Attachment 4-2-4

WiMAX Forum® Network Architecture

Architecture, detailed Protocols and Procedures

Emergency Services Support

WMF-T33-102-R015v02

WiMAX Forum® Network Architecture

Architecture, detailed Protocols and Procedures

Emergency Services Support

WMF-T33-102-R015v02

WiMAX Forum® Approved

(2009-11-21)

WiMAX Forum Proprietary

Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability.

TABLE OF CONTENTS

LIST OF FIGURES

1. Revision History

November 6, 2009	Initial version of Release 1.5.

2. Document Scope

This specification describes the framework for WiMAX networks to support emergency services (ES) for WiMAX commercial VoIP services. It provides an overall architectural framework for emergency services handling in WiMAX networks, and specifies all functionality that is required in the ASN/CSN for ES support.

ES handling for specific VoIP technologies is not specified in this document, but in the respective specification for such VoIP technology. As an example, Emergency Service handling for IMS is defined in [NWG_IMSES].

Location determining procedures and interfaces between location determining network entities are not specified in this document but in the WiMAX Location Based Services specification [NWG_LBS].

The interfaces to existing ES provider network infrastructure are identified in the network architecture, but the specification of such interfaces is beyond the scope of the present document.

This specification lists requirements to WiMAX systems for supporting ES and includes references to the emergency services related service level requirements, procedures, and interfaces as described e.g. in [JSTD034], [JSTD036B], [NENAi2].

3. Abbreviations and Definitions

3.1 Abbreviations

A-GPS	Assisted Global Positioning System
AAA	Authorization, Authentication and Accounting
ASN-GW	Access Service Network Gateway
BGCF	Breakout Gateway Control Function
BS	Base Station
BS ID	Base Station ID
E-CSCF	Emergency Call Session Control Function
E-NAI	Emergency decorated NAI
EAP	Extensible Authentication Protocol
ES	Emergency Services
HA	Home Agent
I-CSCF	Interrogating Call Session Control Function
IMS	IP Multimedia Subsystem
IP-CAN	Internet Protocol Connectivity Access Network
ISF	Initial Service Flow
LA	Location Agent
LBS	Location Based Services
LC	Location Client
LRF	Location Retrieval Function
LS	Location Server
MGCF	Media Gateway Control Function
MGW	Media Gateway
MS	Mobile Station
NAI	Network Access Identifier
NAP	WiMAX Network Access Provider
NAS	Network Access Server
NSP	WiMAX Network Service Provider
P-CSCF	Proxy Call Session Control Function
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDF	Policy Distribution Function
PPSF	Pre-Provisioned Service Flow

PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
SFA	Service Flow Authorization
SIP	Session Initiation Protocol
SPR	Subscription Profile Repository
URN	Uniform Resource Name
USIM	Universal Subscriber Identity Module
VoIP	Voice-over-IP
VSP	VoIP Service Provider

In addition to the above abbreviations the reader is referred to [NWGSTG2-1], [SPWGR1.5], [JSTD034], [JSTD036B], [23.167], and [NENAi2] for acronyms/abbreviations used throughout this document.

3.2 Terms & Definitions

Non-service-initialized Device: A device for which there is no valid service contract with a provider. Other terms: "un-initialized", "un-provisioned", "unbranded" device.

Unauthenticated Emergency Service: The term refers to the case where an emergency caller does not have credentials (e.g., no USIM, no username and password, no private key) to either attach to a WiMAX network or for usage with a VoIP service or both. Still, the device may be granted (limited) access to perform emergency calling. It is important to differentiate between the unavailability of credentials for WiMAX network access and for VoIP access as the network provider and the VoIP provider can be distinct entities and therefore the user might have different credentials for the two.

Unauthorized Emergency Service: The term refers to the case where an emergency caller/device aims to attach to the WiMAX network or to use a VoIP service but the authorization procedure fails. The authorization step may fail as a consequence of triggering different procedures (such as network access authentication or registration at the VoIP provider's registrar). Still, the device is granted (limited) access to perform emergency calling. It is important to differentiate between WiMAX network operator and VoIP provider as they can refer to different business entities and therefore the authorization decision might be executed by a different backend infrastructure.

Lack of authorization might be caused by a number of reasons, including credit exhaustion, expired accounts, locked account, missing access rights (e.g., access to the competitor's enterprise network), etc.

Un-initialized Voice Device: A device without VoIP client software.

VSP: A Voice Service Provider (VSP) is an entity that provides *interconnected VoIP services*[1] (e.g. see FCC 05-116) to the (WiMAX) end user. It is assumed that the provision of ES service is the responsibility of the VSP. If the VSP is the same as the NSP, then the ES requirements apply to the NSP. If not, then the VSP may need to contract with the NSP for some ES service support (e.g. providing terminal location). VoIP services that provide callout only are NOT covered by this specification, per SPWG definition of a VSP.

[1] "Interconnected VoIP services" are services that (1) enable real-time, two-way voice communications; (2) require a broadband connection from the user's location; (3) require IP-compatible customer premises equipment; and (4) permit users to receive calls from and terminate calls to the public switched telephone network. *See* IP-Enabled Services; E911 Requirements for IP-Enabled Service Providers, WC Docket Nos. 04-36, 05-196, *First Report and Order and Notice of Proposed Rulemaking*, 20 FCC Rcd 10245, 10257-58 ¶ 24 (2005), *aff'd*, *Nuvio Corp. v. FCC*, 473 F.3d 302 (D.C. Cir. 2006) (*VoIP 911 Order*); *see also id.* at 10276-77 ¶ 57 (seeking comment on whether and how interconnected VoIP service providers might be able to provide location information automatically). Interconnected VoIP service providers are not subject to Section 20.18 of the Commission's rules; the 911 obligations that apply to interconnected VoIP services are set forth in Part 9. *See* 47 C.F.R. §§ 9.1-9.5. *See* Service Rules for the 698-746, 747-762 and 777-792 MHz Bands et al., WT Docket No. 06-150 et al., *Report and Order and Further Notice of Proposed Rulemaking*, FCC 07-72, paras. 129-136 (rel. Apr. 27, 2007).

4. References

4.1 Federal Communications Commission (FCC)

- [FCC94-102] FCC Docket no 94-102 including order numbers 96-264, 99-96, 99-245
- [FCC 05-116] FCC 05-116, WC Docket Nos. 04-36, 05-196, 'E911 Requirements for IP-Enabled Service Providers', June 2005.

4.2 IEEE

- [802.16g] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Management Plane Procedures and Services, IEEE P802.16g/D6, November 2006
- [802.1AB-LLDPMED] IEEE 802.1AB with Link Layer Discovery Protocol – Media Endpoint Discovery (LLDP-MED) extension - ANSI/TIA-1057, April 2006.

4.3 Internet Engineering Task Force (IETF)

- [RFC5031] H. Schulzrinne, "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", IETF RFC 5031, January 2008. http://www.ietf.org/rfc/rfc5031.txt.
- [RFC5069] Taylor, et al., "Security Threats and Requirements for Emergency Call Marking and Mapping", IETF RFC 5069, January 2008. http://www.ietf.org/rfc/rfc5069.txt.
- [RFC5222] T. Hardie, A. Newton, H. Schulzrinne, H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", IETF RFC 5222, August 2008
- [IETF-Geo] Thomson, M. and C. Reed, "GML 3.1.1 PIDF-LO Shape Application Schema for use by the Internet Engineering Task Force (IETF)", Candidate OpenGIS Implementation Specification 06-142r1, Version: 1.0, April 2007.
- [RFC5139] M. Thomson, J. Winterbottom, "Revised Civic Location Format for PIDF-LO", IETF RFC 5139, February 2008.

4.4 National Emergency Number Association (NENA)

- [NENAi2] NENA Interim VoIP Architecture for Enhanced 9-1-1 Services (i2), NENA 08-001, Issue 1, December 6, 2005 (http://www.nena.org)

4.5 Open Mobile Alliance (OMA)

- [OMASUPL] OMA Secure User Plane Location Architecture, Draft Version 3.0 – 21, January 2007 (OMA-AD-SUPL-V2_0-20070121-D)

4.6 Telecommunication Industry Association (TIA)

- [JSTD034] TIA/EIA J-STD-034 Wireless Enhanced Emergency Services, 1997
- [JSTD036B] TIA-J-STD-036-B Enhanced Wireless 9-1-1 Phase 2, June 2005

4.7 WiMAX Forum

- [SPWGR1.5] WiMAX Forum SPWG, Recommendations and Requirements for Networks based on WiMAX Forum Certified™ Products, Release 1.5, January 07, 2008

- [NWGSTG3] WiMAX Forum, T33-001-R015v01, “Detailed Protocols and Procedures, Base Specification", Release 1.5
- [NWG_IMSES] WiMAX Forum T33-101-R015v02, "Architecture, detailed Protocols and Procedures, IP Multimedia Subsystem (IMS) Interworking", Release 1.5
- [NWG_LBS] WiMAX Forum T33-110-R015v01, "Protocols and Procedures for Location Based Services", Release 1.5
- [NWG_PCC] WiMAX Forum T33-109-R015v01, "Architecture, detailed Protocols and Procedures, Policy and Charging Control", Release 1.5.

4.8 Third Generation Partnership Project (3GPP)

- [23.167] 3rd Generation Partnership Project, Specification Group Services and System Aspects, IP Multimedia Subsystem (IMS) emergency sessions (Release 7), V7.8.0, March 2008.
- [23.228] 3rd Generation Partnership Project, Specification Group Services and System Aspects, Multimedia Subsystem (IMS); Stage 2 (Release 7), V7.11.0, March 2008.]

5. Requirements and Principles

The deployment of commercial VoIP requires the support for emergency services (e.g. known as E9-1-1 in North America, 112 in the European Union) as specified in [SPWGR1.5]. For emergency services (ES), the Mobile Station's location information is needed in order to correctly route the emergency call to an appropriate emergency response center and to deploy an emergency response to the caller's location.

