SPEERMINT Working Group	J-F. Mule	
Internet-Draft	CableLabs	
Intended status: Informational	October 25, 2010	
Expires: April 28, 2011		

TOC

Requirements for SIP-based Session Peering
draft-ietf-speermint-requirements-10.txt

Abstract

This memo captures protocol requirements to enable session peering of voice, presence, instant messaging and other types of multimedia traffic. This informational document is intended to link the various use cases described for session peering to protocol solutions.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress.”
This Internet-Draft will expire on April 28, 2011.

Table of Contents

---

1. Introduction

TOC

Peering at the session level represents an agreement between parties to exchange multimedia traffic. In this document, we assume that the Session Initiation Protocol (SIP) is used to establish sessions between SIP Service Providers (SSPs). SIP Service Providers are referred to as peers and they are typically represented by users, user groups, enterprises, real-time collaboration service communities, or other service providers offering voice or multimedia services using SIP. A number of documents have been developed to provide background information about SIP session peering. It is expected that the reader is familiar with the reference architecture described in [I-D.ietf-speermint-architecture] (Malas, D. and J. Livingood, “SPEERMINT Peering Architecture,” October 2010.), use cases for voice ([I-D.ietf-speermint-voip-consolidated-usecases] (Uzelac, A. and Y. Lee, “VoIP SIP Peering Use Cases,” April 2010.)) and instant messaging

and presence ([RFC5344] (Houri, A., Aoki, E., and S. Parameswar, “Presence and Instant Messaging Peering Use Cases,” October 2008.)).
Peering at the session layer can be achieved on a bilateral basis (direct peering established directly between two SSPs), or on an indirect basis via a session intermediary (indirect peering via a third-party SSP that has a trust relationship with the SSPs) - see the terminology document for more details.
This document first describes general requirements. The use cases are then analyzed in the spirit of extracting relevant protocol requirements that must be met to accomplish the use cases. These requirements are intended to be independent of the type of media exchanged such as Voice over IP (VoIP), video telephony, and instant messaging. Requirements specific to presence and instant messaging are defined in Section 4 (Requirements for Session Peering of Presence and Instant Messaging).
It is not the goal of this document to mandate any particular use of IETF protocols other than SIP by SIP Service Providers in order to establish session peering. Instead, the document highlights what requirements should be met and what protocols might be used to define the solution space.
Finally, we conclude with a list of parameters for the definition of a session peering policy, provided in an informative appendix. It should be considered as an example of the information SIP Service Providers may have to discuss or agree on to exchange SIP traffic.

---

2. Terminology

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).
This document also reuses the terminology defined in [RFC5486] (Malas, D. and D. Meyer, “Session Peering for Multimedia Interconnect (SPEERMINT) Terminology,” March 2009.). It is assumed that the reader is familiar with the Session Description Protocol (SDP) [RFC4566] (Handley, M., Jacobson, V., and C. Perkins, “SDP: Session Description Protocol,” July 2006.) and the Session Initiation Protocol (SIP) [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.). Finally, when used with capital letters, the terms 'Authentication Service' are to be understood as defined by SIP Identity [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.).

3. General Requirements

TOC

The following sub-sections contain general requirements applicable to multiple use cases for multimedia session peering.

3.1. Scope

TOC

The primary focus of this document is on the requirements applicable to the boundaries of Layer 5 SIP networks: SIP entities, Signaling path Border Elements (SBEs), and the associated protocol requirements for the look-up and location routing of the session establishment data. The requirements applicable to SIP User Agents or related to the provisioning of the session data are considered out of scope.
SIP Service Providers have to reach an agreement on numerous points when establishing session peering relationships .
This document highlights only certain aspects of a session peering agreement, mostly the requirements relevant to protocols: the declaration, advertisement and management of ingress and egress border elements for session signaling and media, information related to the Session Establishment Data (SED), and the security properties that may be desirable for secure session exchanges.
Numerous other considerations of session peering arrangements are critical to reach a successful agreement but they are considered out of scope of this document. They include information about SIP protocol support (e.g. SIP extensions and field conventions), media (e.g., type of media traffic to be exchanged, compatible media codecs and transport protocols, mechanisms to ensure differentiated quality of service for media), layer-3 IP connectivity between the Signaling and Data path Border Elements, accounting and traffic capacity control (e.g. the maximum number of SIP sessions at each ingress point, or the maximum number of concurrent IM or VoIP sessions).
The informative Appendix A (Policy Parameters for Session Peering) lists parameters that may be considered when discussing the technical parameters of SIP session peering. The purpose of this list is to capture the parameters that are considered outside the scope of the protocol requirements.

3.2. Border Elements

TOC

For border elements to be operationally manageable, maximum flexibility should be given for how they are declared or dynamically advertised. Indeed, in any session peering environment, there is a need for a SIP

Service Provider to declare or dynamically advertise the SIP entities that will face the peer's network. The data path border elements are typically signaled dynamically in the session description.
The use cases defined in [I-D.ietf-speermint-voip-consolidated-usecases] (Uzelac, A. and Y. Lee, "VoIP SIP Peering Use Cases," April 2010.) catalog the various border elements between SIP Service Providers; they include Signaling path Border Elements (SBEs) and SIP proxies (or any SIP entity at the boundary of the Layer 5 network).

