Security Architecture for WiMAX

Dirk Kroeselberg, Siemens

Semyon Mizikovsky, Lucent

SIEMENS

Lucent Technologies
Bell Labs Innovations

March 2006

Motivation of this presentation

- To provide an overview of the current security architecture developed by the WiMAX Forum Networking Group to SA3
- To provide input for future SAE security discussion as WiMAX is expected to become an important non-3GPP radio access technology
- To discuss iWLAN (Scenarios 2 and 3) mapping to WiMAX networks, and related issues

The overall goal is to improve interworking of WiMAX with future 3GPP networks within the frame of SAE

To support this, the presentation is meant to start discussion in SA3 on the related security aspects.

Presentation overview

WiMAX network architecture

What is new in WiMAX security

Secure Network Access

Mobility and Security

Current WiMAX-3GPP Interworking Model

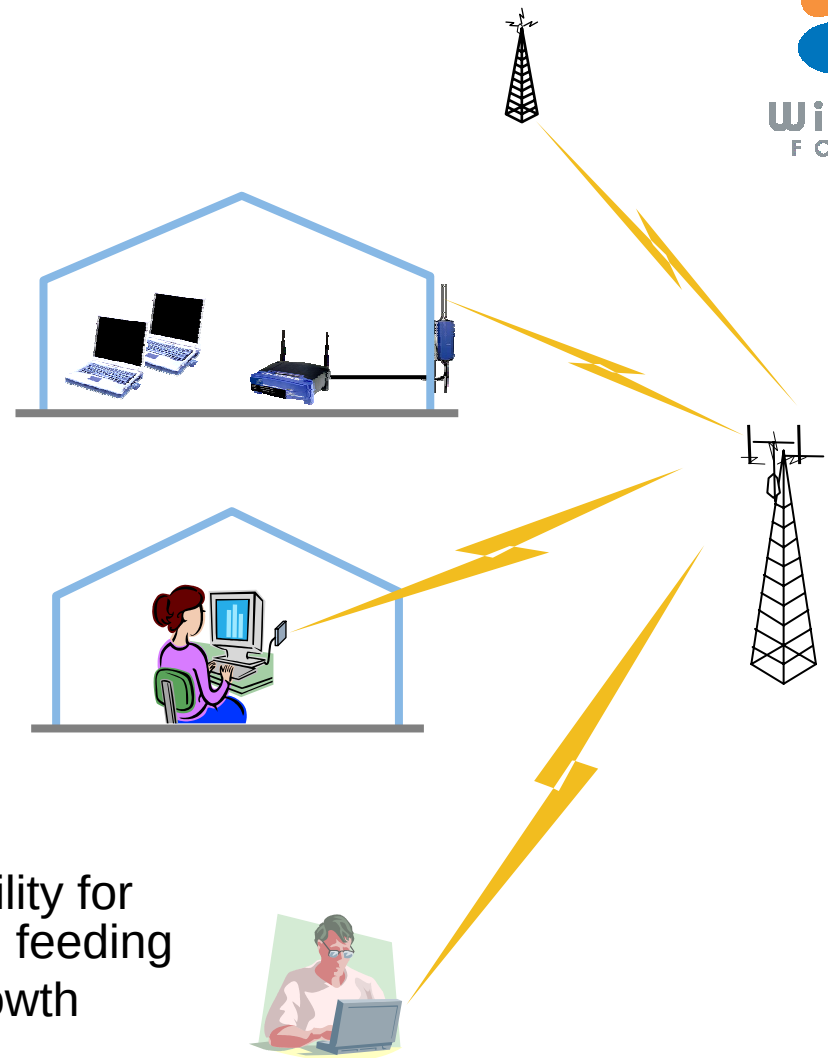
The evolution of WiMAX

Backhaul feeding
- PtP links for fixed infrastructure
- Dedicated market w/ limited size

Fixed Wireless Access
- Wireless local loop, hotspot feeding
- e.g. for remote areas without DSL

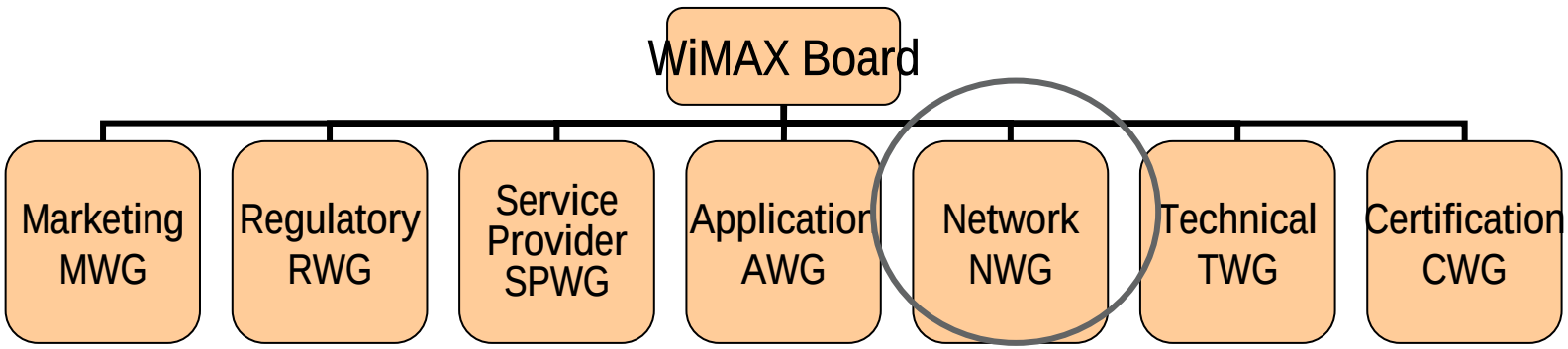
Nomadic Access (Hotzone)
- Indoor CPE thanks to better radio
- CPE may be integrated into terminal
- Most promising for mass market

