ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Q.3647 (02/2023)

SERIES Q: Switching and signalling, and associated measurements and tests

Signalling requirements and protocols for the NGN – VoLTE/ViLTE network signalling

Signalling requirements for emergency services in an Internet protocol multimedia subsystem roaming environment

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3616
Service and session control protocols – supplementary services based on SIP-IMS	Q.3617–Q.3639
VoLTE/ViLTE network signalling	**Q.3640–Q.3655**
NGN applications	Q.3700–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS	Q.4100–Q.4139
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.3647

Signalling requirements for emergency services in an Internet protocol multimedia subsystem roaming environment

Summary

Recommendation ITU-T Q.3647 addresses signalling requirements for emergency services in an Internet protocol multimedia subsystem (IMS) roaming environment. Recommendation ITU-T Q.3647 specifies the signalling architecture, interfaces and functional description, signalling requirements, signalling procedures and security consideration for emergency services in the home routing architecture of IMS roaming over long-term evolution (LTE) and LTE-advanced.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Q.3647	2023-02-13	11	11.1002/1000/15254

Keywords

Emergency service, IMS, roaming.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.3647

Signalling requirements for emergency services in an Internet protocol multimedia subsystem roaming environment

1 Scope

This Recommendation addresses the signalling architecture, interfaces and functional description, signalling requirements, signalling procedures and security consideration of emergency services in the home routing architecture for Internet protocol multimedia subsystem (IMS) roaming over long-term evolution (LTE).

NOTE – In this Recommendation, the term LTE includes both LTE and LTE-advanced.

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]	Technical Specification ETSI TS 123 167 V 14.6.0 (2018), *IP multimedia subsystem (IMS) emergency sessions*.
[ETSI TS 123 203]	Technical Specification ETSI TS 123 203 V14.6.0 (2018*), Policy and charging control architecture*.
[ETSI TS 123 228]	Technical Specification ETSI TS 123 228 V14.7.0 (2022), *IP multimedia subsystem (IMS); stage 2*.
[ETSI TS 123 401]	Technical Specification ETSI TS 123 401 V14.11.0 (2020), *General packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRAN) access*.
[ETSI TS 124 229]	Technical Specification ETSI TS 124 229 V14.16.0 (2021), *IP multimedia call control protocol based on session initiation protocol (SIP) and session description protocol (SDP); Stage 3*.
[ETSI TS 129 214]	Technical Specification ETSI TS 129 214 V14.9.0 (2019), *Policy and charging control over Rx reference point*.

3 Definitions

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BGCF	Breakout Gateway Control Function
CS	Circuit Switched

EPC	Evolved Packet Core
EPS	Evolved Packet System
GIBA	General packet relay system Internet protocol multimedia subsystem Bundled Authentication
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating Call Session Control Function
IMS	Internet protocol Multimedia Subsystem
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP-CAN	Internet Protocol-Connectivity Access Network
ISDN	International Services Digital Network
LTE	Long-Term Evolution
MGCF	Media Gateway Control Function
MSISDN	Mobile Subscriber ISDN Number
NAS	Non-Access Stratum
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDN	Packet Data Network
PGW	Packet data network Gateway
PLMN	Public Land Mobile Network
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
SGW	Serving Gateway
UE	User Equipment
VoLTE	Voice over Long-Term Evolution
VPLMN	Visited Public Land Mobile Network

5 Conventions

None.

6 Signalling architecture for emergency calling in an IMS roaming environment

Roaming architecture with home routed traffic over LTE is specified in [ETSI TS 123 401]. In that architecture, the inter-public land mobile network (inter-PLMN) reference point S8 provides user and control plane between the serving gateway (SGW) in the visited public land mobile network (VPLMN) and the packet data network gateway (PGW) in the home public land mobile network (HPLMN). Therefore, this roaming architecture is referred to as S8 home routing (S8HR). Roaming flows using S8HR do not require IMS interconnection between HPLMN and VPLMN. It can be seen as a voice over IMS extension of evolved packet core (EPC) data roaming. This arrangement is suitable for operators that wish to have IMS services for roaming without deploying interconnection.