Although the exact regional or country-specific regulatory requirements that govern the support of emergency services for VoIP may vary, this document assumes that the basic emergency services capabilities would be universally applicable.

In order to facilitate the development of this feature, the North American E9-1-1 Standards as specified in [JSTD034], [JSTD036B], and [NENAi2] are considered in addition where applicable.

[SPWGR1.5] specifies the following ES-related requirements which are listed below for easy reference. For each of them a statement is given how it is matched by the present specification:

R-[19x] The WIMAX network SHOULD provide high priority for emergency services.

Decoration of the NAI used for initial network entry to indicate the request for emergency as specified in section 7.2.1, allows for prioritization of such entry attempts in the NAP/NSP WiMAX network. Prioritization at the application layer is subject to any specific VoIP technology and is therefore out-of-scope for this document.

R- [378] For emergency service support the WiMAX network SHALL meet the applicable requirements and capabilities defined in Ref [JSTD034], Ref [JSTD036B], and Ref [NENAi2]. This requirement does not require the WiMAX network to use the same protocols, procedures, and mechanisms defined in the referenced standard.

This specification establishes a framework that takes into account these references where applicable.

R-[403] The WiMAX network SHALL be capable of delivering location information to location services upon request. Such request may come from the user, lawful/emergency agencies or other authorized agents on the network.

WiMAX specific location mechanisms are defined by [NWG_LBS] and are not covered by this specification. The framework for emergency location given in this document allows for location information provided by both MS and WiMAX network; however, basic network based location support is mandated as the MS cannot be assumed in general to be able to provide such information.

R-[404] If commercial VoIP is supported in WiMAX Networks supporting Nomadic and/or Mobility Access usage, enhanced location determination SHALL be supported, and the enhanced location determination SHALL be able to meet the location accuracy specified in E911 Phase 2 requirement [FCC94-102].

WiMAX specific location mechanisms are defined by [NWG_LBS] and are not covered by this specification.

R-[469] If device authentication fails, the WiMAX network SHALL support an operator-specified function such as access to emergency services.

This version of the present specification does not support access to emergency services if device authentication fails (see section 7.1.1.3 and section 7.1.4). However, access to emergency services is supported if device authentication can be performed, but authorization fails; this maps to the unauthorized case (see section 7.1.1.2).

Unauthenticated access to emergency services is supported to allow operators to comply with specific regulatory requirements in cases where user authentication cannot be performed. The assumption within the scope of this specification is that any WiMAX device is technically capable of performing device authentication based on EAP-TLS and the device certificate installed in the device at the time of manufacturing.

In addition, location-related requirements are given in section 10.14 of [SPWGR1.5]. These requirements, however, are not listed in this document as they apply to location services in general and are not specific to emergency services.

6. Network Reference Model

This document describes the WiMAX network framework for providing support for emergency services. This framework is built upon the overall WiMAX network architecture of WiMAX Release 1, version 1.2 [NWGSTG3]. It supports VoIP services provided over WiMAX by a VoIP service provider (VSP) that can either be part of an NSP or can be a 3rd party commercial VSP with contractual relationship with the WiMAX NSP. The interfaces to existing ES provider network infrastructure (PSAPs) are identified, but the specification of such interfaces is beyond the scope of the present document. The WiMAX emergency services framework supports communication between a VSP's VoIP server and the PSAP over both VoIP protocols or PSTN based protocols.

The specified scenarios and mechanisms clearly focus on the part that a WiMAX network, providing broadband packet data access, needs to provide for enabling IP emergency calls. All aspects that are specific to the VoIP service itself, are beyond the scope and need to be covered by specifications describing a specific VoIP technology.

As a result, there is a clear and intentional split between the generic framework to offer IP emergency service support in WiMAX networks and required generic building blocks that are covered by this document, and all further aspects specific to the VoIP technology or VoIP service.

As an example, all VoIP specific aspects for providing emergency service support for the IMS are described in [NWG_IMSES] and the underlying 3GPP specifications like [23.167] and [23.228].

The network reference model for the WiMAX ES architecture has been aligned with existing architectures to support IP emergency calls, e.g.:

- [JSTD036B] specifies a network reference model that supports the interfaces between a circuit-switched cellular network and an ES network.
- [NENAi2] recommends migratory solution architecture for supporting emergency calls originated in the IP domain (in this case the WiMAX network) and terminated using the PSTN ES infrastructure.

Based on the network reference model for supporting emergency services in WiMAX networks developed in this section, chapter 7 provides more detailed scenarios and high-level message flows that are subdivided based on whether the scenario considers roaming, or whether the NSP and VSP are in the same domain, or are in separate domains.

Figure 1 describes the overall architecture for WiMAX emergency service support, providing a general description of the functionalities.

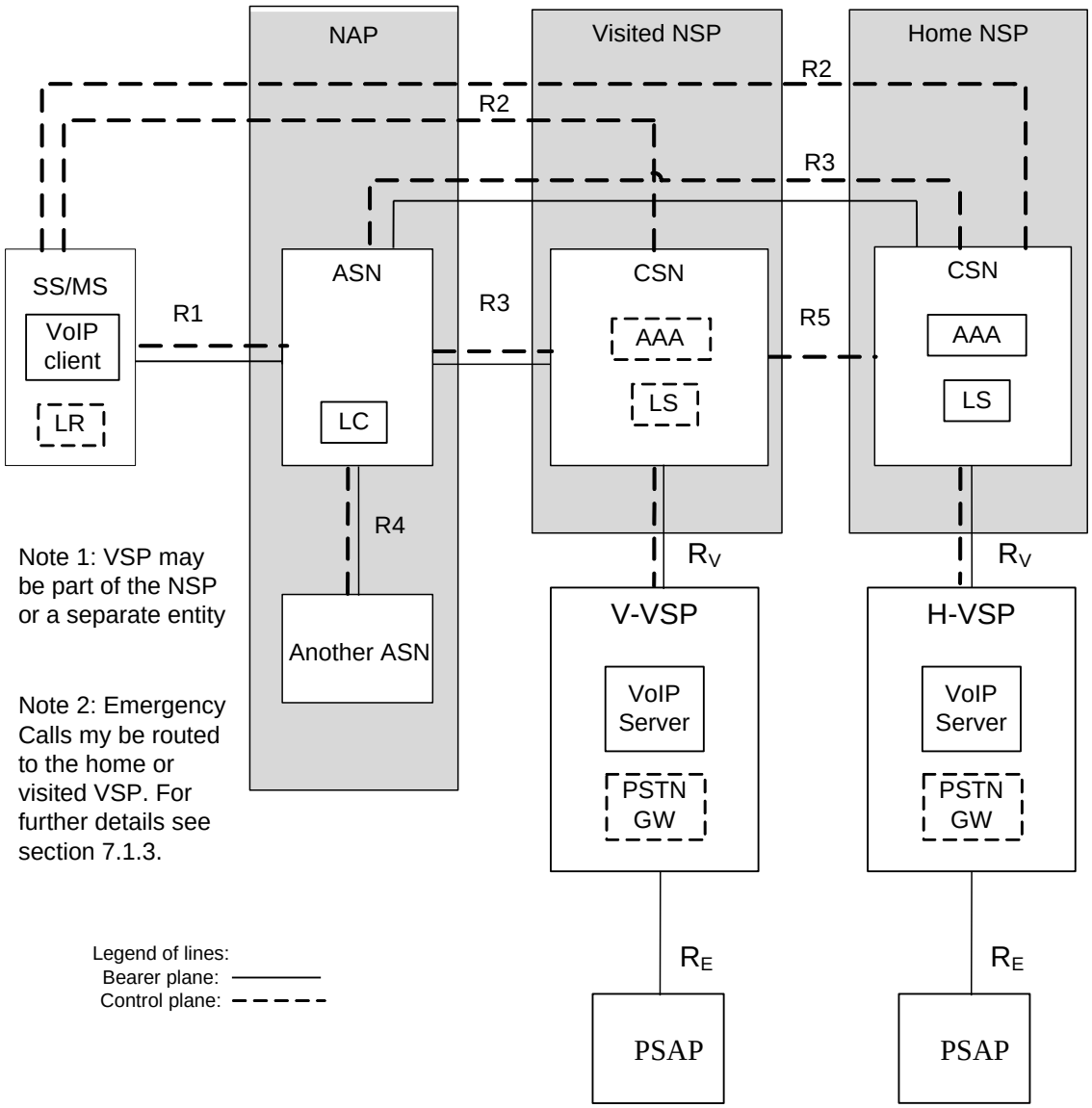


Figure 1: Network reference model for WiMAX based emergency services

Public Safety Answering Point (PSAP)

Physical location where emergency calls are received under the responsibility of a public authority (This terminology is used by both ETSI, in ETSI SR 002 180, and NENA). In the United Kingdom, PSAPs are called Operator Assistance Centres, in New Zealand, Communications Centres.

VoIP Server

The VoIP-Server may be ES enabled. If enabled, the VoIP server should support a specific set of functionalities and protocols to provide a fully featured ES support to the subscriber. The set of functionalities and protocols to be supported depends on the functionalities and protocols supported by the VoIP-Client.

VoIP Client

The VoIP Client is located in the terminal. The client application should take care of the functionalities supported by the VoIP Servers provided by the VSP including ES activation.

LS (Location Server)

The WiMAX LS function is defined by [NWG_LBS]. It has the capability to provide location information to any kind of application. The application should provide an emergency indication to enable the LS to apply the appropriate access rights for emergency access to its information and provide appropriate information for emergency cases. In case of requesting location information for PSAP selection, information with fastest availability sufficient to determine the correct PSAP shall be requested. In case that PSAP should be informed about location information for location tracking, information shall be requested with the location accuracy consistent with local requirements for dispatching emergency responders, among the available location determination methods.