Portable Access
- Handover function enabling data mobility for road warriors, train feeding and coach feeding
- Mobility enables persistent market growth

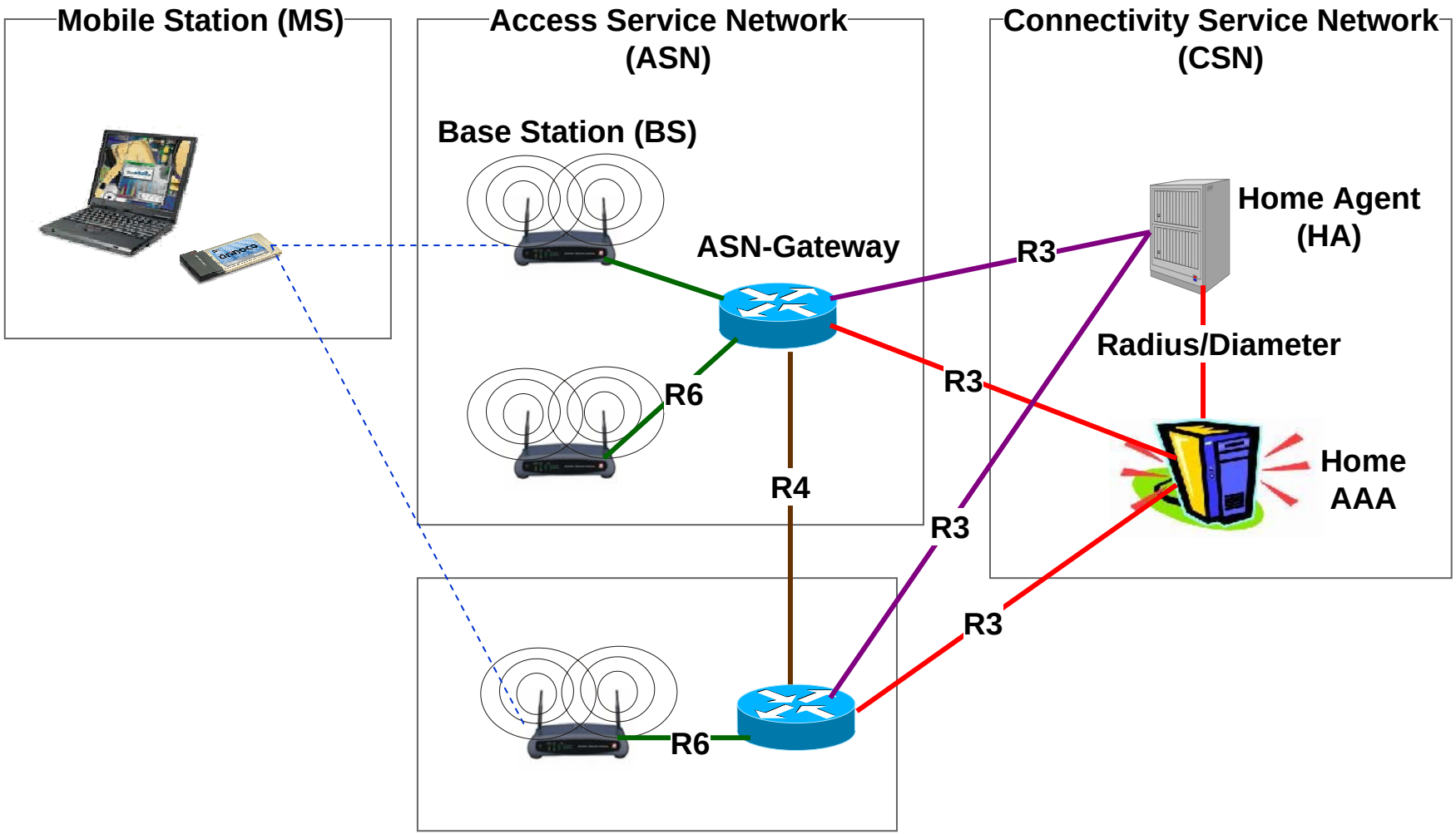


WiMAX Forum:
Worldwide Interoperability for Microwave Access

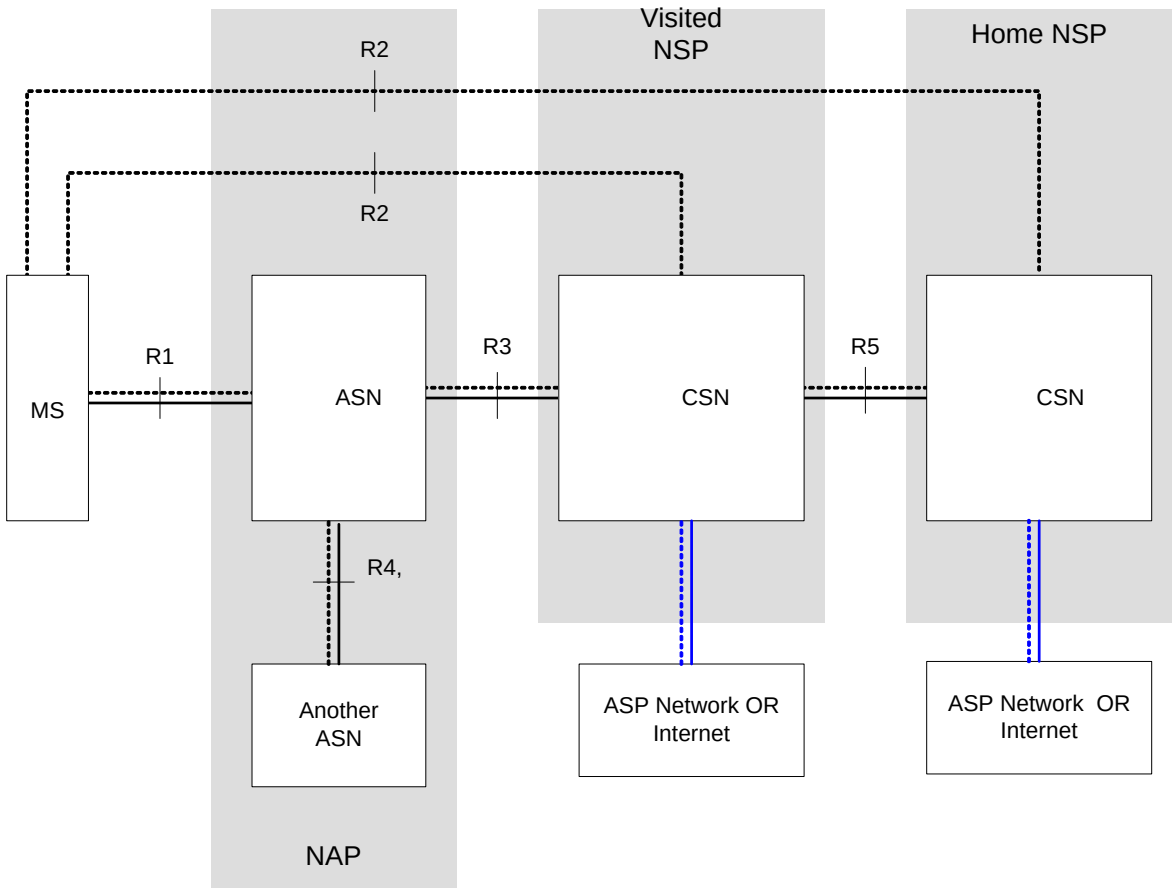
- The purpose of WiMAX is to promote deployment of broadband wireless access networks by using a global standard and certifying interoperability of products and technologies.
  - Support IEEE 802.16 standard, propose and promote access profiles
  - Certify interoperability levels both in network and the cell
  - Achieve global acceptance, promote use of broadband wireless access overall



WiMAX Network Architecture



WiMAX Network Architecture (Roaming Case)



MS: Mobile Station

ASN: Access Service Network

CSN: Connectivity Service Network

NAP: Network Access Provider

NSP Network Service Provider

Rx: reference points

Presentation overview

WiMAX network architecture

What is new in WiMAX security

Secure Network Access

Mobility and Security

Current WiMAX-3GPP Interworking Model

What is new in mobile WiMAX security (overview)

The WiMAX Architecture comes with

- some similarities with WLAN security (EAP), or 3GPP2 (Mobile-IP/AAA)
- a number of new approaches

For Network Security

- EAP-based device **and** user authentication
- Bootstrapping Mobile IP security from network access

For the Wireless Link (802.16e):

- MAC layer security: PKMv2
- Key hierarchy (different from WLAN)

Presentation overview

WiMAX network architecture

What is new in WiMAX security

Secure Network Access

Mobility and Security

Current WiMAX-3GPP Interworking Model

WiMAX secure network access: Overview

User Authentication

- Network access requires EAP-based authentication (Extensible Authentication Protocol, RFC3748, also used for Wi-Fi)
- Radius-based AAA infrastrucure for authentication with home operator

Device Authentication

- Also based on EAP methods and AAA infrastructure.
- If based on Certificates it can terminate in the local/visited network
- If based on PSK it has to terminate in the home CSN
- Can be combined with user authentication, i.e., another EAP round before user authentication takes place

