ApG 25 V3
(2019-11)

Application Guide

Handläggande organ/Standardizing body

SVENSKA INFORMATIONS- OCH
TELEKOMMUNIKATIONSSTANDADISERINGEN

Fastställd/Approved	Utgåva/Edition	Sida/Page
2019-11-07	3	**1(12)**

Guidelines for calls to emergency number 112 in Sweden using SIP

An Application Guide describing the procedures for routing of emergency calls from Voice Service Providers to the PSAPs

Reference

ITS ApG25

Keywords

Emergency Number, Emergency Calls, Municipality Codes, eCall

ITS

Kistagången 16
Box 1284, SE-164 29 KISTA, SWEDEN

Tel.: + Tel.: +46 (0)70 300 9542

Contents

Introduction

This Application Guide is released in edition 2 to describe the procedures to be used by Voice Service Providers for calls to the PSAPs[1] in Sweden to the emergency number 112 using Voice over IP. 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 calls in different call cases and information to be transferred in the emergency call and testing of the emergency call service.

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

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

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

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

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

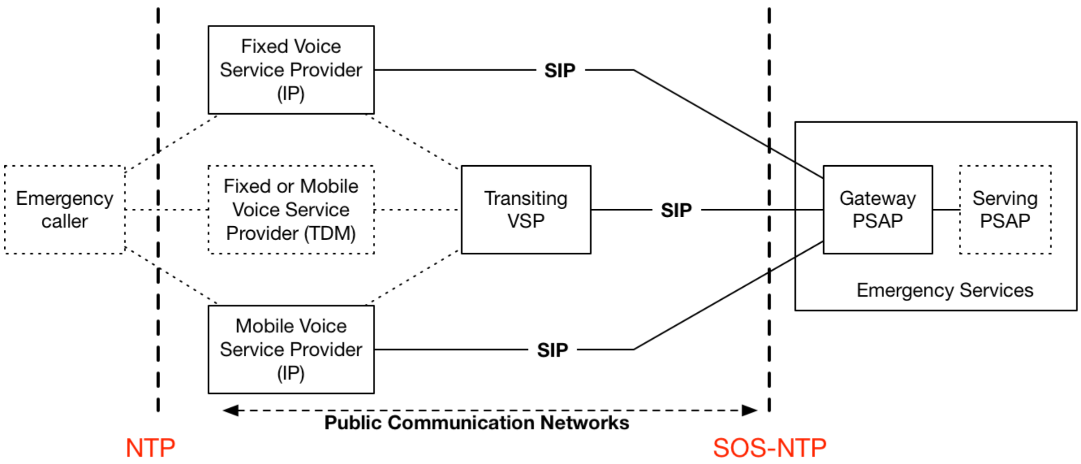

Figure 1: Connecting to the PSAP

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:

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

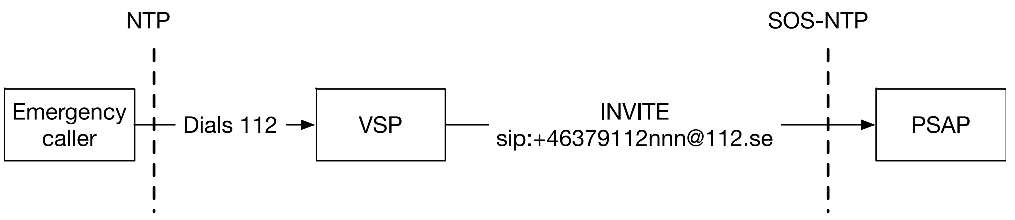

Figure 2: Generic emergency call flow

1. An emergency caller dials 112.
2. A Voice Service Provider forwards the emergency call to a defined PSAP SIP URI (sip:+46379112nnn@112.se).
3. The SOS-NTP accepts the incoming SIP call and forwards it to the PSAP.

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

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

Scope

It must be possible to set up voice calls from emergency callers using different Voice Service Providers, connected via different IP networks, to the PSAP. The purpose of this Application Guide is to give Voice Service Providers guidelines in their setting up of the emergency call service and describe the requirements for connection to the PSAP.

This Application Guide:

– Describes the different routing cases for emergency calls;

– Describes information to be transferred in the emergency call;

– Is applicable for connections between a Voice Service Provider and PSAP using SIP.

