3GPP TR 23.826 V9.0.0 (2009-03)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on Voice Call Continuity Support for Emergency Calls (Release 9)

Keywords
Voice Call, Circuit Switched, IMS, I-WLAN

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

During the course of Release 7, TS 23.206 [3] (Voice Call Continuity between CS and IMS) was developed to provides the capability to offer VCC (Voice Call Continuity) for a subscriber moving from a CS radio environment into a VoIP-capable IMS radio environment connected by an IP-CAN. However, for a variety of reasons, the TS specifically excludes the capability of allowing emergency calls to be subject to domain transfer. This TR documents alternatives for how to provide such voice call continuity between the CS Domain and IP-CANs for emergency calls.

1 Scope

This document contains the results of the feasibility study into the architectural requirements and alternatives for the support of active voice call continuity between Circuit Switched (CS) domain and the IP Multimedia Subsystem (IMS) for emergency calls. Considerations include overall requirements, architectural requirements, evaluation of potential architectural solutions and alternative architectures.

The Feasibility Study considers different solutions for offering voice call continuity for emergency calls when users move between the GSM/UMTS CS Domain and the IP Connectivity Access Network (e.g., WLAN interworking) with home IMS functionality. The objective is to identify an architectural solution that allows completely automatic connectivity to the correct PSAP (from the end-user point of view) as specified in TS 23.167 [4], and allow for the possibility of a domain transfer as specified in TS 23.206 [3]. The study will also identify configuration impacts upon existing networks in order to realize the desired functionality.

Existing solutions developed by the 3GPP (e.g. 3GPP system to Wireless Local Area Network Interworking (I-WLAN)) should be reused as much as possible.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 41.001: "GSM Release specifications".

[2] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking".

[3] 3GPP TS 23.206: "Voice Call Continuity between CS and IMS".

[4] 3GPP TS 23.167: "IMS Emergency Calls".

[5] 3GPP TS 23.226: "Global Text Telephony (GTT)".

[6] IETF RFC 4483: "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages".

[7] 3GPP TR 23.892: "IMS Centralized Services".

[8] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[9] IETF RFC 4119: "A Presence-based GEOPRIV Location Object Format".

[10] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) Centralized Services; Stage 2".

[11] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".

[12] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[13] 3GPP TS 23.237: " IP Multimedia Subsystem (IMS) Service Continuity; Stage 2".

[13] 3GPP TS 22.101: "Service aspects; Service principles".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [8] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [8].

E-RUA: A Remote User Agent (see TR 23.892 [7]) which resides in the serving IMS network and presents an Emergency Call established via the CS domain as an IMS Emergency Call to the E-CSCF.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [8] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [8].

VCC	Voice Call Continuity
I-WLAN	Interworking WLAN
WLAN	Wireless Local Area Network
ICCF	IMS CS Control Function
RUA	Remote User Agent
E-RUA	Emergency RUA
SLR	Subscriber Location Report

4 Overall Requirements

4.1 Service Characteristics

It is intended to develop capabilities that will allow the domain transfer of emergency calls in both the CS to IMS and IMS to CS directions. A minimal requirement is the support of VCC for emergency calls originated in the home PS domain. The following characteristics also need to be evaluated:

1) Emergency calls originated in the CS domain.

2) Roaming scenarios.

3) UEs that cannot be authenticated (e.g., UICC-less or with no roaming agreement).

5 Architectural Requirements and Considerations

5.1 Basic Assumptions

5.2 Architectural Requirements

1) The use of GTT device (e.g., TTY) for CS emergency call TS 23.226 [5] needs to be considered. The solution shall not require changes to the TTY device or the interface toward the terminal.

2) The solution shall be based on domain transfer procedures specified in Rel-07 VCC TS 23.206 [3].

3) The solution shall consider support of domain transfers of emergency Calls in areas where multiple visited IMS networks may be available to the user.

4) Support of the solution shall be optional in the UE and network. A UE or network that does not support the solution shall not be impacted.

5) The solution should be able to provide continuity of location support following domain transfer by providing the PSAP with an accurate initial and updated location estimate, according to applicable regional requirements and subject to the constraints of the PSAP interface.

6) The VCC procedure should be triggered only when both the UE and visited network (both the source and target access technology) support VCC for emergency calls.

7) VCC for emergency shall only be attempted for intra-operator transitions (where IMS and CS core operators are the same).

8) Emergency calls shall not be transitioned from CS to IMS.

9 UE shall not attempt to perform transfer of an emergency call if it is not certain the relevant capabilities are supported by the network.

10 Emergency calls are not automatically anchored for VCC unless they meet certain criteria that are to be defined.

5.3 Session Scenarios

5.3.1 Network preferences for the domain in which an emergency call is established

There are some basic forms of network preferences in existing IMS procedures e.g. it is possible to redirect a UE to use the CS domain for emergency calls and forbid the use of IMS for emergency calls. However, when these are considered in VCC these do not make too much sense since in order to perform VCC you must be allowed to establish emergency calls in both CS and IMS. However, a network operator may still have a preference as to which domain an emergency call ought to be on.

It is necessary to consider how these preferences relate to decision to transition from one access to the next. One key question is whether the network preferences take precedence over other typical reasons for transition e.g. degrading radio conditions. It is envisioned/assumed that device management is used to configure the different network preferences, but does this also extend to the other triggers

It is necessary to specify what are the likely trigger conditions for a transition, since this a safety critical service and needs to be error-free. The type of handover is different from normal 3GPP radio level handover since VCC is UE triggered, but still need to be equally detailed (e.g. signal strength hysteresis regimes).

5.3.2 Control of directionality of the transfer

Taking a comparison with mobility in a "normal" mode of operation, it is possible to apply access restrictions during mobility. This ought to be equally true in the emergency call scenario, although the reason behind such restrictions during mobility will be different.

In direct relation to the above topic of network preferences, there may be certain scenarios where a visited operator prefers to have emergency calls in CS (due to a CS only PSAP potentially) and as such the need for CS to IMS domain transfer is unclear.

One could also consider that CS "coverage" is much greater than for the non-3GPP access that is using IMS for call establishment. Therefore the justification for CS to IMS transfers again is not so obvious.

5.3.3 UE and network capabilities

The ability to perform the domain transfer on any call (irrespective of whether it is emergency or not) is driven by both network and UE capabilities. For non-emergency calls, typically no CS core network functionality is required since the solution is purely IMS driven. However in contrast for emergency calls, it is likely that CS core network functionality is required due to the need to carry information necessary for support of the UICC-less UE case across to IMS for anchoring during both call establishment and during domain transfer.

Blind attempts by UEs (especially those in a limited service state i.e. no UICC or invalid credentials) to perform VCC transfer of emergency calls should be avoided where the UE cannot or has not established the status of the support of network features required. This is due to the undefined/unpredictable behaviour if the network does not support VCC features that may lead to call transfer failures or treatment as a new call establishment.

5.3.4 Decision to anchor a new emergency call for subsequent VCC procedures

The anchoring of a call in IMS (at the E-SCC-AS) is vital to enable the transfer of the call from one domain to another. This concept does not change in VCC emergency. Anchoring of a CS call introduces call setup delay and increases network complexity (which ultimately leads to an increased probably of a failure). Therefore anchoring should not be considered to be applied for all calls but rather it should be avoided when the conditions allow for a call not to be anchored. The decision process must take into account all the points discussed in clauses 5.3.1, 5.3.2 and 5.3.3.

5.3.5 Determination of whether a call attempt is new or VCC domain transfer

In (dual-radio) VCC (emergency or not), the trigger point for domain transfer is firmly at the UE. This needs to coexist with a basic principle that an initial emergency call is always established by the UE. However, when discussing this, it becomes important for the network to differentiate between any incoming call attempt as related to either a new call initiation or a domain transfer.

For initial call establishment in CS, TS12 style signalling (i.e. Service Request = Emergency) will still be used as per TS 22.101 [13]. For domain transfers, the same signalling means may be used, however, this makes determination of the nature of the call very difficult without extensions.

If a call is incorrectly identified, there is a possibility that there is no continuity and a new session / call (at user level) is established and the caller required to re-provide any information to a new operator (at the PSAP end). Furthermore, because of unexpected call termination for the old operator, they may attempt a call back which would almost certainly fail. If these potential error cases aren't avoided, there may be potential service interaction issues between 2 TS 12 calls which had not been previously envisioned (even though there is a possibility for them to occur).

5.3.6 Inter-operator domain transfer

Due to the duty of care residing with the operator providing initial connectivity to the emergency services, it is generally not possible to transfer that duty from one operator to another. Also different operators may connect to different PSAPs which in turn may ultimate connect to a different set of physical operators. It is suggested that VCC for emergency calls are attempted only when the UE can identify that the source and target networks belong to the same network (operator). This ensures the continuity of an emergency call when performing domain transfers.

6 Architecture Alternatives

Editor's Note: This clause will describe and evaluate detailed reference architectures, including network elements, interfaces and reference points, suitable to provide VCC support for emergency calls.

6.1 VCC in the Visited Network - Alternative 1

6.1.1 Architectural Details

6.1.1.1 General

This clause presents an architectural alternative for enablement of Domain Transfers for Emergency calls between CS domain and IMS, which may be invoked multiple times in either direction while the user is engaged in an Emergency call. The solution is applicable to Emergency Calls made by authorized users.

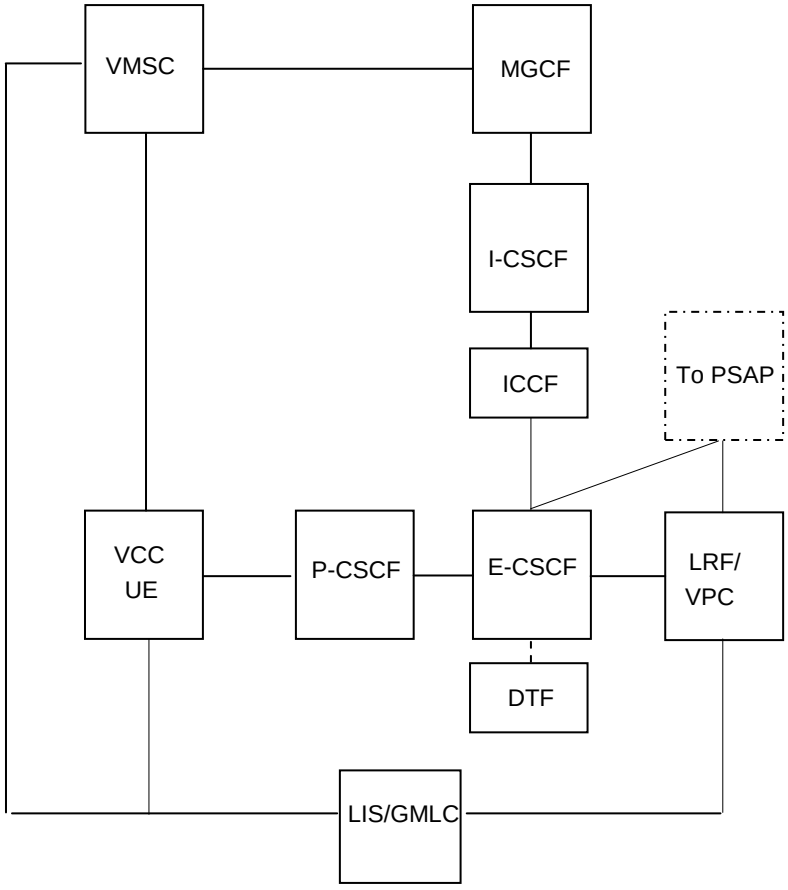
Editors Note: Applicability to Emergency calls made by unauthorized users is FFS.

The solution extends the VCC architecture specified in TS 23.206 [3] using the following architectural principles:

- Standard IMS Emergency call setup procedures are used for establishment of Emergency Calls using IMS and Domain Transfers to IMS.
- The CS network is used as a bare bones access network when establishing an Emergency Call via CS domain. CS Emergency Calls are redirected to the serving IMS for application of IMS Emergency Call procedures.
- An Emergency Remote User Agent (E-RUA) function, similar to the RUA of ICCF being defined as part of ICS in TR 23.892 [7], in the serving IMS presents an Emergency Call established via CS domain as an IMS Emergency Call to the E-CSCF.
- The call control signaling for CS and IMS Emergency Call is anchored at the DTF (Domain Transfer Function) in a local IMS network designated to perform VCC functions of call/session anchoring and Domain Transfers in a particular geographical region. The DTF may be optionally co-located with the E-CSCF and is invoked as a visited network option for Emergency Calls established using a VCC capable terminal.
- Domain Transfers are executed by the DTF which switches the Access Leg from the transferring-out domain to the transferring-in domain, updating the Remote Leg toward the PSAP with the Access Leg info and Location Key associated with the transferring-in domain.

6.1.1.2 Reference Architecture

The reference architecture for VCC Emergency Calls is provided in figure 6.1.1.2-1 below.



NOTE: Only relevant standard functions are shown.
Assumes NENA i2: "To PSAP" represents Emergency Network Elements in-route to PSAP [SIP signalling via MGCF for legacy PSAP].

Figure 6.1.1.2-1: VCC Emergency Call Architecture

6.1.1.2.1 Domain Transfer Function (DTF)

The Domain Transfer Function is defined in TS 23.206 [3]. It anchors call control signalling for the VCC user's CS and IMS sessions for enablement of Domain Transfers between CS domain and IMS. The DTF for Emergency Calls resides in a local IMS network designated to perform VCC functions of call/session anchoring and Domain Transfers in a particular geographical region. The DTF may be optionally co-located with the E-CSCF.

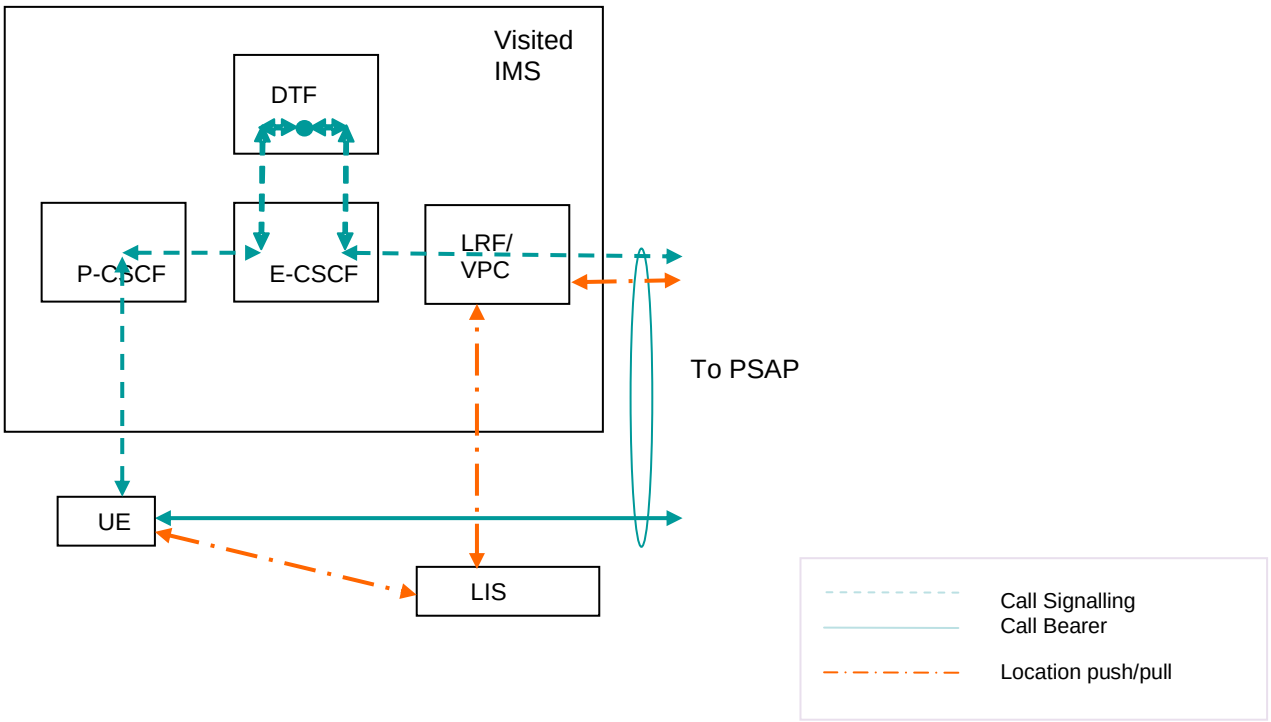
6.1.1.2.2 IMS CS Control Function (ICCF)

The IMS CS Control Function (ICCF) is being defined as part of the ICS study being captured in TR 23.892 [7]. The Emergency Remote User Agent (E-RUA) of ICCF presents SIP User Agent behaviour on behalf of the UE for presentation of Emergency Calls made via the CS domain to the E-CSCF, as an IMS originated Emergency Call. The ICCF for Emergency Calls resides in the serving IMS.

6.1.1.3 Initial Call establishment

6.1.1.3.1 Emergency Calls established in or transferred to IMS

The procedures defined in TS 23.167 [4] are used for establishment of Emergency Calls using IMS. The signalling/bearer paths and the paths for Location Push/Pull for Emergency calls established or transferred to IMS are as identified in Figure 6.1.1.3.1-1 below.



NOTE: LRF shown in proxy mode here; When using LRF in redirection/query mode, the signalling path runs directly out of E-CSCF.

Figure 6.1.1.3.1-1: Signalling/Bearer Paths for IMS Emergency Calls

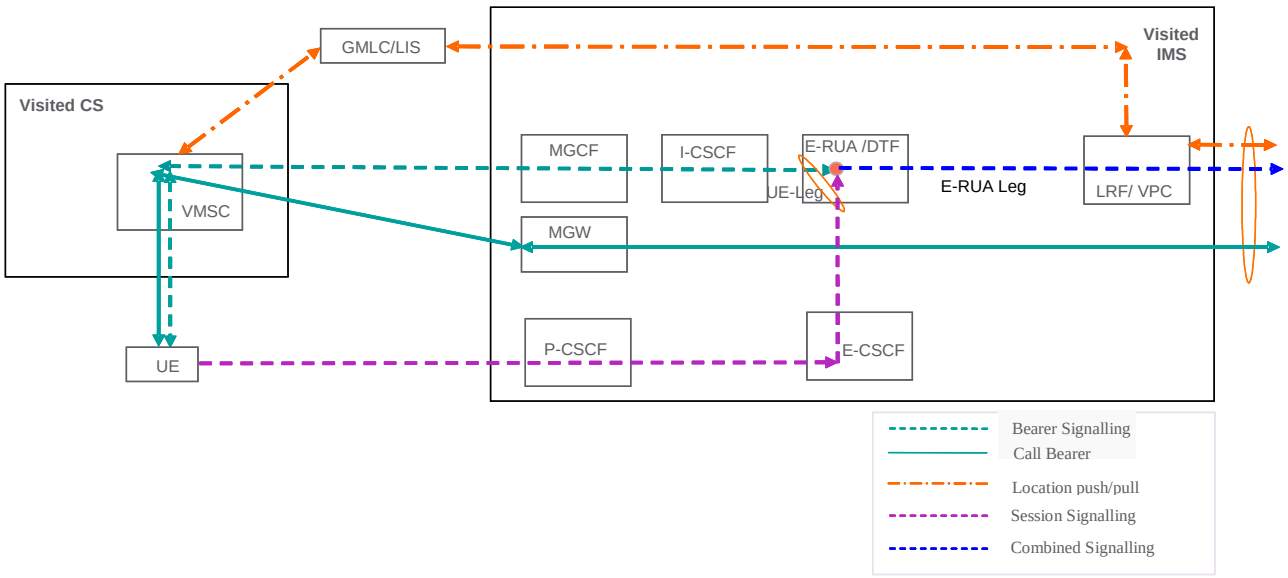
NOTE: The local IMS designated for VCC functions is the same as the visited IMS in this illustration.

The DTF is inserted in the signalling path which invokes a 3pcc for enablement of Domain Transfers for the call as specified in TS 23.206 [3].

The DTF may assign a Session Transfer ID. DTF would assign Session Transfer Identifiers when it receives emergency session request from the UE and could transport it to the UE in a SIP message. The UE would use the Session Transfer Identifiers for requesting handovers to CS and subsequent hand-back to IMS.

6.1.1.3.2 Emergency Calls established in or transferred to CS

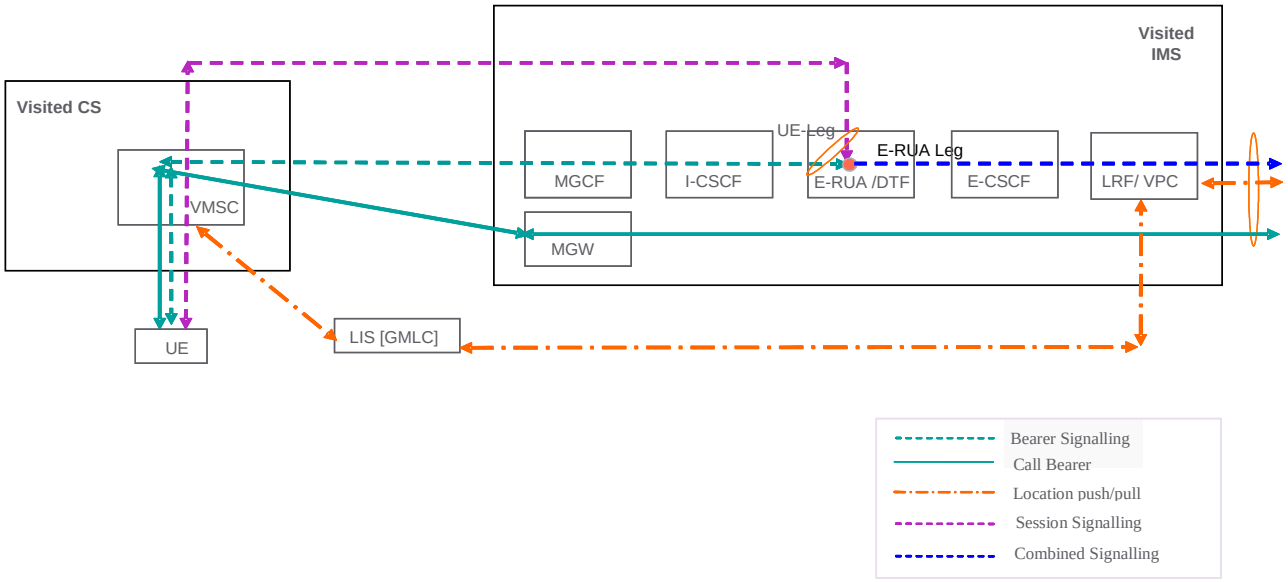
The signalling/bearer paths and the paths for Location Push/Pull for Emergency calls established or transferred to the CS domain are as identified in Figures 6.1.1.3.2-1, 6.1.1.3.2-2 and 6.1.1.3.2-3 below.



NOTE: LRF shown in proxy mode here; When using LRF in redirection/query mode, the signalling path runs directly out of E-CSCF.

Figure 6.1.1.3.2-1: Signalling/Bearer Paths for CS Emergency Calls in conjunction with a logical signalling control channel established over the PS domain

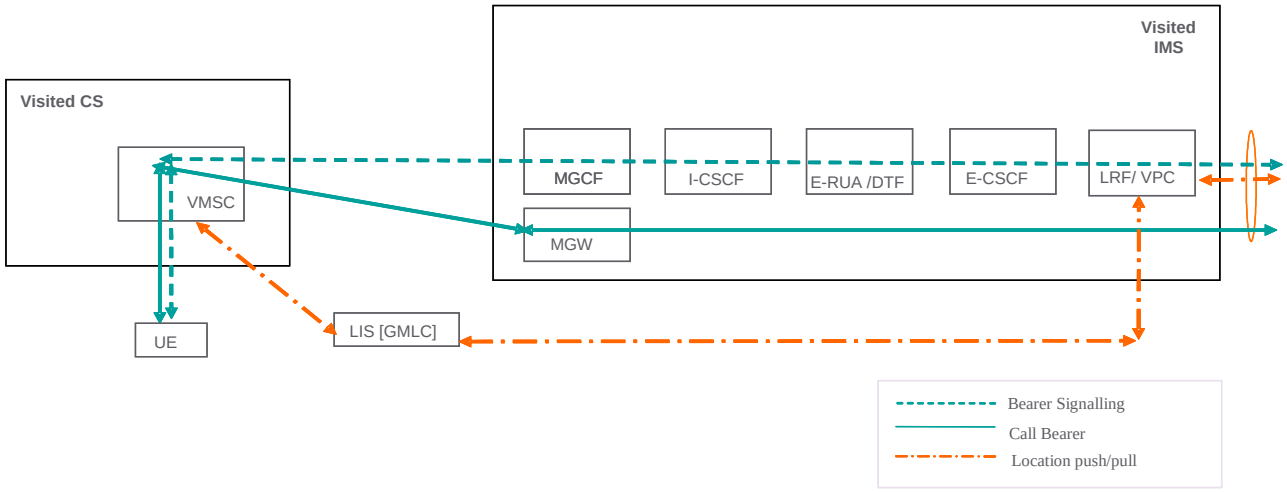
NOTE 1: The local IMS designated for VCC functions is the same as the visited IMS in this illustration.



NOTE: LRF shown in proxy mode here; When using LRF in redirection/query mode, the signalling path runs directly out of E-CSCF.

Figure 6.1.1.3.2-2: Signalling/Bearer Paths for CS Emergency Calls in conjunction with a logical signalling control channel established over the CS domain

NOTE 2: The local IMS designated for VCC functions is the same as the visited IMS in this illustration.



NOTE: LRF shown in proxy mode here; When using LRF in redirection/query mode, the signalling path runs directly out of E-CSCF.

Figure 6.1.1.3.2-3: Signalling/Bearer Paths for CS Emergency Calls for Domain Transfers

NOTE 3: The local IMS designated for VCC functions is the same as the visited IMS in this illustration.

A special E.164 number (termed E-RUA DN) is downloaded to the UE in the visited network (see clause 6.2.2.1). When the user makes an emergency call (e.g. dials 911), the UE sends a Set-up to the VMSC using the E-RUA DN. The serving network (i.e. VMSC) is able to recognise the dialled number as a request to make an emergency call and routes the call as an emergency call. This is accordance with TS 22.101 [13], clause 10.1.

The VMSC performs the standard CS emergency procedures and allocates a routeing key (e.g. ESRK). This involves the VMSC sending a MAP Subscriber Location Report (SLR) request to the GMLC allocated to the geographical region that the UE is roaming within. Based on the received information, the GMLC will store the current location of the user against a call reference.

When the VMSC receives the MAP-SLR response it is still running the call context for the CS Emergency call. The VMSC routes the call to the MGCF based upon the routeing configuration at the VMSC.

NOTE 4: Modifications are required at the VMSC to route the session using the E-RUA DN rather than the ESRK/ESRD after the standard emergency call procedures have been invoked at the VMSC.

The Emergency call routeing toward the PSAP is provided by a serving IMS; this is achieved by routeing the Emergency call through the CS domain network toward the E-RUA in the serving IMS.

Using the concepts defined in TR 23.892 [7] IMS Centralized Services, a logical control channel is used to transport signalling between the UE or E-RUA in the serving IMS network when making Emergency calls in the CS domain. This signalling contains emergency related data that either may not be inter-worked safely by the MGCF or data that plays no part in the routeing decision at the MSC (but needs to be taken into consideration in IMS). For example, the Emergency Service Category (as defined in TS 24.008 [12], clause 10.5.4.33) would need to be sent into IMS to allow the LRF to make a determination of the most appropriate PSAP.

The logical control channel between the UE and the E-RUA can be established over the CS domain network using USSD, or over the PS domain using SIP signalling but no media is associated with the SIP INVITE.

In parallel with the setting up of ICCC, the UE will set up the CS bearer signalling leg (by dialling the E-RUA DN); both of these legs will be combined at E-RUA to present the RUA leg to E-CSCF.

NOTE 5: This architecture does not rely on support of IMS centralized services as the solution requires the setting up of the logical control channel to a function in the visited network. If the visited network supports IMS centralized services for its own users, then it is an implementation option for the E-RUA function to be housed with the existing RUA function for that network.

For establishment of the logical control channel over the PS domain using SIP:

- The location-reference is provided by a location server in the PS network rather than the CS network (as in standard IMS emergency session control).

- This option is recommended for use in 3G networks.

For establishment of the logical control channel over the CS domain using USSD:

- The location-reference is provided by the CS network
- There are two modes of routeing USSD messages. The first mode is home-routed mode where the VMSC routes the USSD message to the HSS and the HSS sends it to the E-RUA. The second mode is visited-routed mode where the VMSC routes the USSD message directly to the E-RUA. It is recommended to use visited-routed mode to remove reliance on the home network.
- This option is recommended for use in 2G networks.

Once the E-RUA has combined the UE-Legs, it presents the Emergency session to E-CSCF as an Emergency call originated in IMS. When the logical control channel is established over the CS domain, the Location Object (see RFC 4119 [9]) in the Emergency Invite is populated by the E-RUA with a Location Reference for retrieval of user's current location from the GMLC using the information passed by the VMSC at call set-up. When the logical control channel is established over the PS domain, the location object received by the E-RUA on the UE-leg in the session control signalling and is populated by the E-RUA in the outgoing INVITE.

The procedures defined in TS 23.167 [4] are used for processing of the Emergency Call at the E-CSCF.

The DTF is inserted in the signalling path which invokes a 3pcc for enablement of Domain Transfers for the call as specified in TS 23.206 [3].

6.1.1.4 Domain Transfers

The UE detects the trigger for Domain Transfer, registers in the transferring-in domain if needed, and establishes an Emergency Call in the transferring-in domain.

For Domain Transfers to CS, the UE uses the E-RUA DN (which was downloaded as part of CS attach procedures as described in clause 6.1.1.6.1) or Session Transfer ID (which was supplied to the UE during the original PS emergency session establishment) to establish the transfer leg of the emergency session through the E-RUA of the ICCF by setting up a call toward the E-RUA of the ICCF; the call is treated as emergency call at the VMSC. This procedure is illustrated in Figure 6.1.1.3.2-3 and uses the same procedures at the VMSC/GMLC for CS emergency originations as defined in clause 6.1.1.3.2.

The DTF processes the Emergency Invite for execution of Domain Transfer as specified in Execution of Domain Transfer procedure specified in TS 23.206 [3]. The Remote Leg toward the PSAP is updated using the Access Leg Update toward the remote end procedure specified in TS 23.206 [3]. The location reference stored against the emergency call instance at the LRF/VPC is updated as part of this procedure.

The source Access Leg established via the transferring-out domain is released. The source Access Leg release is coordinated b/w the UE and the DTF.

6.1.1.5 Enhancements to Initial Call Establishment and Domain Transfers

6.1.1.5.1 General

This clause explores simplifications that are possible with use of logical signalling channel and/or the use of an ICS enhanced MSC server (as defined in TS 23.292 [10]).

The VMSC shown in Figures 6.1.1.3.2-1, 6.1.1.3.2-2 and 6.1.1.3.2-3 could either be a standard MSC Server or an MSC Server enhanced for ICS.

The Signalling/Bearer paths shown in Figure 6.1.1.3.2-1 are used to request domain transfer from IMS to CS when the logical signalling control channel is established over the PS domain.

The Signalling/Bearer paths shown in Figure 6.1.1.3.2-3 are used to request domain transfer from IMS to CS when the logical signalling control channel is not available.

The UE uses different procedures to establish the circuit bearer for IMS emergency sessions depending on the availability of the logical signalling channel and the type of MSC Server it is attached to.

1. When it is possible to establish a logical signalling channel over the PS domain simultaneously with the setup of the CS bearer session:

   - The logical signalling channel is used to establish a standard IMS emergency session indicating use of CS bearer for the session; standard CS origination, i.e. TS 24.008 [12] Setup message addressing the E-RUA PSI DN is used to set up the circuit bearer. The E-RUA PSI DN is used at the MSC Server for routeing of the call to IMS using standard MSC procedures. Standard PS location services procedures as defined in TS 23.167 [4] are used for location retrieval and conveyance over the logical signalling channel.

NOTE 1: The priority for CS bearer resource allocation and retention may be indicated by the UE through standard means; e.g. use of eMLPP priority level 0 which is normally used for TS12, or a higher level.

   - This procedure is used for both CS originations and for Access Transfer from PS to CS, and is applicable when the UE is attached to a standard MSC Server or an MSC Server enhanced for ICS.

2. When it is not possible to establish a logical signalling channel over the PS domain simultaneously with the setup of the CS bearer session:

   a) When the UE is attached to an MSC server enhanced for ICS:

      - Standard CS emergency call with use of TS 24.008 [12] Emergency Setup is used to set up the circuit bearer. The MSC Server uses the CS domain procedures for location retrieval/conveyance and provides the necessary routeing of the emergency call towards the visited IMS network.

      - This procedure is used for both CS originations and Access Transfer from PS to CS.

   b) When the UE is attached to a standard MSC Server:

      i) For calls originating in the CS access: Standard CS emergency call is established with use of TS 24.008 [12] Emergency Setup; standard CS emergency call procedures are used at the MSC Server.

      ii) For PS to CS Access Transfers: Standard CS setup procedures, i.e. TS 24.008 [12] Setup message addressing the E-RUA is used to set up the circuit bearer. The E-RUA PSI DN is used at the MSC Server for routeing of the call to IMS using standard MSC procedures. Location conveyance upon Access Transfer is not supported.

NOTE 2: The priority for CS bearer resource allocation and retention may be indicated by the UE through standard means; e.g. use of eMLPP priority level 0 which is normally used for TS12, or a higher level.

Editor's Note: Mechanisms for indicating priority for the CS bearer setup are FFS. One possible solution is use of eMLPP level 0 which is normally used for TS12, or a higher level. It needs to be determined whether this makes it a requirement to deploy eMLPP.

Editor's Note: Mechanisms for capability exchange between the UE and network are FFS.

6.1.1.5.2 Alternative message flows

The message flows that illustrate the new principles discussed in this clause are referenced below.

Clause 6.1.4.1.2.2 illustrates alternative flows for CS origination when simultaneous CS and PS access is available.

Clause 6.1.4.1.2.4 illustrates flows for CS origination when simultaneous CS and PS access is not available.

Clause 6.1.4.3 illustrates flows for PS-CS access transfer when simultaneous CS and PS access is available.

Clause 6.1.4.4 illustrates flows for PS-CS access transfer when simultaneous CS and PS access is not available.