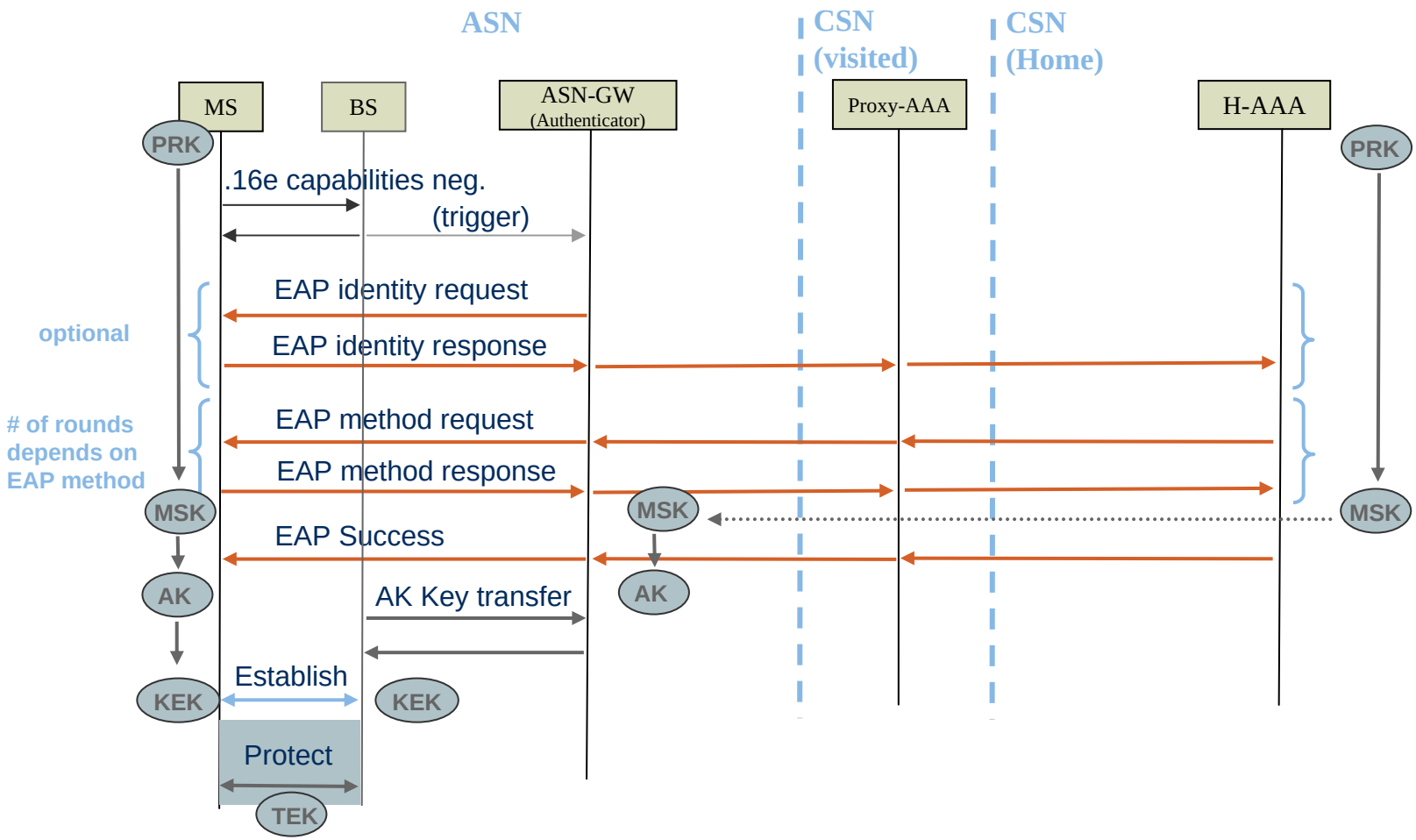
Wireless link security

- Mobile WiMAX (.16e MAC layer) uses PKMv2
- Fixed WiMAX (.16-2004 MAC layer) uses PKM

EAP and key derivation

- EAP exchange yields 512-bit MSK and EMSK keys, derived in MS and AAA home server (based on long-term key PRK)
- MSK transferred from AAA server to Authenticator in ASN-Gateway
- ASN-Gateway and MS truncate MSK to 160-bit PMK, and subsequently generate AK from this:
  AK = Dot16KDF(PMK, MS MAC Address | BSID | "AK", 160)
- AK is transferred from ASN-Gateway to BS

EAP/AAA authentication in WiMAX



User / Device Authentication profiling WiMAX

Device authentication changes

- from local RSA-based (currently used for 802.16 2004 fixed access)
- to more flexible EAP-based

Both user and device authentication can take place

- Starting with device auth that may terminate locally in the ASN
- Followed by user auth terminating in the Home-AAA
- At the wireless MAC layer, EAP user auth is protected by keys generated during device auth (Authenticated EAP-after-EAP)

Optional Optimization:

- only one round of EAP with combined shared secrets
- Prerequisites: Both device and user auth terminate in the same AAA-server, and use the same EAP shared secret method.

User / Device Authentication in IEEE802.16e

Both device and user authentication are supported

IEEE 802.16e defines numerous options

