kommunikationsinfrastruktur.

Das Teilvorhaben der Hochschule Bonn-Rhein-Sieg (H-BRS) verantwortete dabei zwei zentrale Schwerpunkte: die Entwicklung eines durchgängigen Sicherheitskonzepts für die heterogene HiLeit-Infrastruktur sowie die Konzeption und prototypische Implementierung neuartiger, sicherer Funkzugangsknoten. Diese Zugangsknoten ermöglichen BOS-Einsatzkräften und der Bevölkerung einen sicheren, automatisierten und benutzerfreundlichen Netzzugang auf handelsüblichen Endgeräten (COTS) ohne Modifikationen der Gerätesoftware sowie die Integration moderner und zukunftssicherer kryptographischer Verfahren.

## 2. Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Das Verbundvorhaben HiLeit wurde von einem Konsortium aus vier Partnern bearbeitet:

- Fraunhofer FIT, Sankt Augustin (Koordinator)
- Hochschule Bonn-Rhein-Sieg (H-BRS), Sankt Augustin
- Malteser Hilfsdienste e.V., Köln
- DeFuTech UG, Bonn

An der H-BRS wurden die Arbeiten am Institut für Sicherheitsforschung (ISF) unter Leitung von Prof. Dr. Michael Rademacher durchgeführt. Das Vorhaben profitierte von substanziellen Vorarbeiten der Forschungsgruppe zu Sicherheit und Skalierbarkeit von WLAN- und 5G-Netzen sowie zu drahtloser Kommunikation in kritischen Infrastrukturen, insbesondere aus den abgeschlossenen Projekten „5G Opportunity" und „PlusMoSmart".

Der Förderzeitraum wurde kostenneutral um vier Monate bis zum 31.07.2026 verlängert. Grund dafür war die Bindung der technischen Malteser-Kräfte durch die Planung und Betreuung des Katholikentages 2026 in Würzburg bis Ende Mai, wodurch der Feldversuch in den Juni verschoben und der Juli für die Ergebnisauswertung genutzt wurde. Darüber hinaus hatte ein rückwirkend definierter Projektstart im

Förderbescheid zu einem verzögerten Beginn der personalintensiven Arbeiten geführt, der durch die Verlängerung vollständig aufgefangen werden konnte.

## 3. Planung und Ablauf des Vorhabens

Das Teilvorhaben der H-BRS umfasste elf Arbeitspakete bzw. Unterarbeitspakete, die von der Anforderungsanalyse über Konzeption und Implementierung bis zu Demonstration und Evaluierung reichten. Tabelle 1 gibt einen Überblick.

**Tabelle 1** Übersicht der Arbeitspakte

| Arbeitspakte (AP) | Name | Leitung | AP vollständig abgeschlossen |
|---|---|---|---|
| AP 1 | Projektmanagement und Dissemination | Fraunhofer FIT | Ja |
| AP 2 | Anforderungsanalyse | Malteser | Ja |
| AP 3 | Definition der Gesamtarchitektur | H-BRS | Ja |
| AP 4 | Entwicklung der Zugangsknoten | H-BRS | Ja |
| AP 5 | Entwicklung des Backhaulnetzes | Fraunhofer FIT | Ja |
| AP 6 | Feldtest, Evaluation, Bewertung | Malteser | Ja |

Gegenüber der ursprünglichen Planung wurde der geplante Workshop mit BOS-Anwendern an der Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung (BABZ) als Präsenzveranstaltung mit BOS-Akteuren in Aalen (Ostalbkreis) durchgeführt, was einen höheren Praxisbezug und unmittelbareres Feedback der Anwender ermöglichte. Im Bereich der SIM-Provisionierung wurde nach eingehender Analyse der eSIM-Technologie die Entscheidung getroffen, im Demonstrator auf physische SIM-Karten zu setzen. Dies stellt keine Einschränkung der Zielerreichung dar, sondern eine technische Entscheidung zugunsten von Zuverlässigkeit und Praxistauglichkeit.

## 4. Wissenschaftlicher und technischer Stand

Die H-BRS verfügte zu Projektbeginn über belastbare Vorarbeiten im Bereich der 5G-Sicherheit. Veröffentlichte Analysen zu Sicherheitsschwachstellen in 5G-NSA-Netzen belegten, dass bekannte 4G-Angriffe auf 5G-NSA-Deployments übertragbar sind und dass sich die wesentlichen Sicherheitsverbesserungen von 5G auf Standalone-Architekturen konzentrieren. Ergänzend lagen Erfahrungen mit dem Betrieb von 5G-Campusnetzen auf Open-Source-Basis (Open5GS, srsRAN) sowie Untersuchungen zur Skalierbarkeit von TLS-Verbindungen über ressourcenbeschränkte Protokolle vor.

## 5. Kurzdarstellung der wichtigsten Vorhabenergebnisse

Die H-BRS erarbeitete im Projektverlauf zwei zentrale Konzeptdokumente sowie mehrere technische Implementierungen für den gemeinsamen Demonstrator.

Das **Sicherheitskonzept** analysiert die gesamte HiLeit-Netzwerkinfrastruktur hinsichtlich Bedrohungen und definiert konkrete Schutzmaßnahmen. Kernelemente sind ein Post-Quanten-kryptographisch gesichertes VPN auf Basis von WireGuard und Rosenpass sowie ein physisches PQC-VPN-Gateway, das Netzwerkgeräte nach dem Plug-and-Play-Prinzip in verschlüsselte Tunnel einbindet. Das hybride Kryptographiemodell schützt gegen das "Harvest now, decrypt later"-Paradigma (HNDL).