For PS origination in clause 6.1.4.1.1, the STN allocated by the E-RUA/DTF is the E-RUA PSI DN (i.e. there is no need for a separate STN and a separate E-RUA PSI DN to be allocated).

6.1.1.6 Negotiation of VCC Support

6.1.1.6.1 Capability Exchange in the CS Network

6.1.1.6.1.1 Capability Exchange using the Home Network

6.1.1.6.1.1.1 Option 1: Mobile Originated USSD exchange to RUA in Home Network

When the VCC UE attaches to the CS network, the standard update-location message exchange occurs between the UE, VLR and HSS. After completion of this message exchange, the VCC UE sends a mobile-originated USSD message to the RUA in the home network. The USSD message goes through the VMSC (and through standard USSD processing at VMSC, the VMSC adds in its address to the origination-reference parameter in the MAP Dialogue Portion) and arrives at the HLR. The HLR is configured to route the USSD message to the home ICCF based upon the service-code in the USSD message.

The home ICCF is configured with a list of users that have a VCC subscription. The service-code in the USSD message informs the home ICCF to check (via data configuration) if the visited network supports VCC for IMS Emergency. If the visited network does support the procedure, then the Home ICCF sends a USSD-response to the VCC UE containing an E-RUA DN. The E-RUA DN is used by the VCC UE to set-up the emergency call.

The home ICCF sends back a USSD error to the mobile-originated USSD in the following cases:

1. Subscriber does not exist in the home RUA (i.e. subscriber is not a VCC subscriber).
2. VMSC address supplied in the USSD message is from a VMSC in a visited network that does not support VCC for IMS Emergency Calls.

NOTE: The USSD message is only sent on inter-MSC location update. It is not sent during standard CS-attach procedures or during Periodic location update, when the VLR has a confirmed HLR-number stored for the subscriber.

The E-RUA DN is used by the VMSC translations to route the emergency call to IMS after the emergency procedures have been executed to allocate an ESRK/ESRD or PSAP address.

The E-RUA DN can also be used for domain transfers from PS to CS, or alternatively the Home RUA could download an additional number that can serve as the Session Transfer Number (STN) for domain transfers.

If the VCC UE received a E-RUA DN, it uses this E-RUA DN to setup a call using standard CS originating procedures when the user initiates an emergency call. If the VCC UE does not receive the E-RUA DN, then it uses standard procedure to set up the emergency call.

This option allows the session signalling procedures to be carried out in parallel with the bearer control signalling procedures during emergency session establishment.

6.1.1.6.1.1.2 Option 2: Use of IMS Registration

When in a network that has dual CS and PS coverage, the PS network can be used to supply a semi-dynamic E-RUA DN to the UE during IMS registration using similar mechanisms to that described in TR 23.892 [7], clause 6.5.2.1. This option allows the session signalling procedures to be carried out in parallel with the bearer control signalling procedures during emergency session establishment and allows the session related signalling to provide a E-RUA DN for use in the next emergency session.

6.1.1.6.1.2 Capability Exchange using the Visited Network

6.1.1.6.1.2.1 Option 3: Mobile Originated USSD exchange to E-RUA in Visited Network

Instead of routeing the USSD message to the Home RUA function (as described in Option 1) and relying on the analyses of the VCC Subscription at the HSS and Home RUA, the USSD message could be routed to the E-RUA. As the UE will only attempt to send a USSD message with a special USSD service code if modified to support this feature, the VMSC can be configured to route the USSD message to the E-RUA in the visited network. This option allows the session signalling procedures to be carried out in parallel with the bearer control signalling procedures and allows the session related signalling to provide the Next E-RUA DN for use in the next emergency session.

6.1.1.6.1.2.2 Option 4: Session Signalling Channel with CS coverage only using MO-USSD

To remove the need to send the MO-USSD at CS-attach (as described in Options 1 and 3), the E-RUA can supply a dynamic E-RUA DN (i.e. allocated by the visited network) by using a MO-USSD exchange during session establishment. This option can only be used during emergency session establishment when the session control signalling procedures are carried out prior to and in sequence with the bearer control signalling procedures.

6.1.1.6.1.2.3 Option 5: Session Signalling Channel with CS and PS coverage using SIP

When in a network that has dual CS and PS coverage, the PS network can be used to transport the session related information during emergency session establishment by using the session signalling channel established over the PS network (using SIP) to provide a dynamic E-RUA DN allocated by the E-RUA (i.e. the visited network). This option can only be used during emergency session establishment when the session control signalling procedures are carried out prior to and in sequence with the bearer control signalling procedures

6.1.1.6.1.3 Recommendation for Capability Exchange in the CS Network

It is recommended to adopt Option 3 if there is a desire to send the signalling and bearer session establishment signalling in parallel. It is recommended to adopt Options 4 and 5 to remove the need to send USSD at CS-attach if it is accepted that the signalling and bearer session signalling can be sent in sequence. It is not recommended to adopt Options 1 and 2 as they create reliance on the home network to have knowledge of visited network support for the feature.

Editor' Note: The options discussed in this clause do not address support for UICCless/unauthenticated callers. For example, USSD cannot be sent unless the user has done an update location, which will not occur in the UICCless case. This is for further study.

6.1.1.6.2 Capability Exchange in the IMS Network

When the VCC UE makes an IMS Emergency Call, capability information about the UE's capability to support VCC for IMS Emergency can be placed within the INVITE. If the visited IMS network supports VCC for IMS Emergency, then the E-CSCF will act on this capability information and send the INVITE to the E-RUA/DTF to anchor the session.

Alternatively, as described in Alternative 2, clause 6.2.2.1 of this TR, either:

- The E-CSCF may assume that all UEs are VCC capable and send all sessions to the E-RUA/DTF; or,
- The E-CSCF in the visited network could be configured with identities of roaming users from other networks where it should be assumed that all sessions are sent to the E-RUA/DTF.

In the first alternative, this would be wasteful on resources as all calls have to be sent to the E-RUA/DTF and anchored even though the UE may not be VCC-capable.

In the second alternative, this requires configuration in the visited network, and is an option if there is a desire to avoid changes to the SIP signalling.

6.1.2 Impact

6.1.3 Assessment

Clause 6.1.1.5 provides an overview of the current solution for Alternative 1.

The following simplifications to the solution in clause 6.1.1.5 are proposed for Release 9:

- Capability Exchange between the UE and the visited IMS occurs on IMS emergency origination. It may consist of the visited IMS network making a decision to anchor based on configuration data or may consist of the UE inserting its VCC capability within the INVITE towards the visited IMS. If the E-SCC AS is successful in anchoring the call, it returns an STN to the UE for usage in PS to CS domain transfer. The STN enables the CS network to re-route the domain transfer request to the visited IMS network. A non-VCC capable UE ignores the STN returned to it.

- Support for only PS to CS Session Transfer. The UE will always send a standard TS 24.008 [12] SETUP towards the MSC addressing the STN:
- When the Gm reference point is available in the target network:
  - If UE is attached to a standard MSC server, no priority is supported for the emergency call. Standard PS location services are used for location continuity.
  - If the UE is attached to an enhanced MSC server, the MSC will detect the STN as an emergency call and use standard emergency call procedures for priority of the CS bearers. Location information will be obtained by both the PS domain and CS domain in this scenario and the E-SCC-AS chooses one of these methods to update the location reference in the LRF.
- When the Gm reference point is NOT available in the target network:
  - If UE is attached to a standard MSC server, no priority or location continuity is supported for the domain transfer request.
  - If the UE is attached to an enhanced MSC server, the MSC will detect the STN as an emergency call and use standard emergency call procedures for priority of the CS bearers. Location information will be obtained by the CS domain only in this scenario.
- For emergency calls originated in the PS domain, hand-back from the CS domain to the PS domain may be supported by Alternative 1 in Release 9 as determined by service requirements.

The following aspects of the solution are for further study:

- Anchoring of calls established in the CS domain and support for CS to PS session transfer.
- Support for anchoring and session transfer for Unauthenticated UEs.

6.1.4 Procedures

6.1.4.1 Call Initiation

6.1.4.1.1 Calls established in IMS

Figure 6.1.4.1.1-1 provides an example flow for an emergency session established in IMS, illustrating how the emergency session is anchored and how the session transfer identifiers are transported back to the UE.

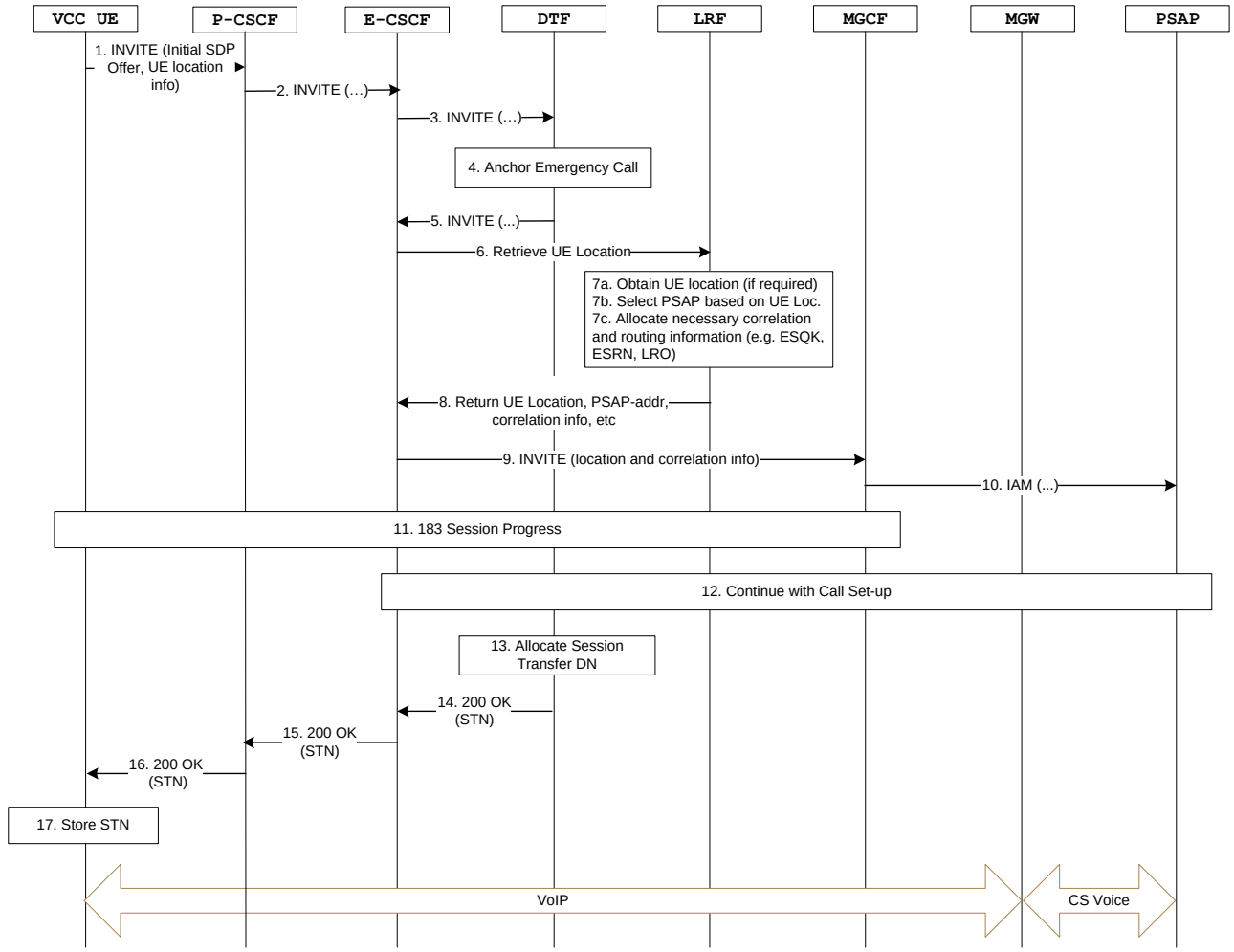


Figure 6.1.4.1.1-1: VCC UE initiating an emergency session in IMS

NOTE 1: A pre-requisite is for the VCC UE to be IMS Emergency Registered if located in a VPLMN or located in the HPLMN are not already IMS Registered.

1. The VCC UE generates a SIP INVITE containing the UE's location information or reference (if available).

2. The P-CSCF selects an E-CSCF and forwards the INVITE to the E-CSCF.

3. The E-CSCF sends the INVITE to the DTF.

NOTE 2: The trigger for routeing the INVITE from the E-CSCF to the DTF could be as simple as configuring the VCC user in the E-CSCF with the address of the DTF located in a local IMS network designated to perform the functions of call/session anchoring and domain transfers in a particular geographical region.

4. The DTF (acting as a routeing B2BUA) anchors the emergency session, i.e. the DTF is inserted in the signalling path which invokes a 3pcc for enablement of Domain Transfers for the call as specified in TS 23.206 [3].

5. The DTF creates an INVITE and sends it back to E-CSCF.

6. The E-CSCF sends the INVITE to the LRF

7. The LRF obtains the UE's location (if not provided in the INVITE), selects the most appropriate PSAP based on the UE's location, allocates the necessary correlation information for the record stored in the LRF (e.g. ESQK) and allocates routeing information for the call (e.g. ESRN).

8. The LRF returns the location information, PSAP address, correlation information (e.g. ESQK) and routeing information (e.g. ESRN) to the E-CSCF.

9. The E-CSCF uses the PSAP address or routeing information (e.g. the ESRN) to format an INVITE message, and it sends it to the MGCF.

10. The MGCF performs the necessary interworking of the INVITE and formulates an IAM containing the correlation information (e.g. ESQK) and sends it to the PSAP.

11. The MGCF initiates 183 Session Progress through the IMS core back to the UE

12. Call set-up continues with the PSAP sending ACM/ANM back to the MGCF which is interworked into a 200OK and sent through the IMS Core Network.

13. The DTF receives the 200 OK from the E-CSCF and allocates a Session Transfer Number (STN) that is used by the UE to initiate domain transfer requests.

NOTE 3 The protocol details related to the transfer of the STN in the 200 OK is a matter for Stage 3. It could be possible to utilise the mechanism defined by RFC 4483 [6].

14. The DTF sends the 200 OK to the E-CSCF

15. The E-CSCF sends the 200 OK to the P-CSCF

16. The P-CSCF sends the 200 OK to the UE

17. The UE stores the STN.

6.1.4.1.2 Calls established in CS

6.1.4.1.2.1 Calls established using a logical signalling control channel over the PS domain – Alternative 1

NOTE 1: The call flows depicted in this clause do not assume support for IMS Centralized Services. However, if IMS Centralized Services is implemented in the visited network (for its own home subscribers) it is possible for the E-RUA function to be implemented in the same node as the RUA function. This is an implementation option.

Figure 6.1.4.1.2.1-1 provides an example flow for an emergency session established in CS using a logical signalling control channel established over the PS domain, illustrating how the emergency session is anchored and how the location reference is provided to the LRF. In this flow, the VMSC recognises the CS bearer set-up as a request to make an emergency call and carries out the standard emergency call CS procedures prior to route the call to the MGCF.

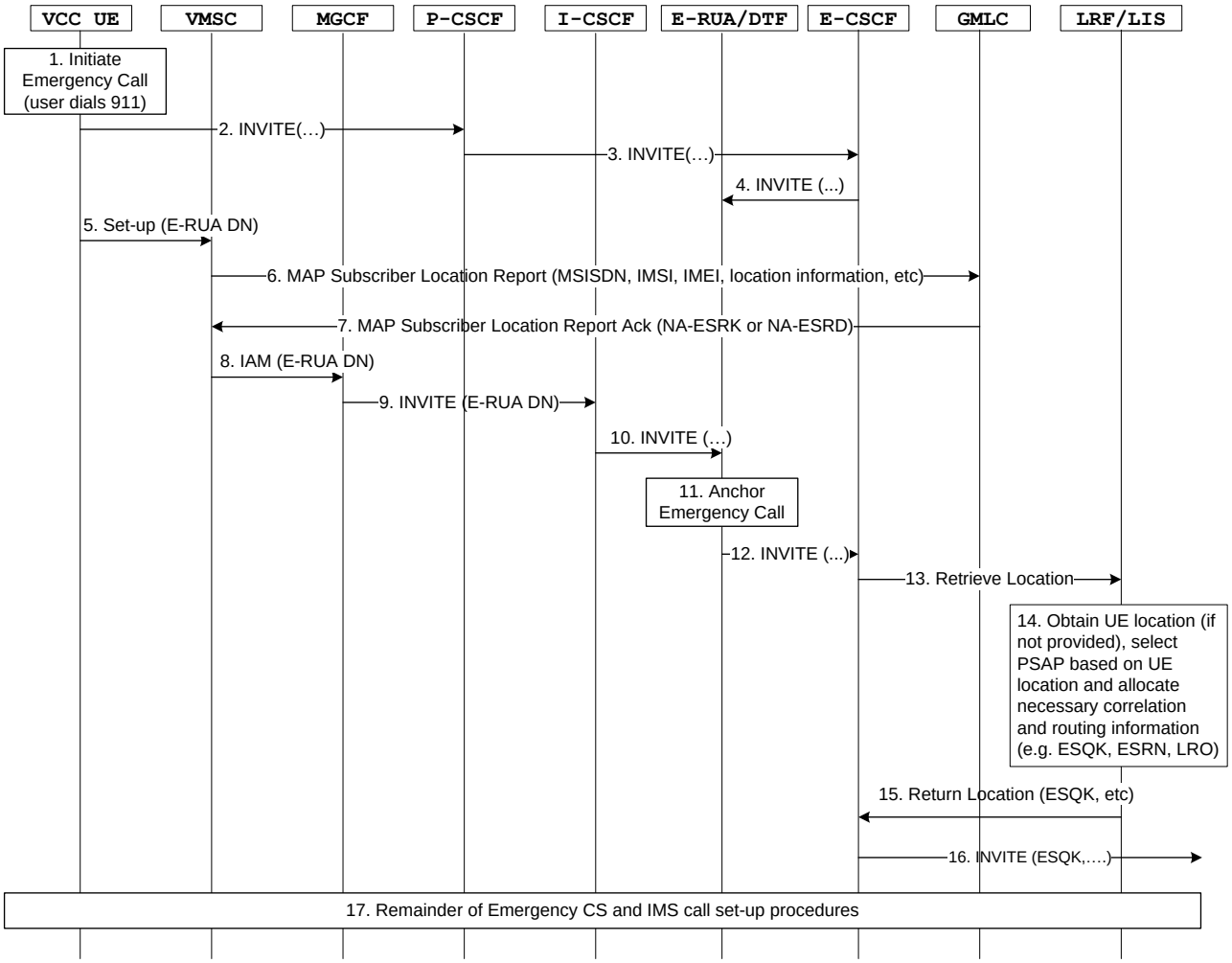


Figure 6.1.4.1.2.1-1: VCC UE initiating an emergency call in CS in conjunction with a logical signalling control channel established over the PS domain (Alternative 1)

NOTE 2: This call flow is depicting the LRF acting in Re-direct mode. The procedure is also applicable when the LRF acts in Proxy mode.

NOTE 3: Steps 2-4 and 5-10 may occur in sequence or in parallel. If they occur in sequence, then the DN used by the UE in Step 5 can be provided by the E-RUA in a provisional response when the E-RUA receives the INVITE in Step 4. If they occur in parallel, then, a mobile-originated USSD exchange between the UE and the E-RUA on CS attach can supply the suitable E-RUA DN for the visited network.

1. The user initiates an emergency call (e.g. dials 911).

2. The VCC UE generates an Emergency SIP INVITE (Request-URI set to a sos-urn) towards the P-CSCF in the visited network. If the UE has location reference available, it includes it in the request as in a standard Emergency INVITE

3. The P-CSCF selects an E-CSCF (for the geographical region) and forwards the INVITE to the E-CSCF. The P-CSCF may query the IP-CAN to obtain the location reference (if it was not included by the UE).

4. The E-CSCF sends the INVITE to the E-RUA/DTF.

NOTE 4: The trigger for routeing the INVITE from the E-CSCF to the E-RUA/DTF is discussed in clause 6.1.1.5.2.

5. The UE sends a normal Setup message (as defined in TS 24.008 [12]) to the VMSC using the E-RUA DN that was previously downloaded to the UE on.

6. The serving network (i.e. VMSC) recognises that the E-RUA DN as a request to make a CS emergency call and carries out standard CS emergency procedures. This may involve the VMSC obtaining an interim location

estimate for the UE as defined in TS 23.271 [11]. The VMSC sends a MAP Subscriber Location Report (SLR) request to the GMLC allocated to the geographical region that the UE is roaming within. The MAP Subscriber Location Report carries the IMSI, MSIDN, IMEI, VMSC address, serving cell identity or SAI for the UE.

7. Based on the received information, the GMLC creates a call context, stores the received location information and returns the MAP-SLR response to the VMSC.

8. When the VMSC receives the MAP-SLR response, it is still running the call context for the CS Emergency call. The VMSC routes the call to the MGCF based upon the routeing configuration at the VMSC.

NOTE 5: Modifications are required at the VMSC to route the session using the E-RUA DN rather than the ESRK/ESRD after the standard emergency call procedures have been invoked at the VMSC.

9. The MGCF initiates an INVITE towards an I-CSCF in the visited network by inter-working the E-RUA DN to a PSI Tel-URI and setting it as the Request-URI. The INVITE contains the identity of the UE (e.g. MSISDN Tel-URI as P-Asserted-Identity).

10. The I-CSCF may contact the HSS (not shown) to retrieve the E-RUA address associated with the PSI Tel-URI. Once the I-CSCF has obtained the address, it sends the INVITE to the E-RUA/DTF.

11. The DTF anchors the emergency session, i.e. the DTF is inserted in the signalling path which invokes a 3pcc for enablement of Domain Transfers for the call as specified in TS 23.206 [3].

12. The E-RUA (acting as an originating UA) combines the relevant data from the INVITEs received in Step 4 and Step 10 into a single INVITE and initiates a new session towards the E-CSCF. The location reference/object provided in Steps 1-4 and 7 are populated into the outgoing INVITE.

13. The E-CSCF sends a Retrieve Location request to the LRF that is associated with the geographical region. This request includes the UE identification (contents of the P-Asserted-Identity) and the location-reference (e.g. contents of PIDF-LO and/or the P-Access-Network-Info), etc.

14. The LRF creates an emergency call instance and may use the location-reference provided via the CS access to interact with the GMLC or may use information provided via the PS access to interact with the LIS to retrieve location data. If a location reference from the PS access is not included in the INVITE, the LRF may obtain it directly from the LIS. The LRF stores the location-reference against the emergency call instance. Based upon the location information, the LRF interacts with an RDF to obtain routeing information for the emergency call. The LRF allocates an ESQK that identifies the call instance in the LRF. The ESQK is correlation information that allows the PSAP to request a location update from the LRF.

15. The LRF returns the ESQK, the PSAP address or routeing information and location-information (location reference or explicit location information) to the E-CSCF.

16. The E-CSCF uses the PSAP address or routeing information provided in Step 6 to send the call to the PSAP. The call request is either sent via an MGCF/MGW in the PSTN towards a PSTN-capable PSAP (not shown) or is sent directly as a SIP INVITE towards an IP-capable PSAP.

17. The rest of the call establishment procedure occurs between the UE, VMSC, E-RUA/DTF, E-CSCF and PSAP based upon the VCC CS origination procedure described in TS 23.206 [3].

6.1.4.1.2.2 Calls established using a logical signalling control channel over the PS domain - Alternative 2

NOTE 1: The call flows depicted in this clause do not assume support for IMS Centralized Services. However, if IMS Centralized Services is implemented in the visited network (for its own home subscribers) it is possible for the E-RUA function to be implemented in the same node as the RUA function. This is an implementation option.

Figure 6.1.4.1.2.2-1 provides an alternative example flow for an emergency session established in CS using a logical signalling control channel established over the PS domain, illustrating how the emergency session is anchored and how the location reference is provided to the LRF. In this flow, the Gm reference point is used for service control and location conveyance. The standard procedures defined in TS 23.167 [4] for the LRF to obtain location from a location server in the PS domain are followed. The UE uses TS 24.008 [12] Setup messages addressing the E-RUA PSI DN to setup the CS bearer session; the VMSC uses the E-RUA PSI DN to route the CS bearer session towards IMS. In this

figure, the VMSC does not recognise the E-RUA PSI DN as a request to make an emergency call, and hence does not carry out the CS domain emergency call procedures.

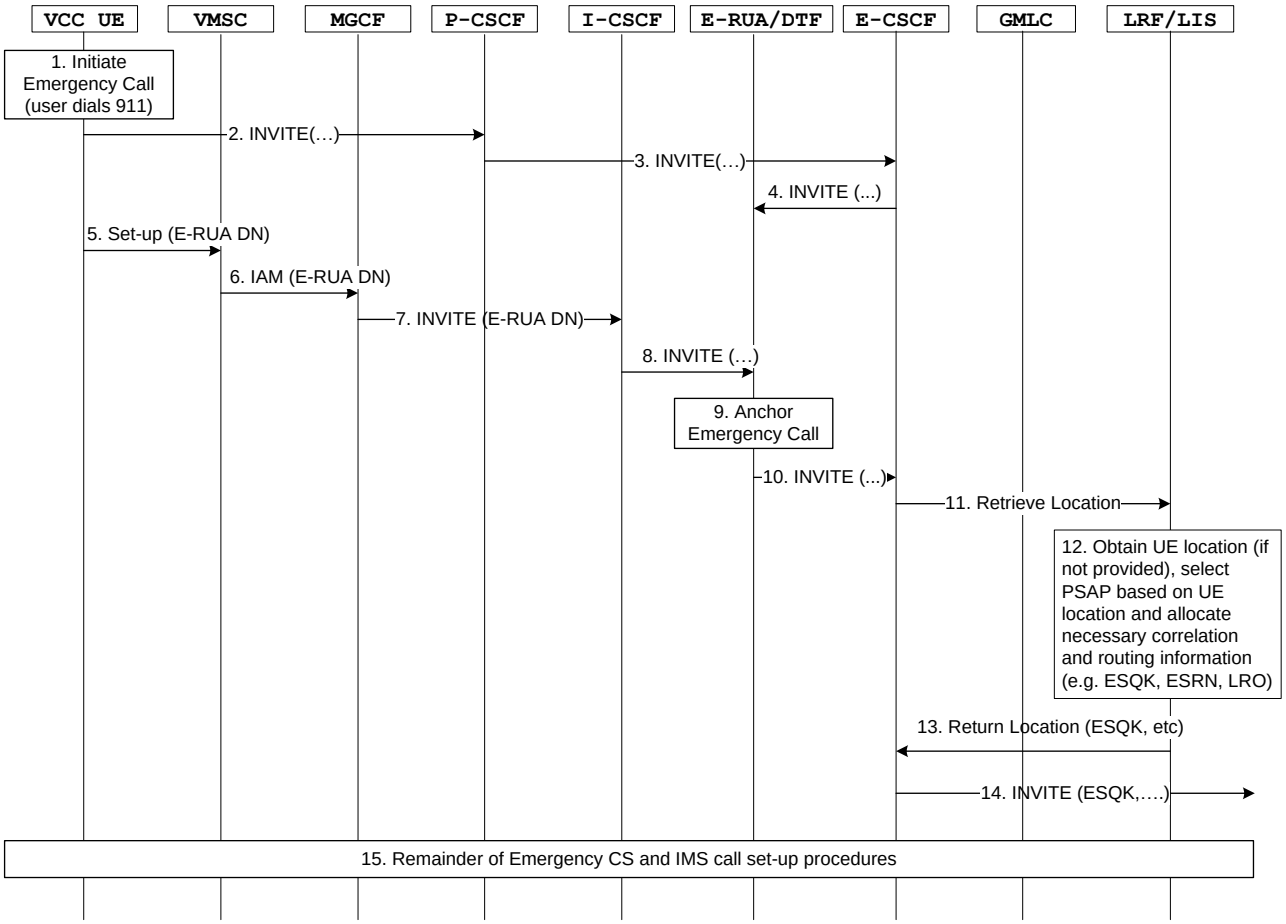


Figure 6.1.4.1.2.2-1: VCC UE initiating an emergency call in CS in conjunction with a logical signalling control channel established over the PS domain (Alternative 2)

NOTE 2: This call flow is depicting the LRF acting in Re-direct mode. The procedure is also applicable when the LRF acts in Proxy mode.

NOTE 3: Steps 2-4 and 5-8 may occur in sequence or in parallel. If they occur in sequence, then the DN used by the UE in Step 5 can be provided by the E-RUA in a provisional response when the E-RUA receives the INVITE in Step 4. If they occur in parallel, then, the E-RUA may be provided to the UE by other means e.g. use of USSD or similar exchange between the UE and the network.

Figure 6.1.4.1.2.2-2 provides a similar flow to that of Figure 6.1.4.1.2.1-1 but uses an MSC Server Enhanced for ICS, the only difference being the MSC Server initiates an INVITE towards the I-CSCF in the visited network instead of sending an ISUP IAM to an MGCF in the visited network.

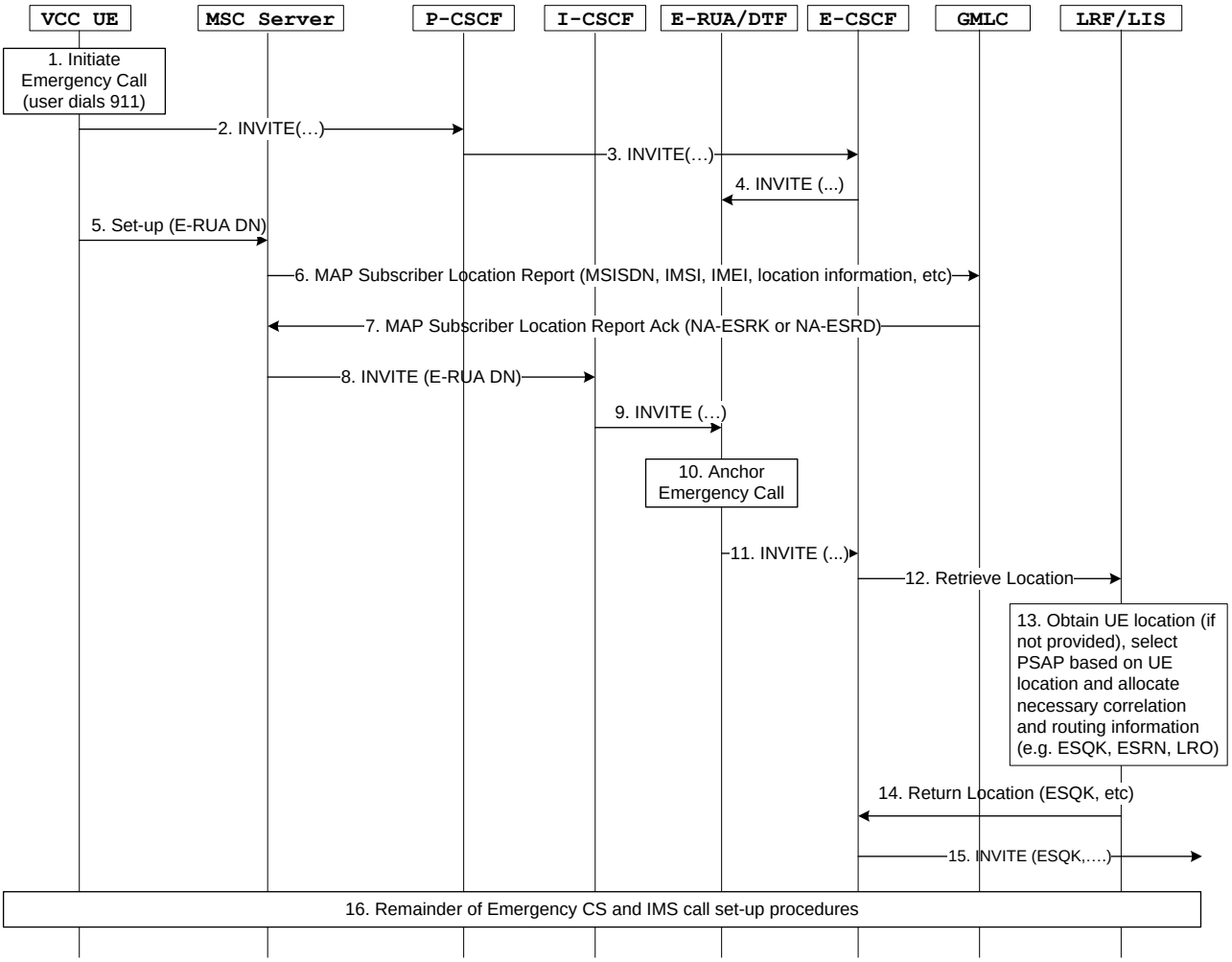


Figure 6.1.4.1.2.2-2: VCC UE initiating an emergency call in CS in conjunction with a logical signalling control channel established over the PS domain and use of an MSC Server Enhanced for ICS (Alternative 2)

6.1.4.1.2.3 Calls established using a logical signalling control channel over the CS domain

NOTE 1: The call flows depicted in this clause do not assume support for IMS Centralized Services. Ho wever, if IMS Centralized Services is implemented in the visited network (for its own home subscribers) it is possible for the E-RUA function to be implemented in the same node as the RUA function. This is an implementation option.

Figure 6.1.4.1.2.2-1 provides an example flow for an emergency session established in CS using a logical signalling control channel established over the CS domain, illustrating how the emergency session is anchored and how the location reference is provided to the LRF.

