Telecommunications Standards Advisory Committee (TSAC)

Technical Specification

SIP standards for Voice Interconnection

IMDA TS SIP-INTC
Issue 1 Rev 1, xxx 2024

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Acknowledgement

The Info-communications Media Development Authority (IMDA) and the Telecommunications Standards Advisory Committee (TSAC) would like to acknowledge the following members of the TSAC Task Force (TF) for SIP standards for Voice Interconnection for their invaluable contributions to the preparation of this Technical Specification:

List of TSAC TF Members (2022-2024)

S/N	Organisation	Name
1	IMDA	Lim Wai Yean
2	IMDA	Sim Bak Chor
3	M1	Goh Bee Guat Emily
4	M1	Goh Lay Teng Christina
5	MyRepublic	Sia Chiew Shin
6	MyRepublic	Walter Klomp
7	Orange	Loris Guilbaud
8	Orange	Patrick Chu
9	Simba	Benjamin Tan
10	Singtel	Tan Wee Tiong
11	Singtel	Tay Wee Chin
12	Starhub	Aw Lay Kuan Janet
13	Starhub	Chern Kok Wai
14	Starhub	Ng Wee Peng Jason
15	SuperInternet	Wing-yan Louey
16	SuperInternet	Chee Peng Kwan
17	Verizon	Au Yeong Pak Wai
18	Verizon	Dong Jae Kum
19	Verizon	Priya Mahajan

Telecommunications Standards Advisory Committee (TSAC)

The TSAC advises IMDA on the setting of ICT standards as well as on the development and recommendation of specifications, standards, information notes, guidelines and other forms of documentation for adoption and advancement of the standardisation effort of the Singapore ICT industry (hereafter termed "IMDA Standards").

Telecommunications standards-setting in Singapore is achieved with the assistance of TSAC, where professional, trade and consumer interest in telecommunications standards is represented on the TSAC with representatives from network and service operators, equipment suppliers and manufacturers, academia and researchers, professional bodies and other government agencies.

List of TSAC Members (2024-2027)

TSAC Chairman:

Dr Chin Woon Hau	Director (Standards Development and Regulatory Technology) Infocomm Media Development Authority (IMDA)

TSAC Members:

Mr George Choo	President Association of Telecommunications Industry of Singapore (ATIS)
Mr Andy Phang	Assistant Director, Standards Development and Regulatory Technology Infocomm Media Development Authority (IMDA)
Mr Marcus Tan Cheng Lin	Head of Cybersecurity Department Institute for Infocomm Research (I2R)
Mr Denis Seek	CTO M1 Limited
Mr Ng Thian Khoon	Head, Broadcast Engineering/ Broadcast Engineering (Technology) Mediacorp Pte Ltd
Associate Professor Chau Yuen	Associate Professor, School of Electrical & Electronic Engineering Provost's Chair in Wireless Communications Nanyang Technological University (NTU)
Dr Biplab Sikdar	Head of Department, Electrical and Computer Engineering, & Area Director (Communications & Networks) National University of Singapore (NUS)
Mr Gao Peng	Head of Radio Planning Simba Telecom Pte. Ltd.
Professor Susanto Rahardja	Professor, Engineering Cluster Singapore Institute of Technology (SIT)
Mr Lim Yu Leong	Vice President, Group Strategy, Engineering & Innovation Singapore Telecommunications Ltd (Singtel)
Professor Tony Quek	Head of Information Systems and Technology Design Pillar; Cheng Tsang Man Chair Professor Singapore University of Technology and Design (SUTD)
Mr Lin Ming Yee	Vice President, Mobile Core StarHub Ltd

Contents

NOTICE

THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY ("IMDA") MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL PROVIDED HEREIN AND EXCLUDES ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. SUBJECT TO THE MAXIMUM EXTENT PERMITTED UNDER LAW, IMDA SHALL NOT BE RESPONSIBLE OR LIABLE TO YOU OR ANY THIRD PARTY FOR ANY ERRORS AND/OR OMISSIONS CONTAINED HEREIN OR FOR ANY LOSSES OR DAMAGES (INCLUDING ANY LOSS OF PROFITS, BUSINESS, GOODWILL OR REPUTATION, AND/OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES) IN CONNECTION WITH THE USE OF THIS MATERIAL.

