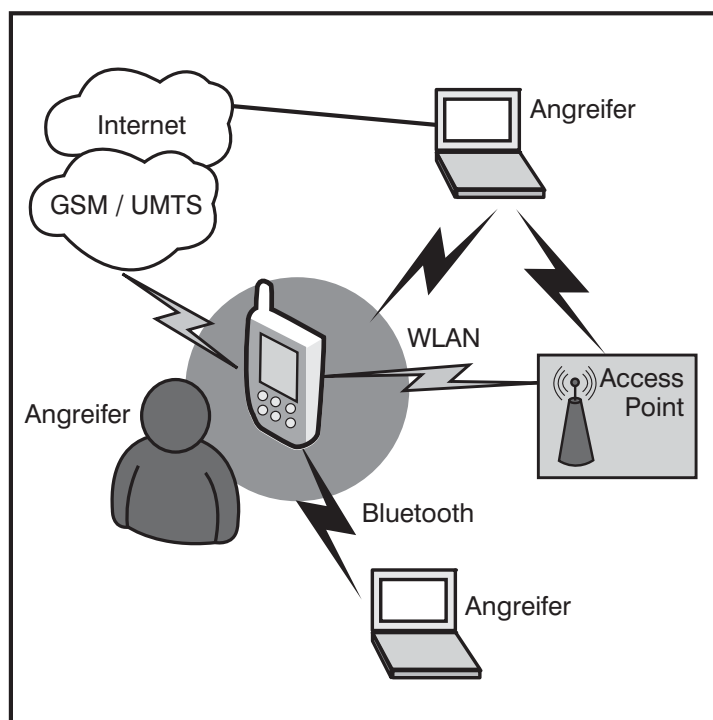


Fixed Mobile Convergence (FMC)

Erreichbarkeit kontra Sicherheit

von Dr. Simon Hoff, Daniel Meinhold, Dr. Michael Wallbaum



Unter Fixed Mobile Convergence (FMC) wird eine Verbindung zwischen einem Festnetz und einem Mobilfunknetz verstanden, die netzübergreifend Leistungsmerkmale zu einem einheitlichen Dienst integriert.

Ein typisches Beispiel ist die Erreichbarkeit unter einer einzigen Rufnummer im

Festnetz und im Mobilfunknetz. Dabei erfolgt eine Anbindung von GSM- bzw. UMTS-Mobiltelefonen an eine lokale TK-Anlage derart, dass der Teilnehmer einerseits am Mobiltelefon unter seiner Festnetznummer erreichbar ist und andererseits auf die vom Festnetzanschluss gewohnten Leistungsmerkmale zurückgreifen kann.

Dieser Artikel beschreibt die für FMC eingesetzten Techniken und betrachtet insbesondere die durch FMC entstehenden Gefährdungen der IT-Sicherheit und analysiert entsprechende Sicherheitsmaßnahmen.

Schwerpunktthema



Dr. Simon Hoff ist technischer Direktor bei der ComConsult Beratung und Planung GmbH und unter anderem verantwortlich für den Bereich IT-Sicherheit. Dr. Hoff blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung und Betrieb in den Bereichen IT-Infrastrukturen, mobiler und drahtloser Kommunikationssysteme zurück.



Dipl.-Inform. Daniel Meinhold ist Consultant bei der ComConsult Beratung und Planung GmbH. Bei ComConsult hat er sich auf Hochverfügbarkeitslösungen im Telekommunikationsumfeld spezialisiert. Im Competence Center Communications, Collaboration, Mobility ist er vor allem für die Konzeption von Telekommunikationslösungen sowie für die Durchführung von Tests und Messungen verantwortlich.



Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.

Fixed Mobile Convergence (FMC) Erreichbarkeit kontra Sicherheit

1. Merkmale einer FMC-Lösung

Eine einheitliche Definition, was man unter FMC versteht und welche Komponenten und Dienste in welchem Umfang dazugehören, existiert nicht. Im Allgemeinen werden jedoch die folgenden Themen mit FMC assoziiert:

- Dienst-Konvergenz (Service Convergence)

Der Benutzer hat Zugriff auf die gleichen Dienste, unabhängig ob er sich in stationären oder mobilen Netzen aufhält.

- Geräte-Konvergenz (Device Convergence)

Der Benutzer benötigt nur ein Endgerät, um sich in verschiedenen Netzen (GSM, UMTS, WLAN, etc.) bewegen zu können.

- Netz-Konvergenz (Network Convergence)

Dieselbe Infrastruktur wird sowohl für

mobile als auch für stationäre Dienste genutzt.

Bisher ist die Regel, dass der Nutzer über mindestens zwei Rufnummern (Festnetz- und Mobilfunknummer), zwei zugehörige Anrufbeantworter und zwei Adressbücher verfügt und je nach Aufenthaltsort unterschiedliche Kommunikationsmittel (Festnetztelefon, Mobiltelefon) verwendet. Teilweise Abhilfe bieten manuell eingerichtete Weiterleitungen bzw. Synchronisierungen zwischen Mobiltelefon und den IT-Systemen des Unternehmens.

Das wesentliche Ziel von FMC ist, dass der Benutzer unter einer einzigen Nummer erreichbar ist und im Büro, Unterwegs oder Zuhause, unabhängig von der jeweiligen Zugangstechnik, auf die gleichen Dienste und Leistungsmerkmale zurückgreifen kann (siehe Abbildung 1).

2. Funktionsweise von FMC-Lösungen

Unter dem Begriff FMC werden unterschiedliche technische Lösungen zusammengefasst, die sich in der Art und Weise der Verbindung der Netze unterscheiden.

Im Wesentlichen gibt es zwei Alternativen:

- Alternative 1: Aufbau einer FMC-Lösung als Ergänzung einer TK-Anlage

In diesem Fall liegt die Verantwortung für das System in der Hand des Unternehmens. Diese Alternative wird auch als Enterprise FMC (eFMC) bezeichnet.

- Alternative 2: Aufbau einer FMC-Lösung als Bestandteil eines GSM/UMTS-Mobilfunknetzes

In diesem Fall liegt die Verantwortung für das System beim Mobilfunkbetreiber (Mobile Network Operator, MNO). Diese Variante wird auch als IMS/FMC oder Carrier FMC bezeichnet und bezieht sich auf die Einführung des IP Multimedia Subsystem (IMS) in die Mobilfunknetze der dritten Generation (d.h. UMTS).

Für diesen Artikel ist primär die erste Alternative wichtig, da hier die unternehmensinterne TK-Infrastruktur im Vordergrund steht. Die zweite Alternative wird im Folgenden trotzdem kurz beschrieben, da

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

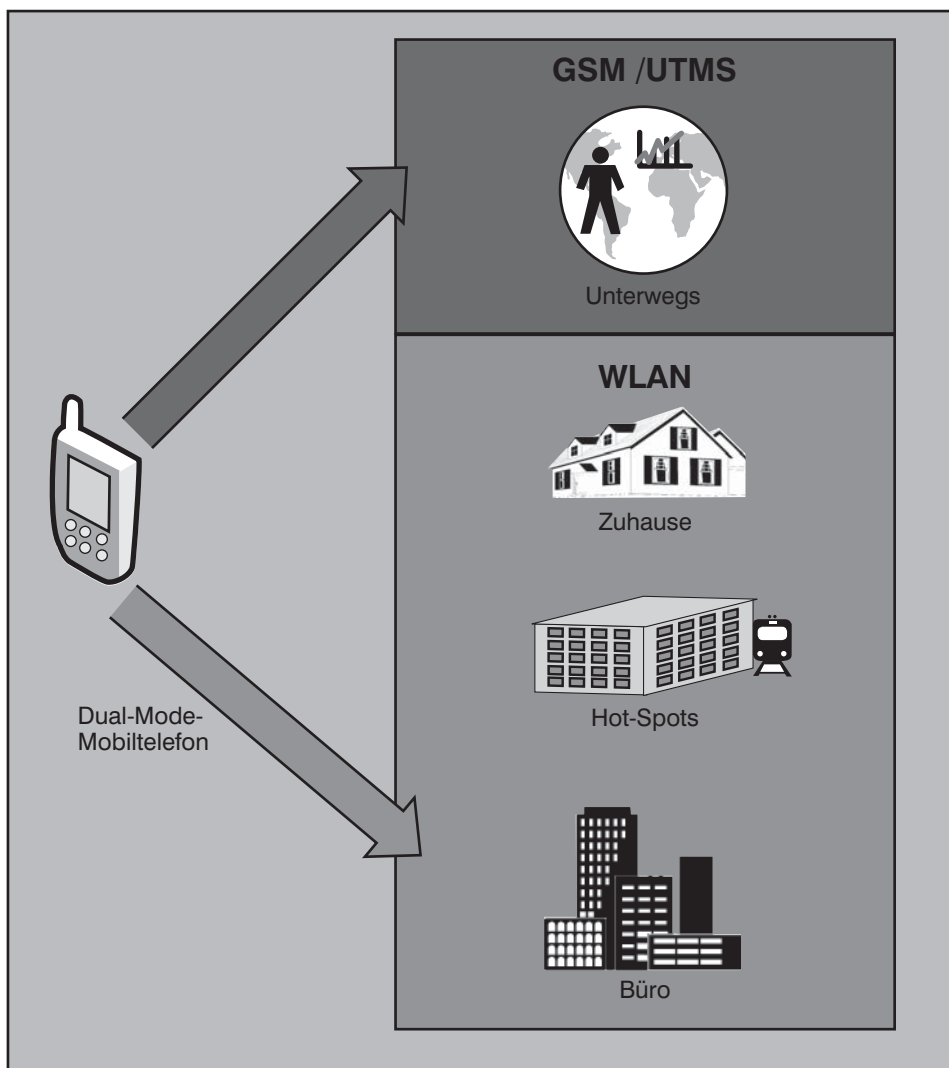


Abbildung 1: Medienübergreifende Erreichbarkeit und Dienstnutzung mit FMC

sie von strategischer Bedeutung für das Zusammenwachsen von Festnetz und Mobilfunknetz ist.