*Requirement #1:
Protocol mechanisms MUST be provided to enable a SIP Service Provider to communicate the ingress Signaling Path Border Elements of its service domain.

Notes on solution space:
The SBEs may be advertised to session peers using static mechanisms or they may be dynamically advertised. There is general agreement that [RFC3263] (Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers," June 2002.) provides a solution for dynamically advertising ingress SBEs in most cases of Direct or Indirect peering. We discussed the DNS-based solution space further in Requirement #4 below, especially in cases where the DNS response varies based on who sends the query (peer-dependent SBEs).

*Requirement #2:
Protocol mechanisms MUST be provided to enable a SIP Service Provider to communicate the egress SBEs of its service domain.

Notes on motivations for this requirement:
For the purposes of capacity planning, traffic engineering and call admission control, a SIP Service Provider may be asked where it will generate SIP calls from. The SSP accepting calls from a peer may wish to know where SIP calls will originate from (this information is typically used by the terminating SSP).
While provisioning requirements are out-of-scope, some SSPs may find use for a mechanism to dynamically advertise or discover the egress SBEs of a peer.

If the SSP also provides media streams to its users as shown in the use cases for "Originating" and "Terminating" SSPs, a mechanism must exist to allow SSPs to advertise their egress and ingress data path border elements (DBEs), if applicable. While some SSPs may have open policies and accept media traffic from anywhere outside their network to anywhere inside their network, some SSPs may want to optimize media

delivery and identify media paths between peers prior to traffic being sent (layer 5 to layer 3 QoS mapping).

*Requirement #3:
Protocol mechanisms MUST be provided to allow a SIP Service Provider to communicate its DBEs to its peers.

Notes: Some SSPs engaged in SIP interconnects do exchange this type of DBE information in a static manner. Some SSPs do not.

In some SIP networks, SSPs may expose the same border elements to all peers. In other environments, it is common for SSPs to advertise specific SBEs and DBEs to certain peers. This is done by SSPs to meet specific objectives for a given peer: routing optimization of the signaling and media exchanges, optimization of the latency or throughput based on the 'best' SBE and DBE combination, and other service provider policy parameters. These are some of the reasons why advertisement of SBEs and DBEs may be peer-dependent.

*Requirement #4:
The mechanisms recommended for the declaration or advertisement of SBE and DBE entities MUST allow for peer variability.

Notes on solution space:
A simple solution is to advertise SBE entities using DNS and [RFC3263] (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.) by providing different DNS names to different peers. This approach has some practical limitations because the SIP URIs containing the DNS names used to resolve the SBEs may be propagated by users, for example in the form of sip:user@domain. It is impractical to ask users to use different target URIs based upon their SIP service provider's desire to receive incoming session signaling at different ingress SBEs based upon the originator. The solution described in [RFC3263] (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.) and based on DNS to advertise SBEs is therefore under-specified for this requirement.
Other DNS mechanisms have been used extensively in other areas of the Internet, in particular in Content Distribution Internetworking to make the DNS responses vary based on the originator of the DNS query (see [RFC3466] (Day, M., Cain, B., Tomlinson, G., and P. Rzewski, “A Model for Content Internetworking (CDI),” February 2003.), [RFC3568] (Barbir, A., Cain, B., Nair, R., and O. Spatscheck, “Known Content Network (CN) Request-Routing Mechanisms,” July 2003.) and [RFC3570] (Rzewski, P., Day, M., and D. Gilletti, “Content Internetworking (CDI) Scenarios,” July 2003.)). The applicability of such solutions needs for session peering needs further analysis.

Finally, other techniques such as Anycast services ([RFC4786] (Abley, J. and K. Lindqvist, “Operation of Anycast Services,” December 2006.)) may be employed at lower layers than Layer 5 to provide a solution to this requirement. For example, anycast nodes could be defined by SIP service providers to expose a common address for SBEs into DNS, allowing the resolution of the anycast node address to the appropriate peer-dependent service address based on the routing topology or other criteria gathered from the combined use of anycast and DNS techniques.

Notes on variability of the SBE advertisements based on the media capabilities:
Some SSPs may have some restrictions on the type of media traffic their SBEs can accept. For SIP sessions however, it is not possible to communicate those restrictions in advance of the session initiation: a SIP target may support voice-only media, voice and video, or voice and instant messaging communications. While the inability to find out whether a particular type of SIP session can be terminated by a certain SBE can cause failed session establishment attempts, there is consensus to not add a new requirement in this document. These aspects are essentially covered by SSPs when discussing traffic exchange policies and are deemed out of scope of this document.