IMDA RESERVES THE RIGHT TO CHANGE, MODIFY OR ADD TO ANY PART OF THIS DOCUMENT. NOTHING HEREIN IS INTENDED TO CREATE OR IMPOSE ANY BINDING LEGAL OBLIGATIONS OR LIABILITY WHATSOEVER ON IMDA, WHETHER EXPRESSED OR IMPLIED, AND WHETHER CONTRACTUAL OR OTHERWISE. WITHOUT PREJUDICE TO THE FOREGOING, NOTHING IN THIS DOCUMENT SHALL BIND IMDA TO ADOPT ANY PARTICULAR COURSE OF ACTION. CONSEQUENTLY, NOTHING HEREIN SHALL BE CONSTRUED AS GRANTING ANY EXPECTATION, WHETHER PROCEDURAL OR SUBSTANTIVE IN NATURE, THAT IMDA WILL TAKE OR NOT TAKE ANY PARTICULAR COURSE OF ACTION IN THE FUTURE, ARISING FROM OR DUE TO ANYTHING IN THIS DOCUMENT OR IN THE EXERCISE OF ITS DISCRETION AS A PUBLIC AUTHORITY.

IMDA DRAWS ATTENTION TO THE POSSIBILITY THAT ANY PRACTICE OR IMPLEMENTATION OF THIS STANDARD/SPECIFICATION MAY INVOLVE THE USE OF INTELLECTUAL PROPERTY RIGHTS AND TAKES NO POSITION CONCERNING THE EXISTENCE, VALIDITY AND/OR APPLICABILITY OF ANY SUCH INTELLECTUAL PROPERTY RIGHTS, WHETHER ASSERTED BY TSAC MEMBERS OR ANY THIRD PARTY.

AS OF THE DATE OF ISSUANCE OF THIS STANDARD/SPECIFICATION, IMDA HAS NOT RECEIVED WRITTEN NOTICE OF ANY PATENT RIGHTS WHICH MAY BE RELEVANT IN RELATION TO THE IMPLEMENTATION OF THIS STANDARD/SPECIFICATION. HOWEVER, IMPLEMENTERS ARE CAUTIONED THAT THIS MAY NOT REPRESENT THE LATEST INFORMATION AND ARE THEREFORE STRONGLY URGED TO CHECK WITH THE RELEVANT DATABASE IN ITU, ISO, IEC OR THE RELEVANT STANDARDS DEVELOPMENT ORGANISATION FOR INFORMATION OF INTELLECTUAL PROPERTY RIGHTS. IMPLEMENTERS ARE ADVISED TO OBTAIN THEIR OWN PROFESSIONAL, TECHNICAL AND/OR LEGAL ADVICE AND CONDUCT ALL NECESSARY DUE DILIGENCE, INCLUDING BUT NOT LIMITED TO MAKING SUCH INVESTIGATIONS OR SEEKING CLARIFICATIONS AS MAY BE APPROPRIATE, IN REGARD TO ANY DECISION OR ACTION THAT THEY INTEND TO TAKE, OR PRIOR TO THE IMPLEMENTATION OF ANY STANDARD/SPECIFICATION AS MAY BE REQUIRED.

Technical Specification for SIP standards for Voice Interconnection

1 Scope

This Specification defines the minimum technical requirements for SIP standards for Voice Interconnection at the Point of Interconnection (POI). While SIP is used for the setting up, modification and tearing down of multimedia sessions consisting of audio, video and/or data applications, the protocol and its extensions described in this document are being considered in the context of voice communications.

In addition to the standards that are used to define the signalling protocol at the POI, this document also provides the basic standards that governs communication over the media plane.

2 References

For the technical requirements captured in this Specification, reference has been made to the following standards. Where versions are not indicated, implementation of this Specification shall be based on current and valid versions of these standards published by the respective Standards Development Organisations.