Alternative 1: FMC-Lösung als Ergänzung einer TK-Anlage

FMC-Systeme können mit den in TK-Anlagen bereitgestellten Funktionen realisiert werden. Die entsprechende Steuerungslogik (als FMC Controller bezeichnet) kann als Komponente der TK-Anlage oder in einer separaten Appliance realisiert werden. Aus dem Blickwinkel der TK-Anlage und des Nutzers wird das Mobiltelefon dabei praktisch zu einer weiteren Nebenstelle, d.h. insbesondere, dass Mobiltelefone integraler Bestandteil der TK- bzw. IT-Infrastruktur werden. Das Mobilfunknetz wird als transparentes Kommunikationsmedium verwendet. Für die Bereitstellung von Leistungsmerkmalen dient eine spezielle Software auf dem Mobiltelefon. Grundlegende Funktionen einer FMC-Lösung können auch mit ein-

fachen Mobiltelefonen ohne spezielle Software genutzt werden. Diese Variante wird aufgrund der praktisch nicht verfügbaren Mehrwertdienste im Folgenden nicht genauer betrachtet.

Enterprise FMC-Lösungen können neben den Diensten zur Sprachübertragung auch GPRS zur spezifischen Signalisierung zwischen der Komponente auf dem Mobiltelefon und der TK-Anlage (z.B. Synchronisation von Kontakten) und Messaging-Dienste nutzen.

Ein eingehender Ruf kann parallel sowohl auf dem Festnetztelefon als auch auf dem Mobiltelefon angezeigt werden, wie in Abbildung 2 gezeigt. Nimmt der Teilnehmer das Gespräch beispielsweise auf dem Festnetzapparat an, kann das Gespräch bei vielen Lösungen anschließend „auf Knopfdruck“ an das Mobiltelefon übergeben und dort nahtlos fortgesetzt werden.

Unterstützt das Mobiltelefon zusätzlich eine WLAN-Schnittstelle mit einem VoIP-Client (Softphone), so gestatten es manche FMC-Lösungen, dass sich das Endgerät bei Empfang des heimatischen WLANs automatisch in dieses Netz einbucht und die Sprachkommunikation über WLAN geführt wird. Bewegt sich das Mobiltelefon aus dem Abdeckungsbereich des WLANs hinaus, wird wieder über GSM/UMTS kommuniziert (siehe Abbildung 3). Dabei kann auch eine nahtlose Gesprächsübergabe (Seamless Handover) zwischen WLAN und GSM/UMTS realisiert werden.

Zu den typischen Merkmalen einer Enterprise FMC-Lösung gehören:

- One Number Service / Single Number Reach: Die einheitliche Erreichbarkeit unter einer Rufnummer ist das entscheidende Merkmal einer FMC-Lösung.
- Seamless Roam-In / Roam-Out: In engem Zusammenhang mit dem One Number Service ist die Funktion der automatischen Einbuchung in das bevorzugte Netz (z.B: bei Empfang des heimatischen WLAN) bzw. in ein anderes Netz, das aktuell empfangen wird. Dabei kann ebenfalls die nahtlose (seamless) Übergabe des laufenden Gesprächs an das jeweils andere Medium unterstützt werden. Dies kann automatisch oder manuell erfolgen. Abbildung 4 illustriert eine manuelle Übergabe anhand der FMC-Lösung von Avaya.
- Over the Air Configuration (OTA): Die Konfiguration der Mobiltelefone inklusive der FMC-bezogenen Parameter muss drahtlos über das jeweilig zur Verfügung stehende Medium (per WLAN oder z.B. mit SMS per GSM oder UMTS) erfolgen können. Die Installation und Konfiguration von Programmen und Diensten über SMS-Nachrichten wird in der Mobilfunkwelt allgemein als Over the Air Configuration (OTA) bezeichnet.
- Präsenzinformationen: Gerade in modernen Arbeitsumgebungen, die von (globaler) Mobilität der Nutzer geprägt werden, sind Informationen hinsichtlich der Erreichbarkeit eines Nutzers eine wesentliche Grundlage der geschäftlichen Telekommunikation. Daher bieten FMC-Lösungen oft eine Integration mit Präsenzdiensten.
- Mehrwertdienste: Eine FMC-Lösung, die als Ergänzung einer TK-Anlage realisiert ist, wird die spezifischen Leis-

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

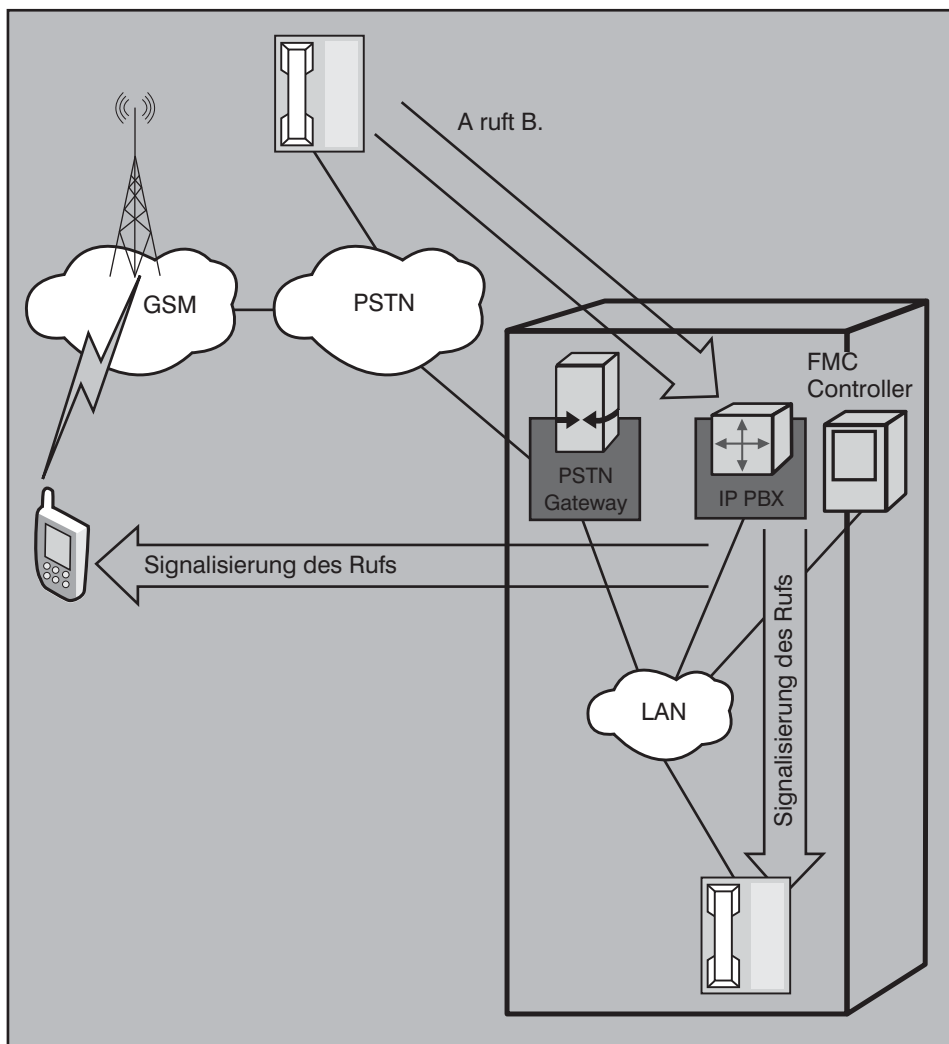


Abbildung 2: Rufvermittlung bei einer Enterprise FMC-Lösung

- Gespräche können unterbrechungsfrei über verschiedene Medien (WLAN, GSM/UMTS) geführt werden (Seamless Handover).
- Aus dem Blickwinkel von TK-Anlage und Nutzer ist das Mobiltelefon eine weitere Nebenstelle geworden.

Alternative 2: FMC-Lösung als Komponente in einem Mobilfunknetz

Eine FMC-Lösung kann auch als Erweiterung eines Mobilfunknetzes realisiert werden, indem über ein spezielles Gateway ein Zugang von einem WLAN zum Mobilfunknetz geschaffen wird. Die Intelligenz hinsichtlich der Bereitstellung, Bearbeitung und Verwaltung von Diensten liegt dann im Mobilfunknetz. Die lokale Komponente (d.h. das WLAN) ist einfach ein weiteres transparentes Trägermedium zur Kommunikation mit einem mobilen Endgerät. In diese Richtung geht ein für GSM/UMTS spezifiziertes, als Generic Access Network (GAN) bezeichnetes, Konzept. GAN ist ursprünglich unter der Bezeichnung Unlicensed Mobile Access (UMA) entwickelt worden, ist aber mit der ersten Veröffentlichung der Spezifikation durch das 3rd Generation Partnership Project (3GPP), das die Spezifikationen für GSM und UMTS erarbeitet, in GAN umbenannt worden.

Kernelement von GANs ist der GAN Controller (GANC), der die Verbindung zum GSM/UMTS-Netz herstellt. Ein Dual-Mode-Endgerät kann gleichzeitig sowohl GSM-Verbindungen als auch WLAN-Technologie nutzen. Bewegt sich ein solches Mobiltelefon in den Bereich eines WLAN, versucht es zunächst eine Verbindung zum WLAN herzustellen, d.h. nach einer Assoziation erfolgt ggf. eine Authentisierung und der Aufbau eines gesicherten Kommunikationskanals mit IEEE 802.11i. Anschließend sucht das Endgerät über das WLAN einen GANC und verbindet sich mit diesem. Der GANC ist seinerseits mit einem GSM/UMTS-Netz verbunden, wie in Abbildung 5 gezeigt. Dem GSM/UMTS-Netz gegenüber verhält sich der GANC wie eine GSM/UMTS-Basisstation. Über den GANC bucht sich das Endgerät dann im GSM/UMTS-Netz ein, als ob es sich über eine normale GSM/UMTS-Funkzelle angemeldet hätte, und kann wie gewohnt die Mobilfunkdienste nutzen. Aus dem Blickwinkel der GSM/UMTS-Infrastruktur befindet sich das Endgerät in einer virtuellen GSM/UMTS-Funkzelle. Bewegt sich das Endgerät während eines Gesprächs aus dem Versorgungsbereich des WLAN heraus, wird ein Handover (Gesprächsübergabe zwischen Funkzellen bzw. Technologien) vom GANC zu einer GSM/UMTS-Basissta-

tungsmerkmale möglichst auch auf Mobiltelefonen zur Verfügung stellen und insbesondere das herstellereigene „Look and Feel“ der kabelbasierten Endgeräte als Anwendung auf dem Mobiltelefon anbieten. Die Leistungsmerkmale beinhalten typischerweise Anrufweiterleitung, Makeln, Konferenzen und die Anwahl von Nebenstellen (Nebenstellenfunktion).