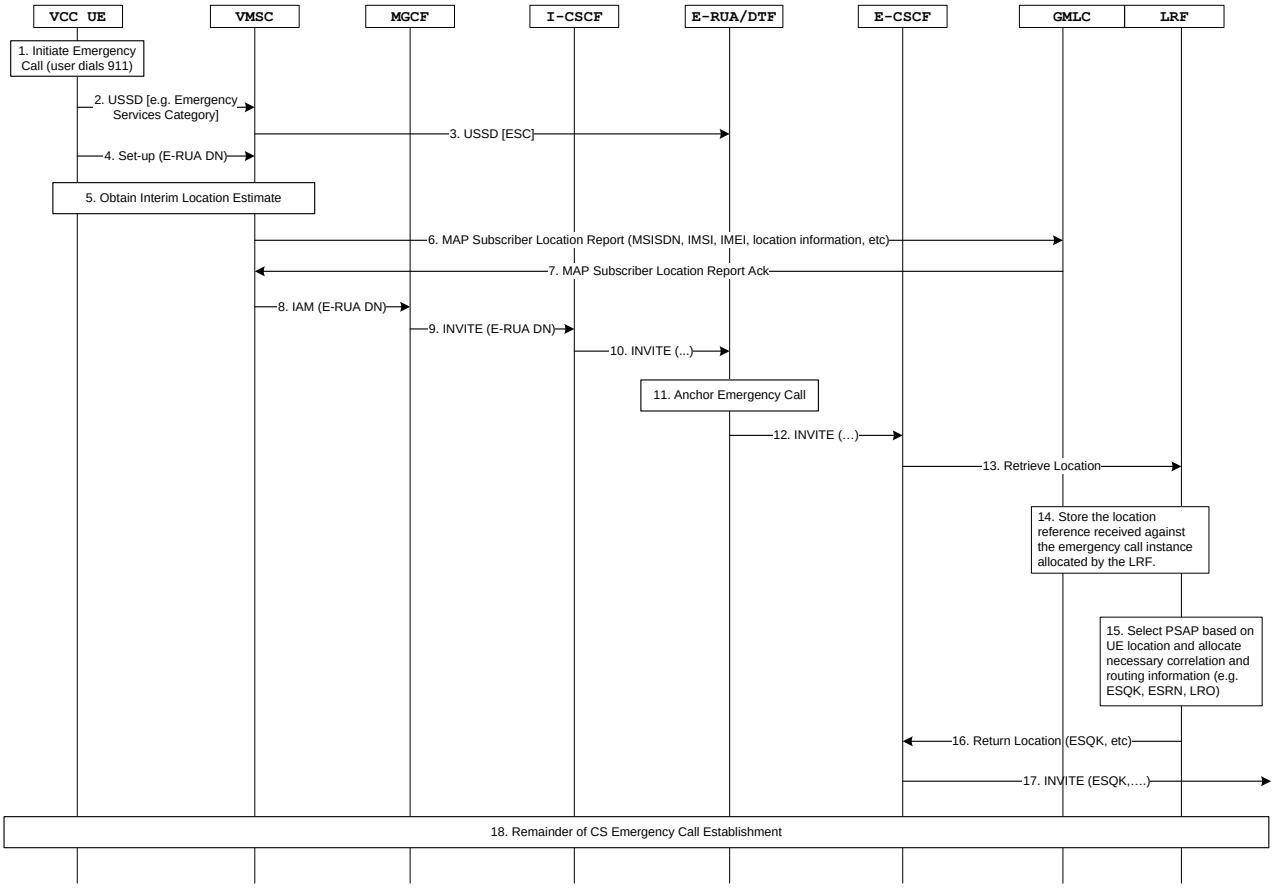


Figure 6.1.4.1.2.3-1: VCC UE initiating an emergency call in CS in conjunction with a logical signalling control channel established over the CS domain

NOTE 2: This call flow is depicting the LRF acting in Re-direct mode. The procedure is also applicable when the LRF acts in Proxy mode.

NOTE 3: Steps 2-3 and 4-10 may occur in sequence or in parallel. If they occur in sequence, then the DN used by the UE in Step 4 can be provided by the E-RUA as part of the USSD dialogue. If they occur in parallel, then a suitable E-RUA DN for the visited network can be supplied by the mobile-originated USSD exchange between the UE and the E-RUA on CS attach.

1. The user initiates an emergency call (e.g. dials 911).

2. The VCC UE generates a USSD message to the VMSC containing relevant data to assist the E-RUA to set up the Emergency session.

3. The VMSC uses visited-routed mode to route the USSD message directly to the E-RUA/DTF based upon the service-key/service-code in the USSD message.

NOTE 4: As an alternative, the USSD message could be routed to the HSS and the HSS could route the message to the E-RUA.

4. The UE sends a normal Setup message (as defined in TS 24.008 [12]) to the VMSC using the E-RUA DN that was previously downloaded to the UE on CS-attach.

5. The VMSC may initiate a procedure in the RAN to obtain an interim location estimate for the UE as defined and allowed in TS 23.271 [11].

6. The serving network (i.e. VMSC) recognises that the E-RUA DN as a request to make a CS emergency call and carries out standard CS emergency procedures. This involves the VMSC sending a MAP Subscriber Location Report (SLR) request to the GMLC allocated to the geographical region that the UE is roaming within. The MAP Subscriber Location Report carries the IMSI, MSIDN, IMEI, VMSC address, and serving cell identity or SAI for the UE. It also includes any interim location estimate obtained in step 3.

7. Based on the received information, the GMLC creates a call context, stores the received location information and returns the MAP-SLR response to the VMSC

8. When the VMSC receives the MAP-SLR response, it is still running the call context for the CS Emergency call. The VMSC routes the call to the MGCF based upon the routeing configuration at the VMSC.

9. The MGCF initiates an INVITE towards an I-CSCF in the visited network by inter-working the E-RUA DN to a PSI Tel-URI and setting it as the Request-URI. The INVITE contains the identity of the UE (e.g. MSISDN Tel-URI as P-Asserted-Identity).

10. The I-CSCF may contact the HSS (not shown) to retrieve the E-RUA address associated with the PSI Tel-URI. Once the I-CSCF has obtained the address, it sends the INVITE to the E-RUA/DTF.

11. The DTF anchors the emergency session, i.e. the DTF is inserted in the signalling path which invokes a 3pcc for enablement of Domain Transfers for the call as specified in TS 23.206 [3].

12. The E-RUA (acting as an originating UA) combines the relevant data from the INVITE received in Step 8 and the USSD message received in Step 10 into a single INVITE and initiates a new session towards the E-CSCF. The location reference is populated in the INVITE.

13. The E-CSCF sends a Retrieve Location request to the LRF that is associated with the geographical region. This request minimally includes the UE identification (contents of the P-Asserted-Identity) and the location-reference (e.g. contents of PIDF-LO and/or the P-Access-Network-Info), etc.

14. The LRF creates an emergency call instance and uses the location-reference to interact with the GMLC and retrieve the call record stored by the GMLC in Step 5. The LRF stores the location-reference against the emergency call instance.

15. Based upon the location information stored in the call record, the LRF interacts with an RDF to obtain routeing information for the emergency call. The LRF may allocate an ESQK that identifies the call instance in the LRF an ESQK. The ESQK is correlation information that allows the PSAP to request a location update from the LRF.

16. The LRF returns the ESQK, the PSAP address or routeing information and location-information to the E-CSCF.

17. The E-CSCF uses the PSAP address or routeing information provided in Step 17 to send the call to the PSAP. The call request is either sent via an MGCF/MGW in the PSTN towards a PSTN-capable PSAP (not shown) or is sent directly as a SIP INVITE towards an IP-capable PSAP.

18. The rest of the call establishment procedure occurs between the UE, VMSC, E-RUA/DTF, E-CSCF and PSAP based upon the VCC CS origination procedure described in TS 23.206 [3].

6.1.4.1.2.4 Calls established in the CS domain without the use of a logical signalling control channel

Figure 6.1.4.1.2.4-1 provides an example flow for an emergency established in the CS domain when the Gm reference point is not available and the UE is attached to an MSC server enhanced for ICS. In this flow, the MSC Server recognises the CS bearer set-up as a request to make an emergency call and carries out the standard emergency call CS procedures prior to routeing the call to the visited IMS network.

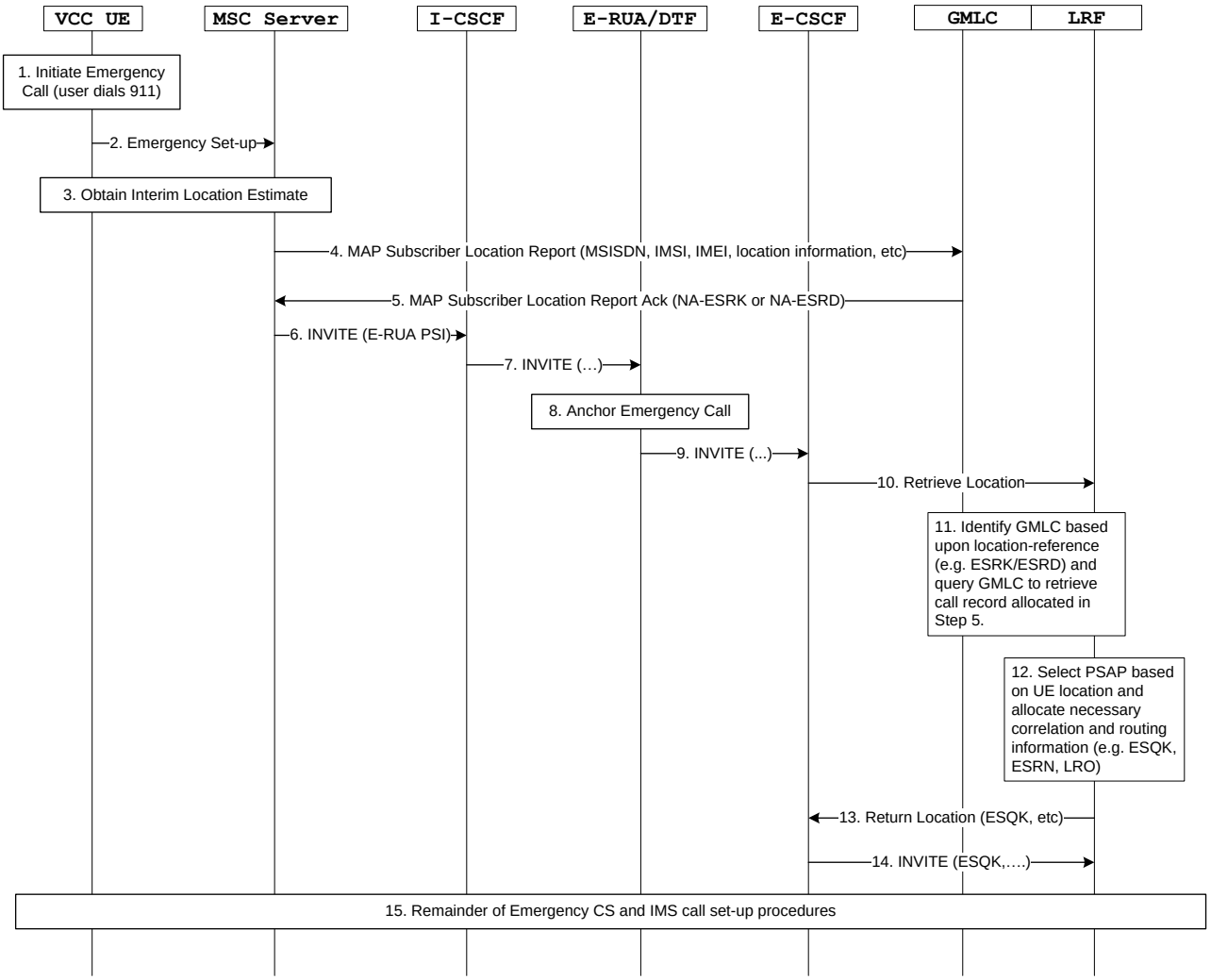


Figure 6.1.4.1.2.4-1: VCC UE initiating an emergency call in CS in when attached to an MSC server enhanced for ICS and without the use of a logical control channel

NOTE 1: This call flow is depicting the LRF acting in Re-direct mode. The procedure is also applicable when the LRF acts in Proxy mode.

1. The user initiates an emergency call (e.g. dials 911).

2. The UE sends an Emergency Set-up request to the MSC Server.

3. The VMSC may initiate a procedure in the RAN to obtain an interim location estimate for the UE as defined and allowed in TS 23.271 [11].

4. The MSC Server applies priority to the call and executes the emergency call procedures in the CS domain by sending a MAP Subscriber Location Report (SLR) request to the GMLC allocated to the geographical region that the UE is roaming within. The MAP Subscriber Location Report carries the IMSI, MSISDN, IMEI, VMSC address, and serving cell identity or SAI for the UE. It also includes any interim location estimate obtained in step 3.

5. Based on the received information, the GMLC creates a call context, stores the received location information and returns the MAP-SLR response to the VMSC.

6. When the MSC Server receives the MAP-SLR response, it is still running the call context for the CS Emergency call. The MSC Server is configured to route the call towards an I-CSCF in the visited IMS network using an E-RUA PSI DN.

Steps 7-15 in Figure 6.1.4.1.2.4-1 are the same as steps 10-18 in Figure 6.1.4.1.2.2-1.

When the UE is attached to a MSC Server not enhanced for ICS, standard CS emergency procedures are applied and the call is routed to a PSAP in the CS domain.

NOTE 2: Access Transfers for calls established via a standard MSC Server not enhanced for ICS without the use of logical control channel are not supported.

6.1.4.2 Domain Transfer from IMS to CS – Alternative 1

Figure 6.1.4.2-1 provides an example flow for domain transfer of an emergency session from IMS towards the CS domain.

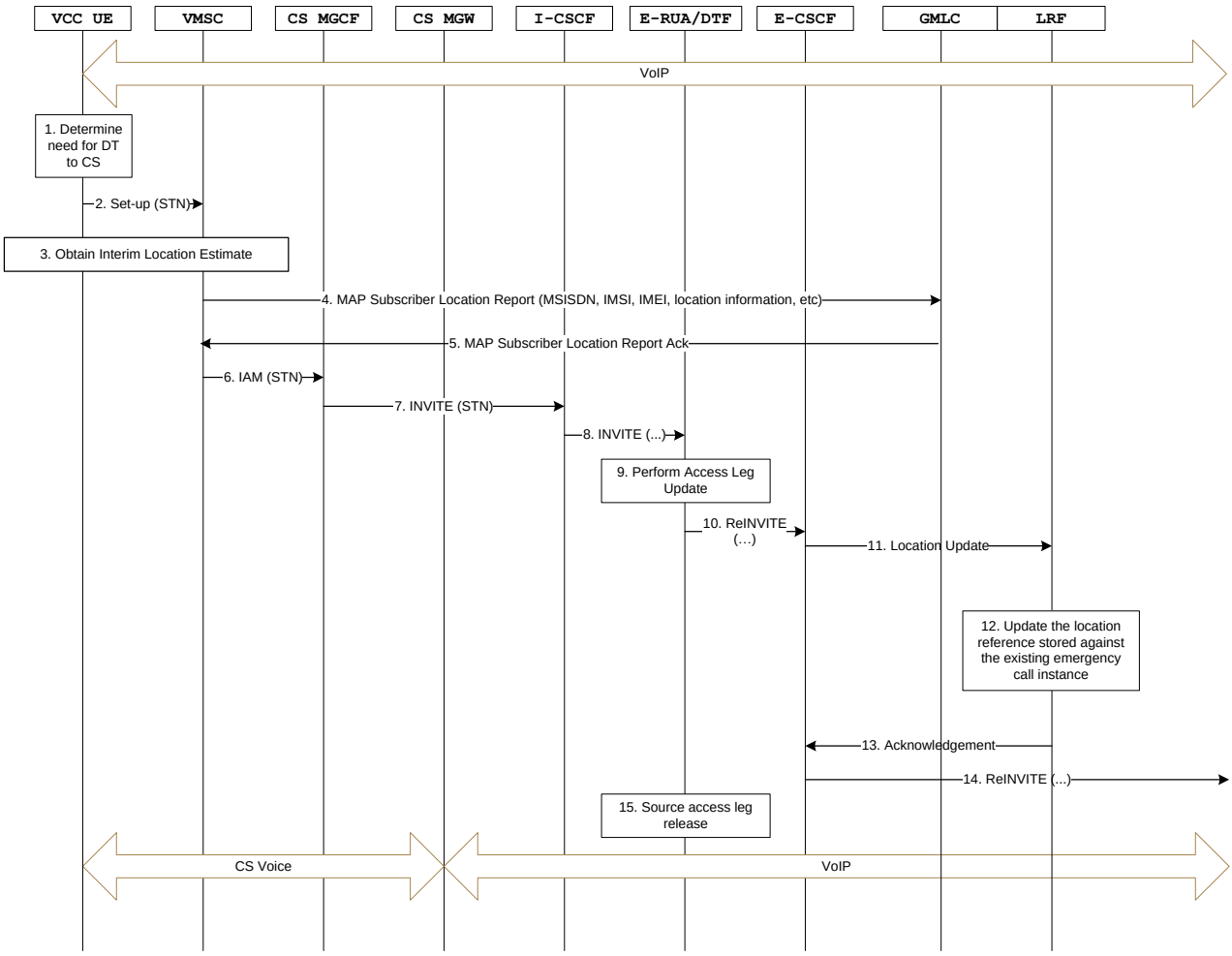


Figure 6.1.4.2-1: VCC UE performing domain transfer from IMS to CS domain

1. The UE detects the necessary conditions and determines the need for domain transfer.

2. The UE establishes the transfer leg of the emergency session towards the E-RUA by setting up a call in the CS domain towards the Session Transfer Number (STN) downloaded as part of the original PS emergency establishment or by using the PSI DN that was obtained on CS attach.

3. The VMSC may initiate a procedure in the RAN to obtain an interim location estimate for the UE as defined and allowed in TS 23.271 [11].

4. The serving network (i.e. VMSC) recognises the STN as a request to make a Session Transfer for CS emergency call and carries out standard CS emergency procedures. This involves the VMSC sending a MAP Subscriber Location Report (SLR) request to the GMLC allocated to the geographical region that the UE is roaming within. The MAP Subscriber Location Report carries the IMSI, MSIDN, IMEI, VMSC address and serving cell identity or SAI for the UE. It also includes any interim location estimate obtained in step 3.

5. Based on the received information, the GMLC creates a call context, stores the received location information and sends the MAP SLR response to the VMSC.

6. When the VMSC receives the MAP SLR response, it is still running the call context for the CS Emergency call. The VMSC routes the call to the MGCF based upon the routeing configuration at the VMSC.

NOTE 1: Modifications are required at the VMSC to route the session using the E-RUA DN rather than the ESRK/ESRD after the standard emergency call procedures have been invoked at the VMSC.

7. The MGCF initiates an INVITE towards an I-CSCF in the visited network by inter-working the PSI DN to a PSI Tel-URI and setting it as the Request-URI. The INVITE contains the identity of the UE (e.g. MSISDN Tel-URI as P-Asserted-Identity) and the location reference.

8. The I-CSCF may contact the HSS (not shown) to retrieve the E-RUA address associated with the PSI Tel-URI. Once the I-CSCF has obtained the address, it sends the INVITE to the E-RUA/DTF.

9. The DTF identifies the anchored call/session from the user identity and then completes the establishment of the Access Leg via the CS domain.

NOTE 2: A new emergency session request received at the E-RUA/DTF while there's already an active emergency session is considered a Domain Transfer request as there can only be one emergency session for a user at any given time.

NOTE 3: In the case where the E-RUA receives a Domain Transfer request at a different E-RUA from the one that anchored the call, this may result in possible re-anchoring and being connected to a new PSAP operator. This issue shall not occur based upon the recommendation that VCC for Emergency should only occur if the visited-IMS and CS core network operators are the same. Additionally, it is assumed that all the MSCs in the CS core network are configured with the appropriate translations to route the Domain Transfer request to the same E-RUA based upon the STN.

10. The E-RUA/DTF then performs the domain transfer by updating the remote leg with the connection information (SDP) of the newly established Access Leg by sending a Re-INVITE to the E-CSCF with the updated location reference.

11. The E-CSCF sends a Location Update request to the LRF that is associated with the geographical region to update the LRF with the new location reference for the UE due to the domain transfer. This request minimally includes the UE identification (contents of the P-Asserted-Identity) and the location-reference (e.g. contents of PIDF-LO and/or the P-Access-Network-Info), etc.

12. The LRF finds the emergency call instance using the information supplied in the Re-INVITE and updates the location reference stored against the emergency call instance.

13. The LRF sends an acknowledgment back to the E-CSCF to allow the E-CSCF to forward the Re-INVITE to the currently allocated PSAP.

14. The E-CSCF forwards the Re-INVITE to the MGCF associated with the PSAP (if the PSAP is located in the PSTN) or the Re-INVITE is sent directly to an IP-capable PSAP (i.e. the u-plane path between the UE and the PSAP is switched end-to-end).

15. When session modification procedures complete, the source access leg (i.e. the access leg previously established over IMS) is released.

NOTE 4: Releasing the source access leg does not result in releasing the resources (e.g. ESQK) allocated to the emergency call.

6.1.4.3 Domain Transfer from IMS to CS – Alternative 2

Figure 6.1.4.3-1 provides an alternative flow for domain transfer of an emergency session from IMS towards the CS domain, using the Gm reference point.

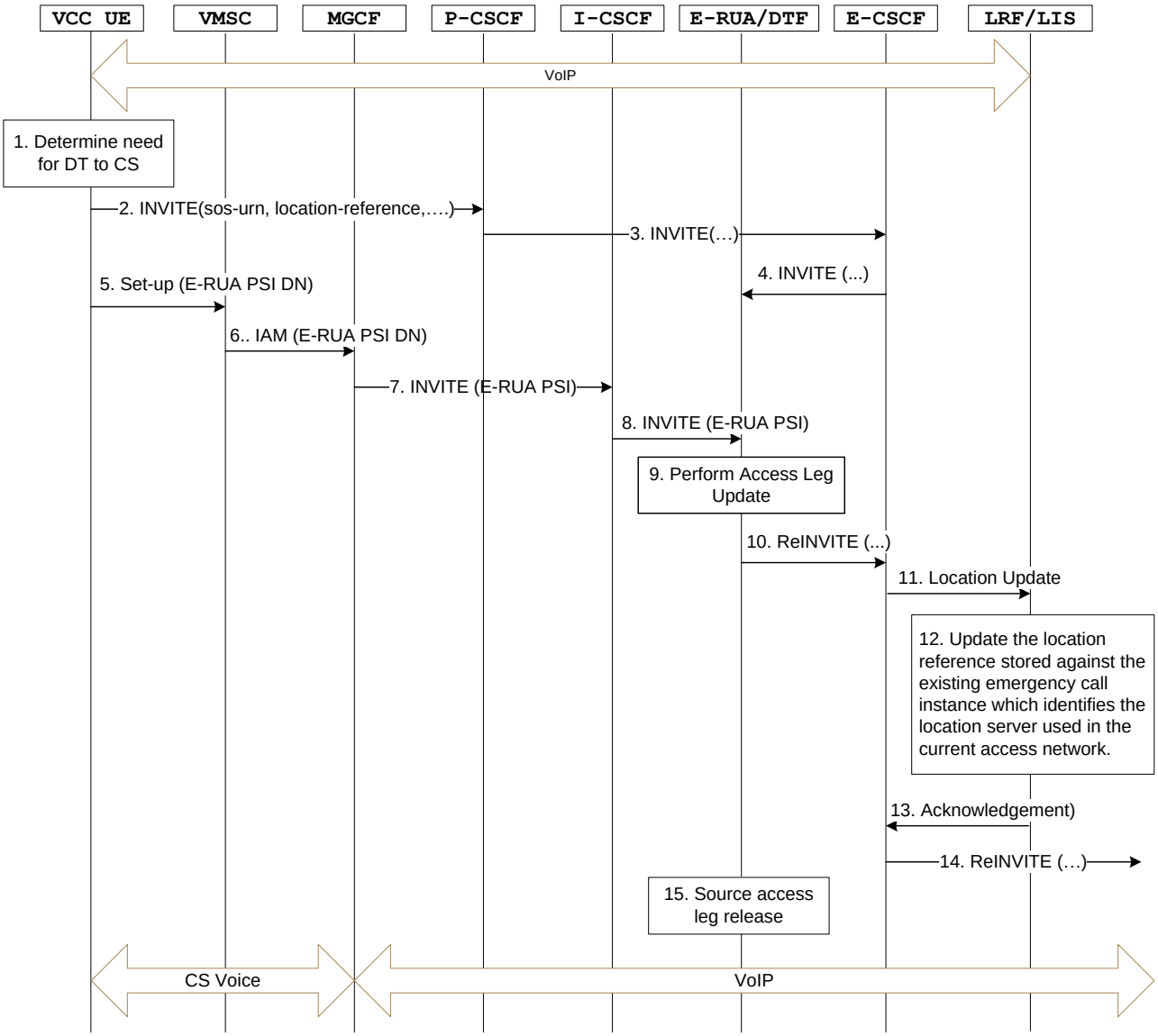


Figure 6.1.4.3-1: VCC UE performing domain transfer from IMS to CS domain with use of Gm reference point (Alternative 2)

NOTE 1: Steps 2-4 and 5-8 may occur in sequence or in parallel.

1. The UE detects the necessary conditions and determines the need for domain transfer

NOTE 2: The UE performs an IMS emergency registration for the same IMPI/IMPU in the new PS access. The S-CSCF will need to support multiple simultaneous emergency registrations for the same IMPI/IMPU.

2. The UE sends a request for domain transfer from IMS to CS by setting up an IMS originated Emergency session (towards the P-CSCF). This establishes the transfer leg of the emergency call (i.e. the new access leg via CS). The INVITE may also include updated location information for the UE.

3. The P-CSCF routes the INVITE to the E-CSCF.

NOTE 3: The P-CSCF may instigate a procedure (as described in TS 23.167 [4]) to obtain the location reference from the IP-CAN.

4. The E-CSCF sends the INVITE to the E-RUA/DTF.

5. The UE sends a normal Setup message (as defined in TS 24.008 [12]) to the VMSC using the E-RUA PSI DN that was originally downloaded to UE when the call was originally established in PS access, as shown in Steps 14-17 of Figure 6.1.4.1.1-1.

6. The VMSC routes the call towards IMS by sending an IAM to the MGCF containing the E-RUA PSI DN

7. The MGCF initiates an INVITE towards an I-CSCF in the visited network by inter-working the E-RUA PSI DN to a PSI Tel-URI and setting it as the Request-URI. The INVITE contains the identity of the UE (e.g. MSISDN Tel-URI as P-Asserted-Identity).

8. The I-CSCF may contact the HSS (not shown) to retrieve the E-RUA address associated with the PSI Tel-URI. Once the I-CSCF has obtained the address, it sends the INVITE to the E-RUA/DTF.

9. The DTF identifies the anchored call/session from the user identity and then completes the establishment of the Access Leg via the CS domain.

NOTE 4: A new emergency session request received at the E-RUA/DTF while there's already an active emergency session is considered a Domain Transfer request as there can only be one emergency session for a user at any given time.

NOTE 5: In the case where the E-RUA receives a Domain Transfer request at a different E-RUA from the one that anchored the call, this may result in possible re-anchoring and being connected to a new PSAP operator. This issue shall not occur based upon the recommendation that VCC for Emergency should only occur if the visited-IMS and CS core network operators are the same. Additionally, it is assumed that all the MSCs in the CS core network are configured with the appropriate translations to route the Domain Transfer request to the same E-RUA based upon the STN.

10. The E-RUA/DTF then performs the domain transfer by updating the remote leg with the connection information (SDP) of the newly established Access Leg by sending a Re-INVITE to the E-CSCF with the updated location reference.

11. The E-CSCF sends a location update request to the LRF containing the location reference for the new access network. The request also contains information that enables the LRF to identify the existing emergency call instance.

12. The LRF updates the existing location reference in the emergency call instance with the one provided in the location update request.

13. The LRF sends an Acknowledgement back to the E-CSCF.

14. The E-CSCF forwards the Re-INVITE to the MGCF associated with the PSAP (if the PSAP is located in the PSTN) or the Re-INVITE is sent directly to an IP-capable PSAP (i.e. the u-plane path between the UE and the PSAP is switched end-to-end).

15. When session modification procedures complete, the source access leg (i.e. the access leg previously established over IMS) is released.

NOTE 6: Releasing the source access leg does not result in releasing the resources (e.g. ESQK) allocated to the emergency call.

Figure 6.1.4.3-2 provides a similar flow to that of Figure 6.1.4.3-1 but uses an MSC Server Enhanced for ICS. This flow is similar in nature to Figure 6.1.4.1.2.2-2 in that the LRF may receive UE location information from both the CS and PS access.

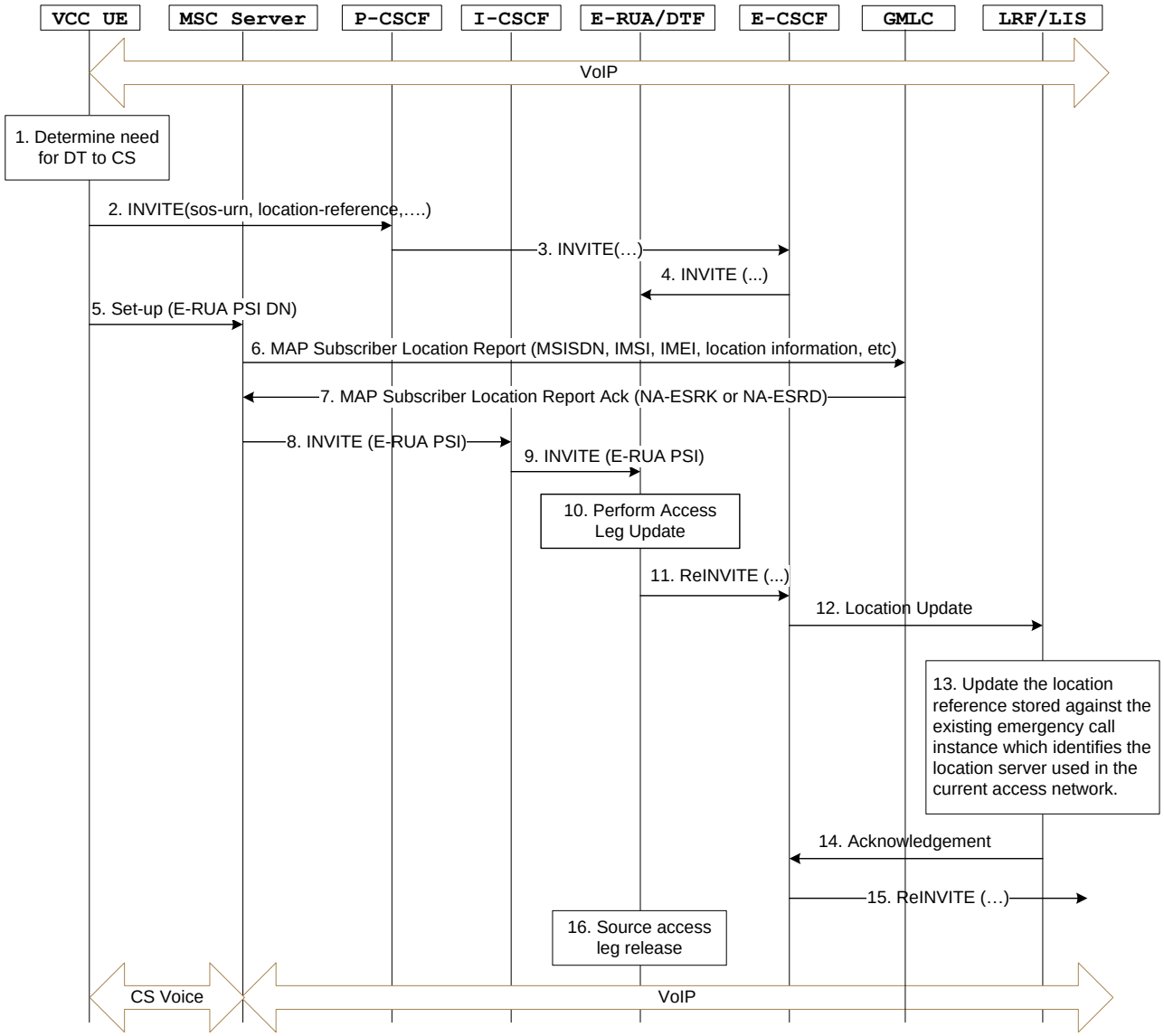


Figure 6.1.4.3-2: VCC UE performing domain transfer from IMS to CS domain with use of Gm reference point and an ICS Enabled MSC (Alternative 2)

6.1.4.4 Domain Transfer from IMS to CS – Alternative 3

Figure 6.1.4.4-1 provides an alternative flow for domain transfer of an emergency session from IMS towards the CS domain, when the Gm reference point is not available and when the UE is attached to a MSC server enhanced for ICS.

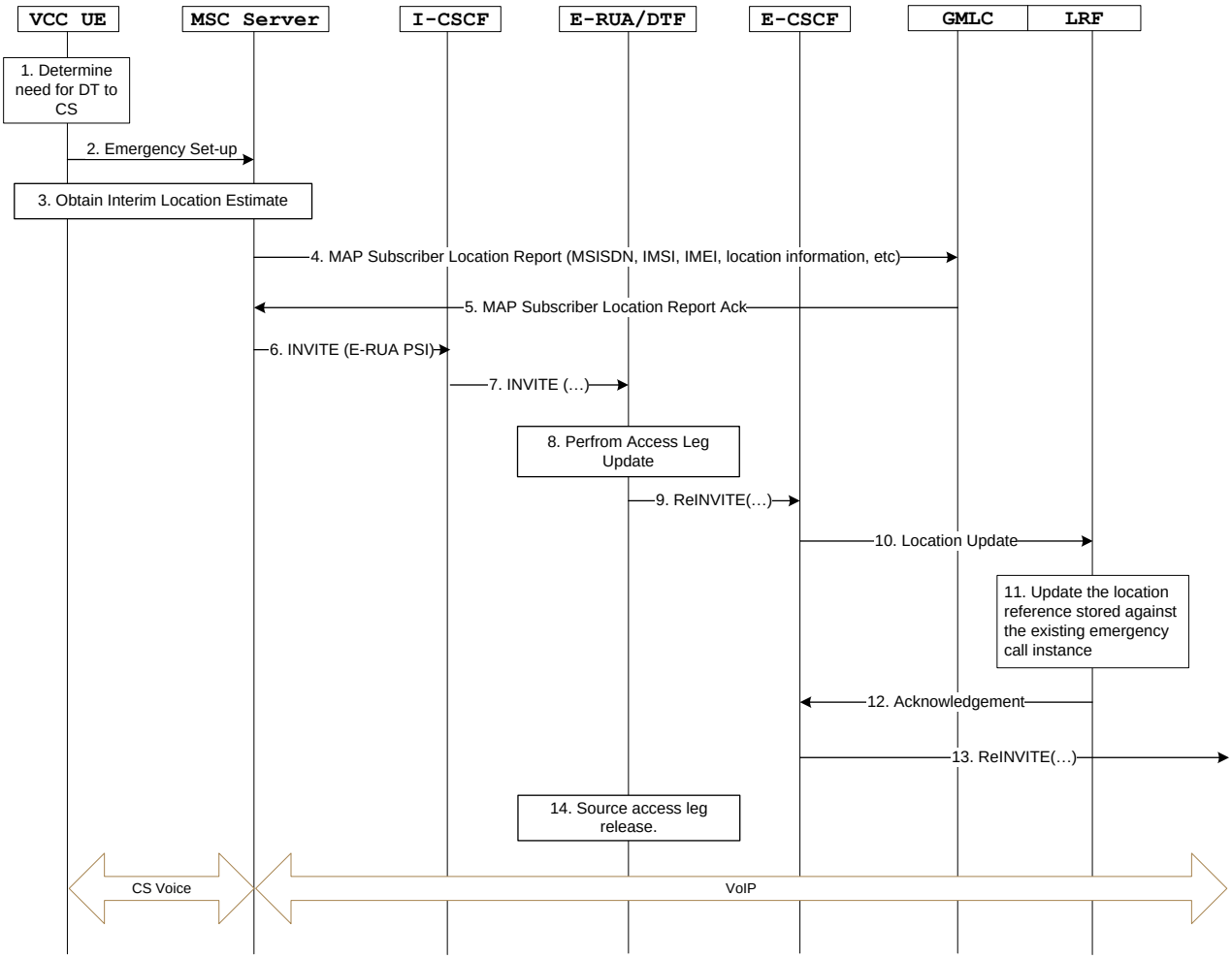


Figure 6.1.4.4-1: VCC UE performing domain transfer from IMS to CS domain when Gm reference point is not available and with use of an ICS Enabled MSC (Alternative 3)

1. The UE detects the necessary conditions and determines the need for domain transfer.

2. The UE establishes the transfer leg of the emergency session towards the E-RUA by setting up an emergency call in the CS domain.