In the use cases provided as part of direct and indirect peering scenarios, an SSP deals with multiple SIP entities and multiple SBEs in its own domain. There is often a many-to-many relationship between the SIP Proxies considered inside the trusted network boundary of the SSP and its Signaling path Border Elements at the network boundaries.
It should be possible for an SSP to define which egress SBE a SIP entity must use based on a given peer destination.
For example, in the case of an indirect peering scenario (section 5. of [I-D.ietf-speermint-voip-consolidated-usecases] (Uzelac, A. and Y. Lee, “VoIP SIP Peering Use Cases,” April 2010.)), it should be possible for the SIP proxy in the originating network (O-Proxy) to select the appropriate egress SBE (O-SBE) to reach the SIP target based on the information the proxy receives from the Lookup Function (O-LUF) and/or Location Routing Function (O-LRF) - message response labeled (2). Note that this example also applies to the case of Direct Peering when a service provider has multiple service areas and each service area involves multiple SIP Proxies and a few SBEs.

*Requirement #5:
The mechanisms recommended for the Look-Up Function (LUF) and the Location Routing Functions (LRF) MUST be capable of returning both a target URI destination and a value providing the next SIP hop(s).

Notes: solutions may exist depending on the choice of the

protocol used between the Proxy and its LUF/LRF. The idea is for the O-Proxy to be provided with the next SIP hop and the equivalent of one or more SIP Route header values. If ENUM is used as a protocol for the LUF, the solution space is undefined.

It is desirable for an SSP to be able to communicate how authentication of a peer's SBEs will occur (see the security requirements for more details).

*Requirement #6:
The mechanisms recommended for locating a peer's SBE MUST be able to convey how a peer should initiate secure session establishment.

Notes: some mechanisms exist. For example, the required protocol use of SIP over TLS may be discovered via [RFC3263] (Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers," June 2002.) and guidelines concerning the use of the SIPS URI scheme in SIP have been documented in [RFC5630] (Audet, F., "The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)," October 2009.).

3.3. Session Establishment Data

TOC

The Session Establishment Data (SED) is defined in [RFC5486] (Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology," March 2009.) as the data used to route a call to the next hop associated with the called domain's ingress point. The following paragraphs capture some general requirements on the SED data.

3.3.1. User Identities and SIP URIs

TOC

User identities used between peers can be represented in many different formats. Session Establishment Data should rely on URIs (Uniform Resource Identifiers, [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.)) and SIP URIs should be preferred over tel URIs ([RFC3966] (Schulzrinne, H., "The tel URI for Telephone Numbers," December 2004.)) for session peering of VoIP traffic.
The use of DNS domain names and hostnames is recommended in SIP URIs and they should be resolvable on the public Internet. As for the user part of the SIP URIs, the mechanisms for session peering should not

require an SSP to be aware of which individual user identities are valid within its peer's domain.

*Requirement #7:
The protocols used for session peering MUST accommodate the use of different types of URIs. URIs with the same domain-part SHOULD share the same set of peering policies, thus the domain of the SIP URI may be used as the primary key to any information regarding the reachability of that SIP URI. The host part of SIP URIs SHOULD contain a fully-qualified domain name instead of a numeric IPv4 or IPv6 address.

*Requirement #8:
The mechanisms for session peering should not require an SSP to be aware of which individual user identities are valid within its peer's domain.

*Notes on the solution space for #7 and #8:
This is generally well supported by IETF protocols. When telephone numbers are in tel URIs, SIP requests cannot be routed in accordance with the traditional DNS resolution procedures standardized for SIP as indicated in [RFC3824] (Peterson, J., Liu, H., Yu, J., and B. Campbell, "Using E.164 numbers with the Session Initiation Protocol (SIP)," June 2004.). This means that the solutions built for session peering must not solely use PSTN identifiers such as Service Provider IDs (SPIDs) or Trunk Group IDs (they should not be precluded but solutions should not be limited to these).
Motivations:
Although SED data may be based on E.164-based SIP URIs for voice interconnects, a generic peering methodology should not rely on such E.164 numbers.

3.3.2. URI Reachability

TOC

Based on a well-known URI type (for e.g. sip:, pres:, or im: URIs), it must be possible to determine whether the SSP domain servicing the URI allows for session peering, and if it does, it should be possible to locate and retrieve the domain's policy and SBE entities.
For example, an originating service provider must be able to determine whether a SIP URI is open for direct interconnection without requiring an SBE to initiate a SIP request. Furthermore, since each call setup implies the execution of any proposed algorithm, the establishment of a

SIP session via peering should incur minimal overhead and delay, and employ caching wherever possible to avoid extra protocol round trips.

*Requirement #9:
The mechanisms for session peering MUST allow an SBE to locate its peer SBE given a URI type and the target SSP domain name.

---

4. Requirements for Session Peering of Presence and Instant Messaging

TOC

This section describes requirements for presence and instant messaging session peering.
Two SSPs create a peering relationship to enable their IM and presence users to collaborate with users on the other SSP network. We focus the requirements on inter-domain subscriptions to presence information, the exchange of messages and privacy settings and the use of standard presence document formats across domains.
Several use cases for presence and instant messaging peering are described in [RFC5344] (Houri, A., Aoki, E., and S. Parameswar, "Presence and Instant Messaging Peering Use Cases," October 2008.), a document authored by A. Houri, E. Aoki and S. Parameswar. Credits for the original content captured from these use cases into requirements in this section must go to them.

