

Technical Working Group
Recommendation Draft

A. Johnston
A. Siddiqui
Avaya
June 2008

Document: sf-draft-johnston-twg-sipconnect11-00
Expires: December 2008

SIPconnect 1.1 Recommendation

Status of this Memo

By submitting this Working Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with current SIP Forum Recommendations (or Working Drafts) dealing with IPR [sf-draft-admin-batson].

The SIP Forum takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the SIP Forum's procedures with respect to rights in SIP Forum Recommendations, both drafts and final versions, or other similar documentation can be found in the SIP Forum's current adopted intellectual property right Recommendation. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the SIP Forum.

This Recommendation-Draft will expire in December, 2008.

Abstract

SIPconnect 1.0 was published in January 2008 and has been widely adopted for IP PBX/Service Provider interoperability. This draft is a proposed extension to this specification. Specifically, this specification adds connected identity, media security, and presence exchange to SIPconnect, and defines a new mode of operation where interconnection is between two enterprises instead of between an enterprise and a service provider.

Table of Contents

Status of this Memo	1
Abstract	1
Overview	2
Changes to SIPconnect 1.0	2
Identity and From URI Changes	2
Limitations on use of From and P-Asserted-Identity	3
Connected Identity Support	3
Enterprise to Enterprise Mode	3
Reference Updates	3
Media Security	3
Presence Exchange	4
Instant Messaging	6
Acknowledgements	6
Informational References	8
Contributors	8

Overview

This recommendation is an extension to the SIP Forum SIPconnect 1.0 specification which was approved in January 2008. This recommendation adds media security and presence exchange to the specification in addition to making a number of small changes to the original specification including adding support for connected identity. For media security, the use of Secure RTP (SRTP) is specified. For presence exchange, the use of SIP Events (SUBSCRIBE/NOTIFY) and the Presence Information Data Format (PIDF) is specified.

Changes to SIPconnect 1.0

This recommendation follows all the recommendations of [SIPconnect 1.0] with the exceptions of the areas listed in this section.

Identity and From URI Changes

This recommendation makes a number of changes to identity and From header field handling.

Limitations on use of From and P-Asserted-Identity

SIPconnect 1.0 allows two options for From header field handling. Option 1 in 12.1.1 allows the usage of a P-Asserted-Identity header field which may not match the From header field. Option 2 uses only the From header field. This recommendation only allows the usage of Option 1 (12.1.1) when it is known the other party only supports SIPconnect 1.0. If both sides support this recommendation, Option 2 **MUST** be used.

Connected Identity Support

This recommendation supports connected identity [RFC 4916]. This allows the changing of a From URI during a SIP dialog. This is useful during redirection, forwarding, and transfer scenarios where the identity of the endpoint changes during a dialog. The UPDATE method [RFC 3311] is used to convey the new identity. All dialog-stateful elements **MUST** support RFC 4916.

Enterprise to Enterprise Mode

This recommendation allows for the usage of the interface between two enterprises instead of exclusively between an enterprise and a service provider. This is in keeping with the fact that non-SIP trunking is often done within and between enterprises in addition to between a service provider and the enterprise. Implementing this is not difficult, but it does require that the enterprise support of the service provider mandatory elements of [SIPconnect 1.0]. In addition, there needs to be a provisioning mechanism between the enterprises for routing and policy. Note that the presence and instant messaging extensions defined in this recommendation fit naturally into this enterprise to enterprise mode.

Reference Updates

The references for the following protocols should be updated: TLS [RFC 4346], SDP [RFC 4566], telephone events [RFC 4733], and STUN [draft-ietf-behave-rfc3489bis],

Media Security

The security of phone calls in the PSTN is typically provided by physical security. That is, an attacker needs to be physically present to the physical connection. With VoIP, the communication needs better protection from eavesdroppers.

SIPconnect 1.0 recommended encryption of the SIP signaling path using TLS. This specification recommends encryption of the RTP media path using SRTP. This provides

confidentiality, message authentication, and replay protection security services for both RTP and RTCP.

Enterprises and Service Providers SHOULD support [RFC 3711] for Secure RTP (SRTP). While a number of methods of keying SRTP are available, the minimum is to support SDP Security Descriptions [RFC 4568]. If RFC 4568 is used, TLS transport for SIP MUST be used to provide confidentiality for the key. Other key management approaches MAY be used if agreed upon between the Enterprise and the Service Provider. Future specifications may allow other key management protocols for SRTP.

Enterprises and Service providers supporting secure media MUST support crypto suite AES_CM_128_HMAC_SHA1_32 and MAY support AES_CM_128_HMAC_SHA1_80.

SRTP MUST only be used if it is known by provisioning that the other side supports it. In this case, the Secure RTP Audio/Video profile MUST be used. Alternatively, an approach such as SDP Capability Negotiation [draft-ietf-mmusic-sdp-capability-negotiation] can be used without this a priori knowledge.

An example call flow and SDP offer/answer is shown in Figure 1.