To support emergency calling initiated by inbound user equipment (UE) attached to the VPLMN, the situation within the IMS roaming architecture using S8HR is depicted in Figure 1. The visiting voice over long-term evolution (VoLTE) UE attaches to the evolved packet system (EPS) of the VPLMN and receives the emergency number list of the visiting network. The VPLMN can send an emergency number list via the existing list of emergency numbers or its extension in the non-access stratum (NAS) attach accept. When the UE identifies an emergency call request and its packet-switched (PS) handling is supported, a packet data network (PDN) connection is established, and IMS registration initiated over it. The proxy call session control function (P-CSCF) of the VPLMN terminates IMS emergency registration. The initial emergency registration is rejected with an indication of whether the network supports general packet relay system Internet protocol multimedia subsystem bundled authentication (GIBA) or anonymous IMS emergency calling. 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 a public safety answering point (PSAP) or emergency centre, to which a media connection is established with the UE.

If PS emergency calling is not supported by the VPLMN, then fallback in the circuit switched (CS) 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].

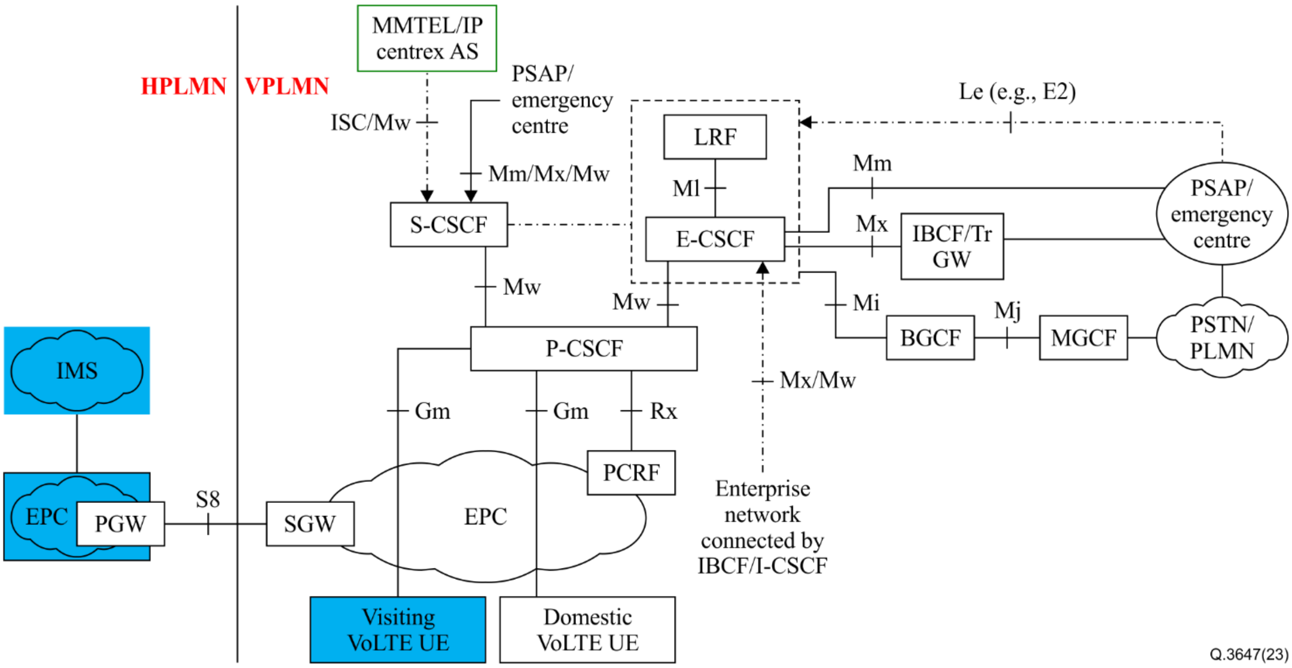


Figure 1 – Emergency call in IMS roaming architecture using S8HR

7 Functional requirements of emergency calling in an IMS roaming environment

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].