Das **Zugangskonzept** beschreibt, wie BOS-Kräfte und Bevölkerung sicher und mit minimaler Einstiegshürde in das Einsatznetz eingebunden werden. Kernstück ist die SIM-basierte automatische Authentifizierung via Hotspot 2.0 (Passpoint, IEEE 802.11u) mit EAP-SIM und EAP-AKA, die dieselben SIM-Credentials für 5G-Campusnetz und WLAN verwendet. Für den Bevölkerungszugang wurde ein OWE-gesichertes Segment mit strikter Netztrennung konzipiert.

Eine umfassende **eSIM-Analyse** untersuchte die praktischen Hürden der eSIM-Provisionierung für private Campusnetze und leitete eine begründete Entscheidung zugunsten physischer SIM-Karten für den Projektbetrieb ab. Im Rahmen von AP6 wurde ein vollständig integrierter Demonstrator auf dem Flugplatz Schönhagen in Trebbin, Brandenburg, erfolgreich unter realistischen Feldbedingungen validiert. Der anschließende Feldversuch im Ostalbkreis erprobte die entwickelten Komponenten in realen BOS-Einsatzszenarien.

## 6. Nutzen und zukünftige Anwendungsmöglichkeiten der Vorhabenergebnisse

Die erarbeiteten Konzepte und Implementierungen adressieren einen konkreten Bedarf von BOS-Organisationen in Deutschland. Das PQC-VPN-Gateway und die Hotspot-2.0-Lösung zur automatischen SIM-basierten Authentifizierung sind direkt auf andere BOS-Kommunikationsplattformen übertragbar. Die konsequente Open-Source-Umsetzung gewährleistet Auditierbarkeit, Herstellerunabhängigkeit und langfristige Wartbarkeit. Die Projektergebnisse können als Grundlage für die zunehmende Digitalisierung der BOS-Kommunikation in Deutschland dienen. Die dokumentierten Erkenntnisse zur eSIM-Problematik und zur Post-Quanten-Kryptographie in ressourcenbeschränkten Einsatzumgebungen sind darüber hinaus für die internationale Forschungsgemeinschaft relevant. Die H-BRS plant, die Ergebnisse in Folgeprojekte einzubringen und dauerhaft in Lehrveranstaltungen zu integrieren.

# II. Eingehende Darstellung

## 1. Erzielte Ergebnisse im Einzelnen

In den folgenden Abschnitten werden die erreichten Ergebnisse der einzelnen Arbeitspakete (AP) unter Berücksichtigung der vorgegebenen Ziele aus der Teilvorhabenbeschreibung erläutert. Zu beschreiben sind die wesentlichen Arbeitsschritte in Zusammenarbeit mit den Konsortialpartnern bzw. weiterer beteiligter Personen und Organisationen. Ggf. ist auf Teilnahme an Veranstaltungen hinzuweisen.

### 1.1 AP1.2 - Dissemination, Transfer von Know-How

Die H-BRS beteiligte sich aktiv an der Dissemination der Projektergebnisse und der Vernetzung mit der einschlägigen Fachgemeinschaft. Im Jahr 2024 wurden die PMR Expo sowie das 1. Innovationsforum der BDBOS besucht. Im Jahr 2025 folgten ein Projektworkshop des HiLeit-Konsortiums, ein öffentlicher Workshop in Kooperation mit dem BMDV-Projekt 5G-Opportunity und verschiedenen BOS-Akteuren, die KoPa_45-Roadshow sowie erneut die PMR Expo. Die Mobilkommtagung 2025 in Osnabrück ermöglichte Vernetzung und Wissensaustausch mit der deutschen Fachgemeinschaft im Bereich Mobilkommunikation. Im Rahmen des 2. Innovationsforums der BDBOS im Jahre 2026 wurde der HiLeit-Demonstrator einem Fachpublikum aus Forschung, Fördergebern und BOS-Praxis
vorgestellt.

Die Projektergebnisse flossen kontinuierlich in Lehrveranstaltungen der Bachelor- und Masterstudiengänge der H-BRS ein. Eine Masterarbeit zum Thema 5G Network Slicing wurde im Projektkontext ausgegeben und betreut.

### 1.2 AP2.2 - Evaluierungsszenarien für Demonstrator

In enger Abstimmung mit den Projektpartnern wurden konkrete Evaluierungsszenarien für den Demonstrator und den Feldversuch im Ostalbkreis erarbeitet. Die H-BRS beteiligte sich an der Definition von vier Erprobungsszenarien:

- **Szenario A** (Stromausfall / Bevölkerungsinformation): Aufbau eines Netzes zur Bevölkerungsinformation mit bandbreitenbegrenztem Internetzugang im Leuchtturm-Betrieb.
- **Szenario B** (Stromausfall / Kräftenetz und Bevölkerung): Parallelbetrieb eines gesicherten BOS-Datennetzwerks und eines Bevölkerungs-WLANs mit strikter Netztrennung.
- **Szenario C** (Dienststellenvernetzung): Anbindung öffentlicher Verwaltungsdienststellen über LEO-Satellit und WiBACK.
- **Szenario D** (Einsatzgebiet-Ausleuchtung): Flächendeckende Kommunikationsversorgung für Einsatzkräfte von einem erhöhten Standpunkt aus.

Aus diesen Szenarien wurden, gemeinsam mit den Projektpartnern, KPIs für die spätere Evaluation abgeleitet. Die sicherheitsrelevanten Anforderungen der Szenarien flossen unmittelbar in AP3.1 (Sicherheitskonzept) und AP3.2 (Zugangskonzept) ein.

## 1.3 AP3.1 - Sicherheitskonzept

Das Sicherheitskonzept bildet das kryptographische und architektonische Rückgrat der HiLeit-Infrastruktur. Die H-BRS erarbeitete ein umfassendes Dokument, das bewusst die gesamte Netzwerkinfrastruktur betrachtet und nicht auf Zugangsnetzwerke beschränkt ist.

