IEEE 802.16
WIMAX

Christof Strauch - Daniel Kuhn

Agenda

- Überblick & Motivation
- IEEE 802.16
  - Ziele
  - Standards
- Anwendungsszenarien
- Konkurrierende Systeme
- WiMAX Security
  - Schutzziele
  - Konzepte & Technologien
  - Prozesse
  - Schachstellen und Gefährdung
- Potenzial, Geräte, Praxiseinsatz
- Fazit und Pressespiegel

Überblick

- Worldwide Interoperability for Microwave Access
- IEEE 802.16 Standard für Wireless Broadband Access
- veröffentlicht seit 2001
- bietet vielseitige Anwendungsszenarien

Motivation

- Nicht alle dt. Haushalte verfügen heute über einen Breitband Internetzugang
  - 90% aller Breitbandverbindungen über DSL (Stand 2007)
  - Anbieter sind gezwungen, die Leitungen der DTAG zu nutzen
  - weite Teile Europas verfügen nicht über ein DSL-Netz
    - alte, nicht aufgerüstete Kupferleitungen
    - oder Glasfaserkabel (z.B. in Ostdeutschland)
  - Internet über Kabelnetz erst in den letzten Jahren interessant
    - meist nur in Verbindung mit TV

Entstanden aus Ziel auch abgelegenen Haushalten einen Breitband-Access zu legen

kleine Dörfer, kein DSL, froh wenn ISDN
=> WiMAX

WiMAX Forum

- Gründung der Arbeitsgruppe IEEE 902.16 im Jahr 1999
- Motiviert durch den Bedarf eines global standardisierten Drahtlossystems für breitbandigen Metropolitan Area Network
- 400 Unternehmen in Telekommunikation und IT
  - Comcast, Fujitsu, Intel Corp., Motorola, Nokia, Samsung, Sprint Nextel
  - D-Link, Netgear, Ericsson, HTC, Acer, Zyxel, Sony, Sharp
  - uvm.
  - Quelle: http://www.wimaxforum.org/about/member-roster

WiMAX Forum

Ziele unabhängig von den Zielen des Standards

- Ziele
  - Vorantreiben der Kompatibilität
  - schnelle Markteinführung
  - zügiger globaler Aufbau von WiMAX Netzen
  - Akzeptanz
  - Gewährleistung eines reibungslosen und gewinnbringenden Betriebs
  - Vermeidung einer Monopolstellung einer oder mehrerer Unternehmen

was zu einer Abhängigkeit führt die man ja nicht will

IEEE 802.16 - Ziele

- Globaler Standard für Metropolitan Area Network (MAN)
- Übernahme von Prinzipen aus IEEE 802.11
- hohe Reichweite über mehrere Kilometer
- hohe Kapazität und hoher Durchsatz (vgl. mit LAN)
- einfache Handhabung (z.B. für Sportevents, ...)
- Skalierbarkeit (einfache Erweiterbarkeit)
- Breites Angebot an Diensten für Realtime Anforderungen (QoS)

QoS im Buch nachzulesen

IEEE 802.16 - Ziele

- Verbindungsorientierte Übertragung mit verschiedenen Operationsmodi:
  - Point to Point,
  - Point to Multipoint und
  - Mesh-Netzwerke

Mesh Netzwerke erklären

- Flexibilität hinsichtlich der benutzbaren Trägerfrequenzen
- Flexibilität hinsichtlich der Kanalbreite
- Betrieb in lizenzfreien und lizenzierten Spektren
- Unabhängigkeit: IEEE 802.16 definiert nur OSI Level 1 und 2
- Flexible und dynamische Anpassung von Codierung und Modulation
- Vermeidung von Fehlern aus anderen Standards wie Bluetooth oder WLAN

Reichweite =
LOS & NLOS
Interferenzen (WLAN, BT)
Trägerfrequenz
Kanalbreite
Multiplexing
Übertragungsdämpfung
(Gelände, Wetter,
Antenne, Mobilität)

Trägerfrequenzen

- keine einheitliche globale Regelung, je eigene Bestimmungen in
  - Nordamerika/Mexiko
  - Zentral-/Südamerika
  - West-/Osteuropa
  - Mittlerer Osten/Afrika
  - Asien/Pazifik
- IEEE 802.16
  - Spektrum zwischen 10 und 66 GHz

Trägerfrequenzen

- Lizenzfrei
  - keine Kosten, kein Zeitaufwand für den Lizenzerwerb
  - geringes Maß an einzuhaltenden Bestimmungen
  - schneller Rollout, wichtig für temporäre Installationen
  - Vielzahl von Betreibern möglich (Private Haushalte und Gewerbe)
  - 2,4 & 5 GHz Bänder
- Lizenzpflichtig
  - Höchstmaß an Kontrolle hinsichtlich Interferenzen und QoS
  - kontrollierter und koordinierter Betrieb über Zellgrenzen hinweg
  - ermöglicht langfristige Netzplanung (Reichweite und Frequenz)
  - nur für kommerzielle Kunden geeignet
  - Verzicht auf Algorithmen und Prozeduren (z.B. Dynamic Frequency Selection)
  - 2,5 & *3,5 GHz* Bänder

keine einheitliche,
globale Regelung,

je eigene Bestimmungen

Trägerfrequenzen

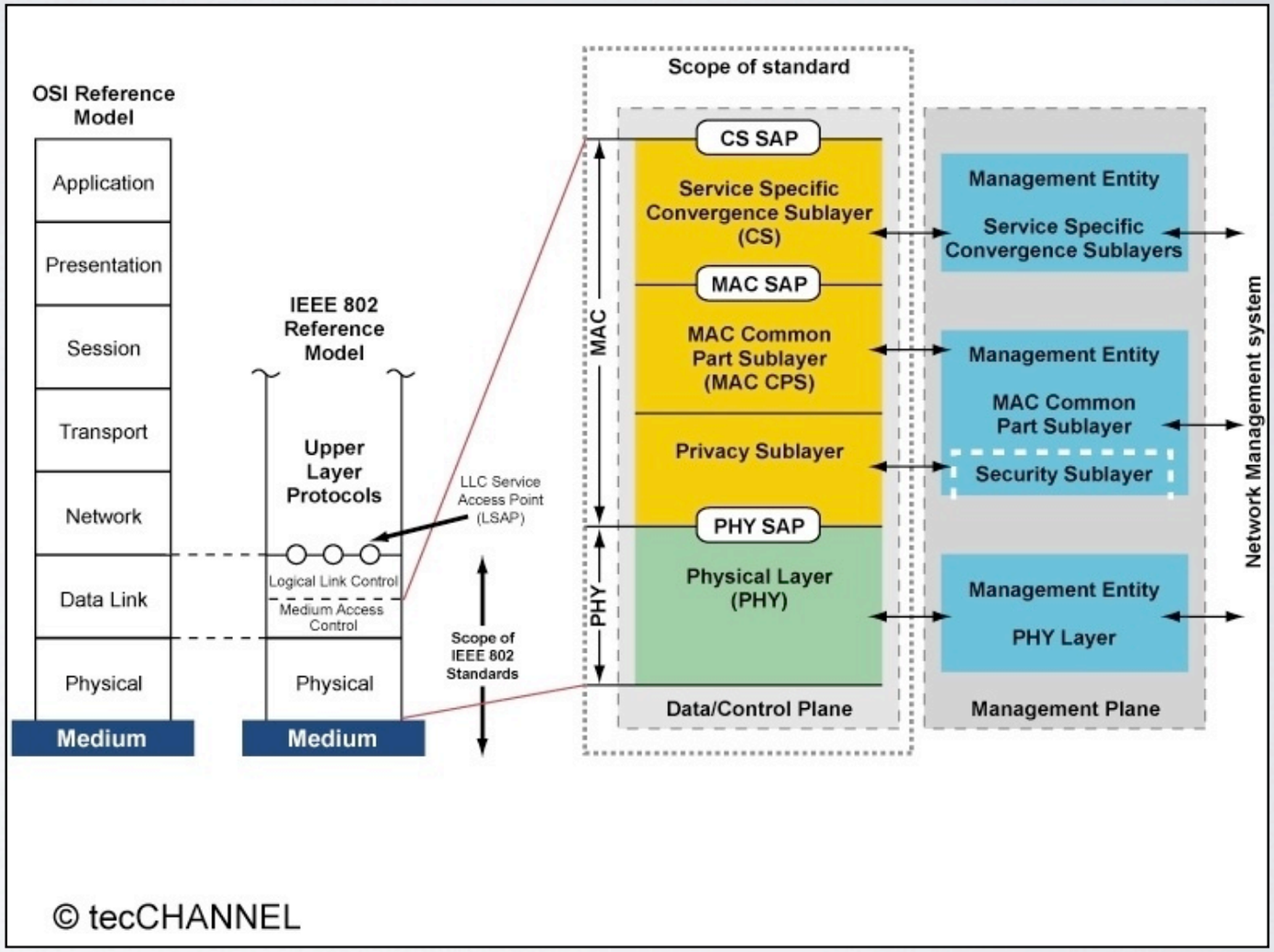
- 2,4 GHz-Band (2,4 - 2,483 GHz) - Lizenzfrei
  - intensive Nutzung von WLAN und Bluetooth
  - dadurch starke Interferenzen
  - Limitierte Sendeleistung auf 100mW (0,1W)
- 2,5 GHz-Band (2,495 - 2,6 GHz) - Lizenzpflichtig
  - WiMAX: Nordamerika, Mexiko, Brasilien und südostasiatischer Raum
  - nicht in Europa verfügbar

