Bundesanstalt
für den Digitalfunk der Behörden und
Organisationen mit Sicherheitsaufgaben

Katalog Forschungsthemen Projekt KoPa_45

Februar 2023

Interessensgebiet App-, Teilnehmer und Endgeräte-Management

Inhaltsverzeichnis

Einführung

Zur Vorbereitung und inhaltlichen Ausrichtung ihres Förderprogramms hat die BDBOS in den vergangenen Monaten Forschungsfragen erarbeitet, die im Hinblick auf künftige breitbandige einsatzkritische Mobilfunknetze von Interesse sind. Die Analyse wurde nach einem festgelegten Schema durchgeführt.

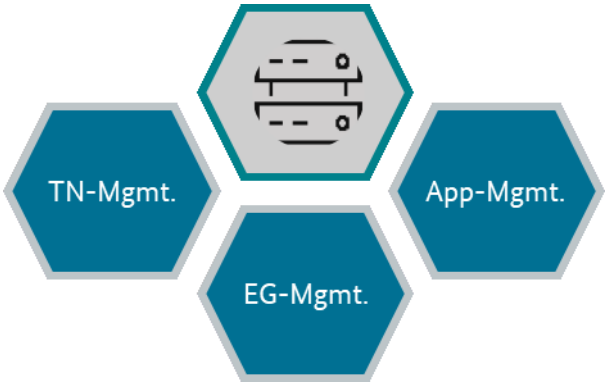
Die im Dokument verwendete Abkürzung GAN steht für eine Expertengruppe von Bund und Ländern, die „Gruppe Anforderungen an das Netz“ (GAN). Diese hat im Jahr 2002 die Anforderungen an das BOS-Digitalfunknetz festgelegt und fünf GAN-Kategorien für das Ziel Funkversorgungsqualität definiert. Im Jahr 2020 wurden die Anforderungen an ein künftiges Digitalfunknetz fortgeschrieben und beschlossen (GAN 2.0).

Schema der Analyse

Abschnitt	Bemerkung
Ist-Zustand	Aktuelle Anforderungen an den Digitalfunk BOS zum Thema
Soll-Zustand	Absehbare zukünftige Anforderungen an ein einsatz-kritisches Breitbandnetz
Input Standards & Produktumfeld	Leistungsfähigkeit aktueller und zukünftiger Breitband-standards (LTE; 5G & 6G) und –produkte zum Thema
Delta	
Forschungsfragen	Abgeleitet aus dem Delta

Interessensgebiet App-, Teilnehmer- und Endgeräte-management

In diesem Interessensgebiet werden die folgenden Themen betrachtet:



Themen im Interessensgebiet App-, Teilnehmer- und Endgerätemanagement

Applikationsverwaltung

1. Aktuelle Anforderungen an den Digitalfunk BOS

Applikationen im Sinne von Smartphone-Apps existieren im TETRA-basierten Digitalfunk BOS nicht. Die folgenden Ausführungen zum Ist-Zustand gelten daher nicht bundesweit, sondern für mindestens einige Bundesländer und ihre BOS-Nutzerorganisationen:

- Breitband-Applikationen werden von Nutzerorganisationen mit eigenen Systemen verwaltet.
- Je Nutzerorganisation existiert eine Übersicht aller in Nutzung befindlichen und freien Lizenzen.
- Eine nutzer- und/oder gerätespezifische Freigabe von Applikationen kann in den App-Stores der Nutzerorganisationen vollzogen werden.
- Anwendungen werden teilweise auf die Erfüllung definierter Sicherheits- und Zertifizierungsvorgaben geprüft.