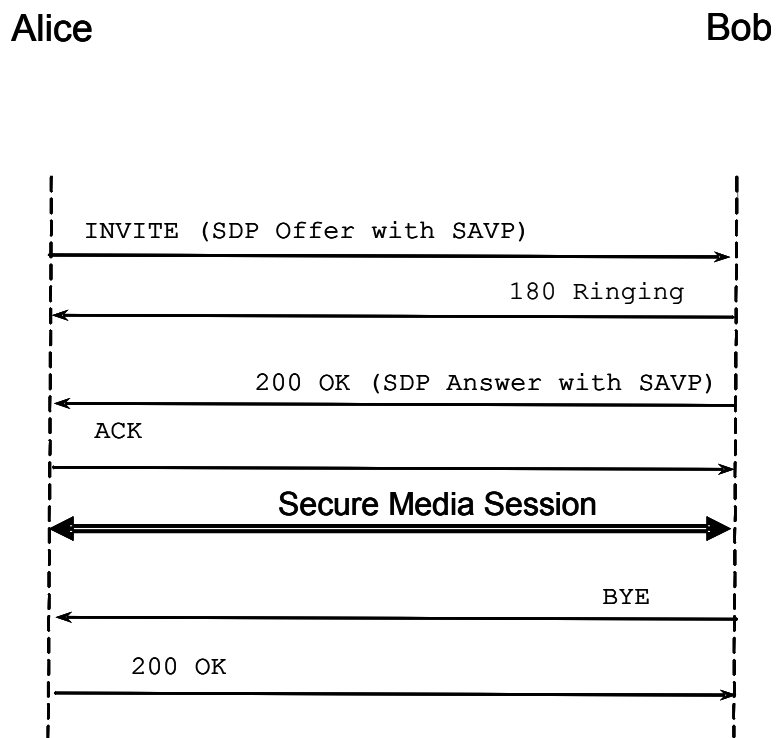


Figure 1. Secure Media Call Flow

Presence Exchange

The exchange of presence information between domains is becoming increasingly important. The set of SIP extensions for presence and instant messaging known as SIMPLE provides this capability.

The use of the SIP Events framework [RFC 3265] provides the basis, and the use of SUBSCRIBE/NOTIFY methods. Enterprises MAY support RFC 3265 and Service Providers MUST be able to proxy it. Presence is conveyed using the Presence Information Data Format (PIDF) [RFC 3863]. The basic call flow is shown below:

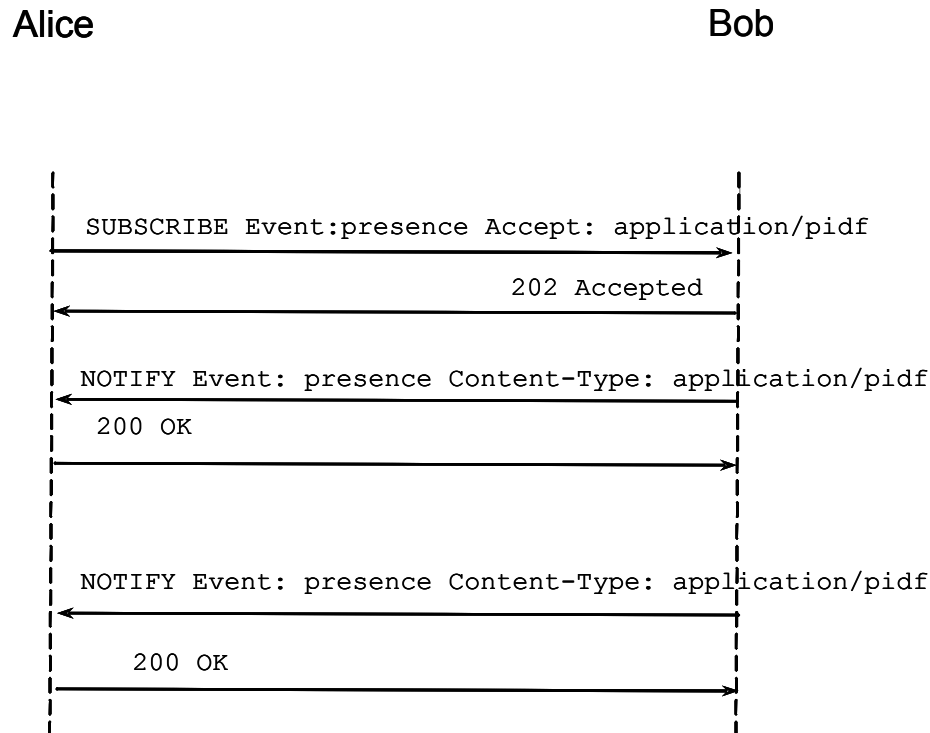


Figure 2. Presence Exchange Call Flow

Enterprises and Service Providers must support all subscription states as conveyed in a Subscription-State header field including: active, pending, terminated, and waiting.

Normal presence URI resolution would utilize DNS per [RFC 3263]. However, it is possible to be configured into a federation/clearing house architecture. In this case, presence requests between enterprises would be routed through a 3rd party such as a service provider.

The use of the Presence URI scheme [RFC 3859] is not currently supported.

The PUBLISH method [RFC 3903] is currently not supported.