Trägerfrequenzen

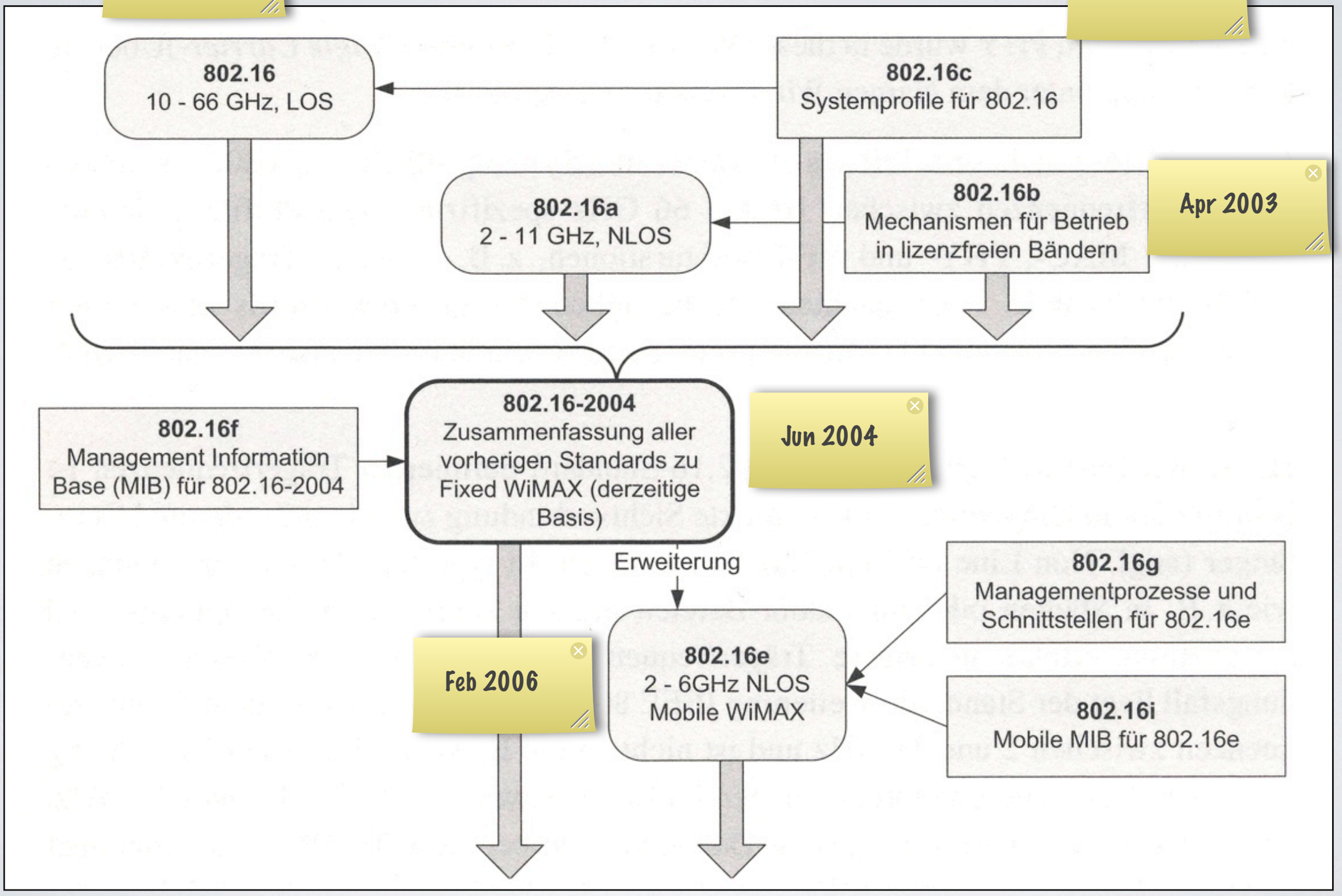
- 3,5 GHz-Band (3,4 - 3,6 GHz) - lizenzpflichtig <<<<
  - global am weitesten für drahtlose Breitbandverbindungen verfügbar
  - nicht in den USA (sondern 3,65 - 3,7 GHz)
  - meist nur für ortsgebundenen Zugriff (fixed)
  - erste WiMAX Geräte sind auf dieses Band ausgelegt
- 5 GHz-Band (5,15 - 5,875 GHz) - lizenzfrei
  - nahezu in allen Ländern nutzbar
  - untere Bereich steht IEEE 802.11a zur Verfügung
  - oberer Bereich mit Sendeleistung von maximal 4 Watt

WiMAX technisch

- 802 Standards definieren
  OSI Level 1 und 2
- Aufteilung in Physical Layer und Medium Access Control Layer
- PHY definiert
  - Zugriff auf Funkkanal
  - Codierungsschemen
  - Modulierungsschemen
  - 4 verschiedene Varianten in 802.16
- MAC definiert
  - Kanalzugriffsteuerung
  - Bandbreitenmanagement
  - Signaling und Verwaltung von Verbindungen
  - Unterstützung versch. Protokolle (ATM, IP, ...)
  - Spezifizierung des Übertragungskonzeptes (zellorientiert oder paketorientiert)
  - *Security Sublayer (Authentifizierung und Encryption)*



Standards in IEEE 802.16



Standards in IEEE 802.16

802.16 Dezember 2001	802.16c Januar 2003	802.16a/b April 2003	802.16d Juni 2004	802.16e Februar 2006
definiert die Physical-Layer (PHY) und die Medium Acces Control (MAC) Outdoorverbindungen mit LOS ortsfeste Base- & Subscriberstations Point-To-Point Verbindung (weniger für LMA, eher Richtfunk)	zum Zweck der Kompatibilität werden Profile definiert. (MAC, PHY und RF-Konfigurationen)	Outdoorverbindungen mit Non-LOS resultierend daraus, geringere Reichweite ortsfeste Base- & Subscriberstations Point-To-Mulitpoint und Mesh-Topologien möglich 802.16 b: lizenzfreie und lizenzierte Frequenzbänder Mechanismen zur Vermeidung von Interferenzen Dynamic Frequency Selection (DFS)	besser bekannt als 802.16 -2004 fasst alle bisherigen Standardversionen überarbeitet zusammen keine mobilen Subscriber-Stations, daher auch als Fixed-WiMAX bezeichnet essentielle Grundlage aller WiMAX Entwicklungen	auch als 802.16 - 2005 bezeichnet Mobile WiMAX durch Erweiterung des IEEE 802.16 - 2004 Standards Mobilität bis 125 km/h Ünterstützung von mobilen Stationen (wie in UMTS/GSM) + Handover + Kommunikation zwischen Base-Stations Erweiterung des PHY um Algorithmen zur dynamischen Sendeleistung

Sehr breiter Standard der viel zulässt, daher Profile zum Eindämmen des Freiraums vgl Bluetooth

Profile beziehen sich auf eine ganz konkrete Trägerfrequenz und Bandbreite

Eigenschaft: mandatory (ü.a. Prof) required conditionally req.

Standards in IEEE 802.16

	IEEE 802.16	IEEE 802.16c IEEE 802.16a/b IEEE 802.16d	IEEE 802.16e
Datum	Dezember 2001	Januar 2003 - Juli 2004	Dezember 2005
Fertigstellung	verfügbar, jedoch keine Relevanz für Privatkunden	ab Mitte 2005	ab 2006
Frequenzband	10 bis 66 GHz	2 bis 11 GHz	0,7 bis 6 GHz
Übertragung	LOS	Non LOS	Non LOS
max. Datenrate	32 bis 134 Mbit/s in 28 MHz Kanälen	bis zu 75 Mbit/s in 20 MHz Kanälen	bis zu 15 Mbit/s in 5 MHz Kanälen
Bandbreiten	20, 25 und 28 MHz	skalierbar von 1,5 bis 20 MHz	1,75 MHz - 20 MHz
Modulationsarten	QPSK, 16QAM, 64QAM	OFDM256, OFDMA 64 QAM, 16QAM, QPSK, BPSK	OFDM256, OFDMA 64 QAM 16QAM, QPSK, BPSK
Position der Empfängereinheit	fest	feste Außenantelle, Innenraumanwendung und eingeschränkte Mobilität	mobil
Reichweite	50 Km	bis zu 50 Km, typisch 15 Km mit Außenantenne, 5 Km mit	bis zu 5 Km, typisch 1,5 KM

Unterscheidung:
- fixed
- portabel

Standards in IEEE 802.16

- IEEE 802.16f
  - Gewährleistung von Interoperabilität zwischen 802.16-2004 Produkten verschiedener Hersteller auf Netzwerkebene
  - MIB und SNMPv2 (?)
- IEEE 802.16g und IEEE 802.16i
  - Als Erweiterung des 802.16f Standards zu sehen
    - definieren Erweiterungen zur mobilen SS bzgl. Management und Kontrollprozeduren zwischen PHY, MAC und CS und dem NCMS spezifiziert
      - z.B. Austausch von Signalisierungsinformationen beim Handover

Anwendungsszenarien

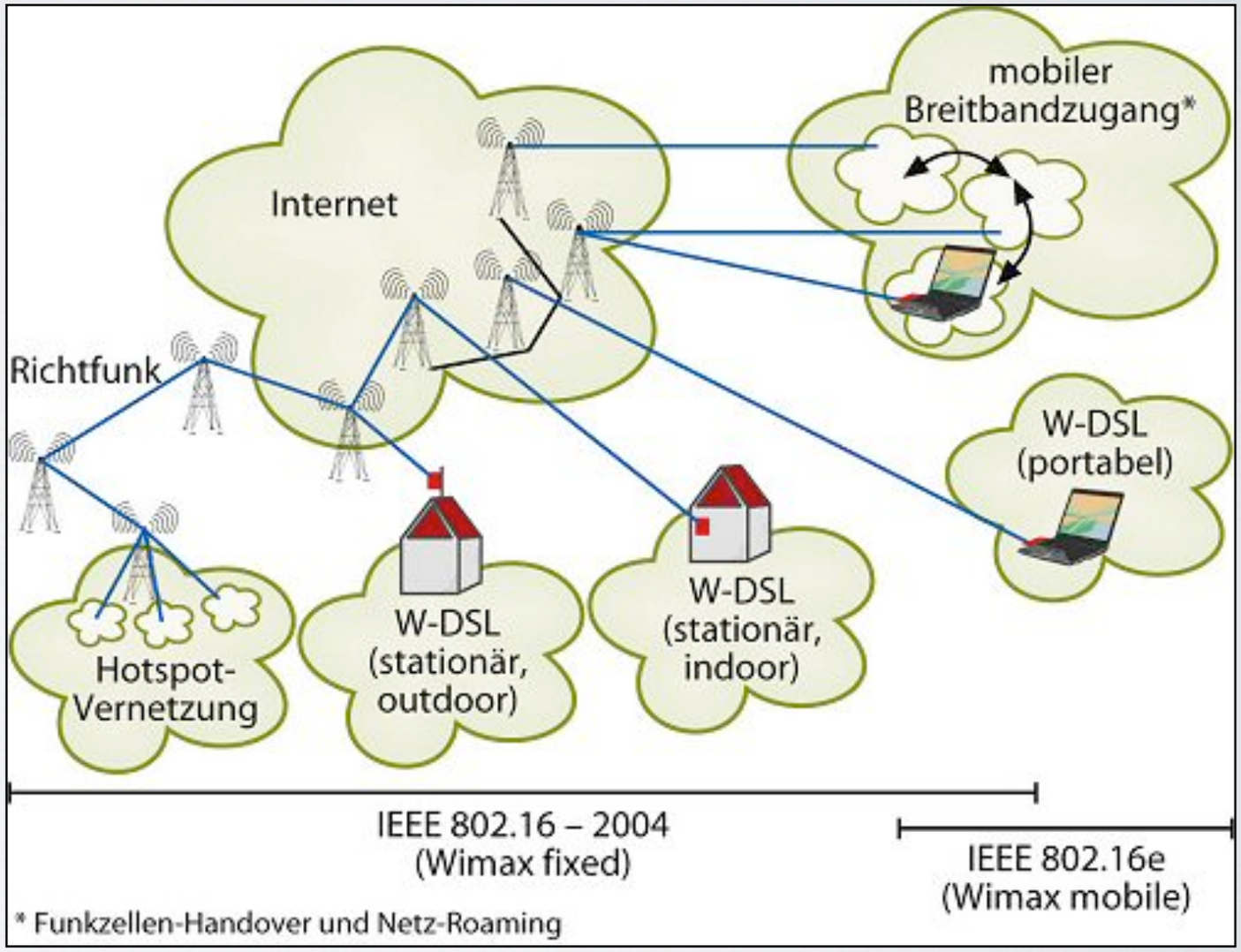
- Einsatzmöglichkeiten abhängig von
  - Bevölkerungsdichte,
  - Bevölkerungsverteilung,
  - Bevölkerungsstruktur in geografischen Regionen
  - Verfügbarkeit alternativer Technologien
- Denkbarer Einsatz in städtischen Regionen, vorstädtischen Regionen als auch in ländlichen Gegenden

