Network Working Group
Request for Comments: 5411
Category: Informational

J. Rosenberg
Cisco

January 2009

A Hitchhiker's Guide to the Session Initiation Protocol (SIP)

Status of This Memo

Abstract

The Session Initiation Protocol (SIP) is the subject of numerous specifications that have been produced by the IETF. It can be difficult to locate the right document, or even to determine the set of Request for Comments (RFC) about SIP. This specification serves as a guide to the SIP RFC series. It lists a current snapshot of the specifications under the SIP umbrella, briefly summarizes each, and groups them into categories.

Table of Contents

1. Introduction

The Session Initiation Protocol (SIP) [RFC3261] is the subject of numerous specifications that have been produced by the IETF. It can be difficult to locate the right document, or even to determine the set of Request for Comments (RFC) about SIP. "Don't Panic!" [HGTTG] This specification serves as a guide to the SIP RFC series. It is a current snapshot of the specifications under the SIP umbrella at the time of publication. It is anticipated that this document itself will be regularly updated as SIP specifications mature. Furthermore, it references many specifications, which, at the time of publication of this document, were not yet finalized, and may eventually be completed or abandoned. Therefore, the enumeration of specifications here is a work-in-progress and subject to change.

For each specification, a paragraph or so description is included that summarizes the purpose of the specification. Each specification also includes a letter that designates its category in the Standards Track [RFC2026]. These values are:

S: Standards Track (Proposed Standard, Draft Standard, or Standard)

E: Experimental

B: Best Current Practice

I: Informational

The specifications are grouped together by topic. The topics are:

Core: The SIP specifications that are expected to be utilized for each session or registration an endpoint participates in.

Public Switched Telephone Network (PSTN) Interop: Specifications related to interworking with the telephone network.

General Purpose Infrastructure: General purpose extensions to SIP, SDP (Session Description Protocol), and MIME, but ones that are not expected to always be used.

NAT Traversal: Specifications to deal with firewall and NAT traversal.

Call Control Primitives: Specifications for manipulating SIP dialogs and calls.

Event Framework: Definitions of the core specifications for the SIP event framework, providing for pub/sub capability.

Event Packages: Packages that utilize the SIP event framework.

Quality of Service: Specifications related to multimedia quality of service (QoS).

Operations and Management: Specifications related to configuration and monitoring of SIP deployments.

SIP Compression: Specifications to facilitate usage of SIP with the Signaling Compression (Sigcomp) framework.

SIP Service URIs: Specifications on how to use SIP URIs to address multimedia services.

Minor Extensions: Specifications that solve a narrow problem space or provide an optimization.

Security Mechanisms: Specifications providing security functionality for SIP.

Conferencing: Specifications for multimedia conferencing.

Instant Messaging, Presence, and Multimedia: SIP extensions related to IM, presence, and multimedia. This covers only the SIP extensions related to these topics. See [SIMPLE] for a full treatment of SIP for IM and Presence (SIMPLE).

Emergency Services: SIP extensions related to emergency services. See [ECRIT-FRAME] for a more complete treatment of additional functionality related to emergency services.

Typically, SIP extensions fit naturally into topic areas, and implementors interested in a particular topic often implement many or all of the specifications in that area. There are some specifications that fall into multiple topic areas, in which case they are listed more than once.

Do not print all the specs cited here at once, as they might share the fate of the rules of Brockian Ultracricket when bound together: collapse under their own gravity and form a black hole [HGTTG].

This document itself is not an update to RFC 3261 or an extension to SIP. It is an informational document, meant to guide newcomers, implementors, and deployers to the many specifications associated with SIP.

2. Scope of This Document

It is very difficult to enumerate the set of SIP specifications. This is because there are many protocols that are intimately related to SIP and used by nearly all SIP implementations, but are not formally SIP extensions. As such, this document formally defines a "SIP specification" as:

- RFC 3261 and any specification that defines an extension to it, where an extension is a mechanism that changes or updates in some way a behavior specified there.
- The basic SDP specification [RFC4566] and any specification that defines an extension to SDP whose primary purpose is to support SIP.
- Any specification that defines a MIME object whose primary purpose is to support SIP.

Excluded from this list are requirements, architectures, registry definitions, non-normative frameworks, and processes. Best Current Practices are included when they normatively define mechanisms for accomplishing a task, or provide significant description of the usage of the normative specifications, such as call flows.

