



INTERNATIONAL TELECOMMUNICATION UNION

**TELECOMMUNICATION
STANDARDIZATION SECTOR**

STUDY PERIOD 2022-2024

SG11-TD179/GEN

STUDY GROUP 11

Original: English

Question(s): 3/11

Geneva, 6-15 July 2022

TD

Source: Editors

Title: Output – draft new Recommendation Q.Sig_Req_ETS_IMS_roaming “Signalling requirements for emergency telecommunication service in IMS roaming environment” (Geneva, 6-15 July 2022)

Contact: Xiaojie ZHU (Judy)
China Telecom
P.R.China
Tel: +8620 38639248
E-mail: zhuxiaojie@chinatelecom.cn

Contact: Jianyin Zhang
China Mobile
P.R.China
Tel: +86 13910022506
E-mail: zhangjianyin@chinamobile.com

Contact: Zhan Liu
China Telecom
P.R.China
Tel: +8620 38639248
E-mail: liuz22@chinatelecom.cn

Keywords: Signalling requirement; ETS; IMS; Roaming

Abstract: This document contains the updated output of Q.Sig_Req_ETS_IMS_roaming “Signalling requirements for emergency telecommunication service in IMS roaming environment”, which was prepared as output of Q3/11 meeting (Geneva, 6-15 July 2022). It is based on SG11-TD1819/GEN and contains revisions based on the received contribution and outcomes of discussion.

No.	Title	Source	Discussion
SG11-C42	Proposed use cases for draft Rec. ITU-T Q.Sig_Req_ETS_IMS_roaming	China Telecom	Agreed with modifications
SG11-C62	Proposed modifications to section 9 and 10 of draft Rec. ITU-T Q.Sig_Req_ETS_IMS_roaming	China Telecom	Agreed with modifications

Table of Contents

1.	Scope.....	3
2.	References.....	3
3.	Definitions	3
4.	Abbreviations and acronyms	4
5.	Conventions	4
6.	Signalling architecture of ETS in IMS roaming environment.....	4
7.	Functional requirements of ETS in IMS roaming environment	5
7.1.	Functional requirements for IMS.....	5
7.2.	Functional requirements for EPC	6
8.	Signalling requirements of ETS in IMS roaming environment.....	6
9.	Signalling procedures of ETS in IMS roaming environment	7
9.1.	Signalling procedure for inbound UE with retrieval MSISDN from PCRF.....	8
9.2	Signalling procedure for inbound UE without retrieval MSISDN from PCRF.....	10
10.	Security considerations	11
	Appendix I Use cases of ETS in IMS roaming over LTE	12
	I.1 UE supports PS emergency call	12
	I.1.1 VPLMN supports PS emergency call with GIBA.....	12
	I.1.2 VPLMN does not support GIBA but support anonymous emergency call.....	13
	I.2 UE does not support PS emergency call	13
	Bibliography.....	15

Draft new Recommendation ITU-T Q.Sig_Req_ETS_IMS_roaming

Signalling requirements for emergency telecommunication service in IMS roaming environment

1. Scope

This draft Recommendation addresses the signalling architecture, interfaces and functional description, signalling requirements, signalling procedures and security consideration of Emergency Telecommunication Service (ETS) in Home Routing architecture of IMS roaming over LTE.

Note: the term LTE refers to both LTE and LTE-Advanced in this draft recommendation.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- | | |
|-------------------|---|
| [ITU-T Y.2701] | Recommendation ITU-T Y.2701 (2007), Security requirements for NGN release 1 |
| [ETSI TS 123 167] | ETSI TS 123 167 V15.4.0 (2018-12), IP Multimedia Subsystem (IMS) emergency sessions |
| [ETSI TS 123 228] | ETSI TS 123 228 V14.6.0 (2018-01), <i>IP Multimedia Subsystem (IMS)</i> . |
| [ETSI TS 124 229] | ETSI TS 124 229 V16.0.0 (2018-12), <i>IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)</i> |
| [ETSI TS 123 401] | ETSI TS 123 401 V14.10.0 (2018-12), <i>General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access</i> . |
| [ETSI TS 129 214] | ETSI TS 129 214 V15.9.0 (2020-11), <i>Policy and charging control over Rx reference point</i> |
| [ETSI TS 129 228] | ETSI TS 129 228 V15.3.0(2019-10), <i>IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents</i> . |

3. Definitions

.