Anwendungsszenarien

Region	Beschreibung
Urban	- hohe Dichte von Teilnehmern - mehrstöckige Bürogebäude und Appartements - großer Bedarf an Bandbreite auf kleinem Raum - hohe Anforderungen bezüglich der Frequenzplanung - große Konkurrenz durch alternative Technologien
Vorstädtisch	- mittlere Dichte von Teilnehmern - großer Anteil von Einfamilienhäusern - Industrie und Gewerbe - größere Abdeckung durch eine BS, aber immer noch großer Bedarf an Bandbreite - alternative Technologien nicht flächendeckend
Ländlich	- weit abgelegen von größeren Städten und Zentren - Wohnhäuser und kleine Unternehmen - steigender Bedarf nach Internetzugängen - eingeschränkte Verfügbarkeit von alternativen Technologien - problematisch: Hochdatenratige Backhaul Verbindungen benötigt

Anwendungsszenarien

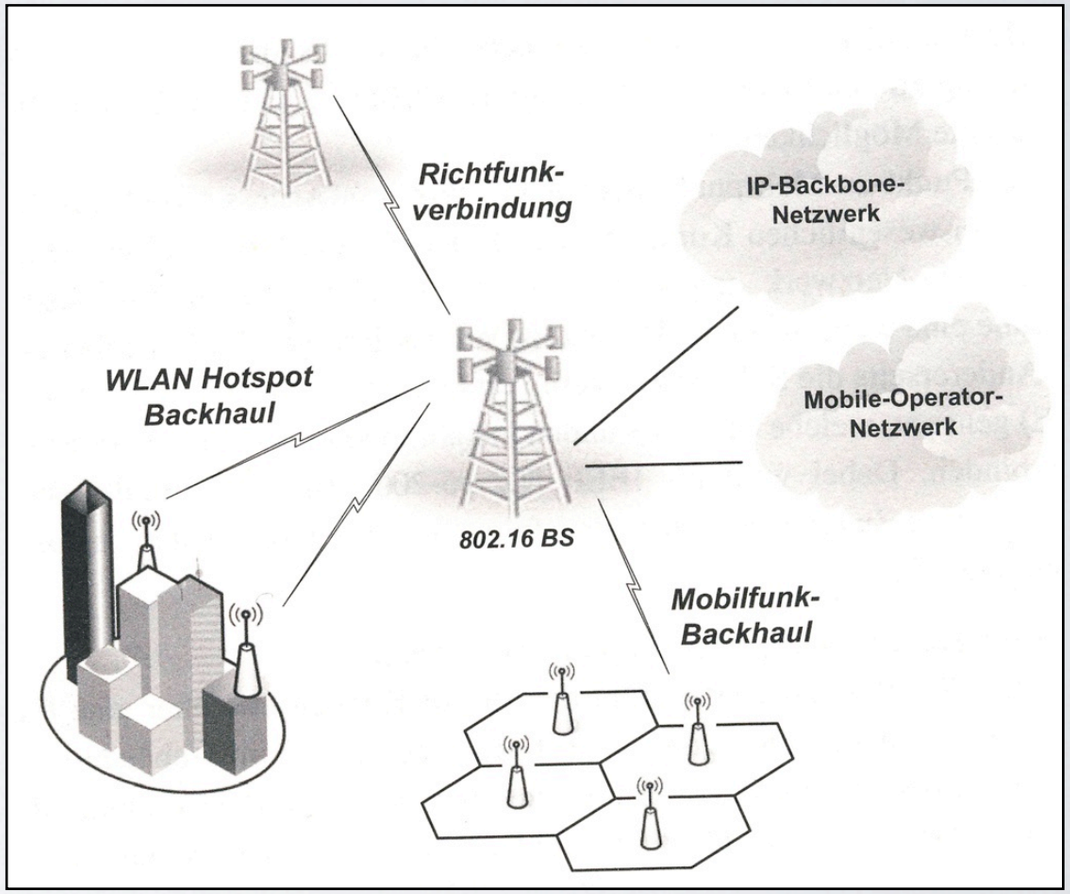
- Backhauling
- Last-Mile Access
- Nischenanwendung
- Zellulares System



von links nach rechts

Anwendungsszenarien

- Backhaul Anwendung
  - Richtfunkverbindung über große Distanz zwischen Access- und Backbone-Infrastruktur
  - Anbindung von WLAN Hotspots
  - Anbindung von Mobilfunkzellen
  - Ziel: kostengünstige Alternative zu drahtgebundenen Lösungen



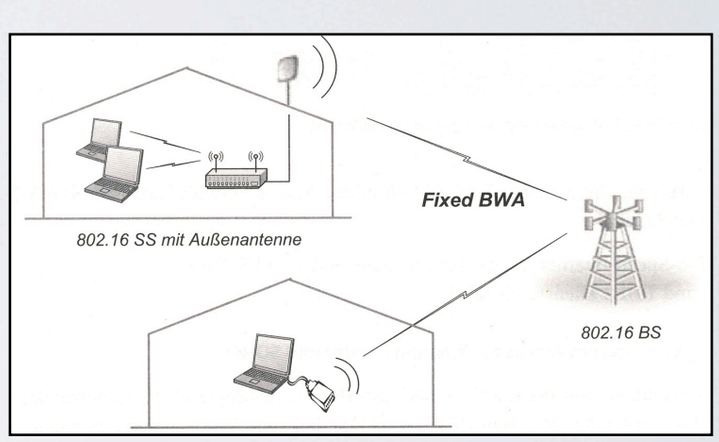
Anwendungsszenarien

- Last Mile Access
  - Grund:
    - hohe Kosten durch Aufbau eines alternativen Netzes
  - Szenarien:
    - fixer Broadband Wireless Access (Outdoor Antenne)
    - Normadischer Broadband Wireless Access (Indoor Antenne)
  - Verwendung
    - High Speed Access für Privatanwender und SOHO (Wireless DSL)
    - IP- und T1/E1 Dienste für kleine und mittlere Unternehmen

DBD Deutsche Breitband Dienste

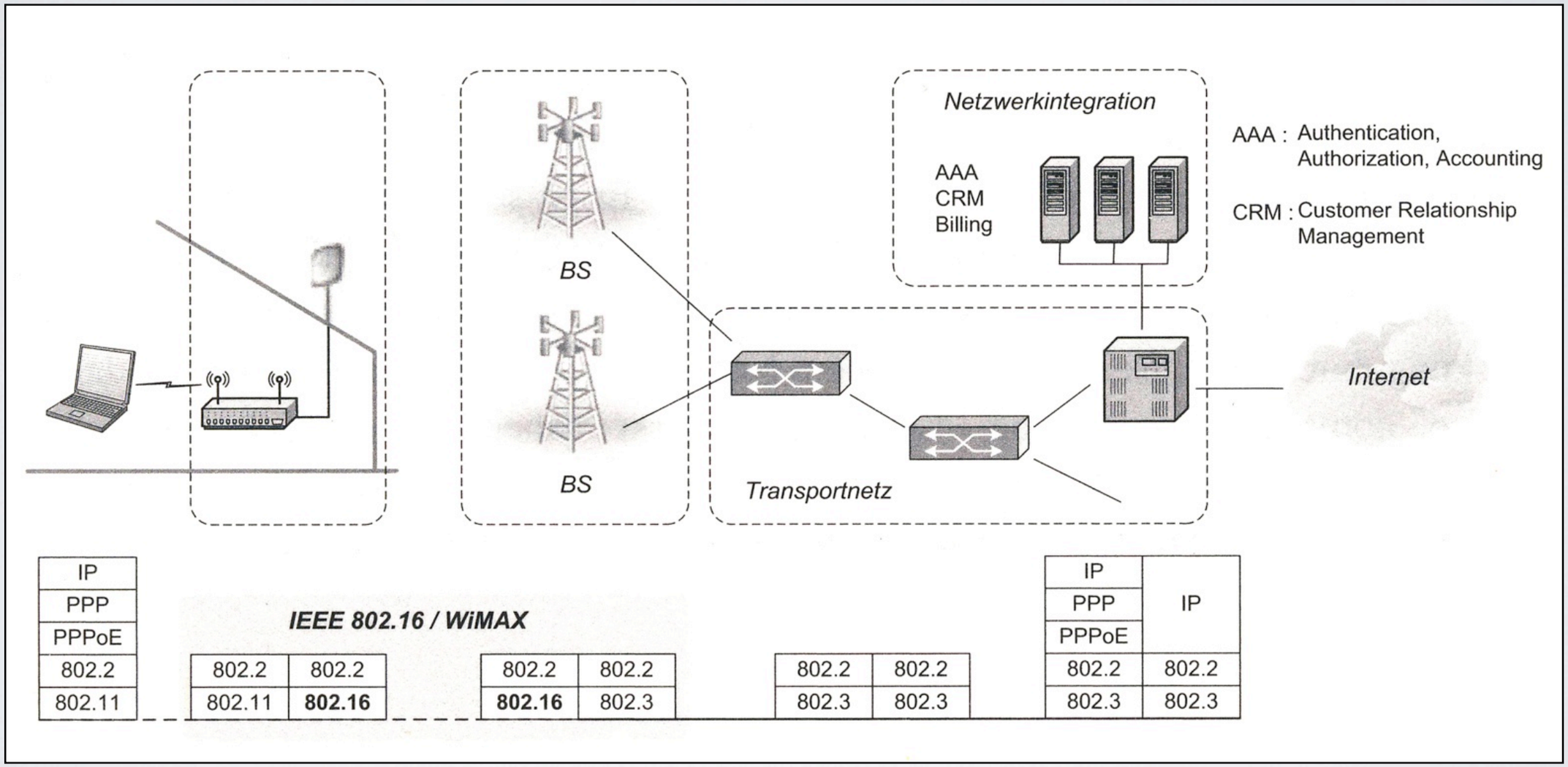
MAXXonair ...hier bin ich der Star.

