

Mobile WiMAX Network Security: Overview and Selected Aspects

MobiSec 2009, June 03-05, Turin, Italy

Dirk Kroeselberg (presenter), Nokia Siemens Networks
Rainer Falk, Siemens Corporate Technology
Christian Guenther, Nokia Siemens Networks
Avi Lior, Bridgewater Systems





Presentation overview

- WiMAX Forum Overview
- Mobile WiMAX Network Reference Architecture
- Security Building Blocks
- Enabling Protocol Security
- Authentication and Identity
- Outlook

The WiMAX Forum

(Worldwide Interoperability for Microwave Access)

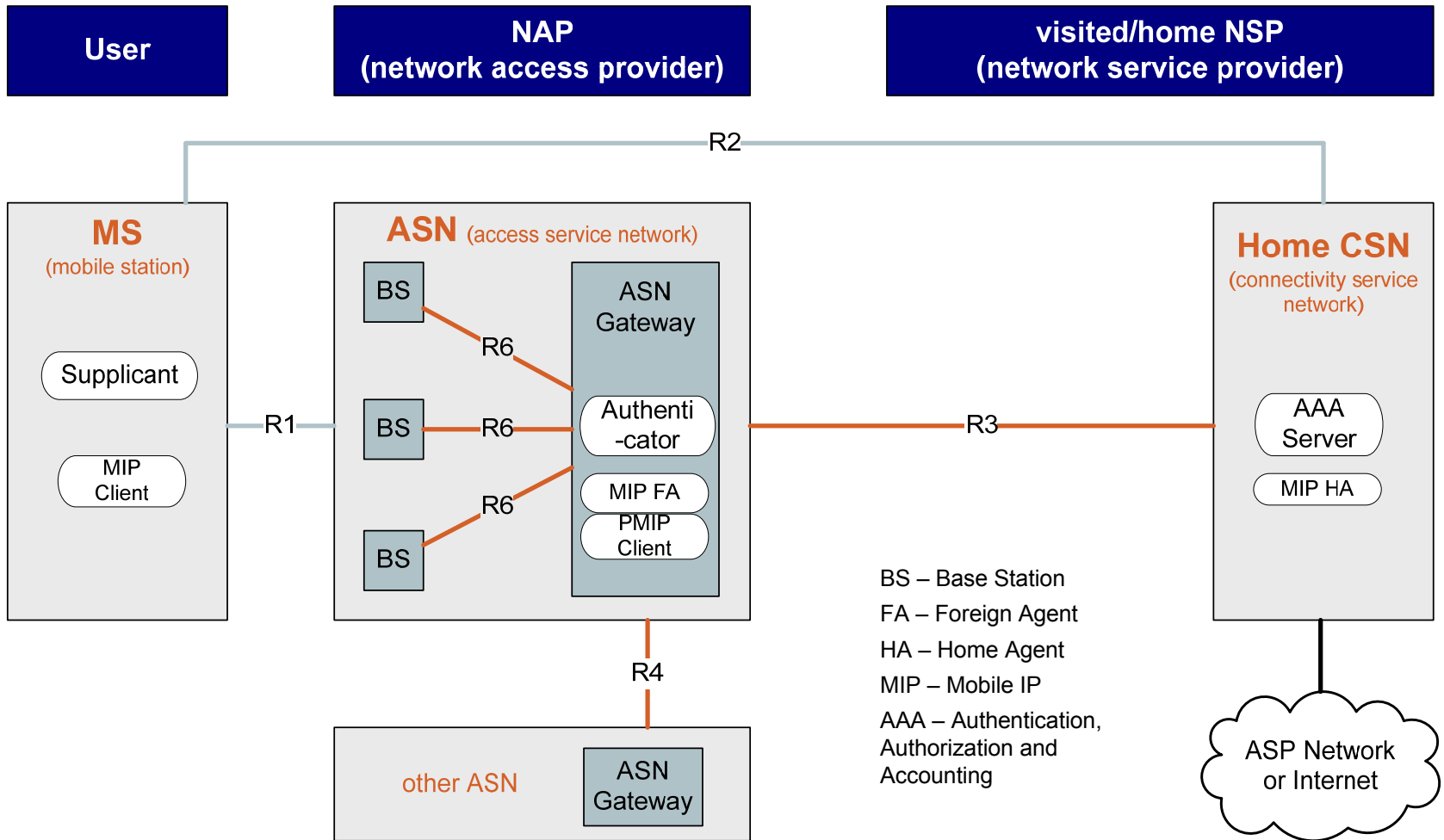


