

3GPP2 X.S0060-0  
Version 1.0  
Date: July 2008



3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"

---

## ***HRPD Support for Emergency Services***

### **COPYRIGHT**

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at [secretariat@3gpp2.org](mailto:secretariat@3gpp2.org). Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See [www.3gpp2.org](http://www.3gpp2.org) for more information.

---

## Revision History

<b>Revision</b>	<b>Description of Change</b>	<b>Date</b>
Rev. 0 v1.0	Initial Publication	July 2008

HRPD Support for Emergency Service

**CONTENTS**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

---

- List of Figures ..... ii
- List of Tables ..... iii
- Foreword ..... iv
- 1 Introduction ..... 1
  - 1.1 Scope ..... 1
- 2 References ..... 2
  - 2.1 Normative References ..... 2
  - 2.2 Informative Reference ..... 2
- 3 Definitions, Abbreviations and Acronyms ..... 3
  - 3.1 Definitions ..... 3
  - 3.2 Abbreviations and Acronyms ..... 3
- 4 IMS Emergency Services Using HRPD/PDS Network ..... 4
  - 4.1 Requirements on the HRPD Network as an IP-CAN ..... 4
  - 4.2 UE Specific Behavior for Emergency Calls over HRPD ..... 4
    - 4.2.1 Without Existing Data Session ..... 4
    - 4.2.2 With Existing Data Session ..... 5
  - 4.3 Information Flows ..... 5
    - 4.3.1 Emergency Call: HRPD Session Establishment for Unauthenticated Caller ..... 5
    - 4.3.2 Emergency Call: Authenticated UE while Roaming ..... 8
- 5 Carrier-ID ..... 11
  - 5.1 DHCPv6 Options ..... 11
  - 5.2 DHCP Options ..... 12

# LIST OF FIGURES

---

<i>Figure 1</i>	Unauthenticated UE Initiates an Emergency Call .....	6
<i>Figure 2</i>	Authorized UE Initiates an Emergency Call while Roaming .....	9

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

# LIST OF TABLES

---

<i>Table 1</i>	DHCPv6 Vendor Class option.....	11
<i>Table 2</i>	DHCPv6 Vendor-Specific Information option.....	11
<i>Table 3</i>	DHCP Vendor Class Identifier option.....	12
<i>Table 4</i>	DHCP Vendor-Specific Information option.....	12

# FOREWORD

---

(This foreword is not part of this Specification.)

This document specifies IMS Emergency Services using the HRPD Network.

This document was developed by the TSG-X Technical Specifications Group of Third Generation Partnership Project 2.

## Terminology

This document uses the following “verbal forms” and “verbal form definitions”:

1. “shall” and “shall not” identify items of interest that are to be strictly followed and from which no deviation is recommended;
2. “should” and “should not” indicate items of interest that are highly desirable and particularly suitable, without identifying or excluding other items; or (in the negative form) indicate items of interest that are not desirable, are not particularly suitable, or are not recommended but not prohibited; and
3. “may” and “may not” indicate items of interest that are optional but permissible within the limits of this recommendation.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

# 1 Introduction

---

This document specifies IMS Emergency Services using the High Rate Packet Data (HRPD) Network.

## 1.1 Scope

---

This document covers the Access Network aspects that are essential for the provisioning of IMS emergency services. In particular HRPD [2], [6], [7] is supported. For cdma2000<sup>1</sup>-1X access networks the traditional circuit switch approach for emergency services [5] should be used.

All other IP based support for Emergency Services has been included in the Common IMS work with 3GPP. Requirements can be found in [4]. Stage 2 descriptions can be found in [3].