Note that many other SIMPLE presence extensions may be supported within a domain such as resource lists [RFC 4662], watcher info, XCAP, etc. Support for some of these may be added in future SIP connect recommendations.

Instant Messaging

This recommendation allows for optional support of instant messaging. The supported method is the MESSAGE [RFC 3428] method which can be negotiated using the standard SIP mechanisms such as the Allow header field and 405 “Method Not Allowed” response code.

Content-Types of text/plain and application/html should be supported.

An example call flow is shown in Figure 3.

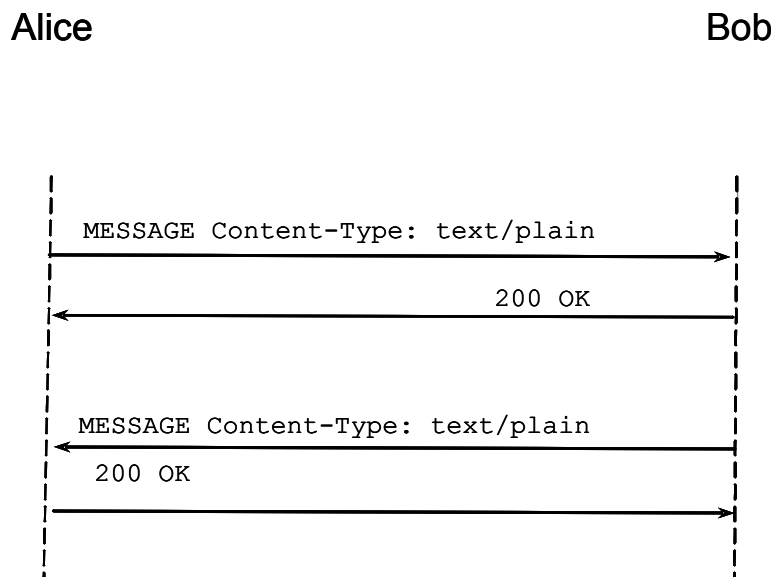


Figure 3. SIP Instant Messaging Exchange

Future recommendations may add support for other instant messaging protocols to be negotiated using SIP.

Acknowledgements

Thanks to Amit Agarwal, Mahalingam Mani, and Benny Rodrig for their comments.

Normative References

1. sf-draft-admin-batson-iprpolicy: "SIP Forum Patent-Related IPR Policy," J. Batson, January 2006
2. SIPconnect 1.0: "SIPconnect 1.0 Technical Recommendation ," C. Sibley and C.Gatch, SIP Forum Recommendation, January 2008
3. RFC 4916: "Connected Identity in the Session Initiation Protocol (SIP)," J. Elwell, IETF, June 2007
4. RFC 3311: "The Session Initiation Protocol (SIP) UPDATE Method," J. Rosenberg, IETF, September 2002
5. RFC 4346: "The Transport Layer Security Protocol Version 1.1," T. Dierks & E. Rescorla, IETF, April 2006.
6. RFC 4733: "RTP Payload for DTMF Digits, Telephony Tones, and Telephone Signals," H. Schulzrinne & T. Taylor, IETF, December 2006.
7. RFC 4566: "SDP: Session Description Protocol," M. Handley et al, IETF, July 2006.
8. draft-ietf-behave-rfc3489bis:"Session Traversal Utilities for NAT (STUN)," J. Rosenberg et al, IETF Internet-Draft, February 2008
9. RFC 3711: "The Secure Real-time Transport Protocol (SRTP)," M. Baugher et al, IETF, March 2004
10. RFC 4568: "Session Description Protocol (SDP) Security Descriptions for Media Streams," F. Andreassen et al, IETF, July 2006
11. RFC 3265: "Session Initiation Protocol (SIP) – Specific Event Notification, A. Roach, IETF, June 2002
12. RFC 3428: "Session Initiation Protocol (SIP) Extension for Instant Messaging," B. Campbell et al, IETF, December 2002
13. RFC 3863: "Presence Information Data Format (PIDF)," H. Sugano, et al, IETF, August 2004
14. RFC 3856: "A Presence Event Package for the Session Initiation Protocol (SIP)," J. Rosenberg, IETF, August 2004
15. RFC 3263: "Session Initiation Protocol (SIP): Locating SIP Servers," J. Rosenberg & H. Schulzrinne, IETF, June 2002

Informational References

16. draft-ietf-mmusic-sdp-capability-negotiation: "SDP Capability Negotiation," F. Andreason, IETF Internet-Draft, December 2007.
17. RFC 4662: "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists," A. Roach, et al, IETF, August 2006
18. RFC 3858: "An Extensible Markup Language (XML) Based Format for Watcher Information," J. Rosenberg, et al, IETF, August 2004
19. RFC 3857: "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)," J. Rosenberg, IETF, August 2004.
20. RFC 3903: "Session Initiation Protocol (SIP) Extension for Event State Publication," A. Niemi, IETF, October 2004
21. RFC 3859: "Common Profile for Presence (CPP)," J. Peterson, IETF, August 2004

Contributors

Alan Johnston
Avaya, Inc.
abjohnston@avaya.com

Anwar Siddiqui
Avaya, Inc.
anwars@avaya.com