

WiMAX Network Architecture and Emergency Service Support

5th SDO Emergency Services Coordination Workshop
October 22-24, Vienna, Austria

The WiMAX Forum Network Working Group

ES Contact: dirk.kroeselberg@nsn.com,
Nokia Siemens Networks

Presentation: Dirk Kroeselberg (NSN), Richard Wisenoeker (Siemens)



Presentation Overview

- Goals/Expectations
- WiMAX Forum (WMF) and Network Working Group (NWG) overview
- Latest status of work in NWG
- Potential Future Work Items

Our Goals and Expectations for this Workshop

- Provide the latest status of Emergency-Services related work in WiMAX Forum NWG
- Collect feedback for planning our next steps
- Exchange, discuss and evaluate latest information regarding new regulatory requirements

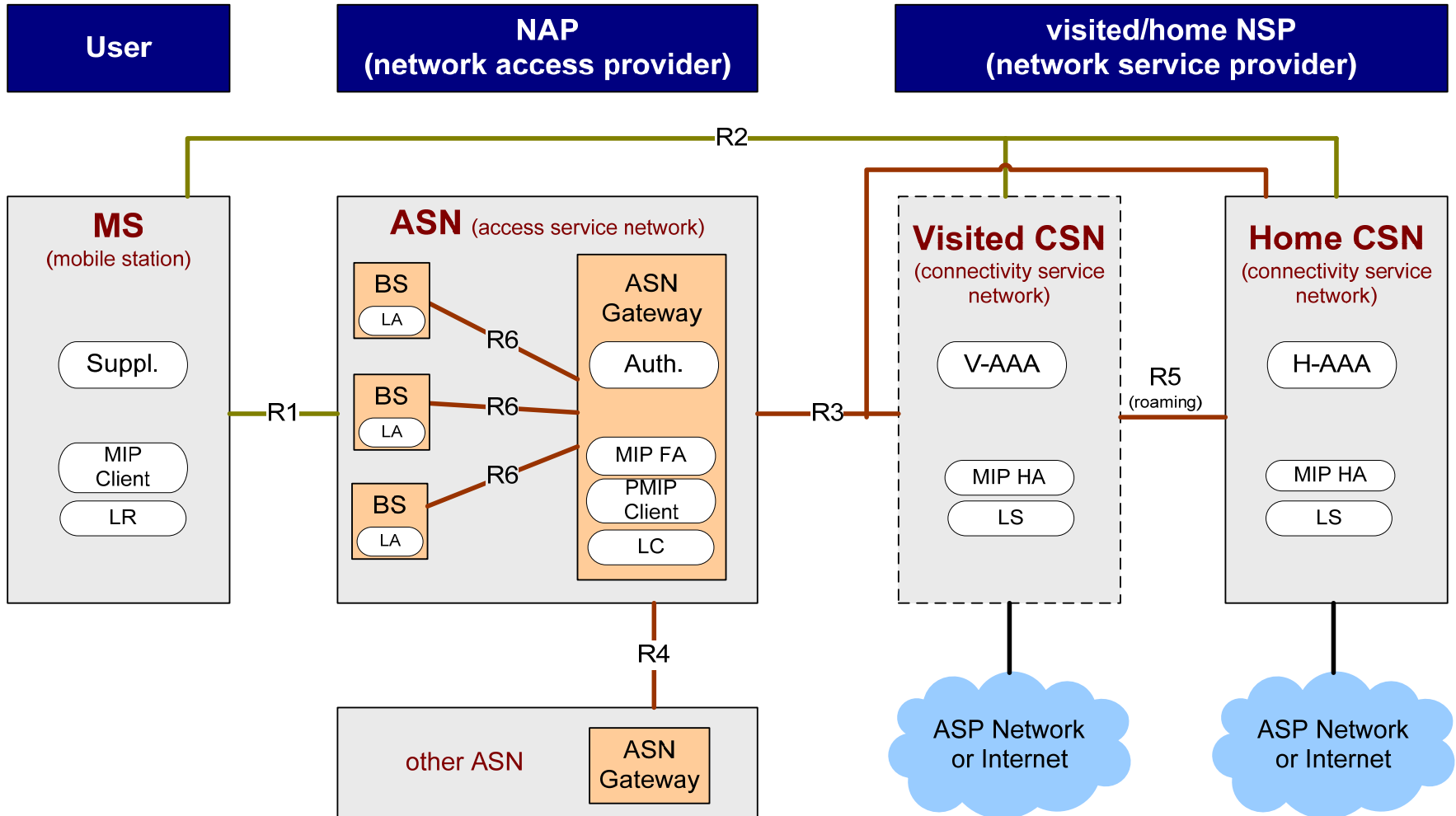
The WiMAX Forum (WMF)