2. Absehbare zukünftige Anforderungen an ein einsatzkritisches Breitbandnetz

- Applikationen sollen über ein zentrales mandantenfähiges System bereitgestellt und verwaltet werden können.
- Die Mandanten (BDBOS, Autorisierten Stellen sowie die ihnen zugeordneten taktisch-technischen Betriebsstellen und ggf. weitere organisatorische BOS-Einrichtungen) sollen in dem zentralen System die BOS-spezifische Applikationsverwaltung durchführen können. Die inhaltliche Administration und Pflege der Applikationen soll in den Fachstellen verbleiben.
- Für einsatzkritische und ggf. auch einsatzunterstützende Applikationen zum Einsatz im BOS-Umfeld sollen einheitliche Mindeststandards (bspw. zu IT-Sicherheit & Datenschutz) entwickelt werden.
- Das Applikationsverwaltungssystem soll die Zugriffsrechte von Applikationen auf Hard- & Softwareebene steuern können. Hier werden unter anderem folgende Fragen betrachtet: Welche (Sensor-)Daten dürfen Apps vom Smartphone oder Tablet lesen? Dürfen Apps untereinander Daten austauschen?
- Die Applikationsverwaltung soll eine Trennung von Daten (Hard- & Software, private- & dienstliche und applikationsübergreifende Daten) innerhalb der Applikationen steuern können.
- Es muss eine Übersicht aller im Bestand vorhandenen Lizenzen und Kosten ermöglicht werden (z. B.: monatlich, jährlich).
- Funktionsgleiche einsatzkritische und ggf. auch einsatzunterstützende Applikationen sollen für alle verwendeten Betriebssysteme (v.a. iOS und Android) bereitgestellt werden können.
- Einzelne Applikationen sollten die Möglichkeit haben, in einer sicheren Umgebung (z. B. Container) zu operieren.
- Die revisionssichere Hinterlegung des vollständigen Quellcodes der verwendeten Applikationen soll durch die Einrichtung und den Betrieb von Repositories und eines Build-Systems ermöglicht werden.

3. Leistungsfähigkeit aktueller und zukünftiger Breitbandstandards (LTE; 5G & 6G sofern absehbar) und –produkte zum Thema

Aktuelle Applikationsverwaltungssysteme (Mobile Application Management) ermöglichen den Mandanten, je nach Berechtigung, folgenden Funktionsumfang:

- Erstellen eines eigenen Katalogs mit Behörden- / Unternehmens-Apps
- Self Service-Portal für Apps
- Nutzergruppenbasierte App-Bereitstellung
- App-Installation/-Aktualisierung/-Löschung im Hintergrund
- Sperrliste für Apps
- Anpassung von App-Konfigurationen und -Berechtigungen
- App-basierte Einschränkungen, App-spezifische Richtlinien
- App-basierte Berichte
- Integrationen mit MDM
- Anpassung des Store-Layouts
- Pflege aller App-Lizenzen (Kauf, Abrechnung Verteilung und Kündigung/löschen von Lizenzen)
- Die Regulierung der Zugriffe von Applikationen auf Hard- & Softwareebene ist durch MAM-Systeme möglich.
- Der Datenaustausch zwischen Applikationen kann beschränkt werden.
- App-Updates können zentral durch das MAM-System gesteuert werden.
- Es besteht die Möglichkeit von Downloads via WLAN oder OTA, in Abhängigkeit der Datenmenge.
- Es kann vorgegeben werden, wann Installationszeitpunkte stattfinden und wie lange eine Installation aufgeschoben werden kann.
- Es können Standard-Speicherorte vorgegeben werden (z. B. keine Speicherung von Daten auf dem Endgerät, der Speicherkarte, Netzwerk oder innerhalb von Apps).
- Funktionalitäten von Apps können eingeschränkt werden (z. B. Unterbinden von Screenshots oder Videoaufnahmen).

4. Delta der Anforderungen und Leistungsfähigkeit der Standards

- Für die Verknüpfung bestehender MAM-Lösungen mit einem Teilnehmermanagement entsprechend den BOS-Anforderungen (ähnlich des Nutzereigenen Managements (NeM) des Digitalfunk BOS) gibt es keine marktreifen Lösungen oder Konzepte.
- Die Mandantenfähigkeit bestehender MAM-Lösungen berücksichtigt BOS-Anforderungen nicht.

- Hard- und Softwarestandards (Mindeststandards, welche von Ländern verfeinert werden können) für BOS-Breitbandendgeräte fehlen.
- Bundeseinheitliche Prozesse und Konzepte für die Zulassung von Anwendungen fehlen.