The SIP change process [RFC3427] defines two types of extensions to SIP: normal extensions and the so-called P-headers (where P stands for "preliminary", "private", or "proprietary", and the "P-" prefix is included in the header field name), which are meant to be used in areas of limited applicability. P-headers cannot be defined in the Standards Track. For the most part, P-headers are not included in the listing here, with the exception of those that have seen general usage despite their P-header status.

This document includes specifications, which have already been approved by the IETF and granted an RFC number, in addition to Internet Drafts, which are still under development within the IETF and will eventually finish and get an RFC number. Inclusion of Internet Drafts here helps encourage early implementation and demonstrations of interoperability of the protocol, and thus aids in the standards-setting process. Inclusion of these also identifes where the IETF is targetting a solution at a particular problem space. Note that final IANA assignment of codepoints (such as option tags and header field names) does not take place until shortly before publication as an RFC, and thus codepoint assignments may change.

3. Core SIP Specifications

The core SIP specifications represent the set of specifications whose functionality is broadly applicable. An extension is broadly applicable if it fits into one of the following categories:

- For specifications that impact SIP session management, the extension would be used for almost every session initiated by a user agent.
- For specifications that impact SIP registrations, the extension would be used for almost every registration initiated by a user agent.
- For specifications that impact SIP subscriptions, the extension would be used for almost every subscription initiated by a user agent.

In other words, these are not specifications that are used just for some requests and not others; they are specifications that would apply to each and every request for which the extension is relevant. In the galaxy of SIP, these specifications are like towels [HGTTG].

RFC 3261, The Session Initiation Protocol (S): [RFC3261] is the core SIP protocol itself. RFC 3261 obsoletes [RFC2543]. It is the president of the galaxy [HGTTG] as far as the suite of SIP specifications is concerned.

RFC 3263, Locating SIP Servers (S): [RFC3263] provides DNS procedures for taking a SIP URI and determining a SIP server that is associated with that SIP URI. RFC 3263 is essential for any implementation using SIP with DNS. RFC 3263 makes use of both DNS SRV records [RFC2782] and NAPTR records [RFC3401].

RFC 3264, An Offer/Answer Model with the Session Description Protocol (S): [RFC3264] defines how the Session Description Protocol (SDP) [RFC4566] is used with SIP to negotiate the parameters of a media session. It is in widespread usage and an integral part of the behavior of RFC 3261.

RFC 3265, SIP-Specific Event Notification (S): [RFC3265] defines the SUBSCRIBE and NOTIFY methods. These two methods provide a general event notification framework for SIP. To actually use the framework, extensions need to be defined for specific event packages. An event package defines a schema for the event data and describes other aspects of event processing specific to that schema. An RFC 3265 implementation is required when any event package is used.

RFC 3325, Private Extensions to SIP for Asserted Identity within Trusted Networks (I): Though its P-header status implies that it has limited applicability, [RFC3325], which defines the P-Asserted-Identity header field, has been widely deployed. It is used as the basic mechanism for providing network-asserted caller ID services. Its intended update, [UPDATE-PAI], clarifies its usage for connected party identification as well.

RFC 3327, SIP Extension Header Field for Registering Non-Adjacent Contacts (S): [RFC3327] defines the Path header field. This field is inserted by proxies between a client and their registrar. It allows inbound requests towards that client to traverse these proxies prior to being delivered to the user agent. It is essential in any SIP deployment that has edge proxies, which are proxies between the client and the home proxy or SIP registrar.

RFC 3581, An Extension to SIP for Symmetric Response Routing (S): [RFC3581] defines the rport parameter of the Via header. It allows SIP responses to traverse NAT. It is one of several specifications that are utilized for NAT traversal (see Section 6).

RFC 3840, Indicating User Agent Capabilities in SIP (S): [RFC3840] defines a mechanism for carrying capability information about a user agent in REGISTER requests and in dialog-forming requests like INVITE. It has found use with conferencing (the isfocus parameter declares that a user agent is a conference server) and with applications like push-to-talk.

RFC 4320, Actions Addressing Issues Identified with the Non-INVITE Transaction in SIP (S): [RFC4320] formally updates RFC 3261 and modifies some of the behaviors associated with non-INVITE transactions. This addresses some problems found in timeout and failure cases.