**Bedrohungsanalyse:** Drei Angreiferkategorien wurden identifiziert und nach Kritikalität bewertet: opportunistische Angreifer mit physischem Zugriff auf ungesicherte Außenknoten, gezielte staatliche und kriminell-organisierte Akteure sowie Insider-Bedrohungen durch z.B. Fehlkonfigurationen unter Stressbedingungen. Für 5G-NSA-Deployments wurden IMSI-Catcher- und False-Base-Station-Angriffe als besonders kritisch eingestuft, gestützt auf eigene Vorarbeiten der H-BRS. Das HNDL-Paradigma wurde als Langzeitbedrohung für alle aufgezeichneten VPN-Verbindungen eingeordnet und begründet die Post-Quanten-Erweiterung des VPN-Konzepts.

**VPN-Konzept:** WireGuard wurde als primäres VPN-Protokoll ausgewählt. Ausschlaggebend waren seine minimale Codebasis, ein formal verifiziertes kryptographisches Design, die native Linux-Kernel-Integration sowie der 1-RTT-Handshake, der auch bei LEO-Satellitenlatenzen performant arbeitet. Zur Absicherung gegen zukünftige Quantencomputerangriffe wurde WireGuard durch Rosenpass erweitert, das parallel einen post-quanten-kryptographischen Schlüsselaustausch durchführt. Dabei kommen ML-KEM-768 (CRYSTALS-Kyber, NIST FIPS 203) als ephemerer Key Encapsulation Mechanism sowie Classic McEliece für statische Langzeitschlüssel zum Einsatz. Das kombinierte Sitzungsgeheimnis wird als Pre-Shared Key in den WireGuard-PSK-Slot eingespeist und liefert Defense-in-Depth: Ein Angreifer müsste beide kryptographischen Schichten brechen, um Verbindungen zu kompromittieren.

**PQC-VPN-Gateway:** Im Rahmen des Projekts wurde ein physisches PQC-VPN-Gateway entwickelt, das beliebige Netzwerkgeräte nach dem Plug-and-Play-Prinzip in einen kryptographisch gesicherten Tunnel einbindet, ohne gerätespezifische VPN-Konfiguration zu erfordern. Post-Quanten-Sicherheit wird damit auch ohne vertiefte IT-Kenntnisse der Einsatzkräfte erreichbar.

**Netzarchitektur und Segmentierung:** Die Segmentierung erfolgt über separate WireGuard-Interfaces je Sicherheitszone (BOS-Daten, Telemedizin, Administration, Behördennetze), die durch Policy-Routing vor unberechtigtem Kreuzverkehr geschützt sind. Das Bevölkerungssegment wird als separates VLAN direkt zum Internet-Gateway geroutet und niemals mit dem verschlüsselten Overlay verbunden.

**Weitere Sicherheitsaspekte:** Das Konzept umfasst Festplattenverschlüsselung mit dm-crypt/LUKS2 und TPM-Sealing, dateibasierte Verschlüsselung mit fscrypt für besonders sensible Daten (Patientendaten, Behördendokumente) sowie verschlüsselte Datensicherung mit age. Netzwerkbasierte Intrusion Detec-

tion mit Suricata und strikte nftables-Firewallregeln mit Default-Deny-Policy vervollständigen das Gesamtkonzept. Die gesamte Umsetzung basiert auf auditierter Open-Source-Software, was Transparenz, Herstellerunabhängigkeit und Offline-Betrieb ohne Lizenzabhängigkeiten gewährleistet.

## 1.4 AP3.2 - Zugang und Backhaul

Die H-BRS erarbeitete ein umfassendes Zugangskonzept für mobile und ad-hoc aufgebaute BOS-Kommunikationsnetze, das gleichermaßen Einsatzkräfte und die versorgte Bevölkerung adressiert.

**5G-Campusnetz:** Die Einsatzmöglichkeiten nomadischer 5G-Campusnetze auf Basis von Open5GS und srsRAN wurden analysiert. Als wesentliche regulatorische Hürde wurde die ortsgebundene Frequenzzuteilung der Bundesnetzagentur im Campusnetz-Band (3,7 bis 3,8 GHz) identifiziert. Lösungsansätze wie Spectrum Sensing und regulatorische Sonderlösungen für BOS wurden als Handlungsoptionen ausgearbeitet und als Empfehlungen für Folgemaßnahmen dokumentiert.

**WiFi 6E und WiFi 7:** Das 6-GHz-Band wurde als besonders vorteilhaft für Katastrophenschutzeinsätze bewertet, da es in Schadensgebieten erheblich weniger belegt ist als konventionelle WLAN-Frequenzbänder. WiFi 7 mit Multi-Link-Operation und QoS ermöglicht die Reservierung von Bandbreiten für einsatzkritische Anwendungen und damit die Priorisierung von BOS-Kommunikation gegenüber dem Bevölkerungssegment.

**Hotspot 2.0:** Das Konzept für die automatische SIM-basierte WLAN-Authentifizierung via Hotspot 2.0 (Passpoint, IEEE 802.11u) wurde ausgearbeitet. Das Verfahren nutzt ANQP-Anfragen (Access Network Query Protocol) für die automatische Netzwerkerkennung und verbindet sich bei passendem Profil ohne Nutzerinteraktion. Die Integration mit EAP-AKA ermöglicht die Nutzung derselben SIM-Karte für 5G und WLAN, sodass ein nahtloser Wechsel zwischen beiden Zugangstechnologien ohne separates Credential-Management möglich ist.