1. IETF RFC 2119: “Key words for use in RFCs to Indicate Requirement Levels”
2. IETF RFC 2822: “Internet Message Format”
3. IETF RFC 3261: “SIP: Session Initiation Protocol”
4. IETF RFC 3262: “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”
5. IETF RFC 3264: “An Offer/Answer Model with the Session Description Protocol (SDP)”
6. IETF RFC 3311: “The Session Initiation Protocol (SIP) UPDATE Method”
7. IETF RFC 3323: “A Privacy Mechanism for the Session Initiation Protocol (SIP)”
8. IETF RFC 3324: “Short Term Requirements for Network Asserted identity”
9. IEFT RFC 3325: “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”
10. IETF RFC 3326: “The Reason Header Field for the Session Initiation Protocol (SIP)”
11. IETF RFC 3550: “RTP: A Transport Protocol for Real-Time Applications”
12. IETF RFC 4028: “Session Timers in the Session Initiation Protocol (SIP)”
13. IETF RFC 4566: “SDP: Session Description Protocol”
14. IETF RFC 4733: “RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals”
15. IETF RFC 5009: “Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media”
16. IETF RFC 5806: “Diversion Indication in SIP”
17. ITU-T T.38: “Procedures for real-time Group 3 facsimile communication over IP networks”
18. ITU-T G.711: “Pulse code modulation (PCM) of voice frequencies”
19. GSMA IR.92: “IMS Profile for Voice and SMS”
20. 3GPP TS 24.229: “IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3”
21. 3GPP TS 24.628: “Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification”

3 Abbreviations

IETF	Internet Engineering Task Force
POI	Point of Interconnection
PoP	Point of Presence
PRACK	Provisional Response Acknowledgement
RFC	Request for Comments
SDP	Session Description Protocol
SIP	Session Initiated Protocol
UA	User Agent which is either a UAC or UAS
UAC	User Agent Client which sends request and receives responses
UAS	User Agent Server which receives requests and sends responses

4 Technical Requirements

4.1 The POI is the physical interface that is used to connect between the gateways of two networks. In order for the smooth connection of the two networks, the operators of the networks have to agree on the signalling protocol(s) to be used at the POI.

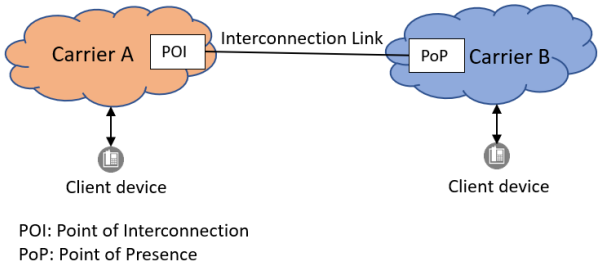

Figure 1. Interconnection between two networks

4.2 The signalling protocol to be used at the POI is the Session Initiation Protocol (SIP) defined by the Internet Engineering Task Force (IETF), a standards development organisation. The IETF produced a set of documents known as the "Request for Comments" (RFC) which have been used to define many internet protocols. SIP is an application layer signalling protocol for establishing, modifying and termination multimedia sessions between participants over an IP network. It is independent of the underlying transport layer protocol and can be used with User Datagram Protocol (UDP), the Transmission Control Protocol (TCP) and the Stream Control Transmission Protocol (SCTP).

4.3 Operators wishing to interconnect their networks using SIP need to agree on the set of RFCs used, so that the networks can communicate seamlessly with one another. The absolute requirements and prohibitions in the agreed RFCs listed in this document form the baseline specifications that the interconnecting networks must comply to. Additional specifications that need to be implemented are be negotiated and agreed to by the operators of the interconnecting networks. Similarly, RFC versions that are not stated in this document could be separately used by operators of the interconnecting networks, subject to agreements by the operators.