RFC 4474, Enhancements for Authenticated Identity Management in SIP (S): [RFC4474] defines a mechanism for providing a cryptographically verifiable identity of the calling party in a SIP request. Known as "SIP Identity", this mechanism provides an alternative to RFC 3325. It has seen little deployment so far, but its importance as a key construct for anti-spam techniques and new security mechanisms makes it a core part of the SIP specifications.

GRUU, Obtaining and Using Globally Routable User Agent Identifiers (GRUU) in SIP (S): [GRUU] defines a mechanism for directing requests towards a specific UA instance. GRUU is essential for features like transfer and provides another piece of the SIP NAT traversal story.

OUTBOUND, Managing Client Initiated Connections through SIP (S): [OUTBOUND], also known as SIP outbound, defines important changes to the SIP registration mechanism that enable delivery of SIP messages towards a UA when it is behind a NAT. This specification is the cornerstone of the SIP NAT traversal strategy.

RFC 4566, Session Description Protocol (S): [RFC4566] defines a format for representing multimedia sessions. SDP objects are carried in the body of SIP messages and, based on the offer/answer model, are used to negotiate the media characteristics of a session between users.

SDP-CAP, SDP Capability Negotiation (S): [SDP-CAP] defines a set of extensions to SDP that allows for capability negotiation within SDP. Capability negotiation can be used to select between different profiles of RTP (secure vs. unsecure) or to negotiate codecs such that an agent has to select one amongst a set of supported codecs.

ICE, Interactive Connectivity Establishment (ICE) (S): [ICE] defines a technique for NAT traversal of media sessions for protocols that make use of the offer/answer model. This specification is the IETF-recommended mechanism for NAT traversal for SIP media streams, and is meant to be used even by endpoints that are themselves never behind a NAT. A SIP option tag and media feature tag [OPTION-TAG] (also a core specification) have been defined for use with ICE.

RFC 3605, Real Time Control Protocol (RTCP) Attribute in the Session Description Protocol (SDP) (S): [RFC3605] defines a way to explicitly signal, within an SDP message, the IP address and port for RTCP, rather than using the port+1 rule in the Real Time Transport Protocol (RTP) [RFC3550]. It is needed for devices behind NAT, and the specification is required by ICE.

RFC 4916, Connected Identity in the Session Initiation Protocol (SIP) (S): [RFC4916] formally updates RFC 3261. It defines an extension to SIP that allows a calling user to determine the identity of the final called user (connected party). Due to forwarding and retargeting services, this may not be the same as the user that the caller was originally trying to reach. The mechanism works in tandem with the SIP identity specification [RFC4474] to provide signatures over the connected party identity. It can also be used if a party identity changes mid-call due to third-party call control actions or PSTN behavior.

RFC 3311, The SIP UPDATE Method (S): [RFC3311] defines the UPDATE method for SIP. This method is meant as a means for updating session information prior to the completion of the initial INVITE transaction. It can also be used to update other information, such as the identity of the participant [RFC4916], without involving an updated offer/answer exchange. It was developed initially to support [RFC3312], but has found other uses. In particular, its usage with RFC 4916 means it will typically be used as part of every session, to convey a secure, connected identity.

SIPS-URI, The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP) (S): [SIPS-URI] is intended to update RFC 3261. It revises the processing of the SIPS URI, originally defined in RFC 3261, to fix many errors and problems that have been encountered with that mechanism.

RFC 3665, Session Initiation Protocol (SIP) Basic Call Flow Examples (B): [RFC3665] contains best-practice call flow examples for basic SIP interactions -- call establishment, termination, and registration.

Essential Corrections to SIP: A collection of fixes to SIP that address important bugs and vulnerabilities. These include a fix requiring loop detection in any proxy that forks [LOOP-FIX], a clarification on how record-routing works [RECORD-ROUTE], and a correction to the IPv6 BNF [ABNF-FIX].

4. Public Switched Telephone Network (PSTN) Interworking

Numerous extensions and usages of SIP are related to interoperability and communications with or through the PSTN.

RFC 2848, The PINT Service Protocol (S): [RFC2848] is one of the earliest extensions to SIP. It defines procedures for using SIP to invoke services that actually execute on the PSTN. Its main application is for third-party call control, allowing an IP host to set up a call between two PSTN endpoints. PINT (PSTN/Internet Interworking) has a relatively narrow focus and has not seen widespread deployment.