- Zugriff auf Verzeichnisdienste: Von einer FMC-Lösung wird natürlich auch erwartet, dass ein Zugriff auf zentrale Verzeichnisdienste (Corporate Directory) ebenso unterstützt wird, wie auf die in Groupware-Anwendungen verwalteten persönlichen Kontakte.
- Übergreifende Dienste: Im Sinne einer Integration von Festnetz- und Mobiltelefonie ist auch die Bereitstellung übergreifender Dienste als wesentliches Merkmal einer FMC-Lösung zu sehen. Hierzu zählen insbesondere ge-

meinsam genutzte Anrufbeantworter (Sprachmailboxen) sowie ein Anrufjournal für alle Endgeräte eines Nutzers.

Die Eckpunkte einer Enterprise FMC-Lösung bestehen also zusammenfassend aus folgenden Elementen:

- Grundlage ist ein Dual-Mode-fähiges Mobiltelefon (in der Regel mit WLAN- und GSM/UMTS-Schnittstelle).
- Die Bereitstellung von Leistungsmerkmalen erfolgt über eine spezielle Software auf dem Mobiltelefon (FMC-Client).
- Bei Empfang des heimatischen WLAN kann sich das Mobiltelefon automatisch in dieses Netz einbuchen.
- Bewegt sich das Mobiltelefon aus dem Abdeckungsbereich des WLAN hinaus, wird über das Mobilfunknetz kommuniziert.

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

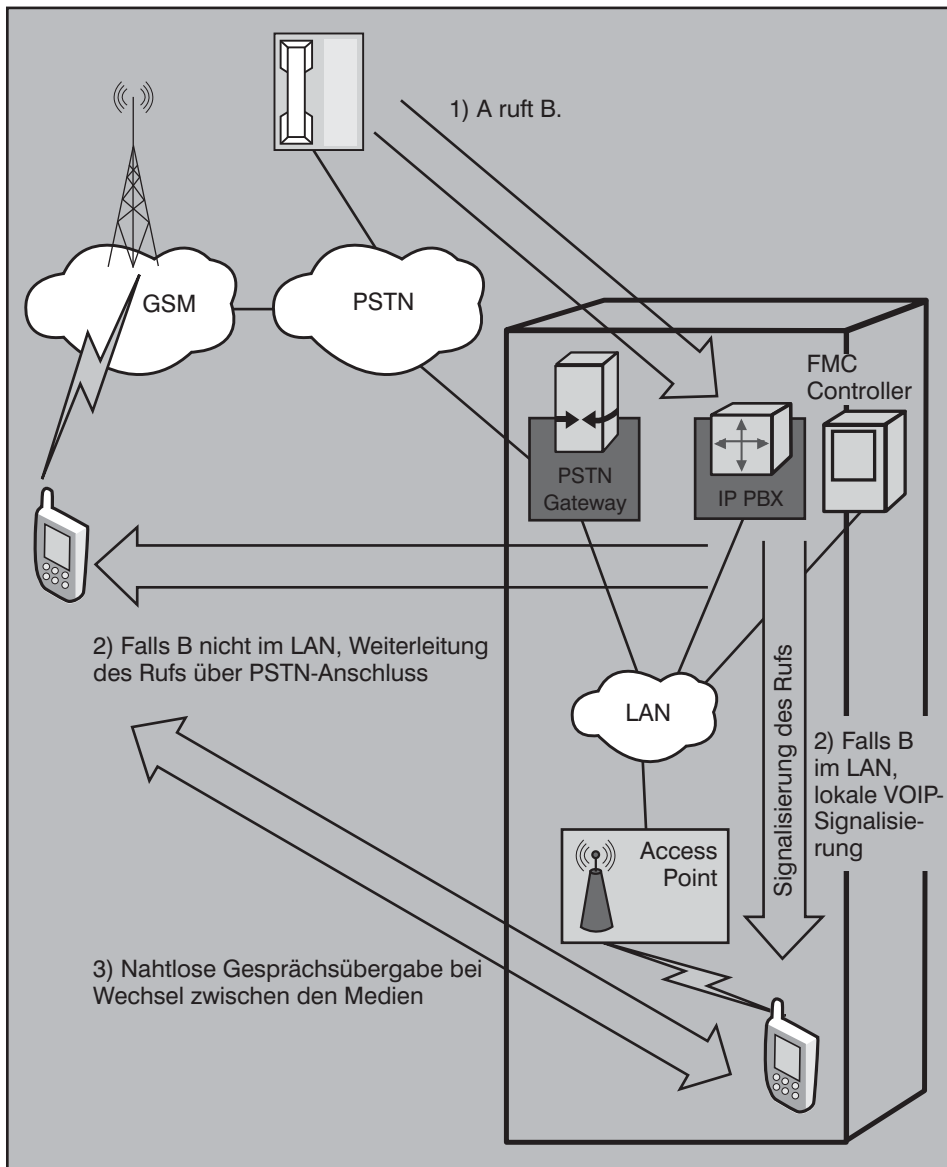


Abbildung 3: Seamless Handover zwischen WLAN und einem Mobilfunknetz

tion durchgeführt.

3. Produkte im Bereich Enterprise FMC
 Nachfolgend wird eine Auswahl an Enterprise FMC-Lösungen betrachtet, um einen Überblick über die aktuelle Marktsituation zu geben:

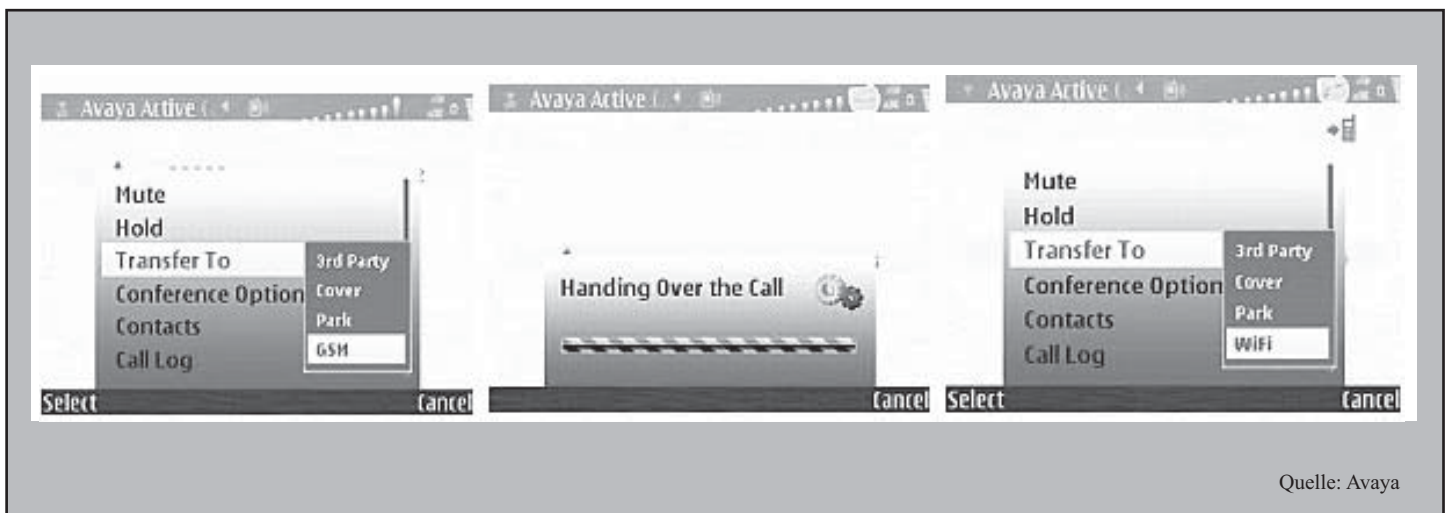
- Alcatel-Lucent Advanced Cellular Extension
- Alcatel-Lucent MyPocket Communicator
- Nokia Intellisync Call Connect
- Comdasy's FMC Serie 2800/3800/4800
- Siemens MobileConnect
- Avaya Extension to Cellular / one-X Mobile
- Cisco Unified Mobility
- Nokia Intellisync Call Connect for Cisco

Neben den unterschiedlichen Varianten, wie eine solche FMC-Lösung realisiert werden kann - ob Software- oder Hardware-basiert - und mit welchen Leistungsmerkmalen, sind insbesondere sicherheitsrelevante Merkmale von Interesse.

Alcatel-Lucent Advanced Cellular Extension

Alcatel-Lucent bietet verschiedene FMC-Lösungsvarianten an. Die erste und einfachste Variante basiert auf einer Nebenstellenfunktion. Das (Single-Mode) GSM-Mobiltelefon wird somit zu einer weiteren Nebenstelle einer bestehenden OmniPCX TK-Anlage. Ermöglicht wird diese Funktionalität durch das Alcatel-Lucent Feature „Advanced Cellular Extension (ACE)“, welches pro Benutzer lizenziert wird und für Geräte mit den Betriebssystemen Windows Mobile und Symbian zur Verfügung steht.

