

CSCF I4 and I5 Interface

Call Session Control Function

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2014–2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
2	Interface Overview	3
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	4
3	Procedures	5
3.1	Emergency Call Establishment over I4 Interface	5
3.2	Emergency Call Access Transfer over I5 Interface	9
3.3	Emergency Call PS Fallback over I4 Interface	11
3.4	Request Within Established Emergency Session	12
4	Information Model	13
4.1	Supported SIP Methods	13
4.2	SIP Header Information	13
5	Formal Syntax	15
6	Security Considerations	17
7	Related Standards	19





1 Introduction

This document describes the interface between the Emergency Access Transfer Function (EATF) and the Call Session Control Function (CSCF) using reference points I4 and I5.

This document only describes the details that are relevant to the I4 and the I5 interfaces. For detailed information about the CSCF Mw Interface, refer to *CSCF Mw Interface*.

Unless otherwise indicated, SIP headers are handled transparently by the Emergency CSCF (E-CSCF), the Interrogating CSCF (I-CSCF), and the EATF over the I4 and I5 interfaces.

For information about status codes generated by the CSCF, refer to *CSCF Fault Codes Catalogue*.



2 Interface Overview

This section describes the interfaces to EATF as shown in Figure 1.

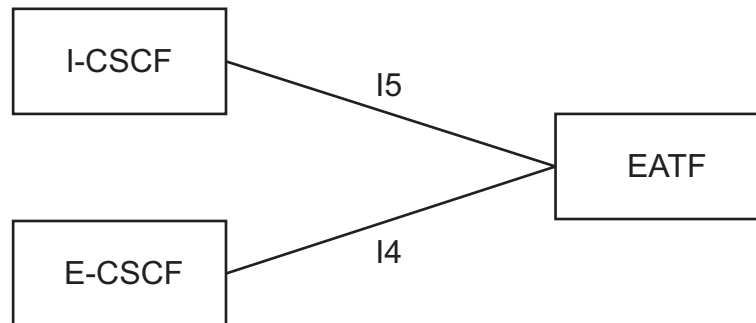


Figure 1 Interface Entities

The I4 interface is between the E-CSCF and the EATF.

The I5 interface is between the I-CSCF and the EATF.

The SIP protocol is used on the I4 and I5 interfaces.

2.1 Interface Role

The I4 interface is used by the E-CSCF and the EATF for emergency call anchoring and Packet Switched Network (PS) Fallback handling. The I5 interface is used by the I-CSCF and the EATF for emergency call access transfer request handling.

2.2 Services

The services offered by the EATF are listed in Table 1.

Table 1 Offered Services

Offered Service	Description
Emergency Call anchoring	An emergency call between the User Equipment (UE) and the Public Safety Answering Point (PSAP) is anchored at the EATF.



Offered Service	Description
Emergency Call access transfer	An emergency call access transfer takes place when the UE of an ongoing emergency session moves from the Packed Switched (PS) network to the Circuit Switched (CS) network. EATF handles the coordination of the related call legs.
Emergency Call PS Fallback	An emergency call PS Fallback takes place when the UE of an emergency session moves from the CS network back to the PS network after an emergency call access transfer. EATF handles the coordination of the related call legs.

2.3 Encapsulation and Addressing

The EATF supports an IPv4/IPv6 dual stack and SIP on UDP and TCP.

The EATF follows the procedures for SIP routing, refer to [RFC 3261 SIP: Session Initiation Protocol](#).

3 Procedures

This section describes the most common signaling sequences over the I4 and I5 interfaces.

3.1 Emergency Call Establishment over I4 Interface

3.1.1 Initial Emergency Request from E-CSCF to EATF

The initial emergency request from the E-CSCF to EATF over the I4 interface is described in Figure 2.

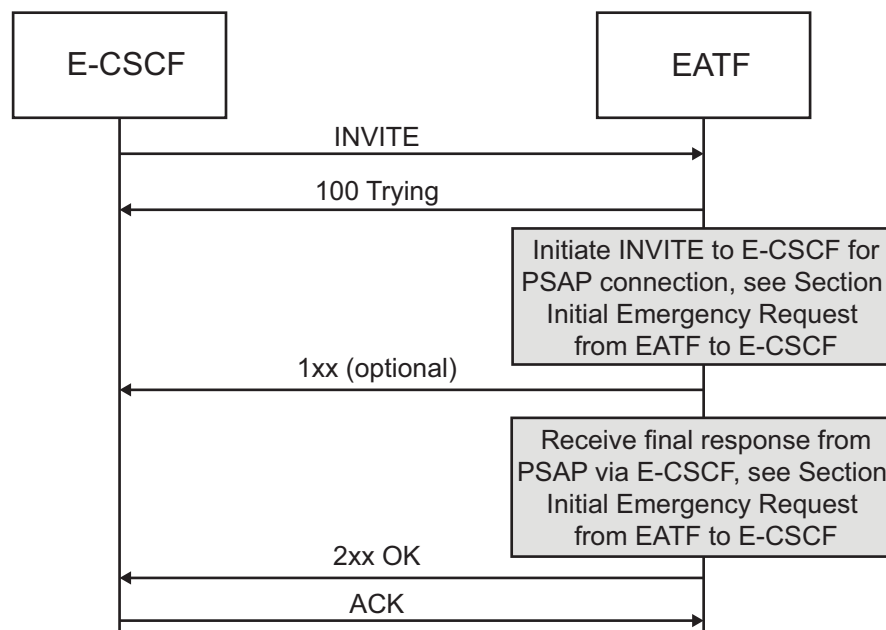


Figure 2 Initial Emergency Request from E-CSCF to EATF over I4 Interface

As illustrated in Figure 2, the E-CSCF anchors an emergency call at the EATF by routing the emergency request to the EATF over the I4 interface. For more information about EATF setup, refer to *CSCF Configuration Management*.

Some related headers are described in Table 2.

Table 2 *Headers of INVITE Request for Emergency Request Sent from E-CSCF to EATF*

Header	Procedure-Specific Values of the Parameter
Route	<ul style="list-style-type: none"> • A top <code>Route</code> header is added to include the address of the EATF in form of a SIP URI • A second <code>Route</code> header is added to include the address of the E-CSCF in form of a SIP URI
Contact	<ul style="list-style-type: none"> • If configured as the session identifier, the value of the <code>sip.instance</code> media feature tag in the “+sip.instance” parameter of the <code>Contact</code> header field is used as the session identifier in EATF.
P-Asserted-Identity	<ul style="list-style-type: none"> • If configured as the session identifier, the value of the <code>P-Asserted-Identity</code> header is used as the session identifier in EATF.

The top `Route` header is used for routing the emergency request from the E-CSCF to the EATF. The EATF is acting as a routing Back-to-Back User Agent (B2BUA). The second `Route` header is used by the EATF for routing a new emergency request back to the same E-CSCF.

3.1.2

Initial Emergency Request from EATF to E-CSCF

The initial emergency request from EATF to the E-CSCF is described in Figure 3.

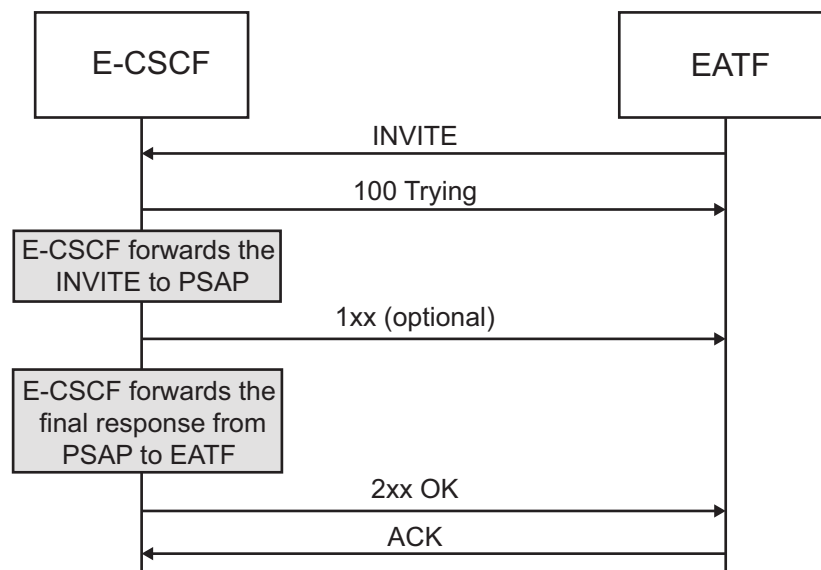


Figure 3 Initial Emergency Request from EATF to E-CSCF over I4 Interface

As a B2BUA, the EATF anchors the initial emergency request from the E-CSCF, then creates and sends a new emergency request back to the E-CSCF for setting up the connections to the PSAP. The EATF copies the headers of the initial emergency request from the E-CSCF to the new request with the changes described in Table 3:

Table 3 Headers of INVITE Request for Emergency Call Sent from EATF to E-CSCF

Header	Procedure-Specific Values of the Parameter
Route	The top <code>Route</code> header is deleted.
Call ID	A new Call ID is generated.
Cseq	A new Cseq is generated.
Record-Route	The value is set to the EATF address.
Via	The value is set to the EATF address.
Max-Forward	The value is set to the default maximum.
Contact	The value is set to the EATF address.
From-tag	The value is set to the EATF address.
UserAgent	The value is set to <code>EatfUacAgent</code> .

3.1.3 Emergency Request Update from EATF to E-CSCF

The `re-INVITE` sent from the EATF to the E-CSCF is described in Figure 4.

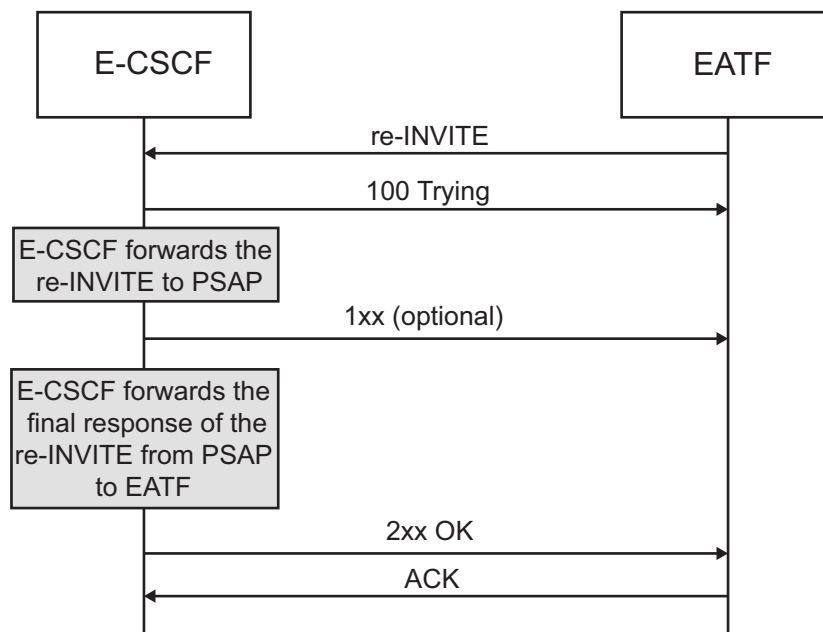


Figure 4 Re-INVITE Sent from EATF to E-CSCF over I4 Interface

Upon receipt of the access transfer request over the I5 Interface, or the PS Fallback request over the I4 Interface, or a session refresh request, the EATF creates and sends a `re-INVITE` to the E-CSCF over the I4 interface for updating the PSAP connection. The EATF copies all headers from the `INVITE` previously sent to the E-CSCF to the `re-INVITE` with the changes described in Table 4.

Table 4 Headers of Re-INVITE Request Owing to Emergency Call Access Transfer or PS Fallback

Header	Procedure-Specific Values of the Parameter
Session-Expires	The value is set to the value in the <code>INVITE</code> received.
Min-SE	The value is set to the value in the <code>INVITE</code> received.
ALLOW	The value is set to the value in the <code>INVITE</code> received.
P-Charging-Vector	The value includes the IMS Charging Identifier (ICID) from the Packet-switched (PS) network as the <code>icid-value</code> parameter and the ICID from the Circuit Switched (CS) network as the <code>related-icid</code> parameter.
SDP	The value is set to the value in the <code>INVITE</code> received.

3.2 Emergency Call Access Transfer over I5 Interface

3.2.1 Emergency Call Access Transfer from I-CSCF to EATF

The emergency call access transfer from the I-CSCF to the EATF is described in Figure 5.

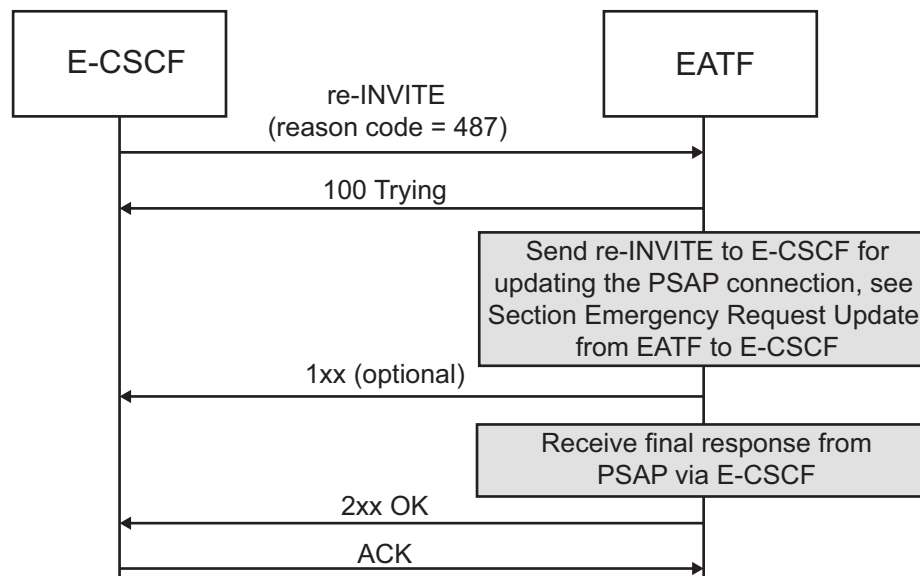


Figure 5 I5 Interface SIP Signaling from I-CSCF to EATF

During an access transfer, the I-CSCF sends the access transfer request to the EATF over the I5 interface. The EATF creates and sends a `re-INVITE` to the E-CSCF over the I4 interface for updating the PSAP connection. For details about the `re-INVITE`, see Section 3.1.3 Emergency Request Update from EATF to E-CSCF on page 7. Some related headers are listed in Table 5.

Table 5 Headers of `INVITE` Received for Access Transfer

Header	Procedure-Specific Values of the Parameter
Contact	<ul style="list-style-type: none"> If configured as the session identifier, the value of the <code>sip.instance</code> media feature tag in the “+sip.instance” parameter of the <code>Contact</code> header field is used as the session identifier in EATF.

Header	Procedure-Specific Values of the Parameter
P-Asserted-Identity	<ul style="list-style-type: none"> If configured as the session identifier, the value of the P-Asserted-Identity header is used as the session identifier in EATF.
P-Charging-Vector	<ul style="list-style-type: none"> The value includes the IMS Charging Identifier (ICID) from the Circuit Switched (CS) network which is used as the <code>related-icid</code> parameter for the <code>re-INVITE</code> sent towards the PSAP, see Section 3.1.3 Emergency Request Update from EATF to E-CSCF on page 7.

3.2.2

Emergency Call Access Transfer from I-CSCF to EATF with Redirection

The I5 interface SIP signaling from I-CSCF to EATF with redirection is described in Figure 6.

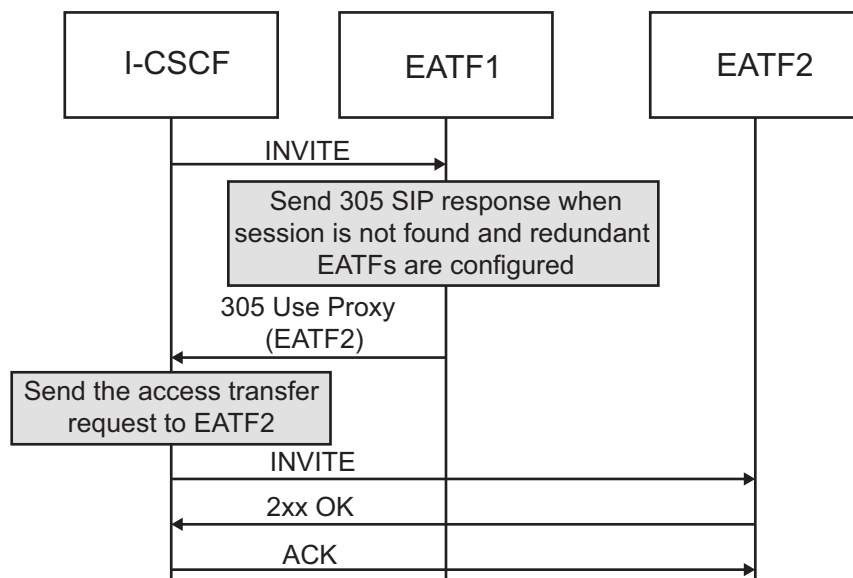


Figure 6 I5 Interface SIP Signaling from I-CSCF to EATF with Redirection

During an access transfer, the I-CSCF sends the access transfer request to EATF1 over the I5 Interface. EATF1 has not anchored the established session therefore the required session is not found. When redundant EATF is configured, EATF1 responds with a `305 Use Proxy` response including the redundant EATF addresses as redirect targets in the `Contact` header, see Table 6. In this case, EATF1 is configured with EATF2 as the redundant EATF. Multiple redirect targets are allowed in the `305` response. If redundant



EATF is not configured, the access transfer request is rejected with a 403 `Forbidden` response. The I-CSCF sends the request to the target that has the highest priority and is not previously tried. The I-CSCF sends the access transfer request to EATF2 over the I5 Interface. EATF2 has anchored the established session then proceeds to update the PSAP call leg as in Section 3.2.1 Emergency Call Access Transfer from I-CSCF to EATF on page 9.

Table 6 Contact Header within 305 Response Received for Access Transfer

Header	Procedure-Specific Values of the Parameter
Contact	<p>The redundant EATF addresses configured in the configuration parameter <code>eatfRedundantEatfEntry</code> are included in the <code>Contact</code> header of the 305 response sent by the EATF. The address is in the form of IPv4 address and port with a <code>q</code>-value or IPv6 address and port with a <code>q</code>-value.</p> <p>For more information about the <code>Contact</code> header or <code>q</code>-value, refer to RFC 3261 SIP: Session Initiation Protocol.</p>

3.3 Emergency Call PS Fallback over I4 Interface

3.3.1 Emergency Call PS Fallback from E-CSCF to EATF

The I4 interface SIP signaling from E-CSCF to EATF is described in Figure 7.

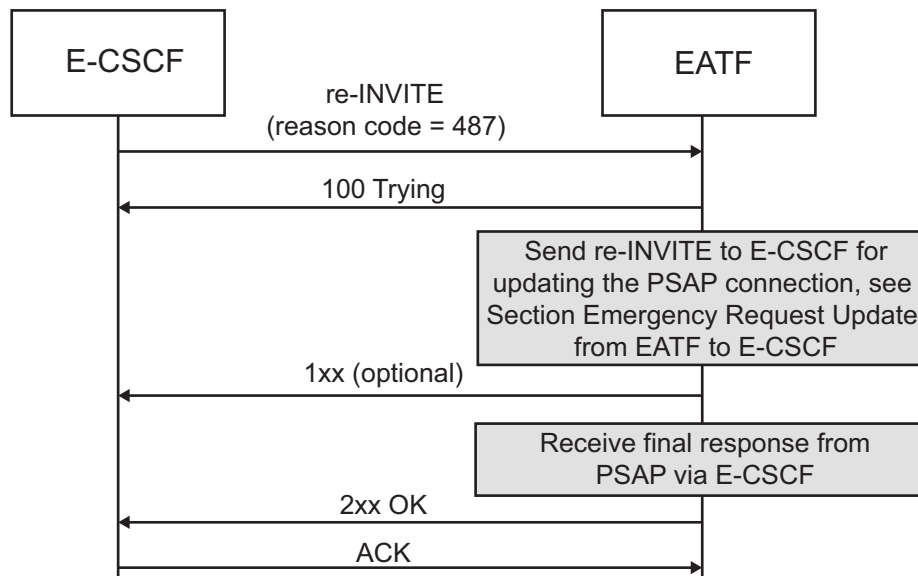


Figure 7 I4 Interface SIP Signaling from E-CSCF to EATF

During or after an access transfer, it is possible that the UE is moved back to the PS access network. The UE sends a PS Fallback request in form of a `re-INVITE` or an `UPDATE` including a `Reason` header field containing a reason parameter `cause` with value 487. The PS Fallback request is sent over the I4 interface towards the EATF.

The EATF creates and sends a `re-INVITE` or an `UPDATE` to the E-CSCF over the I4 interface for updating the PSAP connection. This `re-INVITE` or `UPDATE` does not include the `Reason` header field containing a reason parameter `cause` with value 487, see Table 7. For details about the `re-INVITE` sent to the PSAP, see Section 3.1.3 Emergency Request Update from EATF to E-CSCF on page 7.

Table 7 Reason Header of PS Fallback Request Sent from E-CSCF to EATF

Header	Procedure-Specific Values of the Parameter
Reason	<ul style="list-style-type: none"> The parameter <code>cause</code> with value 487 is used to identify the request as a PS Fallback request to an existing emergency session.

3.4 Request Within Established Emergency Session

The EATF routes all subsequent requests based on the established route set. For more information about route sets, refer to [RFC 3261 SIP: Session Initiation Protocol](#).



4 Information Model

This section describes supported SIP methods and gives information about the SIP header.

4.1 Supported SIP Methods

The SIP methods listed in Table 8 are supported methods and are considered within this document. For more information about the supported SIP methods, refer to [3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol \(SIP\) and Session Description Protocol \(SDP\)](#). For handling of other SIP methods, refer to [RFC 3261 SIP: Session Initiation Protocol](#).

Table 8 Supported SIP Methods

SIP Method	CSCF to EATF	EATF to CSCF	Reference
ACK Request	Supported	Supported	RFC 3261
BYE Request	Supported	Supported	RFC 3261
CANCEL Request	Supported	Supported	RFC 3261
INVITE Request	Supported	Supported	RFC 3261
OPTIONS Request	Supported	Supported	RFC 3261
PRACK Request	Supported	Supported	RFC 3262
UPDATE Request	Supported	Supported	RFC 3311

4.2 SIP Header Information

Not applicable.





5 Formal Syntax

Not applicable.





6 Security Considerations

Not applicable.





7 Related Standards

For information about the related standards, refer to:

- [3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol \(SIP\) and Session Description Protocol \(SDP\)](#)
- [3GPP TS 24.237 IP Multimedia \(IM\) Core Network \(CN\) subsystem IP Multimedia Subsystem \(IMS\) Service Continuity](#)
- [RFC 3261 SIP: Session Initiation Protocol](#)
- [RFC 3311 The Session Initiation Protocol \(SIP\) UPDATE Method](#)