The WiMAX Forum promotes the deployment of broadband wireless access networks by supporting a global standard and certifying interoperability of products and technologies.

- Support IEEE 802.16 standard family
- Propose and promote access profiles for their IEEE 802.16 standard
- Certify interoperability levels both in the network and the radio interface (note: Certification != Certificates)
- More than 500 member companies and many other stakeholders
- **Important for this presentation:**
The network specifications for WiMAX are created by the WiMAX Forum Networking Group (NWG)



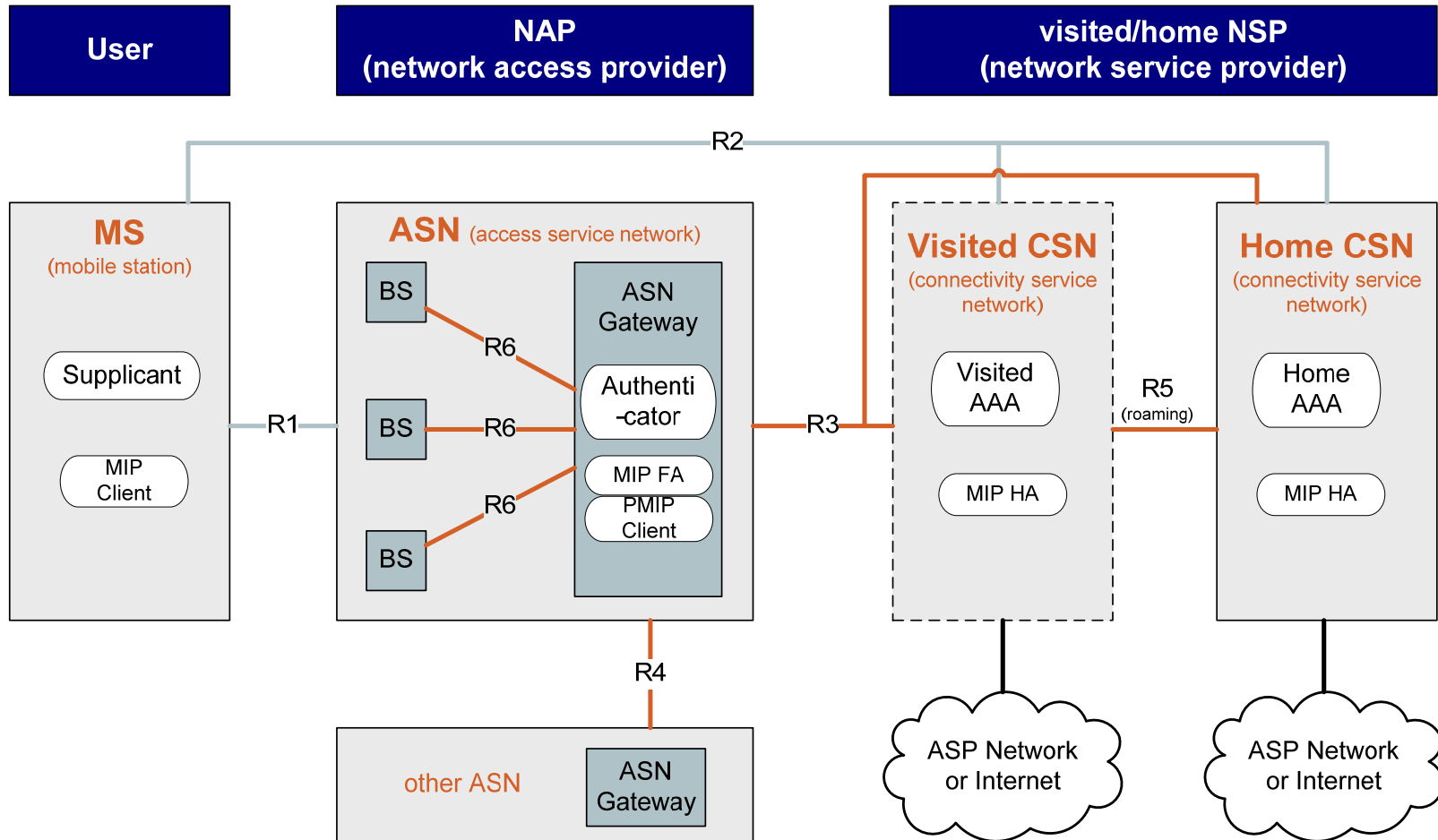
WiMAX Network Reference Model (non-roaming case)



