

SIPconnect Compliance Survey



Thank you for your interest in the SIP Forum's SIPconnect Compliant certification program. This survey is required as part of your application to participate in the SIPconnect Compliant program. A unique survey response should be completed for each product being listed as SIPconnect Compliant.

You may find it helpful to reference the [SIPconnect Technical Recommendation](#) and/or a [PDF version](#) of this survey while completing your on-line response.

In addition to the completion of the survey, applicants must also submit a [Certification Mark Application](#) and sign and return the [License Agreement](#).

If you have any questions about the program, please contact sipconnect@sipforum.org.

1

[Contact Information]

Name:	<input type="text"/>
Company:	<input type="text"/>
Address 1:	<input type="text"/>
Address 2:	<input type="text"/>
City/Town:	<input type="text"/>
State/Province:	<input type="text"/>
Zip/Postal Code:	<input type="text"/>
Country:	<input type="text"/>
Email Address:	<input type="text"/>

2

For what type of product are you reporting compliance with the SIPconnect Technical Recommendation. If the element tested performs two or more functions (i.e. Proxy Server and Application Server or PBX

and Proxy Server) you can select all that apply.

- Service Provider Service
- PBX
- SIP Proxy Server (SPS)
- SIP Application Server (SAS)
- Other, please specify

3

Please specify the product represented by this survey.

Submit

Survey Page 1

SIPconnect Compliance Survey

STANDARDS SUPPORT

4

Please rate your compliance with the following RFCs found in Section 6 of the SIPconnect Technical Recommendation. If the table in the document indicates that compliance is Recommended (RO) or Not Required (-) you may select "Not Required for the Element Being Certified."

1	2	3	4
Compliant	Substantially Compliant	No Compliant	Not Required for the Element Being Certified

ITU-T Recommendation E.164: The international public telecommunication numbering plan

1 2 3 4

RFC 2246: The TLS Protocol Version 1.0

1 2 3 4

RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

1 2 3 4

RFC 2782: A DNS RR for specifying the location of services (DNS SRV)

1 2 3 4

RFC 3261: Session Initiation Protocol

1 2 3 4

RFC 3262: Reliability of Provisional Responses in Session Initiation Protocol (SIP)

1 2 3 4

RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers

1 2 3 4

RFC 3264: An Offer/Answer Model with Session Description Protocol (SDP)

1 2 3 4

RFC 3311: The Session Initiation Protocol (SIP) UPDATE Method

1 2 3 4

RFC 3323: A Privacy Mechanism for the Session Initiation Protocol (SIP)

1 2 3 4

RFC 3324: Short Term Requirements for Network Asserted Identity

1 2 3 4

RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

1 2 3 4

RFC 3489: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)

1 2 3 4

RFC 3581: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing

1 2 3 4

RFC 3725: Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)

1 2 3 4

RFC 4028: Session Timers in the Session Initiation Protocol (SIP)

1 2 3 4

Submit

Survey Page 2

SIPconnect Compliance Survey

LOCATING SIP SERVERS

5

Enterprise Requirements

Enterprise SIP Proxy Servers (or PBXs/SPSs performing this function) MUST utilize DNS NAPTR and SRV queries as described in RFC 3263 to determine the IP address, transport protocol, and port number of the SIP Proxy Server(s) associated with the Service Provider's domain name.

6

Enterprise Requirements

The PBX must support the ability to register a contact address against one or more or more SIP URIs with the Service Provider's SIP Application Server.



7

Service Provider Requirements

The Service Provider MUST operate a publicly-accessible DNS server that is authoritative for its domain. This DNS server SHOULD support NAPTR resource records and MUST support SRV resource records.



8

Service Provider Requirements

Though not required, it is RECOMMENDED that Service Providers deploy redundant SIP Proxy Servers to service customer traffic. If redundant servers are deployed, the Service Provider MUST utilize the mechanism outlined in RFC 2782 to return a prioritized list of contact information for the SIP Proxy Servers in DNS SRV resource records associated with the Service Provider's domain name.



9

Service Provider Requirements

Service Provider SIP Proxy Servers MUST utilize DNS NAPTR and SRV queries as described in RFC 3263 to determine the IP address, transport protocol, and port number of the SIP Proxy Server(s) associated with the Enterprise network's domain name



10

Service Provider Requirements

SIP Application Servers MUST be prepared to accept (but MUST NOT

require) registrations for any valid URI that the Service Provider has assigned to an Enterprise.