3.1 Terms defined elsewhere

TBD

3.2 Terms defined in this Recommendation

TBD

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS	Application Server
BGCF	Breakout Gateway Control Function
CS	Circuit Switched
CSCF	Call Session Control Function
EPC	Evolved Packet Core
EPS	Evolved Packet System
GIBA	GPRS IMS Bundled Authentication
GPRS	General Packet Relay System
HSS	Home Subscriber Server
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating Call Session Control Function
IMS	IP Multimedia Subsystem
LTE	Long Term Evolution
MGCF	Media Gateway Control Function
NAS	Non-Access Stratum
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDN	Packet Data Network
PGW	Packet Gateway
PS	Packet Switched
PSAP	Public Safety Answering Point
S8HR	S8 Home Routing
S-CSCF	Serving Call Session Control Function
SIB	System Information Block
SIP	Session Initiation Protocol
UE	User Equipment
VoLTE	Voice over LTE

5. Conventions

TBD

6. Signalling architecture of ETS in IMS roaming environment

To support the emergency call initiated by inbound UEs attached to the VPLMN, the ETS in IMS roaming architecture using S8HR is depicted in Figure 6-1. The visiting VoLTE UE attaches to the EPS of VPLMN and receives the emergency number list of the visiting network. The VPLMN can send an emergency number list via the Emergency Number List and Extended Emergency Number List in the NAS Attach Accept. When the UE identifies an emergency call request, and PS emergency call is supported an emergency PDN connection will be established and an IMS emergency registration would be initiated over the emergency PDN. The P-CSCF of the VPLMN terminates the IMS emergency registration. The initial emergency registration is rejected with an indicator whether the network supports GIBA or anonymous IMS emergency call. In the former case, a second successful IMS registration occurs using GIBA followed by the IMS emergency call attempt. In the latter case, the UE initiates an IMS emergency call without registration (an anonymous IMS emergency call).

The VPLMN forwards the emergency call request to the PSAP/Emergency centre and establish the media connection between the UE and the PSAP/Emergency centre.

If PS emergency is not supported by the VPLMN, then CS-fallback occurs and the emergency call is attempted in the CS domain. The domain selection rules are described in annex H of ETSI TS 123 167.

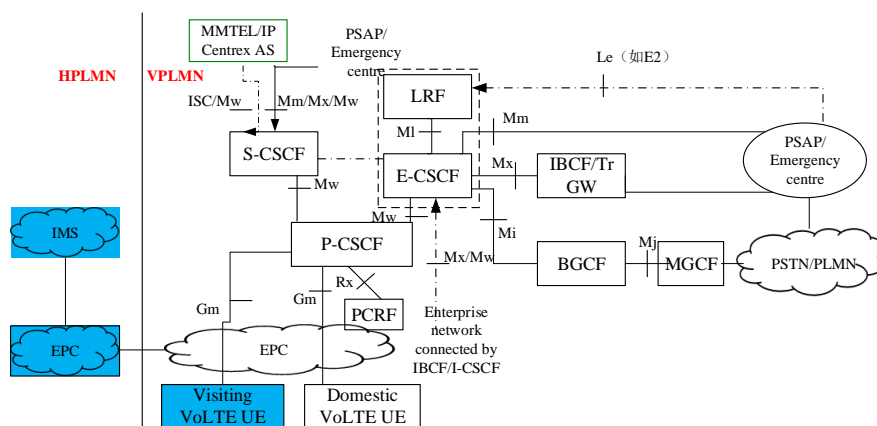


Figure 6-1 ETS in IMS roaming architecture using S8HR

Editor's note: contributions are invited to clarify where the emergency communication types mentioned in the texts are defined.

Editor's note: the figure 6-1 needs to be improved to match the S8HR roaming architecture. Contributions are invited.

7. Functional requirements of ETS in IMS roaming environment

[Contributor's note: this clause describes the details of the functional requirements for IMS and EPC network elements.]

7.1. Functional requirements for IMS

This clause presents the functional requirements for the IMS domains of the HPLMN and VPLMN in addition to the functionality described in [ETSI TS 123 228] and [ETSI TS 123.167].