---

<sup>1</sup> *cdma2000<sup>®</sup> is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000<sup>®</sup> is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.*

## 2 References

---

### 2.1 Normative References

---

The following standards contain provisions which, through reference in this text, constitute provisions of this Specification. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP2 document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

- [1] 3GPP2 X.S0011-005-D: *Wireless IP Network Standard: Accounting Services and 3GPP2 RADIUS VSAs*
- [2] 3GPP2 C.S0024-A: *cdma2000 High Rate Packet Data Air Interface Specification*
- [3] 3GPP TS 23.167: *IP Multimedia Subsystem (IMS) emergency sessions*
- [4] 3GPP TS 22.101: *Service Aspects; Service Principles*
- [5] J-STD-036-B: *Enhanced Wireless 9-1-1, Phase 2*; June 2005
- [6] 3GPP2 A.S0008-C v1.0: Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network, July 2007
- [7] 3GPP2 A.S0009-C v1.0: Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Packet Control Function, July 2007

### 2.2 Informative Reference

---

- [8] 3GPP2 S.R0037: *IP Network Architecture Model for cdma2000 Spread Spectrum Systems*

# 3 Definitions, Abbreviations and Acronyms

---

This section contains definitions, abbreviations and acronyms that are used throughout this document.

## 3.1 Definitions

---

### Emergency-CSCF (E-CSCF)

---

The Emergency-CSCF handles certain aspects of emergency sessions, e.g., routing of emergency requests to the correct PSAP.

### IP Connectivity Access Network (IP-CAN)

---

The collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and the IMS entities. An example of an “IP-Connectivity Access Network” is HRPD/PDS.

### Public Safety Answering Point (PSAP)

---

A physical location that receives emergency calls from the public.

## 3.2 Abbreviations and Acronyms

---

This section provides a definition of the abbreviations used within this recommendation, as:

AAA	Authentication, Authorization, and Accounting
AN	Access Network
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
E-CSCF	Emergency-CSCF
HRPD	High Rate Packet data
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP-CAN	IP Connectivity Access Network
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
L2TP	Layer 2 Tunneling Protocol
MGW	Media Gateway
NAI	Network Access Identifier
P-CSCF	Proxy CSCF
PCRF	Policy Charging Rules Function
PDS	Packet Data Subsystem
PDSN	Packet Data Serving Node
PPP	Point to Point Protocol
PSAP	Public Safety Answering Point
QoS	Quality of Service
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier
UE	User Equipment

## 4 IMS Emergency Services Using HRPD/PDS Network

### 4.1 Requirements on the HRPD Network as an IP-CAN

For an emergency call over HRPD, the requirements on the IP-CAN are covered by the following HRPD specific requirements:

- HRPD networks shall authenticate the UE in accordance with normal authentication procedures, i.e., A12 and PDSN authentication. For support of unauthorized emergency callers, A12 support is optional, PDSN authentication is required.
- HRPD networks may allow limited access to UEs that wouldn't normally be authenticated, but which provide authentication credentials specific to emergency service. In this case, the HRPD network allows access to UEs using emergency NAIs of the form emergency@emergency.com and emergency@a12.emergency.com for PDSN and A12 authentication respectively.
- HRPD networks shall provide data access of the type requested by the UE, i.e., Simple IPv4, Simple IPv6, Mobile IPv4, and Mobile IPv6.
- The HRPD network shall not provide L2TP service to the UE. This is general requirement and not only applicable to emergency services.
- HRPD networks shall provide the address of the local P-CSCF via DHCP or DHCPv6 depending on the type of IP address acquired by the UE. This could be an IP (v4 or v6) address or a SIP URI.
- HRPD networks shall provide Carrier-ID information to the UE via DHCP or DHCPv6 so that the UE may determine if it is roaming or not. Carrier-ID is defined in Section 5.

### 4.2 UE Specific Behavior for Emergency Calls over HRPD

For the specific case of an emergency call over HRPD the UE shall adhere to the following procedures:

#### 4.2.1 Without Existing Data Session

- If the UE wants to make an emergency call but doesn't currently have an existing data session with the HRPD network, it shall create a Simple IPv4 or Simple IPv6 session per its normal procedures.
- If the UE fails in its attempt to access the HRPD network, it may attempt to access again using the emergency NAI. In this case, the UE shall use NAIs of the form emergency@emergency.com and emergency@a12.emergency.com for PDSN and A12 authentication respectively.
- If the UE accesses the network with the emergency NAI it shall obtain either a Simple IPv4 or Simple IPv6 address.
- The UE shall obtain the address of the local P-CSCF via DHCP or DHCPv6, depending on the type of IP address is has acquired. Note: this is done when IP addresses are obtained, not when an emergency call is detected.
- The UE shall include the HRPD Sector ID of the serving AN in the P-Access-Network-Info header of the SIP INVITE request.