Survey Page 3

SIPconnect Compliance Survey

SIGNALING SECURITY

11

SIP Proxy Servers MUST support Transport Layer Security (TLS) as described in RFCs 2246 and 3261.

12

All SIP signaling exchanged between the Service Provider and Enterprise SIP Proxy Servers MUST be secured using TLS.

13

The TLS connection MUST be able to be established by both the Service Provider's and Enterprise's SIP Proxy Server.

14

SIP Proxy Servers MUST utilize a verifiable digital certificate to secure the TLS session.

15

SIP Proxy Servers MUST use canonical hostnames in any 'Via:' and/or 'Route:' SIP header field that it inserts in the SIP message.

16

Certificates used to establish a TLS connection MUST be verified and MAY be validated. Verification steps include verifying that the certificate has not expired, that the issuing certification authority is one the SIP Proxy Server trusts, and finally that the subject of the certificate matches the host portion of the target URI. Validation steps include checking the status of the certificate as well as the status of all the certificates in the certificate chain using CRLs or other mechanisms such as OCSP.

17

Service Provider certificates SHOULD be signed by a third party certification authority.

Survey Page 4

SIPconnect Compliance Survey

FIREWALL AND NAT TRAVERSAL

18

SIP intermediaries MUST NOT modify IP addresses or port numbers in the body or Contact header of any message if any of the following are true:

- Any "application/sdp" body in the message contains any "a=candidate:" lines (indicating use of the ICE extension)
- All the "c=" lines in any "application/sdp" bodies contain only public IP addresses (indicating that another element has already ensured the addresses are correct).

Submit

Survey Page 5

SIPconnect Compliance Survey

AUTHENTICATION AND ACCOUNTING

Authentication of the Enterprise by the Service Provider

Authentication of the Enterprise by the Service Provider can be performed in one of two ways. PBX systems MUST implement Option 1 and MAY implement Option 2.

SIP Application Servers MUST support both Option 1 and Option 2 in order to ensure interoperability with all PBX systems

19

Option 1: Authentication using TLS Credentials

This method relies on authorization of the identity asserted by the Enterprise's verified certificate used to establish the TLS connection with the Service Provider's SIP Proxy Server. This model requires that the Service Provider's SIP Proxy Server and SIP Application Server be capable of exchanging authorization, accounting, and usage information on a per-call basis in order to ensure complete billing traceability through the network. When this model is utilized, information identifying the Enterprise is extracted from the Enterprise's certificate (for example, domain name) by the SIP Proxy Server and conveyed to the "downstream" device as necessary. (It is out of the scope of this interface specification to specify the actual mechanism used to convey this information within the Service Provider's Network.)

20

Option 2: Digest Access Authentication

This method of authenticating an Enterprise utilizes the digest authentication scheme as described in section 22.4 of RFC 3261. In this model the Service Provider assigns the Enterprise Network a username and password (referred to as a "Network Account" hereafter) that is valid within the Service Provider's domain (realm).

When this model is employed, the following rules must be observed:

1. When processing an INVITE request from an unauthenticated PBX, the SIP Application Server **MUST** challenge the message, only accepting authentication credentials that are valid within its realm.
2. When processing a REGISTER request from an unauthenticated PBX, the SIP Application Server **MUST** challenge the message, only accepting authentication credentials that are valid within its realm.
3. When challenged by the SIP Application Server, the PBX **MUST** respond with authentication credentials that are valid within the Service Provider's realm (i.e. the network account username and password supplied by the Service Provider).
4. In order to avoid unnecessary challenges, the PBX **SHOULD** include its authentication credentials using the current nonce in each request sent to the SIP Application Server.

Submit

Survey Page 6

SIPconnect Compliance Survey

ENTERPRISE PSTN IDENTITIES

21

This specification considers a single E.164 address equivalent to a single "PSTN identity." Accordingly, a PBX with 100 assigned telephone numbers would have 100 associated PSTN identities.

The PBX MUST choose which of its valid PSTN identities to use on a per-call basis. For example, on a call from a user without a dedicated telephone number (i.e. DID number) the PBX might choose to assert its "main" identity (e.g. the company's main business number), while a call from a user with a dedicated DID number would use the identity of that user's specific telephone number.

22

At some point a translation between an E.164 address on the PSTN and an Enterprise's SIP URI will need to be performed. This requirement implies that the SIP Application Server MUST maintain an E.164 address to Enterprise domain mapping table that is used to perform routing decisions for calls received from the PSTN.