**Netztrennung und Bevölkerungszugang:** Ein Konzept zur strikten Trennung zwischen BOS-Netz und öffentlichem Segment wurde auf Basis von VLAN-Segmentierung, Default-Deny-Firewallregeln und Opportunistic Wireless Encryption (OWE) für den Bevölkerungszugang ausgearbeitet. Für einen besonders niedrigschwelligen Bevölkerungszugang wurden zusätzlich eSIM-Profile als QR-Code-Option konzipiert.

## 1.5 AP4.1 - Sicherheit und Vertraulichkeit

In AP4.1 wurden Authentifizierungs- und Verschlüsselungsmechanismen für 5G und WLAN evaluiert.

**5G-Authentifizierung:** Die von dem 3GPP spezifizierten Verfahren 5G-AKA sowie EAP-AKA' für den Zugang über Nicht-3GPP-Netze wurden untersucht. 5G Standalone bietet gegenüber 4G wesentliche Sicherheitsverbesserungen: Der Schutz der permanenten Teilnehmeridentität durch SUPI/SUCI sowie die

obligatorische gegenseitige Authentifizierung zwischen Endgerät und Netz wurden als zentrale Sicherheitsmerkmale für den BOS-Einsatz bewertet.

**WLAN-Authentifizierung:** In dem von der H-BRS entwickelten Zugangskonzept wurde EAP-AKA als bevorzugtes Verfahren für BOS-Einsatzkräfte identifiziert, da es die vorhandene SIM-Infrastruktur nutzt und kein separates Credential-Management erfordert. EAP-TLS wurde als robuste Alternative für Geräte ohne SIM-Karte (Notebooks, Tablets, IoT-Geräte) festgelegt.

**eSIM-Analyse:** Die Möglichkeiten der eSIM-Provisionierung für private 5G-Campusnetze wurden umfassend analysiert. Dabei wurden drei Optionen bewertet: GSMA-zertifizierte SM-DP+-Infrastruktur (Erstzertifizierungskosten im fünfstelligen Bereich, für nichtkommerzielle BOS-Einsatznetze unpraktikabel), SGP.26-Testzertifikate (veröffentlichtes Schlüsselmaterial, für Produktivbetrieb ungeeignet) sowie spezialisierte Drittanbieter wie sysmocom und Amarisoft (Live-Zertifikate mit Schlüsselmaterialzugriff zu vertretbaren Kosten). Aufgrund der identifizierten Hürden wurde für das Projekt die begründete Entscheidung getroffen, auf physische SIM-Karten zu setzen. Diese Entscheidung stellt keine Einschränkung der Projektziele dar, sondern eine pragmatische Wahl zugunsten von Zuverlässigkeit und vollständiger Schlüsselkontrolle. Die gewonnenen Erkenntnisse bilden eine fundierte Grundlage für eine spätere eSIM-Migration.

**Gerätekompatibilität:** Die Authentifizierungsverfahren wurden auf Smartphones verschiedener Hersteller erfolgreich getestet und validiert, um die Breite der unterstützten COTS-Endgeräte zu zeigen.

## 1.6 AP4.2 - Einbindung

In AP4.2 wurden die Zugangsknoten in das Gesamtsystem eingebunden und der Einfluss unterschiedlicher Backhaul-Verbindungen auf die Zugangsfunktionalität untersucht.

**Starlink-Anbindung:** Ein Starlink-Terminal wurde beschafft und in Betrieb genommen. Die Beschaffung über die Einkaufsstrukturen einer öffentlichen Einrichtung war mit vergaberechtlichen Herausforderungen verbunden, da der Anbieter keine standardisierten Beschaffungswege für öffentliche Auftraggeber unterstützt. Erste systematische Latenzmessungen über das LEO-Netzwerk wurden durchgeführt. Die Kompatibilität der eingesetzten Sicherheitsprotokolle, insbesondere WireGuards 1-RTT-Handshake, mit Satellitenlatenzen wurde bestätigt.

**Hotspot-2.0-Implementierung:** Der vollständige technische Ablauf der automatischen SIM-basierten WLAN-Authentifizierung wurde implementiert: ANQP-basierte Discovery, EAP-AKA-Authentifizierung über einen lokalen RADIUS-Server (FreeRADIUS) mit UDM-Anbindung des 5G-Cores sowie WPA3-Enterprise-konforme Schlüsselableitung. Eine Android-App wurde entwickelt, die das Passpoint-Profil einma-

lig auf dem Gerät einrichtet. Das Betriebssystem übernimmt danach Netzwerkerkennung und Authentifizierung vollständig eigenständig, ohne dass dauerhaft installierte Zusatzsoftware erforderlich ist. (Abbildung 1)

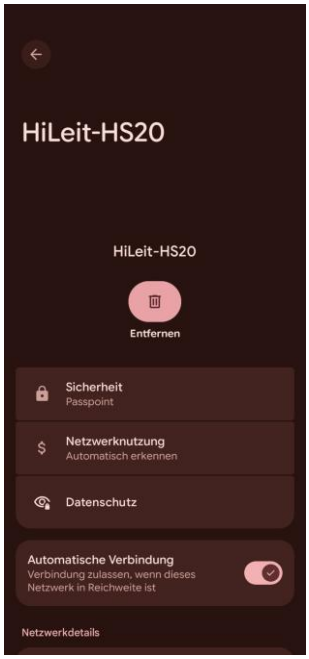



**Abbildung 1** Android-Netzwerkeinstellungen des Hotspot-2.0/Passpoint-Profils mit aktivierter automatischer Verbindung

**Lokaler Betrieb ohne externe Abhängigkeiten:** Es wurde bestätigt, dass 5G-Core (Open5GS) und RADIUS-Server (FreeRADIUS) vollständig lokal betrieben werden können, ohne externe Verzeichnisdienste vorauszusetzen. Dies ist eine zentrale Anforderung für den Katastrophenschutzeinsatz, bei dem keine externe Infrastruktur angenommen werden darf.