4.4 The following is the basic set of standards used for the signalling plane at the POI:

S/N	Standard	Description	Mandatory/Optional
1	RFC 3261	Session Initiation Protocol	Mandatory
2	RFC 4566	SDP: Session Description Protocol	Mandatory
3	RFC 3262	Reliability of Provisional Responses in Session Initiation Protocol	Mandatory
4	RFC 3264	An Offer/Answer Model with the Session Description Protocol	Mandatory
5	RFC 3311	The Session Initiation Protocol UPDATE Method	Mandatory
6	RFC 3323	A Privacy Mechanism for the Session Initiation Protocol	Mandatory

7	RFC 3325	Private Extensions to the Session Initiation Protocol for Network Asserted Identity within Trusted Networks	Mandatory
8	RFC 3326	The Reason Header Field for the Session Initiation Protocol	Mandatory
9	RFC 5806	Diversion Indication in SIP	Mandatory
10	RFC 4028	Session Timers in the Session Initiation Protocol	Mandatory
11	RFC 5009	Private Header (P-Header) Extension to the Session Initiation Protocol for Authorization of Early Media	Mandatory for Mobile Network Operators only

Table 1. List of IETF RFCs for compliance at the POI

Descriptions of the RFCs are provided in section 5.

4.5 Besides the signalling plane standards, there are media plane standards used to ensure the seamless transmission of media streams between networks at the POI. The primary standards for the media plane are as follows:

S/N	Standard	Description
1	ITU-T T.38	Procedures for real-time Group 3 facsimile communication over IP networks
2	ITU-T G.711	Pulse code modulation (PCM) of voice frequencies
3	RFC 4733	RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
4	RFC 3550	RTP: A Transport Protocol for Real-Time Applications
Note: Carriers that are not providing facsimile services are not required to comply to ITU-T T.38. This does not include carriers which are providing the POI in their networks.		

4.6 Cybersecurity requirements

The cybersecurity requirements for operators interconnecting their IP-based networks for voice services can be found in the document IMDA SEC-INTC. This document may be downloaded from the IMDA website at http://www.imda.gov.sg and shall not be distributed without written permission from IMDA. Operators must comply to these requirements.

5 Description of RFCs for the signalling plane

This section provides a brief description of the functionalities given in the list of RFCs in Table 1. The keywords used in the RFCs, “MUST” and “SHALL” are to be interpreted as absolute requirements of the specifications while “MUST” and “MUST NOT” are absolute prohibition of the specification, in accordance to RFC 2119.

It is to be noted that not all the absolute requirements or absolute prohibitions are mentioned in this section. Please refer to the official standards documents for the full details.

5.1 RFC 3261 – SIP: Session Initiation Protocol

A SIP message is either a request from a client to a server, or a response from a server to a client. Both

Request and Response messages use the basic format of RFC 2822. Both types of messages consist of a start-line, one or more header fields, an empty line indicating the end of the header fields, and an optional message-body. The request message is also known as a method.

Generic-message	=	start-line *message-header CRLF [message-body]
Start-line	=	Request-Line / Status-Line

The start-line, each message-header line, and the empty line must be terminated by a carriage-return line-feed sequence (CRLF). Note that the empty line must be present even if the message-body is not.

5.1.1 Request

SIP requests are distinguished by having a Request-Line for a start-line. A Request-Line contains a method name, a Request-URI, and the protocol version separated by a single space (SP) character. SIP responses are distinguished from requests by having a Status-Line as their start-line. There are fourteen SIP Request methods and the six below are the most basic:

SIP Method	**Purpose**	**Remarks**
INVITE	Invites a call by inviting user to participate in session. A media session is established when the INVITE, 200 OK and ACK messages have been exchanged between the UAC and UAS	Mandatory to support
ACK	Confirms that the client has received a final response to an INVITE request	Mandatory to support
BYE	Indicates termination of the call; A BYE is sent only by UAs participating in the session, never by proxies or other third parties	Mandatory to support
CANCEL	Cancels a pending request	Mandatory to support
OPTIONS	Used to query the capabilities of a server	Mandatory to support
REGISTER	Registers the user agent	Not needed for messages between operators

A SIP request must, at a minimum, contain the following header fields.

SIP header	**Description**
To	The To header specifies the recipient of the call. The To header field may contain a SIP or SIPS URI, but it may also make use of other URI such as the tel URL (RFC 2806) when appropriate. All SIP implementations must support the SIP URI scheme, while implementation that supports TLS must support the SIPS URI scheme.
From	The From header specifies who the call is coming from.
CSeq	The CSeq header specifies the number of requests of each type that have been sent. It consists of a sequence number and a method. The method must match that of the request.