LC (Location Controller)

The LC function for WiMAX is defined by [NWG_LBS]. It is located in the ASN. The LC is responsible for coordinating the location measurements of the MS. The LC provides the location measurements for the MS to the LS upon request.

LR in MS (Location Requester)

The LR as specified in [NWG_LBS] is an optional functional entity which may allow to provide location information to an ES enabled VoIP client compatible to an ES enabled VSP. The location determination could be done with any available method (network based and/or terminal based). It is preferred that LR provides location information as GEO information. The location information could be provided to the VSP with the help of an application specific protocol. The VSP may use this information to determine the responsible PSAP.

PSTN Gateway

The PSTN gateway allows a connection to legacy PSAPs. This entity is VoIP application specific and is out of the scope for a WiMAX device making ES calls. WiMAX gives no statement on the PSTN gateway availability as it depends on country laws and capabilities of the responsible PSAP.

R_E (Reference point for Emergency Service)

The R_E reference point consists of protocols and procedures between the VoIP server and the PSAP that handles emergency calls. The reference point includes protocols to provide VoIP stream transport or PSTN based voice. Further, protocol(s) to provide subscriber information like location information are included. R_E is shown for completeness but is not in the scope of this specification.

R_V (Reference point for VoIP Service)

The R_V reference point interconnects an NSP and a VSP to provide VoIP support of a VSP to a subscriber. The reference point covers VoIP service specific protocols for control and user plane. Further, location information of the subscriber should be provided from the NSP to the VSP to allow the VSP to cover regulatory needs. Specification of this reference point is out-of-scope for the present release of this document.

7. Functional Description

7.1 Emergency Scenarios

Based on the available regulatory requirements, it is understood that the obligation to provide appropriate means to enable emergency services support falls upon the VSP. For WiMAX, a network may operate as a combined NSP / VSP, or an NSP may be required to support the actual VSP with functionality required by the VSP to be able to fulfill emergency services requirements.

This document focuses, based on careful consideration of available operator and regulatory requirements, on supporting emergency calls within the following scenarios:

1) Emergency services support for the non-roaming case (NSP acting as VSP or with contractual relationship to a VSP)
2) Roaming, emergency services support in hNSP/VSP. No VSP support in vNSP available
3) Roaming, emergency services support in vNSP/VSP. Visited and home NSP/VSP with roaming agreement
    a) IP-based services provided by hNSP
    b) IP-based services provided by vNSP

    Full local breakout support is currently not specified for WiMAX networks.
4) Roaming, emergency services support in vNSP/VSP; no roaming agreement with hNSP but hNSP reachable (e.g. branded terminal with no initial subscription)

All scenarios assume that the VoIP technology used to perform an emergency call is compatible across the MS and the involved VSPs. A mechanism for discovery of compatible VoIP technology remains for future study and may be added in later versions of this specification.

Within this section, the term ‘subscription’ always refers to a subscription for the WiMAX network (ASN/CSN usage), in contrast to any service-level subscription to the VSP that is providing emergency services. Aspects related to the service-level subscription are considered as VoIP technology dependent and are not in the scope of this specification.

For all the above scenarios, the following general considerations SHALL apply:

- The MS SHOULD be able to recognize and indicate to the network any request by the user to access an emergency service. If the terminal is not able to recognize a user request to access an emergency service or is already attached to a WiMAX network, then the device would not indicate to the network such emergency service access attempt and specific treatment of the actual call over what is applied to an ordinary VoIP call MAY not be available. Also, if the terminal does not recognize a user request to access an emergency service, unauthenticated emergency services access is not possible.
- For any new network entry to access emergency services, an MS recognizing the request for emergency service SHALL indicate to the network that it is requesting emergency services, as described in section 7.2.1. This indication is independent of whether the network access attempt requesting emergency services is using a valid subscription, or is a request for unauthorized or unauthenticated emergency services.

The following text makes use of the terms unauthenticated and unauthorized. Definitions from a service-centric perspective are given in section 3.2. Regarding a WiMAX network, these terms are used for network access, or to describe the existence and access rights of a WiMAX subscription. See section 9.1 for detailed technical discussion. Subscription and unauthenticated/unauthorized access to a VSP service are not in the scope of this document.

7.1.1 Emergency call for non-roaming scenarios

This scenario describes how emergency services are supported by the WiMAX network in a non-roaming case, i.e. where the MS is attached via a NAP to the NSP that owns the subscription used by the MS.

The two cases that are described below are

- NSP acts as the VSP
- or the VSP is provided by a 3rd party service provider

A third-party VSP scenario requires standardized procedures for the NSP and VSP to exchange information required for the provision of emergency services via the Rv reference point. The definition of such reference point and procedures are out-of-scope for the present release of this specification. Therefore, this scenario is limited to the first case.

In the following subsections, one precondition assumed is that the MS is not yet connected to the WiMAX network, and performs a new network entry procedure triggered by the need to place an emergency call. For cases where the MS is already connected to a WiMAX network, no emergency specific considerations apply to the network entry procedure over what is defined in [NWGSTG3]. The MS may perform a network re-entry to force emergency network entry for receiving improved emergency services support by the WiMAX network.

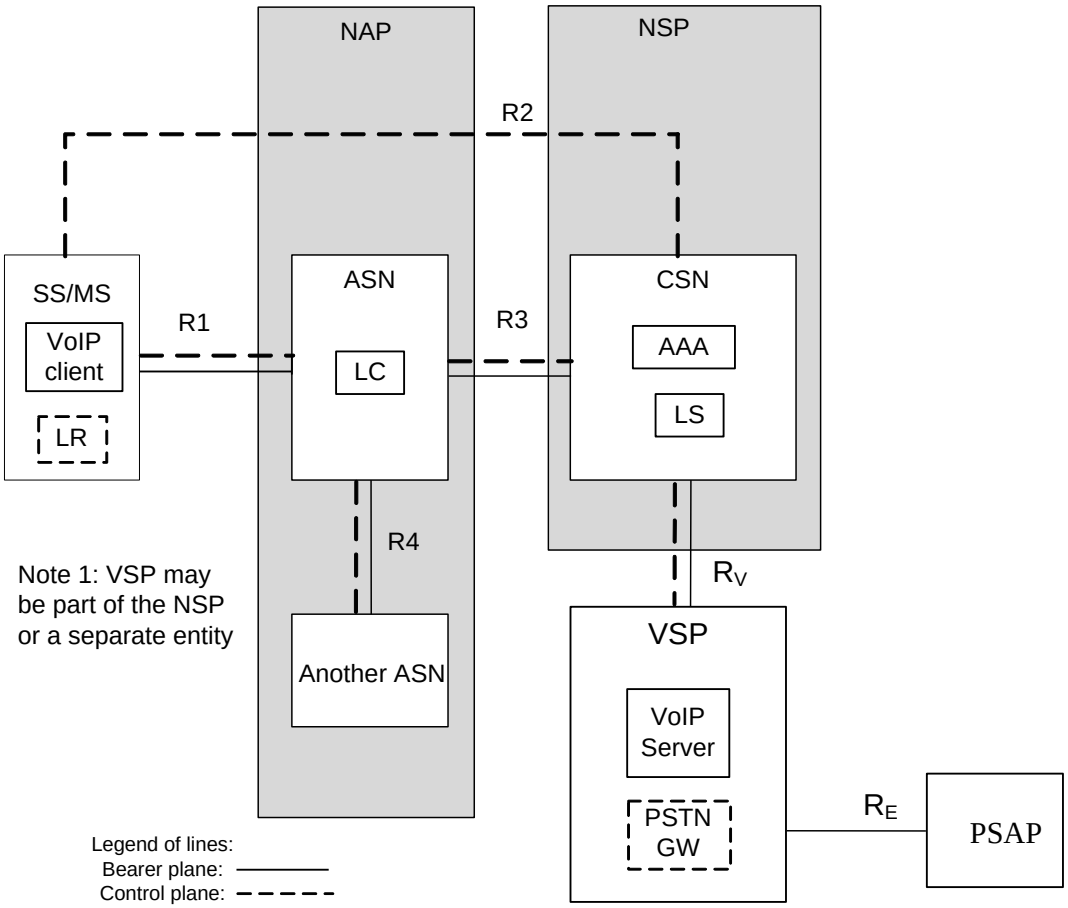


Figure 2: Non-roaming scenario with NSP acting as VSP

7.1.1.1 Emergency network entry for authorized subscription (with non-PCC)

The following figure provides the high-level message flow for the given non-roaming scenario that is performed for an emergency registration with network entry. It is assumed that the MS has a valid subscription for WiMAX network entry excluding NWG Policy and Charging Control [NWG_PCC] architecture.