7.1.1 P-CSCF of HPLMN

To support emergency calling initiated by inbound UEs attached to the VPLMN, when the PS cannot support it and send the emergency number list to inbound UEs during the PS attach procedure, the P-CSCF of the HPLMN that connects to the outbound UEs should support the configuration of the lists of local emergency numbers for various VPLMNs in accordance with applicable roaming agreements and national regulatory rules.

On receipt of an emergency call request initiated by a normal IMS session setup request, P-CSCF should identify that the call is non-UE-detectable. The P-CSCF then instructs the UE to initiate an emergency call in the VPLMN. This is done by sending a 380 response to the session initiation protocol (SIP) INVITE with an extensible markup language body of "alternative service-emergency". This response informs the UE that this is an emergency call. The UE then behaves as if it had detected the emergency call and performs domain selection as per Annex H of [ETSI TS 123 167].

A clash in codes is possible for HPLMN services and VPLMN emergencies. A clash can be handled in one of two ways:

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

7.1.2 P-CSCF of VPLMN

A P-CSCF of a VPLMN should support different emergency registration procedures for domestic and inbound UE.

In the domestic case, the emergency registration request should be forwarded to the interrogating call session control function (I-CSCF) and the normal registration procedure followed with an authentication request to the UE.

For inbound UE, the P-CSCF rejects the initial emergency registration request and instructs the UE to perform a second registration using GIBA or else to use the anonymous IMS emergency call procedure as described in [ETSI TS 124 229].

The P-CSCF shall be able to retrieve the UE or user international mobile subscriber identity (IMSI), international mobile equipment identity (IMEI) and mobile subscriber international services digital number (MSISDN; if available) from the policy and charging rules function (PCRF). The P-CSCF may verify the IMSI or IMEI provided in the SIP REGISTER message against those provided by the PCRF.

7.2 Functional requirements for EPC

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

– PCRF shall be able to provide the IMSI, the IMEI and MSISDN over the Rx reference point to the P-CSCF. The Rx reference point is described in [ETSI TS 129 214].

8 Signalling requirements for emergency calling in an IMS roaming environment

In the IMS roaming environment, emergency calls must be terminated in the VPLMN. The inbound UE is aware of whether a CS or 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 IMS of the HPLMN and rejected with a 380 (use alternative service – emergency), which results in the UE behaving as though it had detected the emergency call and re-attempting it in the VPLMN.

To initiate a PS emergency call in the VPLMN, the UE first 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 calling 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 calling, the P-CSCF can retrieve information from the PCRF (via the Rx reference point) to determine the identity of the user. Otherwise, the P-CSCF can also allocate a (non-ITU-T E.164-based) identity to enable callback. This is also a network option in the VPLMN.

It is a VPLMN option whether GIBA or anonymous IMS Emergency call is supported.

9 Signalling procedures for emergency calling in an IMS roaming environment

9.1 Signalling procedure for inbound UE with retrieval MSISDN from PCRF

NOTE – The procedures contained in Figure 2 comply with [ETSI TS 123 167], except for steps 12 and 15.

1) UE initiates an attach or PDN connectivity request for IMS emergency services.

2) The IMSI and IMEI are retrieved from the UE. The MSISDN (if available) is retrieved from the home subscriber server (HSS).

3) The mobility management entity or serving general packet radio service support node 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) The PGW establishes an Internet protocol-connectivity access network (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 the IPv4 address or IPv6 prefix of the UE associated with the PDN connection for IMS emergency services. The IMSI, IMEI and MSISDN (if available) are passed to the PCRF as part of the establishment of the IP-CAN session.

5) UE completes the attach or requested PDN connection procedure.

Steps 6-12 apply if the UE performs IMS emergency registration, e.g., the UE is 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 a private user identity and optionally a public user identity.

7a) On receipt of the SIP REGISTER message, the P-CSCF determines that there is no IMS network to network interface 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 IP address or prefix of the UE (as specified in [ETSI TS 123 203]) and provides one or more EPS-level identities and the MSISDN (if available) to the P-CSCF.