1. P-CSCF of HPLMN

To support the emergency call initiated by inbound UEs attached to the VPLMN which PS could not support the emergency call and send the emergency number list to inbound UEs during the PS attach procedure, the P-CSCF of HPLMN which connects to the outbound UEs should support the

configuration of the lists of local emergency numbers for various visited PLMNs in accordance with the roaming agreements.

When receives an emergency call request initiated by a normal IMS session setup request, P-CSCF should identify non-UE-detectable emergency call and instruct UE to initiate an emergency call in the PLMN. This is done by sending back a 380 response to the SIP INVITE with an XML body of "Alternative Service-Emergency". This response informs the UE that this is an emergency call. The UE then behaves as for "UE detected emergency call" and performs domain selection as per ETSI TS 123.167 annex H.

It is possible for HPLMN service codes to clash with VPLMN emergency codes. These can be handled in one of two ways:

- 1) VPLMN informs the UE of the local code in the NAS signalling at network attach, in which case the local code would result in "UE detected" emergency call and the HPLMN service code is overridden,
- 2) VPLMN does not inform the UE of the local code in which case the call would be routed to HPLMN and terminated as a HPLMN service call.

2. P-CSCF of VPLMN

P-CSCF of VPLMN should support different emergency registration procedures for the domestic UE and inbound UE. For domestic UE, the emergency registration request should be forwarded to I-CSCF and followed the normal registration procedure with authentication request to the UE.

For inbound UE, the P-CSCF rejects the initial emergency registration request and informs the UE to perform a second registration using GIBA (GPRS-IMS bundled authentication) or else to use the Anonymous IMS Emergency Call procedure as described in in [ETSI TS 124 229].

The P-CSCF shall be able to retrieve the UE/user's IMSI, IMEI and MSISDN (if available) from the PCRF and may verify the IMSI/IMEI provided in the SIP REGISTER message against the IMSI/IMEI provided by the PCRF.

7.2. Functional requirements for EPC

This clause presents the functional requirements for the EPC of the HPLMN and VPLMN in addition to the functional requirements defined in [ETSI TS 123 401].

- PCRF shall be able to provide the IMSI, the ME Identity, and MSISDN over the Rx interface reference point to the P-CSCF. The Rx interface is described in ETSI TS 129 214.
-

8. Signalling requirements of ETS in IMS roaming environment

[Contributor's note: this clause addresses the signalling requirements of ETS in IMS roaming environment.]

In the IMS roaming environment, emergency calls must be terminated in the VPLMN. The inbound UE is aware whether CS or/and PS emergency call is available in the VPLMN in order to perform domain selection. The VPLMN can tell the UE about local emergency numbers via NAS signalling. In addition, the HPLMN is also aware of VPLMN local emergency numbers. Therefore, a "non-UE detected" emergency call can be presented to the HPLMN IMS and be rejected with a 380 (Use

alternative service – emergency) which results in the UE behaving as for a “UE detected” emergency call and re-attempting the emergency call in the VPLMN.

To initiate a PS emergency call in the VPLMN, the UE initially performs an emergency attach followed by an emergency IMS registration. For S8HR based VoLTE roaming, there is no IMS interface between the HPLMN and VPLMN to enable authentication of the UE. Therefore, the initial IMS emergency registration is rejected with either a SIP 403 or 420 response. The 420 response indicates that GIBA is supported and a second (successful) IMS registration occurs using GIBA followed by the emergency call attempt. The 403 response indicates that Anonymous IMS Emergency Call is supported by the VPLMN. In this case, the UE initiates the emergency call attempt without a second IMS registration.

It should be noted that for Anonymous IMS Emergency Call, the P-CSCF can retrieve information from the PCRF (via the Rx interface) to determine the identity of the user. Otherwise, the P-CSCF can also allocate a (non-e164 based) identity to enable callback. This is also a network option in the VPLMN.

It is a VPLMN option whether GIBA and/or Anonymous IMS Emergency call is supported.

9. Signalling procedures of ETS in IMS roaming environment

[Contributor’s note: This clause describes the signalling procedures of ETS in IMS roaming environment.]