## 4.2.2 With Existing Data Session

---

- The UE shall obtain the address of the local P-CSCF via DHCP or DHCPv6, depending on the type of IP address is has acquired.

Note: this is done when IP addresses are obtained, not when an emergency call is detected.

- The UE shall obtain the HRPD's Carrier-ID from a DHCP or DHCPv6 server in the serving HRPD network. Carrier-ID is defined in Section 5.
  - If the UE uses Simple IPv4, it shall use the assigned Simple IPv4 address to send the DHCPINFORM message. The destination address shall be the limited broadcast address (all 1s).
  - If the UE uses Mobile IPv4, it shall use the Direct Delivery style [RFC 3024] to send DHCPINFORM message. The destination address shall be the limited broadcast address (all 1s).
  - If the UE uses Simple IPv6, it shall use the assigned Simple IPv6 address to send the DHCPv6 Information-Request. The destination address shall be the All\_DHCP\_Relay\_Agents\_and\_Servers multicast address (FF02::1:2).
  - If the UE uses Mobile IPv6, it shall use the assigned care-of-address (i.e., a Simple IPv6 address) to send the DHCPv6 Information-Request. The destination address shall be the All\_DHCP\_Relay\_Agents\_and\_Servers multicast address (FF02::1:2).
- The UE shall determine whether it's roaming based on the received Carrier-ID.
  - If the UE is roaming, it shall use the Simple IPv4 address or Simple IPv6 address.
- The UE shall include the HRPD Sector ID of the serving AN in the P-Access-Network-Info header of the SIP INVITE request.