Entities of the WiMAX Network Reference Model

- **CSN: Connectivity Serving Network**
 - Logical representation of the functions of a NSP, e.g.
 - Owning the subscriptions
 - Authentication, Authorization and Accounting
 - IP address management
 - Connectivity to the Internet and to Application Service Providers
 - Layer-3 (IP) mobility and roaming between ASNs
 - Policy & QoS management
 - Location Information Server
- **ASN: Access Serving Network**
 - Logical representation of the functions of a NAP, e.g.
 - 802.16 wireless interface termination (Base Station) including network entry and handover
 - Radio Resource Management & Admission ctrl.
 - Layer-2 session mobility management
 - Policy & QoS enforcement
 - Mobile-IP: Foreign Agent (FA) and Proxy-MIP client
 - Forwarding to selected CSN (ASN/NAP shared by several CSN operators)
 - MS location measurements

WiMAX Network Reference Model (roaming case)



New Security Aspects

The mobile WiMAX network architecture comes with

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

For network security:

- EAP-based device **and** subscription authentication
- Device Certificates (X.509) shipped in all *WiMAX Forum certified* devices
- Bootstrapping security for „services“ like IP mobility, over-the-air device provisioning or location protocols from network access
- Handover aspects of authentication, authorization and accounting (AAA)

For the wireless link (802.16-2005):

- Wireless MAC layer security: PKMv2
- New key hierarchy (different from WLAN)

User / Device Authentication: Motivation

Goals from an operator's perspective:

- Device Auth:
 - Is the device connecting to my network a 'good' device?
 - Secure anchor for initial provisioning over-the-air
- Subscription Auth:
 - Identify and validate the subscription.
 - Ensure proper billing of service usage

Examples from other networks:

- WLAN
 - single auth only (PSK or EAP-based). Hard to map this to WiMAX device or subscription authentication. Often no concept of a permanent 'subscription' in reality.
- DSL
 - device auth closest to implicit „authentication“ of fixed line (port)
 - additional subscription auth via username/password
- GSM/UMTS
 - device auth by verifying mobile phone's IMEI (but not based on cryptographic methods over-the-air)
 - subscription auth exclusively based on (U)SIM card

WiMAX Secure Network Access: Overview

Subscription Authentication

- Network access requires EAP-based authentication (Extensible Authentication Protocol, RFC3748, also used in Wi-Fi)
- RADIUS (RFC2865) or Diameter (RFC3588) based AAA infrastructure for authentication with home operator