8) Based on operator configuration, P-CSCF applies one of the following three approaches.

a) If the network supports the GIBA procedure over Gm as specified in [ETSI TS 124 229], the P-CSCF responds with a 420 response with the 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 specified in [ETSI TS 124 229].

NOTE – If the network supports anonymous IMS emergency sessions, the P-CSCF may add an indication of 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, the 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 if the P-CSCF has reacted with a 420 response in step 8 and if the UE supports the 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 the IMSI. The P-CSCF may verify the IMSI or IMEI provided by the PCRF in step 7b against the IMSI or IMEI derived from the public user identity provided by the UE, prior to accepting the SIP REGISTER message.

10) The P-CSCF accepts the registration with 200 OK and provides a tel uniform resource identifier (URI) based on the MSISDN (if available) received from the PCRF in step 7b to the UE. From the UE point of view, the procedure is the same as specified for GIBA 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 the public identity of the UE (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, the P-CSCF forwards the SIP INVITE towards the PSAP including a P-asserted-identity header field in the form of a 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 an 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) On receipt 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 a 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) After either an IMS registration failure in step 8 or an anonymous SIP INVITE attempt, the UE may attempt an emergency call in the CS domain.

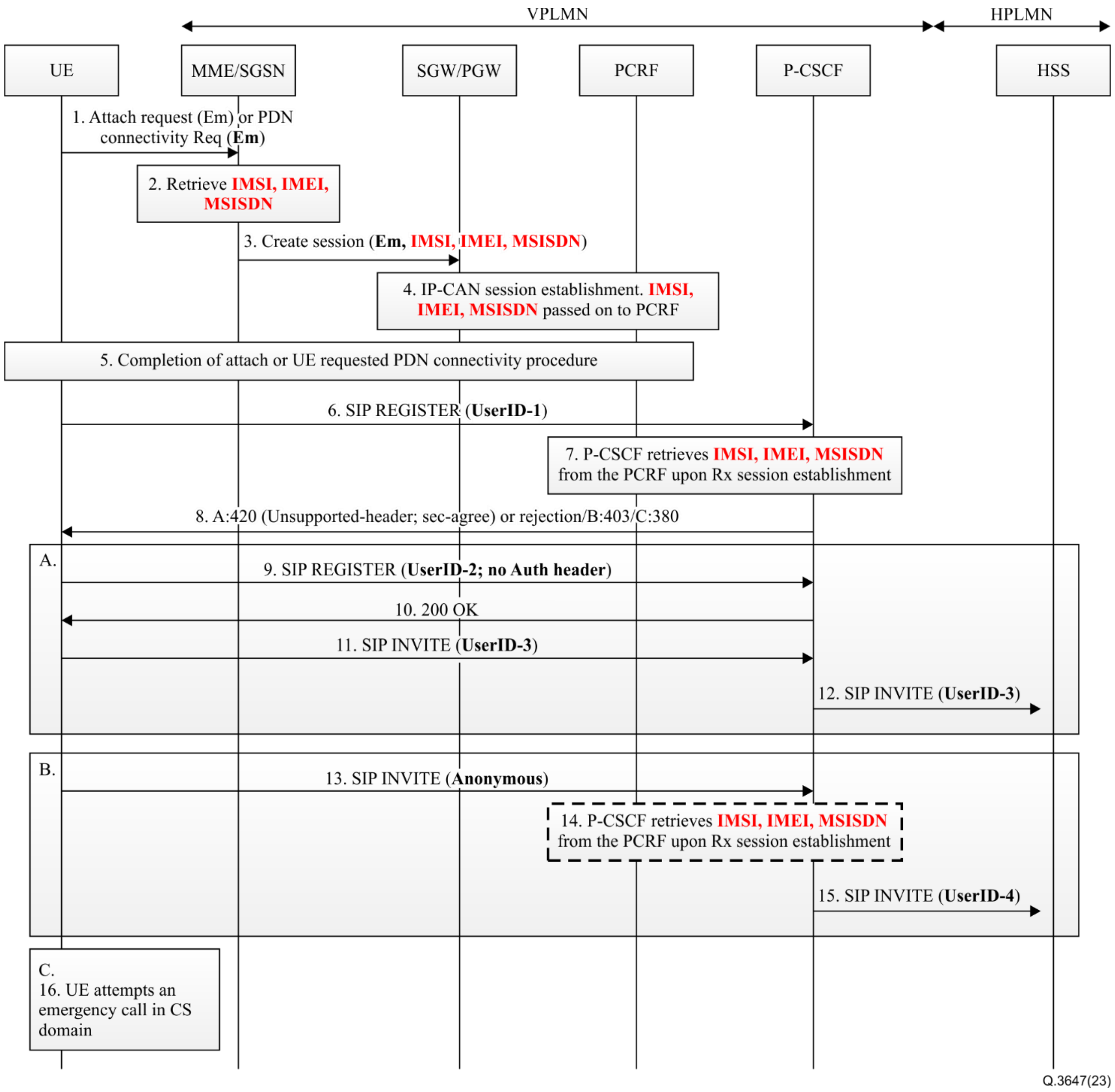
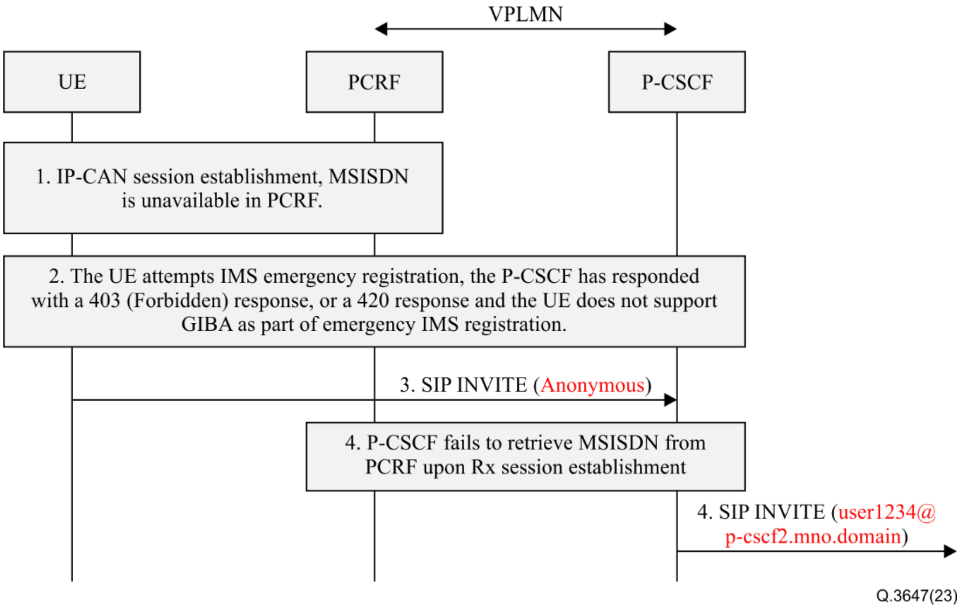

VPLMN
HPLMN
UE
MME/SGSN
SGW/PGW
PCRF
P-CSCF
HSS
1. Attach request (Em) or PDN connectivity Req (Em)
2. Retrieve IMSI, IMEI, MSISDN
3. Create session (Em, IMSI, IMEI, MSISDN)
4. IP-CAN session establishment. IMSI, IMEI, MSISDN passed on to PCRF
5. Completion of attach or UE requested PDN connectivity procedure
6. SIP REGISTER (UserID-1)
7. P-CSCF retrieves IMSI, IMEI, MSISDN from the PCRF upon Rx session establishment
8. A:420 (Unsupported-header; sec-agree) or rejection/B:403/C:380
A.
9. SIP REGISTER (UserID-2; no Auth header)
10. 200 OK
11. SIP INVITE (UserID-3)
12. SIP INVITE (UserID-3)
B.
13. SIP INVITE (Anonymous)
14. P-CSCF retrieves IMSI, IMEI, MSISDN from the PCRF upon Rx session establishment
15. SIP INVITE (UserID-4)
C.
16. UE attempts an emergency call in CS domain
Q.3647(23)