Profiling provided by the WiMAX NWG:

Value			Description	Scope
Bit #0	Bit #1	Bit #2		
0	0	0	No Authorization	SBC-RSP, PKM-RSP
0	0	1	N/A	
0	1	0	Only EAP-based authorization	
0	1	1	Authenticated EAP-based authorization after EAP-based authorization	
1	0	0	Only RSA-based authorization	
1	0	1	Authenticated EAP-based authorization after RSA-based authorization	
1	1	0	EAP-based authorization after RSA-based authorization	
1	1	1	N/A	

PKMv2 Security (1)

Step 1: Security Parameter Negotiation

- Which PKM version / authorization policy?
- Which type of authentication and integrity protection for management messages?

Step 2: Authentication and Derivation of PKM Keys

- Wireless link key hierarchy starts with Authorization Key (AK)
- Derivation of keys for protecting management messages
- Derivation of Key Encryption Key (KEK)

Step 3: 3-Way Handshake

- Validate liveliness of AK using mutually authenticated Bellare-Rogaway protocol
- In case of initial network entry, negotiation of Cryptographic Suite
- BS provides MS with Traffic Encryption Keys (TEKs) encrypted by KEK

Presentation overview

WiMAX network architecture

What is new in WiMAX security

Secure Network Access

Mobility and Security

Current WiMAX-3GPP Interworking Model

WiMAX mobility solution

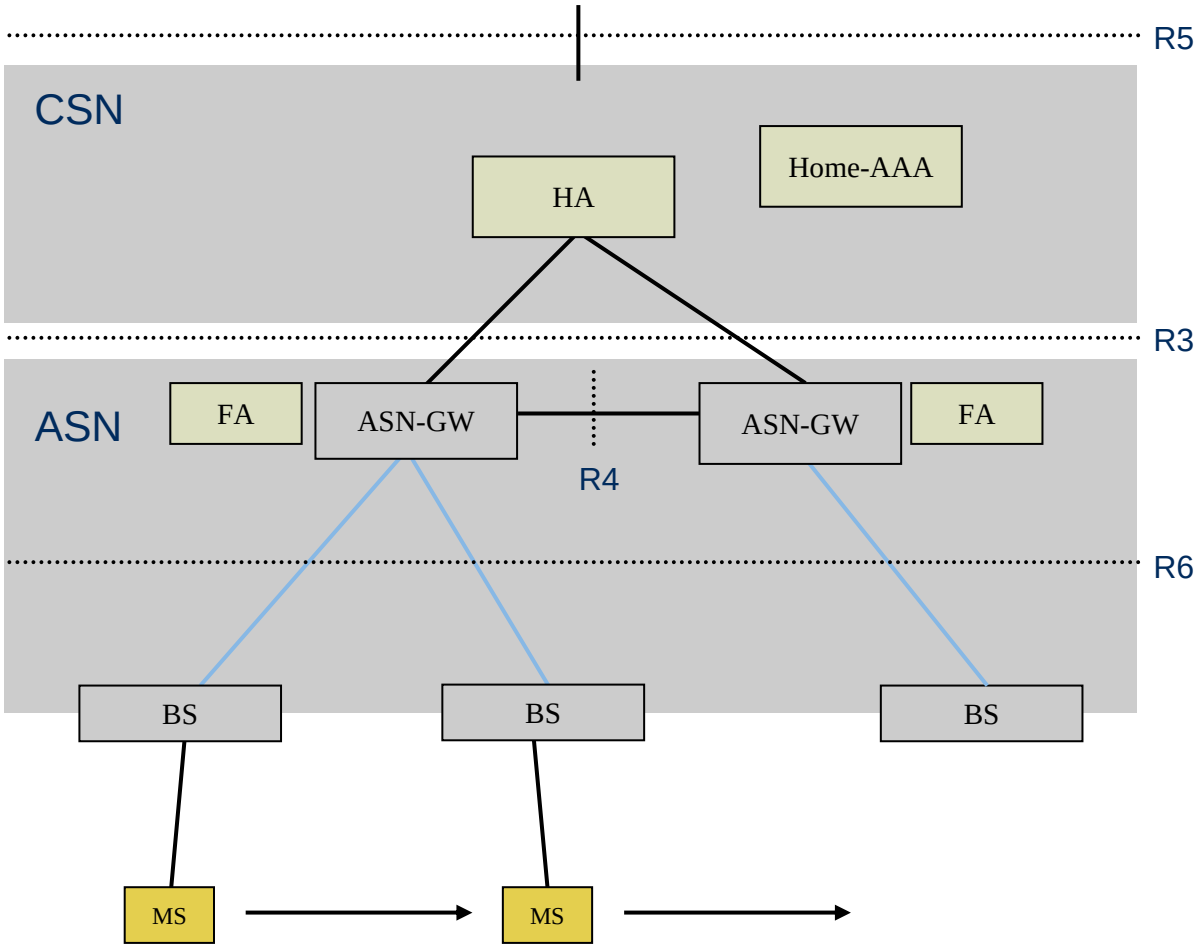
Uses IETF-defined Mobile IP.