Berlin, Halle, Leipzig, Dresden und Magdeburg



Anwendungsszenarien

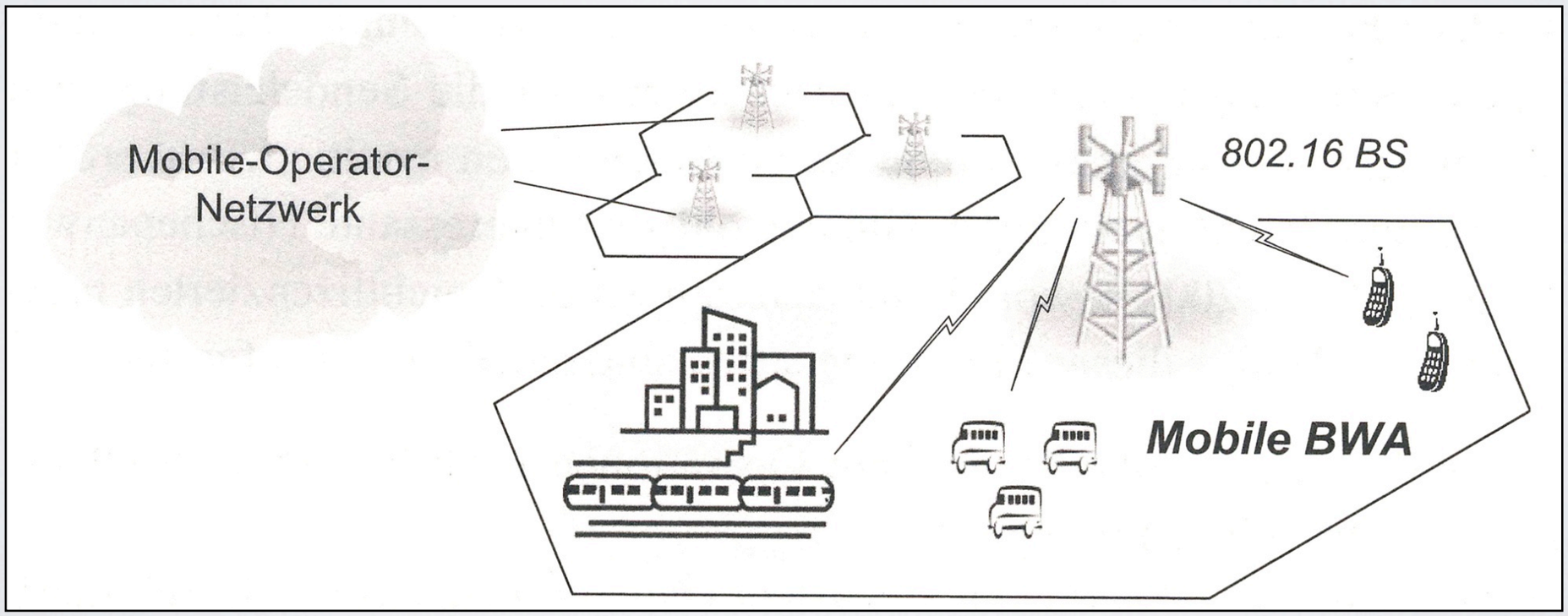
- Last Mile Access



802.3 Ethernet

Anwendungsszenarien

- Zellulare Systeme für mobilen BWA
  - ab IEEE 802.16e (802.16-2005)
  - völlige Mobilität und kontinuierliche Netzwerkanbindung bei großen Geschwindigkeiten
  - nötig ist eine entsprechende Abdeckung wie heute mit GSM oder UMTS

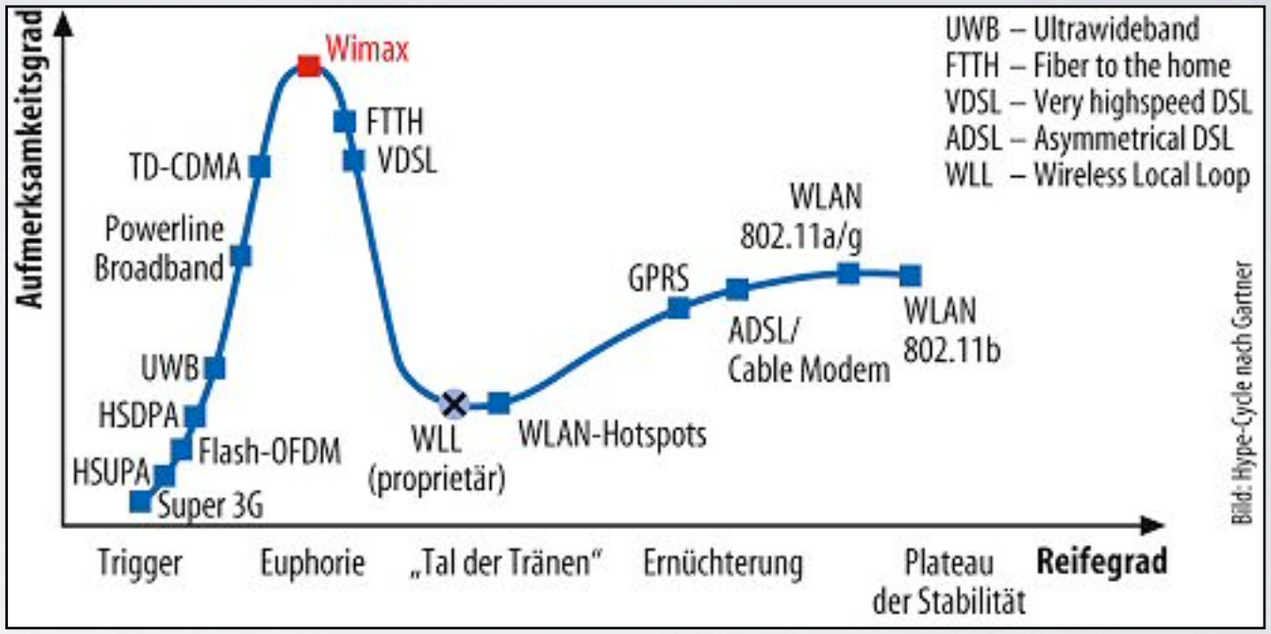


Anwendungsszenarien

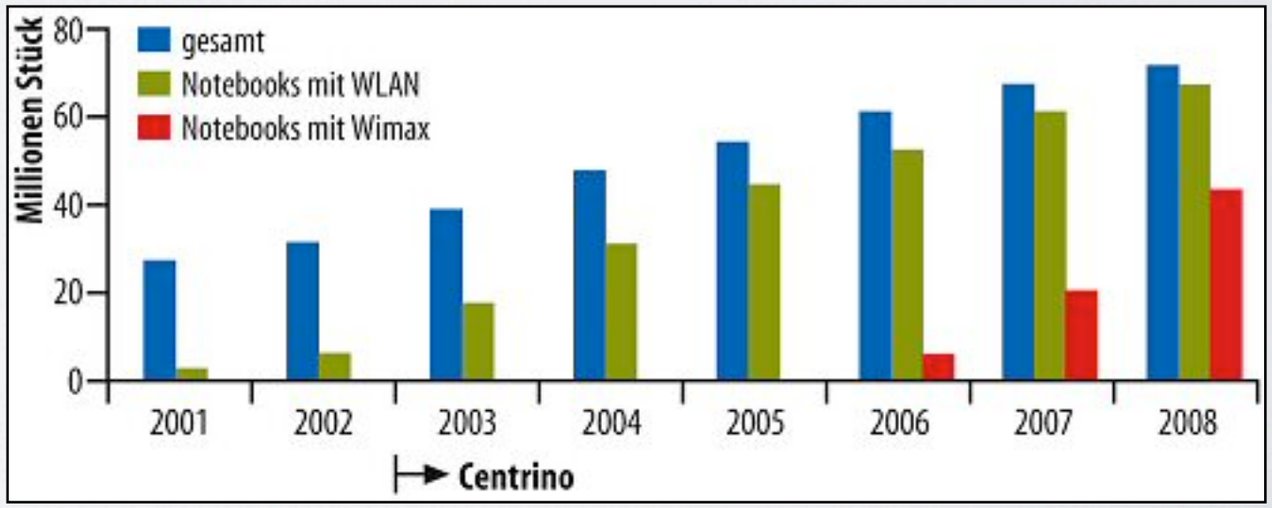
- Nischenanwendungen
  - IEEE 802.16-2004 im lizenzfreien Frequenzband (z.B. 5,8 GHz)
  - Problem:
    - Limitierung der Sendeleistung
    - Interferenzen
- Katastropheneinsätze und humanitäre Hilfe
- Organisationen der öffentlichen Sicherheit
- Private Netzwerke für Firmen, Universitäten und Sportanlagen
- Militärische Kommunikationsnetze
- Tourismus
- Temporärer Betrieb (Tour de France, WM/EM, ...)

Konkurrierende Systeme

- DSL
- TV-Kabel / DOCSIS
- WLAN
- GSM, GPRS, EDGE, UMTS
- HDSPA / HSUPA
- WiBro
- IEEE 802.20

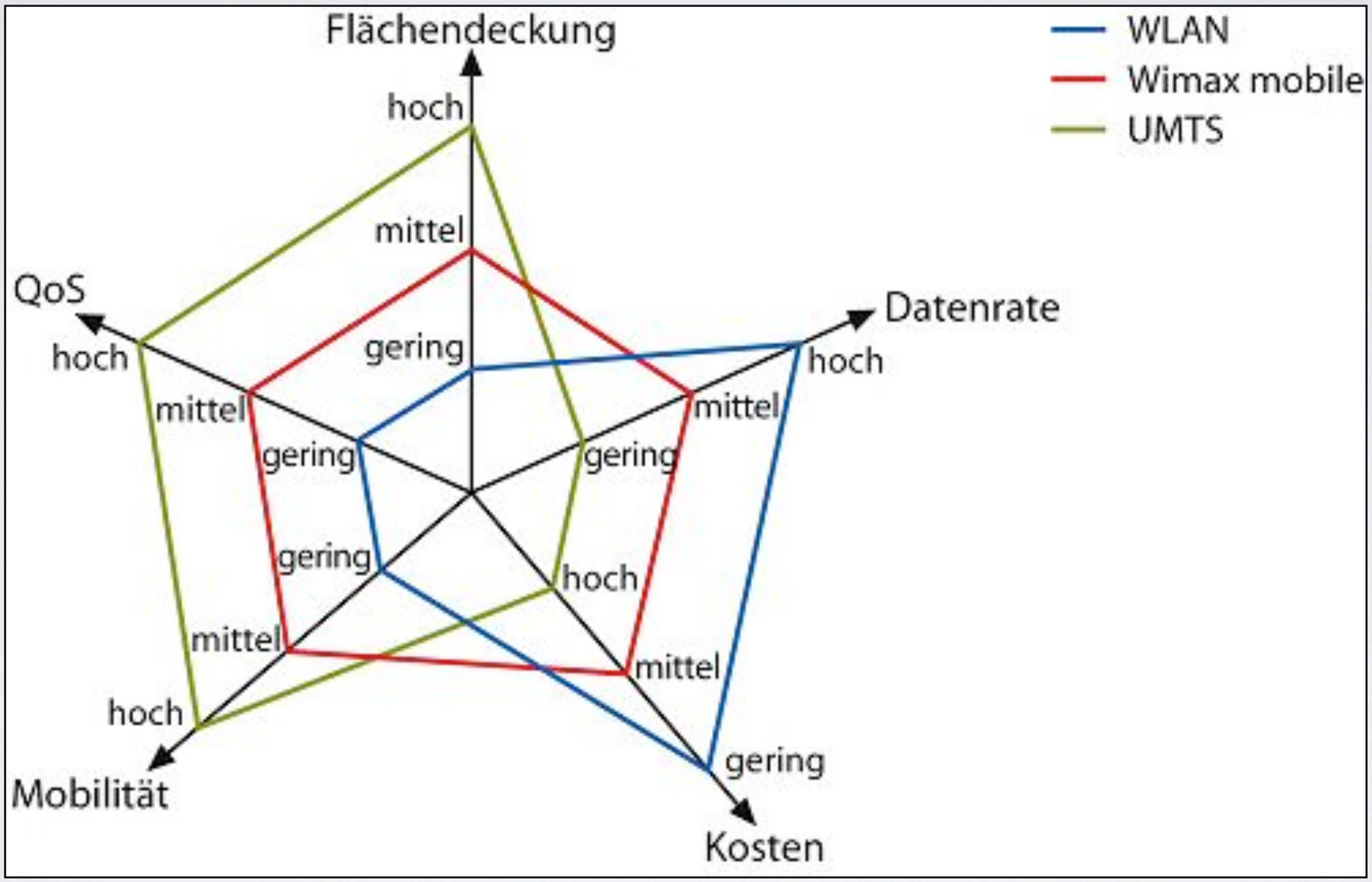


Quelle: heise Artikel 2005



Quelle: heise Artikel 2005

Konkurrierende Systeme



WiMAX vs. WLAN

	WLAN	WiMAX
Frequenz	an Frequenzen gebunden 13 Kanäle	prinzipiell freie Frequenzwahl
Reichweite	geringe Reichweite 802.11n mit ~250m 802.11y mit ~5Km	hohe Reichweite max. 50Km NLOS
Sendeleistung	Sendeleistung begrenzt (100mW; 802.11h: 200mW-1W)	je nach Frequenz keine Begrenzung
Topologien	PTP, PTM & Mesh-Topologien ab 802.11s (2007)	PTP, PTM & Mesh-Topologien ab 802.16a
Datenrate	802.11n: 600 MBit/s (effektiv 74 MBit/s) 802.11y: 54 Mbit/s (effektiv 23 MBit/s)	Datenrate: 15 - 134 MBit/s
Anwendungszweck	private / Kommerzielle Anwendungsszenarien	eher kommerzielle Anwendungsszenarien
Kosten	billig (auch für den Endkunden)	noch zu teuer (für den Endkunden) (45€ Kosten für Intel Chip - 2004)