5. Bisher identifizierte Forschungsthemen

- Wie kann der Zugriff bei Endgeräten auf alle für die Applikationsverwaltung benötigten Informationen gewährleistet werden?
- Wie kann eine zentrale, mandantenfähige, den BOS-Anforderungen genügende Applikationsverwaltung aufgebaut werden?
- Welche am Markt verfügbaren MAM-Systeme wären am geeignetsten, um die BOS-Anforderungen zu erfüllen?
- Wie könnte eine Applikationsverwaltung mit einer Endgeräte- und Teilnehmerverwaltung verknüpft werden?
- Welche datenschutzrechtlichen Probleme könnten durch eine zentrale Applikationsverwaltung entstehen und wie wären sie zu lösen?
- Welche Anforderungen zur Sammlung statistischer Nutzungsdaten gibt es und wie sind diese zu erfüllen?
- Welche Rechte und Rollen werden in einem mandantenfähigen MAM-System zur Erfüllung der BOS-Anforderungen benötigt?
- Gibt es besondere Anforderungen für spezielle Nutzergruppen (Spezialeinsatzkräfte o. ä.) und wie sind diese zu erfüllen?
- Welche App-Installationsmethoden werden benötigt und wie können diese umgesetzt werden (Push/Pull)?
- Wie kann eine Störung in der Endgerätenutzung verhindert werden, wenn das Applikationsmanagement ausfällt oder Störungen produziert?
- Welche Auswirkungen hat ein „Bring your own device“-Ansatz, also die Einbindung privater Endgeräte in den breitbandigen Digitalfunk BOS, auf die Applikationsverwaltung und welche Lösungen bestehen hierfür?

Teilnehmerverwaltung

1. Aktuelle Anforderungen an den Digitalfunk BOS

Teilnehmerverwaltung (Subscriber Management) für Breitbandnetze und -dienste findet derzeit ohne Mitwirkung der BDBOS statt. In Bund und Ländern werden unterschiedliche eigene Infrastrukturen für die Administration der dortigen Teilnehmer vorgehalten und eingesetzt. Die folgenden Ausführungen zum Ist-Zustand gelten daher nicht bundesweit, sondern für mindestens einige Bundesländer und ihre BOS-Nutzerorganisationen, bzw. sind aus aktuellen Anforderungen an den TETRA-Digitalfunk abgeleitet:

- Alle Daten eines Teilnehmers (Geräteeigenschaften, soweit fernadministrierbar, Dienste und Berechtigungen („Subscription“) sowie Daten der Sicherheitskarte wie operativ-taktische Adresse, OPTA) sollen über ein System administrierbar sein.
- Parametergruppen sollen als Profile den Teilnehmern zugewiesen werden können.
- Es sollen Parameter entsprechend GAN 2.0 administriert werden können.
- Die Administration von Berechtigungen und Dienstfreigaben muss - entsprechend der unterschiedlichen Hierarchiestufen - über ein Rechte- und Rollenkonzept delegierbar sein (Mandantenfähigkeit).
- Die Bereitstellung von bestimmten Teilnehmerverwaltungsfunktionen für Leitstellen, z.B. die Möglichkeit, von einer Leitstelle aus einen Gruppenwechsel auch ohne Einwirken der Benutzer zu veranlassen, ist umzusetzen.
- Darüber hinaus sind bislang keine Anforderungen an ein Teilnehmer-Management für BOS-Breitband-Teilnehmer abgestimmt worden.

2. Absehbare zukünftige Anforderungen an ein einsatzkritisches Breitbandnetz

Vordringlich wird eine Teilnehmerverwaltung für das kommende hybride Breitbandnetz der BDBOS (Daten und Telefonie) benötigt. Einsatzkritische Dienste (MCx) nach 3GPP kommen hinzu; eine entsprechende Erweiterung der Teilnehmerverwaltung sollte bereits eingeplant werden. Die Anforderungen an ein einheitliches Digitalfunknetz umfassen nach GAN 2.0 im Allgemeinen mindestens die Grundanforderungen an das TETRA-Digitalfunknetz. Für ein nutzereigenes Management im einheitlichen Digitalfunknetz gelten grundsätzlich die gleichen Anforderungen wie für das Management des TETRA-Digitalfunknetzes. Es müssen jedoch zusätzliche Parameter (z. B. Mobilfunk- und MCx-Teilnehmerdaten) verwalten werden können. Folgende Anforderungen sind bereits jetzt abzusehen:

- Eine Möglichkeit der Zuordnung der Identität von Breitbandendgeräten (Tel.-Nr. des Smartphones) zu Funkrufnamen / OPTA (TETRA-Teilnehmer) wird benötigt.
- Das zukünftige Teilnehmerverwaltungssystem muss mandantenfähig sein (analog zum bisherigen NeM).
- Das einheitliche Digitalfunknetz besteht aus mehreren Teilsystemen, wie Funkzugangsnetz (Radio Access Network, RAN), Kernnetz (EPC / 5GC), IMS, MCS-Server, TETRA und ggf. weiteren, die von verschiedenen Herstellern stammen können. Teilnehmerdaten können über mehrere Teilsysteme verteilt sein. Das zukünftige Teilnehmerverwaltungssystem muss

Schnittstellen zu den relevanten Teilsystemen unterstützen und damit eine zusammengeführte Teilnehmerverwaltung unter einer Oberfläche erlauben.

- Die zukünftige Teilnehmerverwaltung sollte im Verbund mit den Verwaltungssystemen für Endgeräte (MDM) und Anwendungen (MAM) konzipiert werden, um alle abhängigen Datenobjekte eines Teilnehmers darstellen und ggf. modifizieren zu können.
- Das zukünftige nutzereigene Management soll Zugriff auf ein zentrales Namensverzeichnis für alle vergebenen OPTA bieten und die Zugriffsrechte durch ein Rechte- und Rollenkonzept regeln (siehe Abschlussbericht GAN 2.0, Abschnitt 2.9).
- Das Teilnehmerverwaltungssystem soll sicher, umfassend, homogen, nutzerfreundlich und massendatentauglich sein.

3. Leistungsfähigkeit aktueller und zukünftiger Breitbandstandards (LTE; 5G & 6G sofern absehbar) und –produkte zum Thema

- Teilnehmerdaten für die Nutzung des Datenkernnetzes (EPC bzw. 5GC) und der Telefonie (IMS) werden in einem HSS bzw. UDM vorgehalten. Das Teilnehmermanagement ist Teil einer BSS-Suite (Business Support System), welche die Daten im eigentlichen Core-Netzelement verwaltet. Teilnehmerverwaltungssysteme als BSS-Komponenten für MVNO sind am Markt etabliert.
- Die Funktionen des existierenden Nutzereigenen Managements für die TETRA-Teilnehmer sind nicht standardisiert und sind derzeit nicht für die Administration von Breitbandteilnehmern geeignet.
- Das Management der Teilnehmerdaten in MCS-Systemen erfolgt über die UE-Schnittstelle und ist in den 3GPP-Spezifikationen 23.379 (MCPTT), 23.282 (MCData), 23.281 (MCVideo) und 23.280 (gemeinsame Funktionen) spezifiziert.
- Gegebenenfalls stehen weitere Managementfunktionen über herstellerproprietäre Schnittstellen zur Verfügung.
- Eine Teilnehmerverwaltung hat oft eine Anbindung an ein bereits bestehendes Active Directory (meist über LDAP) und damit einen Zugriff auf Benutzerprofile und Berechtigungen, worüber Änderungen oder Abfragen von Teilnehmerdaten durchgeführt werden können.
- Teilnehmerauthentifizierungen werden über verschiedene Methoden ermöglicht (z. B. One-Time Password (OTP), Biometrie (Fingerabdruck / Stimme), Smart Cards, UserID & Passwort).

4. Delta der Anforderungen und Leistungsfähigkeit der Standards

- Ein technologieübergreifendes, den BOS-Anforderungen entsprechendes, Teilnehmerverwaltungssystem ist nicht am Markt etabliert.
- Die Interoperabilität eines übergreifenden Teilnehmerverwaltungssystems mit den Teilsystemen (Kernnetz, IMS, MCx, …) verschiedener Hersteller kann nicht vorausgesetzt werden.
- Eine eindeutige Zuordnung der TETRA-Profile (ID und Dienste) auf MCx-Profile fehlt.

- Ein Konzept für eine Teilnehmerauthentifizierung im Zusammenspiel von Teilnehmermanagement und EMM für eine schnelle und sichere Authentifizierung auf Endgeräten fehlt.