RFC 3910, The SPIRITS Protocol (S): Continuing the trend of naming PSTN-related extensions with alcohol references, SPIRITS (Services in PSTN Requesting Internet Services) [RFC3910] defines the inverse of PINT. It allows a switch in the PSTN to ask an IP element how to proceed with call waiting. It was developed primarily to support Internet Call Waiting (ICW). Perhaps the next specification will be called the Pan Galactic Gargle Blaster

[HGTTG].

RFC 3372, SIP for Telephones (SIP-T): Context and Architectures (I): SIP-T [RFC3372] defines a mechanism for using SIP between pairs of PSTN gateways. Its essential idea is to tunnel ISDN User Part (ISUP) signaling between the gateways in the body of SIP messages. SIP-T motivated the development of INFO [RFC2976]. SIP-T has seen widespread implementation for the limited deployment model that it addresses. As ISUP endpoints disappear from the network, the need for this mechanism will decrease.

RFC 3398, ISUP to SIP Mapping (S): [RFC3398] defines how to do protocol mapping from the SS7 ISDN User Part (ISUP) signaling to SIP. It is widely used in SS7 to SIP gateways and is part of the SIP-T framework.

RFC 4497, Interworking between the Session Initiation Protocol (SIP) and QSIG (B): [RFC4497] defines how to do protocol mapping from Q.SIG, used for Private Branch Exchange (PBX) signaling, to SIP.

RFC 3578, Mapping of ISUP Overlap Signaling to SIP (S): [RFC3578] defines a mechanism to map overlap dialing into SIP. This specification is widely regarded as the ugliest SIP specification, as the introduction to the specification itself advises that it has many problems. Overlap signaling (the practice of sending digits into the network as dialed instead of waiting for complete collection of the called party number) is largely incompatible with SIP at some fairly fundamental levels. That said, RFC 3578 is mostly harmless and has seen some usage.

RFC 3960, Early Media and Ringtone Generation in SIP (I): [RFC3960] defines some guidelines for handling early media -- the practice of sending media from the called party or an application server towards the caller prior to acceptance of the call. Early media is often generated from the PSTN. Early media is a complex topic, and this specification does not fully address the problems associated with it.

RFC 3959, Early Session Disposition Type for the Session Initiation Protocol (SIP) (S): [RFC3959] defines a new session disposition type for use with early media. It indicates that the SDP in the body is for a special early media session. This has seen little usage.

RFC 3204, MIME Media Types for ISUP and QSIG Objects (S): [RFC3204] defines MIME objects for representing SS7 and QSIG signaling messages. SS7 signaling messages are carried in the body of SIP messages when SIP-T is used. QSIG signaling messages can be carried in a similar way.

RFC3666, Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows (B): [RFC3666] provides best practice call flows around interworking with the PSTN.

5. General Purpose Infrastructure Extensions

These extensions are general purpose enhancements to SIP, SDP, and MIME that can serve a wide variety of uses. However, they are not used for every session or registration, as the core specifications are.

RFC 3262, Reliability of Provisional Responses in SIP (S): SIP defines two types of responses to a request: final and provisional. Provisional responses are numbered from 100 to 199. In SIP, these responses are not sent reliably. This choice was made in RFC 2543 since the messages were meant to just be truly informational and rendered to the user. However, subsequent work on PSTN interworking demonstrated a need to map provisional responses to PSTN messages that needed to be sent reliably. [RFC3262] was developed to allow reliability of provisional responses. The specification defines the PRACK method, used for indicating that a provisional response was received. Though it provides a generic capability for SIP, RFC 3262 implementations have been most common in PSTN interworking devices. However, PRACK brings a great deal of complication for relatively small benefit. As such, it has seen only moderate levels of deployment.

RFC 3323, A Privacy Mechanism for the Session Initiation Protocol (SIP) (S): [RFC3323] defines the Privacy header field, used by clients to request anonymity for their requests. Though it defines several privacy services, the only one broadly used is the one that supports privacy of the P-Asserted-Identity header field [RFC3325].

UA-PRIVACY, UA-Driven Privacy Mechanism for SIP (S): [UA-PRIVACY] defines a mechanism for achieving anonymous calls in SIP. It is an alternative to [RFC3323], and instead places more intelligence in the endpoint to craft anonymous messages by directly accessing network services.