Figure 2 – IMS emergency session establishment in deployments without an IMS roaming interface between VPLMN and HPLMN

9.2 Signalling procedure for inbound UE without a retrieved MSISDN from the PCRF

If the P-CSCF cannot retrieve an MSISDN from the PCRF (via the Rx reference point) to determine the identity of the user (e.g., an HSS cannot provide the MSISDN to a VPLMN for a user without international roaming permission), the 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. The domain part of the URI is a unique identity of the P-CSCF that enables the correct P-CSCF to be found in the VPLMN, 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 VPLMN.

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



VPLMN
UE
PCRF
P-CSCF
1. IP-CAN session establishment, MSISDN is unavailable in PCRF.
2. The UE attempts IMS emergency registration, the P-CSCF has responded with a 403 (Forbidden) response, or a 420 response and the UE does not support GIBA as part of emergency IMS registration.
3. SIP INVITE (Anonymous)
4. P-CSCF fails to retrieve MSISDN from PCRF upon Rx session establishment
4. SIP INVITE (user1234@p-cscf2.mno.domain)
Q.3647(23)

Figure 3 – IMS emergency session establishment for inbound UE if a MSISDN is unavailable in the PCRF

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

2) The UE attempts an anonymous IMS emergency session, the P-CSCF has reacted with a 403 (Forbidden) response or the P-CSCF has reacted with 420 response and the UE does not support GIBA as part of emergency IMS registration.

3) The UE attempts an anonymous IMS emergency session.

4) On receipt 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 into 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 can 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 can forward the callback request to the corresponding UE according to the recorded mapping information.

10 Security considerations

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

Appendix I

Use cases of emergency calling in IMS roaming over LTE

(This appendix does not form an integral part of this Recommendation.)

I.1 UE supports emergency calling in a PS domain

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 calling 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 a SIP 403, 420 or 380 response.

I.1.1 VPLMN supports emergency calling with GIBA

1) UE supports GIBA as part of emergency IMS registration

If both 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. See Figure I.1.

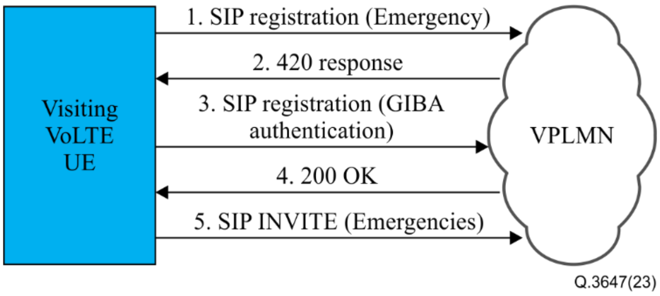

Visiting VoLTE UE
1. SIP registration (Emergency)
2. 420 response
3. SIP registration (GIBA authentication)
4. 200 OK
5. SIP INVITE (Emergencies)
VPLMN
Q.3647(23)

Figure I.1 – UE and VPLMN both support emergency calling with GIBA

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

As UE does not support GIBA as part of emergency IMS registration, it cannot send a second IMS registration to the VPLMN when it receives a 420 response indicating that GIBA is supported in the VPLMN. See Figure I.2.

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

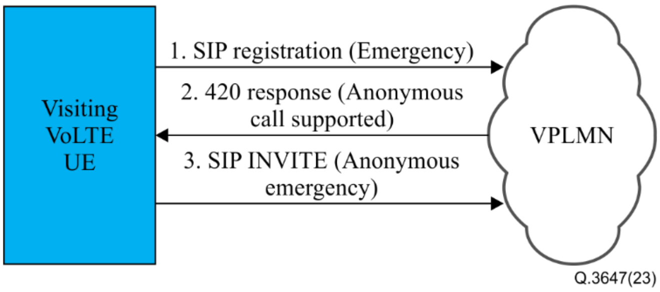

Visiting VoLTE UE
1. SIP registration (Emergency)
2. 420 response (Anonymous call supported)
3. SIP INVITE (Anonymous emergency)
VPLMN
Q.3647(23)