UMTS:
- 14,4 MBit/s je nach Modulation

WIMAX SECURITY

WiMAX Security

- Schutzziele
  - Authentifizierung
  - Authentisierung: Base Station (BS) <> Subscriber Station (SS)
  - Autorisierung: darf die Subscriber Station das WiMAX-Netz nutzen?
- Vertraulichkeit
  - Vertraulichkeit der Management-Nachrichten und Nutzdaten
  - Vertraulicher Schlüsselaustausch
- Integrität
  - Integrität der Datenpakete (Management-Daten, Nutzdaten)
  - Integrität des Schlüsselaustauschs
- Verfügbarkeit

WiMAX Security

- Konzepte und Technologien
  - Security Associations
  - Protokolle
    - Privacy Key Management Protocol (PKM) → Authentisierung,Schlüsselverteilung
    - Encapsulation Protocol → Verschlüsselung
  - X.509-Zertifikate, EAP
  - Verschlüsselung: DES, AES
  - SHA-1 HMACs
- implementiert als Sublayer der MAC-Schicht
  - Security Sublayer (WiMAX fixed)
  - Privacy Sublayer (WiMAX mobile)

WiMAX Security

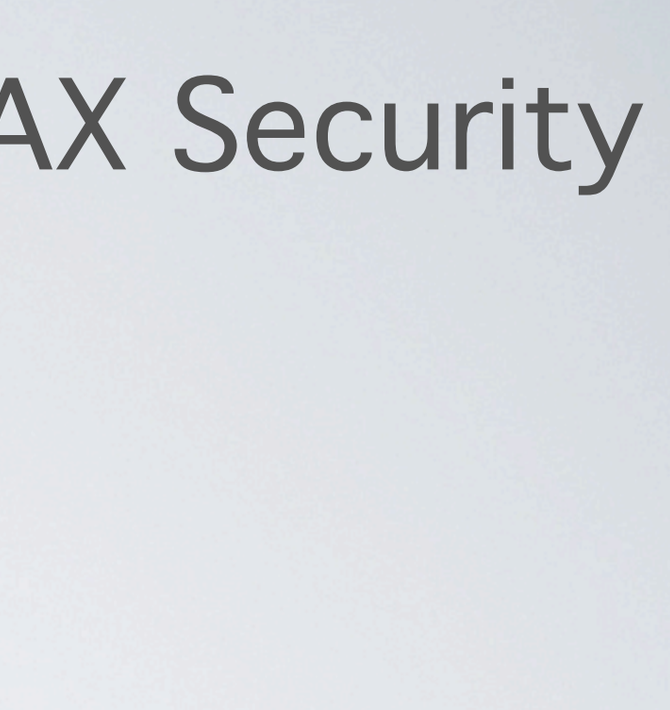
- Konzepte: Security Associations (SAs)
  - Satz von Sicherheitsinformationen für logische Verbindungen BS <> SS
    - genutzte Cryptographic Suite
    - Schlüsselmaterial, Initialisierungsvektoren...
  - zwischen BS und SS synchronisiert mittels PKM-Protokoll
  - Arten:
    - Primary SA: während Initialisierungsphase von SS erstellt
    - Static SA: in der BS vorkonfiguriert
    - Dynamic SA: für dynamisch signalisierte Service Flows
    - Group SA: für Multicast-Gruppen (bei WiMAX mobile)
    - Multicast/Broadcast Service Group SA: für Multimedia-Streaming (mobile)
  - keine SA für *Management-Nachrichten* (Primary-Mgmt-Connection)!

WiMAX Security

- Protokolle:
  - Privacy Key Management (PKM) Protocol
    - Authentisierung
    - sichere Schüsselverteilung zwischen Base Station und Subscriber Stations
  - WiMAX mobile:
    - PKMv1: für Schlüsselverteilung 1 BS <> 1 SS, Authentisierung Zertifikat-basiert (X.509)
    - PKMv2: Erweiterungen, u.a.
      - Authentisierung alternativ über EAP möglich
      - Schlüssel für Gruppen sowie Multicast/Broadcast Service (Multimedia-Streaming)
      - Fast Handover zwischen Base Stations mittels 3-Wege-Handshake
- Encapsulation Protocol
  - Verschlüsselung von Datenpaketen
  - definiert dazu sog. Cryptographic Suites

WiMAX Security

- Schlüsselmaterial: WiMAX fixed
  - Authorization Key (AK)
    - teilt BS einer SS während Authentisierung zu
    - begrenzte Gültigkeitsdauer ➔ Key Refresh durch SS
    - 1 AK pro Verbindung
  - Key Encryption Key (KEK)
    - verschlüsselt TEK beim Schlüsselaustausch
  - Traffic Encryption Key (TEK)
    - verschlüsselt Datenverkehrs zwischen SS und BS
  - Message Authentication Key
    - zur Signatur und Verifikation von *Management-Nachrichten*



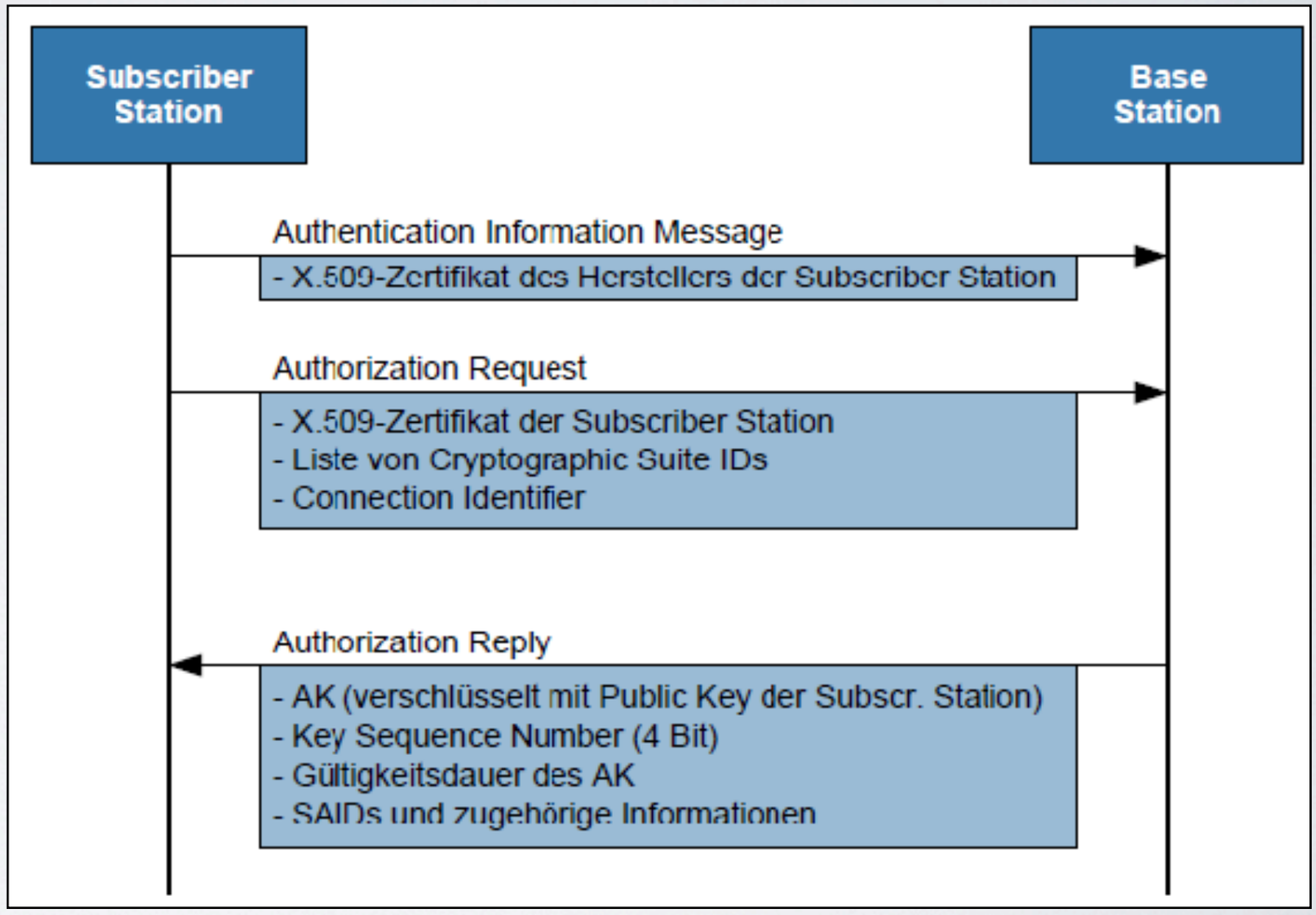
WiMAX Security

Schlüsselmaterial: WiMAX mobile

Unicast/Multicast	Authentisierungsverfahren	Schlüssel
Unicast	X.509	Pre-Primary Authorization Key (Pre-PAK) → Primary Authorization Key (PAK) → HMAC ← Authorization Key (AK) → KEK → TEK
	EAP	Master Session Key (MSK) → Pairwise Master Key (PMK) → HMAC ← Authorization Key (AK) → KEK → TEK
Multicast		Authorization Key (AK) → HMAC Key → Group Key Encryption Key (GKEK) → Group Traffic Encryption Key (GTEK)
Multicast Broadcast Service (für Multimedia-Streaming)		MBS Authorization Key (MAK) → MBS Traffic Key (MTK)