Survey Page 7

SIPconnect Compliance Survey

ENTERPRISE URI FORMATTING AND ADDRESSING RULES

23

Any device that handles signaling MUST support addressing for closed (fixed length) and open (variable length) numbering plans.

24

'From:' Field

Utilizing the 'From:' and 'P-Asserted-Identity:' SIP Header Fields

The first method for communicating PSTN identity information utilizes the 'From:' field in conjunction with the 'P-Asserted-Identity:' field as described in RFC 3325. This method allows the Enterprise to deliver a "public" and "private" PSTN identity to the Service Provider per call. The public identity represents the identity that the Enterprise wants to deliver to the PSTN for a given call. The private identity represents the identity that the Enterprise wants to deliver to the Service Provider for a given call.

When this method is used, the 'From:' field is populated with the Enterprise's desired public identity (e.g. the company or department's main business number) or an anonymous URI as described in RFC 3261. The caller's private identity information is provided to the Service Provider by utilizing the 'P-Asserted-Identity:' and 'Privacy:' SIP header fields as described in RFC 3325. It is important to note that SIP Application Servers **MUST ONLY** use any provided private identity information to provide services and/or features that the Enterprise has subscribed to for that identity.

For the purposes of this specification, the Enterprise SIP Proxy Server is considered part of the Service Provider's "Trust Domain", as defined in RFC 3325. When the SIP Application Server routes the call to any network element in the Service Provider's network that does not support RFC 3325, it **MUST** consider the network element to be outside of its Trust Domain. Per RFC 3325, this means that the SIP Application Server **MUST NOT** disclose or otherwise pass any information contained in the 'P-Asserted-Identity:' header field to that network element. In addition, the SIP Application Server **MUST** remove any 'P-Asserted-Identity:' SIP header fields and the SIP header field requesting privacy.

When this method is used, the PBX **MUST** format all INVITES sent to the Service Provider according to the following rules:

1. The PBX **MUST** populate the 'From:' field with the URI that is associated with its desired public PSTN identity or an anonymous URI. The PBX **SHOULD** also provide any applicable display name information (e.g. "Acme Rockets Sales Department").
2. The PBX **MUST** include a SIP 'Privacy:' header field that requests "id" privacy as defined in RFC 3325.
3. The PBX **MUST** populate the 'P-Asserted-Identity:' SIP header field with one of the options below (listed in order of preference):
 - a. The PBX caller's telephone number in ITU-T E.164 format + Enterprise domain name and (optional) desired display name information.
 - b. Other RFC-3261-compliant URI format agreed upon by the Service Provider and customer.



25**'From:' Field****Utilizing the 'From:' SIP Header Field only**

The second method for passing Enterprise PSTN identity information uses the 'From:' field described in RFC 3261. This method provides less overall flexibility due to the fact that it allows only one identity to be conveyed to the Service Provider on a given call. When this method is used, the single identity is used by the Service Provider as both the "public" and "private" PSTN identities for the call.

When using this method, the following requirements **MUST** be observed:

1. The 'From:' field **MUST** contain a SIP URI containing the PBX's desired PSTN identity for the PBX caller. In the event the PBX caller does not have its own PSTN identity, the main PSTN identity of the PBX **SHOULD** be used to populate the 'From:' field. If available, the PBX **SHOULD** also provide any applicable display name information (e.g. "John Doe", "Acme Rockets").
2. The format of the 'From:' field **MUST** be expressed as one of the following two options listed in order of preference):
 - a. ITU-T E.164 format + Enterprise domain name.
 - b. Other RFC-3261-compliant URI format agreed upon by the Service Provider and Enterprise

26**'To:' Field****PSTN Destinations**

This interface specification provides two methods of communicating the PBX's destination (dialed) E.164 address to the Service Provider's SIP Application Server. PBX systems **MUST** implement at least one of these options. SIP Application Servers **MUST** support both methods in order to ensure interoperability with all PBX systems.

Option 1: SIP URI

To: sip:[E.164 Address]@[Service Provider Domain Name];user=phone

Option 2: tel: URL

To: tel:[E.164 Address]

27**'To:' Field****Emergency Services Destinations**

The PBX SHOULD format the 'To:' field as follows when an emergency services call is made:

```
To: sip:[Country-specific emergency services address];phone-context=[Predetermined Geographic E.164 Address]@[Service Provider Domain Name] ;user=phone
```

The country-specific emergency services address is defined as the dial string used in the country of origin to request emergency services. The phone-context parameter SHOULD contain a valid E.164 address previously agreed upon by the Enterprise and Service Provider to represent the physical location from which the call originated. The Service Provider SHOULD ensure that valid location information for this E.164 address is provisioned in the ALI database.