Figure I.2 – UE does not support GIBA, the VPLMN supports GIBA and anonymous emergency calling

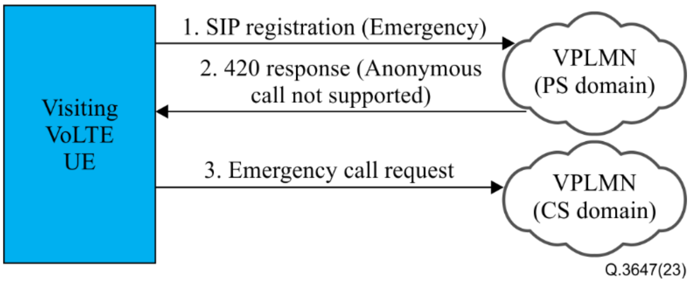

Visiting
VoLTE
UE
1. SIP registration (Emergency)
2. 420 response (Anonymous call not supported)
3. Emergency call request
VPLMN
(PS domain)
VPLMN
(CS domain)
Q.3647(23)

Figure I.3 – UE does not support GIBA, the VPLMN supports GIBA but not anonymous emergency calling

I.1.2 VPLMN does not support GIBA but supports anonymous emergency calling

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

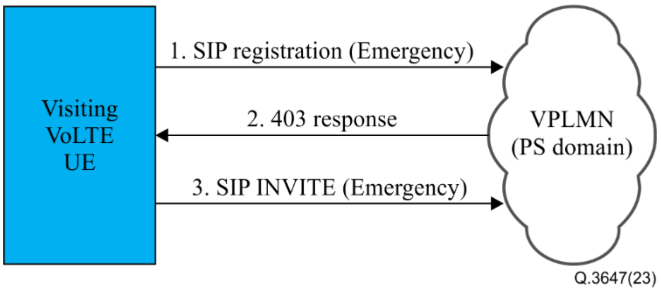


Figure I.4 – UE and VPLMN both support anonymous emergency calling

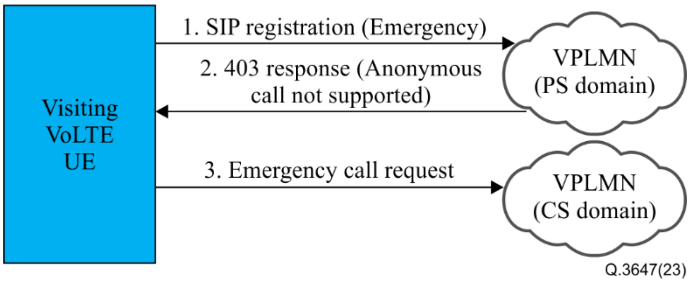

Visiting
VoLTE
UE
1. SIP registration (Emergency)
2. 403 response (Anonymous call not supported)
3. Emergency call request
VPLMN
(PS domain)
VPLMN
(CS domain)
Q.3647(23)

Figure I.5 – VPLMN does not support anonymous emergency calling in a PS domain

I.2 UE does not support emergency calling in a PS domain

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 the VPLMN, as shown in Figure I.6.

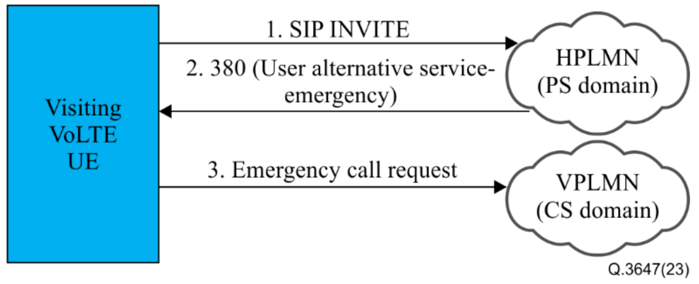


Figure I.6 – UE does not support emergency calling in a PS domain

Bibliography

[b-ITU-T E.164] Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems