Prepared
Hans Ahlsmo, Stefan Tjernell

Document responsible/Approved
Filippa Trossmark

Date
2018-10-23

Rev
8.0

No.
8211-A 353

SIP-I signalling interface for Sweden

0 DOCUMENT HISTORY

Revision	Date	Amendments
1.0	2013-12-16	New document
2.0	2014-03-24	New version after review/Hans Ahlsmo
3.0	2014-06-13	Small changes and One IP address used for signalling/Hans Ahlsmo
4.0	2015-03-05	SIP Options changed, 64kbps Unrestricted service added, Interpretation of SIP-I messages clarified. /Hans Ahlsmo
5.0	2016-05-10	Old req. 21 removed, req. 02 updated and req. 16 updated, Old chapter 4.3 and 4.4 are removed. New req. 22 added. /Hans Ahlsmo&Stefan Tjernell
6.0	2016-12-05	Introduction of Precondition feature in SIP/Hans Ahlsmo&Stefan Tjernell
7.0	2017-03-16	Remove support for Precondition feature due to Interoperability problems. Telia logo changed to Telia Operator Business./Hans Ahlsmo&Stefan Tjernell
8.0	2018-08-07	Logotype changed, SIP Options and SIP response code changed. No forking added and Preconditions added. ISUP supplementary services updated. / Hans Ahlsmo&Stefan Tjernell

1 SCOPE

This specification is to be used between a national fixed or mobile operator in Sweden using SIP-I/IP interconnect towards Telia fixed network (PSTN). The Softswitch in the Transit network act as CCF, MGCF and MGF. The transit network will terminate traffic both towards VoIP platforms and towards PSTN. Both originating/terminating and transit call scenarios are supported based on ref. [7, 8 and 9]. The signalling and media information is transported using IP network.

The requirements are defined using following principles/meaning:

- (M) Mandatory requirement
- (R) Nice to have requirement
- (O) Optional requirement

2 REFERENCES

Documents referred to in this specification are listed below:

[1] ITU-T Q.1912.5	Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part
[2] Telia specification, 8211-A324 rev. B	Interconnect Information
[3] Telia specification, 8211-A340 rev. A	Specification of Route Identity information (RIN) parameter
[4] ITS standard SS	Number Portability in Sweden – Network solutions for Service Provider

636390 ed 1	Portability for fixed public telecommunications services
[5] ITU-T Q.761-767, 769, 850	Signalling system No. 7 – ISDN user part
[6] Mandatory and recommended IETF RFCs	RFC 2474: (M) Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (updated by 3168 and 3260) RFC 2475: (M) An Architecture for Differentiated Services (updated by 3260) RFC 2597: (M) Assured Forwarding PHB Group RFC 2976: (M) The SIP INFO Method RFC 3204: (M) MIME media types for ISUP and QSIG objects RFC 3261: (M) SIP: Session Initiation Protocol RFC 3262: (M) Reliability of Provisional Responses in the Session Initiation Protocol (SIP) RFC 3264: (M) An Offer/Answer Model with Session Description Protocol (SDP) RFC 3311: (M) SIP Update RFC 3312: (O) Integration of Resource Management and Session Initiation Protocol (SIP) RFC 3323: (M) A Privacy Mechanism for the Session Initiation Protocol (SIP) RFC 3325: (M) Private extensions for SIP within trusted network RFC 3326: (M) The Reason Header Field for the Session Initiation Protocol (SIP). RFC 3398: (M) Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping RFC 4028: (R) Session Timers in the Session Initiation Protocol (SIP) RFC 4566: (M) SDP: Session Description Protocol (obsolete 2327)
[7]	8211-A355 IP interconnect interface for SIP/SIP-I
[8]	8211-A354 Media interconnect interface for SIP/SIP-I
[9]	8211-A356 Address formats for Swedish national SIP/SIP-I interconnection

3 DEFINITIONS/ACRONYMS

ACM	Address Complete Message
AF31	DSCP class Assured Forwarding 31
ALG	Application Layer Gateway
B2BUA	Back-to-Back User Agent
CCF	Call Control Function
CLIP	Calling Line Identity Presentation
CLIR	Calling Line Identity Restriction
DOS	Denial of Service
DSCP	Differentiated Services Control Points
FW	FireWall
ISUP	ISDN User Part
IWU	Inter Working Unit
MGCF	Media Gateway Control Function

MGF	Media Gateway Function
MIME	Multipurpose Internet Mail Extensions
RLC	Release Complete Message
RTP	Real Time Protocol
SBC	Session Border Controller
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP-I	Session Initiation Protocol with encapsulated ISUP
STP	Signal Transfer Point
TCP	Transport Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

4 SIP-I SIGNALLING SPECIFICATION (M)

The ISUP signalling part is encapsulated in the SDP part of the SIP message.