5. Bisher identifizierte Forschungsthemen

- Wie können die Teilnehmerdaten / SIMs der derzeit genutzten kommerziellen Mobilfunknetze ggf. durch ein zentrales, bspw. durch die BDBOS geführtes System verwaltet werden?
- Wie kann ein technologieübergreifendes Teilnehmerverwaltungssystem die BOS-Teilnehmerdaten für TETRA-Endgeräte sowie breitbandige Endgeräte in einem eigenen Kernnetz zentral verwalten?
- Welche Phasen bzw. Ausbaustufen sind für ein Teilnehmerverwaltungssystem vom Stand heute bis zur Einführung eines eigenen Kernnetzes mit MCx sinnvoll?
- Lässt sich das bestehende NeM als 5G-MVNO-Teilnehmerverwaltung erweitern bzw. ist dies sinnvoll?
- Sind NeM-Teilnehmerparameter auf MCx übertragbar? Welche eventuellen technologiebedingten Unterschiede gibt es und wie können diese behoben bzw. angepasst werden?
- Wie lassen sich die NeM-Teilnehmerprofile automatisiert in ein ggf. neues Teilnehmerverwaltungssystem übertragen?
- Wie könnte der Authentifizierungsprozess auf breitbandigen Endgeräten gestaltet werden? Welche Vor- und Nachteile ergeben sich daraus für Teilnehmer, BOS und Teilnehmerverwaltung?
- Welche Datenobjekte des Endgeräte- und Applikationsmanagements sollten ggf. mit Datenobjekten des Teilnehmermanagements verknüpft werden, bzw. über das Teilnehmermanagementsystem zugreifbar sein, um ein umfassendes Teilnehmermanagement über ein System zu ermöglichen?
- Wie können die Teilnehmerdaten der Teilsysteme „Mobilfunk (EPS / 5GS)“, „SIP-Core/IMS“ und „MCx“ für die Teilnahme an MCx-Diensten verknüpft und mit einem System verwaltet werden?
- Welche weiteren BSS-Funktionen könnten außerdem gebraucht werden? (z. B. Billing?)
- Wie kann unter Berücksichtigung der Sicherheits- und Verfügbarkeitsanforderungen ein „Bring your own device“-Ansatz, also die Einbindung privater Endgeräte in den breitbandigen Digitalfunk BOS, realisiert werden?

Endgerätemanagement

1. Aktuelle Anforderungen an den Digitalfunk BOS

Endgerätemanagement für Breitbandendgeräte (Consumer-Geräte wie Smartphones und Tablets) findet derzeit ohne Mitwirkung der BDBOS statt. In Bund und Ländern werden unterschiedliche eigene Infrastrukturen für die Administration von bundes- bzw. landesspezifischen Endgeräten vorgehalten und eingesetzt. Die folgenden Ausführungen zum Ist-Zustand gelten daher nicht bundesweit, sondern für mindestens einige Bundesländer und ihre BOS-Nutzerorganisationen:

- Softwarestände (z. B. Betriebssystem) sollen aktuell gehalten werden. Vorgaben zur Nutzung, Pflege und Administration der Endgeräte werden durch die Autorisierten Stellen vorgegeben (z. B. in NRW durch das LZPD) und durch die jeweiligen Dienststellen umgesetzt.
- MCx-fähige Endgeräte werden derzeit nicht berücksichtigt.
- BOS-Nutzerorganisationen wollen ihre eingesetzten Endgeräte selbst verwalten.
- Über ein dediziertes Rollen- und Rechtekonzept wird derzeit teilweise sichergestellt (Unterschiede zwischen Bundesländern existieren), dass sowohl nutzerübergreifende als auch landes- oder nutzerspezifische Anwendungen ausschließlich den berechtigten Nutzerkreisen zur Verfügung gestellt werden.
- Sicherheitsrichtlinien des BSI sollen eingehalten werden.