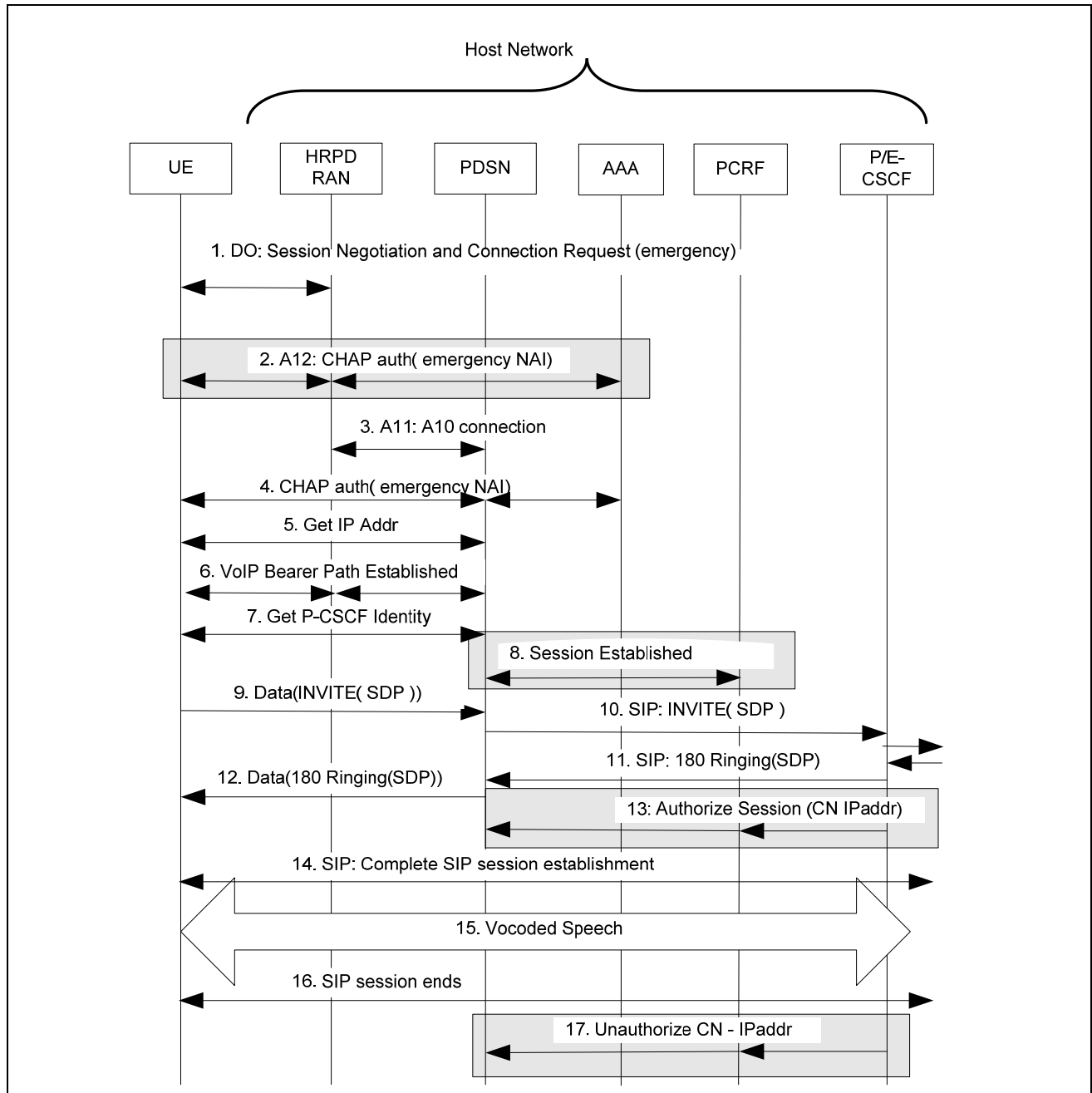
## 4.3 Information Flows

---

### 4.3.1 Emergency Call: HRPD Session Establishment for Unauthenticated Caller

---

In this scenario, a UE without sufficient credentials to establish a HRPD session, requests a HRPD session to be established for an emergency call in a network that supports emergency calls from unauthorized callers. The access, IP and Services layer must each ensure the session is used only for emergency calls. The PDSN, PCRF and P-CSCF are in the same network.



**Figure 1 Unauthenticated UE Initiates an Emergency Call**

**Preconditions:**

- UE attempted to access the system with its stored credentials and was rejected or knows a priori authentication will fail (e.g., system is not in UE’s PRL).
- HRPD system is configured for PDSN authentication, A12 is optional.
- Service Based Bearer Control (SBBC) is required in order to enforce policy for unauthorized UEs allowed HRPD access for emergency calls.

1. UE initiates HRPD session configuration by either by requesting a prior session or performing a normal session negotiation:

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

- 1 a. Prior Session Approach
- 2
- 3 a1. UE requesting a UATI and retrieval of a PriorSession that contains attributes and protocol
- 4 appropriate for VoIP.
- 5
- 6 a2. AN retrieving the PriorSession requested by the UE and assigning a UATI to the UE.
- 7
- 8 a3. The UE requests a connection from the RAN, indicating data is to be sent and includes the
- 9 Emergency Indicator, set to 1, if supported by the UE, and AN assigning a traffic channel to
- 10 the UE.
- 11
- 12 a4. Proceed with step 3.
- 13 b. Negotiated Session Approach
- 14
- 15 b1. UE requesting and receiving a UATI (i.e., RAN session identifier) from the RAN.
- 16
- 17 b2. RAN requesting and receiving a hardware id (HWID) (i.e., MEID) from the UE.
- 18
- 19 b3. UE requesting a connection from the RAN and receiving the assigned channel.
- 20
- 21 b4. UE and RAN negotiate HRPD session parameters (may include prior session request).
- 22
- 23 b5. Closing the connection between the UE and RAN.
- 24
- 25 b6. The UE requests a connection from the RAN, indicating data is to be sent and includes the
- 26 *Emergency Indicator*, set to 1, if supported by the UE and AN assigning a traffic channel to
- 27 the UE.
- 28 NOTE: Because HRPD RAN session negotiation begins at Rev.0, there is no way for the UE
- 29 to indicate emergency or priority at initial setup.
- 30
- 31 2. Once the connection is established, and if the RAN is configured to do A12 (device/access level)
- 32 authentication, the RAN will initiate CHAP. The AN-AAA detects the emergency NAI in the
- 33 UE's CHAP response and authorizes access, if local regulation or carrier policy requires
- 34 unauthorized emergency callers to be supported. No IMSI is returned by the AN-AAA for the
- 35 emergency NAI.
- 36
- 37 3. The RAN creates an IMSI and establishes an A10/A11 connection to the PDSN.
- 38
- 39 4. As part of PDSN (subscriber level) authentication, the PDSN initiates CHAP. The UE includes
- 40 the emergency NAI as part of its CHAP response. The AAA detects the emergency NAI and
- 41 authorizes the user, if local regulation or carrier policy requires unauthorized emergency callers
- 42 to be supported. ASSUMPTION: It is assumed that existing AAA or static mechanisms are used to
- 43 inform the PDSN of the limited authorization for the session (e.g., IP flow restrictions in RADIUS
- 44 Access Request/Response).
- 45
- 46 5. The UE obtains a Simple IP address.
- 47
- 48 6. The bearer path is established for the VoIP call, including QoS negotiation.
- 49
- 50 7. UE obtains the identity of the P-CSCF.
- 51
- 52 8. Optionally, the PDSN establishes a session to the local PCRF.
- 53
- 54 9. The UE starts sending data. The PDSN will only allow data destined to the P-CSCF. Packets
- 55 addressed to other destinations will be dropped. Note: This is existing policy handling
- 56 functionality.
- 57
- 58 10. The P/E-CSCF, along with other IMS entities, processes the INVITE from the UE containing the
- 59 emergency PUID, and forwards it towards the emergency network. The P/E-CSCF will reject any

- other requests. Note: A UE without sufficient credentials is allowed to initiate an emergency call anonymously, without needing to register/authenticate at the IMS/Service layer.
11. As part of call setup, the P-CSCF receives the SDP in the 180 Ringing from the far end, which includes the IP address and media characteristics for the correspondent node (e.g., IP PSAP or MGW connection to legacy PSAP trunk) and forwards it towards the UE via the PDSN.
  12. The PDSN forwards the data to the UE, since it came from the allowed IP address (P-CSCF).
  13. Optionally, in parallel with step 12, once the far end IP address is known, the P-CSCF notifies the local PCRF via Tx, that data (i.e., bearer) is also authorized to the IP address of the Correspondent Node (CN). The PCRF forwards the information to the PDSN via Ty. Priority may also be indicated for some/all of the packet traffic to/from the UE. This priority information will also be sent by the PDSN to the RAN as QoS information so that the RAN can properly handle the emergency call.
  14. The SIP session is established (i.e., 200 OK received from far end)
  15. The UE and PSAP are talking
  16. The session ends (i.e., UE or correspondent node send BYE)
  17. Optionally, once the session is over, the P-CSCF, via Tx, requests the local PCRF to remove the CN (i.e., IP address) from the allowed IP addresses. The request is then forwarded to the PDSN via Ty.