Bei dieser Lösung muss keine zusätzliche Hardware angeschafft werden, wodurch



Quelle: Avaya

Abbildung 4: Manuelle Gesprächsübergabe vom WLAN zum GSM und umgekehrt

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

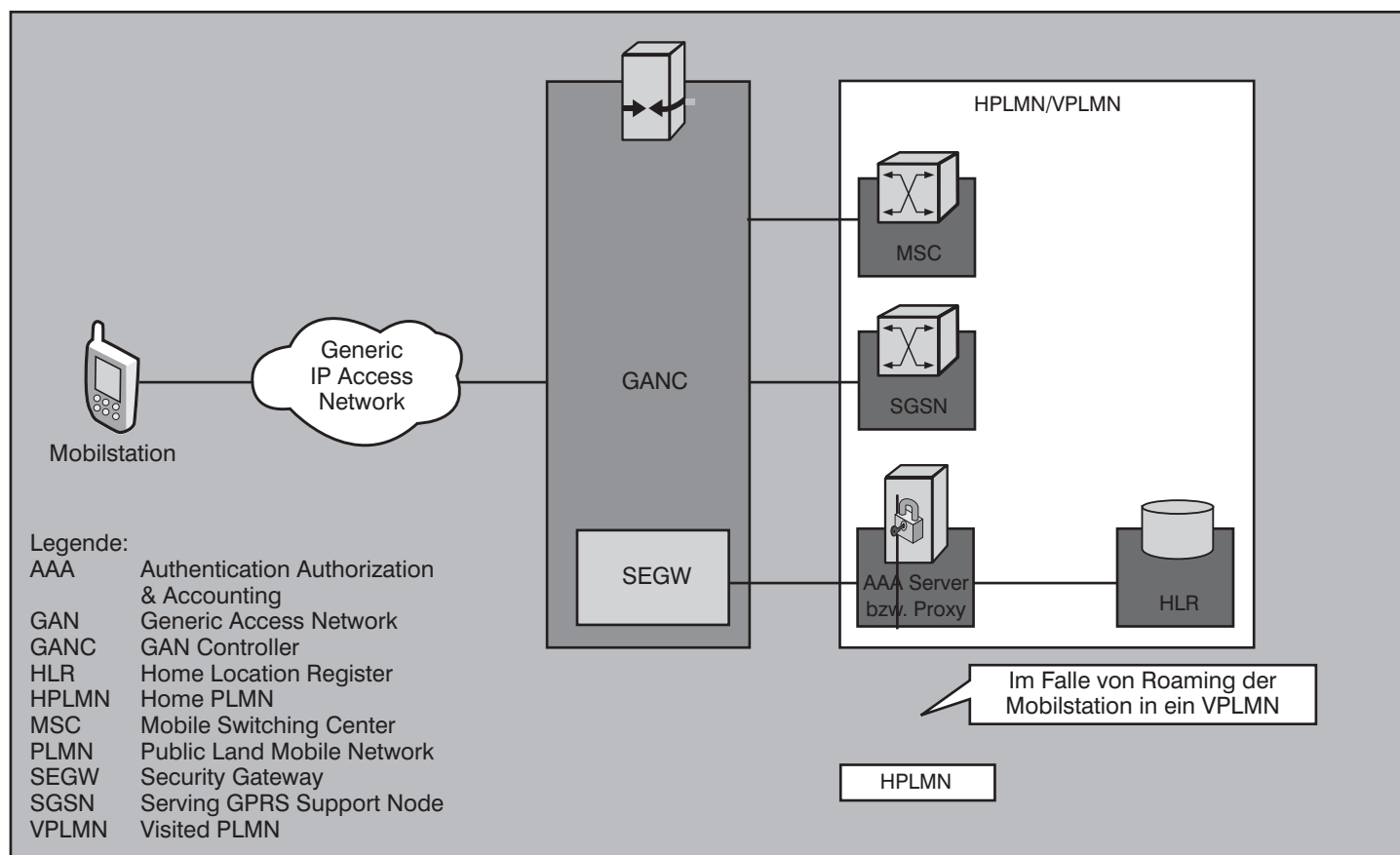


Abbildung 5: Vereinfachte GAN-Architektur

Änderungen an der TK-Infrastruktur entfallen. Allein die zusätzlichen Lizenzen und Änderungen im Betrieb müssen berücksichtigt werden. Advanced Cellular Extension ermöglicht unter anderem die folgenden Leistungsmerkmale:

- Anwahl von Nebenstellen
- Rückruf
- Konferenzgespräche
- Umlegen von Gesprächen (Call Transfer)
- Anrufweiterleitungen
- Benachrichtigung bei Eingang einer Sprachnachricht
- Gleichzeitiges Rufen von Mobil- und Festnetzapparat
- Chef-Sekretär-Funktion

Alcatel-Lucent MyPocket Communicator

Während Advanced Cellular Extension auf Single-Mode-Mobiltelefone abzielt, in diesem Fall GSM, ermöglicht die Software Alcatel-Lucent MyPocket Communicator (MPC) einen Dual-Mode-Betrieb – ein entsprechendes Gerät mit Wi-Fi und GSM-Funktionalität vorausgesetzt.

Der in Abbildung 6 gezeigte MyPocket

Communicator basiert auf der bereits erläuterten Nebenstellenfunktion (Advanced Cellular Extension) einer OmniPCX Enterprise TK-Anlage und benötigt daher ebenfalls keine zusätzliche Hardware. Die Leistungsmerkmale entsprechen daher grundsätzlich den oben aufgeführten Punkten. Zusätzlich wird ein manueller Handover zwischen GSM und WLAN ermöglicht – das Gespräch wird hierfür nicht getrennt. Lizenziert wird die Software auch hier je Benutzer.

Allerdings steht der MyPocket Communicator, im Gegensatz zur ACE-Software, nur auf Windows-basierten mobilen Endgeräten zur Verfügung.

Nokia Intellisync Call Connect

Ein Ergebnis der Zusammenarbeit zwischen Alcatel und Nokia ist die Software „Nokia Intellisync Call Connect for Alcatel-Lucent“. Auf Basis der ACE-Funktion der OmniPCX Enterprise TK-Anlage ermöglicht die Software die Integration von Nokias Mobiltelefonen der E-Serie in eine Alcatel-Lucent-Umgebung. Im Gegensatz zum Alcatel-Lucent MPC ermöglicht die Nokia-Lösung einen Dual-Mode-Betrieb auch für Symbian-basierte Mobiltelefone.

Da die Software auf der Funktion Advanced Cellular Extension aufbaut, gelten auch hier die gleichen Leistungsmerkmale und Funktionen.



Abbildung 6: MyPocket Communicator (Dual-Mode)

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

Für einen Single-Mode-Betrieb muss neben der Nokia-Software die Funktion Advanced Cellular Extension auf einer OmniPCX mit mindestens Version 6.1 bereitgestellt werden.

Für einen Dual-Mode-Betrieb muss zusätzlich die OXE SIP Lizenz vorhanden sein und OmniPCX in Version 8.0.

Comdasys FMC Serie 2800/3800/4800
Die FMC-Lösungen von Comdasys basieren alle auf einer zusätzlichen Hardware-Komponente (FMC Controller), die in drei verschiedenen Ausführungen angeboten wird (alle Angaben gelten inklusive Transcoding und DTMF-Erkennung):

- Comdasys FMC 2800 für bis zu 25 gleichzeitige Gespräche
- Comdasys FMC 3800 für bis zu 80 gleichzeitige Gespräche (siehe Abbildung 7)
- Comdasys FMC 4800 für bis zu 500 gleichzeitige Gespräche

Als Betriebssystem kommt auf allen Systemen Linux zum Einsatz. Die Anbindung der Komponenten erfolgt via Session Initiation Protocol (SIP) an eine bestehende TK-Anlage und ist damit prinzipiell unabhängig von der eingesetzten TK-Lösung. Alle drei Varianten (2800, 3800, 4800) unterstützen:

- OSPF, BGP, RIPv2
- GRE-Tunnel
- Umfangreiche Werkzeuge zur Verkehrskontrolle (Token Bucket, Stochastic Fairness Queuing, Diffserv mark, etc.)

Am auffälligsten ist die weitgehende Unterstützung von Sicherheitsfunktionen, die auch dem erhöhten Schutzbedarf gerecht wird. Neben einer Firewall in Form eines dynamischen Paketfilters und einer Administration via SSH werden unter anderem die folgenden VPN-Funktionen dargeboten:

- VPN-Typ: IPsec, L2TP over IPsec und OpenVPN
- Verschlüsselungsalgorithmen: AES (bis zu einer Schlüssellänge von 256 Bit), 3DES, IDEA (128 Bit), Blowfish (variable Schlüssellänge)
- Authentisierung: X.509-kompatible Zertifikate (IPsec und OpenVPN), Pre-shared Keys



Abbildung 7: Comdasys FMC 3800, Quelle: Comdasys

Zusätzlich stehen folgende VoIP-spezifische Sicherheitsfunktionen zur Verfügung:

- SIP / TLS zur Absicherung der Signalisierung und
- SRTP zur Absicherung des Medienstroms

Client-seitig kommt der in Abbildung 8 gezeigte Comdasys MC Client zum Einsatz, den es ebenfalls – wie bei der Alcatel-Lucent/Nokia-Lösung in zwei Ausführungen gibt: Single-Mode (nur GSM) und Dual-Mode (GSM und WLAN).

Neben den Standardfunktionen wie der Erreichbarkeit unter einer einzigen Nummer (Single Number Reach) und einem nahtlosen Handover zwischen GSM/CDMA/UMTS und WLAN ermöglicht der Client auch Instant Messaging (IM), Präsenz (beides auf Basis von XMPP) und SMS via WLAN. Der MC Client steht sowohl für Symbian-basierte Endgeräte als

auch Windows Mobile 5 und 6 zur Verfügung.

Siemens MobileConnect
Siemens bietet im Bereich FMC das Produkt Siemens HiPath MobileConnect an. Auch hier handelt es sich um eine SIP-kompatible Client-Server-Lösung bestehend aus der Hardware-Komponente Siemens HiPath MobileConnect und dem zugehörigen HiPath MobileConnect-Client für Dual-Mode-Geräte. Eine Single-Mode-Version ist derzeit nicht verfügbar. Der MobileConnect-Client unterstützt sowohl Windows Mobile 5.0 als auch Symbian in Version 9.1.

Ähnlich zur Lösung von Comdasys (einem Technologie-Partner von Siemens) wird das Siemens-System in verschiedenen Ausbaustufen angeboten, die sich in der maximalen Anzahl der Benutzer und der gleichzeitig geführten Gespräche unterscheiden.

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit



Abbildung 8: Comdasys MC Client

Siemens MobileConnect unterstützt neben den klassischen FMC-Merkmalen

- One-Number-Konzept
- Anwahl von Nebenstellen inkl. Anzeige der Festnetzziffern bei abgehenden Gesprächen aus dem Mobilfunknetz heraus und
- nahtloser Handover zwischen Mobilfunk und WLAN

auch weitergehende Leistungsmerkmale der TK-Anlage. In Kombination mit der Siemens HiPath 8000 werden unter anderem nachfolgende Leistungsmerkmale angeboten:

- Anklopfen
- Rufweiterschaltung
- Anrufer-ID
- Rückruf bei besetzt/frei
- Anruf makeln/übergabe
- Dreierkonferenz
- Automatische Wegesuche (LCR)
- Halten
- Chef/Sekretär-Funktion
- Serielles und paralleles Rufen

Ob und in welchem Umfang die bereitgestellten Leistungsmerkmale mit fremden SIP-kompatiblen TK-Anlagen funktionieren, sollte - wie bei allen Herstellern - im Einzelfall überprüft werden.