9.1. Signalling procedure for inbound UE with retrieval MSISDN from PCRF

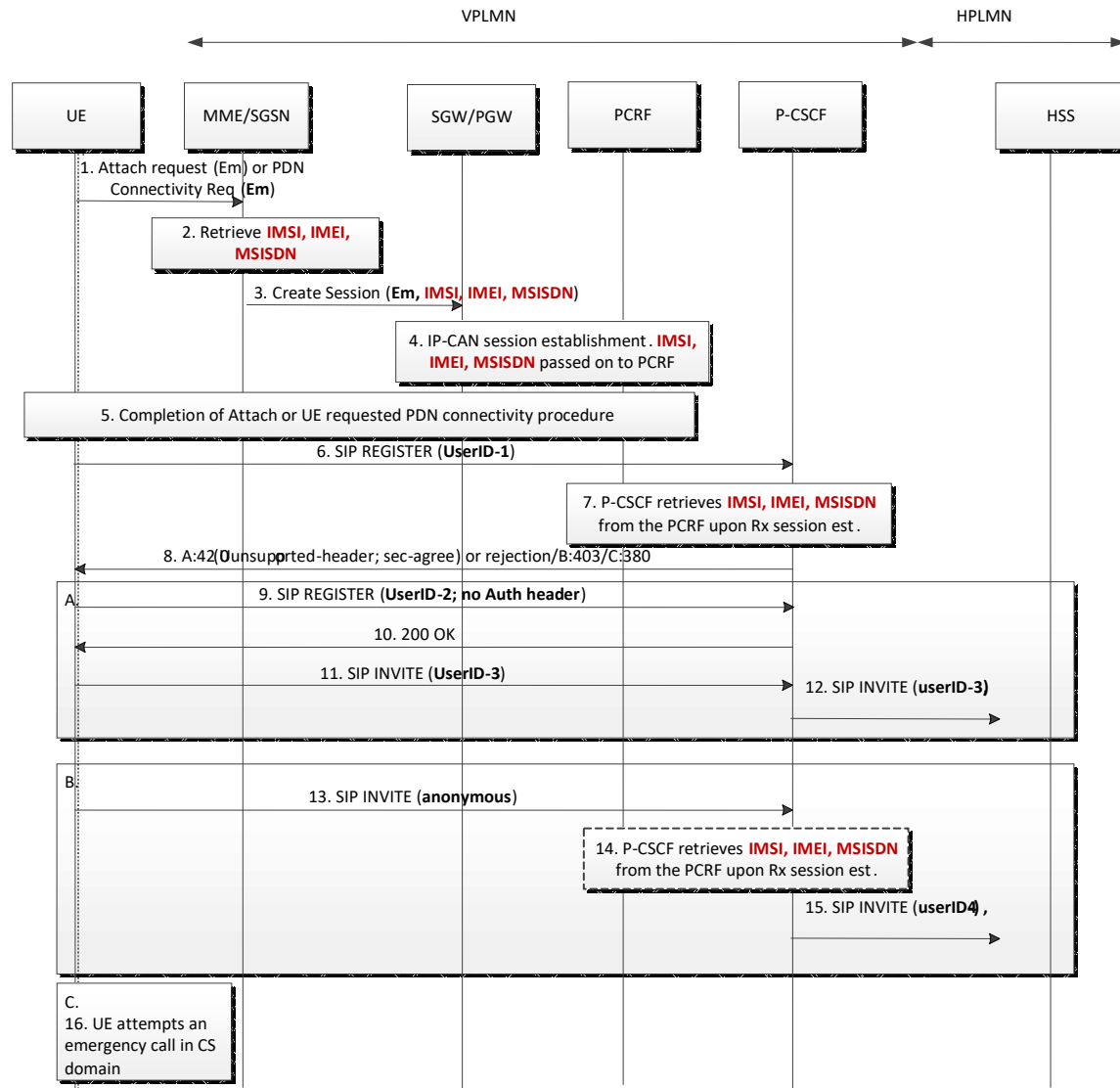


Figure 2: IMS Emergency Session Establishment in deployments without IMS roaming interface between VPLMN and HPLMN

Note: the procedures contained in Figure 2 complies with ETSI TS 123 167 except for the steps 12 and 15.

