Guidelines for emergency communication to emergency number 112 in Sweden using SIP

An Application Guide describing the procedures for routing of emergency communication from Electronic Communications Service Providers to the PSAPs

Reference
ITS ApG25

Keywords
Emergency number, Emergency Calls, Emergency communication, Municipality Codes, eCall

ITS
Kistagången 16
Box 1284, SE-164 29 KISTA, SWEDEN
Tel.: +46 (0)70 300 9542

Important notice
The present document can be downloaded from:
http://www.its.se

Reproduction during the drafting phase is only permitted for the purpose of standardization work undertaken within ITS. The copyright and the foregoing restriction extend to reproduction in all media.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ITS. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ITS deliverable is the one made publicly available in PDF format at www.its.se.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ITS documents is available at https://www.its.se

If you find errors in the present document, please send your comment to the contact email provided through http://www.its.se

Copyright Notification
No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

ITS, Swedish ICT Standardization, 2020.
All rights reserved.

Table of contents

Introduction

This Application Guide is released in edition 3 to describe the procedures to be used by Electronic Communications Service Providers (ECSPs) for emergency communications to the PSAPs[1] in Sweden to the emergency number 112 using IP based communications with support for additional media types and localization information. This Application Guide follows the general directions of emergency calling using Internet technologies, as described by IETF WG ECRIT, EENA/NG112, ETSI and 3GPP.

This Application Guide describes available procedures for routing of emergency communications in different use cases and information to be transferred in the emergency session and testing of the emergency communication service.

The SOS-NTP in this Application Guide is the IP/SIP enabled interface of the PSAP that will receive the IP based communication emergency sessions. The SOS-NTP supports the reception of emergency sessions using SIP (Session Initiation Protocol).

The document is concerned with technical issues and is assumed to be used by ECSPs in their agreements on interconnection directly to the PSAP or to other ECSPs when transferring emergency sessions. For more SIP/IP Interconnect details, please refer to [6].

ECSP networks can be interconnected to enable the subscribers in the different networks to call the PSAP. The ECSP can connect either directly to the SOS-NTP interface or via another ECSP network. (See Figure 1).

An ECSP with a direct connection and established IP/SIP interconnect agreement with the PSAP may additionally act as a transit ECSP for emergency sessions if so agreed with originating ECSP. In that case, originating ECSP does not have a direct agreement with the PSAP.

This Application Guide does not deal with the corresponding internal information in each ECSPs network that might be used. How IP packets are transported between the emergency caller, the ECSP and the PSAP are not specified in this document. Please refer to [6] for SIP and IP Interconnect specifications.

[1] SOS Alarm is acting as the PSAP according to an agreement with Swedish government

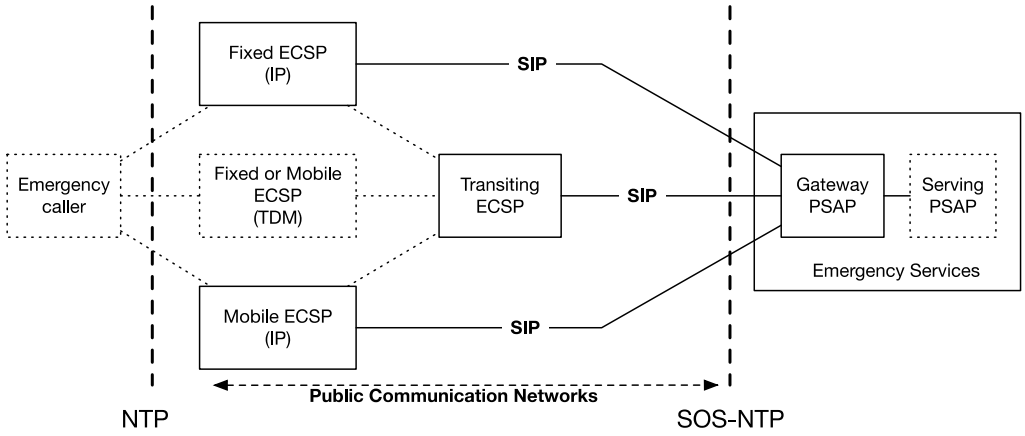

Figure 1: Connecting to the PSAP

In Figure 1, the IP/SIP based communication solution described in this Application Guide is shown.

Even though different types of traffic flows and call scenarios exist, they basically fit one generic case:

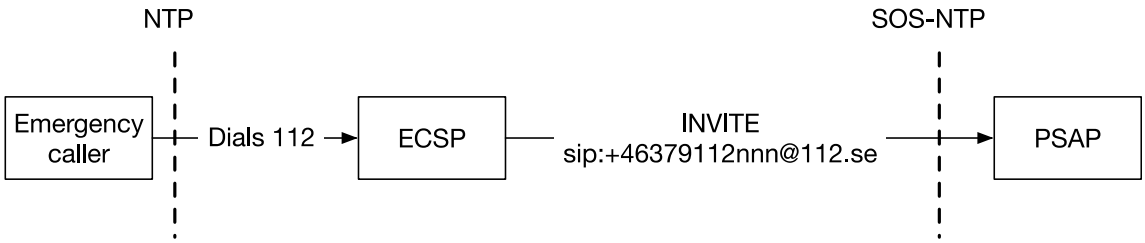

Figure 2: Generic emergency session flow

Generic emergency session flow:

1. An emergency caller dials 112 to initiate the emergency session.
2. An ECSP forwards the emergency session to a defined PSAP SIP URI (sip:+46379112nnn@112.se).
3. The SOS-NTP accepts the incoming SIP emergency sessions and forwards it to the PSAP.

nnn equals municipality identity codes (MIC) according to ITS ApG 21 [1].

112.se is the domain used for the emergency services in Sweden and may be used by ECSPs to resolve the destinations of the SOS-NTP.

Scope

It must be possible to set up emergency sessions from emergency callers using different ECSPs, connected via different IP based networks, to the PSAP. The purpose of this Application Guide is to give ECSPs guidelines in their setting up of the emergency communication service and describe the requirements for connection to the PSAP.

This Application Guide:

- Describes the different routing cases for emergency sessions;
- Describes information to be transferred in the emergency sessions;
- Is applicable for connections between an ECSP and PSAP using SIP.

ISUP-based connection regarding the SOS-NTP is described in ITS 24: Guidelines for calls to emergency numbers 112 and 90 000 in Sweden.

1. References

1.1. Normative references

The following normative documents contain provisions, which through reference in this text constitute provisions of this Application Guide. For dated references, sub-sequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this Application Guide are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to apply.

[1] ITS ApG 21 V5 July 2019	Routing of calls to emergency numbers 112 and 90000 using the Identification Plan of Municipalities
[2] IETF RFC 3261 June 2002	SIP: Session Initiation Protocol
[3] IETF RFC 3325 November 2002	Private Extensions to SIP for Asserted Identity within Trusted Networks
[4] IETF RFC 3966 December 2004	The tel URI for Telephone Numbers
[5] IETF RFC 3986 January 2005	Uniform Resource Identifiers (URI): Generic Syntax
[6] SOS Alarm IP/SIP Interconnect Specification	SOS Alarm IP/SIP Interconnect Specification (https://www.sosalarm.se/kontakt/underlag-och-blanketter/)
[7] IETF RFC 6442 December 2011	Location Conveyance for SIP
[8] IETF RFC 4119 December 2005	A Presence-based GEOPRIV Location Object Format
[9] 3GPP TS23.167 December 2019	IMS Emergency Sessions
[10] IETF RFC 2392 August 1998	Content-ID and Message-ID URL
[11] IETF RFC 4103 June 2005	RTP Payload type for Text Conversations

1.2. Informative references

LEK 2003:389	Lagen om elektronisk kommunikation (LEK)
PTSFS 2008:2/PTSFS 2011:4/PTSFS 2017:2	Post- och telestyrelsens föreskrifter om förmedling av nödsamtal och tillhandahållande av lokaliseringsuppgifter till samhällets alarmeringstjänst
ITS 24 ed 1 2007-03-07	Guidelines for calls to emergency numbers 112 and 90 000 in Sweden
IETF RFC 3550 July 2003	A Transport Protocol for Real-Time Applications
IETF RFC 5012 January 2008	Requirements for Emergency Context Resolution with Internet Technologies
IETF RFC 5031 January 2008	A Uniform Resource Name (URN) for Emergency and other Well-known services
IETF RFC 5222 August 2008	LoST: A Location-to-Service Translation Protocol
ETSI ES 203 178 February 2015	Functional Architecture to support European requirements on emergency call location determination and transport v1.1.1
IETF RFC 6881 March 2013	Best Current Practice for Communications Services in Support of Emergency Calling
EENA NG112 June 2013	Next Generation 112 : Long Term Definition v1.1
SS 636394 2004, Utgåva 1	Positioning of Mobile Terminals at Emergency Calls
ETSI TS 103 479 December 2019	Emergency Communications (EMTEL); Core elements for network independent access to emergency services v1.1.1

2. Terms and definitions

2.1. Emergency caller

The term "caller" or "emergency caller" refers to the person or device placing an emergency session.

2.2. Emergency call taker

The term "emergency call taker" or "call taker" refers to a person at any PSAP that accepts the emergency session.

2.3. Internet Protocol (IP)

In this Application Guide IP refers to both IPv4 and Ipv6.

2.4. Municipality Identity Code

A code from the Identification Plan of Municipalities (Kommun-ID-planen) for sessions to emergency numbers 112.

2.5. Public Safety Answering Point (PSAP)

The PSAP is a call center responsible for answering incoming calls to an emergency service. The Voice Service Provider connects to the PSAP via the SOS-NTP using SIP [2, 6].

2.6. SOS-Network Termination Point (SOS-NTP)

The SOS-NTP is the interface between the public communications network and the PSAP.

2.7. Electronic Communications Service Provider

An undertaking providing publicly available electronic communications services.

2.8. Transiting ECSP

To the PSAP directly connected ECSPs transferring emergency sessions from other, not directly connected ECSPs, to the PSAP.

3. Symbols and abbreviations

3GPP	3rd Generation Partnership Project
CLIR	Calling Line Identity Restriction
DNS	Domain Name System
ECRIT	Emergency Context Resolution with Internet Technologies
ECSP	Electronic Communications Service Provider
EENA	European Emergency Number Association
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force
IP	Internet Protocol (IPv4/IPv6)
ISUP	ISDN User Part
LEK	Lagen om elektronisk kommunikation (Electronic Communication Act)
MLP	Mobile Location Protocol
NTP	Network Termination Point
OIR	Originating Identification Restriction
PIDF-LO	Presence Information Data Format – Location Object
PSAP	Public Safety Answering Point
SIP	Session Initiating Protocol
RTT	Real-time Text
TDM	Time-division Multiplexing
URI	Uniform Resource Identifier

4. General description of information

The operation of efficient emergency services requires that necessary information concerning the emergency caller is made available to the PSAP. The mandatory information components are[2]:

- Calling Party Identity
- Caller Location information
- eCall discriminator

Additional optional information component transferred in the setup of the emergency sessions is:

- Terminal- and / or network provided location information (SIP Geolocation)

Furthermore, a number of optional information components can be made available to the emergency service in the incoming sessions or by subsequent requests from the emergency service.

- Routing information
- Address information of the subscriber (emergency caller).

4.1. Calling Party Identity

The Calling Party Identity is used by the PSAP for two purposes.

1. Make it possible for the emergency call taker to call back.
2. Can be used as one of several methods for finding the address and location information of the emergency caller.

4.2. Caller Location Information

Location information of the caller is used for two purposes.

1. Facilitate routing of an emergency call to the appropriate PSAP / emergency call taker (e.g. using the municipality identity code)
2. To enable geographical location information of the emergency caller, enabling dispatching of rescue resources to the right place (municipality identity code and supplementary information derived from e.g. calling party identity).

4.3. Routing information

Routing information conveyed from the municipality identity code is used for multiple purposes.

1. Enable routing to the appropriate PSAP / emergency call taker.
2. Convey information on the access type the emergency session was made from to the emergency call taker.
3. Convey information on the area the emergency session was made from to the emergency call taker

[2] As specified in LEK (2003:389), and PTSFS 2008:2/2011:4/2017:2.

The routing information is assigned to the emergency call by the emergency caller or the originating ECSP. In the case the assignment of municipality identity codes is done by the ECSP, the municipality identity code shall represent the NTP according to [1].

Note: In the case it is assigned by the emergency caller, e.g. a corporate network, the ECSP cannot guarantee routing to the appropriate PSAP / emergency call taker.

4.4. Description of the procedure

1. The routing information can be assigned by either of the following:
   a. The emergency caller
   b. The ECSP
2. The PSAP uses the routing information to route the emergency session to appropriate emergency call taker.
3. The emergency call taker at the PSAP use the routing information

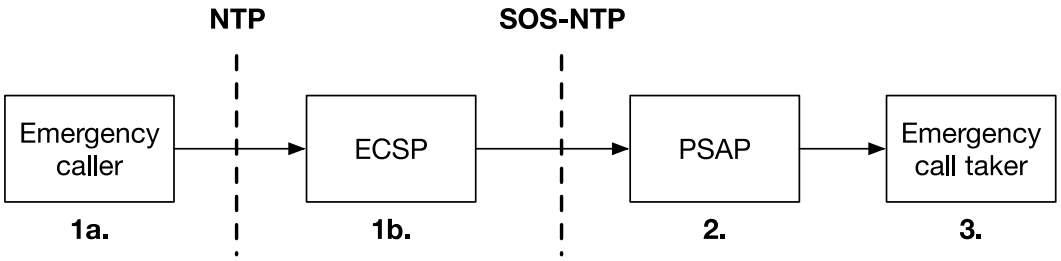

Figure 3: Routing using Municipality Identity Codes

Note: A transiting ECSP will only transfer the routing information required by the SOS-NTP.

4.5. Address and location information

Location information is used by the emergency call taker to locate the emergency caller. It can be a geographical address, e.g. street name and number or a position expressed in geographic coordinates. The location information can be retrieved using two methods.

1. The Calling Party Identity is used as an identifier in a request to a database or location server where the mapping of Calling Party Identity into geographic address or position is made available.
2. The address information is received in or derived from the incoming emergency session

The location information can be of four types

a. NTP of a fixed terminal (e.g. geographic address of the emergency caller)
b. NTP of a mobile terminal (e.g. location of base station as described in SS 636394)
c. Address related to subscriptions (e.g. home or billing address of subscriber or geographical coordinates)
d. Terminal- or network provided location information (e.g. GPS in mobile phone, PIDF-LO)

Note: The types of location information are not listed in priority order here.

If optional location information is included in the call setup of the emergency session, e.g. terminal- or network

provided location information including using SIP Geolocation, this additional location information may be presented to the emergency call taker as well.

Note: In the case of mobile telephones multiple addresses (usually billing address) and location information may be available. These need not give the same information.

5. Protocols for connecting to the PSAP

A ECSP connects directly, or via a transiting ECSP, to the PSAP at the session layer. The signalling protocol used at the session layer is SIP. Different IP networks may be used to connect the ECSP to the PSAP at the IP layer.

Please refer to [6] for SIP and IP Interconnect specifications.

5.1. Transfer of information using SIP

To make it possible for the PSAP to get the necessary information described in chapter 4, the following information has to be transferred in the initial SIP INVITE request of the emergency session.

Element	Transferred in
Calling Party Identity (Identification of the emergency caller in tel URI or SIP URI format)	SIP headers, as defined in 5.2
Called Party Identity (Identification of PSAP and routing information in SIP URI format)	Request URI, as defined in 5.3

Table 1: Mandatory information elements using SIP

Optionally, terminal- or network provided location information present in the SIP Geolocation header and associated PIDF-LO may be transferred to the PSAP as additional location information.

Element	Transferred in
SIP Geolocation (Terminal- and / or network provided location)	Geolocation header and PIDF-LO body content, as defined in 5.6

Table 2: Optional information elements using SIP

5.2. Format of Calling Party Identity

The originating ECSP can use either of the following formats:

Telephone Uniform Resource Identifier, tel URI

- The format of the tel URI is defined in [2] and [4].
- Generic example: tel:+[International E.164 number]3
- Illustrative example: tel:+468678XXXX

SIP Uniform Resource Identifier, SIP URI

- The format of the SIP URI is defined in [2].
- Generic example: sip:+[International E.164 number]@[ECSP-domain]
- Illustrative example: sip:+468678XXXX@[ECSP-domain]

The following SIP headers are used, in preferred order, to identify the calling party identity.

- P-Asserted-Identity header as defined in [3]
- From header as defined in [2]

The originating ECSP should either:

- insert a **P-Asserted-Identity** header providing a tel URI or a SIP URI with a numerical user part containing Calling-Party-Identity as an international E.164 number prefixed by '+'

or

- construct the **From** header to include a SIP URI with a numeric user part that can be used for dial-back purpose. This means that the user part of the SIP URI shall be an international E.164 number prefixed by '+'.

The ECSP shall assure the Calling Party Identity.

If the calling party has requested privacy/restricted presentation (CLIR/OIR) the originating ECSP must include the original Calling party identity in the P-Asserted-Identity header and make sure that the From header is properly anonymized, as well as making sure the Privacy header is set accordingly.

[3] See RFC 3966 section 5.1.4 Global numbers.

5.3. Format of Called Party Information

The Called Party Identity shall contain the following main pieces of information.

1. The Called Party Identity
2. eCall discriminator (only applicable for eCall emergency calls)
3. Identification of originating area

The originating ECSP shall use the following format:

SIP Uniform Resource Identifier, SIP URI

- The format of the SIP URI is defined in [2] and [5].
- Generic example: sip: +46379112[municipality-identity-code]@112.se
- Illustrative example: sip:+46379112274@112.se (call originating from a fixed line in Mellerud)
- Illustrative example: sip:+46379112674@112.se (call originating from a mobile terminal in Mellerud)
- Illustrative example: sip:+4637911200674@112.se (automatic eCall in Mellerud)

Note: If the SIP URI in the Request URI does not contain the municipality code as shown in the example above, the emergency session might be routed to an emergency call taker without local knowledge (e.g. an emergency call from Mellerud without correct municipality identity code might be answered by an emergency call taker anywhere in Sweden).

112.se is the domain for the emergency service in Sweden.

5.4. Identification of originating area

The originating ECSP shall assign a municipality identity code according to [1]. The code shall be transferred in the initial SIP INVITE request as part of the Request URI.

Additionally, the terminal- or network provided location information may be provided as part of the emergency session setup. This is achieved by including the location information object (PIDF-LO) in the body of the initial SIP INVITE message as well as populating the SIP Geolocation header according to [7, 8, 9].

Note: In this revision, terminal- or network provided location information included in the SIP signalling using SIP Geolocation is only to be seen as additional location information provided to the PSAP.

5.5. Identification of originating mobile electronic communications service provider (ECSP)

Since mobile ECSPs implementing this Application guide may transit emergency sesssions via other ECSPs, transparent information about the originating mobile ECSP transferred in the SIP signalling only, cannot be guaranteed. This is also applicable for SIP to ISUP transit of emergency calls. In this case, the geographical reference (ISUP Location Number as described in ITS 24 chapter 5.2) is therefore not a mandatory information element.

Thus, if the emergency session originated from a mobile ECSP, the MLP PUSH mechanism should be implemented to provide appropriate location information to the PSAP (e.g. information about base station).

Mobile originating ECSPs must still support MLP PULL request from the PSAP for emergency sessions where the originating ECSP cannot be determined otherwise.

How this MLP mechanism is implemented is out-of-scope for this Application guide, but the same mechanisms already in place for TDM based emergency calls (ITS 24) must be used.

5.6. Format of Location information conveyance in SIP (SIP Geolocation)

The SIP Geolocation information consist of two different parts. Both must be correctly set by the ECSP if the location information is to be accepted by the PSAP. These parameters must be set in the initial SIP INVITE of the emergency session:

1. The SIP Geolocation header must be present and reference a location object in the message body (location by-value) [7, 10]
2. The SIP message body must contain a location object (PIDF-LO) [8]

6. Protocol standards

For technical SIP and IP interconnect details, please refer to [6].

7. Routing of the emergency session

The routing of emergency session to the SOS-NTP will not be based on municipality identity codes. Call routing policy (e.g. DNS or any other call routing policy provisioned locally by the ECSP), will be used to route the emergency session to the SOS-NTP. The municipality identity code has to be transferred to the SOS-NTP to enable the PSAP to deliver the emergency session to the correct emergency call taker. The municipality identity code has to be included by the originating ECSP or emergency caller, as described in 4.3. The municipality identity code will be displayed to the emergency call taker. For further technical details, please refer to [6].

8. Supported media types

The PSAP accept SIP emergency sessions using the following media types:

1. Voice, audio
2. Real-time text, as defined in [11]

Additional media types may be supported in later revisions.

9. Security considerations

The SOS-NTP interface is deployed as a SIP and IP interface it is very important to enable and provide appropriate integrity and security functions. Every emergency session includes sensitive personal information, including calling party identity as well as location information, and that information must be protected from potential eavesdropping and manipulation. For further technical details, please refer to [6].

10. Testing and verification

The SOS-NTP will provide a SIP URI for testing purposes. This URI can be used to test functionality and reachability of the SOS-NTP.

The SIP URI:s that shall be used to test the PSAP functionality are:

- sip:+46379112493@112.se

11. Document history

Document history		
Edition 1	2009-05-15	First published version
Edition 2	2018-10-12	Latest available published version. Updated revision for calls to the PSAPs in Sweden using Voice over IP
Edition 3	2020-06-23	Updated revision adding support for additional media types and SIP Geolocation information.