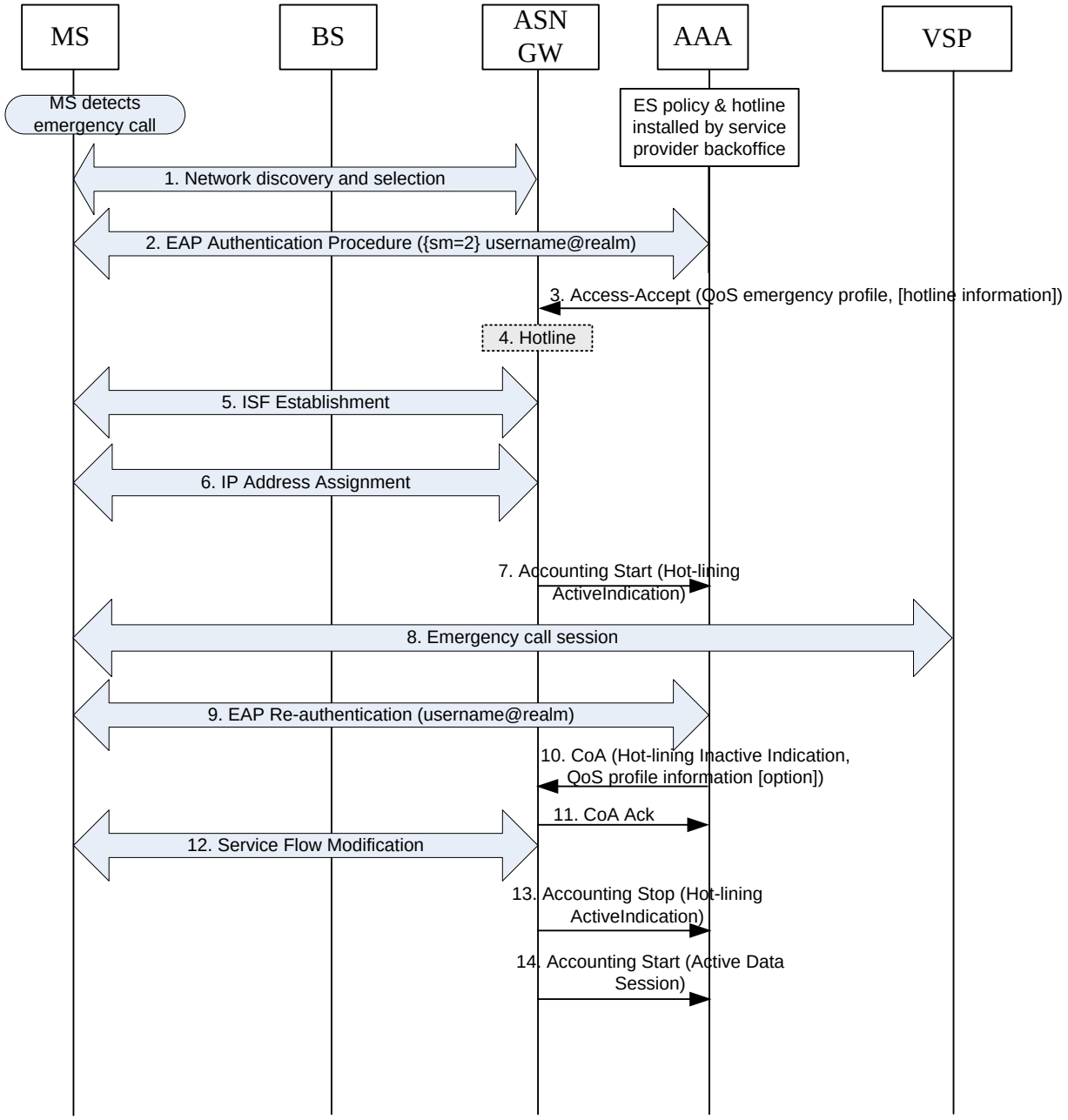


Figure 3: Authorized emergency network entry with non-PCC

In the case where an MS detects an Emergency Call while not being attached to a WiMAX network the MS SHOULD initiate an emergency network entry according to the steps described below.

Note: For cases where the MS is not able to recognize an emergency call, only normal network entry procedures can be used by the MS and no ES-specific treatment during network entry procedures can be applied.

1. MS performs standard network discovery and selection (Initial network entry procedure as per [NWGSTG3], section 4.5.1.1).

2. During EAP authentication that is performed with the same steps as required for the present subscription, the MS decorates the outer NAI as specified in section 7.2.1. In cases where both device and subscription authentication are performed both NAIs SHALL be decorated to indicate the emergency network entry. The decoration of the device NAI SHALL be the same as for the subscription NAI.
   The AAA server responsible for authorizing the access attempt in cases where device authentication is performed MAY decide based on internal policy and on the EAP method used to skip the second authentication after successful device authentication in cases where emergency NAI decoration is present.
3. The AAA server authorizes the emergency network entry and sends Access-Accept to the authenticator. Hotlining MAY apply here. Hotlining is a deployment option where the operator directs the authorized emergency VoIP call to a VSP which further connects the VoIP call to the desired PSAP. Hotline support for Callback parameters is FFS.
   The AAA server SHOULD be pre-configured with a QoS emergency profile. When the AAA server receives access request with an E-NAI, it SHOULD deliver the QoS emergency profile to authenticator/anchor SFA so that it can establish a bearer for the emergency session. The AAA server SHOULD also deliver the default QoS profile for the subscriber.
4. The MS MAY be hotlined depending on the AAA server policy, e.g. if only limited authorization has been performed. The hotline feature is described in section 4.4.3.5 of [NWGSTG3].
5. Anchor SFA establishes the initial service flow (ISF) for the MS and pre-provisioned service flow establishment as specified in NWG Network Architecture Stage-3 [NWGSTG3].
6. The MS gets an IP address (via DHCP or MIP).
7. The accounting client sends an accounting start message to the AAA server according to [NWGSTG3].
8. The MS has performed network entry to the WiMAX network and proceeds with establishing the emergency call with the VSP. Procedures required for this step are specific to the supported VoIP service, and are not in the scope of this document.
9. When the user indicates to terminate emergency services access and change to normal access, the MS MAY perform re-authentication. The MS re-authenticates with a NAI that SHALL NOT carry the emergency decoration as specified in section 7.2.1. If the AAA server receives such re-authentication request for a subscription where the active authentication session has been requested with an emergency decorated NAI, the AAA server based on local policy SHOULD accept a valid re-authentication request and put the authentication session back to normal (non-emergency) access. After a specific time when an emergency call was terminated, the network SHOULD perform re-authentication or network re-entry of the MS.

The subsequent steps apply depending on whether the emergency session is hot-lined or whether re-authentication was performed in step 9.

10. The AAA server MAY send a CoA message to the ASN AAA client / HLD with updated QoS profile information for normal access. If hotlining is applied the AAA server SHALL include ‘Hot-lining Inactive Indication’ in the CoA message carrying the QoS profile, or send a CoA message for hotlining if no QoS profile is sent, to release the hotlining specific to the emergency session. Upon receipt of a CoA message carrying QoS profile information the ASN SHALL update its QoS profile with the one received in CoA. If the CoA does not contain QoS profile information the ASN will either use QoS profile information received during initial network entry, or continues to use the QoS profile used for ES network entry.
11. The ASN-GW/HLD confirms the receipt of a CoA message by sending a CoA Ack message to the AAA server.
12. If the QoS profile has been updated, the Anchor SFA SHALL update the existing service flows.
13. The ASN-GW/HLD generates an Accounting Request (Stop) message for the hotlined session.
14. The Accounting Request (Stop) message SHALL be followed by an Accounting Request (Start) message indicating the start of the normal packet data session.

Note 1: Procedures to perform step 7 with the VoIP service being IMS, are described in [NWG_IMSES].

Note 2: If hot-lining is applied to the ES session and the MS re-authenticates to release hot-lining and get normal access, it is up to the AAA server policy to decide in step 10 above whether to allow this. If re-authentication is successful, the AAA server can change the QoS profile for the subsequent normal session by sending a CoA

message with updated QoS profile information to the ASN. If the AAA server does not send a CoA message carrying such information, the ASN will continue to use the QoS profile used for ES network entry.

If the AAA server does not accept re-authentication, the MS MUST perform a new initial network entry after finalizing emergency access.

7.1.1.2 Emergency network entry for authorized subscription (with PCC)

The following figure provides the high-level message flow for the given non-roaming scenario that is performed for an emergency registration with network entry. It is assumed that the MS has a valid subscription for WiMAX network entry and the NWG Policy and Charging Control [NWG_PCC] architecture is used.