3. The MSC Server may initiate a procedure in the RAN to obtain an interim location estimate for the UE as defined and allowed in TS 23.271 [11].

4. The MSC Server applies priority to the call and executes the emergency call procedures in the CS domain by sending a MAP Subscriber Location Report (SLR) request to the GMLC allocated to the geographical region that the UE is roaming within. The MAP Subscriber Location Report carries the IMSI, MSISDN, IMEI, VMSC address, and serving cell identity or SAI for the UE. It also includes any interim location estimate obtained in step 3.

5. Based on the received information, the GMLC creates a call context, stores the received location information and returns the MAP-SLR response to the VMSC.

6. When the MSC Server receives the MAP-SLR response, it is still running the call context for the CS Emergency call. The MSC Server is configured to route the call towards an I-CSCF in the visited IMS network using an E-RUA PSI DN.

   Steps 7-14 in Figure 6.1.4.4-1 are the same as steps 8-15 in Figure 6.1.4.2-1.

Figure 6.1.4.4-2 provides a similar flow to that of Figure 6.1.4.4-1 but uses an MSC Server not enhanced for ICS.

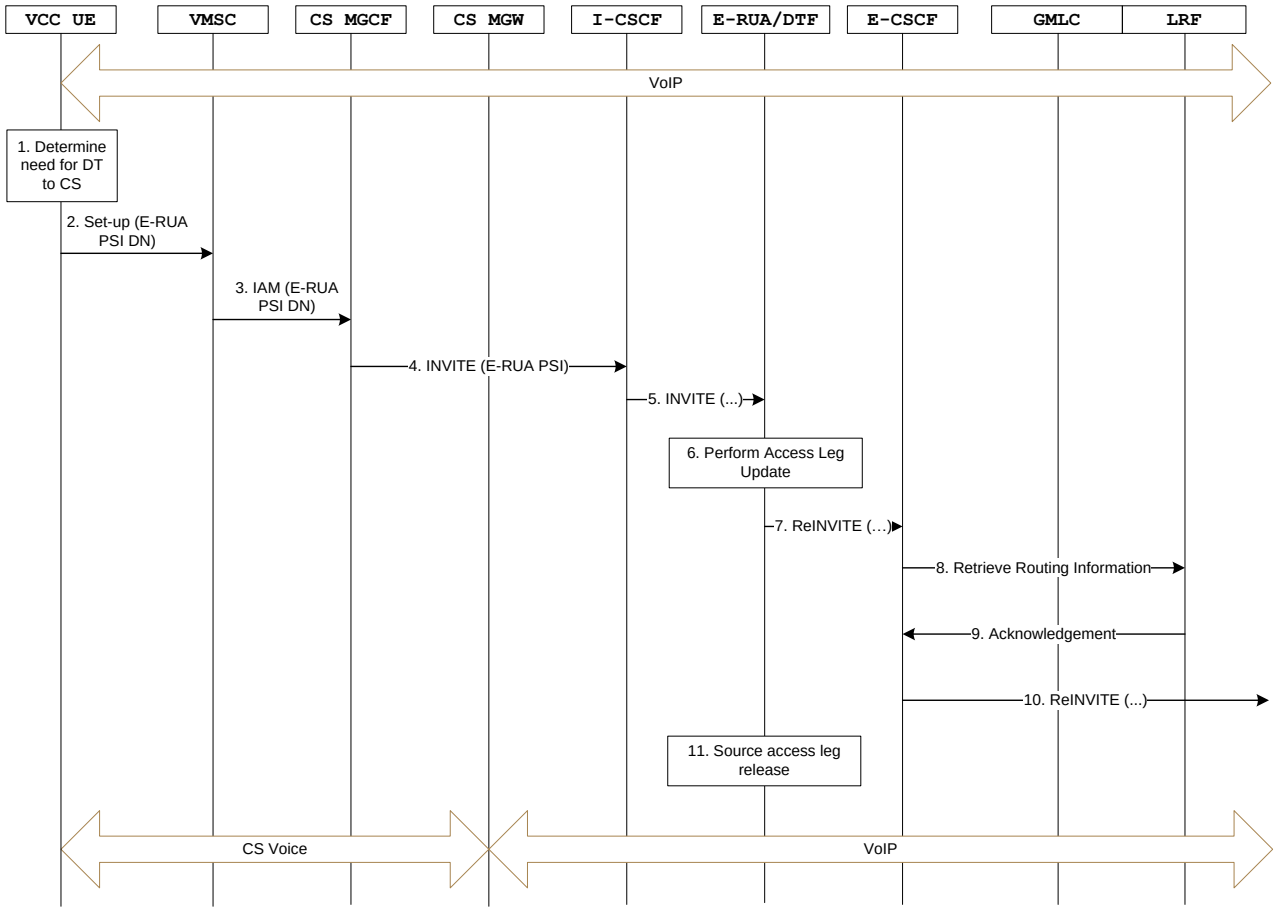


Figure 6.1.4.4-2: VCC UE performing domain transfer from IMS to CS domain when Gm reference point is not available and with use of a MSC not enhanced for ICS (Alternative 3)

1. The UE detects the necessary conditions and determines the need for domain transfer.
2. The UE establishes the transfer leg of the emergency session towards the E-RUA by setting up a call in the CS domain using the E-RUA PSI DN.
3. The MSC Server not enhanced for ICS is configured to route the call to an MGCF in the visited-IMS network.
4. The MGCF initiates an INVITE towards an I-CSCF in the visited network by interworking the PSI DN to a PSI Tel-URI and setting it as the Request-URI. The INVITE contains the identity of the UE (e.g. MSISDN Tel-URI as P-Asserted-Identity).
5. The I-CSCF may contact the HSS (not shown) to retrieve the E-RUA address associated with the PSI Tel-URI. Once the I-CSCF has obtained the address, it sends the INVITE to the E-RUA/DTF.
6. The DTF identifies the anchored call/session from the user identity and then completes the establishment of the Access Leg via the CS domain.

NOTE 1: A new emergency session request received at the E-RUA/DTF while there's already an active emergency session is considered a Domain Transfer request as there can only be one emergency session for a user at any given time.

NOTE 2: In the case where the E-RUA receives a Domain Transfer request at a different E-RUA from the one that anchored the call, this may result in possible re-anchoring and being connected to a new PSAP operator. This issue shall not occur based upon the recommendation that VCC for Emergency should only occur if the visited-IMS and CS core network operators are the same. Additionally, it is assumed that all the MSCs in the CS core network are configured with the appropriate translations to route the Domain Transfer request to the same E-RUA based upon the STN.

7 The DTF then performs the domain transfer by updating the remote leg with the connection information (SDP) of the newly established Access Leg by sending a Re-INVITE to the E-CSCF with the updated location reference.

8. The E-CSCF sends a request to the LRF that is associated with the geographical region to retrieve routeing information to route the request to the PSAP.

9. Routeing information (and optionally location information) is sent back to the E-CSCF.

10. The E-CSCF forwards the Re-INVITE to the MGCF associated with the PSAP (if the PSAP is located in the PSTN) or the Re-INVITE is sent directly to an IP-capable PSAP (i.e. the u-plane path between the UE and the PSAP is switched end-to-end).

11. When session modification procedures complete, the source access leg (i.e. the access leg previously established over IMS) is released.

NOTE 3: Releasing the source access leg does not result in releasing the resources (e.g. ESQK) allocated to the emergency call.

6.1.4.5 Domain Transfer from CS to IMS

Figure 6.1.4.5-1 provides an example flow for domain transfer of an emergency session from the CS domain towards IMS.

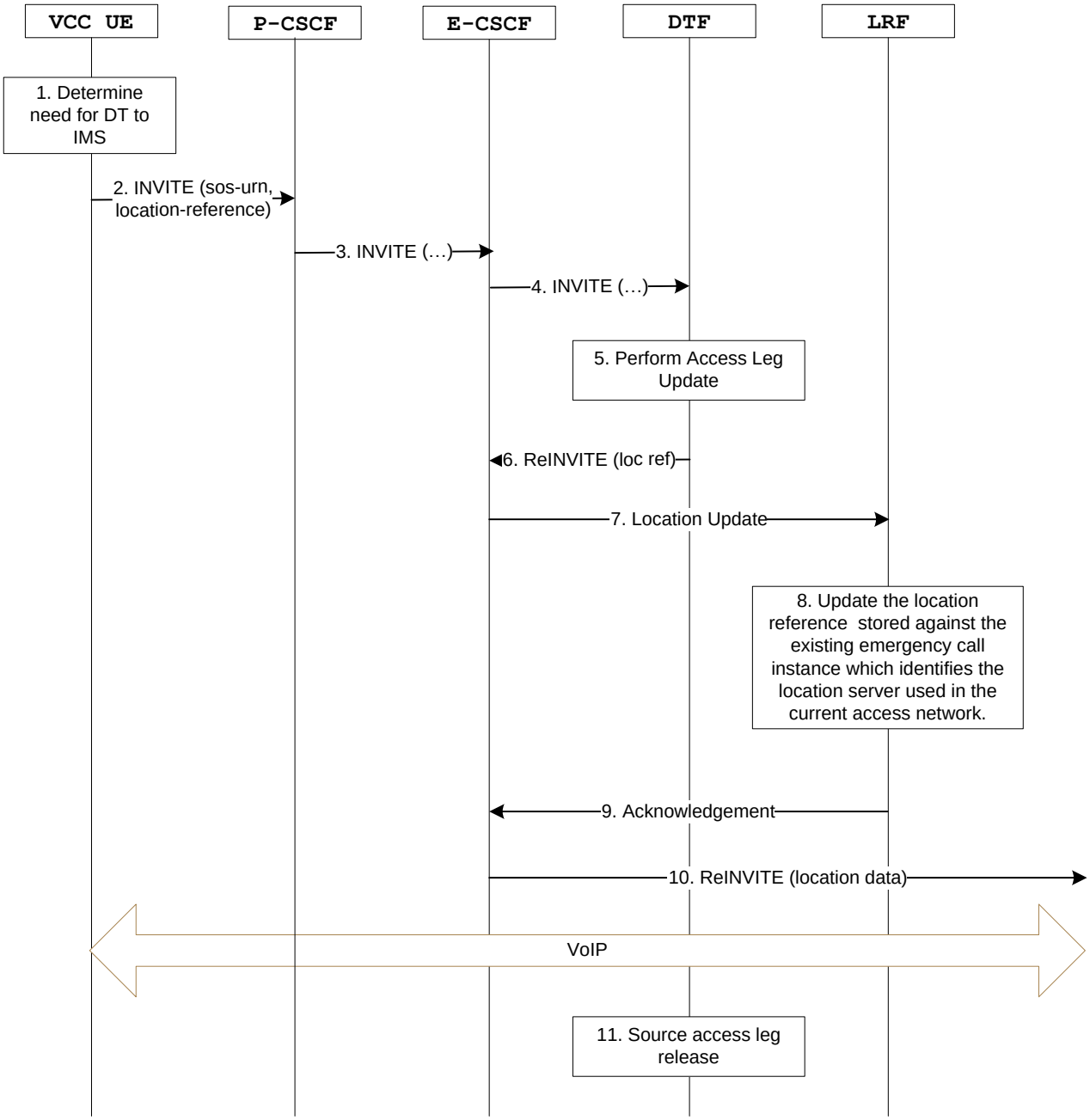


Figure 6.1.4.5-1: VCC UE performing domain transfer from CS domain to IMS

1. The UE detects the necessary conditions and determines the need for domain transfer.

NOTE 1: The UE performs an IMS emergency registration in the new visited IMS network if the UE is not already IMS emergency registered (e.g. the UE may already be IMS emergency registered in the case the UE is doing a domain transfer back to IMS). When the UE is located in the home network and is already IMS registered there is no need to perform an IMS emergency registration.

2. The UE sends a request for domain transfer from CS to IMS by setting up an IMS originated Emergency session (towards the P-CSCF). This establishes the transfer leg of the emergency call (i.e. the new access leg via IMS). The INVITE may also include updated location information for the UE.

NOTE 2: A new emergency session request received at the DTF while there's already an active emergency session is considered a Domain Transfer request as there can only be one emergency session for a user at any given time.

3. The P-CSCF routes the INVITE to the E-CSCF.

NOTE 3: The P-CSCF may instigate a procedure (as described in TS 23.167 [4]) to obtain the location reference from the IP-CAN.

4. The E-CSCF routes the INVITE to the DTF (as it is configured to send all requests for the VCC user to the DTF).

5. The DTF identifies the anchored call/session from the Request-URI and then completes the establishment of the Access Leg via IMS

NOTE 4: In the case where the E-RUA receives a Domain Transfer request at a different E-RUA from the one that anchored the call, this may result in possible re-anchoring and being connected to a new PSAP operator. This issue shall not occur based upon the recommendation that VCC for Emergency should only occur if the visited-IMS and CS core network operators are the same.

6. The DTF then performs the domain transfer by updating the remote leg with the connection information (SDP) of the newly established Access Leg by sending a Re-INVITE to the E-CSCF with the updated location information.

7. The E-CSCF sends a location update request to the LRF containing the location reference for the new access network. The request also contains information that enables the LRF to identify the existing emergency call instance.

8. The LRF overwrites the existing location reference in the emergency call instance with the one provided in the location update request. The LRF finds the most appropriate location server and positioning method for the current access network and stores this information against the currently allocated emergency call instance.

9. The LRF sends an Acknowledgement back to the E-CSCF

10. If the PSAP is located in the IP network, the Re-INVITE sent out by the E-CSCF is extended all the way to the PSAP (i.e. the u-plane path between the UE and the PSAP is switched end-to-end). If the PSAP is located in the PSTN, the E-CSCF forwards the Re-INVITE to the MGCF associated with the PSAP.

11. When session modification procedures complete, the source access leg (i.e. the access leg previously established over CS) is released.

NOTE 5: Releasing the source access leg does not result in releasing the resources (e.g. ESQK) allocated to the emergency call.

6.2 VCC in the Visited Network - Alternative 2

6.2.1 Architectural Details

Figure 6.2.1-1 shows a possible reference model based on Figure 6.4.1.2-1 in TS 23.206 [3]. The E-CSCF and DTF reside in the original visited IMS network. The visited network P-CSCF (which is also part of the model) is not shown in this figure.

NOTE 1: When the UE is not roaming the home IMS network becomes the visited IMS network.

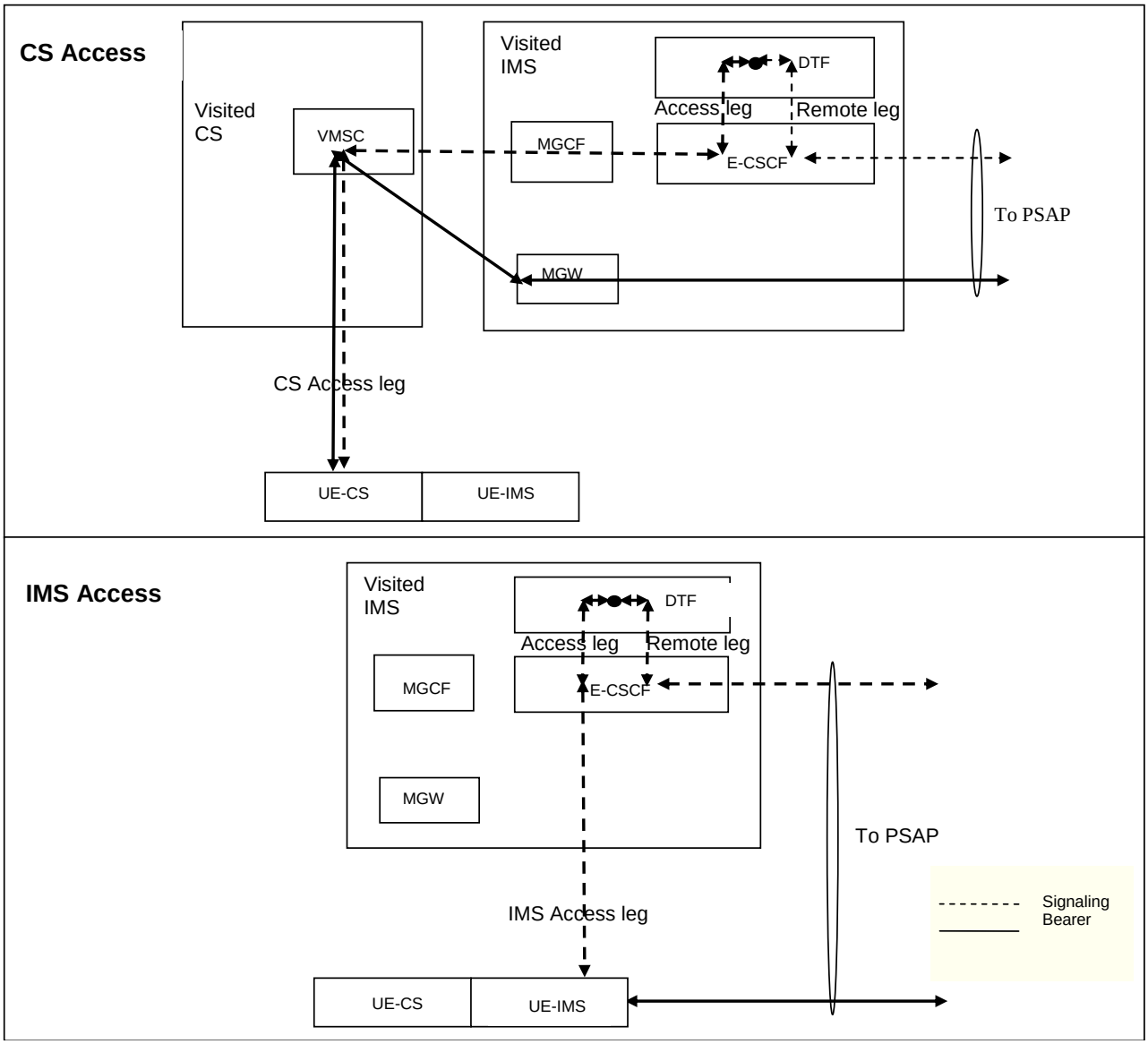


Figure 6.2.1-1: Possible Reference Model for VCC support for an IMS Emergency Call

NOTE 2: It is assumed that for CS access, the MGCF can adequately populate the information needed in a SIP INVITE from information received in an ISUP IAM in the case of emergency call origination from the CS domain or PS to CS domain transfer using a new emergency call origination form the CS domain. It is FFS whether an additional RUA and/or CS Access Function may be needed in the serving IMS to fully populate and correctly route the SIP INVITE and support the remainder of the call establishment or domain transfer in these cases.

The CS Access diagram above does not show all the components in the session path between the MGCF and the E-CSCF, e.g. the I-CSCF which handles the routeing of the PSI in IMS.

Figure 6.2.1-2 shows the same reference model as Figure 6.2.1-1 but from the perspective of the model defined in TS 23.167 [4] to support IMS Emergency calls. In this figure, the VCC DTF is added with an interface to the E-CSCF. The emergency call will be anchored in the VCC DTF. In addition, location support will be anchored in an LRF in the visited network such that the PSAP can continue to obtain updated location estimates from the same LRF following any change of domain. This LRF is referred to as the anchor LRF.

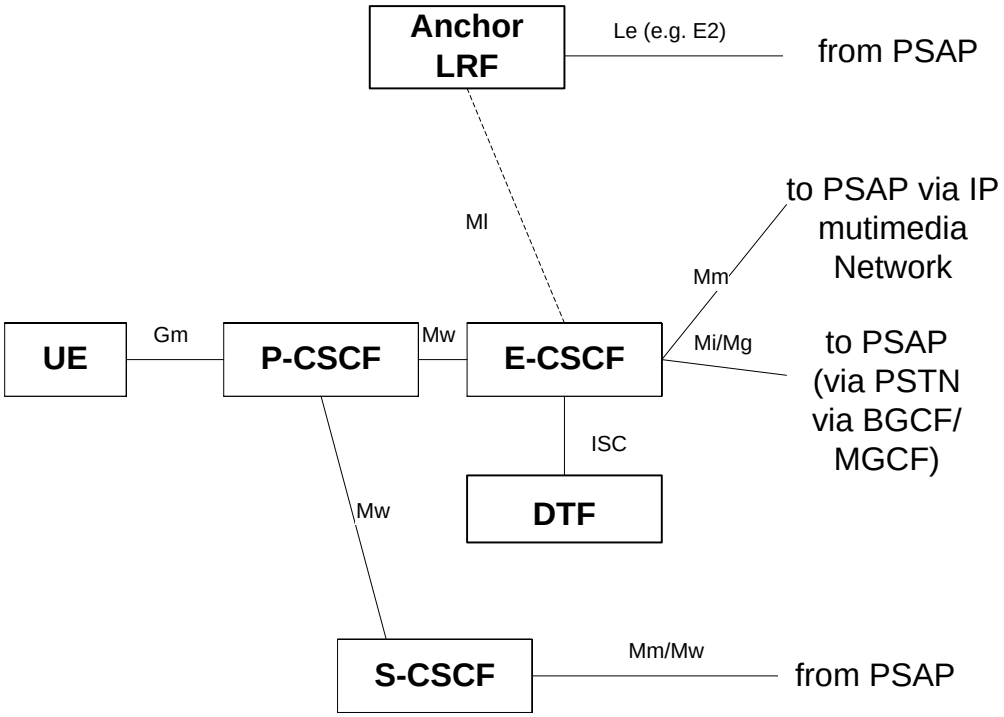


Figure 6.2.1-2: Modified architecture from TS 23.167 [4] perspective

6.2.2 Impact

6.2.2.1 Negotiation of VCC Support

For normal VCC defined in TS 23.206 [3], the network (e.g. S-CSCF and VMSC) is aware of the user's VCC capability from the user's subscription based information stored in the HSS/HLR (i.e. provisioned iFCs and CAMEL subscription). The UE uses a statically provisioned VDN (E.164 Voice Domain Transfer Number) and VDI (Voice Domain Transfer SIP URI) for domain transfer.

For VCC for IMS Emergency, the visited network needs to be aware of the VCC capability of the user. This may be achieved using one of the following alternatives:

a) If the visited network is the home network for the UE, it may discover UE VCC capability from subscription information for the user.

b) The visited network (e.g. E-CSCF) may assume that all UEs are VCC capable (whether or not any particular UE actually is).

c) The visited network (e.g. E-CSCF and GMLC) may be configured with either the identities of particular networks all of whose UEs can be assumed to support VCC or the identities of particular UEs (e.g. belonging to roaming partners) who can be assumed to support VCC.

d) The UE may include information in call establishment and/or registration related messages - e.g. in a SIP INVITE or DTAP SETUP or DTAP EMERGENCY SETUP message. In the case of an EMERGENCY SETUP message, 3 currently unused bits exist in the optional Service Category IE that could be used for this - e.g. 2 of these bits could distinguish call origination with or without VCC support from VCC domain transfer. Another alternative would be to send a normal SETUP message rather than an EMERGENCY SETUP message in which different called party numbers were used to designate an emergency call, support of VCC and distinguish call origination from domain transfer - similarly to the proposals for Alternative 1 in clause 6.1. Defining such numbers globally is probably infeasible but it might be possible to configure the UE with numbers specific to certain networks or, alternatively, a called party number specific to domain transfer might be returned to a UE as a modified VDN as described in clause 6.2.2.3.

Editor's Note: Details of how (a) could be supported are FFS.

With alternative (b), the visited network assumes that the UE is VCC capable and assigns VCC resources when the emergency call is originated. VCC resources would then be wasted for UEs that were not VCC capable. For emergency calls originated in the PS domain the wastage may be small, because the number of such calls will generally be a very small proportion of all IMS calls in the PS domain. In addition, if alternative (a) is combined with alternative (b) such that the visited network assumes UE VCC capability only if it is not the home network, the wastage is further reduced. However, for CS originated emergency calls, there will probably be a higher level of wastage because most CS emergency calls, at least initially, will come from legacy UEs not capable of supporting VCC.

With alternative (c), a particular operator may agree to provide VCC support to the UEs belonging to certain other operators as part of normal roaming agreements.

With alternative (d), the visited network can be sure of UE support or non-support at the expense of some impacts to the UE and possibly to the IP-CAN - e.g. the MSC will be impacted to support any extension to the optional Service Category IE. Alternative (d) also allows the possibility of distinguishing a SIP INVITE or DTAP EMERGENCY SETUP message that is sent to originate an emergency call from one that is sent to perform a domain transfer.

Alternatives (a), (b) and (c) avoid adding new impacts to the UE, which is desirable to enable a common VCC solution, from the perspective of the UE, for both emergency and non-emergency calls.

To convey to the UE that the visited network is VCC capable and transfer the VDN and VDI, the following alternatives are possible.

e) The UE discovers visited network VCC capability (and VDN and VDI) from system broadcast messages.

Editor's Note: Further details of this are FFS.

f) The UE discovers the visited network VCC capability and the VDN and VDI where needed using DHCP or using HTTP or HTTPS from a server in the visited network whose role is to provide information related to emergency calls (e.g. including also local emergency numbers).

Editor's Note: Adoption of this alternative implies some further architectural enhancement (e.g. a new server).

g) The home network downloads information to the UE, or to the UICC, concerning networks that are known to support VCC for emergency calls. For example, the home network could provide the UE with the MCC and MNC of all known networks that support VCC for emergency calls. Additional information, such as the VDNs and VDIs use by such networks, could also be provided.

Editor's Note: Further details of this are FFS.

h) Use of SIP (e.g. UE Subscribe/Notify after call set up or use of 200 OK).

Editor's Note: Further details of this are FFS.

Alternative (e) would be suitable for UMTS, GPRS and GSM networks and may be suitable for WLANs.

Alternative (f), which is applicable to IMS but not CS originated calls could be combined with the provision of local emergency numbers to a UE from some server in the visited network. The address of this server could be obtained by the UE using either DHCP or a DNS query on some known FQDN containing the visited network's known domain name and some fixed user name – e.g. "emergency-support@<visited network domain>"). As a variant, VCC capability (and VDN and VDI addresses if needed) could be signalling directly if and when the UE uses DHCP to discover the P-CSCF and DNS server addresses. The impacts of such a solution remain to be quantified and evaluated.

Alternative (g) can be valid for all UEs but may require protocol enhancements between the home network and the UE.

Alternative (h) is available when an emergency call is originated in IMS. Further study is required when the call is originated in CS.

6.2.2.2 Domain Transfer

Domain transfer can occur in a very similar manner to that for normal VCC as defined in TS 23.206 [3].
Figures 6.2.2.2-3 and 6.2.2.2-4 are modifications of Figures 6.4.1.3-1 and 6.4.1.3-2 in TS 23.206 [3] showing switching of the user plane for IMS emergency calls to an IP capable PSAP and a CS (PSTN) capable PSAP, respectively.

NOTE: Some elements are missing or may be missing from both figures - e.g. I-CSCF and possibly RUA or CSAF between the I-CSCF and E-CSCF in the case of CS domain access - and need to be included once validated by further study.

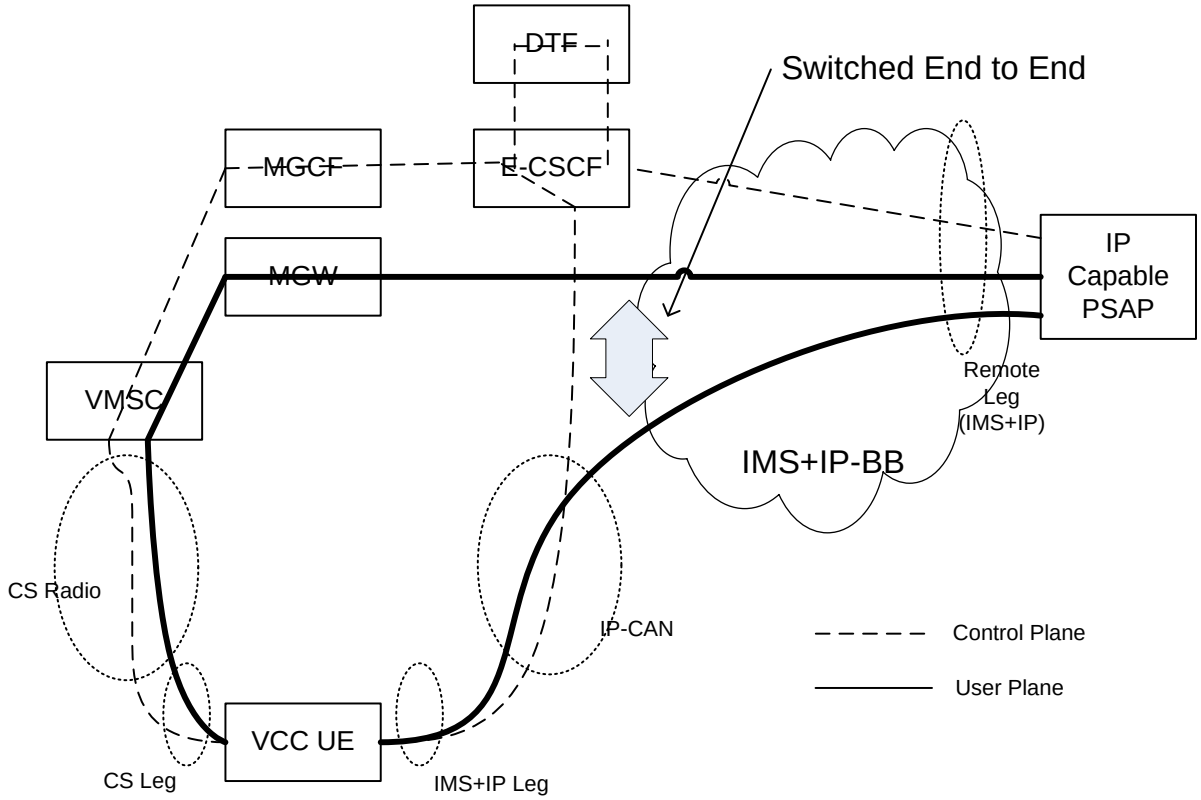
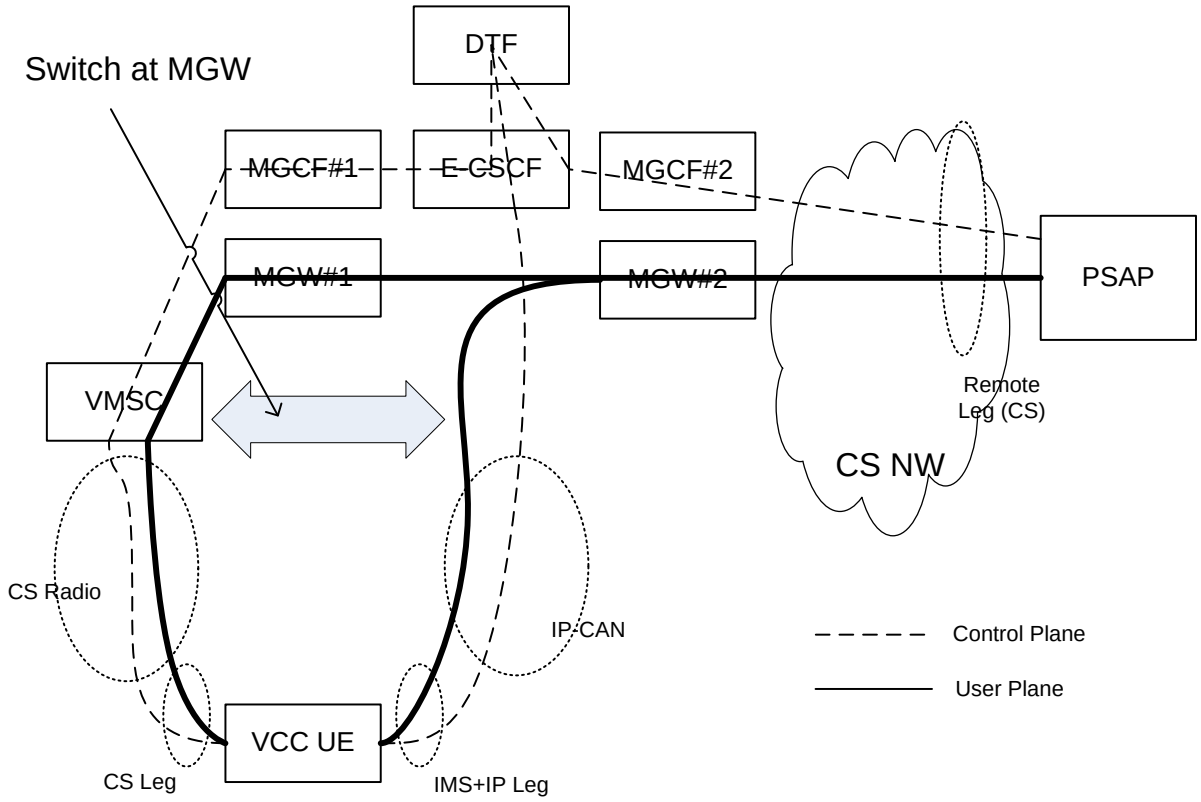


Figure 6.2.2.2-3: U-plane path between VCC UE and IP Capable PSAP



NOTE: MGW#1 and MGW#2 may be merged.