## 1.7 AP4.3 - Parametrisierung

In AP4.3 wurden die Parameter des Mobilfunk- und WLAN-Systems mit Fokus auf Reichweite, Verfügbarkeit, Zugänglichkeit, Sicherheit und Priorisierung festgelegt.

**5G Network Slicing:** Eine im Projektkontext betreute Masterarbeit untersuchte 5G Network Slicing hinsichtlich seiner praktischen Nutzbarkeit in definierten Einsatzszenarien. Unter anderem um Aussagen treffen zu können, in welcher Granularität Slices für die logische Trennung von BOS-Datenverkehr und anderen Diensten in einem nomadischen Campusnetz einsetzbar sind.

**WiFi QoS und Priorisierung:** Die Konfiguration von QoS-Funktionen für WiFi stellt eine Möglichkeit zur Bandbreitenreservierung für einsatzkritische Anwendungen dar und ermöglicht damit die Priorisierung von BOS-Verkehr gegenüber dem Bevölkerungssegment.

## 1.8 AP5.2 - Multi-Gateway / Load-Balancing / Failover

Im Rahmen des Demonstrators wurde die Kompatibilität von WireGuard mit Gateway-Wechseln betrachtet, wie sie im WiBACK-Backhaul-System auftreten. Der integrierte 1-RTT-Handshake und Peer-Roaming-Mechanismus von WireGuard erwiesen sich als geeignet, um VPN-Sessions bei einem Wechsel des aktiven Gateways aufrechtzuerhalten. Dies bestätigte sich beim Demonstrator auf dem Flugplatz Schönhagen: Nach dem Live-Abschalten des aktiv genutzten WiBACK-Knotens leitete das System den Verkehr automatisch um, und die WireGuard-Session überstand das Umschalten ohne Neuaufbau der Verbindung.

## 1.9 AP5.3 - Föderation und Kommunikationssicherheit

Für die sichere Kommunikation zwischen einzelnen Teilnetzen wurde ein grundlegendes Konzept auf Basis von WireGuard-Verbindungen skizziert. Das entwickelte PQC-VPN-Gateway mit vorkonfiguriertem WireGuard-Profil bietet dabei einen möglichen Ansatzpunkt, um neue Knoten ohne aufwändige manuelle Konfiguration in eine föderierte Struktur einzubinden.

## 1.10 AP6 - Feldtest, Evaluation, Bewertung

Die H-BRS integrierte die in AP3 und AP4 entwickelten Komponenten in den gemeinsamen Demonstrator. Kern der H-BRS-Beiträge waren das PQC-VPN-Gateway sowie die Hotspot-2.0-Lösung mit SIM-basierter Authentifizierung. (Abbildung 2)

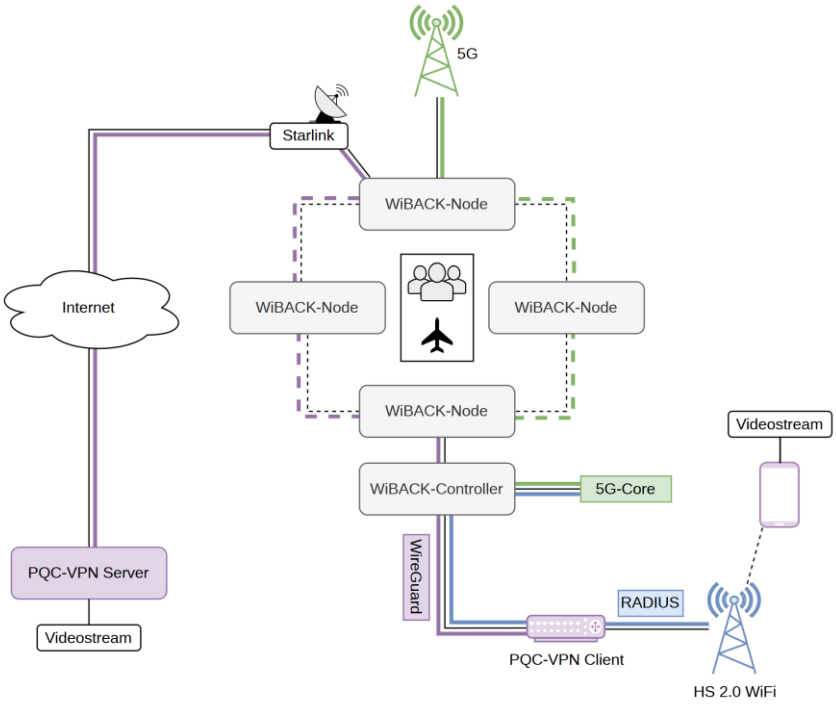



**Abbildung 2** Systemarchitektur des Demonstrators auf dem Flugplatz Schönhagen mit Starlink- und 5G-Backhaul, WiBACK-Ringnetz, PQC-VPN-Gateway und Hotspot-2.0-WLAN-Zugang

Das PQC-VPN-Gateway wurde als physisches Gerät realisiert, das beliebige Netzwerkgeräte per Plug-and-Play in einen kryptographisch gesicherten WireGuard-Tunnel einbindet. Ein WLAN-Access-Point war direkt an das Gateway angeschlossen und befand sich damit automatisch im Schutz des Tunnels, ohne gerätespezifische VPN-Konfiguration zu erfordern.

Für die Hotspot-2.0-Authentifizierung wurde eine Android-App entwickelt, die das Passpoint-Profil einmalig auf dem Endgerät einrichtet. Das Betriebssystem übernimmt danach Netzwerkerkennung und Authentifizierung vollständig. Einsatzkräfte können sich damit ohne manuelle Eingabe sicher und automatisch in das Einsatznetz einwählen.