2. Absehbare zukünftige Anforderungen an ein einsatzkritisches Breitbandnetz

- Applikationen sollen über ein zentrales mandantenfähiges System bereitgestellt und verwaltet werden können.
- Die Mandanten (BDBOS, Autorisierten Stellen sowie die ihnen zugeordneten taktisch-technischen Betriebsstellen und ggf. weitere organisatorische BOS-Einrichtungen) sollen in dem zentralen System die BOS-spezifische Applikationsverwaltung durchführen können. Die inhaltliche Administration und Pflege der Applikationen soll in den Fachstellen verbleiben.
- Für einsatzkritische und ggf. auch einsatzunterstützende Applikationen zum Einsatz im BOS-Umfeld sollen einheitliche Mindeststandards (bspw. zu IT-Sicherheit & Datenschutz) entwickelt werden.
- Das Applikationsverwaltungssystem soll die Zugriffsrechte von Applikationen auf Hard- & Softwareebene steuern können. Hier werden unter anderem folgende Fragen betrachtet: Welche (Sensor-)Daten dürfen Apps vom Smartphone oder Tablet lesen? Dürfen Apps untereinander Daten austauschen?
- Die Applikationsverwaltung soll eine Trennung von Daten (Hard- & Software, private- & dienstliche und applikationsübergreifende Daten) innerhalb der Applikationen steuern können.
- Es muss eine Übersicht aller im Bestand vorhandenen Lizenzen und Kosten ermöglicht werden (z. B.: monatlich, jährlich).
- Funktionsgleiche einsatzkritische und ggf. auch einsatzunterstützende Applikationen sollen für alle verwendeten Betriebssysteme (v.a. iOS und Android) bereitgestellt werden können.

- Einzelne Applikationen sollten die Möglichkeit haben, in einer sicheren Umgebung (z. B. Container) zu operieren.
- Die revisionssichere Hinterlegung des vollständigen Quellcodes der verwendeten Applikationen soll durch die Einrichtung und den Betrieb von Repositories und eines Build-Systems ermöglicht werden.

3. Leistungsfähigkeit aktueller und zukünftiger Breitbandstandards (LTE; 5G & 6G sofern absehbar) und –produkte zum Thema

Aktuelle Endgerätemanagementsysteme (Mobile Device Management, MDM bzw. Enterprise Mobility Management, EMM) ermöglichen den Mandanten, je nach Berechtigung, folgenden Funktionsumfang:

- Authentisierung und Authentifizierung von Teilnehmern
- Nutzerauthentifizierungen über verschiedene Methoden (z.B.: One-Time Password (OTP), Biometrie (Fingerabdruck / Stimme), konvergierte Karten (digitale und physische Sicherheit), Smart Cards, UserID & Passwort)
- Dienstberechtigungen für Sprache, Daten, Alarmierung & Telefonie per Teilnehmerdatenverwaltung
- Geofencing (Zugriff auf Funktionen / Anwendungen, solange Endgerät sich in einem bestimmten Bereich befindet; Sperre oder Funktionseinschränkung, wenn der Bereich verlassen wird)
- Containerisierung (Trennung von dienstlichen und privaten Nutzerdaten)
- Sperrmodus (Beschränkung von Funktionen und Anwendungen auf Endgeräten, die nicht für eine dienstliche Nutzung vorgesehen sind)
- Löschung sicherheitsrelevanter Daten – nach individueller Definition – auf den Endgeräten, nach mehrfacher falscher Authentifizierung
- Remote Wipe (Löschen relevanter Daten aus der Ferne)
- Inventarisierung (alle in den jeweiligen Organisationen befindlichen Endgeräte sind zentral sichtbar, alle wichtigen Eigenschaften wie Systemzustand, mögliche Updates und Sicherheitslücken können eingesehen werden
- Endgeräte-Updates „Over-The Air“ abhängig vom Rollen- und Rechtekonzept
- Remote-Updates und Remote-Konfiguration von Einstellungen
- Verknüpfung mit einem eSIM-Management

4. Delta der Anforderungen und Leistungsfähigkeit der Standards

- Ein umfassendes Endgerätemanagement und eine Verwaltung unterschiedlicher Endgerätetechnologien (neben reinen TETRA-Endgeräten z.B. auch TETRA-Hybridgeräte, Smartphones und Tablets, ggf. mit einer speziellen TETRA-Anwendung) ist nicht frei am Markt verfügbar.