Figure 6.2.2.2-4: U-plane path between VCC UE and CS Capable PSAP

6.2.2.3 Modified VDN and VDI

Similar to the concept of a Session Transfer Number (STN) for solution alternative 1 in clause 6.1, the VDN and VDI could be modified to enable domain transfer in the context of emergency call recognition and treatment. In the case of the VDN, a VPLMN could assign a modified VDN (and provide it to the UE via one of the mechanisms described in clause 6.2.2.1) that would be recognized by an MSC as an emergency number thereby triggering a MAP query with a GMLC as described further down in clause 6.2.4.4.

To convey to a GMLC that a MAP SLR concerns a request for domain transfer as opposed to a new CS emergency call, a new parameter or parameter value might be included in the MAP SLR. Note that as an alternative, information at the SCCP level might be used although that is not preferred due to dependence on implementation support. With the SCCP alternative, a different GMLC SCCP E.164 address might be configured in the MSC in association with a modified VDN to implicitly inform the GMLC that the MAP SLR was associated with an existing emergency call (as opposed to a new emergency call) for which a domain transfer was requested. The E.164 address would need to be transferred (as an SCCP called party global title address) end-to-end to the GMLC (which is allowed though not guaranteed by SCCP) and could select a distinct process in the GMLC to process the MAP SLR or otherwise inform the GMLC that the MAP SLR is associated with a request for domain transfer.

NOTE 1: The received E.164 address needs to indicate to the GMLC that a MAP SLR refers to a request for domain transfer as opposed to a new originating call.

NOTE 2: It is assumed that translations in the network will not change.

In the case of a modified VDI, a URI (e.g. SIP URI) could be assigned by the VPLMN or defined globally that indicated a request for domain transfer for an existing emergency call. This could be used for the domain transfer procedure described in clause 6.2.4.6. A PLMN assigned VDI would need to be provided to the UE (e.g. using any of the methods described in clause 6.2.2.1) although a globally defined VDI would not.

The significance of using a modified VDN and VDI (and a reason for retaining the existing VDN and VDI terms) is that from the UE perspective, domain transfer could proceed (mostly or entirely) as for normal VCC defined in TS 23.206 [3].

The use of a modified VDN and/or modified VDI to support domain transfer may be used in combination with any of alternatives (a), (b), (c) and (d) in clause 6.2.2.1 to convey support of VCC by a UE to the VPLMN. Thus, for example, use of a modified VDN and VDI may be combined with conveyance of VCC support by the UE using spare bits in the optional Service IE in an Emergency Setup message (alternative (d)) or it may be combined with any of the other alternatives (a), (b) or (c).

6.2.3 Assessment

This clause defines three variants of alternative 2 that are considered suitable to support of PS to CS domain transfer in Release 9:

6.2.3.1 Variant A

This variant uses the IMS emergency call origination procedure defined in clause 6.2.4.1 in which the UE indicates VCC capability in the SIP INVITE and the VCC DTF returns a VDN in the SIP 200 OK. The procedure A defined in clause 6.2.4.3 is then used for IMS to CS domain transfer.

6.2.3.2 Variant B

This variant uses the IMS emergency call origination procedure defined in clause 6.2.4.1 in which the UE indicates VCC capability in the SIP INVITE and the VCC DTF returns an indication of VCC support in the SIP 200 OK. The procedure B defined in clause 6.2.4.4 is then used for IMS to CS domain transfer in which the UE sends an Emergency SETUP to the VMSC, the VMSC queries the GMLC using a MAP SLR as for a normal emergency call and the GMLC determines that this is a request for domain transfer by finding the call record in the LRF. The GMLC returns a routeing number to the VMSC to route the DT request.

6.2.3.3 Variant C

This variant uses the IMS emergency call origination procedure defined in clause 6.2.4.1 in which the UE indicates VCC capability in the SIP INVITE and the VCC DTF returns a modified VDN in the SIP 200 OK. The procedure B defined in clause 6.2.4.4 is then used for IMS to CS domain transfer in which the UE sends a normal SETUP to the VMSC containing the modified VDN in the called party number parameter. The modified VDN is either recognized by the VMSC as a request for domain transfer or is configured in the VMSC to cause a MAP SLR query to a distinct GMLC SCCP address. The GMLC recognizes the domain transfer from either the distinct SCCP address used by the VMSC or from a new indication included by the VMSC in the MAP SLR query. The GMLC returns a routeing number to the VMSC to route the DT request.

6.2.4 Procedures

In the following procedures, the VDN and VDI are assumed to be assigned by the visited IMS network (e.g. may be static in the visited network) and are thus not configured in the UE as for normal VCC defined in TS 23.206 [3].

Editor's Note: Assumptions and requirements concerning the involved network elements in these procedures (e.g. possible sharing of a GMLC among multiple service providers) remain to be specified in clause 6.2.2 (Impact).

6.2.4.1 IMS Emergency Call Origination

Emergency call origination could occur as defined in TS 23.167 [4] but with some changes to add negotiated usage of VCC. In particular, in order to preserve continuity of location support as well as continuity of the voice call following any domain transfer, the E-CSCF in the visited network would need to send the SIP INVITE (for the IMS emergency call) to the VCC DTF before invoking the LRF to obtain or verify location and select the destination PSAP. The VCC DTF would then anchor the incoming call leg and originate a new outgoing call leg through the E-CSCF towards the PSAP. On receiving the SIP INVITE from the VCC DTF, the E-CSCF would perform normal location and routeing as defined in TS 23.167 [4] and transfer the call to the PSAP either via IP or through an MGCF and the PSTN. This will result in the E-CSCF being part of the outgoing call leg from the DTF which means the LRF can remain associated with the outgoing call leg following any domain transfer and will thus be able to provide continuing support of location provided it is updated with new information regarding changes to the access network following any change of domain. Figure 6.2.4.1-1 illustrates the ensuing call origination procedure.

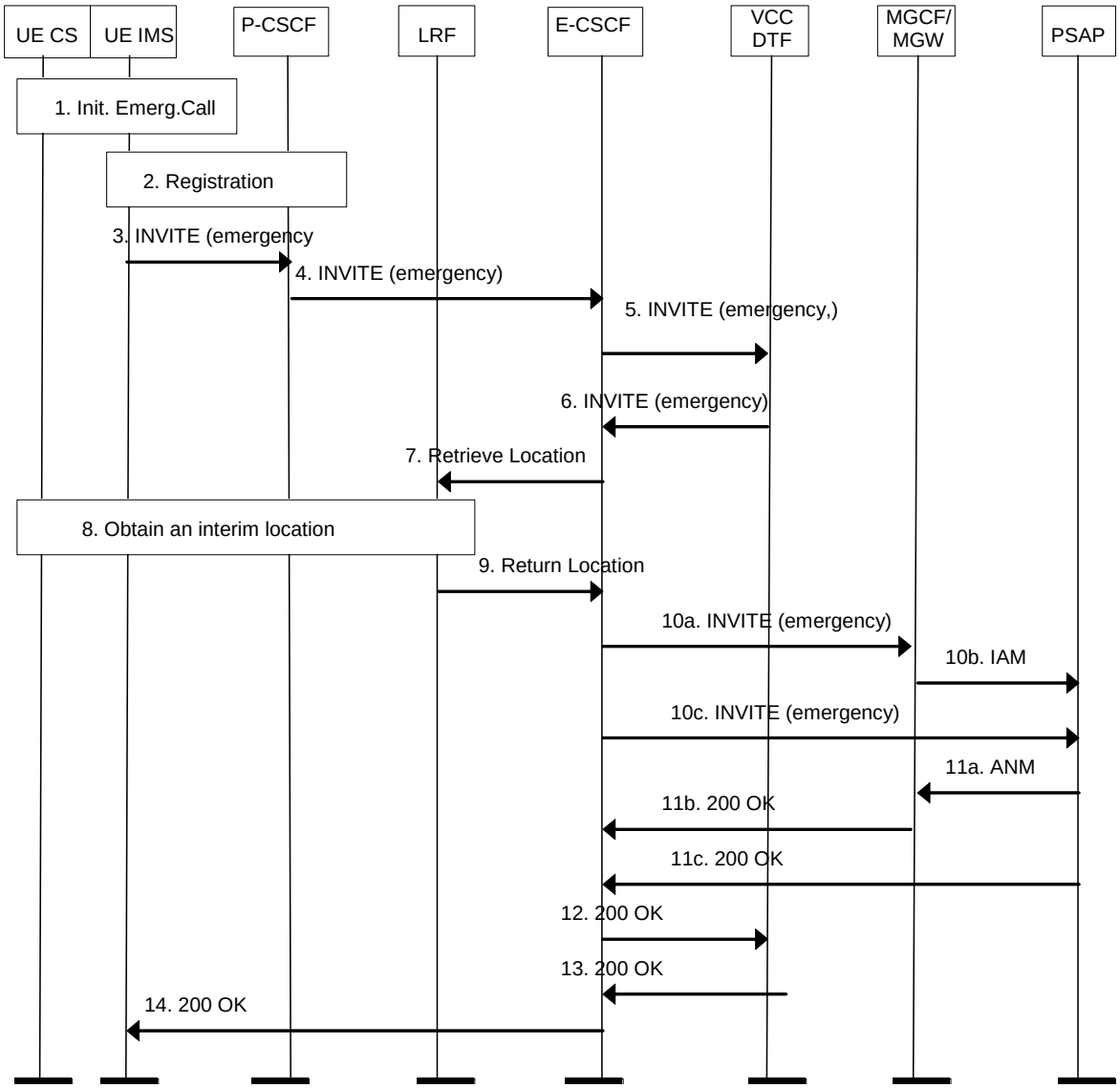


Figure 6.2.4.1-1: IMS Emergency Call Origination with VCC support

1. The user initiates an emergency call.

2. If the UE is roaming or if the UE is not roaming and not yet IMS registered, the UE performs an emergency registration procedure with the visited network P-CSCF and home network S-CSCF (not shown) as described in TS 23.167 [4] if it contains the necessary credentials.

3. The UE sends an INVITE with an emergency indication to the visited network P-CSCF. The INVITE may contain any location objects that the UE has. The INVITE should contain identification information for the UE - e.g. public user SIP URI and Tel URI. The INVITE may indicate that the UE supports VCC and may indicate that this is a call origination as opposed to a request for domain transfer.

4. The P-CSCF forwards the SIP INVITE to an E-CSCF.

5. The E-CSCF based on assumption or knowledge of VCC support by the UE, or based on an indication of VCC support in the INVITE, forwards the SIP INVITE to a VCC DTF.

6. The VCC DTF anchors the incoming call leg and originates an outgoing leg by sending the INVITE to (or back to) the E-CSCF. The INVITE still carries an emergency indication.

7. The E-CSCF performs normal treatment for emergency call setup as defined in TS 23.167 [4]. If the location object provided in the INVITE is insufficient to determine the correct PSAP or if the IMS core requires the assistance of an RDF, of if the IMS core is required to verify the location object, a retrieve location request is sent to the LRF performing the location retrieval functionality. The retrieve location request shall include

information identifying the UE (e.g. public user Tel UEI and SIP URI), the IP-CAN and may include means to access the UE (e.g. UE IP address). The retrieve location request may also include any location objects provided in the INVITE in step 3. The retrieve location request may further include an indication of VCC support by the UE and identification information for the VCC DTF - e.g. the VDN and VDI assigned by the VCC DTF - if this is not already known (e.g. provisioned in) the LRF. This information enables continuity of location support by the LRF as described in other clauses in association with domain transfer.

8. The LRF may obtain an interim location estimate as described in TS 23.167 [4]. The LRF may invoke an RDF to convert the interim location or any location object received in step 6 into the address of a PSAP. The LRF may record the information received in step 6.

9. The location information and/or the PSAP address obtained in step 7 are returned to the E-CSCF. The LRF may also return correlation information (e.g. ESQK) identifying itself and any record stored in step 7. For the remainder of the call, the LRF serves as the anchor LRF.

10. The E-CSCF uses the PSAP address provided in step 8 or selects an emergency centre or PSAP based on location information provided in step 8 and sends the request including the location information and any correlation information to the emergency centre or PSAP:

    10a. The INVITE is sent to an MGCF/MGW;

    10b. The IAM is continued towards the emergency centre or PSAP; or

    10c. The INVITE is sent directly to the emergency centre or PSAP.

11. Intermediate signalling for call establishment may occur (e.g. return of an ACM from a PSTN capable PSAP) which is not shown. When the PSAP answers the call, the following steps occur:

    11a. The PSAP returns an ANM to the MGCF/MGW;

    10b. The MGCF/MGW returns a 200 OK to the E-CSCF; or

    11c. The PSAP returns a 200 OK directly to the E-CSCF.

12. The E-CSCF returns the 200 OK to the VCC DTF (on the outgoing call leg started in step 5).

13. The VCC DTF returns a 200 OK to the E-CSCF. The VCC DTF (or the E-CSCF) may insert a VDN and/or VDI into the 200 OK to support the domain transfer procedures A and C in clauses 6.2.4.3 and 6.2.4.5. Alternatively, the VCC DTF (or the E-CSCF) may insert a modified VDN and/or modified VDI (as defined in clause 6.2.2.3) into the SIP INVITE to support the domain transfer procedures B and D in clauses 6.2.4.4 and 6.2.4.6.

14. The E-CSCF returns the 200 OK to the UE via the P-CSCF.

6.2.4.2 CS Emergency Call Origination

Figure 6.2.4.2-1 shows VCC support for an emergency call originated in the CS domain.

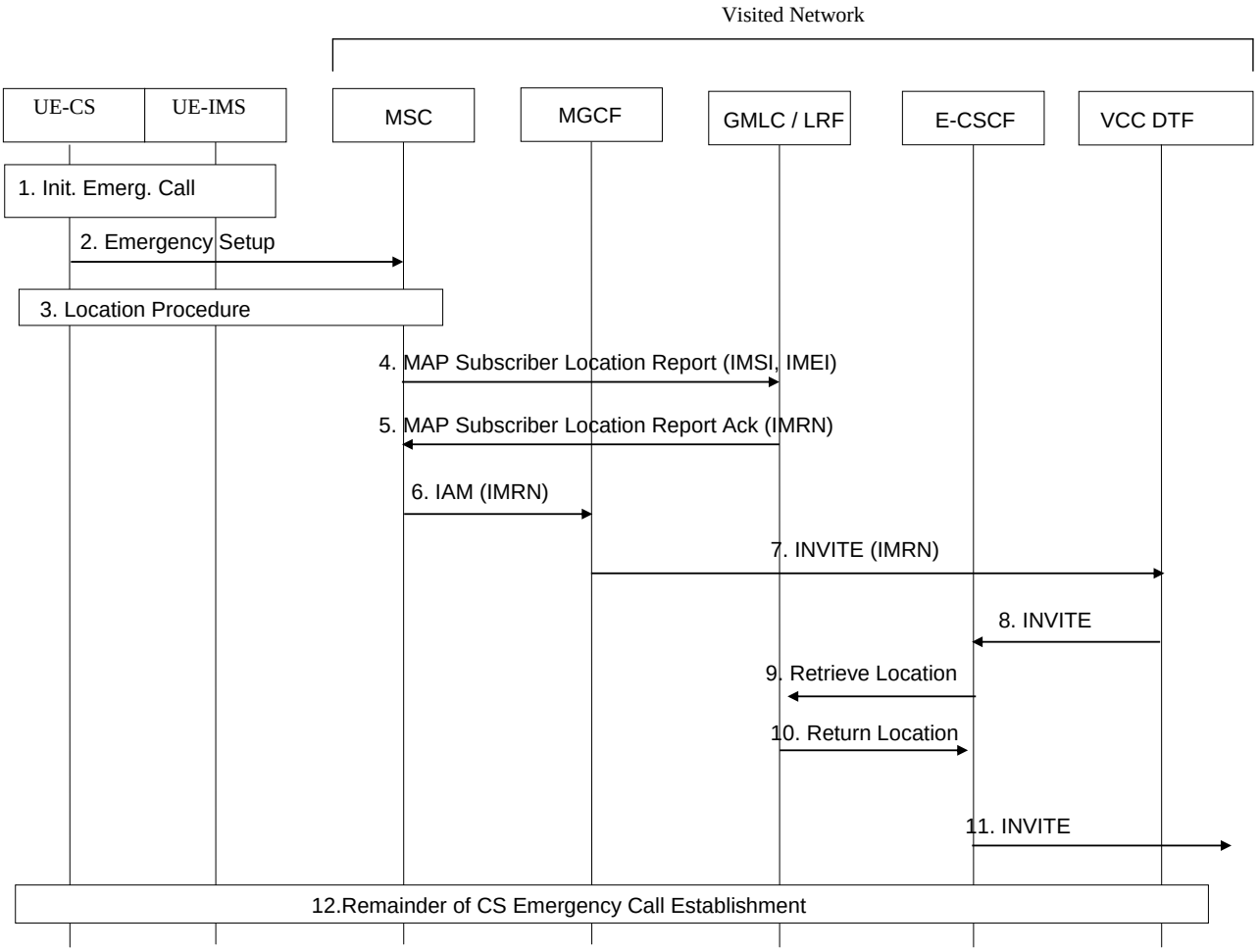


Figure 6.2.4.2-1: CS Emergency Call Origination with VCC support

1. The user initiates an emergency call.

2. The UE originates an emergency voice call in the CS domain by sending an Emergency Setup message to the VMSC (as defined in TS 24.008 [12]). The Emergency Setup may indicate that the UE supports VCC and may further indicate that this is a call origination as opposed to a request for domain transfer.

3. The VMSC may initiate a procedure in the RAN to obtain an interim location estimate for the UE as defined and allowed in TS 23.271 [11].

4. Based on normal handling for all CS emergency calls (e.g. as described in TS 23.271 [11]) or based on assumed VCC support according to the UE's home network operator or based on subscription information obtained from the UE's home HLR/HSS or based on an explicit indication of VCC support in the Emergency Setup message, the VMSC sends a MAP Subscriber Location Report (SLR) to a GMLC associated with the emergency service provider (PSAP) to which the call would normally be sent (e.g. based on the serving cell ID and dialled emergency number). The MAP Subscriber Location Report carries the IMSI, MSIDN, IMEI, VMSC address and serving cell identity or SAI for the UE. It also includes any interim location estimate obtained in step 3. In regions where the VMSC and not the GMLC normally determines the PSAP (e.g. the EU), the message may carry the address of the intended destination PSAP. The message may also carry any indication of VCC support and/or whether for a call origination or domain transfer that was received in the Emergency Setup. This indication could be an explicit parameter or parameter value in the MAP SLR or it could (less preferably) be associated with a distinct SCCP E.164 address (associated with the GMLC) to which the MAP SLR is routed.

5. The GMLC assumes the UE supports VCC (e.g. an assumption for all UEs or just certain operators' UEs) or possibly determines this from subscription information if the UE is served by the home network or determines this from an indication in the MAP SLR or the address (e.g. SCCP E.164 address) to which the MAP SLR was routed. The GMLC stores a call record for the UE including all the information received in step 4. The GMLC assigns an IP Multimedia Routeing Number (IMRN) to the call. Minimally, the IMRN enables call routeing to the VCC DTF in steps 6 and 7 and, if needed, identifies the GMLC. Optionally, the IMRN may also temporarily

identify the call record stored in the GMLC. The IMRN is used in later steps to select an LRF associated with the GMLC enabling the call record stored in the GMLC in this step to be retrieved by the LRF and enabling the LRF to locate the UE via the GMLC. The GMLC returns a MAP Subscriber Location Report Ack. to the VMSC carrying the IMRN in the NA-ESRD or NA-ESRK or in some other new parameter. The GMLC may subsequently instigate a CS-MT-LR with the VMSC (not shown) to obtain either an interim location estimate for routeing or an accurate location estimate for later provision to the PSAP. As an alternative, the MSC rather than GMLC could assign the IMRN and transfer this to the GMLC in step 4.

6. The VMSC routes the call based on the IMRN received in step 5. If the IMRN is conveyed using the existing NA-ESRK or NA-ESRD parameter then the call routeing procedure in the VMSC can be the same as that used for normal emergency call origination in TS 23.271 [11] (i.e. the IMRN appears like an ESRK or ESRD to the VMSC). Based on IMRN routeing, the VMSC routes the call to an MGCF in the visited network.

7. The MGCF initiates an INVITE towards an I-CSCF in the visited IMS (not shown) or possibly the MGCF routes directly to the E-CSCF, an S-CSCF or VCC DTF. The INVITE contains the identity of the UE (e.g. MSISDN Tel URI as Contact address). The I-CSCF or S-CSCF (not shown) or E-CSCF, based on the IMRN, instigates PSI based application server termination to the VCC DTF.

NOTE: Routeing via an E-CSCF or S-CSCF needs further study since it is not normal; routeing to the VCC DTF may also require the support of an RUA and/or CSAF.

8. The VCC DTF anchors the incoming call leg and originates an outgoing leg by sending the INVITE to (or back to) the E-CSCF. The INVITE carries information identifying an emergency call and carrying or enabling recovery of the IMRN.

9. Based, for example, on inclusion of IMRN information in step 8, the E-CSCF sends a retrieve location request to an LRF identified by or associated with the IMRN. The retrieve location request includes IMRN information and any UE identification received in step 8 – e.g. an MSISDN Tel URI. The retrieve location request may further include an indication of VCC support and identification information for the VCC DTF – e.g. the VDN and VDI.

10. Based on any UE identification received in step 9 (e.g. MSISDN) and/or on IMRN information, the LRF interacts with the GMLC and retrieves the call record stored by the GMLC in step 5. Using any interim location information already in the call record or any interim location obtained according to step 5, the LRF returns a PSAP address and possibly location information to the E-CSCF. The LRF will provide the anchor point for further support of location and may copy the call record obtained from the GMLC as well as storing information received from the E-CSCF in step 9. The LRF may return correlation information (e.g. ESQK) to the E-CSCF identifying itself and the call record. The LRF may further interact with the GMLC to instigate a CS-MT-LR procedure with the VMSC (as defined in TS 23.271 [11]) to obtain an accurate location estimate for the UE.

11. The E-CSCF uses the PSAP address provided in step 10 and sends on the call request including the location information and any correlation information to the emergency centre or PSAP. The call request is either sent via an MGCF/MGW into the PSTN (not shown) or is sent directly as a SIP INVITE towards an IP capable emergency centre or PSAP.

12. The rest of the call establishment procedure occurs between the UE, VMSC, VCC DTF, E-CSCF and PSAP based on the VCC CS origination procedure described in TS 23.206 [3].

The above procedure preserves support for existing PSAP routeing options (e.g. using cell ID or an interim location estimate), does not necessarily require any new impacts to MSCs and supports accurate location retrieval by the PSAP in the manner currently defined in TS 23.271 [11]. It also enables CS originated emergency calls to be sent to IP capable PSAPs.

6.2.4.3 Domain Transfer IMS to CS – Procedure A

Two alternative procedures are described to support domain transfer for an IMS emergency call from the IMS domain to the CS domain when the UE moves out of IMS coverage and into CS coverage. In procedure A, the VCC capable UE behaves as for normal VCC (described in TS 23.206 [3]) and originates a new call leg in the CS domain to the VCC DTF using the VDN obtained from the visited network using any of alternatives (e), (f), (g) or (h) described in clause 6.2.2.1.

Procedure A is only applicable to a UE that has sufficient credentials to register in the new visited network supporting the CS domain and places limitations on the continuity of support for providing further UE location updates to the PSAP. However, the procedure has the advantage of being compatible from the UE perspective with IMS to CS domain transfer for normal VCC.

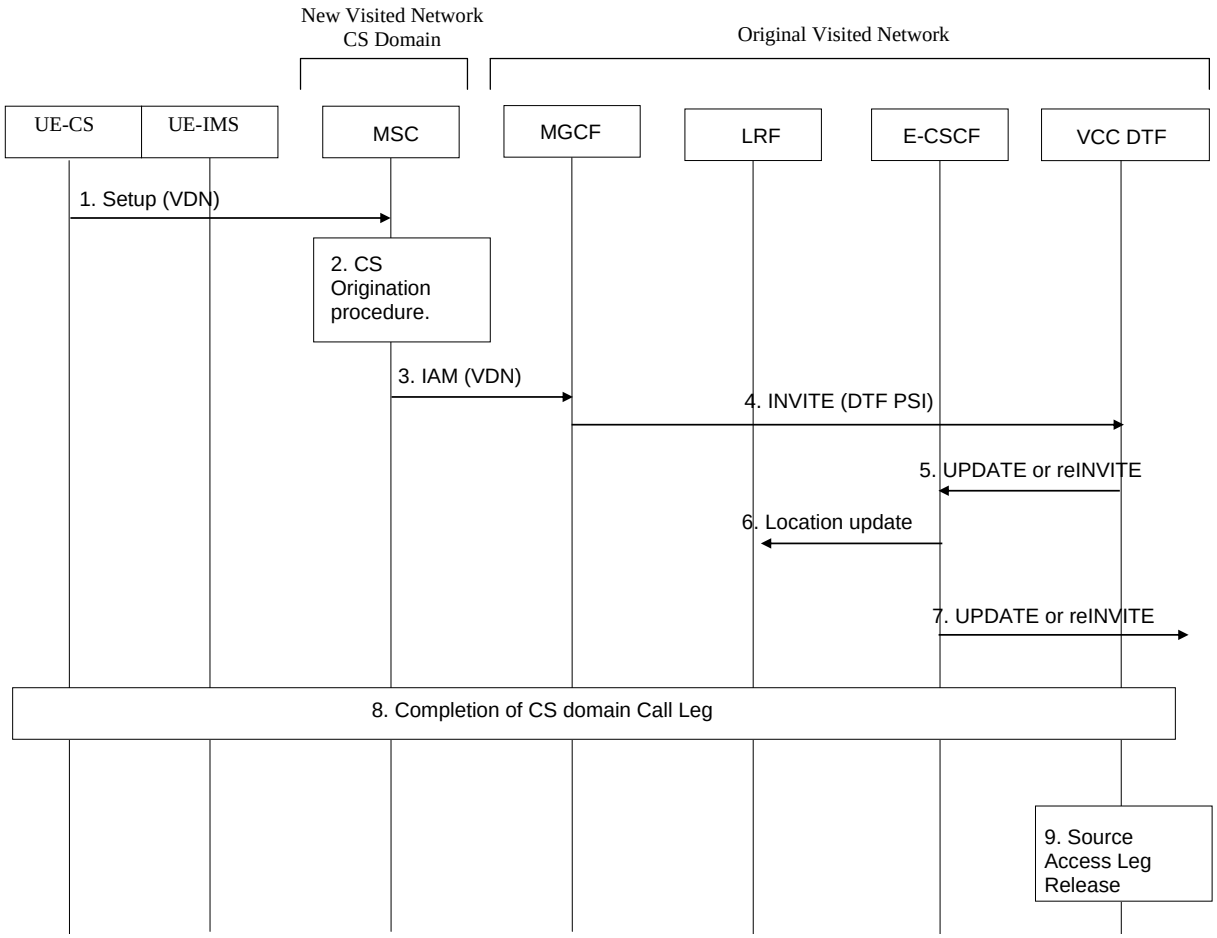


Figure 6.2.4.3-1: Procedure A for IMS to CS domain transfer

1. If the user is not attached to the CS domain at the time when the UE determines a need for Domain Transfer to CS, the UE performs a CS Attach including a location update to its HLR/HSS. It subsequently originates a voice call in the CS domain using the VDN obtained earlier from the original visited network to establish an Access Leg via the CS domain. It is assumed for this procedure that the UE can be authenticated in the CS domain.

NOTE 1: Because a normal call is originated, the domain transfer will not receive priority treatment in the new CS domain.

2. The originating call is processed as for normal CS call originations in the CS network.

3. The VMSC routes the call towards the original visited IMS network via an MGCF in the original visited network.

NOTE 2: The VMSC is not aware of the emergency call or VCC support and thus will not perform a GMLC query as for CS emergency call origination. Continued support of location is described further down.

4. The MGCF initiates an INVITE towards an I-CSCF in the original visited IMS (not shown) or possibly the MGCF routes directly to the E-CSCF, an S-CSCF or VCC DTF. The I-CSCF or S-CSCF (not shown) or E-CSCF, based on the VDN, instigates PSI based application server termination to the VCC DTF.

5. The DTF updates the outgoing Access Leg by communicating the SDP of the Access Leg established in the transferring-in domain to the remote end via the E-CSCF. Access Leg update happens according to SIP session modification procedures in IETF RFC 3261. The DTF may also explicitly indicate domain transfer to the E-CSCF to allow the E-CSCF to notify the LTF in the next step.

6. The E-CSCF sends a Location Update to the anchor LRF with the new SDP information which may assist the LRF in identifying the type of domain transfer. Minimally the E-CSCF indicates to the LRF that there has been a CS domain transfer (e.g. this can be known by the DTF from use of a VDN rather than VDI and/or from domain transfer involving an MGCF).

7. The update continues towards the PSAP if IP capable or to an MGCF.

8. The new call leg in the transferring-in CS domain is established between the VCC DTF, E-CSCF or S-CSCF if present, I-CSCF if present, MGCF, VMSC and UE.

9. The previous incoming Access Leg which is the Access leg previously established over IMS is released. The UE should de-register if possible in the visited network P-CSCF and home network S-CSCF.

Continuing support of location after procedure A has transferred the UE to the CS domain is restricted as follows. If the PSAP sends a request to the anchor LRF to obtain the location of the UE, it may not be possible for the LRF to continue using the same procedure to obtain location as it may have been using (or expecting to use) while the UE was in the IMS domain. For example, if the LRF was using OMA SUPL based on UDP/IP or SIP Push initial transport between the LRF and UE, the loss of access to the PS domain by the UE following IMS to CS domain transfer may prevent further use of SUPL. In addition, the LRF may not be able to use the control plane location solutions defined in TS 23.271 [11] for CS emergency calls (e.g. in clause 9.1.3 of TS 23.271 [11]) because it may not know the VMSC address. However, the LRF could use the more general CS-MT-LR procedure described in clauses 9.1.1 and 9.1.2 of TS 23.271 [11] in which the LRF (behaving as or accessing a GMLC) obtains the VMSC address by querying the UE's home HLR/HSS. A disadvantage of this, however, is that the UE's HLR/HSS will need to support the CS-MT-LR query procedure and there may be billing issues between the visited network and home network (since the home network may not be aware of the emergency call significance).

6.2.4.4 Domain Transfer IMS to CS – Procedure B

Procedure B enabling IMS to CS domain transfer may be applicable to a UE whether or not it has sufficient credentials to register in the new visited network and enables continuity of location support without limitation. However, it may have to be restricted to domain transfer between networks belonging to the same operator (e.g. networks sharing the same MCC and MNC). The procedure requires a new variant of VCC domain transfer in the UE in which knowledge of a VDN may not be needed.

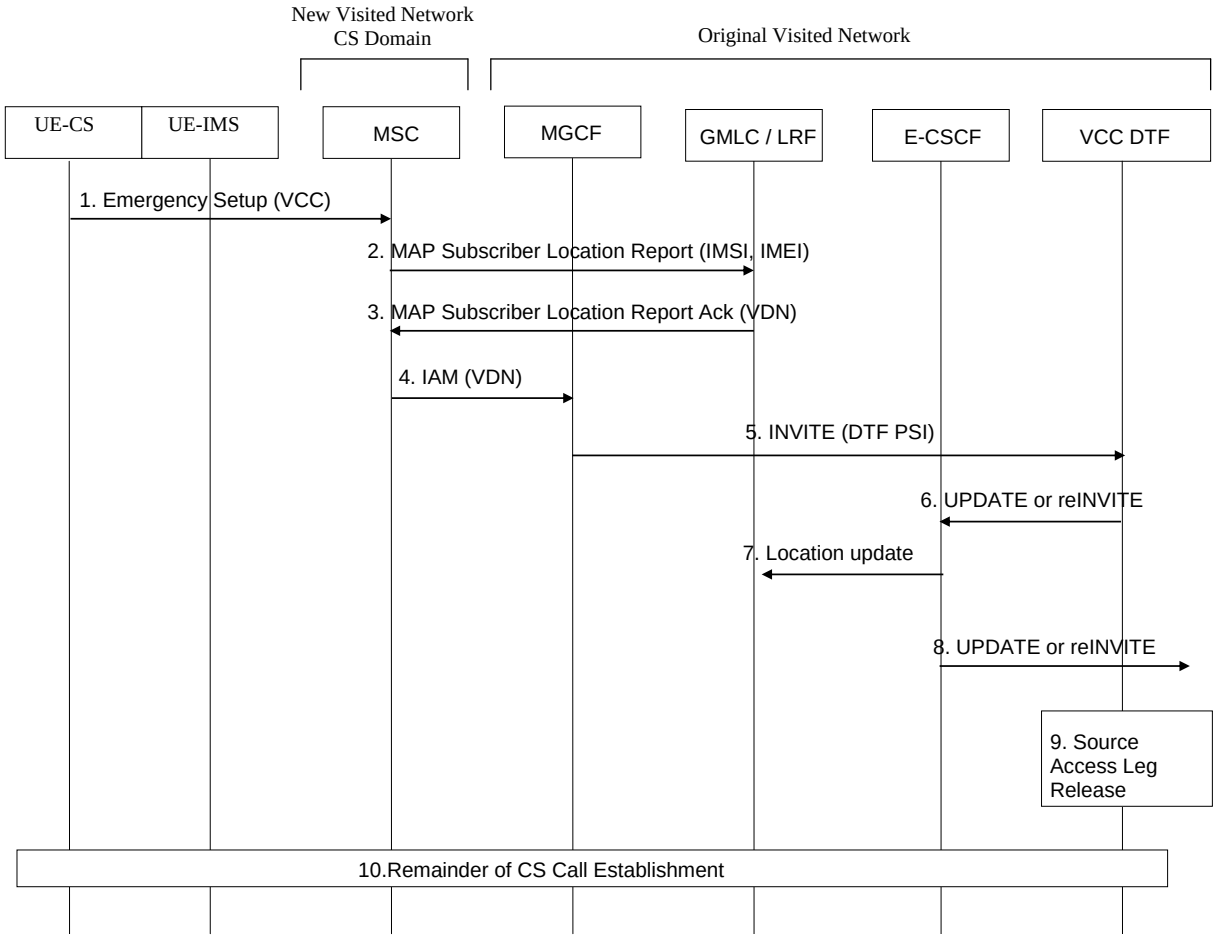


Figure 6.2.4.4-1: Procedure B for IMS to CS domain transfer

1. If the user is not attached to the CS domain at the time when the UE determines a need for Domain Transfer to CS, the UE may perform a CS Attach if it contains the necessary credentials. It subsequently originates an emergency voice call in the CS domain by sending an Emergency Setup message to the VMSC (as defined in TS 24.008 [12]). The Emergency Setup may indicate that the UE supports VCC and may further indicate that this is a request for domain transfer. As an alternative, the UE may send a normal Setup message carrying a modified VDN (see clause 6.2.2.3) in the called party number parameter.