Die Validierung des Demonstrators wurde auf dem Flugplatz Schönhagen in Trebbin, Brandenburg, erfolgreich durchgeführt. Das vollständige autarke Kommunikationsnetz wurde unter realistischen Feldbedingungen betrieben, gespeist durch akkugepufferte WiBACK-Knoten und Starlink-Backhaul. Als unmittelbarer Nachweis der funktionierenden Ende-zu-Ende-VPN-Verbindung diente ein Videostream einer Webcam der H-BRS, die ausschließlich innerhalb des WireGuard-geschützten PQC-VPN-Tunnels erreichbar ist. Die automatische SIM-basierte WLAN-Authentifizierung via Hotspot 2.0 und EAP-AKA funktionierte störungsfrei ohne manuelle Nutzerinteraktion. Das PQC-VPN-Gateway stellte die Post-Quanten-gesicherte Verbindung transparent bereit. (Abbildung 3)

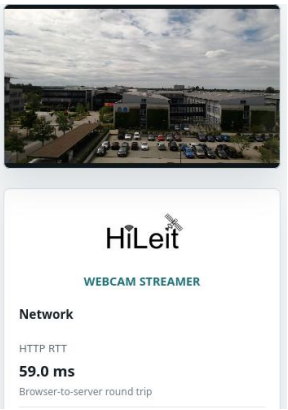



**Abbildung 3** Im Feldtest genutzte Testanwendung zur Überprüfung der Netzwerkverbindung, mit Live-Videostream und Messung der Verbindungslaufzeit (HTTP RTT)

Im Resilienztest wurde der WiBACK-Knoten, über den der aktive Videostream geroutet war, live abgeschaltet. Das System erkannte den Ausfall automatisch, leitete den Datenverkehr über verbleibende Knoten des Ringnetzes um, und der Videostream wurde nach wenigen Sekunden wiederhergestellt. Die WireGuard-Session überstand das Umschalten ohne Neuaufbau. Dieser Test bestätigte die automatische Ausfallsicherheit des Gesamtsystems unter realistischen Ausfallbedingungen, ohne dass ein Eingriff der Einsatzkräfte erforderlich war.

Aufgrund von Frequenzkonflikten mit parallel operierenden Gruppen am Standort Schönhagen konnte die 5G-Basisstation dort nicht aktiviert werden. Alle übrigen Systemkomponenten arbeiteten störungsfrei. Die 5G-Integration wurde im Rahmen der Laborarbeiten und der Vorbereitung des Feldversuchs gesondert validiert.

## 2. Beitrag zu den Zielen der Fördermaßnahme, voraussichtlicher Nutzen und Verwertbarkeit

Das Teilvorhaben der H-BRS leistete direkte Beiträge zu den Zielen des Förderprogramms KoPa_45. Es adressierte Forschungsfragen zu sicheren verlegbaren Campusnetzen im BOS-Umfeld, zu praxistauglichen Zugangs- und Anbindungskonzepten für heterogene Endgeräte sowie zu Netzmanagementfunktionen für den Betrieb unter schwierigen Bedingungen ohne externe Infrastruktur. Das entwickelte Sicherheitskonzept, das Zugangskonzept und der PQC-VPN-Demonstrator belegen, dass eine autarke breitbandige BOS-Kommunikationsinfrastruktur mit handelsüblichen Endgeräten und ohne spezialisiertes IT-Personal im Feld betrieben werden kann. Die Projektergebnisse wurden im Konsortium positiv aufgenommen und in den gemeinsamen Demonstrator integriert

**Tabelle 2** Verwertungsplan

| Vorhabenergebnisse und ihre Verwertung | … aktuell | … voraussichtlich innerhalb der nächsten zwei Jahre |
|---|---|---|
| Schutzrechte: z.B. Patente, Lizenzen, Vergabe von Lizenzen an Dritte | Keine | Keine |
| Beiträge für die Standardisierung, z. B. 3GPP | Keine | Keine |
| Produkte: z.B. Komponentenverbesserung, Erweiterung des Produktportfolios mit neuen oder verbesserten Produkten | PQC-VPN-Gateway als funktionierender Prototyp | |
| Technologie: z.B. verbesserter Fertigungsprozess, Messverfahren… Verfahren bei der Fertigung von Produkten bzw. Erstellung von Dienstleistungen | | Umstellen des Labor WLANs auf Hotspot 2.0 |
| Dienstleistungen: z.B. erweiterte Beratungs- und Zuliefermöglichkeiten… Neue oder verbesserte Dienstleistungen | Beratungskompetenz zu sicherer BOS-Kommunikation | Schulungs- und Beratungsangebote für BOS |
| Know-how Transfer: z.B. in interdisziplinäre Bereiche, Anschlussfähigkeit an weitere Forschungs- und Entwicklungsvorhaben | Projektergebnisse in Lehrveranstaltungen und Abschlussarbeite | Einwerben weiterer Drittmittelprojekte |
| Wissenstransfer: z.B. durch Verbesserung von Forschung und Lehre, Veröffentlichungen | Teilnahme an Konferenzen | Wissenschaftliche Publikationen auf nationalen, sowie internationalen einschlägigen Konferenzen |
| Netzwerk und Ökosystem: z.B. Teilnahme an Veranstaltungen | Vernetzung mit BOS-Akteuren und Kontakte zur BDBOS und weiteren KoPa_45-Projekten | Beteiligung an weiteren BOS-Digitalisierungsprojekten |

## 2.1 Wirtschaftliche Erfolgsaussichten nach Vorhabenende

**Drittmitteleinwerbung für Folgeprojekte:** Die entwickelten Konzepte (PQC-VPN-Gateway, Hotspot-2.0-Zugang) sowie die identifizierten offenen Fragen (5G-Integration, MCX-Dienste, eSIM-Migration, Frequenzregulierung) bilden eine gute Grundlage für Anschlussanträge.