For example, an emergency services call originating in the United States with a Geographic E.164 address of +16789901234 would be formatted as follows:

```
To: sip:911;phone-context=+16789901234@serviceprovider.net;user=phone
```



28**'To:' Field****Other Destinations**

While this interface specification defines no particular call handling behavior for URI formats other than those described above, the SIP Proxy Server and SIP Application Server SHOULD support any URI format that conforms to RFC 3261.



29**Request-URI**

The initial Request-URI of any SIP message generated by an IP PBX system MUST adhere to the same formatting rules as that of the 'To:' field described in sections 12.2, 12.3, and 12.4 of the SIPconnect Technical Recommendation

Survey Page 8

SIPconnect Compliance Survey

SERVICE PROVIDER URI FORMATTING AND ADDRESSING RULES

30

'From:' Field

If the PSTN caller has supplied their E.164 address and did not request calling number privacy, SIP Application Servers MUST populate the 'From:' field with the E.164 address of the PSTN caller + Service Provider domain name as shown below. If any display name information is available and has not been restricted for delivery, it SHOULD also be provided.

From: "Acme
Rockets" [sip:+15616261234@serviceprovider.net;user=phone];tag=5320917

If the PSTN caller has not supplied their E.164 address or has requested calling number privacy, one of the following two anonymous URIs MUST be populated in the 'From:' field:

From: "Anonymous" [sip:anonymous@anonymous.invalid];tag=0728361

From: "Anonymous" [anonymous@[domain name];tag=0728361

31

'To:' Field

The SIP Application Server MUST populate the 'To:' field with the Enterprise PSTN identity associated with the dialed E.164 address + Enterprise domain name as shown below:

To: sip:+16789901234@acmerockets.com;user=phone

32

Request-URI

The initial Request-URI of any SIP message generated by a SIP Application Server MUST adhere to the same formatting rules as that of the 'To:' field described in section 13.2 of the SIPconnect Recommendation.

Survey Page 9

SIPconnect Compliance Survey

QUALITY OF SERVICE CONSIDERATIONS

33

IP Packets containing SIP signaling messages or RTP voice samples MUST be marked with a predefined value in the packet header before being sent to the peer's network. This provides the Service Provider and Enterprise with a standard mechanism for identifying and prioritizing voice-related packets at the edge and in the core of their packet networks.

In order to accomplish this goal, the interface specification outlined by this document requires the use of the Differentiated Services Field as specified in RFC 2474.

34

The following IP packet marking values are RECOMMENDED for use between the Enterprise and Service Provider network edges.

Packet Type	DiffServ PHB	DSCP Value	Binary Equivalent Value
SIP Signaling Message	CS5	40	Binary = 101000
RTP Media	EF	46	Binary = 101110

Survey Page 10

SIPconnect Compliance Survey

MEDIA ATTRIBUTES AND MINIMUM REQUIREMENTS

35

Media Capability Negotiation

Any device that originates and/or terminates RTP traffic MUST utilize the Session Description Protocol (SDP) as described in RFC 2327 in conjunction with the offer/answer model described in RFC 3264 to exchange session information (IP address, port number, media type, send/receive mode, codec, DTMF mode, etc).

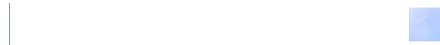
36

Media Capability Negotiation

Any device that originates and/or terminates RTP traffic MUST include an attribute specifying the device's desired directionality (i.e. a=inactive/sendonly/recvonly/sendrecv) as described in RFC 3264 for all media streams listed in an SDP offer or answer that is generated by the device.

37**Media Capability Negotiation**

Any device that originates and/or terminates RTP traffic **MUST** support the ability to receive SDP session descriptions that have the 'c=' field set to all zeros (0.0.0.0).



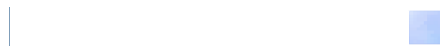
38**Codec Support and Media Transport**

Voice samples **MUST** be transported using the real-time transport protocol (RTP) as described in RFC 3550.



39**Codec Support and Media Transport**

Any device that originates and/or terminates RTP traffic over UDP **MUST** use the same UDP port for sending and receiving session media (i.e. symmetric RTP.)



40**Codec Support and Media Transport**

Any device that originates and/or terminates RTP traffic **SHOULD** be capable of processing RTP packets with different packetization rate than the one used for sending.