2. If the UE sent an Emergency Setup message in step 1, then based on normal handling for all CS emergency calls (e.g. as described in TS 23.271 [11]) or based on assumed VCC support according to the UE's home network operator or based on an explicit indication of VCC support in the Emergency Setup message, the VMSC sends a MAP Subscriber Location Report (SLR) to a GMLC associated with the emergency service provider (PSAP) to which the call would normally be sent (e.g. based on the current serving cell or SAI). Alternatively, if the UE sent a normal Setup message in step 1 carrying a modified VDN, the MSC may recognize the VDN as signifying a domain transfer request for an existing emergency call and similarly send a MAP SLR to the GMLC. The MAP SLR carries the same information as that which would be sent for a normal emergency call origination (e.g. as in step 4 in Figure 6.2.4.2-1) including the IMSI, MSIDN, IMEI, VMSC address and serving cell identity or SAI. No location estimate is included. The message may carry any indication of VCC support and whether for a domain transfer that was received in the Emergency Setup. This indication could be an explicit parameter or parameter value in the MAP SLR or it could (less preferably) be associated with a distinct E.164 address (associated with the GMLC) to which the MAP SLR is routed.

3. Based on local policy or based on an explicit indication of VCC support and request for a domain transfer received in the MAP SLR or based on the address (e.g. SCCP E.164 address) to which the MAP SLR was routed, the GMLC interacts with an associated LRF (e.g. which may be within the same physical entity) to search for the call record for the UE that was originally established in the anchor LRF (e.g. using the procedure described in clause 6.1.4.1 or 6.1.4.2). The anchor LRF may use the IMSI, MSISDN and/or IMEI received in step 2 to identify the correct call record. Note that in the case of an unauthenticated emergency call, the IMEI would have to be used to identify the call record which is an item for further study since the identification cannot be completely reliable. If no call record is found and no indication was received in or associated with the MAP SLR that this was a request for domain transfer, the GMLC should assume that this is a new emergency call and proceed as in Figure 6.2.4.2-1. However, if no call record is found and the MAP SLR does indicate a request for domain transfer, the GMLC should return a MAP SLR return error response to cause rejection of the domain transfer request by the VMSC, in which case the UE must continue with the call in the IMS domain or release the call if that is not possible. Otherwise, if the call record is found, the GMLC returns a MAP Subscriber Location Report Ack. to the VMSC carrying the VDN (note different to any modified VDN received in step 1) needed to establish the new access leg. This VDN would have been obtained by the LRF when the call was first originated (e.g. in step 6 in Figure 6.2.4.1-1 or step 9 in Figure 6.2.4.2-1). The VDN could be carried by the existing NA-ESRK or existing NA-ESRD parameter in the MAP Subscriber Location Report ack. The GMLC also stores the information received from the VMSC in step 2.

4. The VMSC routes the new leg based on the VDN received in step 3. If the VDN is conveyed using the existing NA-ESRK or NA-ESRD parameter then the call routeing procedure can be the same as that used for normal emergency call origination (i.e. there would be no additional VMSC impact). Based on VDN routeing, the VMSC routes the call towards the original visited IMS network via an MGCF in the original visited network.

5. The MGCF initiates an INVITE towards an I-CSCF in the original visited IMS (not shown) or possibly the MGCF routes directly to the E-CSCF, an S-CSCF or VCC DTF. The I-CSCF or S-CSCF (not shown) or E-CSCF, based on the VDN, instigates PSI based application server termination to the VCC DTF.

6. The DTF updates the outgoing Access Leg by communicating the SDP of the Access Leg established in the transferring-in domain to the remote end via the E-CSCF. Access Leg update happens according to SIP session modification procedures in IETF RFC 3261. The DTF may also explicitly indicate CS domain transfer to the E-CSCF.

7. The E-CSCF sends a Location Update to the anchor LRF with the new SDP information. Minimally the E-CSCF indicates to the LRF that there has been a CS domain transfer. The LRF correlates this indication with the indication of domain transfer determined in step 3 and determines that the UE has now changed domain to that indicated in step 2. The LRF communicates this information to the GMLC selected by the VMSC in step 2.

8. The update continues towards the PSAP or MGCF.

9. The new call leg in the transferring-in CS domain is established between the VCC DTF, E-CSCF or S-CSCF if present, I-CSCF if present, MGCF, VMSC and UE.

10. The source Access Leg which is the Access leg previously established over IMS is released. The UE should de-register if possible in the visited network P-CSCF and home network S-CSCF.

Besides possibly allowing domain transfer for unregistered UEs, procedure B also enables the anchor LRF to make use of the normal location procedure defined in TS 23.271 [11] (e.g. in clause 9.1.3) to locate a UE that has originated an emergency call. This is enabled due to steps 2 and 3 in Figure 6.2.4.4-1 in which the VMSC obtains and stores information concerning the GMLC, and the LRF and GMLC obtain and store information concerning the VMSC. This then permits a CS-MT-LR without the need to query the UE's home HSS/HLR.

A further aspect of procedure B is that the call origination procedure at the VMSC can be identical or almost identical to that for a normal emergency call as described in TS 23.271 [11] or identical or almost identical to that for VCC support for a CS originated emergency call as described in clause 6.1.4.2. From the perspective of the GMLC, the procedure is also almost identical to that for a normal emergency call with regard to the MAP signalling transaction with the VMSC.

A disadvantage of procedure B is that it depends on the GMLC and LRF finding the original call record in step 3. This seems to be possible provided the GMLC and LRF belong to the same operator – e.g. because then the GMLC and LRF could be part of the same physical entity or could at least be interconnected. But if the original call record is not found and there is no explicit or implicit indication of a domain transfer in the Emergency Setup message, the GMLC will assume that this is a new emergency call and not a domain transfer resulting in connection of the user to a new PSAP operator. This disadvantage can be averted, however, by including VCC and domain transfer indications in the Emergency Setup and MAP SLR messages as described above though at the cost of possibly making the procedure visible (not entirely transparent) to the VMSC.

6.2.4.5 Domain Transfer CS to IMS – procedure C

Two alternative procedures are described to support domain transfer for an emergency call from the CS domain to the IMS domain. In procedure C described in this clause, the VCC capable UE behaves as for normal VCC (described in TS 23.206 [3]) and originates a new call leg in the IMS domain to the VCC DTF using the VDI obtained from the visited network using any of alternatives (e), (f), (g) or (h) described in clause 6.1.2.1. The call is treated like a normal originating SIP call and thus is only applicable to a UE that has sufficient credentials to register in the new visited network.

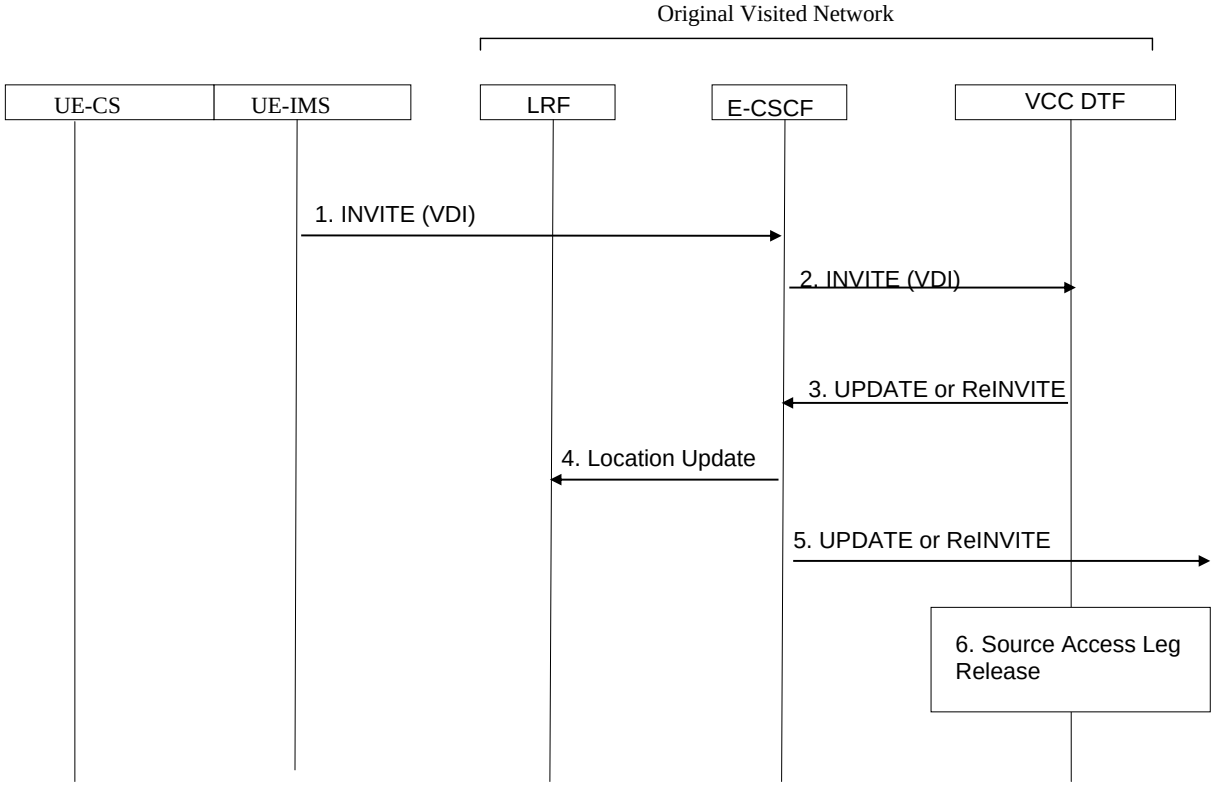


Figure 6.2.4.5-1: Domain Transfer CS domain to IMS – procedure C

1. If the user is not registered with IMS at the time when the UE determines a need for Domain Transfer to IMS, the UE initiates Registration with IMS as specified in TS 23.206 [3]. It subsequently initiates an IMS originated session toward the DTF in the original visited network using the VDI obtained earlier from the visited network (e.g. as described in clause 6.1.2.1 and in Figures 6.1-5 and 6.1-6) to establish an Access Leg via IMS and request Domain Transfer of the active CS session to IMS. Due to normal call handling, the SIP INVITE may be routed through a P-CSCF in either the new visited network or home network (not shown) and an S-CSCF in the home network (not shown) and will eventually reach either an S-CSCF (not shown) or the E-CSCF in the original visited network.

NOTE: Because a normal call is originated, the domain transfer will not receive priority treatment in the new IMS domain.

2. The IMS session is processed at an S-CSCF (not shown) or the E-CSCF in the original visited network and delivered to the VCC DTF.

3. The DTF completes the establishment of the new incoming Access Leg via IMS. The DTF performs the Domain Transfer by updating the Remote Leg with connection information of the newly established Access Leg using the Access Leg Update procedure as specified in TS 23.206 [3]. The UPDATE or ReINVITE is sent to the E-CSCF used to originate the call (e.g. according to Figure 6.2.4.1-1 or 6.2.4.2-1). The DTF may also explicitly indicate domain transfer to the E-CSCF.

4. The E-CSCF updates the anchor LRF with the new SDP information – e.g. indicates that the UE is now using the IMS domain and provides the UE IP address.

5. The update continues towards the PSAP or MGCF.

6. The source Access Leg which is the Access leg previously established over CS is subsequently released as specified in TS 23.206 [3]. This includes releasing the previous incoming CS leg through the E-CSCF.

Once procedure C has been completed, it will be possible to continue location support for the UE because the LRF should now have the UE's IP address and can thus invoke OMA SUPL (or any other solution involving IP transport). However, use of the 3GPP control plane solution to enable location of the UE for GPRS access will only be possible using the more general PS-MT-LR procedure described in clauses 9.1.1 and 9.1.6 of TS 23.271 [11] in which the LRF queries the UE's home HLR/HSS for the visited SGSN address.

6.2.4.6 Domain Transfer CS to IMS – Procedure D

The other procedure D supporting CS to IMS domain transfer may not require use of a VDI and places fewer restrictions on continued location support. However, it may have to be restricted to domain transfer between networks owned and managed by the same operator as for procedure B.

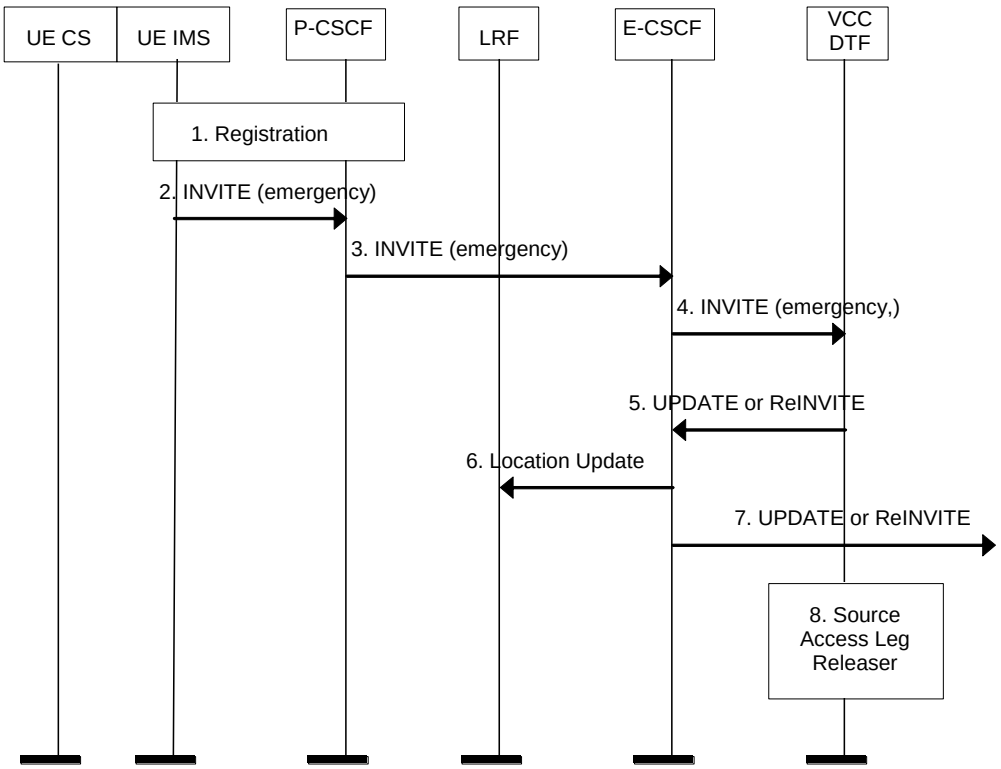


Figure 6.2.4.6-1: Domain Transfer CS domain to IMS – procedure D

1. Prior to sending the INVITE, the UE executes an emergency registration in the new visited IMS network if it contains adequate credentials as defined in TS 23.167 [4] (i.e. a normal registration is not used). This will be needed to support call back to the UE (via the new visited network) and to authenticate the UE in the new visited IMS.

2. The UE then sends an INVITE with an emergency indication to the visited network P-CSCF. The INVITE should contain identification information for the UE – e.g. MSISDN Tel URI. The INVITE may indicate that the UE supports VCC and may indicate that this is a request for domain transfer as opposed to a call origination. This indication may be conveyed in a modified VDI (see clause 6.2.2.3) carried in the SIP To header field – in which case no separate emergency indication may be needed.

3. Based on knowledge or assumption of VCC support according to alternatives (a), (b) or (c) in clause 6.1.2.1, or based on an indication of VCC support in the INVITE (e.g. via inclusion of a modified VDI), the P-CSCF forwards the SIP INVITE to an E-CSCF.

4. The E-CSCF based on assumption or knowledge of VCC support forwards the SIP INVITE to a VCC DTF.

5. The VCC DTF finds the original call record – e.g. as established according to step 5 in Figure 6.2.4.1-1. The DTF then updates the outgoing Access Leg by communicating the SDP of the Access Leg established in the transferring-in domain to the remote end via the E-CSCF. The DTF may also explicitly indicate domain transfer to the E-CSCF. If the VCC DTF does not find the original call record and no indication was received in the INVITE that this was a request for domain transfer, it could assume that this is a new emergency call (not a domain transfer) and proceed as in step 5 in Figure 6.2.4.5-1. However, if no call record is found and the INVITE does indicate a request for domain transfer, the VCC DTF should reject the domain transfer request, in which case the UE must continue with the call in the CS domain or release the call if that is not possible.

6. The E-CSCF updates the anchor LRF with the new SDP information – e.g. indicates that the UE is now using the IMS domain and provides the UE IP address.

7. The update continues towards the PSAP or MGCF.

8. The source Access Leg which is the Access leg previously established over CS is subsequently released as specified in 3GPP draft TS 23.206 [3]. This includes releasing the previous incoming CS leg through the E-CSCF.

Continuing location support can be the same as that for procedure C – e.g. by using OMA SUPL with the UE IP address provided to the anchor LRF in step 5 or using the 3GPP PS-MT-LR procedure for location with GPRS access. However, as an added benefit, it may be possible to use the 3GPP PS-NI-LR and PS-MT-LR procedures specific to emergency calls defined in TS 23.271 [11] (in clauses 9.1.6A and 9.1.7). This can be enabled if the UE indicates an emergency call for GPRS access and/or GPRS PDP context establishment. This can trigger the SGSN into instigating a PS-NI-LR either to obtain location or provide its address to a GMLC. If the GMLC is associated with the anchor LRF, it will be possible to provide the anchor LRF with the SGSN address thereby enabling use of a PS-MT-LR without having to query the home HLR/HSS (and also allowing location for an unauthorized UE with possibly no HLR/HSS).

A disadvantage of procedure D, as with procedure B, is that it depends on the DTF finding the original call record in step 4 which in turn requires that the P-CSCF or E-CSCF route the call to the correct DTF in step 3. This is likely to be possible only for domain transfer to the IMS of the original visited network operator and would not be feasible for domain transfer to a different operator unless possibly the DTF and anchor LRF are shared among multiple operators which is FFS.

6.3 VCC in the Visited Network - Alternative 3

6.3.1 Architectural Details

Figure 6.3.1-1 combines the IMS Service Centralization and Continuity Reference Architecture from TS 23.292 [10] and session transfer functionality from TS 23.237 [13] with the additional functional entities from the IMS Emergency Sessions reference architecture from figure 5.1 of TS 23.167 [4]. All the functional entities reside in the local/serving network. The clear boxes are based on the MSC Server session establishment procedures in clause 7.1.2 of the IMS Centralized Services architecture in TS 23.292[10] and the shaded boxes are from the IMS Emergency Sessions architecture in TS 23.167 [4].

The Emergency-Service Centralization and Continuity Application Server (E-SCC AS) varies from the SCC AS in TS 23.237[13] in that it resides in the visited/serving network. In addition, the CS Access Adaptation (CAA) functionality is extended to support the Lg' interface so that the Location messages from the MSC can provide similar functionality as the CAMEL operations in TS 23.237[13] to obtain IMRNs. The S-CSCF from the reference architecture TS 23.292[10] is replaced with an E-CSCF from the IMS Emergency Session reference architecture TS 23.167 [4].

This alternative, supports full VCC for emergency call functionality, including: CS and IMS emergency call anchoring and domain transfers in both the IMS to CS direction and CS to IMS direction. This alternative also supports unauthorized emergency callers.

For this alternative, to support CS to IMS VCC, the UE must be configured with CS network identities that support VCC for emergency calls. When the UE originates an emergency call in IMS, SIP signalling can indicate to the UE that the network supports VCC and/or the emergency call has been anchored. The UE and network do not need to support local emergency VDIs and VDNs since the UE addresses the network with the emergency number or SIP URN.

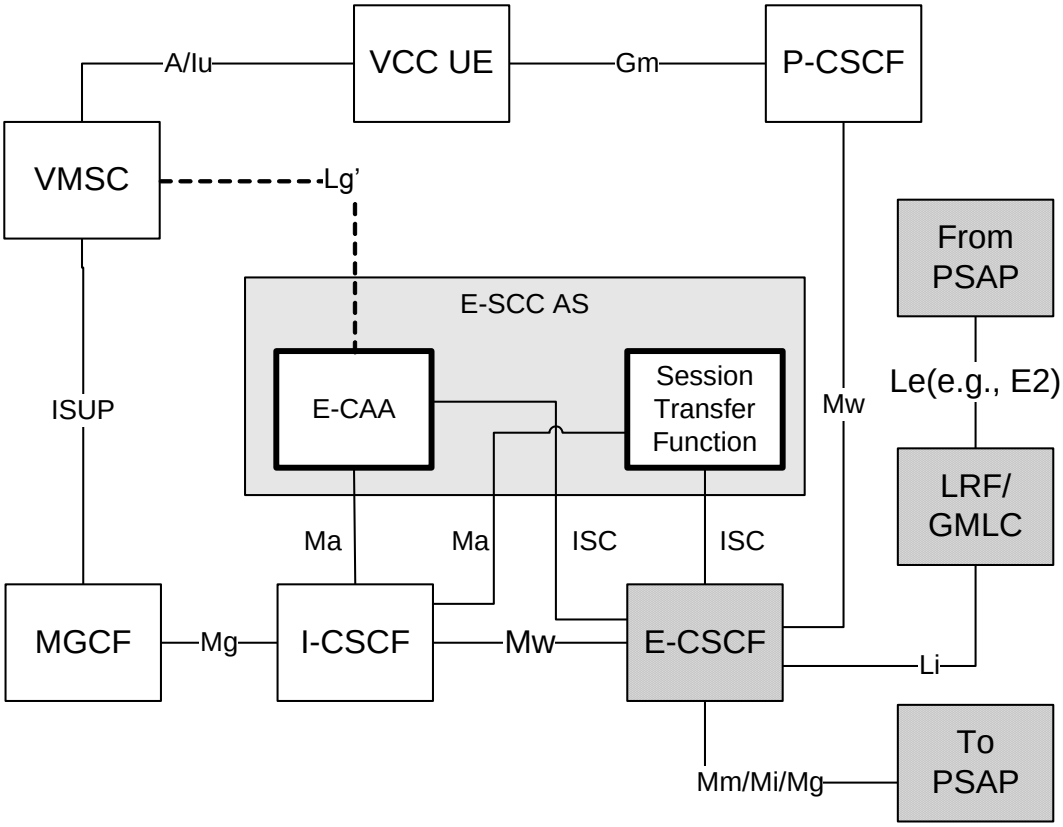


Figure 6.3.1-1: IMS Emergency Session with VCC Reference Architecture

6.3.2 Impact

See Alternative 3 in Table 7.1-1 of the Evaluation section.

6.3.3 Assessment

This alternative has the following benefits:

- No MSC upgrades required.
- No CS signalling enhancements required.
- Provides a total solution for CS and IMS emergency call anchoring and domain transfers in both the IMS to CS direction and CS to IMS direction.
- Supports unauthorized emergency callers.
- Has the ability to centralize emergency call handling, including routeing all emergency calls out of the IM CN (allows CS calls to be routed to IP PSAPs) and invoking geolocation from the LRF/GMLC in the IM CN.
- UE does not need to obtain a local emergency VDI or VDN.
- Can be provided as a solution for UEs in their home network or while roaming.

This alternative has the following disadvantages:

- Due to invoking the E-SCC AS for every CS emergency call origination to determine if the call should be anchored or not, there will be at least one additional entity invoked for every UE, including those that do not have VCC capabilities.

- The E-SCC-AS acting as a transit for all MAP-SLRs that are not related to CS emergency calls would affect all MAP-SLR transactions and add a delay to non-emergency, network initiated location requests.

- The beauty of not using emergency VDIs and VDNs may also be of concern since the local emergency number or SIP URN will be used for the domain transfers as well as the emergency call origination. Not detecting the emergency domain transfer request, especially on the CS domain, may result in a second emergency call origination.
This alternative has the following system requirements:

- Emergency call handling is centralized in IMS. This can be beneficial for operators that want this cenralized. However, some operators may be concerned with the additional signalling required to central emergency call handling, especially for UEs without VCC capabilities. If centralization in not desired, at a minimum, all CS emergency call originations invoke the E-SCC-AS to determine if they are anchored or not. If not, the E-SCC AS forwards the SLR to the GMLC and once the SLR is complete, the MSC continues routeing per normal CS emergency call origination.

- The MSC is configured so that it does not initiate interim geolocation procedures.

- The MSC is configured to use a "GMLC" during emergency call routeing (this provides the "hook" into IMS). The GMLC address is then configured to route to the E-SCC AS

- The MSC is configured to route the IMRN to IMS.

- The E-CSCF, LRF and UE must be upgraded to support VCC for emergency calls.

- The IM CN must add E-SCC AS functionality.

Due to Release 9 requirements of only anchoring IMS emergency calls and only supporting IMS to CS domain transfers, this alternative is not recommended. To meet these requirements, MSC functionality is needed to distinguish a CS emergency call origination from a domain transfer. The needed upgrades are similar to those described in alternative 1. Therefore, see Alternative 1 for Release 9.

6.3.4 Procedures

6.3.4.1 IMS Emergency Call Origination

This procedure is similar to that in clause 6.2.4.1.

Emergency call origination could occur as defined in TS 23.167 [4] but with some changes to add negotiated usage of VCC. In particular, in order to preserve continuity of location support as well as continuity of the voice call following any domain transfer, the E-CSCF in the visited network would need to send the SIP INVITE (for the IMS emergency call) to the E-SCC-AS before invoking the LRF to obtain or verify location and select the destination PSAP. The E-SCC AS would then anchor the incoming call leg and originate a new outgoing call leg through the E-CSCF towards the PSAP. On receiving the SIP INVITE from the E-SCC AS, the E-CSCF would perform normal location and routeing as defined in TS 23.167 [4] and transfer the call to the PSAP either via IP or through an MGCF and the PSTN. This will result in the E-CSCF being part of the outgoing call leg from the E-SCC AS which means the LRF can remain associated with the outgoing call leg following any domain transfer and will thus be able to provide continuing support of location provided it is updated with new information regarding changes to the access network following any change of domain. Figure 6.3.4.1-1 illustrates the ensuing call origination procedure.

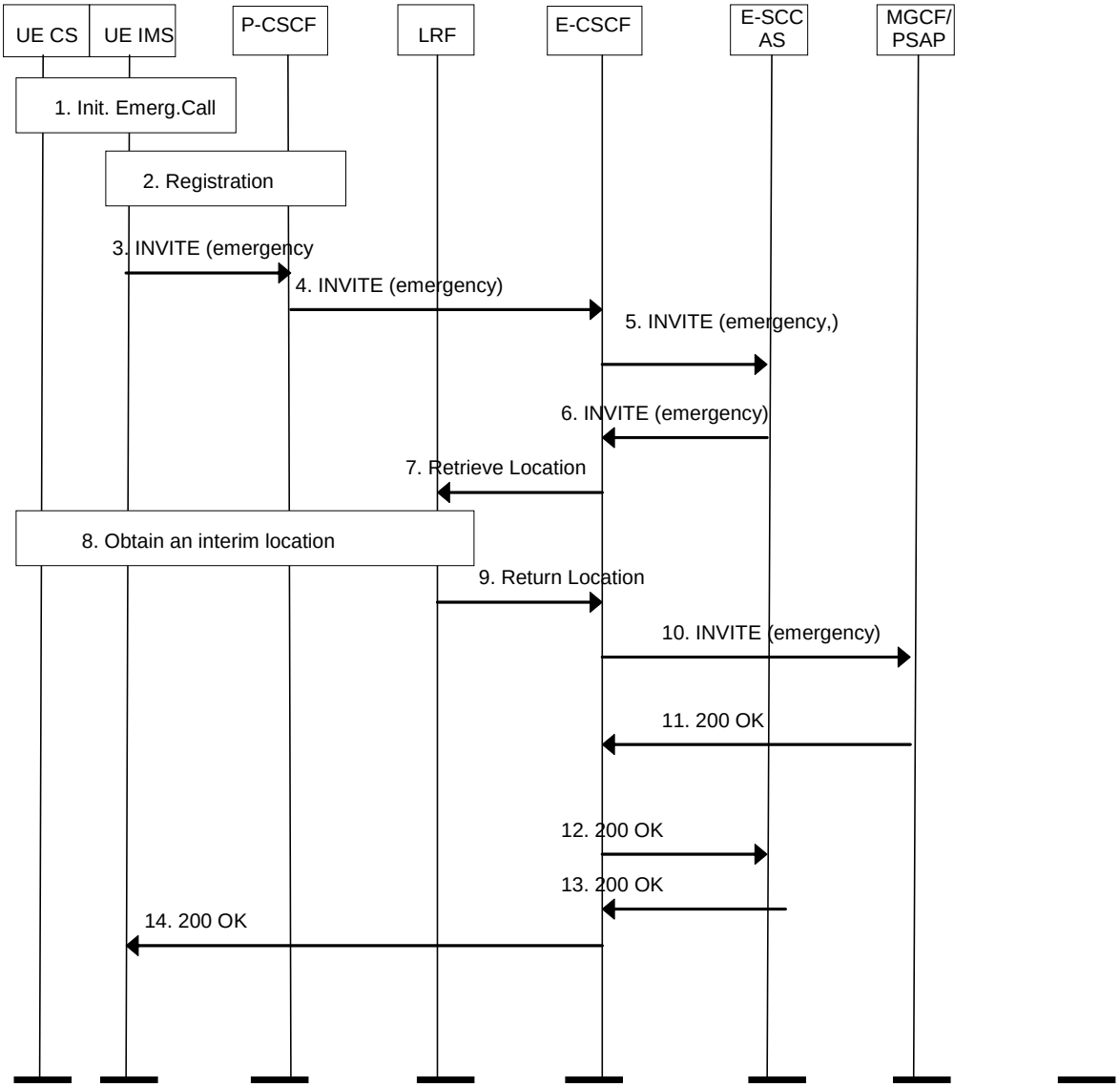


Figure 6.3.4.1-1: IMS Emergency Call Origination with VCC support

1. The user initiates an emergency call.

2. If the UE is roaming or if the UE is not roaming and not yet IMS registered, the UE performs an emergency registration procedure with the visited network P-CSCF and home network S-CSCF (not shown) as described in TS 23.167 [4] if it contains the necessary credentials.

3. The UE sends an INVITE with an emergency indication to the visited network P-CSCF. The INVITE may contain any location objects that the UE has. The INVITE should contain identification information for the UE – e.g. public user SIP URI and Tel URI. The INVITE may indicate that the UE supports VCC and may indicate that this is a call origination as opposed to a request for domain transfer.

4. The P-CSCF forwards the SIP INVITE to an E-CSCF.

5. The E-CSCF based on assumption or knowledge of VCC support by the UE, or based on an indication of VCC support in the INVITE, forwards the SIP INVITE to the E-SCC AS.

6. The E-SCC AS anchors the incoming call leg then sends the INVITE back to the E-CSCF. The INVITE still carries an emergency indication.

7. The E-CSCF performs normal treatment for emergency call setup as defined in TS 23.167 [4]. If the location object provided in the INVITE is insufficient to determine the correct PSAP or if the IMS core requires the assistance of an RDF, of if the IMS core is required to verify the location object, a retrieve location request is sent to the LRF performing the location retrieval functionality. The retrieve location request shall include

information identifying the UE (e.g. public user Tel UEI and SIP URI), the IP-CAN and may include means to access the UE (e.g. UE IP address). The retrieve location request may also include any location objects provided in the INVITE in step 3.

8. The LRF may obtain an interim location estimate as described in TS 23.167 [4]. The LRF may invoke an RDF to convert the interim location or any location object received in step 6 into the address of a PSAP. The LRF may record the information received in step 6.

9. The location information and/or the PSAP address obtained in step 7 are returned to the E-CSCF. The LRF may also return correlation information (e.g. ESQK) identifying itself and any record stored in step 7. For the remainder of the call, the LRF serves as the anchor LRF.

10. The E-CSCF uses the PSAP address provided in step 8 or selects an emergency centre or PSAP based on location information provided in step 8 and sends the request including the location information and any correlation information to the emergency centre or PSAP. The INVITE is sent towards the far end (e.g., an MGCF or IP PSAP),

11. The MGCF or IP PSAP returns a 200 OK to the E-CSCF.

12. The E-CSCF returns the 200 OK to the E-SCC AS.

13. The E-SCC AS returns a 200 OK to the E-CSCF. The E-SCC AS inserts an indication that the call has been anchored into the 200 OK to support domain transfer procedures.

14. The E-CSCF returns the 200 OK to the UE via the P-CSCF with the call anchor indication.

6.3.4.2 CS Emergency Call Origination

The following figure is based on TS 23.292 [10], Figure 7.1.2-1 "*Session signalling and bearer path using CS call control*" to support emergency calls in the visited/serving network. The serving IMS system is now labelled "Visited IMS", the S-CSCF is replaced with the E-CSCF, the SCC AS is replaced with the E-SCC AS, and the signalling path for location is shown.