**Schulungs- und Beratungsangebote für BOS:** Die aufgebauten Kompetenz zu sicherer BOS-Kommunikation soll in konkrete Schulungs- und Beratungsangebote für BOS-Organisationen überführt werden.

**Lehre:** Die Projektergebnisse fließen bereits kontinuierlich in Bachelor- und Masterlehrveranstaltungen sowie Abschlussarbeiten ein und werden dauerhaft Bestandteil der Lehre an der H-BRS bleiben.

## 2.2 Wissenschaftliche und/oder technische Erfolgsaussichten nach Vorhabenende

Auf wissenschaftlicher Ebene eröffnen die Projektergebnisse mehrere Anschlusspfade. Wissenschaftliche Publikationen auf einschlägigen internationalen Konferenzen sind geplant. Die Bedrohungsanalyse des Sicherheitskonzepts, gestützt auf eigene 5G-NSA-Vorarbeiten, kann als Grundlage für Security-by-Design-Ansätze in zukünftigen BOS-Netzentwicklungen dienen. Die Erkenntnisse zur eSIM-Problematik erfordern weitere Forschungsarbeit, um niederschwellig für Testbetriebe und private Campusnetze eSIMs als lohnenswerte Erweiterung der Bedienfreundlichkeit zu etablieren.
Die interdisziplinäre Verbundkonstellation hat sich als sehr produktiv erwiesen. Eine Fortführung der Zusammenarbeit in Folgeprojekten wird angestrebt.

## 2.3 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Aus den Projektergebnissen ergeben sich mehrere konkrete Anschlussbedarfe. Die regulatorische Frage der Frequenzzuteilung für nomadische 5G-Campusnetze bleibt ein offenes Problem. Die im Projekt vorgeschlagenen technischen Lösungsansätze (Spectrum Sensing, automatisierte Frequenzanfrage) und die dokumentierten Einsatzerfahrungen können als Grundlage für Regulierungsdiskussionen mit der Bundesnetzagentur dienen.

Technisch stellt die vollständige Integration der 5G-Basisstation in einen nomadischen, feldfähigen Demonstrator einen nächsten konkreten Entwicklungsschritt dar. Mission-Critical-Services (MCX) nach 3GPP-Standard (MCPTT, MCVideo, MCData) bieten als funktionale Brücke zwischen TETRA und breitbandiger IP-Kommunikation ein attraktives Forschungs- und Entwicklungsfeld für Folgeprojekte.

# III. Anlagen

## 1. Wichtige Positionen des zahlenmäßigen Nachweises

Der größte Anteil der Fördermittel entfiel auf Personalausgaben. Das mit der Bearbeitung des Teilvorhabens betraute wissenschaftliche Personal war bereits an der Hochschule Bonn-Rhein-Sieg beschäftigt und wurde für die Projektlaufzeit aus den Fördermitteln des Teilvorhabens finanziert. Eigens neu eingestellt wurde lediglich eine studentische Hilfskraft. Ein Einsatz grundfinanzierten Personals war für die Durchführung des Teilvorhabens nicht vorgesehen.

Mit den Fördermitteln wurden zudem Reisen finanziert, insbesondere nach Berlin zu dem Innovationsforum der BDBOS sowie zu weiteren Maßnahmen der Öffentlichkeitsarbeit (u. a. Workshops und Fachkonferenzen).

Die wichtigsten technischen Beschaffungen lassen sich wie folgt in Kategorien zusammenfassen:

- Mobilfunk (5G-/LTE-Laborumgebung): ca. 14.000 € – Lizenzverlängerungen für Netz- und Endgerätesimulation sowie Test-SIM- und eSIM-Profile
- Funkmesstechnik und Abschirmung: ca. 9.500 € – geschirmte Messkammer
- Endgeräte: ca. 3.800 €
- WLAN und Zugangsnetz: ca. 900 €
- Satellitenanbindung (LEO): ca. 300 €

Die Fördermittel waren notwendig, weil die Arbeiten einen zusätzlichen, projektbezogenen Forschungs- und Entwicklungsaufwand darstellten. Die dafür benötigte spezialisierte Hard- und Software ist nicht der Grundausstattung der Hochschule zuzurechnen. Ohne die Förderung hätten diese Arbeiten daher weder zeitnah noch in der erforderlichen fachlich-technischen Tiefe durchgeführt werden können.

## 2. Zusammenarbeit und Projektmanagement

Im folgenden Abschnitt reflektieren wir die Zusammenarbeit im Projektverlauf, zunächst innerhalb des Konsortiums, anschließend mit der Zuwendungsgeberin BDBOS und dem Projektträger VDI/VDE.

## 2.1 Zusammenarbeit mit dem Konsortium

Die Zusammenarbeit im Konsortium aus Fraunhofer FIT (Koordination), Hochschule Bonn-Rhein-Sieg, Malteser Hilfsdienste e.V. und DeFuTech UG wurde über die gesamte Projektlaufzeit als konstruktiv und partnerschaftlich erlebt. Ein wesentlicher Rahmen für die Abstimmung war ein fester, zweiwöchentlich stattfindender Konsortial-Jour-fixe, in dem technische Abhängigkeiten zwischen den Arbeitspaketen, der Stand der Anforderungsanalyse aus AP2 sowie die Vorbereitung von Demonstrator und Feldversuch kontinuierlich abgestimmt wurden. Ergänzend fanden persönliche Treffen bzw. gemeinsame Vor-Ort-Termine statt, insbesondere im Rahmen der Vorbereitungen des Demonstratoraufbaus.