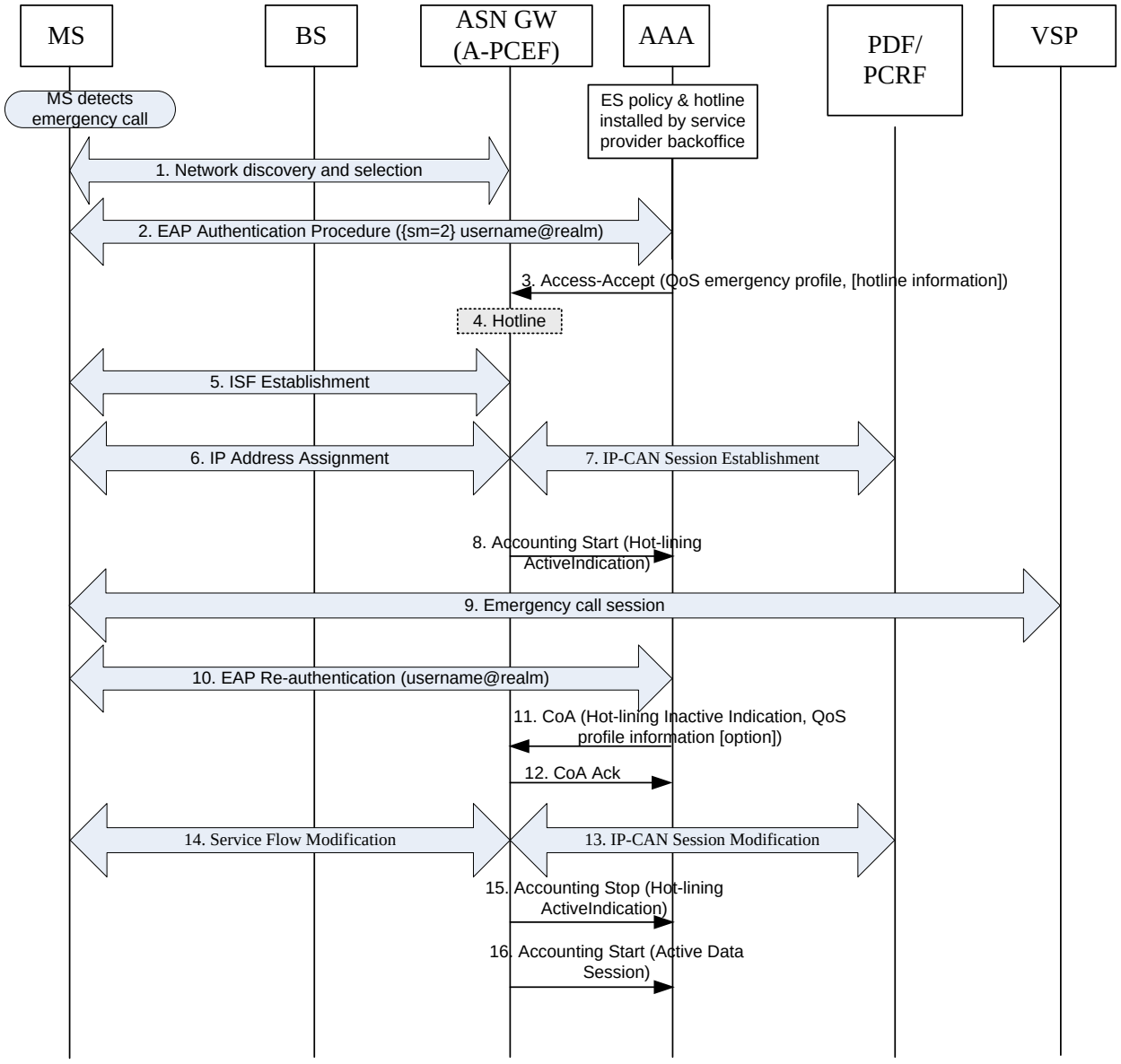


Figure 4: Authorized emergency network entry with PCC

In the case where an MS detects an Emergency Call while not being attached to a WiMAX network the MS SHOULD initiate an emergency network entry according to the steps described below.

Note: For cases where the MS is not able to recognize an emergency call, only normal network entry procedures can be used by the MS and no ES-specific treatment during network entry procedures can be applied.

1. MS performs standard network discovery and selection (Initial network entry procedure as per [NWGSTG3], section 4.5.1.1).
2. During EAP authentication that is performed with the same steps as required for the present subscription, the MS decorates the outer NAI as specified in section 7.2.1. In cases where both device and subscription authentication are performed both NAIs SHALL be decorated to indicate the emergency network entry. The decoration of the device NAI SHALL be the same as for the subscription NAI.
   The AAA server responsible for authorizing the access attempt in cases where device authentication is performed MAY decide based on internal policy and on the EAP method used to skip the second authentication after successful device authentication in cases where emergency NAI decoration is present.
3. The AAA server authorizes the emergency network entry and sends Access-Accept to the authenticator. Hotlining MAY apply here. Hotlining is a deployment option where the operator directs the authorized emergency VoIP call to a VSP which further connects the VoIP call to the desired PSAP. Hotline support for Callback parameters is FFS.
   The AAA server SHOULD be pre-configured with a QoS emergency profile. When the AAA server receives access request with an E-NAI, it SHOULD deliver the QoS emergency profile to authenticator/anchor SFA so that it can establish a bearer for the emergency session.
4. The MS MAY be hotlined as described in [NWGSTG3], section 4.4.3.5, depending on the AAA server policy, e.g. if only limited authorization has been performed.
5. Anchor SFA establishes the initial service flow(s) (ISF) or optionally all the pre-provisioned service flows establishment as specified in NWG Network Architecture Stage-3 [NWGSTG3] / NWG Policy and Charging Control [NWG_PCC].
6. The MS gets an IP address (via DHCP or MIP).
7. The Anchor SFA/A-PCEF should initiate the IP CAN session establishment Procedure with PDF/PCRF. The Anchor SFA/A-PCEF may send the QoS profile obtained from AAA server during the step 3 to PDF/PCRF. After IP CAN session establishment, the Anchor SFA gets the appropriate PCC rules from the PDF/PCRF and if the received PCC rules are different from those received from the AAA, the A-PCEF/Anchor-SFA SHALL modify the QoS of ISF and if applicable, PPSFs.
   The detailed procedure is defined in [NWG_PCC].
8. The accounting client sends an accounting start message to the AAA server according to [NWGSTG3].
9. The MS has performed network entry to the WiMAX network and proceeds with establishing the emergency call with the VSP. Procedures required for this step are specific to the supported VoIP service, and are not in the scope of this document. The VSP SHOULD initiate QoS authorization to the PCRF to support priority for emergency service signalling and/or bearer as needed.
10. When the user indicates to terminate emergency services access and change to normal access, the MS MAY perform re-authentication. The MS re-authenticates with a NAI that SHALL NOT carry the emergency decoration as specified in section 7.2.1. If the AAA server receives such re-authentication request for a subscription where the active authentication session has been requested with an emergency decorated NAI, the AAA server based on local policy SHOULD accept a valid re-authentication request and put the authentication session back to normal (non-emergency) access. After a specific time when an emergency call was terminated, the network SHOULD perform re-authentication or network re-entry of the MS.

The subsequent steps apply depending on whether the emergency session is hot-lined or whether re-authentication was performed in step10:

11. The AAA server MAY send a CoA message to the ASN AAA client / HLD with updated QoS profile information for normal access. If hotlining is applied the AAA server SHALL include ‘Hot-lining Inactive Indication’ in the CoA message carrying the QoS profile, or send a CoA message for hotlining if no QoS profile is sent, to release the hotlining specific to the emergency session. Upon receipt of a CoA message carrying QoS profile information the ASN SHALL update its QoS profile with the one received in CoA. If the CoA does not contain QoS profile information the ASN will either use QoS profile information received during initial network entry, or continues to use the QoS profile used for ES network entry.

12. The ASN-GW/HLD confirms receipt of the CoA message by sending a CoA Ack message to the AAA server.
13. If the QoS profile has been updated, the anchor SFA/A-PCEF triggers the IP CAN session modification procedure with PDF/PCRF according to [NWG_PCC]. After IP CAN session modification, the Anchor SFA gets the appropriate PCC rules from the PDF/PCRF, and
14. The Anchor SFA SHALL update the existing service flow via PCC rules.
15. The ASN-GW/HLD generates an Accounting Request (Stop) message for the hotlined session.
16. The Accounting Request (Stop) message SHALL be followed by an Accounting Request (Start) message indicating the start of the normal packet data session.

Note 1: Procedures to perform step 7 with the VoIP service being IMS, are described in [NWG_IMSES].

Note 2: If hot-lining is applied to the ES session and the MS re-authenticates to release hot-lining and get normal access, it is up to the AAA server policy to decide in step 10 above whether to allow this.

If the AAA server does not accept re-authentication, the MS MUST perform a new initial network entry after finalizing emergency access.

7.1.1.3 Emergency network entry for unauthorized subscription

The following figure provides the high-level message flow for the given non-roaming scenario that is performed for an emergency registration with network entry. It is assumed that the MS subscription information for WiMAX network entry is available, but the authorization procedure fails. The device is subsequently granted limited access to perform emergency calling.

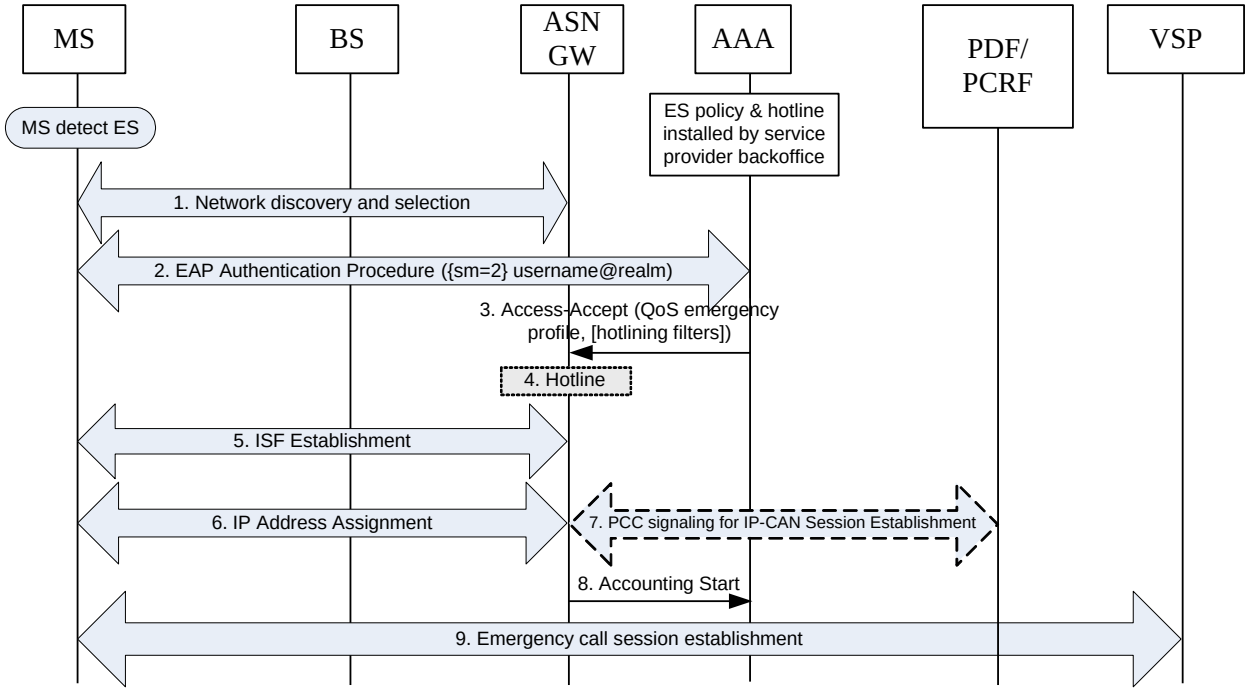


Figure 5: Emergency network entry for unauthorized subscription

In the case where an MS detects an Emergency Call while not being attached to a WiMAX network the MS SHOULD initiate an emergency network entry according to the steps described below.