Call-ID	The Call-ID SIP header creates a globally unique identifier for the call. Call-IDs are case-sensitive.
Max-Forwards	The Max-Forwards header sets the limit of the number of hops a request can transit on the way to its destination.
Via	The Via header identifies the call's path. When UAC creates a request, it must insert a Via into that request together with the protocol name and protocol version, which are SIP and 2.0, respectively. The Via header field values must contain a branch parameter, which is a unique token and must start with the value z9hG4bK. It is used to identify the transaction created by that request and helps to ensure route back to originator.

5.1.2 Response and Status/Response codes

As opposed to requests, a SIP response has Status-Line as their start-line. A Status-Line consists of the protocol version followed by a numeric Status-Code and its associated textual phrase.

The response codes that are used in SIP are given in the below table, where "1xx" refers to any response with a status code between 100 and 199, "2xx" refers to a status code between 200 and 299, and so on.

Response codes	**Description**
1xx	Provisional
2xx	Success
3xx	Redirection
4xx	Client Error
5xx	Server Error
6xx	Global failures

5.2 RFC 4566 – SDP: Session Description Protocol

This RFC defines the Session Description Protocol which is used to describe multimedia sessions for the purposes of session announcement, session invitation and other forms of multimedia session initiation.

An SDP session description is denoted by the media type "application/sdp". SDP session descriptions are text-based and consists of a number of lines of text of the form:

Type=value

The type field is always one lower case character and the format of the value field depends on which type it applies. Whitespace must not be used on either side of the "=" sign.

An SDP session description starts with the session-level section followed by zero or more media-level sections. The session-level section contains information for the whole session, while media-level section contains information that applies to specific media stream. Session-level values are the default for all media unless overridden by an equivalent media-level value.

The descriptions contain REQUIRED and OPTIONAL lines, and all must appear in the order as given below:

Field	Name	Mandatory/Optional
Session description		
v	Protocol version	Mandatory
o	Originator and session identifier	Mandatory
s	Session name	Mandatory
i	Session information	Optional
u	URI of description	Optional
e	Email address	Optional
p	Phone number	Optional
c	Connection information	Mandatory (Not required if included in all media)
b	Bandwidth information	Optional
Time description		
t	Time session start and stop	Mandatory
r	Repeat times	Optional
Session description		
z	Time zone corrections	Optional
k	Encryption key	Optional
a	Attribute lines	Optional
Media description, if present		
m	Media information	Optional
i	Media title	Optional
c	Connection information	Optional
b	Bandwidth information	Optional
k	Encryption key	Optional
a	Media attributes	Optional

5.3 RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

This document specifies an extension to the Session Initiation Protocol (SIP) providing reliable provisional response messages. SIP defines two types of responses, provisional and final. A final response is defined as a response that terminates a SIP transaction and is sent reliably. All 2xx, 3xx, 4xx, 5xx and 6xx responses are final.

A provisional response is one that does not terminate a SIP transaction and is not sent reliably. However, there are cases where reliable provision responses need to be sent. That capability is provided in this specification.

The UAS must send any non-100 provisional response reliably if the initial request contained a Require header with the option tag 100rel. UAS could also reject the initial request with a 420 (bad Extension) by including an Unsupported header field containing the option tag 100rel.

When using reliable provisional responses, responses are retransmitted by the UAS in response to an INVITE until a Provisional Response Acknowledgement (PRACK) is received from the UAC.

5.4 RFC 3264 – An Offer/Answer Model with the Session Description Protocol

This RFC defines a mechanism by which two entities can make use of the Session Description Protocol (SDP) to arrive at a common view of a multimedia session between them. While SDP describes multimedia sessions, it lacks the semantics and operational details on how it is actually done. RFC 3264 defines a simple offer/answer model based on SDP. In this model, one participant in the session, known as the offerer, generates an SDP message that lists the set of media streams and codecs, along with the IP addresses and ports, which the offerer would like to use to receive the media. Another participant in the session, known as the answerer, will generate an answer which has a matching media stream for each stream in the offer, indicating whether the stream is accepted or not, along with the codecs that will be used and the IP addresses and ports that the answerer wants to use to receive media.