1. UE initiates an Attach or PDN connectivity request for IMS emergency services.
2. IMSI and IMEI are retrieved from the UE. The MSISDN (if available) is retrieved from the HSS.
3. MME/SGSN sends a Create Session Request towards the PGW including the IMSI, the IMEI and the MSISDN (if available) as specified in ETSI TS 123 401.
4. PGW establishes an IP-CAN session with the PCRF as described in ETSI TS 123 401 and ETSI TS 123 203. The IP-CAN session is identified with UE's IPv4 address or IPv6 prefix associated with the PDN connection for IMS emergency services. The IMSI, the IMEI and the MSISDN (if available) are passed to the PCRF as part of the IP-CAN session establishment.
5. UE completes the Attach or UE requested PDN connection procedure.

Steps 6-12 apply in case the UE performs IMS Emergency Registration, e.g. the UE aware that it has sufficient IMS authentication material.

6. UE initiates IMS emergency registration by sending a SIP REGISTER (UserID-1) message. The UserID-1 parameter is an IMPI and optionally an IMPU.

7a. Upon reception of the SIP REGISTER message the P-CSCF determines that there is no IMS NNI to the user's HPLMN. The P-CSCF requests the PCRF for EPS-level identities (e.g. IMSI, IMEI, MSISDN) in the Rx session establishment request.

7b. The PCRF performs session binding based on the UE's IP address/prefix (as defined in ETSI TS 123 203) and provides one or more EPS-level identities and the MSISDN (if available) to the P-CSCF.

10. Based on operator configuration, P-CSCF applies one of the three approaches below.

A. if the network supports the GIBA procedure over Gm as defined in ETSI TS 124.229 , the P-CSCF responds with a 420 response with sec-agree value listed in the unsupported header field.

B. if the network does not support the GIBA procedure, it rejects the IMS registration request with SIP 403 (Forbidden) as defined in ETSI TS 124.229.

Note: if the network supports anonymous IMS emergency sessions, P-CSCF may add an indication whether it supports anonymous IMS emergency sessions to the 403 or 420 response.

C. if the network does not support the GIBA procedure and anonymous IMS emergency sessions, P-CSCF responds with a 380 (alternative service) response denoting an emergency call.. UE attempts an emergency call in the CS domain.

Steps 9-12 (as shown in Box A of Figure 2) apply in case the P-CSCF has responded with a 420 response in step 8 and if the UE supports GIBA procedure as part of emergency IMS registration.

9. UE according to ETSI TS 124.229, performs a new initial registration by sending a SIP REGISTER (UserID-2, IMEI) message and without inclusion of the Authorization header field. UserID-2 is a public user identity derived from IMSI. P-CSCF may verify the IMSI/IMEI provided by the PCRF in step 7b against the IMSI/IMEI derived from the public user identity provided by the UE, prior to accepting the SIP REGISTER message.

10. P-CSCF accepts the registration with 200 OK and provides a tel-URI based on the MSISDN (if available) received from PCRF in step 7b to the UE. From the UE point of view, the procedure is the same as specified for GIBA (GPRS-IMS bundled authentication) procedures in ETSI TS 124.229.

11. UE then attempts an IMS emergency session by sending a SIP INVITE (UserID-3) message. UserID-3 is set to UE's public identity (i.e. MSISDN as Tel-URI received in step 10).

12. The P-CSCF verifies whether the UserID-3 indicated in the SIP INVITE message complies with the tel-URI that was provided to the UE. If compliant, P-CSCF forwards the SIP INVITE towards the PSAP including a P-Asserted-Identity header field in the form of TEL-URI derived from the MSISDN received in step 7. The procedure stops here.

Steps 13-15 (as shown in Box B of Figure 2) apply if the UE attempts anonymous IMS emergency session, e.g. the P-CSCF has responded in step 8 with a 403 (Forbidden) response, or the P-CSCF has responded in step 8 with 420 response and the UE does not support GIBA as part of emergency IMS registration, or if the UE skipped IMS emergency registration:

13. The UE may attempt an unauthenticated IMS emergency session including an "anonymous user" parameter in the SIP INVITE message.

14. Upon reception of the SIP INVITE the P-CSCF either internally retrieves the one or more EPS-level identities and the MSISDN (if available) that were received in step 7b, or performs step 7 again.
15. The P-CSCF forwards the SIP INVITE (UserID-4) towards the PSAP. UserID-4 is derived from one of the EPS-level identities received in step 7b. A P-Asserted-Identity header field is included in the form of TEL-URI derived from the MSISDN received in step 7b. The procedure stops here.