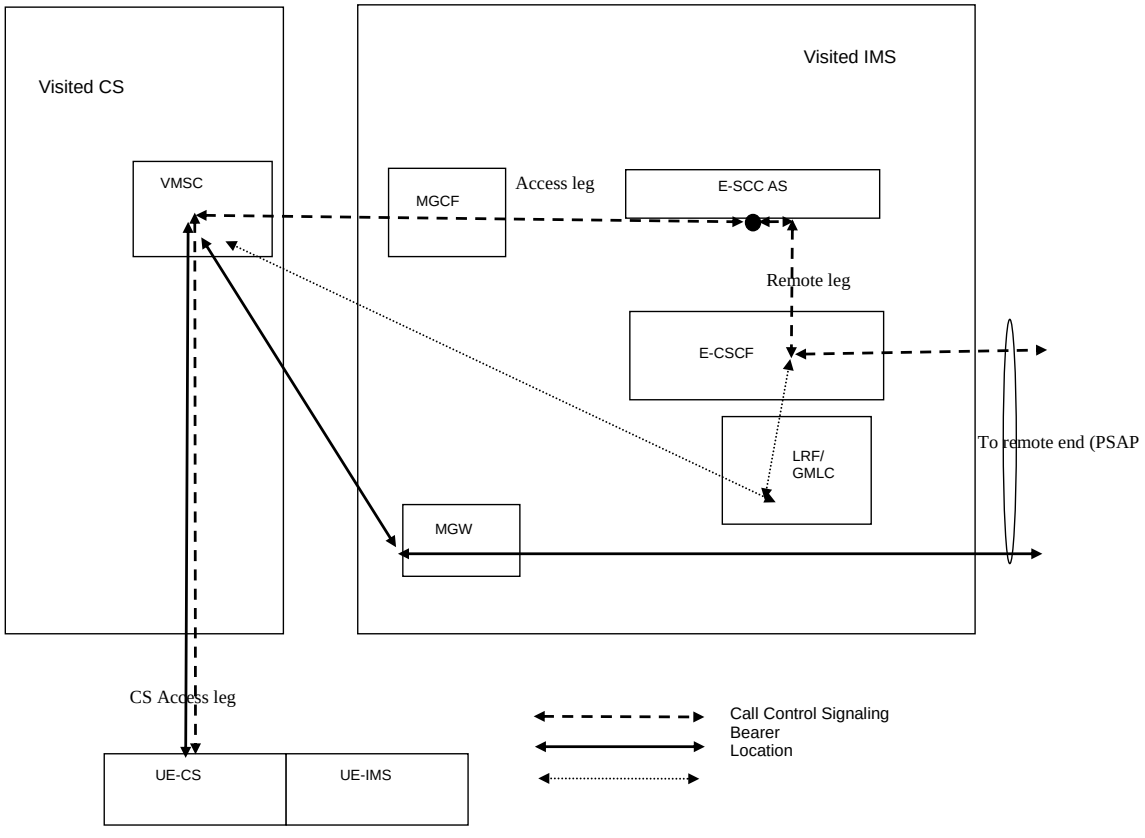


Figure 6.3.4.2-1: Session signalling and bearer path using CS call control for CS Emergency Call Origination

The following call flow is similar to the previous CS Emergency Call Origination scenario in clause 6.2.4.2 except the MAP Subscriber Location Report (SLR) is sent to an E-SCC AS instead of a GMLC for IMRN assignment. To the VMSC, the E-SCC AS interface is the same as that of a GMLC. Like the CAMEL interface in a non-emergency CS origination, the SLR is used to assign an IMRN so the call can be routed to and anchored in the IM CN. Once the call is received in the IM CN, the LRF, as in TS 23.167 [4], is invoked to perform the necessary location and routeing functionality for the emergency call. This architecture has the potential of minimizing impact to the legacy VMSC and GMLC entities, where most of the new functionality is provided by the E-SCC AS and E-CSCF.

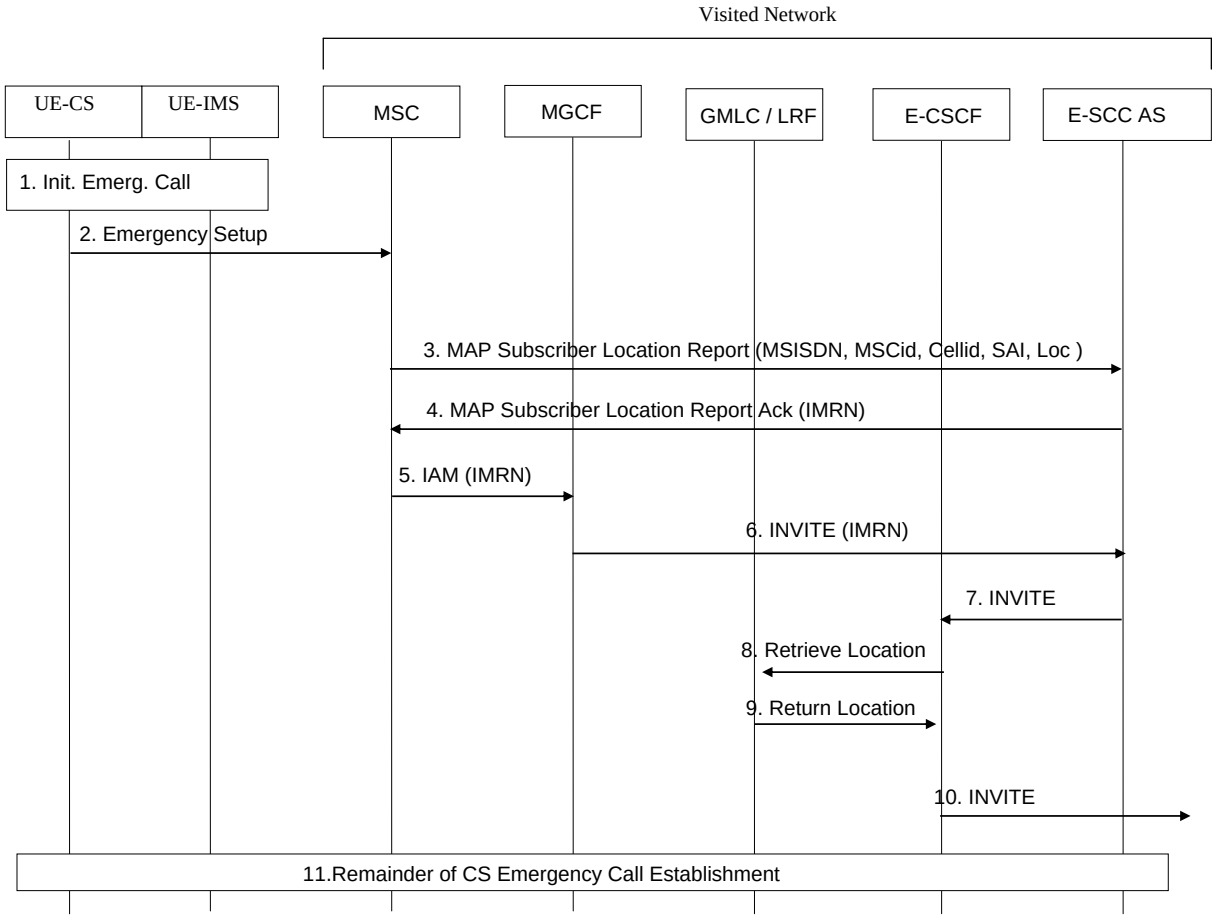


Figure 6.3.4.2-2: CS Emergency Call Origination

1. The user initiates an emergency call.

2. The UE originates an emergency voice call in the CS domain by sending an Emergency Setup message to the VMSC (as defined in TS 24.008 [12]). The VMSC is configured so that it does not initiate an interim location estimate.

3. Based on normal handling for all CS emergency calls (e.g. as described in TS 23.271 [11]) the VMSC sends a MAP Subscriber Location Report (SLR) to an E-SCC AS. To the VMSC, the E-SCC AS interface is the same as a GMLC. The MAP Subscriber Location Report carries the IMSI, MSISDN, IMEI, VMSC address and serving cell identity or SAI for the UE. In regions where the VMSC and not the GMLC normally determines the PSAP (e.g. the EU), the message may carry the address of the intended destination PSAP. For a SIM-less UE, the IMEI is sent along with a MSISDN set to a non-dialable callback number per TS 23.271 [11].

Note: Emergency call handling is centralized in IMS. The MSC is not aware of VCC capable UEs.

4. The E-SCC AS determines the UE supports VCC. The E-SCC AS stores a call record for the UE including all the information received in step 3. The E-SCC AS assigns an IP Multimedia Routeing Number (IMRN) to the call. Minimally, the IMRN enables call routeing to the E-SCC AS in steps 5 and 6. The E-SCC AS returns a MAP Subscriber Location Report Ack to the VMSC carrying the IMRN in the NA-ESRD or NA-ESRK.

   The E-SCC AS can determine if a UE is VCC capable via the HLR/HSS and only anchor those that are VCC capable. For unauthorized UEs, the E-SCC AS will anchor all UEs.

   The IMRN can be static for authorized UEs. For unauthorized UEs, the E-SCC AS allocates a unique IMRN since there is no MSISDN for these UEs.

For UEs that are not anchored, the E-SCC AS will transit the SLR to the LRF/GMLC for legacy GMLC handling without anchoring the call. The E-SCC AS then transits the SLR Ack returned from the GMLC to the VMSC where the VMSC routes the call to the PSAP. The E-RUA remains in the call for transiting SLR/SLRA operations. If the operator desires all emergency calls to be centralized and routed out of the IM CN, the UE can be anchored in IMS like VCC capable UEs. In this case, the E-SCC AS would not have to determine which UEs are VCC capable..

5. The VMSC routes the call based on the IMRN received in step 4. Since the IMRN is conveyed using the existing NA-ESRK or NA-ESRD parameter, the call routeing procedure in the VMSC can be the same as that used for normal emergency call origination in TS 23.271 [11] (i.e. the IMRN appears like an ESRK or ESRD to the VMSC). Based on IMRN routeing, the VMSC routes the call to an MGCF in the visited network.

6. The MGCF initiates an INVITE to the E-SCC AS via the I-CSCF (not shown) in the visited IMS The INVITE contains the identity of the UE (e.g. MSISDN Tel URI as Contact address). The I-CSCF, based on the IMRN, instigates PSI based application server termination to the E-SCC AS. The E-SCC AS retrieves the stored CS call information received in Step 3. This includes available location information received (e.g., MSC/cell id is passed in SIP P-Access-Network-Info header, Location information passed in PIDF-LO).

7. The E-SCC AS anchors the incoming call leg and originates an outgoing leg by sending the INVITE to the E-CSCF. The INVITE carries information identifying an emergency call, including any location info received in Step 3. The location information would be passed in the PIDF-LO and/or P-Access-Network-Information header. The IMRN is released.

8. The E-CSCF sends a retrieve location request to an LRF containing the UE identification received in step 7 – e.g. an MSISDN Tel URI, PIDF-LO, P-Access-Network-Info.

9. Based on any UE identification received in step 8 (e.g. MSISDN), the LRF interacts with the GMLC per 23.892 [7] to retrieve additional location information if necessary. The LRF then interacts with an RDF if necessary to obtain emergency routeing information. The LRF returns a PSAP address, optionally location information, and depending on local regulation an ESRK to the E-CSCF. The LRF will provide the anchor point for further support of location.

10. The E-CSCF uses the PSAP address provided in step 9 and sends on the call request including the location information and any correlation information to the emergency centre or PSAP. The call request is either sent via an MGCF/MGW into the PSTN (not shown) or is sent directly as a SIP INVITE towards an IP capable emergency centre or PSAP.

11. The rest of the call establishment procedure occurs between the UE, VMSC, VCC DTF, E-CSCF and PSAP based on the VCC CS origination procedure described in TS 23.206 [3].

The above procedure preserves support for existing PSAP routeing options (e.g. using cell ID or an interim location estimate), except for configuration, this solution does not require any new impacts to MSCs and supports accurate location retrieval by the PSAP in the manner currently defined in TS 23.271 [11]. It also enables CS originated emergency calls to be sent to IP capable PSAPs.

6.3.4.3 Domain Transfer IMS to CS

The following procedure describes domain transfer for an IMS emergency call from the IMS domain to the CS domain when the UE moves out of IMS coverage and into CS coverage. This callflow is similar to the the IMS to CS Domain Transfer scenario in clause 6.2.4.3 except the MAP Subscriber Location Report (SLR) is sent to an E-RUA instead of a GMLC for IMRN assignment. To the VMSC, the E-RUA interface is the same as that of a GMLC on an emergency call origination. Like the CAMEL interface in a non-emergency CS origination, the SLR is used to assign an IMRN so

the call can be routed to the IM CN for Domain Transfer. Once the Domain Transfer request is received in the IM CN, the LRF is invoked to update the LRF with the serving system location information.

As in procedure 6.2.4.4, this procedure can be applicable to a UE whether or not it has sufficient credentials to register in the new visited network and enables continuity of location support without limitation. However, it may have to be restricted to domain transfer between networks belonging to the same operator (e.g. networks sharing the same MCC and MNC). The procedure requires a new variant of VCC domain transfer in the UE in which knowledge of a VDN is not needed.

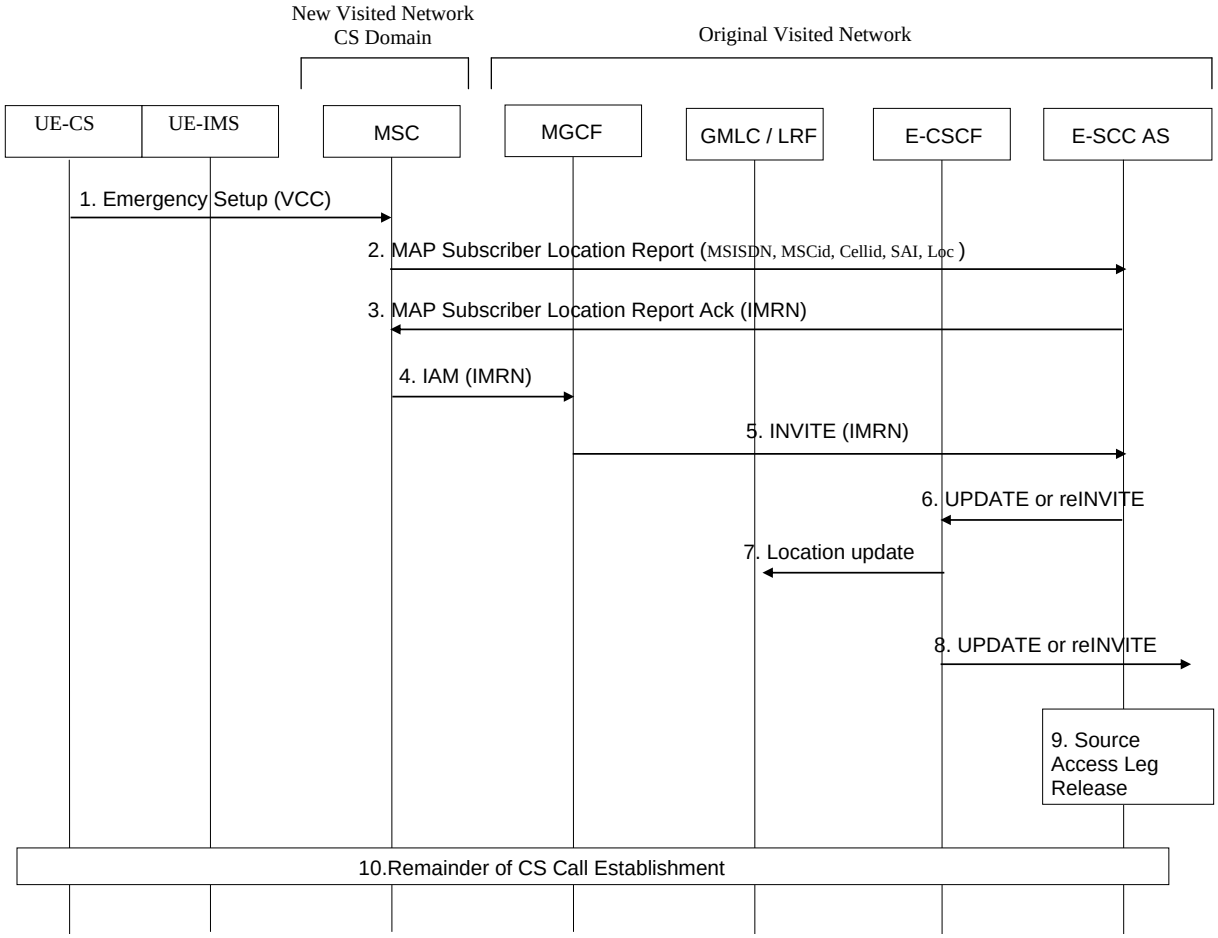


Figure 6.3.4.3-1: IMS to CS domain transfer

1. If the user is not attached to the CS domain at the time when the UE determines a need for Domain Transfer to CS, the UE may perform a CS Attach if it contains the necessary credentials. It subsequently originates an emergency voice call in the CS domain by sending an Emergency Setup message to the VMSC (as defined in TS 24.008 [12]).

2. Based on normal handling for all CS emergency calls (e.g. as described in TS 23.271 [11]) the VMSC sends a MAP Subscriber Location Report to the E-SCC AS. The MAP Subscriber Location Report carries the same information as that which would be sent for a normal emergency call origination (e.g. as in step 3 in Figure 6.3.4.2-1) including the IMSI, MSISDN, IMEI, VMSC address and serving cell identity or SAI.

NOTE: The VMSC is configured to so it does not initiate location determination during emergency call originations. Location determination is centralized in IMS.

3. The E-SCC AS stores the UE information received in the SLR in the call record for the UE that was originally established when the call was anchored. The E-SCC AS may use the IMSI, MSISDN and/or IMEI received in step 2 to identify the correct call record. Note that in the case of an unauthenticated emergency call, the IMEI would have to be used to identify the call record. If no call record is found, the E-SCC AS handles this as a new emergency call and proceeds as in Figure 6.3.4.2-1. Otherwise, if the call record is found, the E-SCC AS returns a MAP Subscriber Location Report Ack. to the VMSC carrying the IMRN needed to establish the new access

leg. The IMRN could be carried by the existing NA-ESRK or existing NA-ESRD parameter in the MAP Subscriber Location Report Ack. The E-SCC AS also stores the information received from the VMSC in step 2.

4. The VMSC routes the new leg based on the IMRN received in step 3. If the IMRN is conveyed using the existing NA-ESRK or NA-ESRD parameter then the call routeing procedure can be the same as that used for normal emergency call origination (i.e. there would be no additional VMSC impact). Based on IMRN routeing, the VMSC routes the call towards the original visited IMS network via an MGCF in the original visited network.

5. The MGCF initiates an INVITE towards an I-CSCF in the original visited IMS (not shown) or possibly the MGCF routes directly to the E-RUA.

6. The E-SCC AS interacts with the E-RUA to determine this is a domain transfer for an ongoing call. The E-SCC AS updates the outgoing Access Leg by communicating the SDP of the Access Leg established in the transferring-in domain to the remote end via the E-CSCF. The E-SCC AS also includes any stored location information that was stored by the E-RUA from Step 3. Access Leg update happens according to SIP session modification procedures in IETF RFC 3261. The E-SCC AS may also explicitly indicate CS domain transfer to the E-CSCF.

7. The E-CSCF sends a Location Update or SIP re-INVITE or SIP UPDATE to the anchor LRF with the new location and SDP information. The E-CSCF may indicate to the LRF that there has been a CS domain transfer. The LRF will note the domain change and interact with the appropriate GMLC if necessary. The LRF may not have to interact with a GMLC until the PSAP requests a location update. The LRF determines the appropriate GMLC based on the serving MSC identity received in step 3 and passed in the P-Access-Network-Info.

8. The update continues towards the PSAP or MGCF.

9. The new call leg in the transferring-in CS domain is established between the VCC DTF, E-CSCF or S-CSCF if present, I-CSCF if present, MGCF, VMSC and UE.

10. The source Access Leg which is the Access leg previously established over IMS is released. The UE should de-register if possible in the visited network P-CSCF and home network S-CSCF.

Like the IMS to CS procedure in 6.2.4.4, besides possibly allowing domain transfer for unregistered UEs, this procedure also enables the anchor LRF to make use of the normal location procedure defined in TS 23.271 [11] (e.g. in clause 9.1.3) to locate a UE that has originated an emergency call. This is enabled due to steps 2 and 3 in Figure 6.3.4.4-1 in which the VMSC obtains and stores information concerning the E-SCC AS, and the LRF and GMLC obtain and store information concerning the VMSC. This then permits a CS-MT-LR without the need to query the UE's home HSS/HLR.

A further aspect of this procedure is that the call origination procedure at the VMSC can be identical to that for a normal emergency call as described in TS 23.271 [11] or identical that for VCC support for a CS originated emergency call as described in clause 6.3.4.2. From the perspective of the GMLC, the procedure is also almost identical to that for a normal emergency call with regard to the MAP signalling transaction with the VMSC.

A disadvantage of this procedure is that it depends on the E-SCC AS finding the original call record so that the domain transfer can be distinguished from a new emergency call origination. This seems to be possible provided the VMSC and E-RUA belong to the same operator and the UE is aware of VCC for Emergency Call support by that operator.

6.3.4.4 Domain Transfer CS to IMS

This procedure is similar to that in 6.2.4.6.

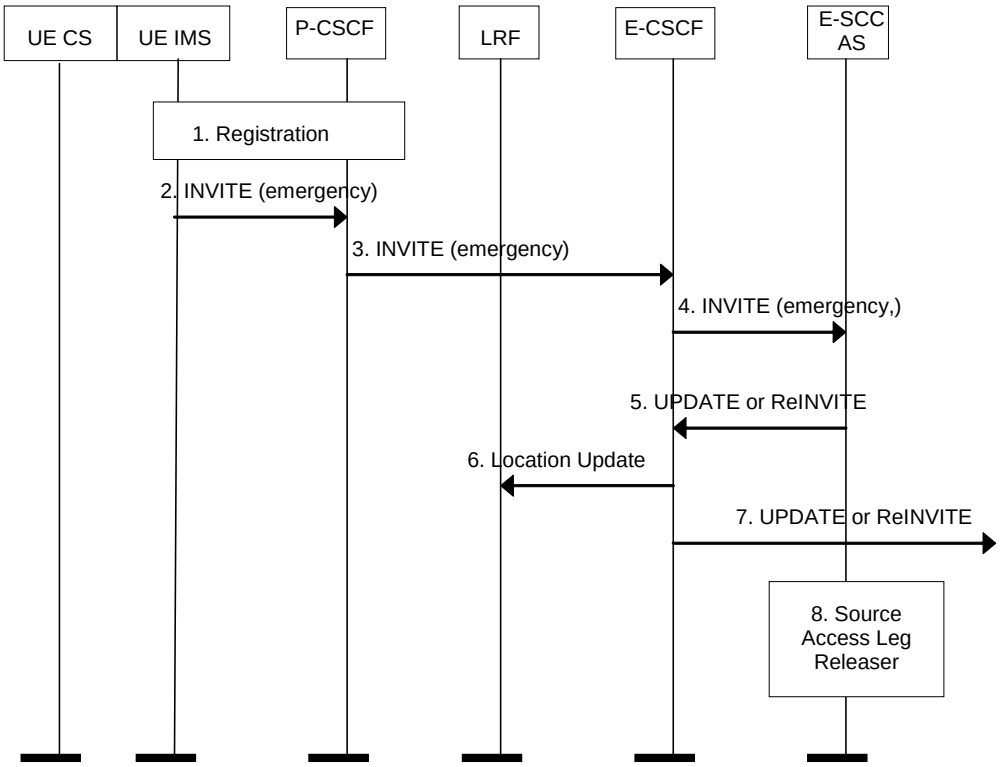


Figure 6.3.4.4-1: Domain Transfer CS domain to IMS

1. Prior to sending the INVITE, the UE executes an emergency registration in the new visited IMS network if it contains adequate credentials as defined in TS 23.167 [4] (i.e. a normal registration is not used). This will be needed to support call back to the UE (via the new visited network) and to authenticate the UE in the new visited IMS.

2. The UE then sends an INVITE with an emergency indication to the visited network P-CSCF. The INVITE should contain identification information for the UE – e.g. MSISDN Tel URI. The INVITE may indicate that the UE supports VCC and may indicate that this is a request for domain transfer as opposed to a call origination. This indication may be conveyed in a modified VDI (see clause 6.2.2.3) carried in the SIP To header field – in which case no separate emergency indication may be needed. A UE without credentials would include its IMEI as its identity.

3. The P-CSCF forwards the SIP INVITE to an E-CSCF.

4. The E-CSCF based on assumption or knowledge of VCC support (e.g., domain transfer indication in the INVITE), forwards the SIP INVITE to the E-SCC AS that has this call anchored.

5. The E-SCC AS finds the original call record and updates the outgoing Access Leg by communicating the SDP of the Access Leg established in the transferring-in domain to the remote end via the E-CSCF. The E-SCC AS may also explicitly indicate domain transfer to the E-CSCF. If the E-SCC AS does not find the original call record and no indication was received in the INVITE that this was a request for domain transfer, it means that this is a new emergency call (not a domain transfer). However, if no call record is found and the INVITE does indicate a request for domain transfer, the E-SCC AS should reject the domain transfer request, in which case the UE must continue with the call in the CS domain or release the call if that is not possible.

6. The E-CSCF updates the anchor LRF with the new SDP information – e.g. indicates that the UE is now using the IMS domain and provides the UE IP address.

7. The update continues towards the PSAP or MGCF.

8. The source Access Leg which is the Access leg previously established over CS is subsequently released as specified in TS 23.206 [3]. This includes releasing the previous incoming CS leg through the E-CSCF.

Continuing location support can be supported by using OMA SUPL with the UE IP address provided to the anchor LRF in step 5 or using the 3GPP PS-MT-LR procedure for location with GPRS access.

A disadvantage is that it depends on the E-SCC AS finding the original call record in step 4 which in turn requires that the P-CSCF or E-CSCF route the call to the correct E-SCC AS in step 3. This is likely to be possible only for domain transfer to the IMS of the original visited network operator.

6.4 Emergency Session Continuity in the Visited Network – Alternative 4

6.4.1 General

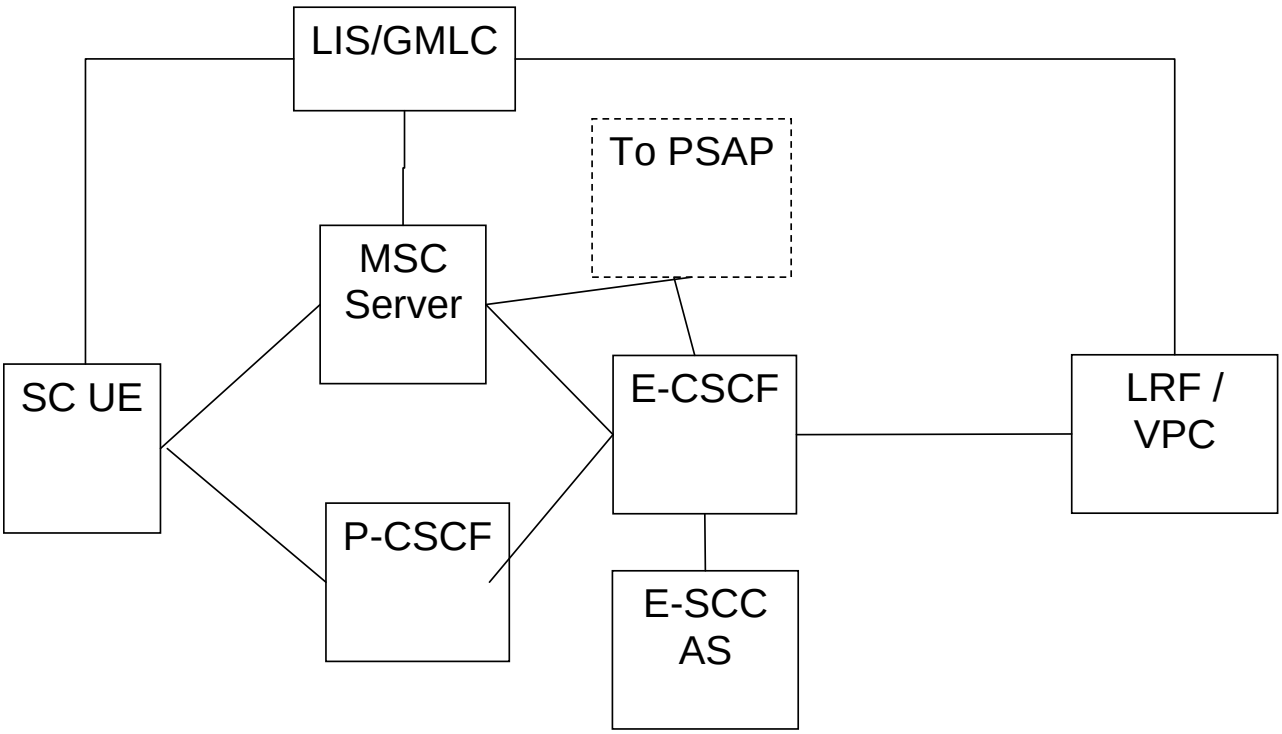
This clause presents an architectural alternative for enablement of Session Transfers for Emergency Calls between CS domain and IMS, which may be invoked multiple times in either direction while the user is engaged in an Emergency call. The solution is applicable to Emergency Calls made by authorized users only. This solution assumes that the network has been fully upgraded with enhanced MSC servers supporting the VCC emergency.

The solution extends the SC architecture specified in TS 23.237 [13] using the following architectural principles:

- IMS Emergency call setup procedures are used for establishment of Emergency Calls using IMS and Session Transfers to IMS.
- Emergency sessions established over CS (both UE detected and MSC detected) of authorized users cause the MSC Server to perform IMS emergency registration if needed, and to origin an IMS emergency session towards the E-CSCF.
- The Emergency SCC AS (E-SCC AS) function, extending the SCC AS defined in TS 23.237 [13], performs anchoring of emergency sessions in the visited IMS domain and executes session transfer..
- Session Transfers are executed by the E-SCC AS by switching the Access Leg from the transferring-out domain to the transferring-in domain, and by updating the Remote Leg if necessary.
- Emergency sessions established over CS by unauthorized users are not supported in this solution therefore, are routed by the MSC to the PSAP directly.
- It is assumed that the CS, PS, and IMS operators are the same.
- If call back is required, session transfer from PS to CS of the emergency call is only allowed in the serving (visited if roaming) network when the user is registered by the MSC server and allowed to use ICS in the serving (visited if roaming) network. The MSC Server has to perform registration in IMS if call back has to be supported when using CS access.

6.4.2 Reference Architecture

The reference architecture is provided in Figure 6.4.2-1 below.



NOTE: Only relevant standard functions are shown.

Figure 6.4.2-1: Emergency Session Continuity Architecture

The E-SCC AS is an SCC AS as defined in TS 23.292 [10] and TS 23.237 [13] enhanced for emergency session continuity. The E-SCC AS may be co-located with the E-CSCF.

6.4.3 Procedures

6.4.3.1 Registration in IMS

A pre-requisite is for the UE is to be IMS registered over the PS access, in accordance with the requirements in TS 23.167 [4]. The registration in the IMS by the MSC Server enhanced for ICS is specified in TS 23.292 [10], and may be performed if the UE is attached to CS, and holds an ICS subscription.

6.4.3.2 Emergency calls established in IMS

The figure 6.4.3.2-1 provides an example flow for an emergency session established in IMS, illustrating how the emergency session is anchored and how the session transfer identifiers are transported back to the UE.

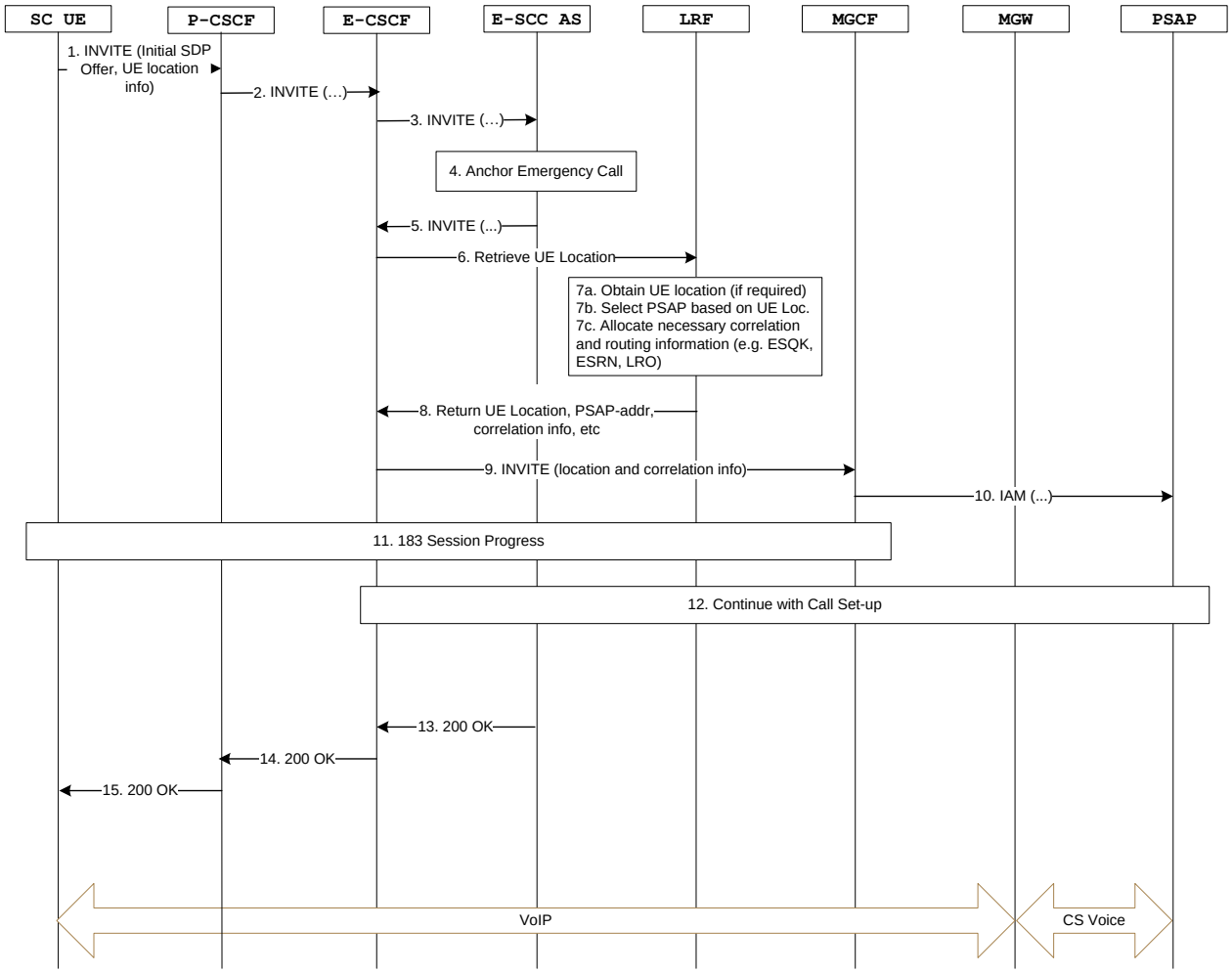


Figure 6.4.3.2-1: SC UE initiating an emergency session in IMS

NOTE 1: A pre-requisite is for the SC UE to be IMS Emergency Registered if located in a VPLMN or located in the HPLMN and IMS Registered.