Wie auch das Comdasys-System unterstützt das System die Routing-Protokolle OSPF, BGP, RIPv2, GRE-Tunnel und umfangreiche Werkzeuge zur Verkehrskontrolle. Hinzu kommen die Möglichkeiten einer VPN-Terminierung – einen Un-

terschied gibt es jedoch: Laut Datenblatt unterstützen die Comdasys-Plattformen bereits SIP/TLS und SRTP, während diese Funktionen bei Siemens derzeit noch nicht aufgeführt sind. Aufgrund der Ähnlichkeiten ist zu erwarten, dass beide Systeme auf der gleichen Plattform basieren und zumindest SIP/TLS und SRTP in Zukunft auch bei der Siemens-Lösung zu finden sind.

Avaya Extension to Cellular / one-X Mobile

Wie auch bei Alcatel-Lucent basiert die FMC-Lösung von Avaya auf einer softwarebasierten Lösung; Voraussetzung ist eine Avaya TK-Anlage (Avaya Communication Manager). Der Ausgangspunkt ist auch hier eine Zusammenführung von Nebenstelle und Mobiltelefon, was bei Avaya unter der Bezeichnung „Extension to Cellular“ bzw. Nebenstelle-zu-Mobiltelefon-Funktion zu finden ist. Diese muss für jeden FMC-Nutzer im Avaya Communication Manager lizenziert sein.

Avaya bietet eine umfangreiche Palette an FMC-Clients (Avaya one-X Mobile), unter anderem für folgende Systeme:

- Symbian (Single- und Dual-Mode)
- Windows Mobile
- RIM
- Palm
- Java
- iPhone

Allerdings stehen nicht alle Funktionen auch auf allen Plattformen zur Verfügung. Beispielsweise wird ein nahtloser Han-

dover zwischen WLAN und GSM nur mit Symbian angeboten.

Neben den grundlegenden Leistungsmerkmalen stehen auch bei Avaya erweiterte Leistungsmerkmale der TK-Anlage zur Verfügung, sofern der Teilnehmer für diese freigeschaltet ist. Hierzu zählen bei Avaya beispielsweise:

- Automatischer Rückruf
- Anrufweiterleitung
- Anruf Parken
- Anrufübernahme
- Anrufer-ID Anzeigen/Ausblenden
- Alle Anrufe Weiterleiten

Cisco Unified Mobility

Die FMC-Lösung von Cisco wird unter dem Schlagwort Cisco Unified Mobility vermarktet und besteht im Wesentlichen aus einem Dienst der eine Cisco Telefonie-Infrastruktur voraussetzt. Für die Versionen 4.x und 5.x des Cisco Unified Communications Managers (CUCM) wird für Unified Mobility ein dedizierter Cisco 7800 Series Media Convergence Server (MCS) benötigt. Mit der Version 6.0 ist der MobilityManager im CUCM integriert, d.h. es wird kein zusätzlicher Server benötigt.

Im Einzelnen unterstützt Unified Mobility folgende Leistungsmerkmale:

- Mobile Connect: Anrufsignalisierung und -annahme an allen mit einer Rufnummer verknüpften Endgeräten, d.h. insbesondere auch an mobilen Endgeräten

Jetzt Leser werden

Der Netzwerk Insider



Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

- Endgerätewechsel: Wechsel des Endgerätes im Laufenden (Mobile Connect) Gespräch, z.B. kann ein Gespräch per Tastendruck von einem Festnetztelefon auf ein mobiles Endgerät umgelegt werden.

Das ganze System ist - im Unterschied zu Comdasy/Siemens - eine geschlossene Lösung, die nur in Kombination mit dem CUCM funktioniert.

Je nach Ausbaustufe der Appliance (MCS Server) unterstützt der MobilityManager maximal 300 Benutzer (MCS 7815, CUCM Server) bis hin zu 4500 Benutzern bei Verwendung eines Clusters aus drei MobilityManager-Servern in Kombination mit einem CUCM-Cluster.

Aufbauend auf dieser Infrastruktur wird die eigentliche FMC-Funktionalität unter dem Namen Cisco Mobile Connect angeboten, die entsprechend für jeden Nutzer zu lizenzieren ist. Dabei ist zu beachten, dass es sich um keine Dual-Mode-Lösung samt FMC-Client handelt, sondern primär geht es um die Erreichbarkeit unter einer Rufnummer, was sich auch in der Terminologie widerspiegelt. So wurde das Produkt von SNR (Single Number Reach) in Cisco Unified Mo-

bilityManager umbenannt. Entsprechend eingeschränkt, im Vergleich zu den anderen Lösungen, ist auch der Funktionsumfang.

Nokia Intellisync Call Connect for Cisco

Ebenso wie Alcatel-Lucent kooperiert auch Cisco im Bereich der Dual-Mode-Funktionalität mit Nokia, womit auch bei Cisco eine Nutzung von WLAN und GSM einschließlich manuellem Handover ermöglicht wird. Das Ergebnis dieser Kooperation lautet Nokia Intellisync Call Connect for Cisco (aktuell in Version 1.1). Die Symbian-Applikation gibt es für die folgenden Systeme:

- Nokia E51
- Nokia E60 (PR3)
- Nokia E61 (PR3)
- Nokia E61i
- Nokia E65

Serverseitig werden die folgenden Cisco-Systeme unterstützt:

- Cisco Unified Communications Manager 4.1x, 4.2, 5.x, 6.x
- Cisco Unified Communications Mana-

ger Express 4.1

- Cisco Unified Communications 500 Series for Small Business

Somit sind auch Leistungsmerkmale wie die Anwahl von Nebenstellen, Halten, Weiterleiten (mit und ohne Rücksprache), Konferenzen (max. fünf Teilnehmer), Parken oder MWI (via SMS) über eine grafische Benutzeroberfläche auf Nokia-Modellen der E-Serie zusammen mit Cisco möglich.

4. Gefährdungen durch FMC

Begleitend mit dem Gewinn durch die verbesserte Erreichbarkeit resultiert aus der Zusammenführung von Diensten und Schnittstellen auch eine spezifische Gefährdungslage durch die Verwendung von FMC.

Gefährdungen: Mobiles Endgerät

Eine besondere Rolle spielt das mobile Endgerät, das als Dual-Mode-Gerät simultan über WLAN und über GSM/UMTS eine Netzverbindung unterhält. Über WLAN ist das Gerät ein Teilnehmer der lokalen Infrastruktur, und über GSM/UMTS können gleichzeitig nicht nur Sprachver-

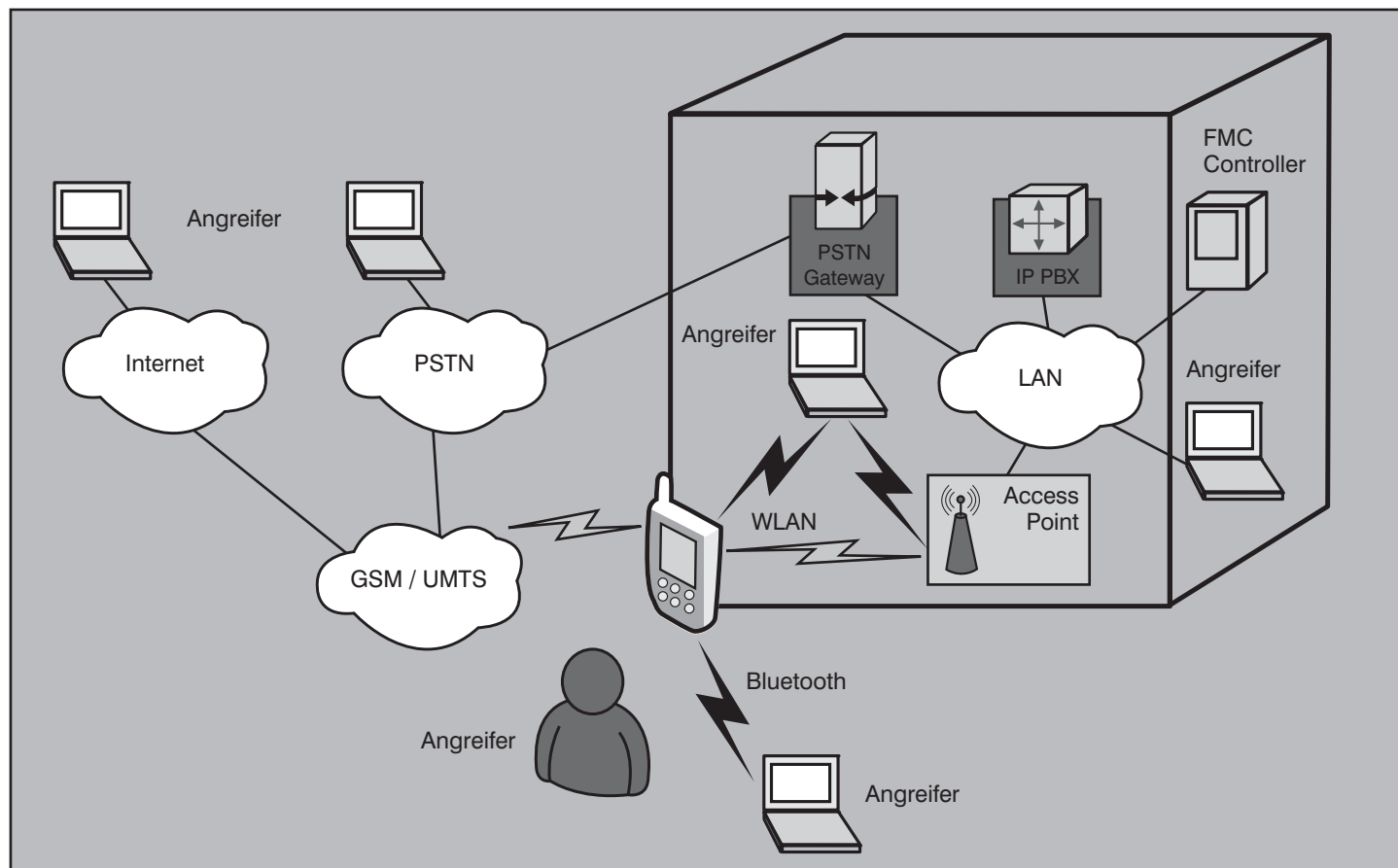


Abbildung 9: Gefährdungen des mobilen Endgeräts

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

bindungen sondern insbesondere auch beliebige Datenverbindungen über das Internet geöffnet werden. Das Mobiltelefon mutiert so zum Koppellement zwischen LAN-Infrastruktur und Internet, einer Rolle, die eigentlich nur ausgesprochen abgesicherten Netzelementen wie Firewalls vorbehalten ist. Erschwerend kommt hinzu, dass mit Bluetooth typischerweise noch eine weitere angreifbare Schnittstelle präsent ist (die in der Vergangenheit zumindest hinsichtlich verschiedener Implementierungen deutliche Schwächen gezeigt hat).

Durch diese Rolle des mobilen Endgeräts besteht unmittelbar die Gefahr, dass ein mobiles Endgerät als Transportwirt für eine schadenstiftende Software fungiert. Dabei geht es zunächst weniger um die potentielle Infektion des mobilen Endgeräts, sondern über die direkte Internet-Verbindung des mobilen Endgeräts kann eine schadenstiftende Software auf das Endgerät geladen werden, die beispielsweise im Rahmen eines Synchronisationsvorgangs über eine andere Schnittstelle in die weitere Infrastruktur getragen wird.

Natürlich können durch schadenstiftende Software mobile und drahtlose Systeme auch selbst betroffen werden und derart gestört werden, dass die eigentliche Applikation der Telekommunikation nur noch unzureichend nutzbar ist. Beispielsweise startet das Gerät nach einer Infektion nicht mehr oder man kann nicht mehr telefonieren oder das Telefonbuch wird gelöscht usw. Darüber hinaus gibt es für mobile Endgeräte zusätzliche Möglichkeiten einer Infektion über unterschiedliche Kommunikationsschnittstellen (Bluetooth, lokaler Angriff über WLAN, Internet via WLAN, Internet via GPRS). Trojanische Pferde sind mittlerweile auch für PDAs und Smartphones vorhanden. Computer-Viren sind für Spezialbetriebssysteme für Mobiltelefone, PDAs und Smartphones aber auch für Windows Mobile zwar noch nicht verbreitet, jedoch ist eine steigende Tendenz erkennbar.

Vereinfacht wird die Infektion durch ein fehlendes oder nicht genutztes Berechtigungskonzept. In der Regel ist der Benutzer zugleich der Administrator, wodurch die Installation von Fremdsoftware und Manipulation bestehender Software keinen Restriktionen unterworfen ist. Signierte Software findet sich nicht bei allen Herstellern, speziell im Bereich privat genutzter bzw. entwickelter Software, so dass die Überprüfung der Signaturen häufig deaktiviert wird.

Weiterhin sind mobile Endgeräte besonders dadurch gefährdet, dass sie einerseits leicht zu transportieren sind, oft die gleichen (sensiblen) Daten (Texte, Tabellen, Zeichnungen, E-Mails, ...) wie auf dem Bürorechner transportieren können und in der Regel über schwächere Sicherheitsmechanismen verfügen als PCs.

Moderne Mobiltelefone und Smartphones sind aufgrund dieser Gefährdungen wie mobile PCs und mobile Datenträger einzustufen.

Gefährdung: LAN, WLAN und VoIP-Infrastruktur

Weitere Gefährdungen zielen auf die WLAN-Kommunikation ab. Unternehmensintern liegt die Verantwortung der Absicherung der WLAN-Infrastruktur beim Unternehmen selbst. Wird das mobile Endgerät, z.B. ein Smartphone, jedoch an öffentlichen WLAN-Zugangspunkten (Hot Spots) genutzt, obliegt die Sicherheit der WLAN-Infrastruktur beim Anbieter des Zugangspunktes und ist damit prinzipiell als nicht vertrauenswürdig einzustufen.

Gefährdungen aufgrund von vorsätzlichen Handlungen bzgl. Access Points sind beispielsweise:

- Beabsichtigte Störung des Funknetzes
- Abhören der WLAN-Kommunikation
- Unerlaubte Mitnutzung des WLAN
- Angriffe auf Access Points und die dahinterliegende Infrastruktur
- Vortäuschung eines gültigen Access Point

Außerdem bestehen grundsätzlich auch Gefährdungen im Bereich der VoIP-Infrastruktur, insbesondere hinsichtlich DoS und des Abhörens der Sprachkommunikation, da der FMC-Client auf dem mobilen Endgerät zugleich als Softphone fungiert.

Für ausführliche Informationen zur Gefährdungslage in WLAN und in VoIP-Systemen sei hier auf die einschlägigen Veröffentlichungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) verwiesen.

5. Maßnahmen zur Absicherung einer FMC-Lösung

Im Folgenden wird eine Auswahl an Sicherheitsmaßnahmen aufgeführt, die illustrieren, wie den oben aufgeführten Gefährdungen begegnet werden kann. Die Maßnahmen lassen sich grob in folgende Bereiche unterteilen:

- Maßnahmen zur Absicherung der Endgeräte
- Maßnahmen auf Ebene der Server und Anwendungen
- Maßnahmen im Bereich des Netzwerks
- Maßnahmen zum Netz- und Systemmanagement

5.1 Maßnahmen Endgeräte

Härtung des Endgeräts

Ein wichtiges Element zum Schutz vor Gefährdungen, die das Endgerät betreffen, ist die Deaktivierung von nicht benötigten bzw. sicherheitskritischen Funktionen, um die Angriffsfläche möglichst gering

Jetzt Leser werden



Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

zu halten. Die verbliebenen Schnittstellen, Dienste und Leistungsmerkmale sollten nur bei Bedarf aktiviert und weitestgehend abgesichert werden. Dies trifft insbesondere auf mobile Endgeräte zu, die über mehrere Kommunikationsschnittstellen verfügen (z.B. GSM/UMTS, Bluetooth, WLAN).

Absicherung der Kommunikationsschnittstellen

Während der Nutzer praktisch keinen Einfluss auf die Absicherung der GSM/UMTS-Funkschnittstelle besitzt, welche automatisch über die in den GSM/UMTS-Standards spezifizierten Mitteln abgesichert wird, obliegt ihm dennoch die Absicherung der WLAN- und Bluetooth-Schnittstelle. Bezüglich der Absicherung der WLAN-Kommunikation sei auf das folgende Kapitel zu den Maßnahmen im Bereich des Netzwerks verwiesen sowie auf die „Technische Richtlinie Sicheres WLAN“ des BSI bzw. auf den Baustein WLAN der BSI IT-Grundschutz-Kataloge. Für eine Absicherung der Bluetooth-Schnittstelle kann beispielsweise die Informationsschrift „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ des BSI zu Rate gezogen werden.

Absicherung von gespeicherten Daten

Um einen Datenverlust, insbesondere von sensiblen Daten, zu verhindern, sollten nach Möglichkeit erst gar keine Daten mit erhöhtem Schutzbedarf auf dem Endgerät gespeichert werden. Die Praxis zeigt immer wieder, dass auch bei Vorhandensein einer Sicherheitslösung, aufgrund von Termindruck oder einer zu komplexen Bedienung, auf diese verzichtet wird und die Daten somit ungesichert auf dem mobilen Endgerät abgelegt werden.

Aus diesem Grund sollten nach Möglichkeit alle Daten auf dem Mobiltelefon verschlüsselt abgelegt werden, sowohl Daten auf dem internen Speicher als auch auf separaten Speicherkarten. Wichtig ist auch hier, dass die Nutzer über die Risiken aufgeklärt werden. Somit sind organisatorische Regelungen für den Umgang mit Daten auf mobilen Endgeräten ein essentieller Bestandteil eines Sicherheitskonzepts für FMC.

Sperrung des Mobiltelefons für Nutzereingaben

Eine effektive Maßnahme, um einen Missbrauch des mobilen Endgeräts zu verhindern, ist eine Sperrung bei Nichtbenutzung. Im Idealfall wird diese nach einem einstellbaren Zeitintervall automatisch aktiv, sollte jedoch im Bedarfsfall auch manuell aktiviert werden können. Bei einem gesperrten Gerät steht nur ein einge-



Abbildung 10: Automatische Sperrung des mobilen Endgerätes (Quelle: Microsoft, Windows Mobile 6)

schränkter Dienstumfang (Annahme von Rufen, Absetzen von Notrufen) zur Verfügung. Zum Entsperren muss der Nutzer sich am Endgerät entsprechend authentisieren, beispielsweise durch eine PIN.

Auch hier sollte der Benutzer entsprechend aufgeklärt und mit der Nutzung dieser Funktion vertraut gemacht werden. Diese Sperre sollte zusätzlich auch erzwungen werden können, so dass der Nutzer diese nicht manuell aus Komfortgründen deaktiviert.

Schutz vor schadenstiftender Software

Wie bei den Gefährdungen bereits erläutert, besteht auch für Handys, Smartphones und PDAs eine zunehmende Gefahr durch schadenstiftende Software (z.B. Viren, Würmer, Trojaner und Spyware), die einerseits das Gerät unbrauchbar machen kann aber auch – trotz Verschlüsselung – zum Abhören genutzt werden kann. Da das mobile Endgerät in einer FMC-Lösung integraler Bestandteil der IT-Infrastruktur wird und universell Dienste und Anwendungen unterstützt, ist der Einsatz einer entsprechenden Schutzsoftware dringend angeraten. Allerdings liegen Produktverfügbarkeit und Funktionsumfang noch deutlich hinter dem Stand der entsprechenden Schutzsysteme für PCs zurück.

Schutzmaßnahmen für das Herunterladen von Inhalten

Um ein Einfallstor für schadenstiftende Software zumindest einzuschränken, sollten Maßnahmen für das Herunterladen von Inhalten (Applikationen, MMS, Be-

such von Webseiten) ergriffen werden. Dazu gehört beispielsweise auch, dass eine Verbindung über das Internet nur nach Bestätigung durch den Nutzer aufgebaut werden darf. Eine Ausnahme bilden geeignet authentifizierte Computer, die dem Vertrauensbereich der lokalen IT-bzw. TK-Infrastruktur zugeordnet sind und zu denen eine verschlüsselte Verbindung aufgebaut wird.

Weiterhin sollte das mobile Endgerät so konfiguriert werden, dass eine Bestätigung durch den Nutzer vor dem Herunterladen von Inhalten (inklusive MMS) erforderlich ist. Beim Zugriff auf aktive Inhalte können grundsätzlich die für andere Endgerätetypen (PCs) festgelegten Schutzmaßnahmen sinngemäß auch auf mobile Endgeräte übertragen werden.

5.2 Maßnahmen Server und Anwendungen

Neben den Maßnahmen zur Absicherung der Endgeräte gilt es auch deren Endpunkte sowie die Kommunikation zwischen beiden abzusichern. Eine Auswahl von Maßnahmen wird im Folgenden kurz dargestellt.

Authentisierung zwischen Endgerät und Server

Je nach FMC-Variante, ob als Erweiterung einer bestehenden TK-Anlage oder als Dienst des Mobilfunkbetreibers, sollte eine gegenseitige Authentisierung zwischen mobilem Endgerät und der jeweiligen zentralen Komponente (FMC Controller) stattfinden. Erst anschließend sollte der Nutzer die Dienste des FMC-Systems in Anspruch nehmen dürfen.

Für die Authentisierung kommen beispielsweise zertifikatsbasierte Verfahren in Betracht.

Erwähnenswert ist in diesem Zusammenhang die GAN-Lösung, die ja FMC als Erweiterung eines Mobilfunknetzes realisiert. Die Absicherung in GAN erfolgt über IPsec (siehe Abbildung 11), und für den Aufbau der IPsec Security Association (SA) zwischen Mobilstation und GANC des Mobilfunkbetreibers wird im Rahmen des Schlüsselaustauschs eine gegenseitige Authentisierung von Mobilstation und GANC durchgeführt. Diese Authentisierung erfolgt über das Extensible Authentication Protocol (EAP) entweder mit der Methode EAP-SIM für GSM oder EAP-AKA für UMTS. Konzeptionell ist dieser Ansatz durchaus als vorbildlich zu bezeichnen. In der Praxis begegnen einem GAN-basierte Lösungen allerdings noch recht selten. Erste Netzbetreiber bieten aber bereits Dienste basierend auf GAN an

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

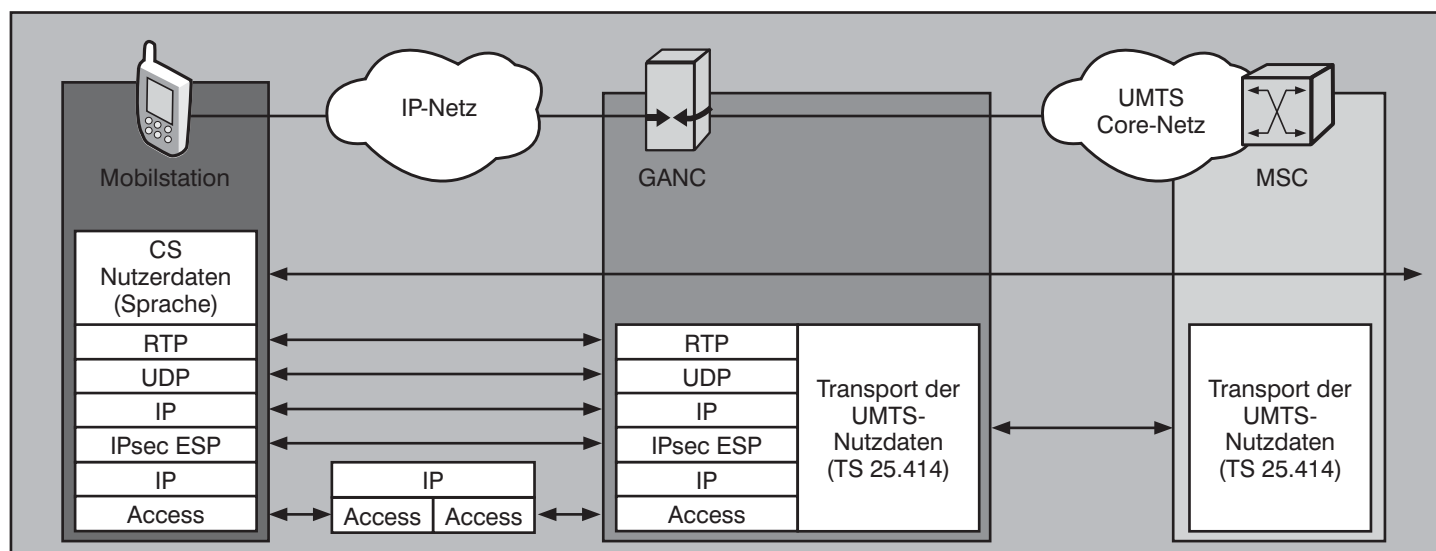


Abbildung 11: Protokoll-Stack für die Sprachübertragung über GAN (vereinfacht)

(beispielsweise T-Mobile in den USA mit HotSpot@Home) und diverse Smartphones unterstützen GAN (etwa BlackBerry 8820).

Absicherung der zentralen FMC-Komponenten

Der FMC Controller muss einen Zugriff der mobilen Endgeräte gestatten. Hierzu ist diese zentrale Komponente zu härten und der Zugang entsprechend zu kontrollieren. Die Anbindung sollte über Sicherheits-Gateways (je nach Sicherheitsanforderungen eine Kombination aus Firewalls, Application Layer Gateways und Intrusion-Prevention-Systemen) erfolgen.

Verwendung einer Ende-zu-Ende-Verschlüsselung

Bei erhöhtem Schutzbedarf ist generell der Einsatz einer Ende-zu-Ende-Verschlüsselung zwischen den beteiligten Endgeräten bzw. zwischen dem mobilen Endgerät und einem Gateway im Sicherheitsbereich der privaten lokalen TK-Anlage erforderlich. Dies gilt sogar unabhängig davon, ob ein Endgerät gerade über GSM/UMTS oder WLAN verbunden ist.

Empfohlen wird hierbei der Einsatz von AES als Verschlüsselungsalgorithmus mit mindestens 128 Bit Schlüssellänge und ein dynamisches Schlüsselmanagement z.B. basierend auf Zertifikaten oder dem Diffie-Hellman-Verfahren. Für die Übertragung der Sprachdaten in IP-basierten Netzen wird der Einsatz von SRTP angeraten.

Sofern sich die Anforderung ergibt, eine Ende-zu-Ende-Verschlüsselung auch im Mobilfunknetz einzusetzen, ist man in der Regel auf eine spezielle Software angewiesen, welche auf allen Endgeräten, die

untereinander verschlüsselt kommunizieren wollen, eingerichtet wird. Anschließend können sowohl Sprach- als auch Datenübertragungen (z.B. Kurznachrichten) verschlüsselt über den Datenkanal des Mobilfunknetzes übertragen werden. An dieser Stelle müssen praktisch alle aktuell verfügbaren FMC-Produkte passen und für den erhöhten Schutzbedarf die Gesamtlösung dediziert durch Produkte dritter Hersteller ergänzt werden.

5.3 Maßnahmen Netzwerk

Die Maßnahmen, die im Netzwerk für die Absicherung einer FMC-Lösung umgesetzt werden sollten, sind eher allgemeiner Natur und betreffen primär die WLAN-Übertragung und die Integration des WLAN in die LAN-Infrastruktur.

WLAN-Übertragung

Die Absicherung der WLAN-Übertragung sollte unter Verwendung von IEEE 802.11i möglichst mit CCMP (d.h. WPA2) erfolgen. Weiterhin sollte im Enterprise-Bereich mit IEEE 802.1X über eine sichere EAP-Methode (beispielsweise über EAP-TLS oder EAP-FAST) authentisiert werden.

Eine solche Authentisierung kann allerdings bei einem Handover während eines Telefonats zu einer kurzzeitigen aber dennoch spürbaren Leistungseinbuße führen. Die Verwendung eines Controller-basierenden WLAN-Designs kann diese Leistungsbeeinträchtigung mildern. Langfristig wird hier der noch in Arbeit befindliche Standard IEEE 802.11r eine besondere Rolle übernehmen, da dieser Standard eine für die Mobilität der Endgeräte optimierte Schlüsselverwaltung realisiert, die eine Neuauthentisierung bei einem Zellwechsel

innerhalb einer Mobility Domain überflüssig macht.

In kleineren WLANs, in denen nur eine geringe Anzahl von WLAN-Stationen zu verwalten ist, können natürlich Pre-Shared Keys (d. h. WPA2-Personal bzw. WPA-Personal) eingesetzt werden, sofern die zugrundeliegende Passphrase eine genügend hohe Komplexität aufweist.

Weiterhin muss berücksichtigt werden, dass die WLAN-Funkzellen so geplant werden, dass die WLAN-Ausleuchtung den Anforderungen einer Sprachübertragung hinsichtlich Mobilität und Verfügbarkeit gerecht wird. Sofern das WLAN auch für andere Anwendungen genutzt wird, sollte außerdem durch den Einsatz von Wi-Fi Multimedia (WMM) bzw. IEEE 802.11e sichergestellt werden, dass die Sprachkommunikation gegenüber anderen Anwendungen auf dem gemeinsam genutzten Funkmedium bevorzugt übertragen wird.

Trennung von LAN und WLAN

Das WLAN muss durch ein Sicherheitssegment von der LAN-Infrastruktur entkoppelt werden. Typischerweise kommt hier eine VoIP-taugliche Firewall und ggf. ein Intrusion Prevention System zum Einsatz. Die Trennung der beiden Netzbereiche kann dann auf logische Weise mittels Controller-basierendem Design (d.h. über IP-Tunnel) oder beispielsweise über VLAN ggf. in Kombination mit L3 Access Control Lists (ACLs) oder Virtual Routing and Forwarding (VRF) erfolgen. Im Einzelfall kann (bei entsprechend hohem Schutzbedarf) auch eine physikalische Netztrennung von LAN und WLAN durch Verwendung eigener aktiver Komponenten für das WLAN in Betracht gezogen werden. (siehe Abbildung 12)

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

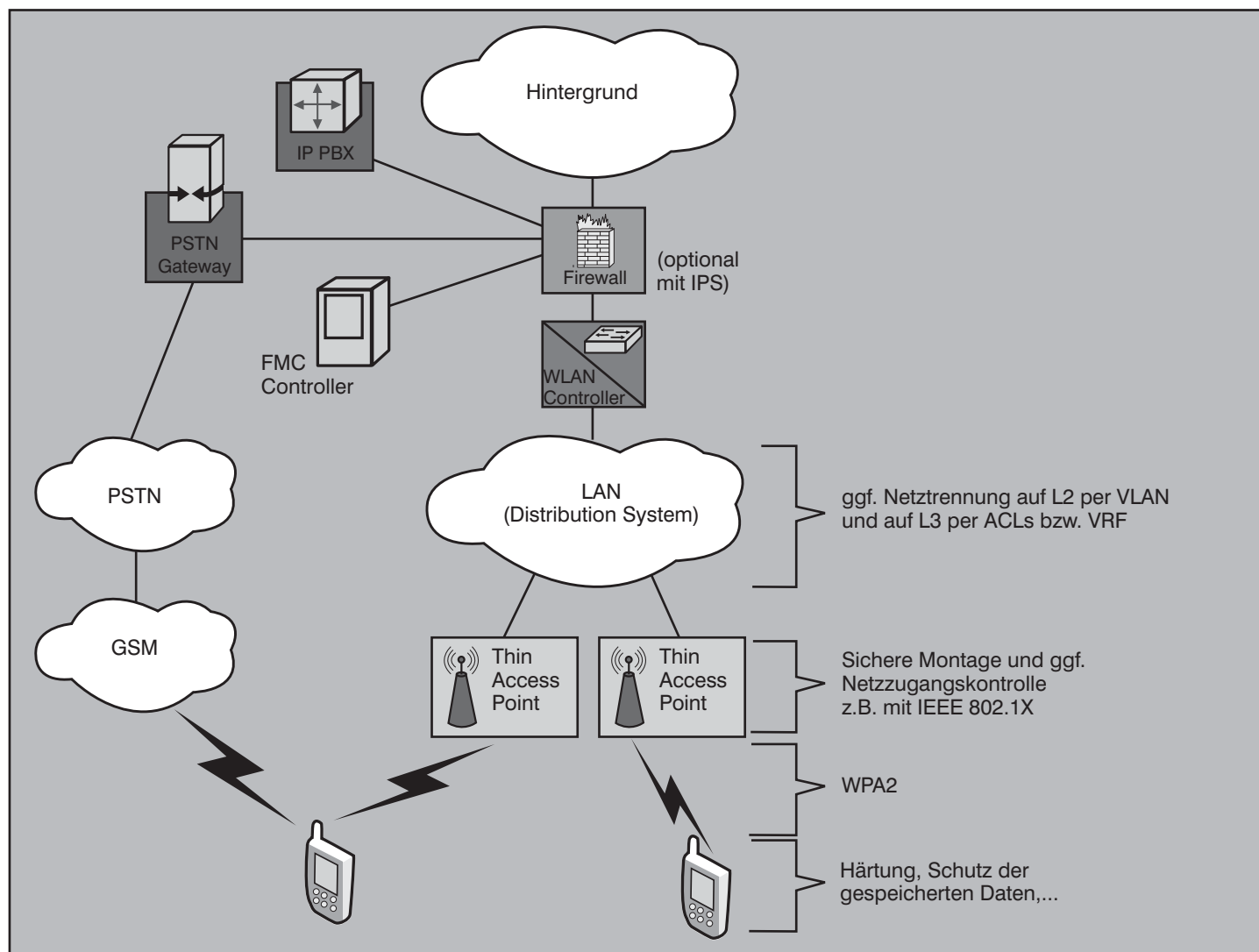


Abbildung 12: Typischer Aufbau einer Enterprise FMC-Lösung

5.4 Maßnahmen Netz- und Systemmanagement

Das Management der mobilen Endgeräte, denen für FMC ja ein direkter IP-Zugriff auf die lokale Infrastruktur gestattet werden muss, ist von besonderer Wichtigkeit für eine sichere FMC-Lösung.

Sperrung eines mobilen Endgeräts

Ein Prozess zur Sperrung eines mobilen Endgeräts, inklusive der Behandlung des Verlusts eines mobilen Endgeräts muss implementiert werden. Dabei müssen Zugangsberechtigungen gesperrt werden, Zertifikate und Passwörter zurückgezogen werden. Kritisch ist die Behandlung von vertrauenswürdigen Daten auf mobilen Endgeräten. Hier ist es erforderlich, per Kommando über GSM/UMTS oder WLAN ein Endgerät zu sperren und alle relevanten Daten löschen zu können. Eine solche Funktion ist inzwischen für alle gängigen Betriebssysteme für mobile Endgeräte auch

verfügbar (ggf. als zusätzliche Software).

Fernadministration der mobilen Endgeräte per GSM/UMTS und WLAN

Die mobilen Endgeräte einer FMC-Lösung müssen zentral über GSM/UMTS und WLAN verwaltet werden können. Dabei muss auch die Möglichkeit bestehen, gewisse Einstellungen zentral zu erzwingen (z.B. Sicherheitseinstellungen). Eine solche Fernadministration darf nur über eine sichere Kommunikationsverbindung erfolgen.

Kontinuierliche Überwachung der WLAN-Luftschnittstelle und der WLAN-Infrastruktur

Die Sprachübertragung über WLAN stellt erhöhte Anforderungen an Verfügbarkeit und Dienstgüte im WLAN. Kritische Ressource ist dabei die Luftschnittstelle, die (zumindest an allen besonders wichtigen Stellen im WLAN-Versorgungsbereich)

überwacht werden sollte. Dabei sollten auch VoIP-spezifische Leistungsindikatoren berücksichtigt werden. Außerdem sollte das WLAN-Management auch eine Funktion zur Lokalisierung von WLAN-Geräten unterstützen.

Der Einsatz einer solchen Überwachungsfunktion auf den produktiv genutzten Access Points kann die Leistung des WLAN und insbesondere die Sprachübertragung spürbar beeinträchtigen. Dies muss bei der Planung des WLAN-Managementsystems unbedingt berücksichtigt werden und kann beispielsweise dazu führen, dass für die WLAN-Überwachung zusätzliche dedizierte Access Point genutzt werden, was die Kosten für die WLAN-Infrastruktur deutlich erhöhen kann.

Weiterhin müssen auch die Netzelemente der WLAN-Infrastruktur (Access Points, WLAN Controller und RADIUS-Server)

Fixed Mobile Convergence (FMC) - Erreichbarkeit kontra Sicherheit

kontinuierlich hinsichtlich ihrer Verfügbarkeit überwacht werden.

6. Fazit

Die Attraktivität einer FMC-Lösung ist zunächst bestechend, denn die Vorteile des global verfügbaren Mobilfunks werden mit einer lokalen Technik auf eine transparente Weise gekoppelt. Auf diese Weise kann beispielsweise eine drahtlose Telefonversorgung in Gebäuden geschaffen werden, die mit GSM/UMTS (noch) nicht zufriedenstellend versorgt werden, und die sich für den Nutzer nahtlos in Mobilfunk und lokale TK-Anlagentechnik integriert.

Allerdings ist der Aufwand für den sicheren Aufbau und Betrieb solcher Systeme erheblich, wie die Betrachtungen in diesem Artikel gezeigt haben. Dies liegt einerseits daran, dass die Sprachtauglichkeit einer WLAN-Übertragung eine hohe Qualität der Funkversorgung im WLAN erfordert, andererseits aber an den mobilen Endgeräten selbst, die durch die Integration in die IT-Infrastruktur zu einem erheblichen Sicherheitsrisiko werden. Damit verbunden ist ein nicht zu unterschätzender Maßnahmenkatalog.

Die Alternative wäre eine GAN-basierte Lösung, denn GAN nutzt solide und bewährte Technik zur Absicherung der Kommunikation und mit GAN verschieben sich nicht unerhebliche Anteile der Komplexität hin zum Mobilfunkbetreiber, der schließlich bereits über eine entsprechende Infrastruktur für Betrieb und Überwachung komplexer Netze verfügt. Bleibt noch das WLAN als lokale drahtlose Zugangstechnik. Aber auch hier nähert sich eine interessante Konkurrenz aus dem Mobilfunksektor. Mit dem Konzept der Femtozellen, das aktuell vom 3GPP standardisiert wird, soll künftig eine flexible und preiswerte Indoor-Versorgung mit GSM/UMTS erfolgen können. Dabei ist nicht überraschend, dass der Femtozellenstandard auf GAN basieren wird.

7. Abkürzungen

3DES	Triple DES (TDES)
3GPP	3rd Generation Partnership Project
ACL	Access Control List
AES	Advanced Encryption Standard
BGP	Border Gateway Protocol
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CDMA	Code Division Multiple Access
DES	Data Encryption Standard
DoS	Denial of Service
EAP	Extensible Authentication

EAP-AKA	EAP Method for UMTS Authentication and Key Agreement	PDA	Personal Digital Assistant
EAP-SIM	EAP Method for GSM Subscriber Identity	PIN	Personal Identification Number
eFMC	Enterprise FMC	PSTN	Public Switched Telephone Network
FMC	Fixed Mobile Convergence	RADIUS	Remote Authentication Dial-in User Service
GAN	Generic Access Network	RIP	Routing Information Protocol
GANC	GAN Controller	SA	IPsec Security Association
GPRS	General Packet Radio Service	SIP	Session Initiation Protocol
GRE	Generic Routing Encapsulation	SMS	Short Message Service
GSM	Global System for Mobile communications	SRTP	Secure Real-time Transport Protocol
IDEA	International Data Encryption Algorithm	SSH	Secure Shell
IM	Instant Messaging	TLS	Transport Layer Security
IMS	IP Multimedia Subsystem	UMA	Unlicensed Mobile Access
IPS	Intrusion Prevention System	UMTS	Universal Mobile Telecommunications System
IPsec	IP Security	VLAN	Virtual LAN
JTAPI	Java Telephony API	VPN	Virtual Private Network
L2TP	Layer 2 Tunneling Protocol	VRF	Virtual Routing and Forwarding
LCR	Least Cost Routing	VXML	Voice Extensible Markup Language
MMS	Multimedia Messaging Service	WMM	Wi-Fi Multimedia
MNO	Mobile Network Operator	WPA	Wi-Fi Protected Access
MWI	Message Waiting Indicator	XMPP	eXtensible Messaging and Presence Protocol
OSPf	Open Shortest Path First		
OTA	Over the Air (Provisioning)		

Jetzt Leser werden



Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>