The offer/answer assumes the existence of a higher-layer protocol (such as SIP) which is capable of exchanging SDP for the purposes of session establishment between agents. Protocol operation begins when one agent sends an initial offer to another agent. The agent receiving the offer may generate an answer, or it may reject the offer. Either agent may generate a new offer that updates the session but it must not generate a new offer if it has received an offer which it has not yet answered or rejected. It must also not generate a new offer if it has generated a prior offer for which it has not yet received an answer or a rejection.

5.4.1 Generating an Offer

The offer (and answer) must be a valid SDP message, and the SDP message used in the offer/answer model must contain exactly one session description.

The offer will contain zero or more streams (each media stream is described by an “m=” line and its associated attributes). Zero media streams implies that the offerer wishes to communicate, but that the streams for the session will be added at a later time through a modified offer.

If the offerer wishes to only send media on a stream to its peer, it must mark the stream as send-only with the “a=sendonly” attribute. If the offerer wishes to only receive media from its peers, it must mark the stream with the “a=recvonly” attribute. If the offerer wishes to communicate, but wishes to neither send nor receive media at this time, it must mark the stream with the “a=inactive” attribute.

If the offer has a port number of zero, it indicates that the stream is offered but must not be used.

5.4.2 Generating an Answer

For each “m=” line in the offer, there must be a corresponding “m=” line in the answer. The answer must contain exactly the same number of “m=” lines as the offer.

If the answer contains a zero port then it indicates that the stream is rejected, or if the stream is accepted then it contains a nonzero port number.

5.4.3 Modifying a Session

The “o=” line of the new SDP must be identical to that in the previous SDP, except that the version in the origin field must increment by one from the previous SDP. If the version in the origin line does not increment, the SDP must be identical to the SDP with that version number.

If an SDP is offered, which is different from the previous SDP, the new SDP must have a matching media stream for each media stream in the previous SDP. Deleted media streams from a previous SDP must not be removed in a new SDP; however, attributes for these streams need not be present.

Additional media streams can be added below the existing ones. Existing streams can also be terminated by setting the port number to zero.

5.5 RFC 3311 – The Session Initiation Protocol UPDATE Method

This specification defines the new UPDATE method for the SIP. UPDATE allows a client to update parameters of a session (such as the set of media streams and their codecs) but does not impact the state of a dialog. In this respect, it is different from RE-INVITE, which changes the state of a dialog. Also, as opposed to RE-INVITE, an UPDATE needs to be answered immediately. Another aspect which UPDATE is different from RE-INVITE is that it can be sent prior to session establishment. RE-INVITE is sent after a session has been established.

5.6 RFC 3323 – A Privacy Mechanism for the Session Initiation Protocol

This RFC provides privacy requirements and mechanisms for the Session Initiation Protocol. Privacy is defined in this RFC as the withholding of the identity of a person (and related personal information) from one or more parties in an exchange of communications.

RFC 3323 describes three degrees of privacy – one level of user-provided privacy and two levels of network-provided privacy (header privacy and session privacy).

This document defines a new SIP header, Privacy, that can be used to specify privacy handling for requests and responses. The syntax of the header field is as follows:

Privacy-hdr = “Privacy” HCOLON priv-value *(“;” priv-value)
priv-value = “header” / “session” / “user” / “none” / “critical” / token

When a Privacy header is constructed, it must consist of either the value “none”, or one or more of the values ‘user’, ‘header’, and ‘session’ (each of which must appear at most once which may in turn be followed by the ‘critical’ indicator.

When Privacy: none, it means that privacy services must not perform any privacy function, and intermediaries must not remove or alter the Privacy header.

5.7 RFC 3325 – Private Extensions to the Session Initiation Protocol for Asserted Identity within Trusted Networks

This RFC describes private extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy. The use of these extensions is only applicable inside a 'Trust Domain' as defined in RFC 3324.

The behaviour of a proxy could be summarised as follows:

Proxy behaviour when it receives a message

1. If proxy receives a message from a node that it trusts, it will use the information in the P-Asserted-Identity header field as though it had authenticated the user itself. If there is no P-Asserted-Identity header field, it may add at most one SIP/SIPS URI or at most one tel URI.
2. If proxy receives a message from a node that it does not trust, it must authenticate the originator of the message, and use the identity which results from this authentication to insert a P-Asserted-Identity header field into the message. If there is already a P-Asserted-Identity that contains a SIP/SIPS or tel URI then it must replace or remove the header field.