Step 16 (as shown in Box C of Figure 2) applies if the UE attempts an emergency call in the CS domain:

16. Subsequent to the IMS registration failure in step 8 or subsequent to an anonymous SIP INVITE attempt the UE may attempt an emergency call in the CS domain.

9.2 Signalling procedure for inbound UE without retrieval MSISDN from PCRF

In case the P-CSCF cannot retrieve MSISDN from the PCRF (via the Rx interface) to determine the identity of the user (for example, HSS could not provide the MSISDN to VPLMN for a user without international roaming permission), P-CSCF should allocate a temporary user identity to the inbound UE to enable callback. The temporary user identity should be a URI of format “user@domain”. The user part of the URI is a unique identity of the inbound UE within the P-CSCF, and the domain part of the URI is a unique identity of the P-CSCF which enables the correct P-CSCF to be found in the visited PLMN, such as [user1234@p-cscf2.mno.domain](#). The P-CSCF should record the mapping of the temporary user identity and IP address of the inbound UE to enable the correct UE to be found on callback. The effective time of the mapping between temporary user identity and IP address of the inbound UE should be configurable in accordance with the policy of the visited PLMN.

The signalling procedure for inbound UE without retrieval MSISDN from PCRF is shown in Figure 3.

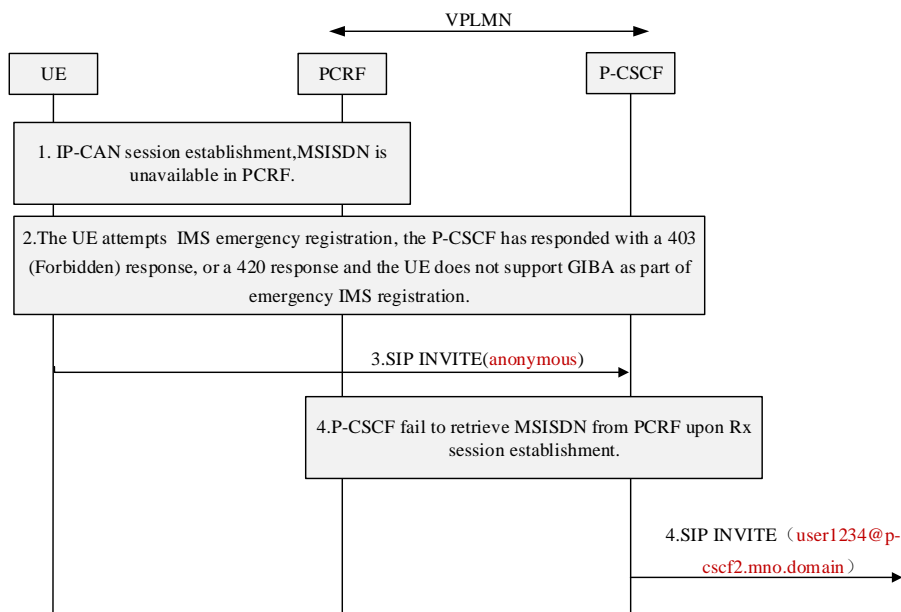


Figure 3: IMS Emergency Session Establishment for inbound UE in case MSISDN is unavailable in PCRF

1. UE initiates an Attach or PDN connectivity request for IMS emergency services. The MSISDN of the inbound UE could not be retrieved from the HSS and is unavailable in PCRF.

2. The UE attempts anonymous IMS emergency session, the P-CSCF has responded with a 403 (Forbidden) response, or the P-CSCF has responded with 420 response and the UE does not support GIBA as part of emergency IMS registration.
3. The UE attempts anonymous IMS emergency session.
4. Upon reception of the SIP INVITE, the P-CSCF attempts to retrieve the one or more identities either internally or from PCRF. The P-CSCF fails to retrieve the MSISDN of the UE and allocates a temporary user identity, such as [user1234@p-cscf2.mno.domain](#), to the inbound UE to enable callback. The temporary user identity is inserted in the P-Asserted-Identity header field of the SIP INVITE. Then the SIP INVITE is forwarded to the subsequent network elements.

Note: the P-CSCF records the mapping of the temporary user identity and the IP address of the UE to enable the correct UE to be found on callback. The P-CSCF could set the effective time period of the recorded mapping information in accordance with the regulatory policy. Subsequently, when a callback request is received, the P-CSCF could forward the callback request to the corresponding UE according to the recorded mapping information.