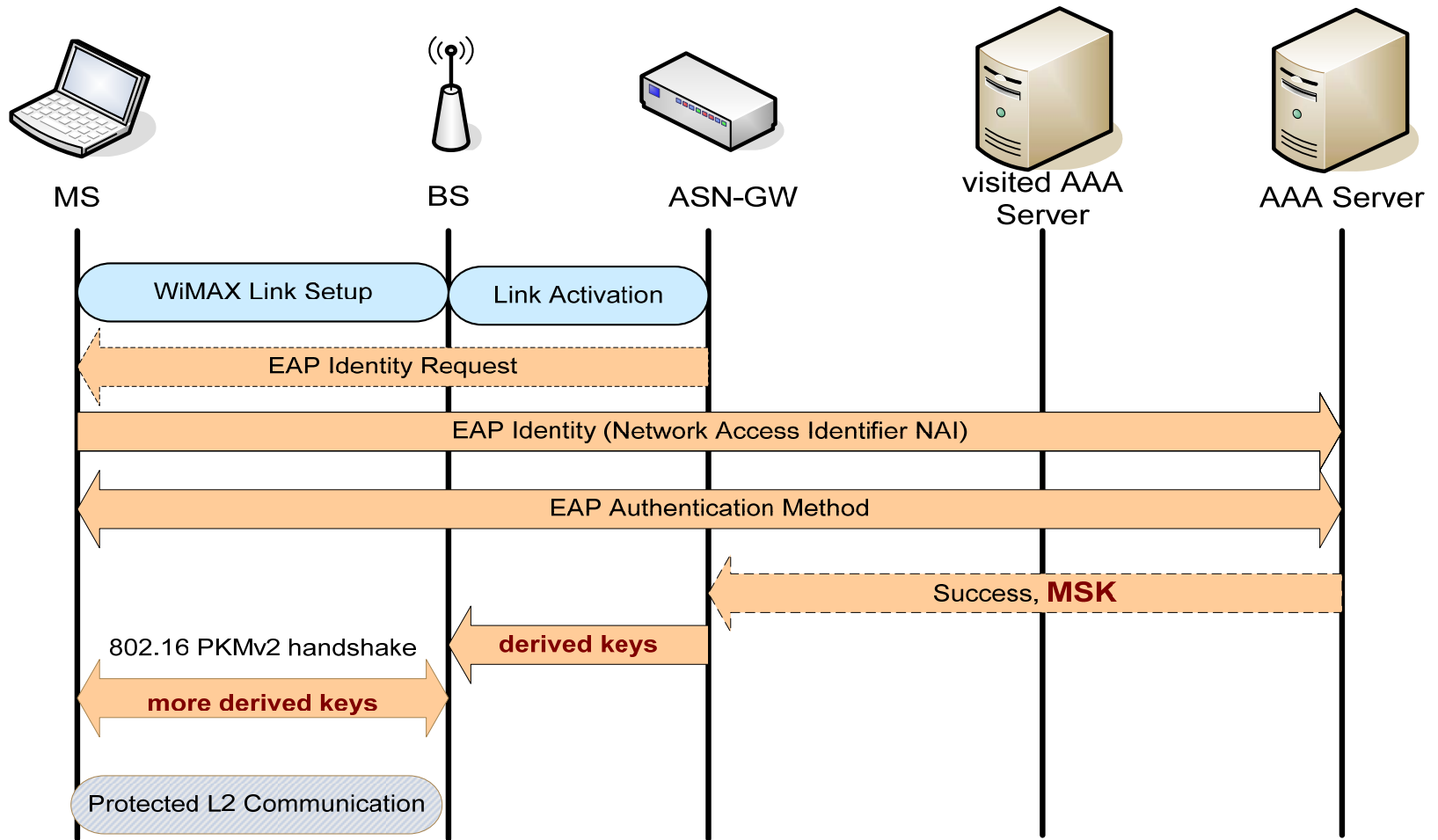
Device Authentication

- Also based on EAP methods and AAA infrastructure
- Using X.509 Device Certificates
- Can be executed in addition to subscription authentication or exclusively for initial provisioning of a new subscription over-the-air

Default EAP methods in WiMAX

- EAP-TTLSv0 with MS-CHAPv2 (Subscription)
- EAP-AKA (Subscription)
- EAP-TLS (Device)
- other methods are possible but require device support