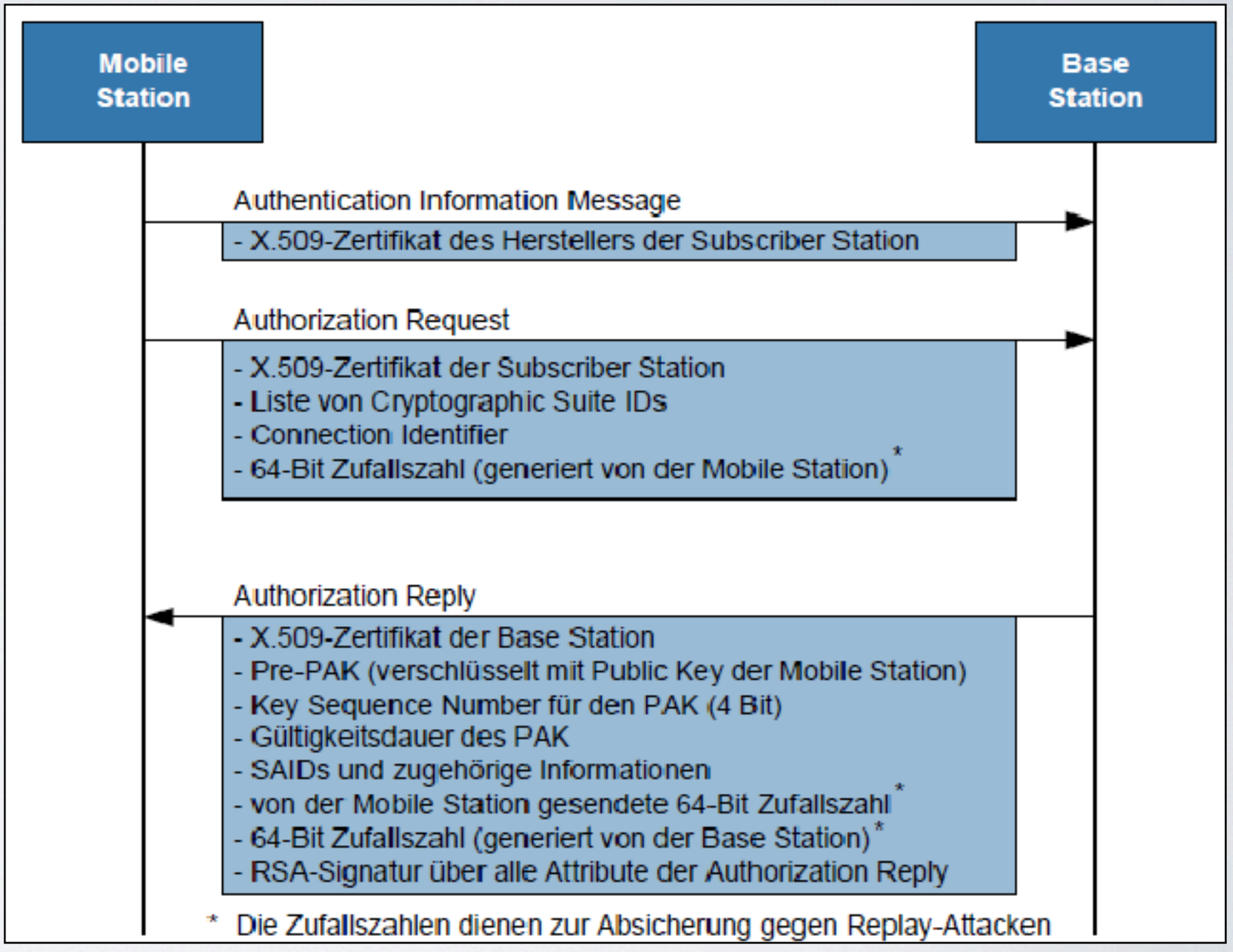
WiMAX Security

- Prozesse: Authentisierung
  - bei Netzeintritt
  - Zertifikat-basiert
  - *einseitige* Authentisierung (WiMAX fixed, WiMAX mobile)



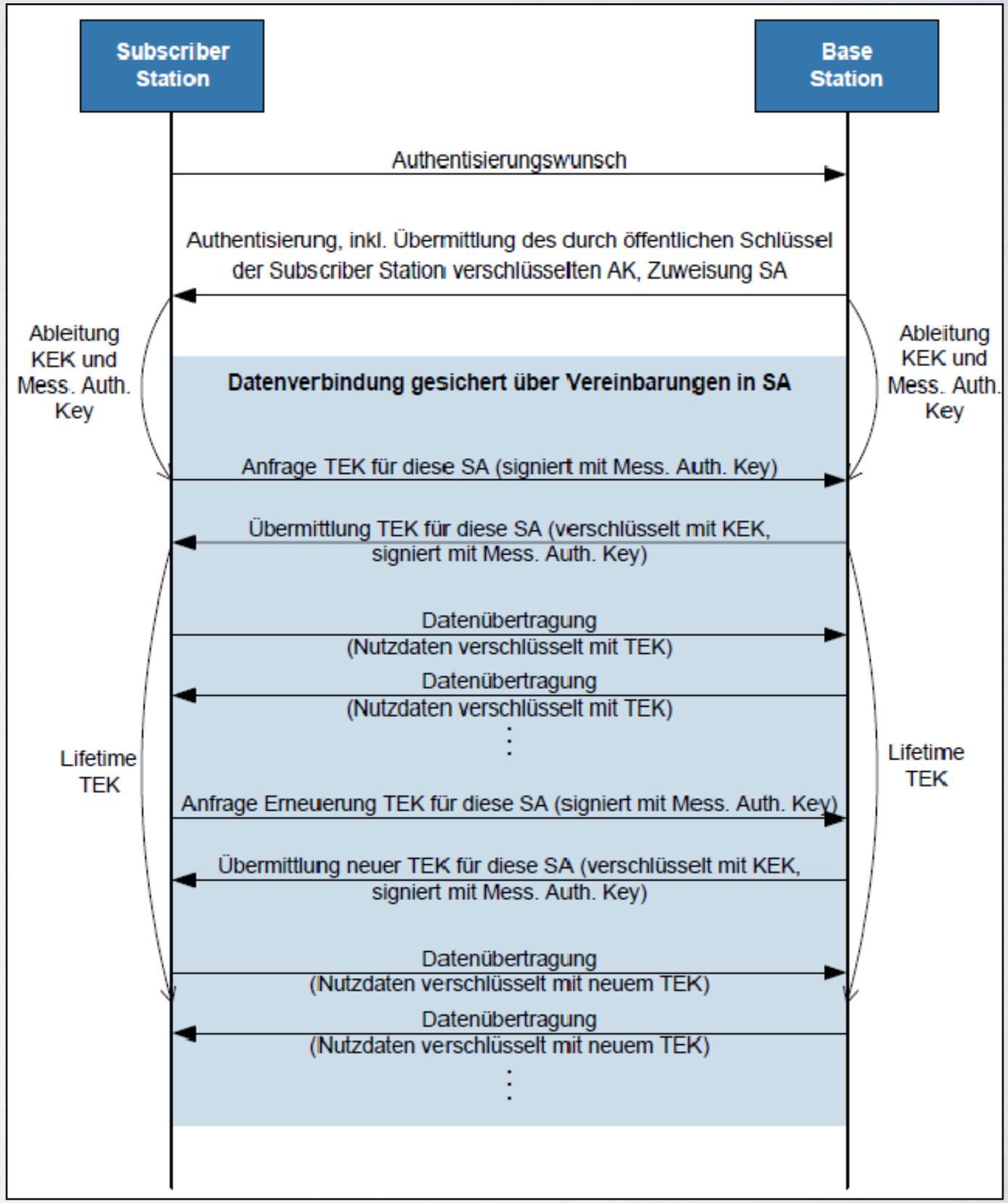
WiMAX Security

- Prozesse: Authentisierung
  - bei Netzeintritt
  - Zertifikat-basiert
  - *beidseitige* Authentisierung (nur WiMAX mobile)
  - weitere Option in WiMAX mobile: EAP

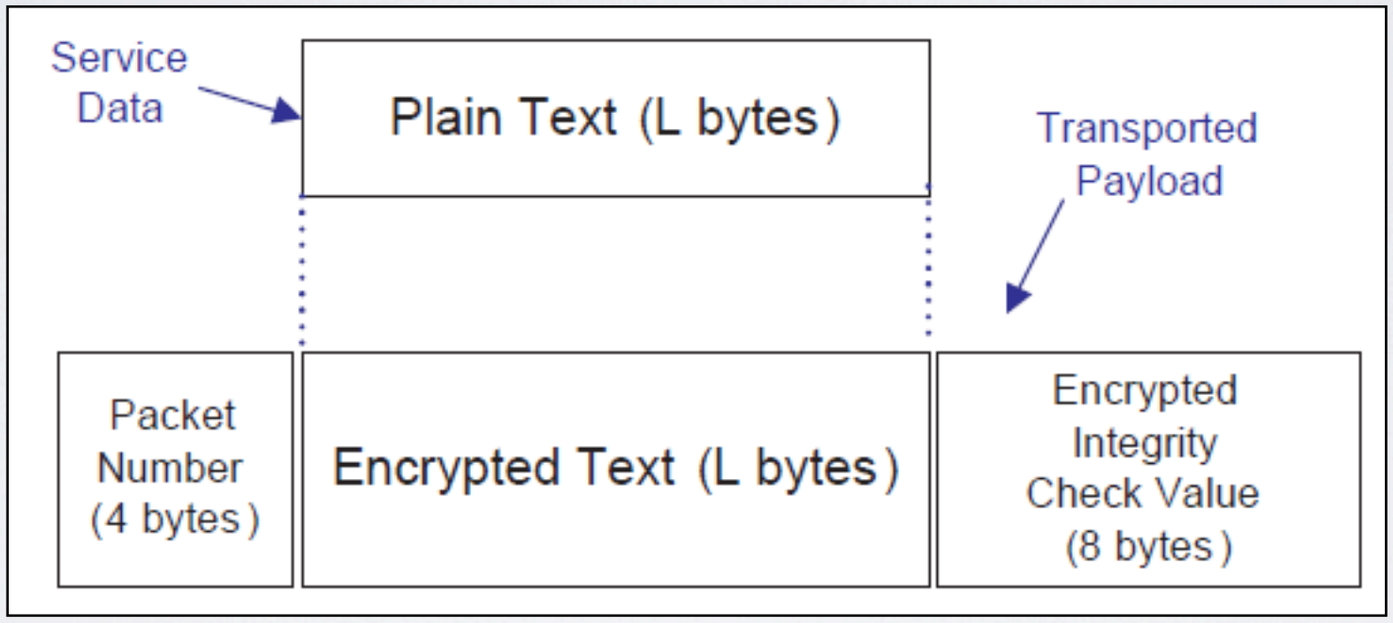


WiMAX Security

- Prozesse: Schlüsselverteilung



- Verschlüsselung
  - grundsätzlich nur für Payload eines MAC-Pakets möglich



  - keine Verschlüsselung von MAC Management-Nachrichten möglich
  - Encapsulation Protocol spezifiziert Cryptographic Suites für Verschlüsselung und Datenauthentisierung

WiMAX Security

- Verschlüsselung und Datenauthentisierung
  - Cryptographic Suites in WiMAX fixed

Cryptographic Suite ID	Datenverschlüsselung	Datenauthentisierung	TEK-Verschlüsselung
0x000001	keine	keine	3DES im EDE-Mode mit 128-Bit-Schlüssel
0x100001	DES im CBC-Mode mit 56-Bit-Schlüssel		
0x000002	keine		RSA mit 1024-Bit-Schlüssel
0x100002	DES im CBC-Mode mit 56-Bit-Schlüssel		
0x020103	AES im CCM-Mode mit 128-Bit-Schlüssel	(implizit durch AES im CCM-Mode)	AES im ECB-Mode mit 128-Bit-Schlüssel

WiMAX Security

- Verschlüsselung und Datenauthentisierung
  - Cryptographic Suites in WiMAX mobile