Note: For cases where the MS is not able to recognize an emergency call, only normal network entry procedures can be used by the MS. In the case of authorization failure, the MS would be rejected and would not be able to enter the WiMAX network.

1. The MS performs standard network discovery and selection procedures according to [NWGSTG3].
2. During EAP authentication, the MS uses the available subscription credentials and decorates the outer NAI as specified in section 7.2.1. The same procedure as in step 2 of section 7.1.1.1 holds if device and subscription authentication are performed. The AAA server detects an authorization failure based on the subscription information provided by the MS. It SHOULD (based on internal policy) grant limited authorization for unauthorized emergency service access to the MS. If such limited authorization is not granted, the AAA server answers to the authorization request with an Access-Reject message according to the standard procedures specified in [NWGSTG3].
3. The AAA server authorizes the emergency network entry and sends Access-Accept to the authenticator. The Access-Accept SHOULD include an Authorization-Status VSA set to the value 01 to indicate limited service mode due to lack of authorization has been granted for emergency access. The AAA server MAY depending on local policy for unauthorized MS entry, activate hotlining if hotlining support is available. Hotlining may be activated either in the ASN or CSN.
   The AAA server provides hotline attributes. In the example shown in Figure 5, the hotline attributes are provided to the ASN, and are included in the Access-Accept.
   The AAA server SHOULD be pre-configured with the QoS emergency profile. When the AAA server receives access request with an E-NAI, it SHOULD deliver the QoS emergency profile to authenticator/anchor SFA to establish the bearer for the emergency session.
4. The MS MAY be hotlined. Hotlining is a deployment option where the operator directs the authorized emergency VoIP call to a VSP which further connects the VoIP call to the desired PSAP. The hotline feature is described in section 4.4.3.5 of [NWGSTG3]. Hotline support for Callback parameters is not in scope of this document.
5. Anchor SFA establishes the initial service flow (ISF) for the MS as specified in NWG Network Architecture Stage-3 [NWGSTG3] / NWG Policy and Charging Control [NWG_PCC].
6. The MS gets an IP address (via DHCP or MIP) through ISF.
   WiMAX network assigns local IP address to MS when MS performs DHCP or MIP procedure using ISF.
7. If PCC functionality is used, the anchor SFA/A-PCEF should initiate the IP CAN session establishment Procedure via PDF/PCRF. After IP CAN session establishment, the Anchor SFA gets the appropriate PCC rules from the PDF/PCRF and establishes PPSF for the MS. The detailed procedure is defined in [NWG_PCC].
8. The accounting client sends an accounting start message to the AAA server according to [NWGSTG3].
9. The MS has performed network entry to the WiMAX network and proceeds with establishing the emergency call with the VSP. Procedures required for this step are specific to the supported VoIP service, and are not in the scope of this document.

Note 1: Procedures to perform step 7 with the VoIP service being IMS, are described in [NWG_IMSES].

The MS is expected to perform a new initial network entry after finalizing emergency access. If the MS performs re-authentication (as described in section 7.1.1.1 for authorized cases), the AAA server SHALL reject the re-authentication.

7.1.1.4 Network entry for unauthenticated emergency services

Unauthenticated access using the emergency request indication must only be used for requesting access to an emergency service. As a result, reauthentication subsequent to the limited-access emergency network entry as described in section 7.1.1.1, step 9 of Figure 3 SHALL NOT be allowed.

In the case where support for unauthenticated emergency services through the WiMAX network is required e.g. based on regulatory requirements that apply to the WiMAX network operator, the WiMAX network SHALL support limited service mode network entry to allow access to emergency services, as described in this subsection.

A limited service mode network entry is granted by the operator in cases where the MS does not possess a valid WiMAX subscription or uses a subscription that does not allow authentication to be performed (in contrast to the unauthorized case where authentication can be performed but the subsequent authorization process results in a lack of authorization for normal operation).

If user authentication is not possible for a MS and the MS requests unauthenticated access to the WiMAX network for emergency, the MS SHALL perform a device-only authentication based on EAP-TLS during initial emergency network entry and indicate emergency in the WiMAX NAI decoration as per section 7.2.1.

When the CSN AAA server recognizes a network entry attempt indicating emergency and decides to grant limited service mode network entry to allow direct access to emergency services although authorized or unauthorized network entry is not possible the CSN SHALL negotiate the use of EAP-TLS with the MS. The AAA server includes its CSN certificate with the EAP-TLS server_hello message. When the MS receives a AAA server certificate during unauthenticated emergency network entry, the MS SHOULD validate the AAA server certificate and act as defined in the section 4.4.1.2 with the exception that the MS SHALL NOT reject the connection in the case of a validation failure.

A WiMAX network that supports unauthenticated network entry for emergency services SHALL support, in compliance with the applying regulatory framework and operator policy, device-only authentication based on EAP-TLS and SHALL allow limited service mode network entry for an MS that performs initial network entry based on EAP-TLS with the emergency service request indicated in the WiMAX NAI decoration as per section 7.2.1.

Network entry for unauthenticated emergency services access is performed as described in section 7.1.1.3 for unauthorized cases with the following difference:

- In step 3, the Access-Accept SHOULD include an Authorization-Status VSA set to the value 02 to indicate limited service mode due to unauthenticated emergency access.

The support of unauthenticated access as covered by this specification is orthogonal to and does not introduce any limitations regarding access to the VSP service. The provision of unauthenticated emergency service at the service level is subject to the specific VoIP service.

7.1.2 Roaming with VSP reachable through hNSP

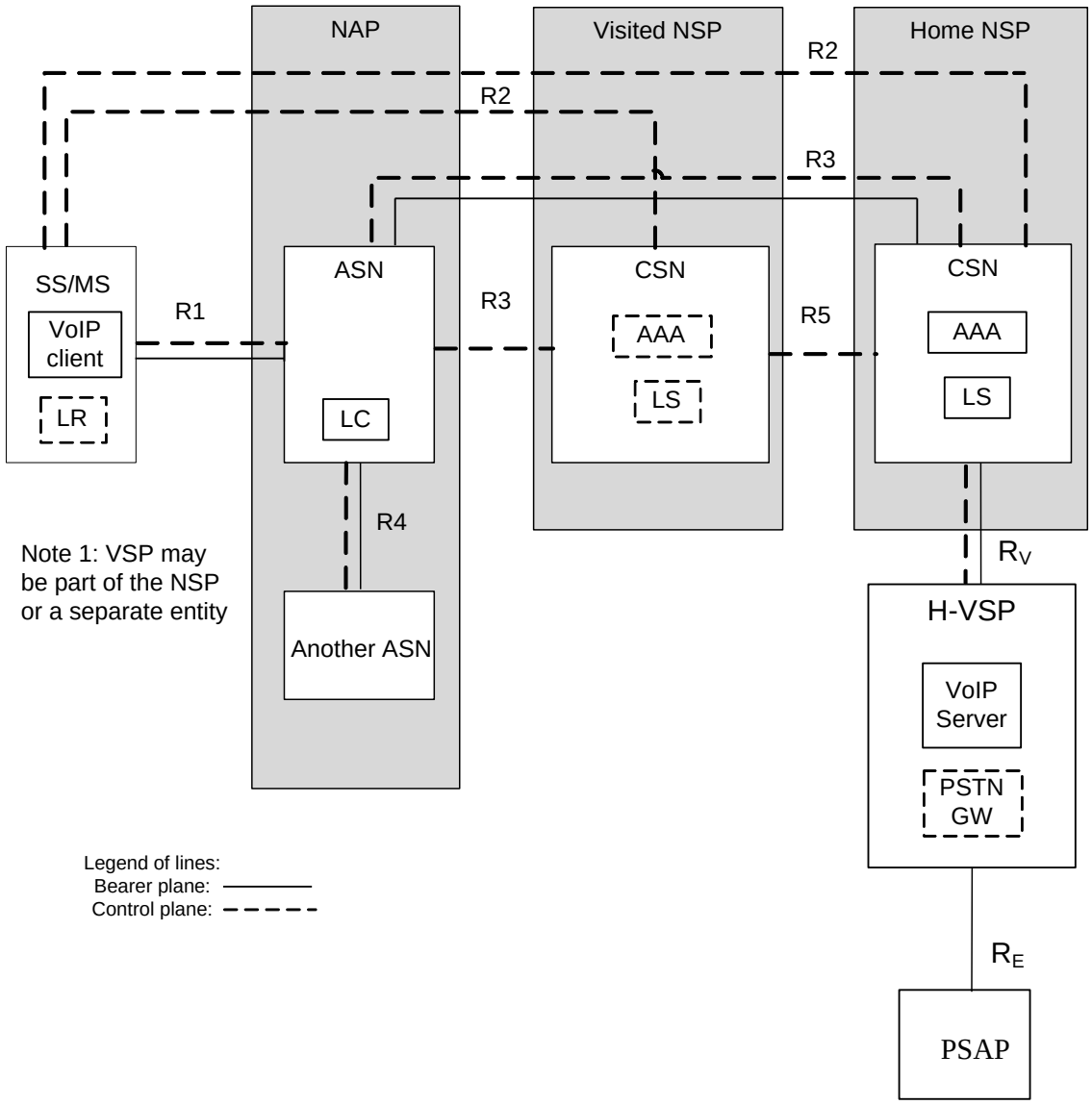


Figure 6: Roaming with VSP reachable through hNSP

In this scenario an MS is located in a visited network and is connected to its Home CSN (as Home Agent). Example of such case is when no compatible VSP in the visited domain is available, or as fallback in case local breakout cannot be provided. This case happens when no compatible VSP in the visited domain is available, or as fallback in case local breakout cannot be provided.