1. The SC UE generates a SIP INVITE containing the UE's location information or reference (if available) and information about the device, e.g., GRUU.

NOTE 2: The UE indicates in the Invite that it supports the E-VCC functionality.

2. The P-CSCF selects an E-CSCF and forwards the INVITE to the E-CSCF.

3. The E-CSCF sends the INVITE to the E-SCC AS. The E-SCC AS decides based on operator policy and UE capability whether to anchor the emergency session.

NOTE 3: The trigger for routeing the INVITE from the E-CSCF to the E-SCC AS could be as simple as configuring the E-CSCF with the address of the E-SCC AS located in a local IMS network designated to perform the functions of call/session anchoring and session transfers.

4. The E-SCC AS anchors the emergency session, i.e. the E-SCC AS is inserted in the signalling path which invokes a 3pcc for enablement of Session Transfers for the call as specified in TS 23.237 [13].

NOTE 4: The E-SCC AS will indicate in the response back to the UE that the call has been anchored and E-VCC function is used.

5. The E-SCC AS creates an INVITE and sends it back to E-CSCF.

6. The E-CSCF sends the INVITE to the LRF

7. The LRF obtains the UE's location (if not provided in the INVITE), selects the most appropriate PSAP based on the UE's location, allocates the necessary correlation information for the record stored in the LRF (e.g. ESQK) and allocates routeing information for the call (e.g. ESRN).

8. The LRF returns the location information, PSAP address, correlation information (e.g. ESQK) and routeing information (e.g. ESRN) to the E-CSCF.

9. The E-CSCF uses the PSAP address or routeing information (e.g. the ESRN) to format an INVITE message, and it sends it to the MGCF.

10. The MGCF performs the necessary interworking of the INVITE and formulates an IAM containing the correlation information (e.g. ESQK) and sends it to the PSAP.

11. The MGCF initiates 183 Session Progress through the IMS core back to the UE

12. Call set-up continues with the PSAP sending ACM/ANM back to the MGCF which is interworked into a 200OK and sent through the IMS Core Network.

13. The E-SCC AS receives the 200 OK from the E-CSCF and sends the 200 OK to the E-CSCF

14. The E-CSCF sends the 200 OK to the P-CSCF

15. The P-CSCF sends the 200 OK to the UE

6.4.3.3 Emergency Calls established in CS

The figure 6.4.3.3-1 provides an example flow for an emergency call established in CS, illustrating how the emergency session is anchored and how the location reference is provided to the LRF. In this flow, the MSC Server recognises the CS bearer set-up as a request to make an emergency call and carries out the IMS emergency call registration prior establishing an IMS emergency call.

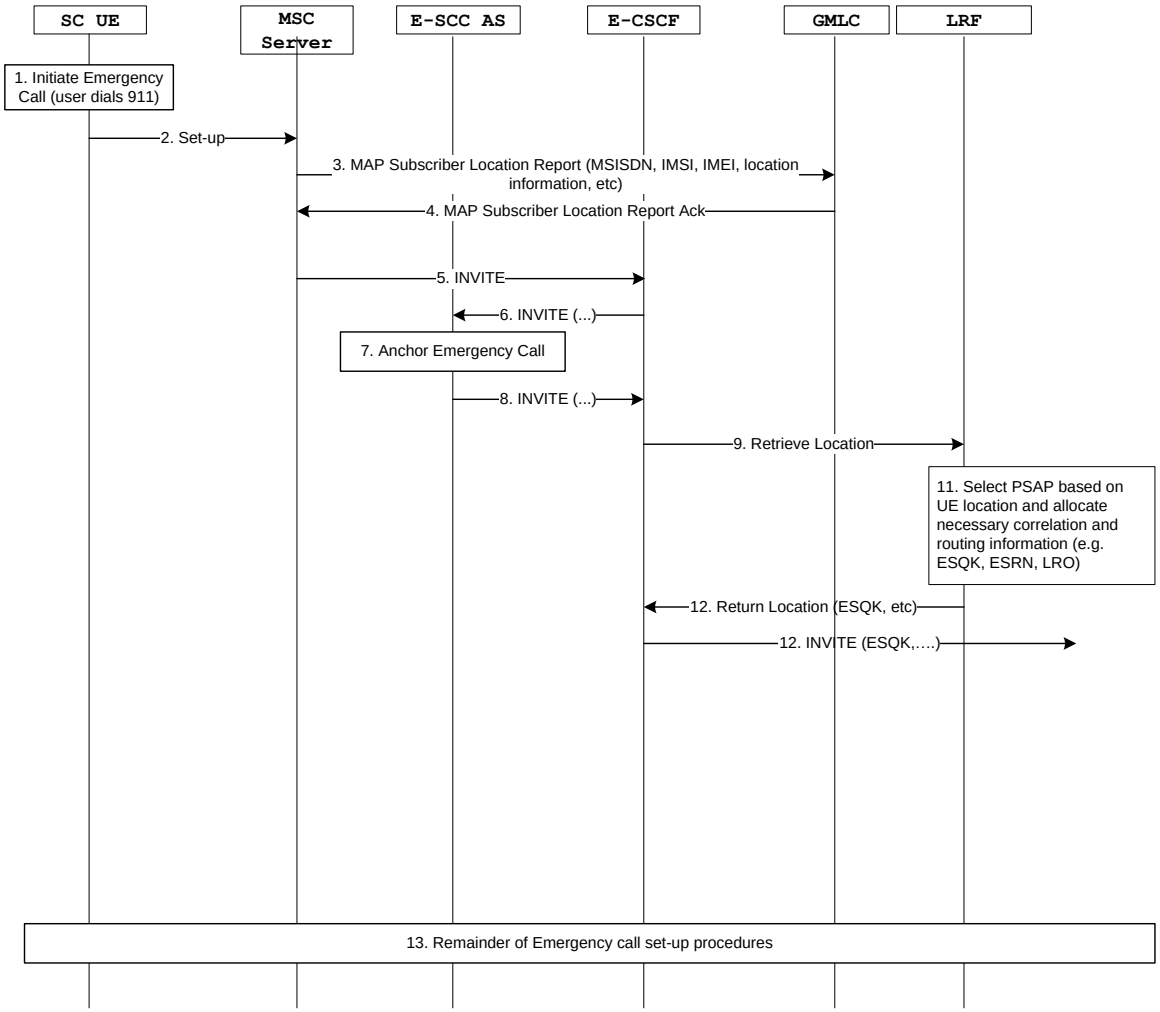


Figure 6.4.3.3-1: SC UE initiating an emergency call in CS

NOTE 1: This call flow is depicting the LRF acting in Re-direct mode. The procedure is also applicable when the LRF acts in Proxy mode.

1. The user initiates an emergency call (e.g. dials 911).

2. The UE sends an Emergency call setup message (as defined in TS 24.008 [12]) to the MSC Server.

3. The MSC Server carries out standard CS emergency procedures. This involves the MSC Server sending a MAP Subscriber Location Report (SLR) request to the GMLC allocated to the geographical region that the UE is roaming within. The MAP Subscriber Location Report carries the IMSI, MSIDN, IMEI, VMSC address, serving cell identity or SAI for the UE.

4. Based on the received information, the GMLC creates a call context, stores the received location information (ESRK/ESRD) and returns the MAP-SLR response to the MSC Server.

NOTE 2: Based on operator policy, the MSC Server decides whether to route the emergency session to the IMS. Only if the MSC Server decides to route the emergency session to the IMS, the following steps are performed.

NOTE 3: The MSC Server performs an IMS emergency registration on behalf of the UE in the new visited IMS network if the UE is not already IMS emergency registered (see clause 6.4.3.1). When the MSC Server is located in the home network and has already IMS registered the UE then there is no need to perform an IMS emergency registration.

5. The MSC Server selects the E-CSCF for the geographic region (local configuration), maps emergency types to sos-urn, and generates an Emergency SIP INVITE towards the E-CSCF including information about the used

device, e.g., GRUU. Since the MSC Server has location information available, it includes it in the request as in the Emergency INVITE.

6. The E-CSCF sends the INVITE to the E-SCC AS.

7. Based on operator policy and UE capability, the E-SCC AS anchors the session, i.e. the E-SCC AS is inserted in the signalling path which invokes a 3pcc for enablement of Session Transfers for the call as specified in TS 23.237 [13].

8. The E-SCC AS sends the INVITE to the E-CSCF.

9. The E-CSCF sends a Retrieve Location request to the LRF that is associated with the geographical region. This request includes the UE identification (contents of the P-Asserted-Identity) and the location-reference, etc.

10. The LRF creates an emergency call instance and stores the location-information against the emergency call instance. Based upon the location information, the LRF interacts with an RDF to obtain routeing information for the emergency call. The LRF may allocate an ESQK that identifies the call instance in the LRF. The ESQK is correlation information that allows the PSAP to request a location update from the LRF.

11. The LRF returns the ESQK, the PSAP address or routeing information and location-information (location reference and explicit location information) to the E-CSCF.

12. The E-CSCF uses the PSAP address or routeing information provided in Step 8 to send the call to the PSAP. The call request is either sent via an MGCF/MGW in the PSTN towards a PSTN-capable PSAP (not shown) or is sent directly as a SIP INVITE towards an IP-capable PSAP (not shown).

13. The rest of the call establishment procedure occurs between the UE, MSC Server, E-SCC AS, E-CSCF and PSAP based upon the SC CS origination procedure.

6.4.3.4 Session Transfer from IMS to CS

The figure 6.4.3.4-1 provides an example flow for session transfer of an emergency session from IMS towards the CS domain.

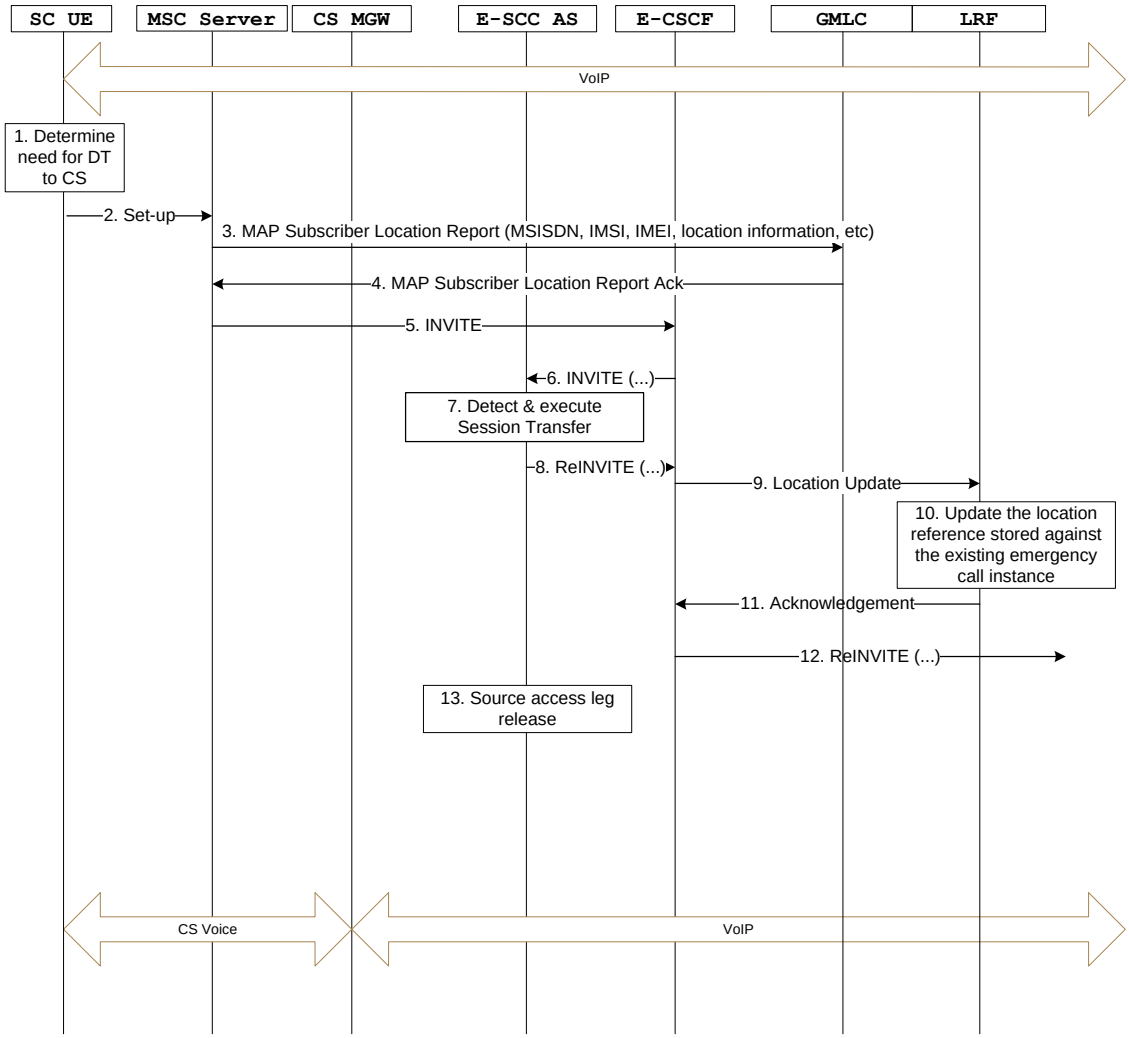


Figure 6.4.3.4-1: SC UE performing session transfer from IMS to CS domain

1. The UE detects the necessary conditions and determines the need for session transfer

2. The UE sends an Emergency call setup message (as defined in TS 24.008 [12]) to the MSC Server.

NOTE 1: A pre-requisite for performing the session transfer is that the UE during the initial emergency call establishment received an indication that the session has been anchored and E-VCC is allowed.

3. The MSC Server carries out standard CS emergency procedures. This involves the MSC Server sending a MAP Subscriber Location Report (SLR) request to the GMLC allocated to the geographical region that the UE is roaming within. The MAP Subscriber Location Report carries the IMSI, MSIDN, IMEI, VMSC address, serving cell identity or SAI for the UE.

4. Based on the received information, the GMLC creates a call context, stores the received location information and returns the MAP-SLR response to the MSC Server.

NOTE 2: Based on operator policy, the MSC Server decides whether to route the emergency session to the IMS. Only if the MSC Server decides to route the emergency session to the IMS, the following steps are performed.

5. The MSC Server selects the E-CSCF that the UE is anchored to and generates an Emergency SIP INVITE (Request-URI set to a sos-urn) towards the E-CSCF including information about the used device, e.g., GRUU. Since the MSC Server has location reference (ESRK/ESRD) available, it includes it in the request as in a standard Emergency INVITE.

6. The E-CSCF sends the INVITE to the E-SCC AS.

7. The E-SCC AS detects the incoming INVITE to be a Session Transfer request since having anchored an emergency session for the same user from the same device, e.g. identified by the GRUU. The E-SCC AS performs session transfer as defined in TS 23.237 [13].

8. The E-SCC AS sends the ReINVITE to the E-CSCF to update the remote end.

9. The E-CSCF sends a Location Update request to the LRF that is associated with the initial call instance, to update the LRF with the new location reference for the UE due to the session transfer.

NOTE 3: The LRF is not changed when establishing the call in PS.

10. The LRF finds the emergency call instance using the information supplied in the Re-INVITE (e.g., P-Asserted-Identity, GRUU) and updates the location reference stored against the emergency call instance.

11. The LRF sends an acknowledgment back to the E-CSCF to allow the E-CSCF to forward the Re-INVITE to the currently allocated PSAP.

12. The E-CSCF forwards the Re-INVITE to the MGCF associated with the PSAP (if the PSAP is located in the PSTN) or the Re-INVITE is sent directly to an IP-capable PSAP.

13. When session modification procedures complete, the source access leg (i.e. the access leg previously established over IMS) is released.

NOTE 4: Releasing the source access leg does not result in releasing the resources (e.g. ESQK) allocated to the emergency call.

6.4.3.5 Session Transfer from CS to IMS

The figure 6.4.3.5-1 provides an example flow for session transfer of an emergency session from the CS domain towards IMS where CS, PS and IMS operator are the same.

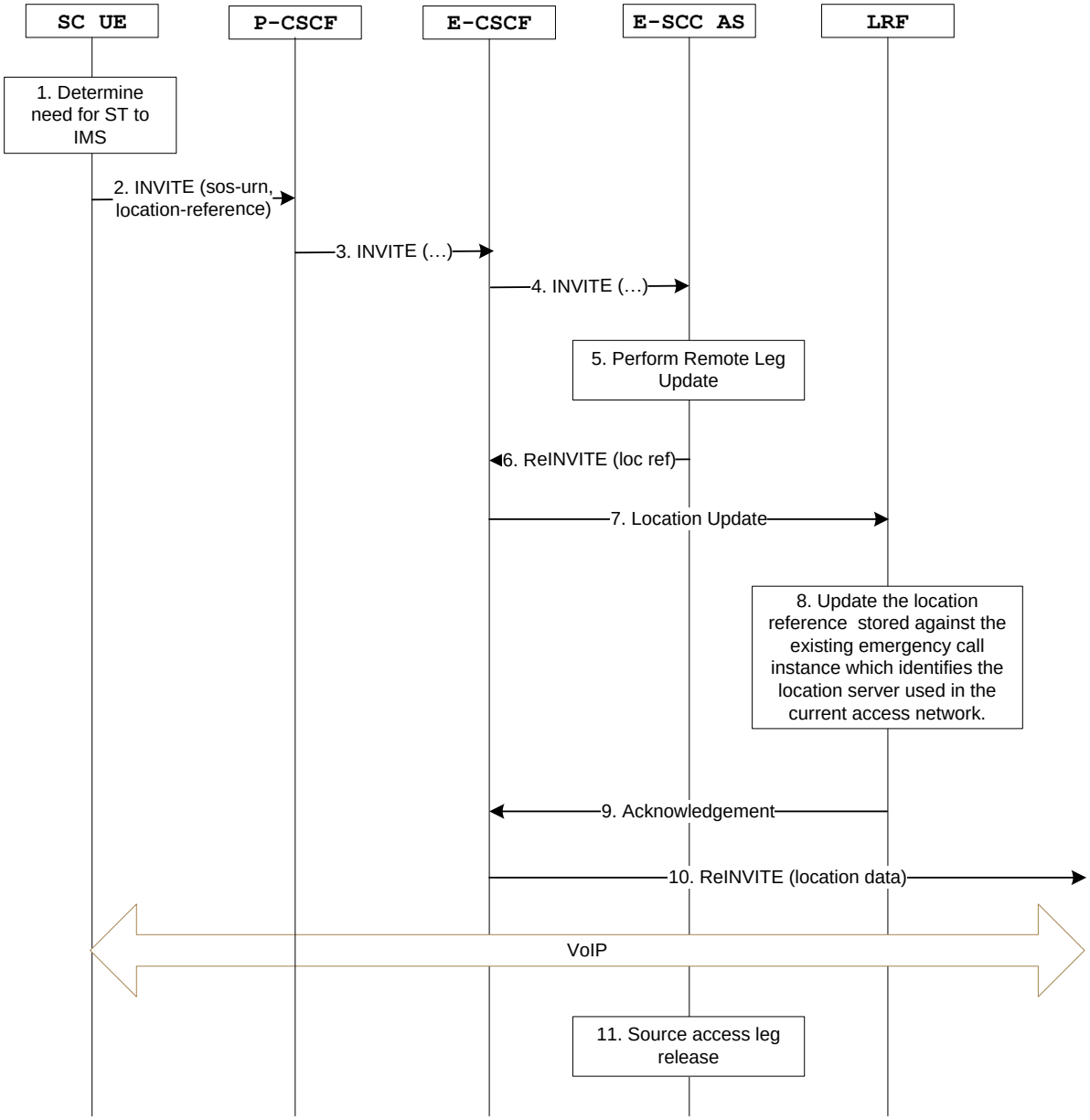


Figure 6.4.3.5-1: SC UE performing session transfer from CS domain to IMS

1. The UE detects the necessary conditions and determines the need for session transfer

NOTE 1: The UE performs an IMS emergency registration in the new visited IMS network if the UE is not already IMS emergency registered (e.g. the UE may already be IMS emergency registered in the case the UE is doing a domain transfer back to IMS). When the UE is located in the home network and is already IMS registered there is no need to perform an IMS emergency registration.

2. The UE sends a request for session transfer from CS to IMS by setting up an IMS originated Emergency session (towards the P-CSCF). This establishes the transfer leg of the emergency call (i.e. the new access leg via IMS). The INVITE may also include updated location information for the UE.

NOTE 2: A new emergency session request received at the E-SCC AS while there's already an active emergency session for same user from the same device, e.g. identified by the GRUU, is considered a Session Transfer request as there can only be one emergency session for a user at any given time.

3. The P-CSCF routes the INVITE to the E-CSCF.

NOTE 3: The P-CSCF may initiate a procedure (as described in TS 23.167 [4]) to obtain the location reference from the IP-CAN.

4. The E-CSCF routes the INVITE to the SCC AS (as it is configured to send all requests for the SC user to the E-SCC AS).

5. The E-SCC AS identifies the anchored call/session from the P-Asserted-Identity and then completes the establishment of the Access Leg via IMS

6. The E-SCC AS then performs the session transfer by updating the remote leg with the connection information (SDP) of the newly established Access Leg by sending a Re-INVITE to the E-CSCF with the updated location information.

7. The E-CSCF sends a location update request to the LRF containing the location reference for the new access network. The request also contains information that enables the LRF to identify the existing emergency call instance (e.g., P-Asserted-Identity, GRUU).

NOTE 4: The LRF is not changed when establishing the call in PS.

8. The LRF overwrites the existing location reference in the emergency call instance with the one provided in the location update request. The LRF finds the most appropriate location server and positioning method for the current access network and stores this information against the currently allocated emergency call instance.

9. The LRF sends an Acknowledgement back to the E-CSCF

10. If the PSAP is located in the IP network, the Re-INVITE sent out by the E-CSCF is extended all the way to the PSAP (i.e. the u-plane path between the UE and the PSAP is switched end-to-end). If the PSAP is located in the PSTN, the E-CSCF forwards the Re-INVITE to the MGCF associated with the PSAP.

11. When session modification procedures complete, the source access leg (i.e. the access leg previously established over CS) is released.

NOTE 5: Releasing the source access leg does not result in releasing the resources (e.g. ESQK) allocated to the emergency call.

7 Evaluation

Use the following assumptions to help define the evaluation criteria for each architectural option to agree on a solution in the Release 9 timeframe.

1) Only allow the support of IMS to CS session continuity for Emergency calls to satisfy the minimal requirements stated in TS 22.101 [13] and clause 4.1 of this TR.

2) No support of transitioning of emergency calls from CS to IMS for cases of CS originated calls and hand-back of calls originated in IMS.

3) VCC for emergency shall only be attempted for intra-operator transitions (where serving IMS and serving CS core operators are the same).

4) UE shall not attempt to perform transfer of an emergency call if it is not certain the relevant capabilities are supported by the network (covers UICC-less case also).

The following criteria should be used to compare the architectural options:

1) The degree to which the solution minimizes the impact to existing CS core and IMS network elements (e.g., IMS core elements, MSC Server)

2) The capabilities that each architectural option provides that are required for the solution (e.g. location continuity, priority of calls)

Table 7.1-1 defines the comparison criteria for each architectural option which covers capabilities and impacts.

Table 7.1-2 highlights the functionality implemented by each component for each architectural option.

NOTE: The evaluation of Alternative 1 is based upon clause 6.1.3 Assessment which provides an overview of the proposed solution.

Editor's Note: The evaluation of the alternatives has not been fully reviewed and completed.

Table 7.1-1: Capability and Impacts comparison

Comparison criteria	Priority	Alt 1	Alt 2	Alt 3	Alt 4
List of new and existing components impacted		E-SCC-AS, MSC, E-CSCF, LRF	All variants: UE, VCC DTF, LRF, GMLC, E-CSCF, MGCF Variant C: MSC	E-SCC-AS, LRF, E-CSCF, UE	
Impacts to the MSC		MSC changes required to route the emergency request using the STN once emergency call procedures have been invoked at the MSC. Solution can exist without changes to the MSC but it means that priority and location update cannot be supported. Architecture allows for use of enhanced MSC server and standard MSC server	Variants A, B: none Variant C: possible impact to recognize and indicate domain transfer to the GMLC in a MAP SLR	No software upgrades if emergency number is used for DT. Requires. MSC configuration changes to appear to be interfacing w/GMLC when it is actually the E-SCC-AS	
Impacts to the GMLC		The GMLC associated with the legacy MSC needs to support the LRF interface.	A: establish a call record based on data from the LRF for IMS to CS domain transfer (DT) B, C: query the LRF to find and copy a call record when a MAP SLR is received from an MSC indicating DT or possible DT; provide the VCC DTF address to the VMSC in the SLR response All: support location requests from the LRF after DT using an existing MT-LR for CS emergency calls C: possible additional impact to detect a domain transfer indication in a MAP SLR	The GMLC associated with the legacy MSC needs to support the LRF interface.	
Impacts to the LRF		Requires support for location update procedure between the E-CSCF and the LRF.	A: provide a call record to the GMLC for IMS to CS domain transfer B, C: find and provide a call	LRF is made VCC aware (records that a DT has taken place and subsequently updates LRF to use CS location server to obtain	

Comparison criteria	Priority	Alt 1	Alt 2	Alt 3	Alt 4
			record when queried by the GMLC for IMS to CS domain transfer All: transfer any location request from the PSAP to the GMLC after DT	location information).	
Impacts to the E-CSCF		If selective anchoring required, E-CSCF may need to ensure that not all requests are sent to the E-SCC-AS for anchoring/domain transfer. Requires the capability to request an update of location towards the LRF.	All: determine VCC support by a UE and route an IMS emergency origination to the VCC DTF. Detect a domain transfer and update the LRF	If selective anchoring required, E-CSCF may need to ensure only VCC capable requests are sent to the E-SCC-AS for anchoring and domain transfer.	
Impacts to the MGCF		ESRK/ESRD passed into IAM and inter-worked into PIDF-LO in the INVITE.	All: some ISUP to SIP signalling conversion for domain transfer	None.	
Impact to CS Access Signalling		None	No changes	None.	
Impacts (and mechanism) related to routeing of CS calls to IMS (domain transfer)		Use Normal Set-up towards STN which MSC recognises as an Emergency Call. Use translations based routeing at the MSC by routeing on the STN after emergency procedures invoked towards the GMLC. Modifications required at MSC. For a standard MSC, routeing occurs on the STN with no execution of CS emergency call procedures.	A: CS side treats DT as a normal call routed to the VCC DTF using a VDN (or STP) B: MSC sees DT as an Emergency call and queries GMLC which finds the call record in the LRF and returns a VDN (or STN) to the MSC C: as B, but MSC is also aware of DT and signals this to the GMLC to improve DT reliability	Uses an Emergency Set-up. MSC sends MAP-SLR for the Emergency request to the E-SCC-AS to obtain an STN (if call record found in the E-SCC-AS). MSC uses STN to route to IMS.	
Impacts (and mechanism) related to obtaining session transfer number for PS to CS DT		E-SCC-AS allocates it as part of the PS emergency session and returns it to the UE for it to store for later use in the CS origination (for DT).	A, C: VCC DTF provides the VDN/STN to the UE on IMS emergency origination in the 200 OK B: does not need a VDN/STN	E-SCC-AS allocates the STN by emulating the GMLC interface when the MSC sends a MAP-SLR request to it to record location estimate.	
Support for handling of DT request when UE		Yes.	A, B: can use a standard MSC server without	Yes, just a config change to route to SCC-AS instead	

Comparison criteria	Priority	Alt 1	Alt 2	Alt 3	Alt 4
attaches to a standard MSC server			new impacts C: may use a standard MSC server without new impacts if SCCP address configuration in the MSC is flexible and SCCP address transfer to the GMLC is reliable; otherwise additional impacts are needed to the MSC	of GMLC.	
Support of (and mechanism for) capability exchange for IMS Originations		Either the E-SCC-AS anchors all calls in IMS, returns the STN which the UE understands or does not. Or, on emergency IMS origination, INVITE contains VCC capability. If visited IMS network supports VCC, STN returned to the UE.	All: can be supported using SIP extensions (e.g. new parameter values or new fields)	SIP extensions: for UE to indicate DT request, and for IMS to indicate to UE VCC support.	
Support of (and mechanism for) location continuity		When using PS signalling channel and standard MSC/enhanced MSC update the location using standard PS location procedures defined in TS 23.167 [4] (note: E-SCC-AS provides PS location ref to E-CSCF rather than CS location ref when enhanced MSC server is used) When not using PS signalling channel and enhanced MSC server, ESRK/ESRD used as a location-reference for the LRF to locate the GMLC and call record. ESRK/ESRD stored against the current emergency call instance in the	A: supported if MSC address can be transferred to the LRF for DT; LRF then obtains location from a GMLC which uses the existing emergency CS-MT-LR procedure B, C: supported by using the existing MAP SLR procedure to establish a call record in the GMLC when DT is invoked; LRF then obtains location from the GMLC which uses the existing emergency CS-MT-LR procedure	E-SCC-AS inserts information like MSC-id and cell-id into the P-visited-network-id and PIDF-LO. E-CSCF indicates to the LRF that there has been a CS domain transfer. LRF (based on this information) updates the emergency call instance.	

Comparison criteria	Priority	Alt 1	Alt 2	Alt 3	Alt 4
		LRF. When attached to an unmodified MSC, then no support for location continuity.			
Support of (and mechanism for) prioritization of the CS bearers and signalling (for DT request)		When using an enhanced MSC server, MSC can provide priority of bearers and signalling. When using a standard MSC, no priority supported.	A: not supported B, C: MSC will see an emergency call or emergency DT and can then prioritize bearers and signalling	Yes – ES setup is used.	
Support for priority on radio channel		None	B: supported A, C: might be supported if the UE indicates a T12 to the BSS; otherwise not supported	Yes – ES setup is used.	
Support for UICC-less UEs		Needs more study	A, C: not supported B: supported using an Emergency SETUP for DT	Yes.	

Table 7.1-2: Functionality implemented by each component

Functionality	Alt 1	Alt 2	Alt 3	Alt 4
Functions of the E-SCC-AS	Anchor call, provide adaptation of the CS origination, provides domain transfer. Provide STN back to the UE.	Anchor an IMS emergency origination; return a VDN/STN to the UE for A and C; detect DT and then release the IMS call leg and substitute the CS call leg	Uses MAP-SLR instead of CAMEL for obtaining IMRN. Anchor call, provide adaptation of the CS origination, provides domain transfer. Provide STN/VCC support indication back to the UE on SIP orig. Acts as a transit for non emergency SLR requests.	
Functions of the MSC-Server	Standard CS Emergency Call Processing, implementation of Priority and routeing call to IMS.	A: treat DT as a normal call origination B: treat DT as a normal emergency call origination C: as B, but also transfer a DT indication to the GMLC	Configuration changes to support CS Emergency Call Processing (i.e. to route to E-SCC-AS and not GMLC).	
Functions of the GMLC	Standard CS emergency call procedures.	A: setup a new call record for DT based on data from the LRF and support further location requests from the LRF B, C: existing MAP SLR procedure used for DT with the addition of finding the call record in the LRF and returning a VDN/STN to the MSC in the SLR response; support of further location requests from the LRF using an existing emergency CS-MT-LR	Nothing new. Std CS emergency call procedures.	
Functions of the LRF	Location updating from E-CSCF. LRF updates the call instance with the ESRK/ESRD which is a reference to the GMLC/user.	A: provide a call record to the GMLC following DT B, C: find and provide a call record to the GMLC when the GMLC queries the LRF for DT	Location updating from E-CSCF. LRF is made "VCC-aware" as it records the fact that a domain transfer has occurred to CS such that a request from the PSAP directs the	

Functionality	Alt 1	Alt 2	Alt 3	Alt 4
		All: send any location requests to the GMLC after DT has occurred	LRF to a GMLC. When there are multiple GMLCs, requires use of visited-MSC address mapping functionality to locate the GMLC.	
Functions of the E-CSCF	Location updating from E-CSCF. May support selective anchoring.	All: determine VCC support by a UE and forward an IMS emergency call origination to the VCC DTF; detect DT and update the LRF	Supports selective anchoring. Location update towards LRF on domain transfer.	
Functions of the UE	UE is VCC-Em capable and may indicate its support for VCC-Em. UE accepts network indication of VCC-Em support (i.e. E-STN)	All: UE is VCC for EMC capable. UE includes an indication of VCC support in the initial SIP INVITE; obtains a VDN (A), indication of VCC support (B) or modified VDN (C) from the VCC DTF in the SIP 200 OK A, C: UE invokes PS to CS DT by sending a normal SETUP to the VMSC containing a VDN (A) or modified VDN (C) B: UE invokes PS to CS DT by sending an emergency SETUP to the VMSC	Must be VCC4Em capable. On CS originations, must be configured with network support for VCC. On PS, must indicate DT and/or VCC support, must accept network indication of VCC4Em support.	

8 Conclusion

8.0 General

Different alternatives have been studied, all of which place the session transfer function for the VCC of emergency calls in the visited IMS network. Some aspects of the study are complete, whereas some other key aspects require further study as recommended below:

8.1 Placement of Session Transfer Function

The session transfer function for the VCC of emergency calls shall be placed in the serving (visited if roaming) IMS network.

8.2 PS to CS Session Transfer

The PS-CS access transfer for emergency sessions of authenticated UEs which are initially established via PS access shall be specified in Rel-09.

8.3 CS to PS Session Transfer

Standard CS domain emergency call procedures shall be applied for emergency calls initially established via CS access. Session Transfer of emergency sessions initially established via CS access shall not be specified in Rel-09 as further studies are required to resolve outstanding key issues.

9 Recommendation

It is recommended not to pursue with the specification of dual radio VCC support of emergency calls in Release 9.

There is no consensus on which alternative to best use for dual radio VCC support of emergency calls.

Annex A:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2009-03	SP-43	SP-090090	-	-	MCC Update for presentation to TSG SA for approval	1.1.0	2.0.0
2009-03	-	-	-	-	Approved at TSG SA#43. Upgraded to Release 9	2.0.0	9.0.0