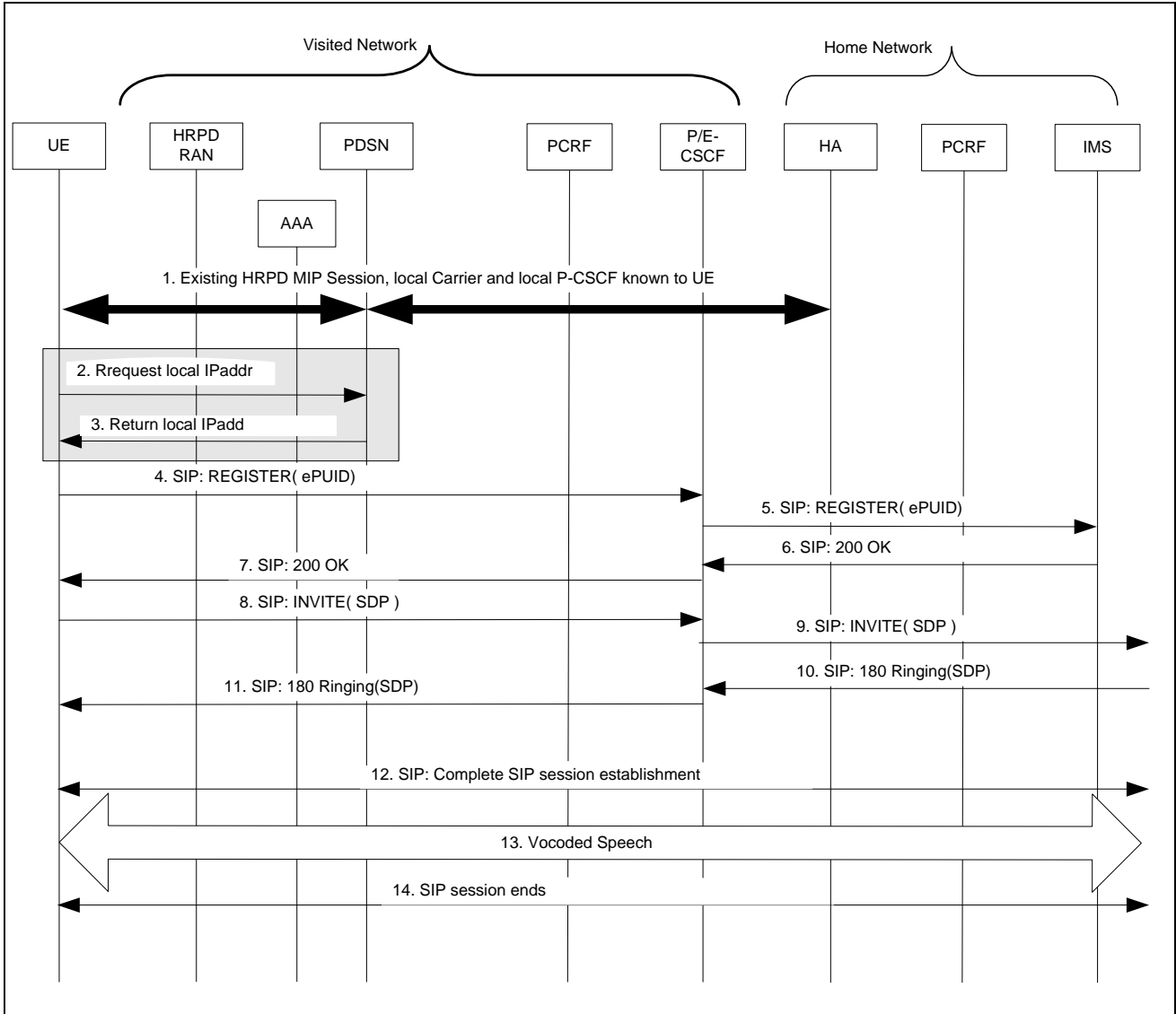
### **4.3.2 Emergency Call: Authenticated UE while Roaming**

---

A roaming and authorized UE with a Mobile IP HRPD session established, initiates an emergency call. The UE must obtain a local IP address and local P-CSCF so that the call can be serviced by the roaming carrier. The main functionality to support this is:

- a. After PPP establishment, the UE performs a local DHCP query to obtain the local Carrier and local P-CSCF.
- b. When the UE detects an emergency call, if the local Carrier is not its home Carrier, the UE obtains a local IP address if necessary.
- c. The UE performs an IMS registration with its home service provider using an emergency public user id.
- d. IMS ensures this registration is only used for emergency calls.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59