- **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 (I/IOT) and the radio interface (R/ICT/P/ICT/N/ICT)
 - There are more than 500 member companies including all stakeholders
 - see <http://www.wimaxforum.org/> for further information

Entities of the WiMAX Network Reference Model

- CSN: Connectivity Serving Network
 - Logical representation of the functions of a NSP, e.g.
 - Connectivity to the Internet, ASPs
 - Authentication, authorization and accounting
 - IP address management
 - L3 Mobility and roaming between ASNs
 - Policy & QoS management based on a SLA
 - Location Server
- ASN: Access Serving Network
 - Logical representation of the functions of a NAP, e.g.
 - 802.16 interface w/ network entry and handover
 - Radio Resource Management & Admission ctrl.
 - L2 Session/mobility management
 - QoS and Policy Enforcement
 - Foreign Agent (FA)
 - Forwarding to selected CSN
 - Location Controller

WiMAX network reference model (roaming case)



NWG Specification

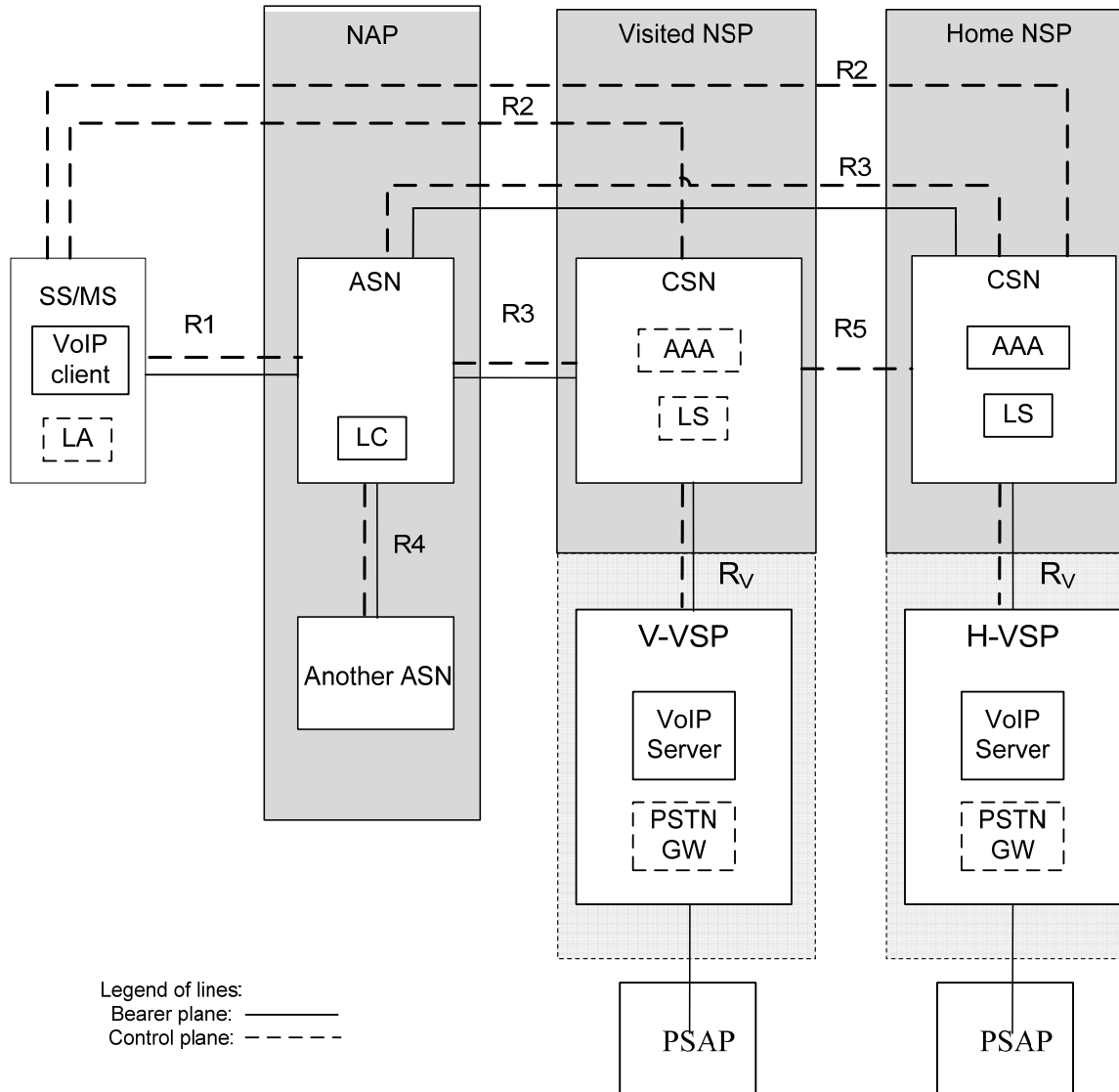
Releases and Features Overview

- The latest public NWG base specification of Release 1 (version 1.2) is here: http://www.wimaxforum.org/technology/documents/WiMAX_Forum_Network_Architecture_Stage_2-3_Rel_1v1.2.zip
- NWG is about finalizing Release 1 version 1.3 as maintenance update (expected to become public soon)
- NWG has been working during 2008 on a Release 1.5 that provides a set of additional features. Release closure planned for Q1/2009.
- A first set of Release 1.5 features is available (but not yet published). Some examples:
 - Over-the-air provisioning and device management
 - 'Simple-IP' (MobileIP-less core)
 - Diameter AAA core signaling in addition to RADIUS.
 - Support for IMS (IP-based multimedia subsystem) as per 3GPP specifications
 - PCC (Policy&Charging Control framework based on 3GPP)
 - **Emergency services** support (citizen-to-authority)
- **Location based services** support is still progressing towards closure in Q4/2008, will also be part of the Release 1.5 feature set.

NWG Status for ES Support

- ES framework specification
 - already approved by NWG in April 2008
 - only minor changes added since then
 - focusing on Emergency network entry scenarios
 - no aspects specific to the ,VoIP-technology‘
- WiMAX IMS support specification
 - approved by NWG in June 2008
 - covers all VoIP-specific aspects for IMS ES support
 - based on 3GPP Release 7 IMS, aligned with “common“ IMS specifications and the ES framework document
- Location-based services support specification
 - supporting network-based location and MS-based location determination
 - technical completion expected for end of Q4/2008
 - reflecting also emergency location requirements