Two levels of mobility:

- Micro Mobility (ASN Mobility Management)
  - MS moves between base stations but keeps ASN-Gateway as anchor for data traffic
  - The CSN is not affected by this

- Macro-Mobility (CSN Mobility Management)
  - MS moves between ASN-Gateways (Mobile IP Foreign Agents)
    - Mobile IP (CMIP) for MS with MIP support
    - Proxy Mobile IP (PMIP) for devices without MIP support
  - CSN is involved via reference point R3

WiMAX Micro- and Macro-Mobility

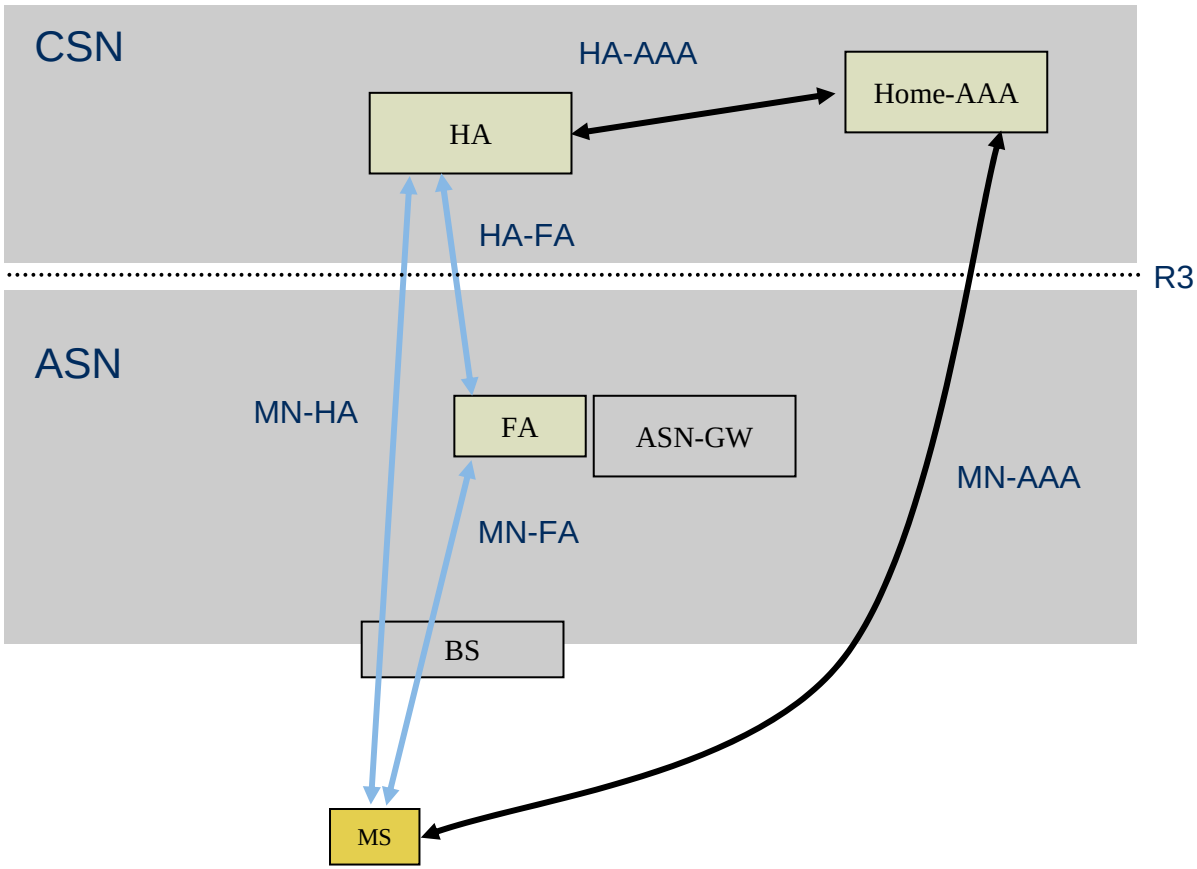


Interfaces affected by:

Micro-Mobility

Macro-Mobility

WiMAX CMIP security associations

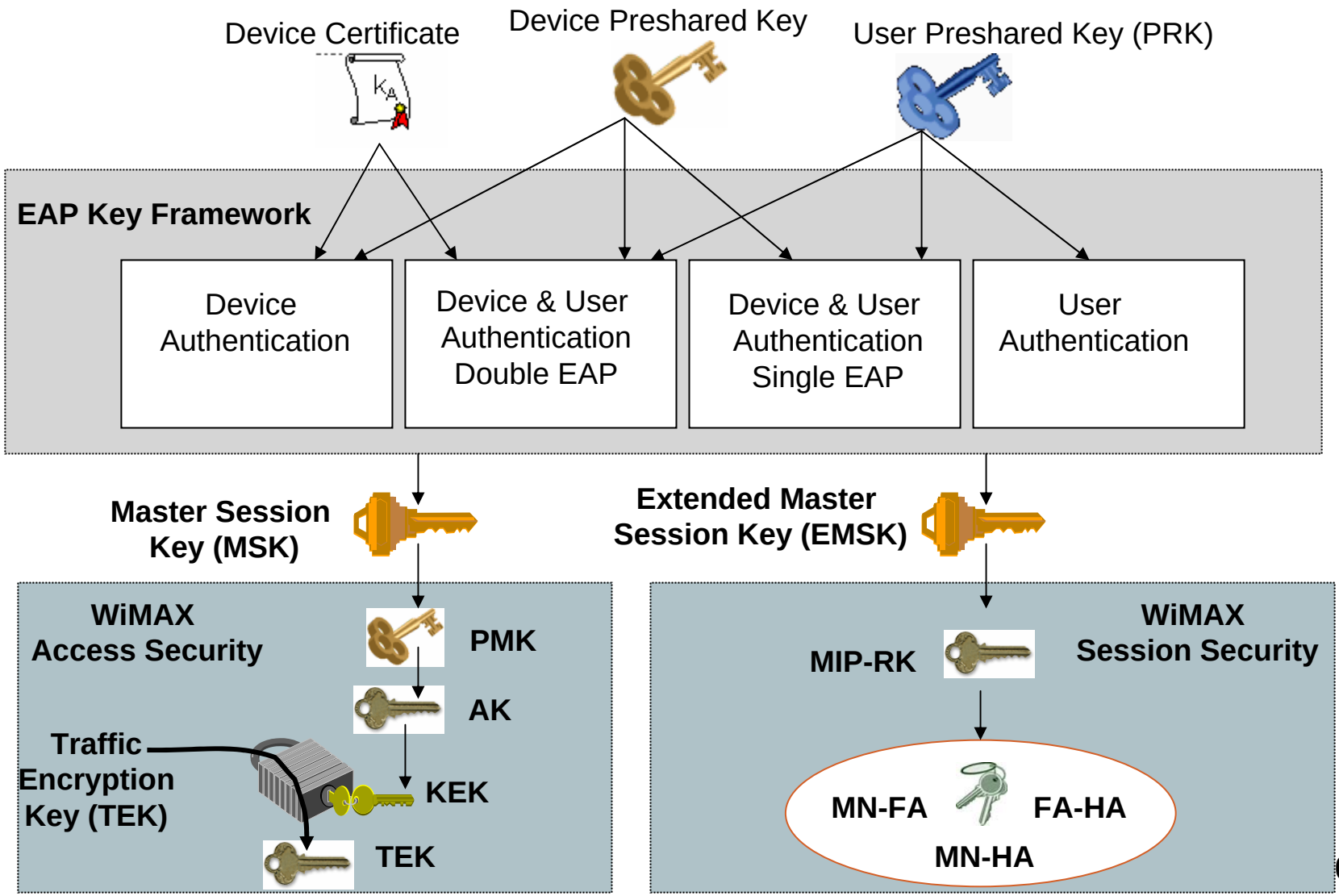


Mobile IP Security associations:

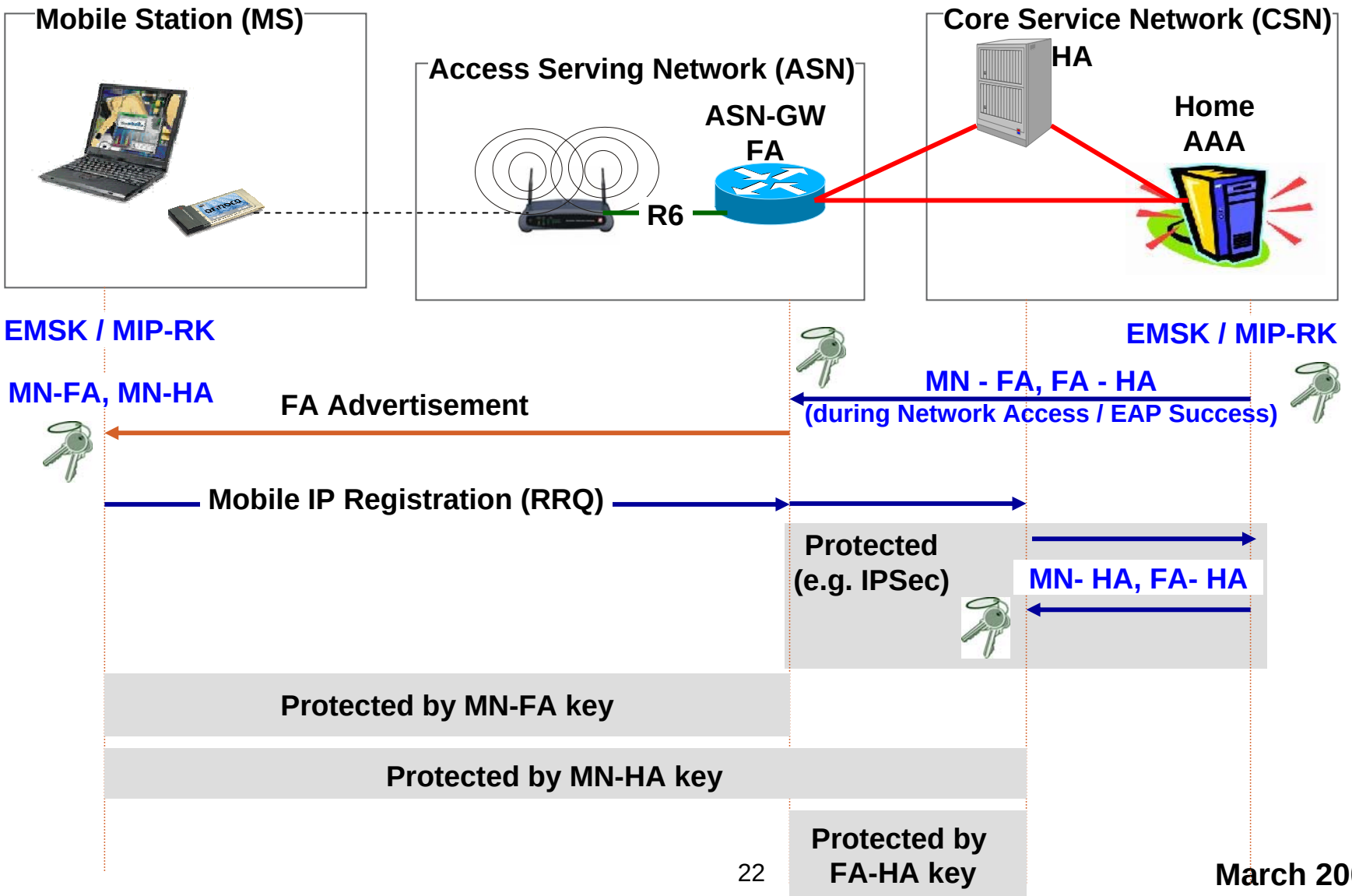
Created during MIP registration

Required prior to MIP registration

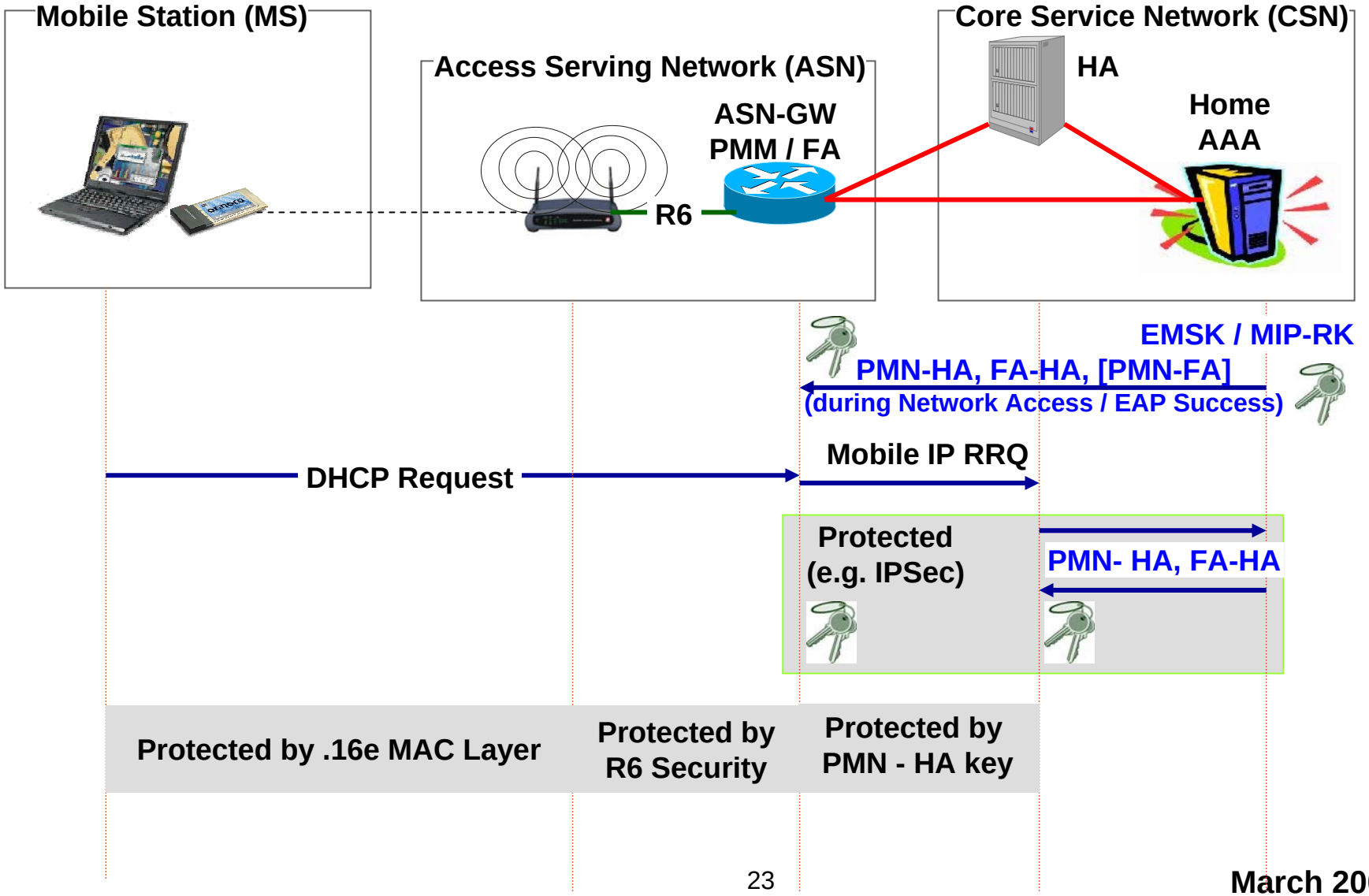
WiMAX Key Hierarchy supporting Mobile IP security