10. Security considerations

[Contributor's note: This chapter provides the security mechanism used for the ETS in IMS roaming environment.]

The security requirements for ETS in home routing architecture of IMS roaming over LTE should be aligned with the requirements defined in [ITU-T Y.2701]. No specific considerations of security mechanisms are required in this Recommendation.

Appendix I

Use cases of ETS in IMS roaming over LTE

(This appendix doesn't form an integral part of this Recommendation)

I.1 UE supports PS emergency call

When the UE initially attaches to the VPLMN, the VPLMN can tell the UE about local emergency numbers via NAS signalling with the Emergency Numbers List and Extended Emergency Numbers List IEs. The VPLMN also broadcasts support of IMS Emergency Call in the System Information Block Type 1 (SIB-1). The UE is aware via the SIB-1 and NAS whether PS emergency is available.

To initiate a PS emergency call in the VPLMN, the UE initially performs an emergency attach followed by an emergency IMS registration. For S8HR based VoLTE roaming, there is no IMS interface between the HPLMN and VPLMN to enable authentication of the UE. Therefore, the initial IMS emergency registration is rejected with either a SIP 403, 420, or 380 response.

I.1.1 VPLMN supports PS emergency call with GIBA

1. UE supports GIBA as part of emergency IMS registration

In case both of the VPLMN and UE support GIBA as part of emergency IMS registration, a 420 response indicates that GIBA is supported and a second (successful) IMS registration occurs using GIBA followed by the emergency call attempt.

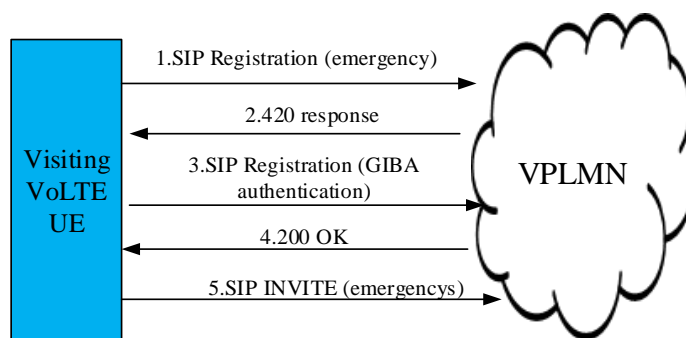


Figure I.1: UE and VPLMN both support PS emergency call with GIBA

2. UE does not support GIBA as part of emergency IMS registration

Since UE does not support GIBA as part of emergency IMS registration, it could not send a second IMS registration to VPLMN when it receives a 420 response indicates that GIBA is supported in VPLMN.

If the 420 response indicates that anonymous emergency call is supported in VPLMN, the UE should initiate an IMS anonymous emergency call of VPLMN, as shown in Figure I.2. Otherwise the UE initiate an emergency call in CS domain of VPLMN, as shown in Figure I.3.

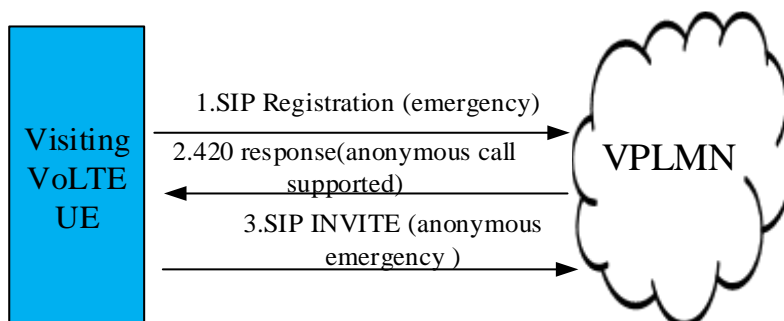


Figure I.2: UE does not support GIBA, VPLMN support GIBA and anonymous emergency call