Proxy behaviour when it forwards a message

1. If proxy forwards a message to a node that it trusts, it does not remove any P-Asserted-Identity header fields that it generated, or that it received from a trusted source.
2. If proxy forwards a message to a node that it does not trust, it must examine the Privacy header (if present). If Privacy header field value is set to “id” then all the P-Asserted-Identity header fields must be removed. If Privacy header field value is set to “none” then P-Asserted-Identity header fields must not be removed. If there is no Privacy header field, then the proxy may include the P-Asserted-Identity header field or it may remove it.

On dealing with multiple identities

If proxy receives a P-Preferred-Identity header field from a node that it does not trust, it may use this information as a hint suggesting which of multiple valid identities for the authenticated user should be inserted. If such a hint is not possible, then the proxy can add a P-Asserted-Identity header of its own construction, or it can reject the request. The proxy must remove the user-provided P-Preferred-Identity header from any message it forwards.

The syntax of the P-Asserted-Identity header field is as follows:

PAssertedID	=	“P-Asserted-Identity” HCOLON PAssertedID-value *(COMMA PAssertedID-value)
PAssertedID-value	=	name-addr / addr-spec

The syntax of the P-Preferred-Identity header field is as follows:

PPreferredID	=	“P-Preferred-Identity” HCOLON PPreferredID-value *(COMMA PPreferredID-value)
PPreferredID-value	=	name-addr / addr-spec

The syntax of the Privacy header field is as follows:

priv-value = “id”

5.8 RFC 3326 – The Reason Header Field for the Session Initiation Protocol

This RFC defines a header field, Reason, that provides the reason to why a particular SIP request is being issued.

One example of such a use could be when a SIP CANCEL request is being issued. Such a request can be issued when the call has been completed on another branch or it was abandoned before answer.

Providing a reason for the CANCEL request will provide context to the recipient about the nature of the cancellation and this could be used for diagnostic and logging purposes.

The syntax of the header field is as follows:

Reason	=	"Reason" HCOLON reason-value *(COMMA reason-value)
reason-value	=	protocol *(SEMI reason-params)
protocol	=	"SIP" / "Q.850" / token
reason-params	=	protocol-cause / reason-text / reason-extension
protocol-cause	=	"cause" EQUAL cause
cause	=	1*DIGIT
reason-text	=	"text" EQUAL quoted-string
reason-extension	=	generic-param

5.9 RFC 5806 – Diversion Indication in SIP

This RFC proposes an extension to SIP that provides the ability for the called SIP user agent to identify from whom the call was diverted and why the call was diverted. A header field, Diversion, is used to convey the diversion information.

The Diversion header should be added when a call is redirected or forwarded. It should not be added for normal call routing changes to the Request-URI. Prior to a diversion, the Diversion header must contain the Request-URI of the request. The Diversion header should also contain a reason that the diversion occurred.

Existing Diversion headers received in an incoming request must not be removed or changed in forwarded requests.

Existing Diversion headers received in an incoming response must not be removed or changed in the forwarded response.

The syntax of the Diversion header field is as follows:

Diversion	=	"Diversion" ":" 1# (name-addr *(";" diversion_params))
diversion-params	=	diversion-reason | diversion-counter | diversion-limit | diversion-privacy | diversion-screen | diversion-extension
diversion-reason	=	"reason" "=" ("unknown" | "user-busy" | "no-answer" | "unavailable" | "unconditional" | "time-of-day" | "do-not-disturb" | "deflection" | "follow-me" | "out-of-service" | "away" | Token | quoted-string)
diversion-counter	=	"counter" "=" 1*2DIGIT
diversion-limit	=	"limit" "=" 1*2DIGIT
diversion-privacy	=	"privacy" "=" ("full" | "name" | "uri" | "off" | token | quoted-string)
diversion-screen	=	"screen" "=" ("yes" | "no" | token | quoted-string)

diversion-extension = token [“=” (token | quoted-string)]

5.10 RFC 4028 – Session Timers in the Session Initiation Protocol

The Session-Expires header field conveys the session interval for a SIP session. It is placed only in INVITE or UPDATE requests, as well as in any 2xx response to an INVITE or UPDATE. Like the SIP Expires header field, it contains a delta-time. The absolute minimum for the Session-Expires header field is 90 seconds.