ES Roaming Reference Architecture



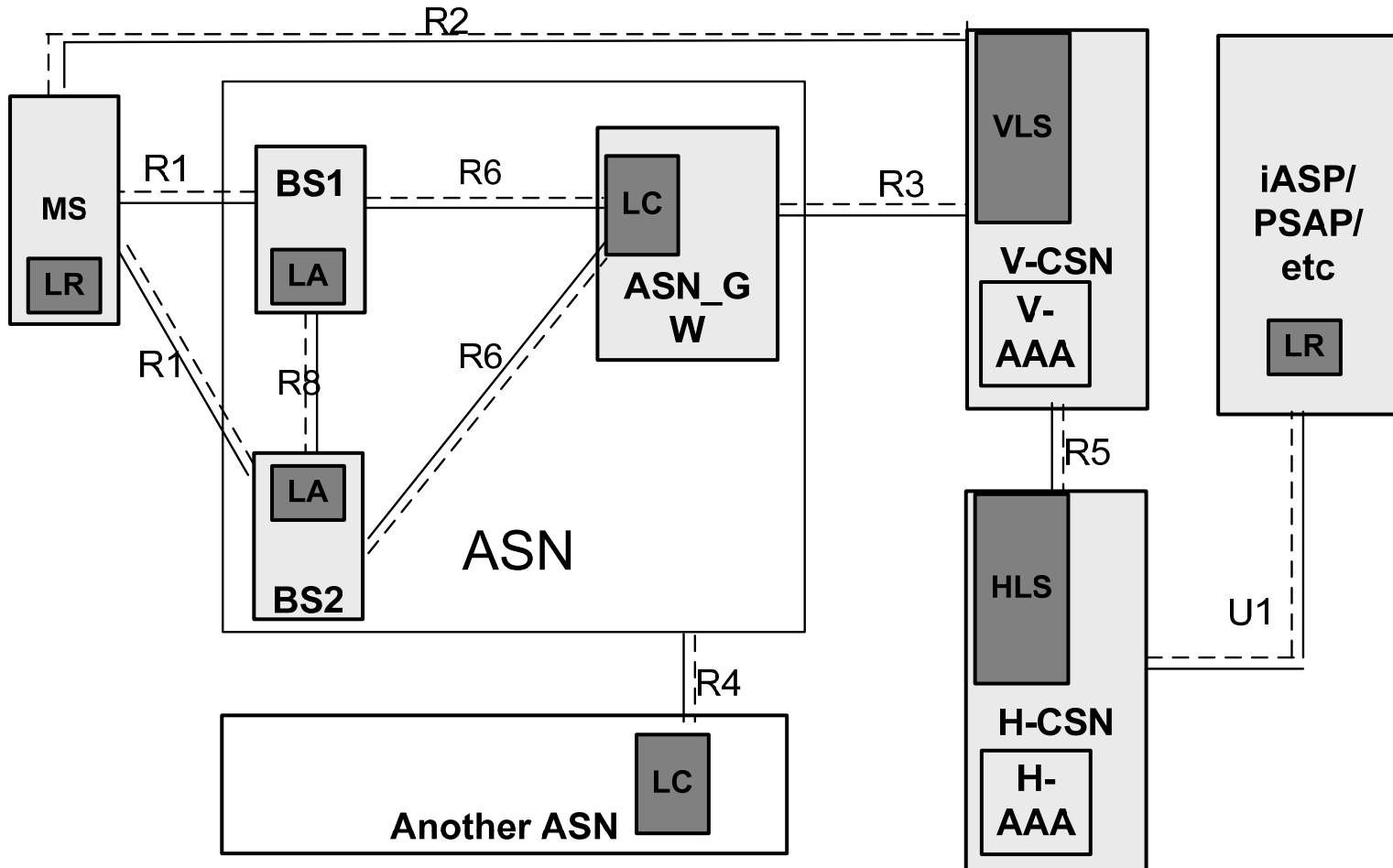
ES network entry overview

- The ES specification technical focus is on initial network entry for emergency cases
 - Placing an emergency call while already on network is handled by the VoIP application
(separate specification available for IMS ES)
- WiMAX uses EAP/AAA-based network entry
 - EAP = Extensible Authentication Protocol, IETF RFC 3748
 - Access security and authorization via EAP methods
 - Set up quality-of-service profiles with RADIUS/Diameter
 - Network (visited CSN) selection supported via NAI decoration
- Emergency is indicated through NAI decoration
 - NAI = network access identifier, IETF RFC 4282
 - NAI carries the user identity of the WiMAX subscriber within EAP/AAA
 - **{sm=2} <username> @<NSPRealm> indicates emergency**
 - No impact or dependency on 802.16e MAC layer (however, emergency indication currently being discussed in IEEE)