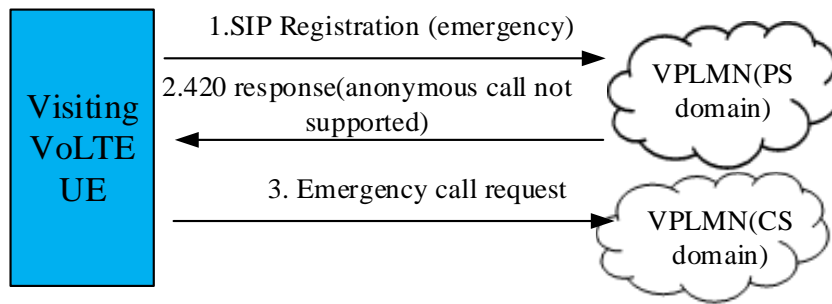


Figure I.3: UE does not support GIBA, VPLMN supports GIBA but does not support anonymous emergency call

I.1.2 VPLMN does not support GIBA but support anonymous emergency call

VPLMN responds to the emergency IMS registration with a 403 response indicating that anonymous emergency call is supported in VPLMN. The UE should initiate an IMS anonymous emergency call in VPLMN, as shown in Figure I.4. Otherwise the UE initiate an emergency call in CS domain of VPLMN, as shown in Figure I.5.

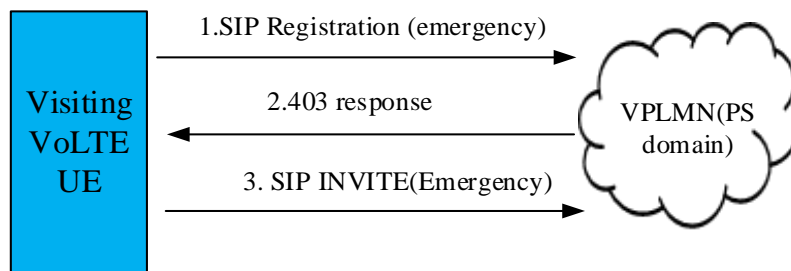


Figure I.4: UE and VPLMN both support anonymous emergency call

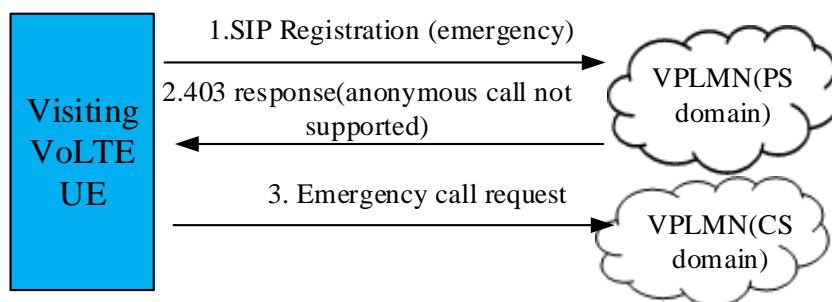


Figure I.5: UE and VPLMN both support anonymous emergency call

I.2 UE does not support PS emergency call

The VPLMN cannot tell the UE about local emergency numbers via NAS signalling. The HPLMN is aware of VPLMN local emergency numbers. The UE initiated a normal (i.e. non-emergency) session to the HPLMN. Therefore, a “non-UE detected” emergency call can be presented to the HPLMN IMS and be rejected with a 380 (Use alternative service – emergency) which results in the

UE behaving as for a “UE detected” emergency call and re-attempting the emergency call in the CS domain of VPLMN, as shown in Figure I.6.

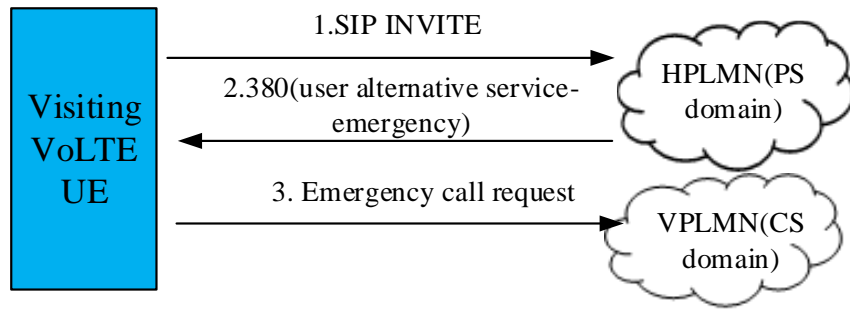


Figure I.6: UE does not support PS emergency call

Bibliography

[b-GSMA PRD IR.65]
[b-3GPP TR 23.749]

IMS Roaming, Interconnection and Interworking Guidelines
Study on S8 Home Routing Architecture for VoLTE