Note: Local breakout, i.e. anchoring the IP session of a MS in the visited CSN, is possible when being set up during initial network entry. In cases where an IP session is anchored in the home CSN, establishing a new IP session anchored in the visited CSN without a new network entry is currently not supported.

Support of emergency services might be limited in this scenario, e.g. in cases where the VSP being in a different region than the roaming MS might not be able to identify and contact the correct PSAP being responsible for the current location of the MS. Solutions like LoST [RFC5222] MAY be used in this scenario to support PSAP discovery.

MS MAY perform network re-entry with emergency NAI to force local breakout if available. If local breakout is not available, MS will be routed to H-NSP.

Note: Full support of emergency services in this scenario is currently under study.

7.1.3 Roaming with visited VSP available

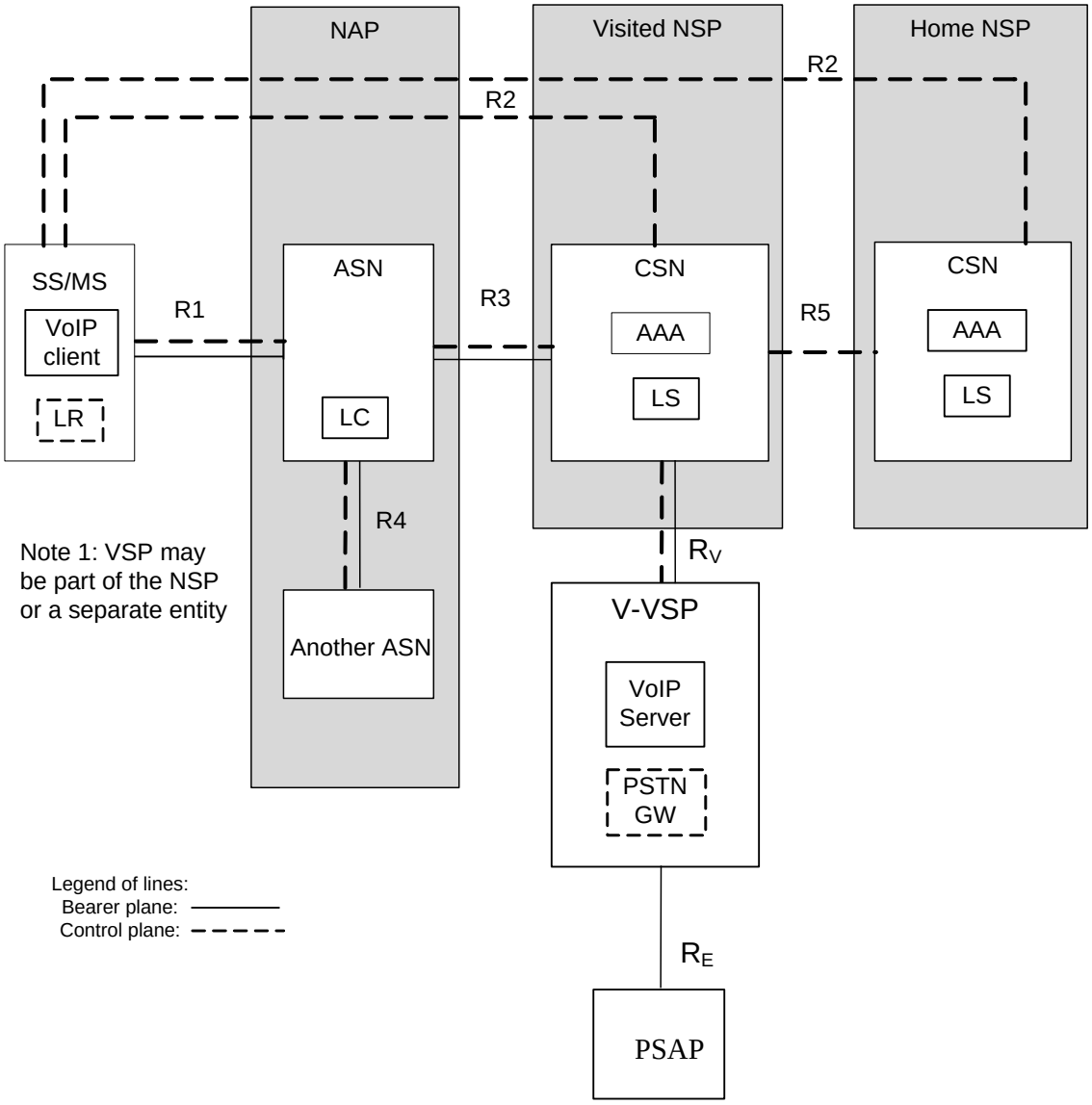


Figure 7: roaming with VSP available in visited domain

In this scenario an MS is located in a visited network. If local breakout capability is available, the IP traffic is routed through the visited NSP while the authorization of services is performed by the Home NSP. In this case, voice services are provided by a VSP in the visited network.

Local breakout (see 7.1.2) in case of an ES call is the preferred configuration. However, full local breakout support is currently not specified for WiMAX networks. As a fallback solution and also in the case of incompatible VoIP applications, home routed traffic may be used as described in section 7.1.2.

Note: DN assignment for roaming subscriber for callback support from the PSAP may be limited.

7.1.4 Emergency network entry for unauthenticated cases in roaming

Possible cases within this scenario are e.g. network entry attempts where the indicated home CSN is not reachable, or where a terminal prepared for a specific WiMAX service, but not yet provisioned with any valid subscription, attempts to access unauthenticated emergency services.

See section 7.1.1.4 for unauthenticated emergency network entry. In addition, the following rules apply in case of roaming.

When a visited CSN recognizes a network entry attempt indicating emergency and decides to grant limited service mode network entry to allow direct access to emergency services without involvement of the home CSN (because the MS does not provide sufficient information to identify any home CSN, because it has no roaming agreement with the home CSN, or because the home CSN is not reachable for other reasons), the visited CSN SHALL negotiate the use of EAP-TLS with the MS. EAP-TLS is then handled by the visited AAA server. The Visited AAA server includes its visited CSN certificate with the EAP-TLS server_hello message. When the MS receives a AAA server certificate during unauthenticated emergency network entry, the MS SHOULD validate the AAA server certificate and act as defined in the section 4.4.1.2 with the exception that the MS SHALL NOT reject the connection in the case of a verification failure.

7.2 Numbers/Identifiers for Emergency Services

7.2.1 ES Identifiers in Network Entry

For any new network entry to access emergency services the MS SHALL indicate to the network that it is requesting emergency services, the MS SHALL use the following value in the WiMAX decoration (per [NWGSTG3] section 4.4.1.3.1):

{sm=2}<username>@<NSPRealm>

Where:

sm=2: indicates that the network entry attempt is performed to access emergency services

username: is either the username information for subscription authentication, or the MAC address if EAP-TLS is being used (per [NWGSTG3] section 4.4.1.2.1)

NSPRealm: is the home realm of the subscription used by the MS.

If no NSPRealm of a subscription is available to the device (e.g. in case the device is requesting unauthenticated emergency service), the NSPRealm to be used by the device is FFS.

7.3 Location Information & Technology

7.3.1 Location Information

The location information of the MS is an essential part for ES. Two ES location related capabilities SHALL be supported as listed below:

1. In the initial phase of establishing an emergency call, location information SHALL be provided that provides sufficient accuracy to determine the responsible PSAP serving the location of the terminal (PSAP selection).
2. In a later phase of an established emergency call, if Nomadic and/or Mobility Access usage is supported, more accurate location information SHALL be supported; otherwise more accurate location information MAY be supported e.g. for sending emergency aid personnel to the correct place and to assist them in their response.

7.3.1.1 Location information required for PSAP selection

In case of an emergency call establishment, the PSAP responsible for the location area needs to be determined. This requires location information at the VSP.

The WiMAX CSN SHALL support providing location information to the VSP for PSAP selection using network based methods as not all terminals may be able to provide location information or match the required trust level regarding such information. Also, a VSP may not be able to interpret the terminal-provided information (which may happen if the MS provides just the BSID and the VSP is not able to resolve this to the appropriate PSAP).

In addition, location information MAY be provided by the MS itself.

The VSP as well as the LBS service of the WiMAX network SHOULD choose a location determining method where location information will be available as quick as possible as it impacts the call setup time which SHOULD be kept short. At least location information of sufficient accuracy to determine the correct PSAP SHALL be supported.

7.3.1.2 Location information to determine subscriber location and to perform location tracking

A PSAP MAY request location information for a subscriber within an active call or where the call was terminated a short time ago. The time for location determination in this case is less critical compared to what is required for PSAP selection. More precise location information SHOULD be provided to the PSAP by the MS or the network (depending on the respective capabilities).

Location information to determine subscriber location may consist of the associated geographical location information which may be in civic or geodetic format (see e.g. [IETF-Geo] and [RFC5139]). Note that depending on the regulator, either civic location or geodetic information may be required.

7.3.2 Location Information exchange between WiMAX network and VSP

This document does not consider the VoIP technology used by the VSP. It is expected that the VSP performs the selection of the PSAP, and is the entity to connect with the PSAP. To cover location information related requirements, the CSN SHALL provide location information to the VSP to allow the VSP the PSAP selection as well as determination of subscriber location and location tracking as far this is required by the responsible PSAP.

For this release of the standard, no specific protocol is recommended to be used to interconnect a VSP with a WiMAX CSN to exchange such location information.

7.3.3 Location Determining Technology

Generally, any location determination technology could be used to provide location information for the purpose of ES as far as requirements for ES are covered. The location determination technology might include the use of or a combined use of the following methods: BSID, A-GPS/GPS, cell area based location, the LBS capability as specified in [802.16g], IEEE 802.1AB with LLDP-MED extension as specified in [802.1AB-LLDPMED], and/or other network-based and/or MS-based location determination technologies. Its main objective is to provide a determination and validation of location information of a WiMAX mobile station.