Cryptographic Suite ID	Datenverschlüsselung	Datenauthentisierung	TEK-Verschlüsselung
0x000001	keine	keine	3DES im EDE-Mode mit 128-Bit-Schlüssel
0x100001	DES im CBC-Mode mit 56-Bit-Schlüssel		
0x000002	keine		RSA mit 1024-Bit-Schlüssel
0x100002	DES im CBC-Mode mit 56-Bit-Schlüssel		
0x020103	AES im CCM-Mode mit 128-Bit-Schlüssel	(implizit durch AES im CCM-Mode)	AES im ECB-Mode mit 128-Bit-Schlüssel
0x020104			AES Key Wrap mit 128-Bit-Schlüssel
0x030003	AES im CBC-Mode mit 128-Bit-Schlüssel	keine	AES im ECB-Mode mit 128-Bit-Schlüssel
0x800003	AES im CTR-Mode mit 128-Bit-Schlüssel für Multicast-/Broadcast Services mit 8 Bit Rollover Counter		
0x800004			AES Key Wrap mit 128-Bit-Schlüssel

WiMAX Security

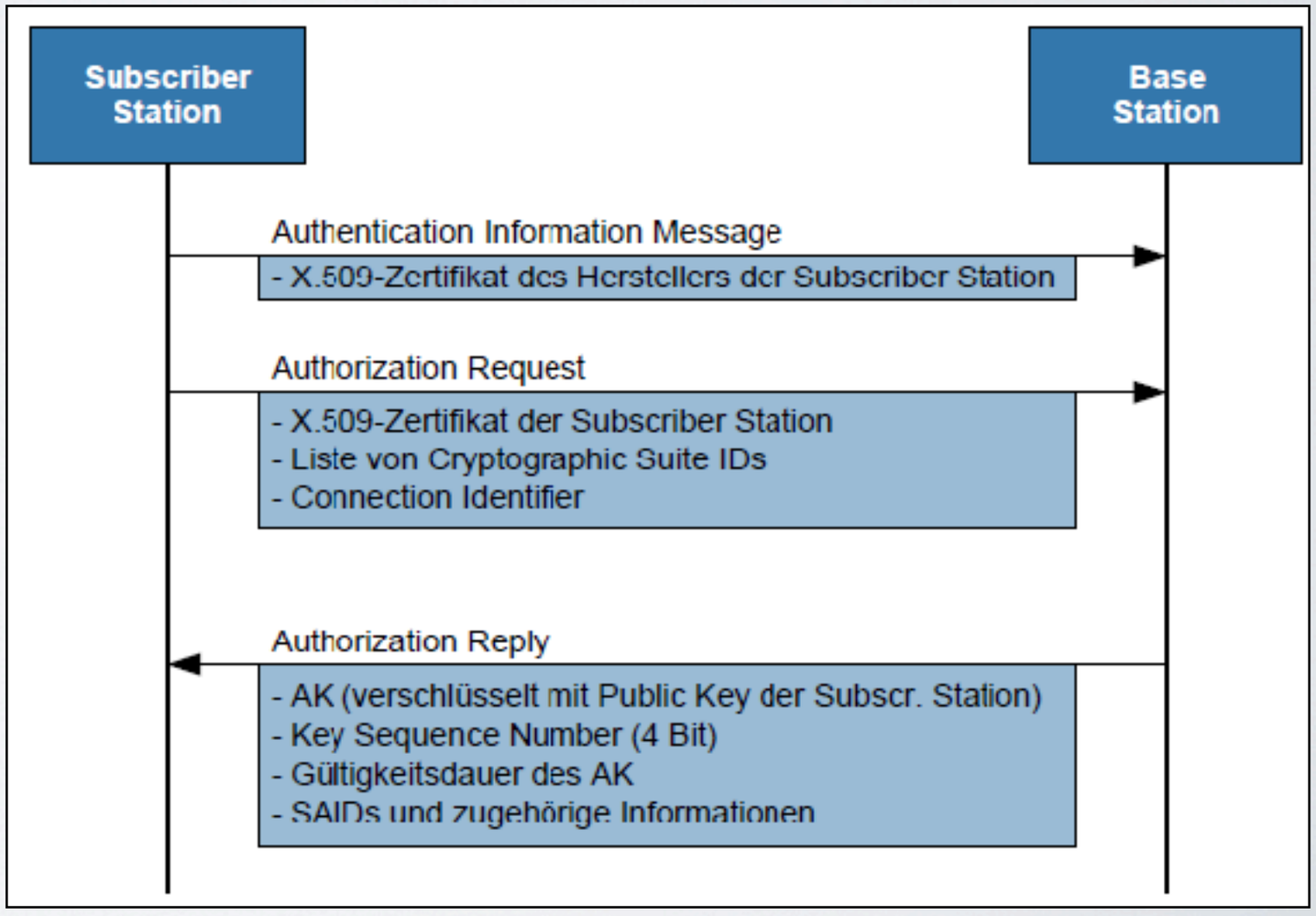
- Schwächen allgemein I
  - WiMAX fixed:
    - nur einseitige Authentisierung (SS <> BS): Meet/Man in the Middle-Attacks
    - keine oder schwache Verschlüsselungsmethoden wählbar (DES mit 56-Bit Key)
    - keine Datenauthentisierung vorgesehen: Manipulationen nicht erkennbar
  - WiMAX mobile:
    - PKMv1: nur einseitige Authentisierung (SS <> BS): s.o.
    - wenig sichere EAP-Methoden wählbar (z.B. Passwort-basierte)
  - MAC Management Nachrichten
    - unverschlüsselt: Informationsgewinnung möglich, da unverschlüsselt
    - anfällig für Replay-Attacken (keine Nonces/Timestamps, 2-Bit Key Sequence)
    - DoS-Attacken möglich

WiMAX Security

- Schwächen allgemein II
  - Schlüssematerial allein von BS bestimmt
    - Subscriber Station nicht an der Festlegung der Schlüssel beteiligt
    - Sicherheit der Schlüssel vom Schlüsselgenerator der BS abhängig
  - keine perfekte Forward Secrecy
    - bei Handover
    - bei Kompromittierung des Authorization Key
  - Erstellung von Bewegungsprofilen mobiler Nutzer möglich
  - ...und wie bei allen mobilen Technologien:
    - Störung, Jamming, Scrambling
    - Ausbreitung der Funkwellen in nicht-kontrollierte Gebiete
    - höhere Gewalt (Blitze, Witterung, Überspannung...)

WiMAX Security

- Schwächen des Authentisierungsprotokolls
  - einseitige Authentisierung
  - Replay-Attacken mit Nachricht 2 und 3
    - DoS-Angriff ggf. Ablehnung legitimer SS durch BS
- Verbesserungen:
  - Nachricht 2 zusätzlich mit
    - Timestamp der SS
    - Signatur
  - Nachricht 3 zusätzlich mit
    - Timestamp der BS und SS
    - Zertifikat der BS
    - Signatur



WiMAX Security

- Schwächen des Schlüsselverteilungsprotokolls
  - Protokoll:
    1. BS ➔ SS: Sequenznr, SAID, HMAC (optional)
    2. SS ➔ BS: Sequenznr, SAID, HMAC
    3. BS ➔ SS: Sequenznr, SAID, HMAC, bisheriger TEK, neuer TEK, HMAC
  - Replay-Attacken möglich mit Nachrichten 1 und 2:
    - jeweiliger Empfänger kann Replay-Attack nicht erkennen
    - erzeugt Last, führt zu häufigem Schlüsselaustausch + Irritation über aktuell gültige TEKs
  - Verbesserungen:
    1. BS ➔ SS: Timestamp(BS), Sequenznr, SAID, HMAC
    2. SS ➔ BS: Timestamp(BS), Timestamp(SS), Sequenznr, SAID, HMAC
    3. BS ➔ SS: Timestamp(BS), Timestamp(SS), Sequenznr, SAID, TEK(alt), TEK (neu), HMAC

WiMAX Security

- Schutzmaßnahmen
  - Absicherung der Datenkommunikation:
    - jeweils höchstmögliche Verschlüsselungsmethode wählen
    - Datenauthentisierung
    - beidseitige Authentisierung BS <> SS
    - bei sensiblen Daten durch VPN-Lösung zu ergänzen
  - Absicherung der Netzelemente
    - Voreinstellungen prüfen und anpassen, härten
  - Absicherung mobiler Clients
    - lokale Schutzmaßnahmen notwendig: Zugriffsschutz, Benutzerauthentisierung, Firewall, restriktive Ressourcenfreigabe und Browserkonfiguration etc.
  - Rest-Risiken: Bewegungsprofile erstellbar, bedrohte Verfügbarkeit

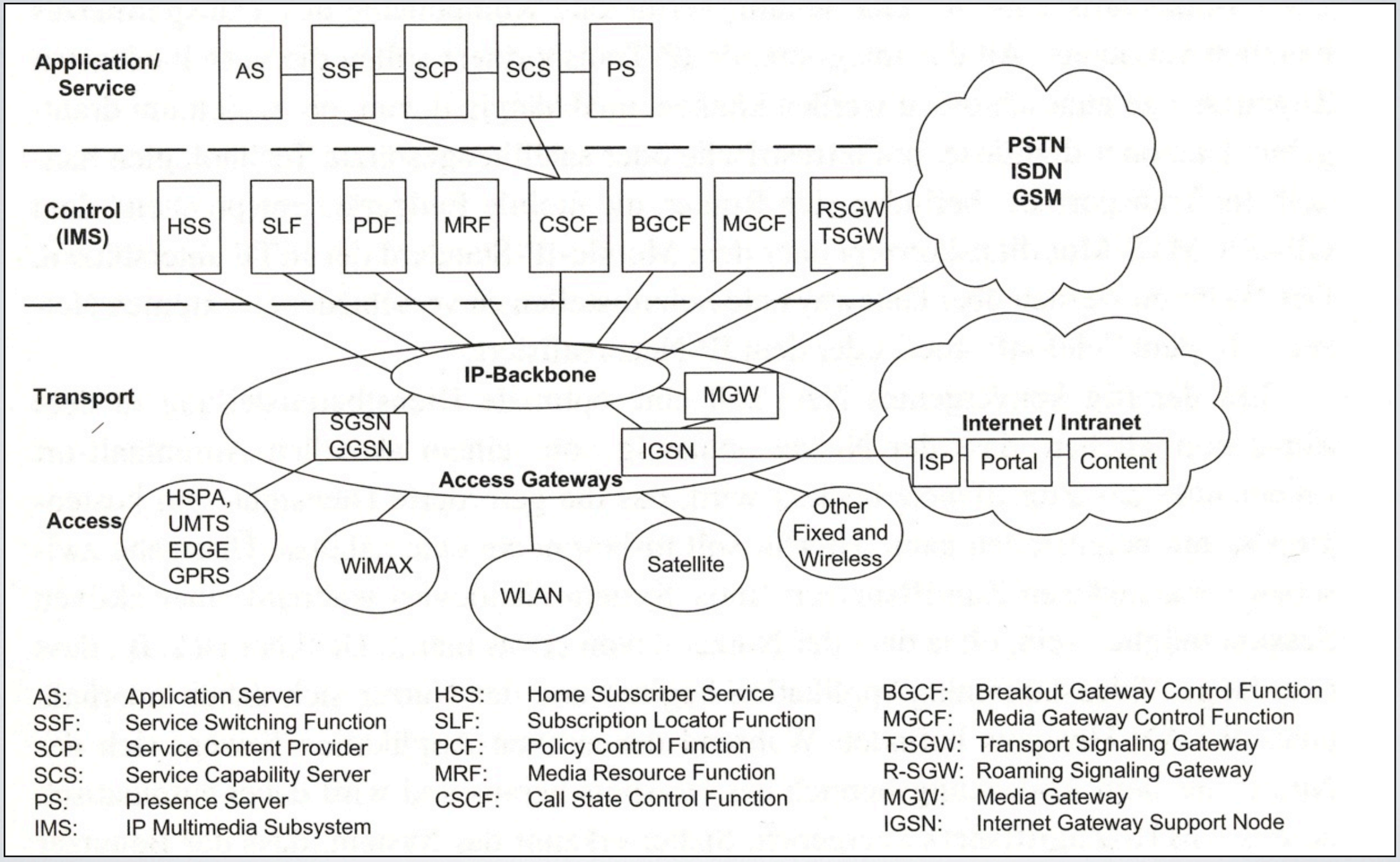
WiMAX Security

- Fazit
  - Authentizität
    - :-) Subscriber Station ➔ Base Station
    - :-| Base Station ➔ Subscriber Station (mobile)
    - :-(Base Station ➔ Subscriber Station (fixed)
  - Vertraulichkeit
    - :-) Schlüsselaustausch
    - :-| Datenpakete
    - :-(Management-Nachrichten
  - Integrität
    - :-) Schlüsselaustausch
    - :-) Management-Nachrichten
    - :-(Datenpakete