- Es besteht die Notwendigkeit eines einheitlichen Konzepts für Endgeräteupdates (OTA vs. stationär) unter Berücksichtigung der operativ-taktischen und sicherheitstechnischen Anforderungen.
- Die Möglichkeit zur Erkennung und Anzeige von Störungen durch Bereitstellung erweiterter Störungscodes über das Netzwerkmanagement, u. a. mit Referenz zu dem gestörten Element und der räumlichen Ausdehnung, ist wünschenswert.
- Die zu verwaltenden Datenobjekte sind nicht standardisiert.
- Der Zugriff auf Datenobjekte in OS und installierten Apps (API) ist nicht spezifiziert und mit Herstellern abgestimmt.
- 3GPP MCx sieht kein Device Management vor.
- Eine vereinfachte Authentifizierung, z.B. mittels SSO, ist nicht verfügbar.
- Nutzerauthentifizierung muss im Zusammenspiel von Teilnehmermanagement und EMM ermöglicht und umgesetzt werden (sichere und schnelle Authentifizierung der Nutzenden auf Endgeräten und Anwendungen in Einsatzlagen).

5. Bisher identifizierte Forschungsthemen

- Wie könnte eine nicht-proprietäre technologieübergreifende (TETRA, Smartphones, MC-Endgeräte, IoT, sonstige Smart Devices) Endgeräteverwaltung realisiert werden?
- Wie könnte eine zentrale, mandantenfähige Endgeräteverwaltung aufgebaut werden?
- Wie könnten eine Endgeräteverwaltung und eine zentrale übergeordnete Teilnehmerverwaltung integriert werden bzw. zusammenarbeiten?
- Welche datenschutzrechtlichen Probleme könnten durch eine zentrale mandantenfähige Endgeräteverwaltung entstehen und wie wäre sie zu lösen?
- Wie könnte die Authentisierung des Zugriffs auf Endgeräte und Applikationen vereinfacht werden (z. B. SSO)?
- Wie könnte der Lebenszyklus eines BDBOS-gemanagten Breitband-Endgeräts von der Beschaffung bis zur Entsorgung gestaltet sein (unter Berücksichtigung der gegenwärtigen Nutzung kommerzieller Mobilfunknetze, des Phasenmodells der BDBOS und der Nutzung missionskritischer Dienste (MCx nach 3GPP))?
- Wie könnte der Prozess einer zentralen Aktivierung von dienstlichen Endgeräten gestaltet sein (z. B. mittels eSIM/QR-Code und initialer Konfiguration mittels MDM)?
- Wie kann der Zugriff in Endgeräten auf alle benötigten Datenobjekte gewährleistet werden?
- Welche Datenobjekte werden für die Verwaltung handelsüblicher Smartphones für eine einsatzkritische Verwendung benötigt?
- Auf welche Datenobjekte kann in Smartphones mit unterschiedlichen Betriebssystemen bzw. von unterschiedlichen Herstellern zugriffen werden, bzw. wo gibt es für die oben beschriebenen Anforderungen relevante Einschränkungen?
- Welche weiteren Datenobjekte werden für die Verwaltung von MCX-kompatiblen Endgeräten benötigt?
- Welche Rolle könnte MCOP (Mission Critical Open Platform, https://www.mcopenplatform.org/) beim Zugriff auf Datenobjekte spielen?

- Wie könnte die Einführung von MCOP ggf. gefördert werden?
- Gibt es eine Anforderung für die Sicherung und Wiederherstellung kompletter Endgeräte-Konfigurationen (z. B. beim Austausch eines defekten Endgeräts) und wie kann diese realisiert werden?
- Gibt es Anforderungen zur Sammlung statistischer Nutzungsdaten und wie können diese datenschutzkonform umgesetzt werden?
- Gibt es Funktionen, die von 3GPP nicht spezifiziert, aber ggf. mit Unterstützung des OS / MDM realisierbar sind? (z. B. Stun / Ambience Listening)
- Wie kann eine Nutzerauthentifizierung für Einsatzkräfte innerhalb von Einsatzlagen geschaffen werden, ohne die Sicherheit der Daten zu gefährden? Wie kann zudem gleichzeitig ein schneller Zugriff auf das Endgerät sowie die benötigten Applikationen erfolgen (zeitkritisch)?
- Wie kann unter Berücksichtigung der Sicherheits- und Verfügbarkeitsanforderun-gen ein „Bring your own device“-Ansatz, also die Einbindung privater Endgeräte in den breitbandigen Digitalfunk BOS, realisiert werden?