Location-based Services (LBS): Key Features

- MS based and Network based Location Determination.
- GPS and Assisted-GPS support.
- Support of both OMA-SUPL and IETF HELD-based protocol on R2 between MS and Location Server.
- WiMAX specific protocol on R3 where RADIUS and Diameter could be used as transport.

LBS Architecture



LBS Entities and their responsibility

LS (Location Server) in the WiMAX CSN

- Checks the authorization with support by the AAA server.
- Triggers measurements.
- Performs the location calculation based on the received measurement.

LC (Location Controller) in the WiMAX ASN

- Triggers and collects location measurements.
- Forwards measurements to the LS.

LA (Location Agent) in the ASN/BS

- Responsible for measurements and reporting.
- It may communicate to the MS to collect measurements.

LR (Location Requester) in the MS or external

- The requester who asks for location data.

Supported measurements

- Serving Cell (Base Station ID)
- LBS-ADV to broadcast cell location information
- Network based location determination based on delay measurements and/or RF signature
- GPS based measurements on the MS triggered by the Location Server

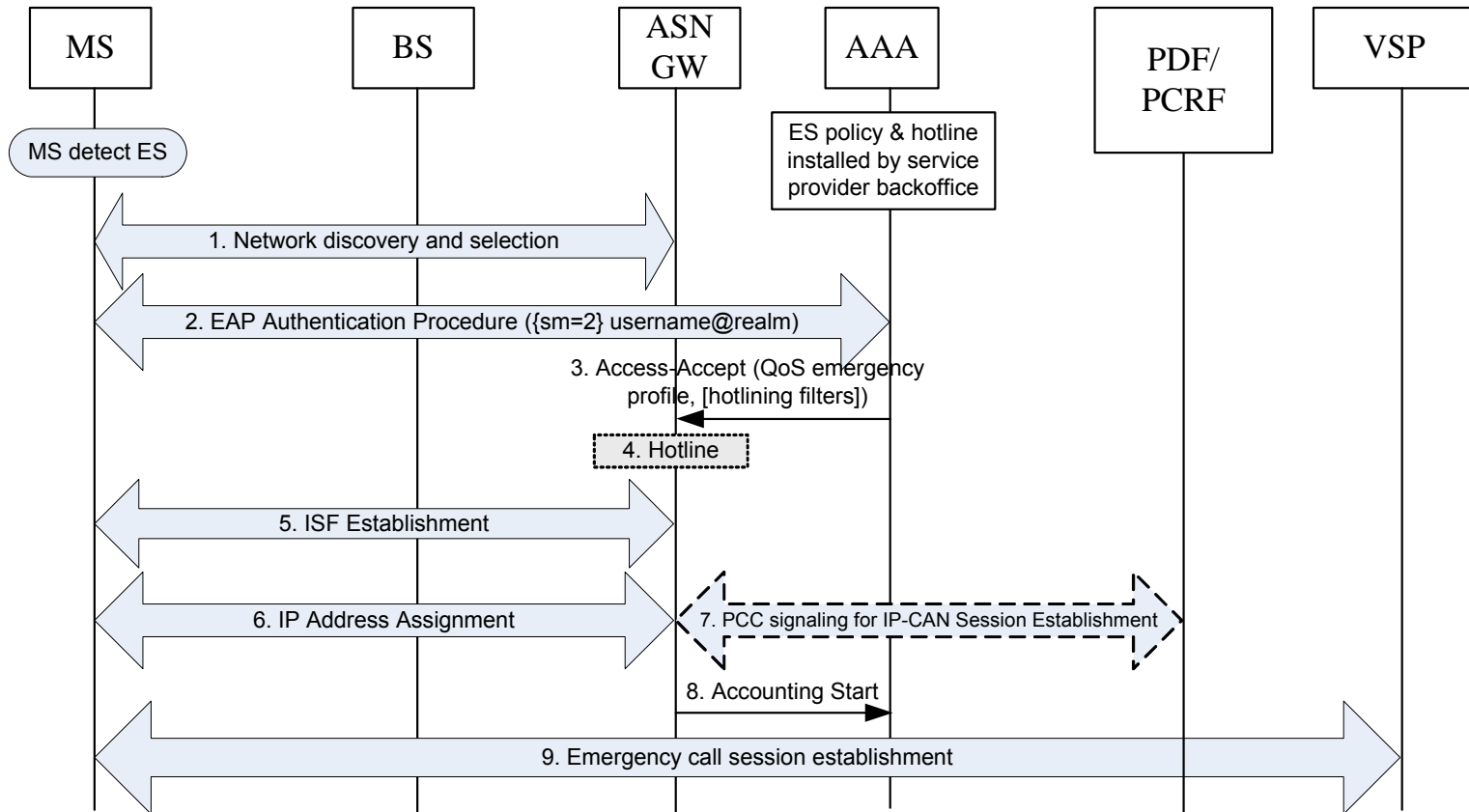
Future activities under consideration

- Re-assess regulatory requirements status, especially regarding support for 'unauthenticated access'
- Improved IP session concept for local breakout
 - Currently NWG supports limited breakout capability in the visited CSN (only when assigned during network entry, no MS control)
 - Potential improvements for emergency call support in roaming cases like parallel IP sessions under consideration (anchored in both home and visited)
- WMF Service Provider work group recently started a new work item for ETS (Emergency Telecommunication Services)
 - driven by NGN GETS
 - still at an early requirements stage in WMF

Backup slides

- Emergency Network Entry
- Unauthorized vs. Unauthenticated NW entry

ES network entry message flow



ES network entry steps