*Requirement #10:
The mechanisms recommended for the exchange of presence information between SSPs SHOULD allow a user of one presence community to send a presence subscription request to presentities served by another SSP via its local community, including subscriptions to a single presentity, a personal, public or ad-hoc group list of presentities.

Notes: see sections 2.1 and 2.2 of [RFC5344] (Houri, A., Aoki, E., and S. Parameswar, "Presence and Instant Messaging Peering Use Cases," October 2008.).

*Requirement #11:
The mechanisms recommended for Instant Messaging exchanges between SSPs SHOULD allow a user of one SSP's community to communicate with users of the other SSP community via their local community using the various methods. Note that some SSPs may exercise some control over which methods are allowed based on service policies. Such methods include sending a one-time IM message, initiating a SIP session for transporting sessions of messages, participating in n-way chats using chat rooms with users from the peer SSPs, etc.

Notes: see sections 2.4, 2.5 and 2.6 of [RFC5344] (Houri, A., Aoki, E., and S. Parameswar, "Presence and Instant Messaging Peering Use Cases," October 2008.).

*Requirement #12: Privacy Sharing

In some presence communities, users can define the list of watchers that receive presence notifications for a given presentity. Such privacy settings for watcher notifications per presentity are typically not shared across SSPs causing multiple notifications to be sent for one presentity change between SSPs. The sharing of those privacy settings per presentity between SSPs would allow fewer notifications: a single notification would be sent per presentity and the terminating SSP would send notifications to the appropriate watchers according to the presentity's privacy information.

The mechanisms recommended for Presence information exchanges between SSPs SHOULD allow the sharing of some user privacy settings in order for users to convey the list of watchers that can receive notification of presence information changes on a per presentity basis.

The privacy sharing mechanism must be done with the express consent of the user whose privacy settings will be shared with the other community. Because of the privacy-sensitive information exchanged between SSPs, the protocols used for the exchange of presence information must follow the security recommendations defined in section 6 of [RFC3863] (Sugano, H., Fujimoto, S., Klyne, G., Bateman, A., Carr, W., and J. Peterson, "Presence Information Data Format (PIDF)," August 2004.).

Notes: see section 2.3 of [RFC5344] (Houri, A., Aoki, E., and S. Parameswar, "Presence and Instant Messaging Peering Use Cases," October 2008.).

*Requirement #13: Multiple Watchers

It should be possible to send a presence document with a list of watchers on the other community that should receive the presence document notification. This will enable sending less presence document notifications between the communities while avoiding the need to share privacy information of presentities from one community to the other.

The systems used to exchange presence documents between SSPs SHOULD allow a presence document to be delivered to one or more watchers.

Note: The privacy sharing mechanisms defined in Requirement #12 also apply to this requirement.

*Requirement #14: Standard PIDF Documents and Mappings

Early deployments of SIP-based presence and Instant Messaging

gateways have been done in front of legacy proprietary systems that use different naming schemes or name values for the elements and properties defined in a Presence Information Data Format (PIDF) document ([RFC3863] (Sugano, H., Fujimoto, S., Klyne, G., Bateman, A., Carr, W., and J. Peterson, “Presence Information Data Format (PIDF),” August 2004.)). For example the value "Do Not Disturb" in one presence service may be mapped to "Busy" in another system for the status element. Beyond this example of status values, it is important to ensure that the meaning of the presence information is preserved between SSPs.
The systems used to exchange presence documents between SSPs SHOULD use standard PIDF documents and translate any non-standard value of a PIDF element to a standard one.

---

5. Security Considerations

TOC

This section describes the security properties that are desirable for the protocol exchanges in scope of session peering. Three types of information flows are described in the architecture and use case documents: the acquisition of the Session Establishment Data (SED) based on a destination target via the Lookup and Location Routing Functions (LUF and LRF), the SIP signaling between SIP Service Providers, and the associated media exchanges.
This section is focused on three security services, authentication, data confidentiality and data integrity as summarized in [RFC3365] (Schiller, J., “Strong Security Requirements for Internet Engineering Task Force Standard Protocols,” August 2002.). However, this text does not specify the mandatory-to-implement security mechanisms as required by [RFC3365] (Schiller, J., “Strong Security Requirements for Internet Engineering Task Force Standard Protocols,” August 2002.); this is left for future protocol solutions that meet the requirements.
A security threat analysis provides additional guidance for session peering ([I-D.ietf-speermint-voipthreats] (Seedorf, J., Niccolini, S., Chen, E., and H. Scholz, “SPEERMINT Security Threats and Suggested Countermeasures,” September 2010.)).