WiMAX Potenzial

- WiMAX Integration in zukünftige heterogene Netze
  - WiMAX nicht zwingend Konkurrenz zu WLAN oder UMTS
  - sondern als Backhaul einsetzbar
  - Netzarchitektur, die verschiedene Zugangsnetze an ein gemeinsames Transport- und Kontrollnetz anbindet = Netz der 4. Generation (4G)
  - z.B. unterbrechungsfreies Handover zwischen verschiedenen Zugriffsnetzen
- Vorteile
  - optimale Dienstbereitstellung
  - Session bleibt beim Handover aktiv
  - günstigere Lizenzen als bei UMTS

WiMAX Potenzial



AS:	Application Server	HSS:	Home Subscriber Service	BGCF:	Breakout Gateway Control Function
SSF:	Service Switching Function	SLF:	Subscription Locator Function	MGCF:	Media Gateway Control Function
SCP:	Service Content Provider	PCF:	Policy Control Function	T-SGW:	Transport Signaling Gateway
SCS:	Service Capability Server	MRF:	Media Resource Function	R-SGW:	Roaming Signaling Gateway
PS:	Presence Server	CSCF:	Call State Control Function	MGW:	Media Gateway
IMS:	IP Multimedia Subsystem			IGSN:	Internet Gateway Support Node

erste Geräte

- Nokia N810 WiMAX Edition
  - seit April 2008
  - nur in ausgewählten Gegenden der USA vertrieben, in denen WiMAX verfügbar ist
  - unterstützt WiMAX mobile
  - 2-4 Mbit/s in Funkzellen von 6-10 Km Durchmesser
  - Roaming-fähig

- Siemens Gigaset SE68 Express Card
  - seit Sommer 2008
  - basiert auf 802.16-2005
  - mögliche Frequenzbänder: 2.5 und 3.5 GHz
  - bis 20 Mbit/s

WiMAX Einsatz

- http://www.neckarcom.de
  - 44,90€ / Monat
  - 3.072 kbit/s Downstream
  - 348 kbit/s Upstream
- http://www.dbd-breitband.de
- http://www.maxxonair.de/
  - ab 9,99€ / Monat Datenflatrate
  - 64 kbit/s
- http://www.dslonair.de
  - keine Preise einsehbar ohne Verfügbarkeitsprüfung
- Offene Fragen
  - Anzahl der Nutzer?

DBD Deutsche Breitband Dienste

MAXXonair ...hier bin ich der Star.

DSLonair

WiMAX Einsatz

- Clearwire:
  - bietet bereits in Belgien an
  - Services in Deutschland in Vorbereitung
- Inquam / Nextwave
  - seit 2008 strategische Kooperation mit Alcatel Lucent für WiMAX-Geräte
  - insbesondere WiMAX-Lösungen für gewerbliche Nutzung, z.B. für Mobilfunkbetreiber im Backhauling Bereich
- MGM Productions
  - keine Angaben zum Netzausbau gefunden

Iquam kooperiert mit Nextwave und die Kooperieren mit Alcatel

hörte sich eher nach einer gewerblichen Lösung an

kommen aus Italien,

Lizenzen für Oberbayern

Pressespiegel

- "Die Versteigerung der so genannten Wimax-Frequenzen für den Internetzugang per Funk ist beendet. Nach Angaben der Bundesnetzagentur brachte die Auktion insgesamt 56,1 Millionen Euro."

...

"Mit rund 56 Millionen Euro fließt nun viel weniger Geld in die Staatskassen als erhofft. Das Mindestgebot für alle 112 Frequenzpakete hatte bei knapp 60 Millionen Euro gelegen. Allerdings wurden für 25 gar keine Gebote abgegeben."
[tagesschau.de]

Pressespiegel

- "Die Regulierungsbehörde hatte 2006 Frequenzpakete aus dem 3,5-GHz-Band für den Broadband Wireless Access (BWA) versteigert, um die weißen Flecken in der Breitbandversorgung zu schließen. Derzeit sieht es nicht danach aus, als ob das Versorgungsziel von mindestens 15 Prozent Abdeckung im Lizenzgebiet bis Ende 2009 und von 25 Prozent bis Ende 2011 erreicht würde; vier der fünf Lizenznehmer hinken mit dem Ausbau weit zurück."

  ...

  "Die in der Bundesnetzagentur für die Telekom-Regulierung zuständige Vizepräsidentin Henseler-Unger versuchte gar nicht erst, den Wimax-Flop zu beschönigen. „Wir sind alle gebrannte Kinder“, konzedierte sie. „Die Unternehmen hatten uns versprochen, der ländliche Raum werde versorgt.“ Jetzt sei klar, „eine Selbstverpflichtung der Mobilfunker reicht eindeutig nicht“."

  [Richard Sietmann, Spektrum in bester Lage, c't 26/2008, http://www.heise.de/ct/Mobilfunker-starten-zum-Angriff-auf-die-Rundfunk-Festung--/artikel/126538]

- - "...wurde Wimax teilweise bereits als Alternative zu DSL und UMTS gefeiert. "Eine Euphorie, vor der Fabio Zoffi, CEO bei der DBD, warnt: "Es ist absurd zu denken, dass Wimax der DSL- oder UMTS-Killer wird"."

  ...

  "Reichhaltige Möglichkeiten sieht auch Intel-Manager Thiel. Er hebt noch einen anderen Aspekt hervor: "Da zum Aufbau eines Wimax-Netzes nur die Basisstation und ein entsprechender Empfänger beim Benutzer benötigt werden, eignet sich die Technik auch, um temporäre Netze auf Großveranstaltungen wie Messen oder Sport-Events kostengünstig einzurichten.""

  [tecchannel, Vom Wimax-Hype zur Realität, tecchannel 2005, http://www.tecchannel.de/kommunikation/news/433783/vom_wimax_hype_zur_realitaet/]

Pressespiegel

- "Damit stellt sich WiMAX nicht nur als Konkurrent zu den Brückenverbindungen, sondern auch zu den zukünftig zu erwartenden vermaschten Topologien des WLAN auf. Vor allem aber bietet es sich dort als Alternative zu DSL-Netzen an, wo aus Kostengründen eine Verkabelung nicht sinnvoll erscheint. Hier ist auch der Ursprung des markigen Wahlspruchs von Intel „Connecting the Next Billion People" zu sehen, da WiMAX die Möglichkeit bietet, breitbandige Zugangsnetze ohne aufwendige und leitungsgebundene Infrastruktur bereitzustellen."
  [Prof. Dr. Axel Sikora, Grundlagen WiMAX - Anwendung, Architektur und Aufbau, tecchannel 2005, http://www.tecchannel.de/netzwerk/wan/433538/grundlagen_wimax_anwendung_architektur_und_aufbau/]

- "Mit als realistisch angesehenen 3 Mbit/s eignet sich der technisch als 802.16d (Fixed Wimax) benannte Standard aber noch immer als alternativer Breitbandzugang in den bislang nicht mit DSL ausgebauten Regionen. Problematisch wird es jedoch, wenn man an die Geschäftsmodelle der Unternehmen denkt, die im Dezember 2006 eine der bundesweiten oder regionalen Broadband-Wireless-Access-(BWA-)Lizenzen ersteigert haben."

  ...

  "Gemäß den Vorgaben der Bundesnetzagentur müssen die Lizenznehmer bis zum Jahresende 2009 für ihr Gebiet in 15 Prozent aller Gemeinden zumindest eine Grundversorgung sicherstellen. Bis 2011 soll diese auf 25 Prozent aller Gemeinden ausgeweitet werden. Angesichts der Kosten von fast 100.000 Euro je Wimax-Basisstation ist anzunehmen, dass die Provider zumindest eine "Mischkalkulation" fahren und die Technik neben strukturschwachen Gemeinden ohne DSL-Versorgung auch in mittleren und großen Städten anbieten."
  [Manfred Bremmer, Schluss mit lahmen Anschlüssen: Breitbandalternativen zu DSL, tecchannel 2007, http://www.tecchannel.de/netzwerk/wan/1716548/schluss_mit_lahmen_anschluessen_breitbandalternativen_zu_dsl/]

Fazit

- Potenzial zu global anerkanntem und implementierten Standard für im Wireless Metropolitan Area Network-Bereich
- WiMAX-Forum als Zertifizierer bürgt für Interoperabilität und Kompatibilität
  → Wettbewerb möglich
- Standard aber recht flexibel und weit gefasst
  → Gefahr proprietärer Implementierungen
- Intel als Antreiber
  → WiMAX-Chipsets in Endgeräten, ähnliche Strategie wie bei WLAN
- viele Anwendungsszenarien: Backhauling, Last Mile, zellulare Netze...
- Konkurrenztechnologien: WLAN, UMTS, HSPA
- entscheidende Faktoren für Erfolg/Misserfolg:
  - Kosten
  - Verfügbarkeit
  - Akzeptanz
  - Interoperabilität

Fragen?

Quellen

- Literatur
  - WiMAX - Der IEEE-802.16-Standard: Technik, Anwendung, Potenzial; Johannes Maucher, Jörg Furrer; Heise Verlag 2007
- Internetartikel
  - Bundesamt für Sicherheit in der Informationstechnik: Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte, 2006 http://www.bsi.de/literat/doc/drahtkom/drahtkom.pdf
  - Konkurrenzwellen - Richard Sietmann 2005; Heise Mobil http://www.heise.de/mobil/Wimax-soll-den-Markt-fuer-mobiles-Internet-aufrollen--/artikel/62460/0
  - Grundlagen WiMAX - Prof. Dr. Alex Sikora 2005; Tecchannel http://www.tecchannel.de/netzwerk/wan/433538/grundlagen_wimax_anwendung_architektur_und_aufbau/index.html
  - Xu, S., Matthews, M., Huang, C.-T.: Security Issues in Privacy and Key Management Protocols of IEEE 802.16, ACM South East Conference 2006 http://www.cse.sc.edu/~huangct/acmse06cr.pdf
  - Barbeau, M.: WiMax/802.16 Threat Analysis, Carleton University Ottawa 2005 http://www.scs.carleton.ca/~barbeau/Publications/2005/iq2-barbeau.pdf
- sonstige Internetquellen
  - http://wimaxxed.com/
  - http://www.dbd-breitband.de/
  - http://4gtrends.com/?page_id=29
  - http://www.wimax-industry.com/

Vielen Dank für Ihre/eure Aufmerksamkeit!