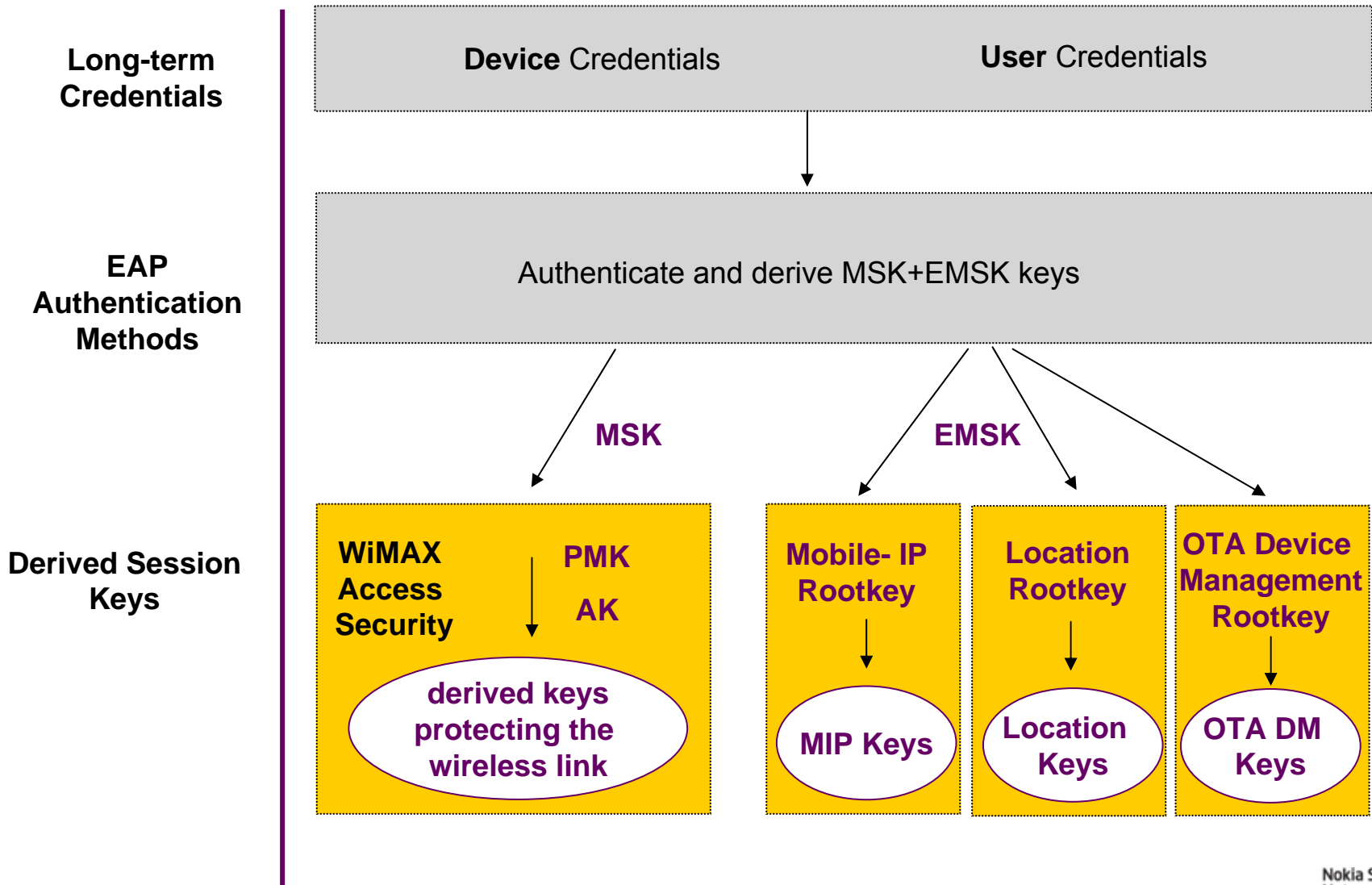
Secure Network Access in WiMAX: EAP-based Authentication and Authorization



Enabling Security for "Network Services"

- The MS exchanges signaling with the WiMAX network for different add-on services.
 - IP mobility control (using the Mobile-IP protocol)
 - Exchange of location information (via OMA-SUPL or IETF HELD)
 - Over-the-air device activation and provisioning (OMA-DM)
- All these protocols have integrated security mechanisms, but require a pre-shared key to be set up.
- In WiMAX, these protocols are secured by session keys that are dynamically derived from the EAP-based access authentication.
- In the network, all session keys are distributed via the AAA framework.