For the purpose of supporting the WiMAX ES feature, this specification focuses on the use of cell area based and/or the optional A-GPS/GPS method though other methods for determining the device location are possible (see [NWG_LBS]).

As location service is also part of WiMAX, the location services specified in [NWG_LBS] SHALL be the preferred solution. At least network based methods which do not require specific support from the MS SHALL be supported by the network where cell area based location information SHOULD be provided as a minimum. Furthermore, the network SHOULD provide assistance for MS based location determination. The method to provide location related assistance data to the MS is specified in [NWG_LBS]. Providing assistance information such as GPS assistance data to the MS reduces the time for location determination dramatically.

8. Detailed impact on Functional Entities

This section describes the functional entities and ES specific capabilities they need to provide for ES support in WiMAX networks.

8.1 Access Service Network (ASN)

ASN should support the determination of location information of the device requested by the LS. WiMAX specific functionality for providing such location information is specified in [NWG_LBS].

Upon receiving the Authorization-Status VSA value set to 01 or 02 in the Access-Accept, the action taken by the ASN is based on local policy.

8.2 Connection Service Network (CSN)

8.2.1 Authorization, Authentication, Accounting (HAAA) Server

The AAA server MAY store the QoS emergency profile, authorize requests for emergency access and delivers the ES specific QoS profile information to the NAS.

The AAA server is responsible, based on regulatory requirements, to grant network access for emergency in cases where a MS fails authorization or authentication for network access for an existing subscription.

The AAA server SHALL support the indication for requesting emergency services as per section 7.2.1.

In case of granting unauthorized access for emergency service, the AAA server SHOULD include an Authorization-Status VSA set to the value 01 in the Access-Accept.

In case of granting unauthenticated access for emergency service, the AAA server SHOULD include an Authorization-Status VSA set to the value 02 in the Access-Accept.

The AAA server MAY provide hotline information when authorizing network entry in limited service mode.

8.2.2 HA

This specification does not introduce new functionality specific to the HA as defined per [NWGSTG3].

8.2.3 PCRF

PCRF MAY be preconfigured with emergency session profile or may get it from the SPR.

PCRF MAY be involved in authorizing the emergency session and generating PCC rule based on the emergency session profile and the priority of emergency service. Also the PCRF MAY set the charging rule as no-charging, based on the emergency session profile. The classifiers defined as part of the PCC rules SHOULD be limited to carry emergency data/signals only.

8.2.4 Location Server

The WiMAX CSN SHALL support a Location Server, which provides location information to the VSP (LRF) for PSAP selection using network based methods. WiMAX specific functionality for providing such location information is defined in [NWG_LBS].

8.3 Mobile Station (MS)

If the MS has a capability to recognize emergency calls, it SHALL support the indication for requesting emergency services as per section 7.2.1.

If unauthenticated network entry for emergency service access is supported, the MS SHALL support device-only authentication based on EAP-TLS.

1

9. Additional considerations

9.1 Security Considerations

Many of the security considerations applying to emergency services relate to the support for unauthenticated access to the network resources in case unauthenticated emergency services are required. This includes careful consideration of how to allow limited access for a device to receive emergency services in cases where no subscription is available for WiMAX access on the device, or where the existing subscription does not work for some reason.

This version of the document provides means for enabling unauthenticated network entry for emergency service access based on WiMAX device-only authentication. Unauthorized access to emergency services is supported. In the former case, the only authenticated identity that is available to the WiMAX network is the MS_ID (MS MAC address).

The following elaborates from a technical perspective on the difference between an unauthenticated and unauthorized access to a WiMAX network.

In general, when emergency services are provided, this version of the present specification assumes that at least authentication to the WiMAX network can be performed (i.e. the MS can denote a valid home CSN that is reachable for the NAP or visited NSP and the keys shared between MS and home AAA server allow successful execution of EAP authentication and provide an authenticated subscription identity to the WiMAX CSN). In fact, this means that the MS must at least be able to provide sufficient credentials and information to allow the WiMAX network to create a link to an existing subscription. If this cannot be achieved, the MS attempts to enter the WiMAX network unauthenticated (unauthenticated case).

Subsequently, however, after successfully identifying a subscription and cryptographic authentication the underlying WiMAX subscription might lack sufficient authorization for normal WiMAX network service (unauthorized case).

In both an unauthorized and an unauthenticated case, it is the responsibility of the WiMAX network to guarantee that any MS lacking authorization (e.g. in the case where a prepaid subscription is lacking sufficient credits for further service) or not being able to provide a meaningful subscription is restricted to access the minimum required services including emergency services.

Similar considerations hold for the subscription with the actual VSP. Here, it is the responsibility of the VSP to guarantee that (assuming compatible VoIP technologies) the subscriber is limited to access emergency services only (and e.g. not be able to establish normal service, like standard VoIP calls). This also holds for the case where unauthenticated emergency services are requested from the VSP (i.e. WiMAX subscription available, but unauthenticated access to the VSP services). Note that the provisioning of unauthenticated access to the VSP service is out-of-scope for this document, but MAY be supported by the specific VoIP technology like for IMS [NWG_IMSES].

[RFC5069] gives general security requirements that any solution following the guidelines given in this document SHOULD match.

9.2 Emergency Indication in VoIP signaling

If SIP is used as VoIP protocol, the special indications for emergency sessions within the SIP signaling as specified in [RFC5031] SHALL be supported:

- urn:service:sos - The generic 'sos' service reaches a public safety answering point (PSAP) which in turn dispatches aid appropriate to the emergency. It encompasses all of the services listed below.
- urn:service:sos.ambulance
- urn:service:sos.animal-control
- urn:service:sos.fire

- urn:service:sos.gas
- urn:service:sos.marine
- urn:service:sos.mountain
- urn:service:sos.physician
- urn:service:sos.poison
- urn:service:sos.police

9.3 Priority

Access priority in the WiMAX network for establishing an ES session SHOULD be provided by using an appropriate emergency session profile either in the AAA downloaded to the NAS (during initial network entry) or in the PCRF/SPR resulting in PCC rules for ES installed in the ASN (for both initial network entry and an already connected MS). If PCC functionality is used, the VSP SHOULD initiate QoS authorization to the PCRF to support priority for emergency service signaling and/or bearer as needed.

The method for providing priority in call processing is specific to the VoIP technology available in the VSP. See e.g. [NWG_IMSES] for priority call processing support in case IMS is used.

9.4 Support for Callback

The method for providing support for callback is specific to the VoIP technology available in the VSP.

However, support for callback is limited to emergency calls with valid credentials, and SHOULD NOT be assumed for unauthenticated or unauthorized emergency calls.

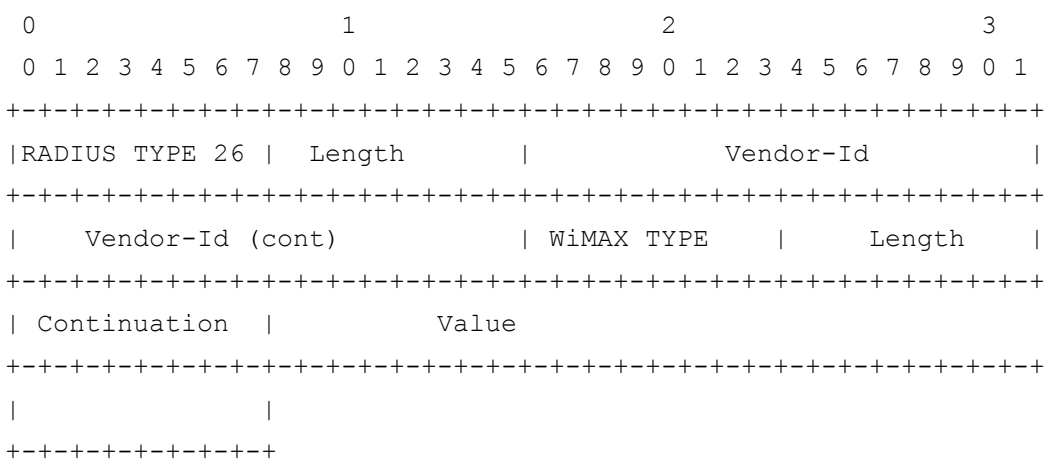
9.5 Handover

No specific requirements regarding handover of emergency calls apply to this specification.

10. Message and Parameter Definitions

This section describes additional WiMAX VSAs that are defined for emergency services support.

RADIUS attributes for emergency support



WTypeTLV- ID	105 for Authorization-Status
Description	In an Access-Accept message indicates that access has been granted in limited service mode, and provides the reason.
Length	6+3+4 octets
Continuation	**C-bit = 0**
Value	Unsigned Integer. In an Access-Accept the AAA specifies a reason in case access has been granted although authorization of the subscription is not sufficient. If not present, no limitation of authorization is indicated. The enumeration is defined as follows: • 0 = fully authorized • 1 = lack of authorization, but access granted for emergency • 2 = unauthenticated (device-only), access granted for emergency All other values are reserved for future use. If the attribute is present with a reserved value set, it SHALL be ignored.

Diameter AVPs for emergency support

This section describes additional WiMAX vendor specific AVPs that are defined for emergency services support.

WType-ID	82 for Authorization-Status
Description	In a WDEA message indicates that access has been granted in limited service mode, and provides the reason.
Value-Type	Enumerated
Value	In an Access-Accept the AAA specifies a reason in case access has been granted although authorization of the subscription is not sufficient. If not present, no limitation of authorization is indicated. The enumeration is defined as follows: • 0 = fully authorized • 1 = lack of authorization, but access granted for emergency • 2 = unauthenticated (device-only), access granted for emergency All other values are reserved for future use. If the attribute is present with a reserved value set, it SHALL be ignored.

1

2