5.1. Security Properties for the Acquisition of Session Establishment Data

TOC

The Look-Up Function (LUF) and Location Routing Function (LRF) are defined in [RFC5486] (Malas, D. and D. Meyer, “Session Peering for Multimedia Interconnect (SPEERMINT) Terminology,” March 2009.). They provide mechanisms for determining the SIP target address and domain

the request should be sent to, and the associated SED to route the request to that domain.

*Requirement #15:
The protocols used to query the Lookup and Location Routing Functions SHOULD support mutual authentication.

Motivations:
A mutual authentication service should be provided for the LUF and LRF protocol exchanges. The content of the response returned by the LUF and LRF may depend on the identity of the requestor: the authentication of the LUF & LRF requests is therefore a desirable property. Mutual authentication is also desirable: the requestor may verify the identity of the systems that provided the LUF & LRF responses given the nature of the data returned in those responses. Authentication also provides some protection for the availability of the LUF and LRF against attackers that would attempt to launch DoS attacks by sending bogus requests causing the LUF to perform a lookup and consume resources.

*Requirement #16:
The protocols used to query the Lookup and Location Routing Functions SHOULD provide support for data confidentiality and integrity.

Motivations:
Given the sensitive nature of the session establishment data exchanged with the LUF and LRF functions, the protocol mechanisms chosen for the lookup and location routing should offer data confidentiality and integrity protection (SED data may contain user addresses, SIP URI, location of SIP entities at the boundaries of SIP Service Provider domains, etc.).

*Notes on the solution space for Requirements #15 and #16: ENUM, SIP and proprietary protocols are typically used today for accessing these functions. Even though SSPs may use lower layer security mechanisms to guarantee some of those security properties, candidate protocols for the LUF and LRF should meet the above requirements.

5.2. Security Properties for the SIP signaling exchanges

TOC

The SIP signaling exchanges are out of scope of this document. This section describes some of the security properties that are desirable in the context of SIP interconnects between SSPs without formulating any normative requirements.

In general, the security properties desirable for the SIP exchanges in an inter-domain context apply to session peering. These include:

- securing the transport of SIP messages between the peers' SBEs. Authentication of SIP communications is desirable, especially in the context of session peering involving SIP intermediaries. Data confidentiality and integrity of the SIP message body may be desirable as well given some of the levels of session peering indirection (indirect/assisted peering), but they could be harmful as they may prevent intermediary SSPs from "inserting" SBEs/DBEs along the signaling and data paths.

- providing an Authentication Service to authenticate the identity of connected users based on the SIP Service Provider domains (for both the SIP requests and the responses).

The fundamental mechanisms for securing SIP between proxy servers intra- and inter-domain are applicable to session peering; refer to Section 26.2 of [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.) for transport-layer security of SIP messages using TLS, [RFC5923] (Gurbani, V., Mahy, R., and B. Tate, “Connection Reuse in the Session Initiation Protocol (SIP),” June 2010.) for establishing TLS connections between proxies, [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.) for the protocol mechanisms to verify the identity of the senders of SIP requests in an inter-domain context, and [RFC4916] (Elwell, J., “Connected Identity in the Session Initiation Protocol (SIP),” June 2007.) for verifying the identity of the sender of SIP responses).

5.3. End-to-End Media Security

TOC

Media security is critical to guarantee end-to-end confidentiality of the communication between the end-users' devices, independently of how many direct or indirect peers are present along the signaling path. A number of desirable security properties emerge from this goal.
The establishment of media security may be achieved along the media path and not over the signaling path given the indirect peering use cases.
For example, media carried over the Real-Time Protocol (RTP) can be secured using secure RTP (SRTP [RFC3711] (Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, “The Secure Real-time Transport Protocol (SRTP),” March 2004.)). A framework for establishing SRTP security using Datagram TLS [RFC4347] (Rescorla, E. and N. Modadugu, “Datagram Transport Layer Security,” April 2006.) is

described in [RFC5763] (Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)," May 2010.): it allows for end-to-end media security establishment using extensions to DTLS ([RFC5764] (McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)," May 2010.)).
It should also be noted that media can be carried in numerous protocols other than RTP such as SIP (SIP MESSAGE method), MSRP (the Message Session Relay Protocol, [RFC4975] (Campbell, B., Mahy, R., and C. Jennings, "The Message Session Relay Protocol (MSRP)," September 2007.), XMPP (the Extensible Messaging and Presence Protocol, [RFC3920] (Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core," October 2004.)) and many others. Media may also be carried over TCP ([RFC4571] (Lazzaro, J., "Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport," July 2006.)), and it can be encrypted over secure connection-oriented transport sessions over TLS ([RFC4572] (Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)," July 2006.)).
A desirable security property for session peering is for SIP entities to be transparent to the end-to-end media security negotiations: SIP entities should not intervene in the Session Description Protocol (SDP) exchanges for end-to-end media security.

*Requirement #17:
The protocols used to enable session peering MUST NOT interfere with the exchanges of media security attributes in SDP. Media attribute lines that are not understood by SBEs MUST be ignored and passed along the signaling path untouched.