TDM-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 v4.1.2 2016-09-15	Routing of calls to emergency numbers 112 and 90 000 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] SIP/IP Interconnect Specification - version 1.0 2018-05-23	SOS Alarm SIP/IP Interconnect Specification (https://www.sosalarm.se/contentassets/19366c5d09194a1d9e10de8c1b312f70/sipinterconnect-specification-v1.0.pdf)

1.2 Informative references

LEK 2003:389	Lagen om elektronisk kommunikation
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 https://tools.ietf.org/html/rfc5012
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
IETF RFC 6442 December 2011	Location Conveyance for the Session Initiation Protocol
ETSI ES203176 February 2015	Functional Architecture to support European requirements on emergency call location determination and transport v1.1.1
3GPP TS 23.167 March 2016	IMS Emergency Session (Release 13)
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

2 Terms and definitions

2.1 Emergency caller

The term “caller” or “emergency caller” refers to the person or device placing an emergency call.

2.2 Emergency call taker

The term “emergency call taker” or “call taker” refers to a person at any PSAP that accepts the call and may dispatch emergency help.

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 calls 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 Voice Service Provider (VSP)

An undertaking providing publicly available fixed and / or mobile voice services. In this document the term VSP include network operators, e.g. the visited mobile network in the case of inbound roaming subscriber.

2.8 Transiting VSP

To the PSAP directly connected VSPs transferring calls from other, not directly connected VSPs, 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
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
PSAP	Public Safety Answering Point
SIP	Session Initiating Protocol
TDM	Time-division Multiplexing
URI	Uniform Resource Identifier
VSP	Voice Service Provider

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
- eCall discriminator

Furthermore, a number of optional information components can be made available to the emergency service in the incoming call 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 of the emergency caller.

4.2 Caller Location

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

2. To enable geographical location 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 call was made from to the emergency call taker.
3. Convey information on the area the emergency call was made from to the emergency call taker

The routing information is assigned to the emergency call by the emergency caller or the originating VSP. In the case the assignment of municipality identity codes is done by the VSP, 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 VSP 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 VSP
2. The PSAP uses the routing information to route the call to appropriate emergency call taker.
3. The emergency call taker at the PSAP use the routing information

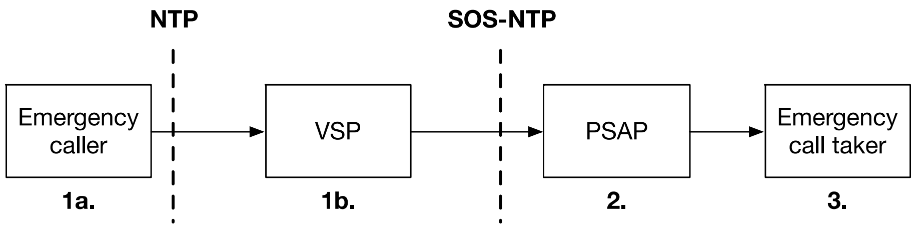

Figure 3: Routing using Municipality Identity Codes

Note: A transiting VSP 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 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 call

The location information can be of three types

a. NTP of a fixed telephone line (e.g. geographic address of the emergency caller)

b. NTP of a mobile telephone (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)

Note that in the case of mobile telephones both address (usually billing address) and location can be available. These need not give the same information.

5 Protocols for connecting to the PSAP

A VSP connects directly, or via a transiting VSP, 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 VSP 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.

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: Information elements using SIP

5.2 Format of Calling Party Identity

The originating VSP can use either of the following formats:

<u>Telephone Uniform Resource Identifier, tel URI</u>

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

<u>SIP Uniform Resource Identifier, SIP URI</u>

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

[3] See RFC 3966 section 5.1.4 Global numbers

The originating VSP 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 VSP shall assure the Calling Party Identity.

If the calling party has requested privacy/restricted presentation (CLIR/OIR) the originating VSP 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.

5.3 Format of Called Party Information

The Called Party Identity shall contain two 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 VSP shall use the following format:

<u>SIP Uniform Resource Identifier, SIP URI</u>

– 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:+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 call 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 VSP 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.

5.5 Identification of originating mobile voice service provider (VSP)

Since mobile VSPs implementing this Application guide may transit emergency calls via other VSPs, transparent information about the originating mobile VSP 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 call originated from a mobile VSP, the MLP PUSH mechanism should be implemented to provide appropriate location information to the PSAP (e.g. information about base station).

Mobile originating VSPs must still support MLP PULL request from the PSAP for emergency calls where the originating VSP 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.

6 Protocol standards

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

7 Routing of the emergency call

The routing of emergency call to the SOS-NTP will not be based on municipality identity codes. The DNS, or any call routing policy provisioned locally by the VSP, will be used to route the emergency call to the SOS-NTP. The municipality identity code has to be transferred to the SOS-NTP to enable the PSAP to deliver the emergency call to the correct emergency call taker. The municipality identity code has to be included by the originating VSP 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 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 call 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].

9 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