41**Codec Support and Media Transport**


Any device that originates and/or terminates voice traffic **MUST** minimally support the ITU-T G.711 u-Law and G.711 A-Law PCM codecs with a packetization rate of 20 ms.



42

Codec Support and Media Transport


Any device that originates and/or terminates voice traffic **MUST** support the ability to convert between G.711 A-Law to G.711 u-Law (by the u-Law end).



43

Transport of DTMF Tones


Trunking Gateways **MUST** support the ability to transport DTMF tones in-band when using the G.711 codec. Trunking Gateways **MUST** also support the ability to transport DTMF tones using the RTP telephone-event payload format as described in RFC 2833 when using any codec.



44

Transport of DTMF Tones


Any Enterprise device that originates and/or terminates voice traffic **MUST** support at least one of the above two methods for transporting DTMF tones (with RFC 2833 DTMF Relay being the preferred method).



45

15.4 Echo Cancellation

Any device that originates and/or terminates voice traffic **MUST** provide ITU-T G.168 compliant echo cancellation.



46

15.4 Echo Cancellation

Any device that supports fax and/or modem transmissions MUST recognize in-band 2100 Hz tones (+/- 15 Hz) in conjunction with phase reversals at 450 ms intervals (+/- 25 ms). Upon detection of this tone, echo cancellation MUST be disabled and remain disabled for the duration of the call or until one of the following events occurs:

1. No single-frequency sinusoid is present as defined in Section 7 of G.168.
2. The end of the call is detected.
3. The end of data transmission is detected by the lack of modem or fax tones on the channel.



47

Fax and Modem Calls

When performing in-band transport of fax or modem calls, any device that supports fax and/or modem transmissions MUST upon recognition of a 2100 Hz tone (+/- 15 Hz) tone:

1. Switch the active codec in use on the call to G.711 (if a codec other than G.711 was previously in use).
2. Disable the high pass filter.
3. Disable voice activity detection (VAD) and comfort noise generation (CNG).
4. Switch from any adaptive/dynamic jitter buffer in use to a fixed-length jitter buffer. (A RECOMMENDED depth of 200-ms is suggested when switching to a fixed-length jitter buffer.)



48

Fax and Modem Calls

Renegotiation of the session media attributes MUST be performed using the SIP reINVITE request as described in RFC 3261 or the SIP UPDATE request as described in RFC 3311



49

Fax and Modem Calls

Superior performance of fax transmissions over packet networks can be achieved by utilizing the ITU-T T.38 [22] fax relay specification (as opposed to in-band transport). In-band fax transmissions are especially problematic over packet networks, especially for calls that traverse the public Internet or other network that doesn't offer adequate QOS. Accordingly, it is RECOMMENDED that Enterprise devices utilize T.38 fax relay when possible.

Trunking Gateways MUST support the ITU-T T.38 specification and Enterprise devices SHOULD support the specification

Survey Page 11

SIPconnect Compliance Survey

CALL PROGRESS TONES

50

Call Progress Tones

PBX systems MUST locally generate call progress tones in response to the following subset of standard SIP response codes. Selection of the particular tone is left to the equipment manufacturer's discretion.

SIP Response Code
180 Ringing
400 Bad Request
403 Forbidden
404 Not Found
408 Request Timeout
480 Temporarily Unavailable
482 Loop Detected
483 Too Many Hops
486 Busy Here
500 Server Internal Error
503 Service Unavailable
504 Server Time-out
600 Busy Everywhere
604 Does Not Exist Anywhere



51

Call Progress Tones

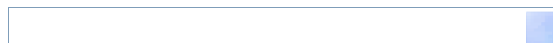
In addition to the response codes outlined above, PBX systems SHOULD generate some form of call progress tone for the remaining set of standard SIP response codes (where a call progress tone is applicable). Selection of the particular tone is left to the equipment manufacturer's discretion.



52

Early Media

In order to support delivery of in-band announcements and call progress tones, upon receipt of SDP information in any '183 Session Progress', '200 OK', or '202 Accepted' message the PBX MUST immediately disable any locally generated call progress tones and cut-through the early media to the end-user as described in RFC 3261.



53

Early Media

After sending an SDP offer, the IP PBX MUST be prepared to receive media on all offered "recvonly" or "sendrecv" transport protocol / transport port / codec (media stream) combinations. Upon receipt of

media on any such media stream, the PBX MUST immediately disable any locally generated call progress tones and cut-through the early media to the end-user as described in RFC 3261.

Survey Page 12