---

6. Acknowledgments

TOC

This document is based on the input and contributions made by a large number of people including: Bernard Aboba, Edwin Aoki, Scott Brim, John Elwell, Mike Hammer, Avshalom Houri, Richard Shocky, Henry Sinnreich, Richard Stastny, Patrik Faltstrom, Otmar Lendl, Daryl Malas, Dave Meyer, Sriram Parameswar, Jon Peterson, Jason Livingood, Bob Natale, Benny Rodrig, Brian Rosen, Eric Rosenfeld, Peter Saint-Andre, David Schwartz and Adam Uzelac.
Specials thanks go to Rohan Mahy, Brian Rosen, John Elwell for their initial drafts describing guidelines or best current practices in various environments, to Avshalom Houri, Edwin Aoki and Sriram

Parameswar for authoring the presence and instant messaging requirements and to Dan Wing for providing detailed feedback on the security consideration sections.

7. IANA Considerations

TOC

This document does not register any values in IANA registries.

8. References

TOC

8.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

8.2. Informative References

TOC

[I-D.ietf-pmol-sip-perf-metrics]	Malas, D. and A. Morton, “Basic Telephony SIP End-to-End Performance Metrics,” draft-ietf-pmol-sip-perf-metrics-07 (work in progress), September 2010 (TXT).
[I-D.ietf-speermint-architecture]	Malas, D. and J. Livingood, “SPEERMINT Peering Architecture,” draft-ietf-speermint-architecture-12 (work in progress), October 2010 (TXT).
[I-D.ietf-speermint-voip-consolidated-usecases]	Uzelac, A. and Y. Lee, “VoIP SIP Peering Use Cases,” draft-ietf-speermint-voip-consolidated-usecases-18 (work in progress), April 2010 (TXT).
[I-D.ietf-speermint-voipthreats]	Seedorf, J., Niccolini, S., Chen, E., and H. Scholz, “SPEERMINT Security Threats and Suggested Countermeasures,” draft-ietf-speermint-voipthreats-05 (work in progress), September 2010 (TXT).
[RFC2198]	Perkins, C., Kouvelas, I., Hodson, O., Hardman, V., Handley, M., Bolot, J., Vega-Garcia, A., and S. Fosse-Parisis, “RTP Payload for Redundant Audio Data,” RFC 2198, September 1997 (TXT, HTML, XML).
[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” RFC 3261, June 2002 (TXT).
[RFC3263]	Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” RFC 3263, June 2002 (TXT).
[RFC3365]	Schiller, J., “Strong Security Requirements for Internet Engineering Task Force Standard Protocols,” BCP 61, RFC 3365, August 2002 (TXT).
[RFC3455]	Garcia-Martin, M., Henrikson, E., and D. Mills, “Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP),” RFC 3455, January 2003 (TXT).
[RFC3466]	Day, M., Cain, B., Tomlinson, G., and P. Rzewski, “A Model for Content Internetworking (CDI),” RFC 3466, February 2003 (TXT).
[RFC3550]	Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” STD 64, RFC 3550, July 2003 (TXT, PS, PDF).
[RFC3568]	

	Barbir, A., Cain, B., Nair, R., and O. Spatscheck, “Known Content Network (CN) Request-Routing Mechanisms,” RFC 3568, July 2003 (TXT).
[RFC3570]	Rzewski, P., Day, M., and D. Gilletti, “Content Internetworking (CDI) Scenarios,” RFC 3570, July 2003 (TXT).
[RFC3611]	Friedman, T., Caceres, R., and A. Clark, “RTP Control Protocol Extended Reports (RTCP XR),” RFC 3611, November 2003 (TXT).
[RFC3702]	Loughney, J. and G. Camarillo, “Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP),” RFC 3702, February 2004 (TXT).
[RFC3711]	Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, “The Secure Real-time Transport Protocol (SRTP),” RFC 3711, March 2004 (TXT).
[RFC3824]	Peterson, J., Liu, H., Yu, J., and B. Campbell, “Using E.164 numbers with the Session Initiation Protocol (SIP),” RFC 3824, June 2004 (TXT).
[RFC3863]	Sugano, H., Fujimoto, S., Klyne, G., Bateman, A., Carr, W., and J. Peterson, “Presence Information Data Format (PIDF),” RFC 3863, August 2004 (TXT).
[RFC3920]	Saint-Andre, P., Ed., “Extensible Messaging and Presence Protocol (XMPP): Core,” RFC 3920, October 2004 (TXT, HTML, XML).
[RFC3966]	Schulzrinne, H., “The tel URI for Telephone Numbers,” RFC 3966, December 2004 (TXT).
[RFC3986]	Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” STD 66, RFC 3986, January 2005 (TXT, HTML, XML).
[RFC4347]	Rescorla, E. and N. Modadugu, “Datagram Transport Layer Security,” RFC 4347, April 2006 (TXT).
[RFC4474]	Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” RFC 4474, August 2006 (TXT).
[RFC4566]	Handley, M., Jacobson, V., and C. Perkins, “SDP: Session Description Protocol,” RFC 4566, July 2006 (TXT).
[RFC4571]	Lazzaro, J., “Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport,” RFC 4571, July 2006 (TXT).
[RFC4572]	

	Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)," RFC 4572, July 2006 (TXT).
[RFC4786]	Abley, J. and K. Lindqvist, "Operation of Anycast Services," BCP 126, RFC 4786, December 2006 (TXT).
[RFC4916]	Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)," RFC 4916, June 2007 (TXT).
[RFC4975]	Campbell, B., Mahy, R., and C. Jennings, "The Message Session Relay Protocol (MSRP)," RFC 4975, September 2007 (TXT).
[RFC5344]	Houri, A., Aoki, E., and S. Parameswar, "Presence and Instant Messaging Peering Use Cases," RFC 5344, October 2008 (TXT).
[RFC5411]	Rosenberg, J., "A Hitchhiker's Guide to the Session Initiation Protocol (SIP)," RFC 5411, February 2009 (TXT).
[RFC5486]	Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology," RFC 5486, March 2009 (TXT).
[RFC5503]	Andreasen, F., McKibben, B., and B. Marshall, "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture," RFC 5503, March 2009 (TXT).
[RFC5630]	Audet, F., "The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)," RFC 5630, October 2009 (TXT).
[RFC5763]	Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)," RFC 5763, May 2010 (TXT).
[RFC5764]	McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)," RFC 5764, May 2010 (TXT).
[RFC5923]	Gurbani, V., Mahy, R., and B. Tate, "Connection Reuse in the Session Initiation Protocol (SIP)," RFC 5923, June 2010 (TXT).

TOC

Appendix A. Policy Parameters for Session Peering

This informative section lists various types of parameters that should be considered by implementers when deciding what configuration variables to expose to system administrators or management stations, as well as SSPs or federations of SSPs when discussing the technical part of a session peering policy.

In the context of session peering, a policy can be defined as the set of parameters and other information needed by an SSP to exchange traffic with another peer. Some of the session policy parameters may be statically exchanged and set throughout the lifetime of the peering relationship. Others parameters may be discovered and updated dynamically using by some explicit protocol mechanisms. These dynamic parameters may be session-dependent, or the may apply over multiple sessions or peers.

Various types of policy information may need to be discovered or exchanged in order to establish session peering. At a minimum, a policy should specify information related to session establishment data in order to avoid session establishment failures. A policy may also include information related to QoS, billing and accounting, layer-3 related interconnect requirements which are out of the scope of this document.

Some aspects of session peering policies must be agreed to and manually implemented; they are static and are typically documented as part of a business contract, technical document or agreement between parties. For some parameters linked to protocol support and capabilities, standard ways of expressing those policy parameters may be defined among SSP and exchanged dynamically. For e.g., templates could be created in various document formats so that it could be possible to dynamically discover some of the domain policy. Such templates could be initiated by implementers (for each software/hardware release, a list of supported RFCs, RFC parameters is provided in a standard format) and then adapted by each SSP based on its service description, server or device configurations and variable based on peer relationships.

A.1. Categories of Parameters for VoIP Session Peering and Justifications

TOC

The following list should be considered as an initial list of "discussion topics" to be addressed by peers when initiating a VoIP peering relationship.

* IP Network Connectivity:
  Session peers should define the IP network connectivity between their respective SBEs and DBEs. While this is out of scope of session peering, SSPs must agree on a common mechanism for IP

transport of session signaling and media. This may be accomplish via private (e.g. IPVPN, IPsec, etc.) or public IP networks.

*Media-related Parameters:

-Media Codecs: list of supported media codecs for audio, real-time fax (version of T.38, if applicable), real-time text (RFC 4103), DTMF transport, voice band data communications (as applicable) along with the supported or recommended codec packetization rates, level of RTP payload redundancy, audio volume levels, etc.

-Media Transport: level of support for RTP-RTCP [RFC3550] (Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," July 2003.), RTP Redundancy (RTP Payload for Redundant Audio Data - [RFC2198] (Perkins, C., Kouvelas, I., Hodson, O., Hardman, V., Handley, M., Bolot, J., Vega-Garcia, A., and S. Fosse-Parisis, "RTP Payload for Redundant Audio Data," September 1997.)) , T.38 transport over RTP, etc.

-Media variability at the Signaling path Border Elements: list of media types supported by the various ingress points of a peer's network.

-Other: support of the VoIP metric block as defined in RTP Control Protocol Extended Reports [RFC3611] (Friedman, T., Caceres, R., and A. Clark, "RTP Control Protocol Extended Reports (RTCP XR)," November 2003.) , etc.

*SIP:

-A session peering policy should include the list of supported and required SIP RFCs, supported and required SIP methods (including private p headers if applicable), error response codes, supported or recommended format of some header field values , etc.

-It should also be possible to describe the list of supported SIP RFCs by various functional groupings. A group of SIP RFCs may represent how a call feature is implemented (call hold, transfer, conferencing, etc.), or it may indicate a functional grouping as in [RFC5411] (Rosenberg, J., "A Hitchhiker's Guide to the Session Initiation Protocol (SIP)," February 2009.).