The SIP-I signalling protocol shall be based on ITU-T Q.1912.5 Profile C [1].	REQ 01
The ISUP related information in the SIP-I messages shall be used and not information in SIP headers.	REQ 02

The ISUP version is based on:

National ISUP based on ITU-T Q.761-764 shall be used.	REQ 03
The Content Type header field associated with the ISUP MIME body shall be supplied as follows: Content Type: application/ISUP; version = itu t92+; NOTE – itu t92+ means ISUP '92 plus every later ISUP Version.	REQ 04
ISUP Timers: In Profile C (SIP-I), the following ISUP timers defined in ITU-T Rec. Q.764 shall not be supported by ISUP procedures on the SIP side of the IWU: a) T1 (release RLC message) b) T4 (user part test message) c) T5 (release RLC message) d) T10 (reception of ACM message) e) T12 through T32 (circuit block/unblocking) f) T36 and T37 (continuity check failure	REQ 05
The ISUP messages listed in Table 1 in clause 5.4.3 in ref. [1] are either not encapsulated within any SIP message, or receive a special treatment with regard to ISUP encapsulation.	REQ 06
CLIP/CLIR treated according to Annex B.1 in ref. [1].	REQ 07
Call Hold treated according to Annex B.10 Table B.1-2 in ref. [1].	REQ 08

The SIP protocol shall comply with specifications in ref. [6].	REQ 09
Number format in SIP headers used in SIP-I shall comply with ref. [9] and this is required to facilitate fault tracing of SIP-I calls.	REQ 10

4.1 Signalling capabilities (M)

The following basic capabilities shall apply:

Basic signalling capabilities: a) Early media negotiations b) Offer/answer model c) Reliable provisional responses d) Multiple Early Dialogues (not supported) e) Forking (not supported)	REQ 11

The following supplementary services are supported:

Supplementary Services a) Calling Line Identity Presentation (CLIP) b) Calling Line Identity Restriction (CLIR) c) DDI (Direct Dialling In) d) Call Hold (HOLD) e) Call Forwarding (CFNR, CFB, CFU) f) CD (Call Deflection) g) CW (Call Waiting) h) CONF (Conference Calling) i) 3PTY (Three-Party call) j) 64kbps Unrestricted Service	REQ 12

Only SIP-URI shall be used and this format of the SIP-I URI scheme shall apply: a) SIP URI used with parameter user=phone	REQ 13

The authority control shall follow:

The relation will be trusted and hence no SIP-I Challenge Response shall be used.	REQ 14

4.2 SIP methods (M)

The following SIP methods shall apply:

a) INVITE b) ACK c) OPTIONS d) CANCEL e) BYE f) INFO g) PRACK h) UPDATE	REQ 15

The following special treatment of SIP messages shall apply:

a) An initial INVITE message without SDP part shall be rejected. b) An INVITE message shall include that 100Rel is supported. c) A 183 response message with included SDP part shall be accepted. d) When we receive the 183/200 OK response with SDP part we interpret this as media session is established.	REQ 16
To secure the functionality of reliable transport of SIP-I information and messages, we must include PRACK (Reliability of Provisional Responses - equals 100Rel header) according to RFC3262 in the SIP dialogue. PRACK could be included as two different options and we suggest the following use: a) 100Rel shall be included in the SIP Invite message as "supported" (supported header) b) 100Rel could be included in the SIP Invite message as "required" (optional). (PRACK will use more capacity related to SIP-I signalling.)	REQ 17

4.3 SIP response codes (M)

The response codes shall be based on RFC 3261 with the following additions/changes:

Reliable provisional responses RFC3262 (Reliability of Provisional Responses - PRACK) shall be applied.	REQ 18
Basic mapping of ISUP and SIP response code values are according to ref [6] ITU-T Q.1912.5.	REQ 19
The SIP response codes with 3XX are not supported.	REQ 20
Telia will only interpret a 503-response code as service unavailable. Telia will then select an alternative route (if available) to reroute the establishment of the SIP session.	REQ 21

If a SBC is used the SBC shall act as a B2BUA (similar to a stateful proxy) and only return the appropriate response codes.

4.4 Preconditions (O)

The signalling capability Preconditions can be used in case of delayed bearer setup where first part of the media is lost.

The supported condition for the Precondition capability is: Supported:Preconditions a=curr:qos local none a=curr:qos remote none a=des:qos mandatory local sendrecv a=des:qos optional remote sendrecv	REQ 22
The configuration is used on the I/C route in each network.	REQ 23
The Required:Preconditions is not supported.	REQ 24

The use of the Precondition function can be enabled after agreement with Telia.