Mobility Support & Security (Client MIP)



Mobility Support & Security (Proxy MIP)



Bootstrapping MIP in WiMAX: Conclusion

Advantages

- **Keying MIP from H-AAA** instead of HA is required for mobility/roaming
  - otherwise, hard and less secure to share keys between different HAs
- **Dynamic MIP keying from EAP** authentication
  - Reduces administrational overhead (two sets of keys per user)
  - Generates fresh MIP keys
  - Provides keys for **both CMIP and PMIP**

Note

- Concept may still be subject to change during stage-3 work in WiMAX NWG

Presentation overview

WiMAX network architecture

What is new in WiMAX security

Secure Network Access

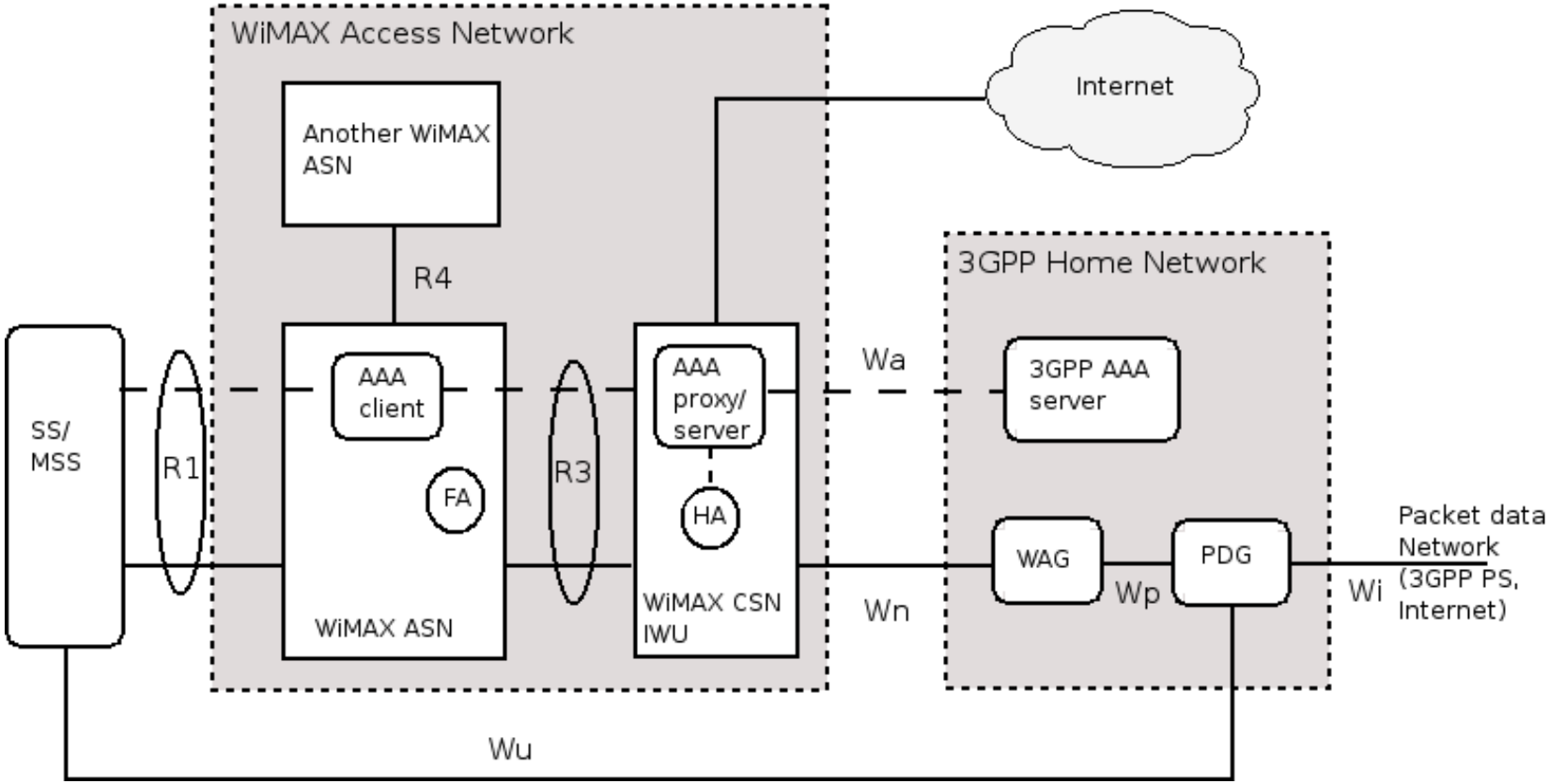
Mobility and Security

Current WiMAX-3GPP Interworking Model

Current WiMAX Interworking Model for 3GPP Subscribers

- Defined as initial solution for WiMAX Release 1; further advancements are required with focus on SAE time frame
- Approach is similar to iWLAN
  - „Scenario 2“ allows to bootstrap WiMAX security; 3GPP AAA server acts as home AAA, instead of a WiMAX CSN
  - „Scenario 3“ allows access to 3GPP PS core; also uses 3GPP IPsec tunnel between MS and PDG
  - Scenario 3 is on top of scenario 2 in WiMAX, as security for the wireless link is mandatory and is always based on EAP
  - Authentication methods: EAP-SIM, EAP-AKA

WiMAX Interworking Model with 3GPP



Conclusion for 3GPP-WiMAX interworking

- The idea in WiMAX NWG is to participate in 3GPP SAE discussion to evolve towards a more flexible long-term solution for non-3GPP radio access systems

- Possible issues for WiMAX in SAE are:
  - 3GPP AAA server does not support WiMAX MIP keying, or interface to Mobile IP Home Agent (currently limited to PMIP only)
  - is an IPsec tunnel from the MS to a 3GPP-controlled PDG across a WiMAX network infrastructure required in SAE for security reasons?

Thanks for your attention!