*Accounting:
Methods used for call or session accounting should be specified. An SSP may require a peer to track session usage. It is critical for peers to determine whether the support of any SIP extensions for accounting is a pre-requisite for SIP interoperability. In

some cases, call accounting may feed data for billing purposes but not always: some operators may decide to use accounting as a 'bill and keep' model to track session usage and monitor usage against service level agreements.
[RFC3702] (Loughney, J. and G. Camarillo, “Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP),” February 2004.) defines the terminology and basic requirements for accounting of SIP sessions. A few private SIP extensions have also been defined and used over the years to enable call accounting between SSP domains such as the P-Charging* headers in [RFC3455] (Garcia-Martin, M., Henrikson, E., and D. Mills, “Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP),” January 2003.), the P-DCS-Billing-Info header in [RFC5503] (Andreasen, F., McKibben, B., and B. Marshall, “Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture,” March 2009.), etc.

*Performance Metrics:
Layer-5 performance metrics should be defined and shared between peers. The performance metrics apply directly to signaling or media; they may be used pro-actively to help avoid congestion, call quality issues or call signaling failures, and as part of monitoring techniques, they can be used to evaluate the performance of peering exchanges.
Examples of SIP performance metrics include the maximum number of SIP transactions per second on per domain basis, Session Completion Rate (SCR), Session Establishment Rate (SER), etc.
Some SIP end-to-end performance metrics are defined in [I-D.ietf-pmol-sip-perf-metrics] (Malas, D. and A. Morton, “Basic Telephony SIP End-to-End Performance Metrics,” September 2010.); a subset of these may be applicable to session peering and interconnects.
Some media-related metrics for monitoring VoIP calls have been defined in the VoIP Metrics Report Block, in Section 4.7 of [RFC3611] (Friedman, T., Caceres, R., and A. Clark, “RTP Control Protocol Extended Reports (RTCP XR),” November 2003.).

*Security:
An SSP should describe the security requirements that other peers must meet in order to terminate calls to its network. While such a list of security-related policy parameters often depends on the security models pre-agreed to by peers, it is expected that these parameters will be discoverable or signaled in the future to allow session peering outside SSP clubs. The list of security parameters may be long and composed of high-level requirements (e.g. authentication, privacy, secure transport) and low level protocol configuration elements like TLS parameters.

The following list is not intended to be complete, it provides a preliminary list in the form of examples:

- Call admission requirements: for some providers, sessions can only be admitted if certain criteria are met. For example, for some providers' networks, only incoming SIP sessions signaled over established IPsec tunnels or presented to the well-known TLS ports are admitted. Other call admission requirements may be related to some performance metrics as described above. Finally, it is possible that some requirements be imposed on lower layers, but these are considered out of scope of session peering.

- Call authorization requirements and validation: the presence of a caller or user identity may be required by an SSP. Indeed, some SSPs may further authorize an incoming session request by validating the caller's identity against white/ black lists maintained by the service provider or users (traditional caller ID screening applications or IM white list).

- Privacy requirements: an SSP may demand that its SIP messages be securely transported by its peers for privacy reasons so that the calling/called party information be protected. Media sessions may also require privacy and some SSP policies may include requirements on the use of secure media transport protocols such as SRTP, along with some constraints on the minimum authentication/encryption options for use in SRTP.

- Network-layer security parameters: this covers how IPsec security associated may be established, the IPsec key exchange mechanisms to be used and any keying materials, the lifetime of timed Security Associated if applicable, etc.

- Transport-layer security parameters: this covers how TLS connections should be established as described in Section Section 5 (Security Considerations).

TOC

A.2. Summary of Parameters for Consideration in Session Peering Policies

The following is a summary of the parameters mentioned in the previous section. They may be part of a session peering policy and appear with a level of requirement (mandatory, recommended, supported, ...).

- *IP Network Connectivity (assumed, requirements out of scope of this document)

- *Media session parameters:

  - -Codecs for audio, video, real time text, instant messaging media sessions

  - -Modes of communications for audio (voice, fax, DTMF), IM (page mode, MSRP)

  - -Media transport and means to establish secure media sessions

  - -List of ingress and egress DBEs where applicable, including STUN Relay servers if present

- *SIP

  - -SIP RFCs, methods and error responses

  - -headers and header values

  - -possibly, list of SIP RFCs supported by groups (e.g. by call feature)

- *Accounting

- *Capacity Control and Performance Management: any limits on, or, means to measure and limit the maximum number of active calls to a peer or federation, maximum number of sessions and messages per specified unit time, maximum number of active users or subscribers per specified unit time, the aggregate media bandwidth per peer or for the federation, specified SIP signaling performance metrics to measure and report; media-level VoIP metrics if applicable.

- *Security: Call admission control, call authorization, network and transport layer security parameters, media security parameters

Author's Address

TOC

	Jean-Francois Mule
	CableLabs
	858 Coal Creek Circle
	Louisville, CO 80027
	USA
Email:	jf.mule@cablelabs.com