- EAP authentication with ES-decorated NAI is performed (2)
- The AAA server performs EAP and based on the authorization result decides whether to
 - allow network entry
 - apply a specific hot-lining policy (4)
 - grant ES network entry with limited access due to lack of authorization
- Service flow establishment (5-7)
- ES call establishment via WiMAX access is subject to the VoIP application (NWG specs currently cover IMS)
- After ES call termination, the MS or network may switch to normal operation by performing EAP re-authentication by sending an undecorated NAI.

Unauthorized versus Unauthenticated Definitions

- NWG is using similar terminology as in <draft-schulzrinne-ecrit-unauthenticated-access>
- Unauthorized
 - MS has credentials to successfully complete network access authentication, but lacks authorization for 'normal service'
 - credit exhaustion, expired/locked account, roaming not allowed, etc.
- Unauthenticated
 - MS does not have credentials to successfully complete network access authentication
 - blank terminal, visited network cannot reach/identify home network
- Note: The ES specification is handling WiMAX network entry. This is independent of whether a VoIP service supports unauthenticated emergency service.

Unauthorized/Unauthenticated Support in WiMax ES

- Current Release supports Unauthorized
 - mainly depending on home CSN (AAA-server) policy
 - possible in WiMAX to grant (limited) network access even for unauthorized access
- Unauthenticated not yet supported
 - not pushed as prio-1 feature due to time constraints and lack of clear requirements from service provider community
 - technically rather simple to solve for WiMAX, by mandating device authentication or using TLS-based EAP without client-side certificate
 - no real need to impact wireless MAC layer,
 - but location and VoIP discovery need further study
 - technically much harder if we assume that EAP authentication cannot be performed, or fails.
 - National Requirements may eventually dictate support for this in certain countries