**Figure 2 Authorized UE Initiates an Emergency Call while Roaming**

1. A Mobile IP Session exists between the UE, PDSN in the visited network and the HA in the home network. The UE has been authenticated at the access/device layer, IP layer and IMS/Services layer. After PPP establishment, the UE obtained the local Carrier and local P-CSCF identity via DHCP.
2. The UE detects the user has initiated an emergency call. If the UE determines it is roaming (e.g., based on local Carrier id from step 1), the UE obtains a local IP address if necessary (e.g., For a MIPv4 session, the UE obtains a local IP address. For a MIPv6 session, this step is not needed since the UE has a local IP address in the CoA).
3. If a local IP address was requested in step 2, the local IP address is returned to the UE.
4. The UE sends an emergency registration to the local P-CSCF, using an emergency Public User Id.
5. IMS registers the UE with the ePUIID.
6. IMS registration completes.

7. The UE receives the registration response. 1
  8. The UE sends the INVITE to the local P-CSCF, including the ePUIID and emergency URN. 2
  9. The P/E-CSCF, along with other IMS entities, processes the INVITE from the UE and forwards it towards the emergency network. The P-CSCF may reject any other non-emergency requests. 3
  10. As part of call setup, the P-CSCF receives the SDP in the 180 Ringing from the far end, which includes the IP address and media characteristics for the far end (e.g., IP PSAP or MGW connection to legacy PSAP trunk) 4
  11. The 180 Ringing is forwarded to the UE. 5
  12. The SIP session is established (i.e., 200 OK received from far end) 6
  13. The UE and PSAP are connected. 7
  14. The session ends (i.e., UE or far end send BYE) 8
- 9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

# 5 Carrier-ID

Operators can be uniquely identified by the Carrier-ID value. The UE shall acquire the Carrier-ID value from the HRPD network via DHCP or DHCPv6 so that the UE may determine if it is roaming or not. The Carrier-ID value is based on the Mobile Country Code (MCC) and Mobile Network Code (MNC) values assigned to the operator. This value is also a RADIUS VSA specified in [1]. Carrier-ID is a 5 or 6 byte string comprising the 3 byte MCC and 2 or 3 byte MNC of the operator.

## 5.1 DHCPv6 Options

Upon receiving the DHCPv6 Information-Request that contains the Vendor Class option indicating 3GPP2-specific, the DHCPv6 server shall send the DHCPv6 Reply that contains the Vendor-Specific Information option for MCC/MNC.

**Table 1 DHCPv6 Vendor Class option**

0	8	16	24
Option-Vendor-Class (16)		Length	
Enterprise Number			

Option-Vendor-Class: 16

Length: 8

Enterprise Number: 5535

**Table 2 DHCPv6 Vendor-Specific Information option**

0	8	16	24
Option-Vendor –Opts (17)		Length 1	
Enterprise Number			
Option Code (4)		Length 2	
MCC/MNC			
MCC/MNC			

Option-Vendor –Opts: 17

Length 1: 18 octets

Enterprise Number: 5535

Option Code: 4 (for MCC/MNC)

Length 2: 10 octets

MCC/MNC: The first 3 octets are MCC, and the last 3 octets are MNC. An unassigned/invalid MCC/MNC is set to all zeros.

## 5.2 DHCP Options

Upon receiving the DHCPINFORM that contains the Vendor Class Identifier option indicating 3GPP2-specific, the DHCP server shall send the DHCPACK that contains the Vendor-Specific Information option for MCC/MNC.

**Table 3 DHCP Vendor Class Identifier option**

0	8	16	24
Code (60)	Length	Enterprise Number	
Enterprise Number			

Code: 60

Length: 6

Enterprise Number: 5535

**Table 4 DHCP Vendor-Specific Information option**

0	8	16	24
Code (43)	Length 1	Enterprise Number	
		Option Code (4)	
Length 2	MCC/MNC		
MCC/MNC			

Code: 43

Length 1: 16 octets

Enterprise Number: 5535

Option Code: 4 (for MCC/MNC)

Length 2: 10 octets

MCC/MNC: The first 3 octets are MCC, and the last 3 octets are MNC. An unassigned/invalid MCC/MNC is set to all zeros.