The WiMAX Key Hierarchy



EAP methods in Mobile WiMAX

- EAP (IETF RFC 3748) is just a container protocol to carry the actual authentication protocols (EAP methods).
- In general, WiMAX allows to use any EAP method matching the WiMAX requirements (e.g. capable of generating an EMSK key in addition to MSK).
- Default EAP methods in WMF specifications and certification testing, are:
 - EAP-TTLSv0/MS-CHAPv2
 - EAP-AKA
 - EAP-TLS
- The CSN AAA server has to support all three methods.
- Devices must support EAP-TLS (for device authentication in secure over-the-air provisioning, unauthenticated emergency calls).
- Devices must support at least one of the other two methods.
- From the set of default methods only EAP-TTLS (with any inner method if not MS-CHAPv2) allows to perform device+user authentication.
- "Double-EAP" (running two subsequent EAP methods for device and user authentication with cryptographic binding of the two in the ASN) was specified but later on deprecated by the IEEE.

Identities in WiMAX network access

- EAP uses the Network Access Identity (NAI, RFC 4282) as central identity for network entry and AAA routing: „username@realm“
- The "username" part may be
 - the real subscriber's identity
 - a pseudonym whenever identity hiding is used (recommended deployment)
 - a MAC address for device authentication
- Identity hiding via pseudonym identities
 - to prevent exposure over-the-air (that allows collecting/tracking IDs)
 - to prevent (visited) NSPs collecting information about competing (home) NSP's subscribers
- The NAI can be „decorated“ for visited network selection and for indicating special needs
 - Over-the-air provisioning
 - Emergency calls
- Some NAI Examples
 - localmax.com!dirk@wimax.homemax.com (selecting localmax as visited NSP)
 - {sm=2} dirk@homemax.com (MS requesting an emergency call)
 - A234F6789B123456123456789C12345E@homemax.com (my latest pseudonym)

WiMAX Forum Public-Key Infrastructure

- WMF has defined and offers a PKI to leverage device authentication.
- This covers
 - X.509 Device and Server Certificate profiles
 - WiMAX certificates for device authentication being slightly different from standard TLS certificates e.g. used in Web browsing
 - Certificate Revocation
 - Certificate revocation lists (CRL) usage, or
 - Online certificate status checking through OCSP (RFC 2560) that is better suited for mobile devices, creating less load on the wireless link
 - Operational and process documents (including pricing)
- Root Certificate Authorities are hosted by the WiMAX forum.

Future Topics in WiMAX Security

- WiMAX Femto
 - Femtocell support for the home environment creates new security challenges.
 - WFAP (wireless Femto access point) must be authenticated by the WiMAX CSN network and must securely communicate with the ASN.
 - Work is ongoing in WMF NWG. Existing Femto security architectures like the one of 3GPP are taken into account, but WiMAX specific requirements need to be matched.
- Evolution of authentication modes and methods
 - Current specifications mainly triggered by initial operator needs and existing device implementations.
 - Need for more flexibility is increasing, potentially leading to adopting newer EAP methods with better performance for faster network entry.
- More identity hiding
 - A Subscription Identity can be hidden over the wireless link; however, the device ID (MAC address) cannot.
 - Additional steps might be taken in the future to make the WiMAX network more independent of the actual MAC address and enable device ID hiding in addition.

Useful Links

- WiMAX Forum Home Page
<http://www.wimaxforum.org>
- Network Group (NWG) Specifications, Stage-2 and Stage-3
<http://www.wimaxforum.org/resources>
- WiMAX Forum PKI and X.509 Certificate Information
<http://www.wimaxforum.org/resources/pki>