Besonders hervorzuheben ist die Zusammenarbeit mit den Maltesern Hilfsdiensten als Anwendungspartner. Als BOS-Organisation mit unmittelbarer Einsatzerfahrung haben die Malteser der technischen Konzeption von Anfang an eine belastbare Praxisgrundlage gegeben, die sich rein akademisch nicht hätte erarbeiten lassen.

Herausforderungen ergaben sich vor allem aus externen Randbedingungen: Der rückwirkend im Förderbescheid definierte Projektstart führte zu einem erheblichen Bearbeitungsrückstand, da zentrale Schritte wie Stellenausschreibung sowie Personal- und Materialbeschaffung erst nach Erhalt des Bescheids eingeleitet werden konnten. Eine im Projektverlauf notwendig gewordene personelle Neubesetzung an der H-BRS verursachte zusätzlichen Verzug durch die erforderliche Einarbeitungszeit. Dieser Rückstand konnte durch temporär erhöhten Personalaufwand aufgefangen werden, ohne dass inhaltliche Einschränkungen entstanden sind.

## 2.2 Zusammenarbeit mit der BDBOS und VDI/VDE

Wir bedanken uns herzlich für die Organisation der Projektreihe KoPa_45 und die damit verbundene Gelegenheit, den Digitalfunk der Zukunft in Deutschland aktiv mitzugestalten. Insbesondere die beiden Innovationsforen der BDBOS in Berlin möchten wir positiv hervorheben: Sowohl die Vorstellung des Vorhabens auf dem 1. Innovationsforum 2024 als auch die Präsentation des fertigen Demonstrators und der Projektergebnisse auf dem 2. Innovationsforum 2026 haben wir als hervorragend organisiert und inhaltlich sehr bereichernd erlebt. Gerade an diesem Format wird für uns spürbar, dass die BDBOS als Zuwendungsgeberin ein echtes inhaltliches Interesse an den Projektergebnissen hat: Die Innovationsforen sind erkennbar nicht als reine Pflichttermine angelegt, sondern bieten Raum für vertiefte fachliche Diskussion, gezielte Nachfragen zu den technischen Ergebnissen und eine sichtbare Auseinandersetzung mit dem, was die einzelnen Teilvorhaben tatsächlich erarbeitet haben. Der direkte Austausch mit BOS-Anwendern, Fördergebern und anderen KoPa_45-Konsortien vor Ort war für die Projektbearbeitung außerordentlich motivierend. Auch die KoPa_45-Roadshow sowie die begleitete Vernetzung mit anderen Vorhaben der Förderrichtlinie haben wir als sehr hilfreich für die eigene Projektarbeit empfunden.

Als verbesserungsfähig haben wir erlebt, dass der Projektstart im Förderbescheid rückwirkend definiert wurde. Da wesentliche Schritte wie Stellenausschreibung sowie Personal- und Materialbeschaffung an der Hochschule erst nach Erhalt des Bescheids eingeleitet werden konnten, entstand von Beginn an ein spürbarer Bearbeitungsrückstand bei den personalintensiven Arbeiten, der erst durch die spätere kostenneutrale Verlängerung vollständig aufgefangen werden konnte. Für zukünftige Ausschreibungen dieser Art würden wir uns eine frühzeitigere Zustellung des Zuwendungsbescheids bzw. eine Antragsstartdefinition wünschen, die den tatsächlichen administrativen Vorlauf an Hochschulen stärker berücksichtigt.

Positiv hervorzuheben ist demgegenüber, dass die von uns beantragte kostenneutrale Verlängerung um vier Monate unkompliziert und ohne nennenswerten bürokratischen Mehraufwand bewilligt wurde, sodass der durch den Malteser-Einsatz beim Katholikentag 2026 bedingte Zeitversatz im Feldversuch (AP6) ohne Qualitätseinbußen aufgefangen werden konnte.

Im Rückblick auf den Projektverlauf sind wir überzeugt, dass KoPa_45 einen wichtigen Beitrag zum Digitalfunk der Zukunft in Deutschland leistet, und freuen uns auf die weitere Zusammenarbeit mit der BDBOS und dem VDI/VDE in Folgevorhaben.

## 3. Übersicht der Maßnahmen der Öffentlichkeitsarbeit

| Veranstaltung | Zeitraum | Art | Beitrag H-BRS |
|---|---|---|---|
| 1.Innovationsforum BDBOS | 2024 | Fachveranstaltung | Vorstellung des Teilvorhabens |
| Projektworkshop HiLeit-Konsortium | 2025 | Workshop | Präsentation von Zwischenergebnissen, Fortführung eines Projektplans |
| Öffentlicher Workshop mit BOS-Akteuren mit BMDV-Projekt 5G-Opportunity | 2025 | Workshop | Präsentation und Diskussion, Vernetzung |
| KoPa_45 Roadshow | 2025 | Fachveranstaltung | Präsentation von Zwischenergebnissen |
| Mobilkommtagung Osnabrück | 2025 | Fachkonferenz | Teilnahme und Austausch mit Forschungsgemeinschaft |
| PMRExpo | 2025 | Fachmesse | Teilnahme, Netzwerken |
| 2. Innovationsforum der BDBOS | 2026 | Fachveranstaltung | Netzwerken, Präsentation von Ergebnissen und Live-Demonstrator |

Über das Vorhabenende hinaus sind weitere Disseminationsmaßnahmen geplant. Unteranderem fließen die Ergebnisse und Erkenntnisse unmittelbar in die Lehre ein. Weiterhin sind wissenschaftliche Publikationen der Projektergebnisse auf internationalen Konferenzen geplant.

## 4. Übersicht der Schutzrechtsanmeldungen

Keine