The syntax of the Session-Expires header field is as follows:

Session-Expires = (“Session-Expires” / “x”) HCOLON delta-seconds *(SEMI se-params)
se-params = refresher-param / generic-param
refresher-param= “refresher” EQUAL (“uas” / “uac”)

Note that a compact form, the letter x, has been reserved for Session-Expires.

Header	where	proxy	ACK	BYE	CAN	INV	OPT	REG	PRA	UPD	SUB	NOT
Session-Expires	R	amr	-	-	-	o	-	-	-	o	-	-
Session-Expires	2xx	ar	-	-	-	o	-	-	-	o	-	-
Min-SE	R	amr	-	-	-	o	-	-	-	o	-	-
Min-SE	422		-	-	-	m	-	-	-	m	-	-

Table 2: Session-Expires and Min-SE Header Fields

The Min-SE header field indicates the minimum value for the session interval, in units of delta-seconds. When used in an INVITE or UPDATE request, it indicates the smallest value of the session interval that can be used for that session. When present in a request or response, its value must not be less than 90 seconds.

5.11 RFC 5009 – Private Header (P-Header) Extension to the Session Initiation Protocol for Authorization of Early Media

It is a GSMA requirement that mobile UE need to support this. In the GSMA document, IR. 92, it is stated that:

> The UE must behave as specified in section 4.7.2.1 of 3GPP Release 13 TS 24.628.
>
> In addition, the UE must support the P-Early-Media header field with the “supported” parameter to initial INVITE requests it originates as specified in section 5.1.3.1 of 3GPP TS 24.229.
>
> The UE must also maintain an early media authorization state per dialog as described in RFC 5009.
>
> As stated in 3GPP TS 24.628, the UE must render locally generated communication progress information, if:

- an early dialog exists where a SIP 180 response to the SIP INVITE was received;
- no early dialog exists where the last received P-Early-Media header field as described in IETF RFC 5009 contained “sendrecv” or “sendonly”; and
- in-band information is not received from the network.

6. Example showing RFC extracts that are being used in a typical SIP INVITE message

Below is a typical SIP INVITE message showing the different headers and message body with their RFC references.

Sample INVITE message

Session Initiation Protocol (INVITE) //**IETF RFC 3261**
Request-Line: INVITE sip:69741234@domain.org;user=phone SIP/2.0
Message Header //**IETF RFC 3261**
Content-Length:430
From:<sip:90920000@domain.org;user=phone>;tag=i484WbAA93745Ug5
To:<sip:69741234@domain.org;user=phone>
Via:SIP/2.0/UDP
172.27.X.X:5080;branch=z9hG4bK7YDc0D979b3C8Z26;yop=00.00.CCEA4CC2.0000.7003
Call-ID:0369F14BDD2BC156877D4397@0370ffffffff
CSeq:1 INVITE
Max-Forwards: 64
P-Asserted-Identity:sip:90920000@domain.org;user=phone;cpc=ordinary //**IETF RFC 3325**
Session-Expires:1800;refresher=uac //**IETF RFC 4028**
Contact:<sip:172.27.X.X:5080;yop=00.00.CCEA4CC2.0000.7003>
Require:precondition
Supported:100rel //**IETF RFC 3262**
Allow:ACK,BYE,CANCEL,INFO,INVITE,NOTIFY,OPTIONS,PRACK,REFER,UPDATE
Content-Type:application/sdp //**IETF RFC 4566**

Message Body
Session Description Protocol //**IETF RFC 4566**
Media Description, name and address (m): audio 43078 RTP/AVP 96 97 3 8 98 //**IETF RFC 3264**
Media Attribute (a): rtpmap:96 AMR/8000
Media Attribute (a): rtpmap:97 GSM-EFR/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): rtpmap:98 telephone-event/8000 //**IETF RFC 4733**

Example provided by M1