4.5 SIP session timers (O)

The SIP session timer values shall be based on ref. [6].
The SIP session refresh function is recommended to be used. On the Telia side this function is activated and will be setup according to:

a) The session-Expire header shall have value 1800 seconds (The Session-Expires header field establishes the upper bound for the session refresh interval; i.e., the time period after processing a request for which any session-stateful proxy must retain its state for this session.) b) The Min-SE header shall have the value 90 seconds (The Min-SE header field establishes the lower bound for the session refresh interval; i.e., the fastest rate any proxy servicing this request will be allowed to require.)	REQ 25

4.6 SIP Options (M)

SIP Options message shall be used as a PING function to detect the status of the remote SIP entity. If Telia SBC detects a destination fault a SIP Options message will be sent to detect when the destination (SBC or first SIP proxy) is working again. The SIP Options shall be used according to the following setup:

The OPTIONS message shall be addressed to a peer SIP entity using a SIP URI of the form “sip:hostport” (see Section 25.1 of RFC 3261 for definitions). For example, “sip:192.168.1.5” is preferred, whereas “sip:bob@example.com” is not preferred since it might resolve to a plurality of addresses. The request URI required when addressing a proxy is described in Section 11 of RFC 3261.	REQ 26
The OPTIONS message shall be transmitted directly to the SIP peer’s IP address and not to an intermediary SIP entity.	REQ 27
Further, SIP peer entities shall set the Max-Forwards header field value to 0.	REQ 28
A SIP entity may transmit an OPTIONS message to a peer SIP entity, even when there are other on-going message exchanges. The reason is that, though a receiving SIP entity may be responsive to other SIP messages, it may have been put into a maintenance state, meaning it should not facilitate the establishment of new SIP sessions. Use of OPTIONS messages as per this specification can help facilitate the graceful shutdown of equipment.	REQ 29
A SIP peer entity shall respond to an OPTIONS method with a 200 OK response code when it is willing and able to process SIP messages, unless one of the following response codes is more appropriate. When a receiving SIP peer entity is unable to process additional SIP messages, it shall respond with a 503 response code. A 503 response code is also used when a SIP peer entity is placed into a maintenance mode to indicate that it shall not accept new SIP dialogs. A receiving SIP peer entity may include a Retry-After header in a response to the OPTIONS message to avoid further requests for a desired period of time. Note that a SIP peer entity may respond with other 5xx or 4xx error codes as appropriate and as recommended in RFC 3261.	REQ 30

If a requesting entity fails to receive a response to an OPTIONS message, it may retransmit that message following the procedures defined in RFC 3261. If a requesting SIP peer entity receives a 483 or 503 response code, it can send a subsequent OPTIONS messages in order to detect a change in operational status, but it should, as per RFC 3261, honour the Retry-After header field received in the previous response.	REQ 31
The SIP OPTIONS message shall be sent with a recommended interval of 30-60 seconds.	REQ 32

4.7 IP transport (M)

The IP transport is preferred to be based on TCP and QoS marking of the IP packets:

Port number recommended to be used for SIP-I shall be TCP port 5060.	REQ 33
Transport protocol preferred to be used for SIP-I signalling shall be TCP (RFC 793).	REQ 34
As an option UDP/TCP port 5060 could be used as transport protocol for SIP-I.	REQ 35
Diffserv class for SIP-I packets shall be AF31 (see ref. [6]).	REQ 36
DSCP value shall be 26 and IPP value shall be 3.	REQ 37
One dedicated IP-address (other than used for RTP) is used on the Telia side for SIP-I signalling.	REQ 38

4.8 Security (R)

In the existing ISUP solution there is a screening mask implemented at the STPs preventing unauthorised messages or parameters to enter the Call Servers/Switches. The problem when changing to SIP-I/IP is that the SBC most likely cannot enforce security with respect to ISUP since it has no knowledge about ISUP semantics. The SBC will only prevent unauthorised IP messages or unauthorised SIP messages to enter the PSTN network. To be able to prevent ISUP related unauthorised messages or parameters to enter the PSTN we have implemented a SIP-I based screening mask in the Call Servers. This SIP-I based screening mask will have the same design/rules as the ISUP based screening mask. The SBC used on the Telia side will prevent unauthorised IP messages or unauthorised SIP messages to enter the PSTN network.
The SBC will also provide topology hiding, session limiting, prevent DOS attacks, SIP ALG function, SIP header manipulation and also act as a dynamic FW.

5 INFLUENCED NODE TYPES AND EQUIPMENT

The equipment affected is Telia fixed transit network nodes and Operator X network nodes.