RFC 2976, The INFO Method (S): [RFC2976] was defined as an extension to RFC 2543. It defines a method, INFO, used to transport mid-dialog information that has no impact on SIP itself. Its driving application was the transport of PSTN-related information when using SIP between a pair of gateways. Though originally conceived for broader use, it only found standardized usage with SIP-T [RFC3372]. It has been used to support numerous proprietary and non-interoperable extensions due to its poorly defined scope.

RFC 3326, The Reason Header Field for SIP (S): [RFC3326] defines the Reason header field. It is used in requests, such as BYE, to indicate the reason that the request is being sent.

RFC 3388, Grouping of Media Lines in the Session Description Protocol (S): RFC 3388 [RFC3388] defines a framework for grouping together media streams in an SDP message. Such a grouping allows relationships between these streams, such as which stream is the audio for a particular video feed, to be expressed.

RFC 3420, Internet Media Type message/sipfrag (S): [RFC3420] defines a MIME object that contains a SIP message fragment. Only certain header fields and parts of the SIP message are present. For example, it is used to report back on the responses received to a request sent as a consequence of a REFER.

RFC 3608, SIP Extension Header Field for Service Route Discovery During Registration (S): [RFC3608] allows a client to determine, from a REGISTER response, a path of proxies to use in requests it sends outside of a dialog. It can also be used by proxies to verify the Route header in client-initiated requests. In many respects, it is the inverse of the Path header field, but has seen less usage since default outbound proxies have been sufficient in many deployments.

RFC 3841, Caller Preferences for SIP (S): [RFC3841] defines a set of headers that a client can include in a request to control the way in which the request is routed downstream. It allows a client to direct a request towards a UA with specific capabilities, which a UA indicates using [RFC3840].

RFC 4028, Session Timers in SIP (S): [RFC4028] defines a keepalive mechanism for SIP signaling. It is primarily meant to provide a way to clean up old state in proxies that are holding call state for calls from failed endpoints that were never terminated normally. Despite its name, the session timer is not a mechanism for detecting a network failure mid-call. Session timers introduce a fair bit of complexity for relatively little gain, and have seen moderate deployment.

RFC 4168, SCTP as a Transport for SIP (S): [RFC4168] defines how to carry SIP messages over the Stream Control Transmission Protocol (SCTP) [RFC4960]. SCTP has seen very limited usage for SIP transport.

RFC 4244, An Extension to SIP for Request History Information (S): [RFC4244] defines the History-Info header field, which indicates information on how and why a call came to be routed to a particular destination.

RFC 4145, TCP-Based Media Transport in the Session Description Protocol (SDP) (S): [RFC4145] defines an extension to SDP for setting up TCP-based sessions between user agents. It defines who sets up the connection and how its lifecycle is managed. It has seen relatively little usage due to the small number of media types to date that use TCP.

RFC 4091, The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework (S): [RFC4091] defines a mechanism for including both IPv4 and IPv6 addresses for a media session as alternates. This mechanism has been deprecated in favor of ICE [ICE].

SDP-MEDIA, SDP Media Capabilities Negotiation (S): [SDP-MEDIA] defines an extension to the SDP capability negotiation framework [SDP-CAP] for negotiating codecs, codec parameters, and media streams.

BODY-HANDLING, Message Body Handling in the Session Initiation Protocol (SIP): [BODY-HANDLING] clarifies handling of bodies in SIP, focusing primarily on multi-part behavior, which was under-specified in SIP.

6. NAT Traversal

These SIP extensions are primarily aimed at addressing NAT traversal for SIP.

ICE, Interactive Connectivity Establishment (ICE) (S): [ICE] defines a technique for NAT traversal of media sessions for protocols that make use of the offer/answer model. This specification is the IETF-recommended mechanism for NAT traversal for SIP media streams, and is meant to be used even by endpoints that are themselves never behind a NAT. A SIP option tag and media feature tag [OPTION-TAG] have been defined for use with ICE.

ICE-TCP, TCP Candidates with Interactive Connectivity Establishment (ICE) (S): [ICE-TCP] specifies the usage of ICE for TCP streams. This allows for selection of RTP-based voice on top of TCP only when NAT or firewalls would prevent UDP-based voice from working.

RFC 3605, Real Time Control Protocol (RTCP) Attribute in the Session Description Protocol (SDP) (S): [RFC3605] defines a way to explicitly signal, within an SDP message, the IP address and port for RTCP, rather than using the port+1 rule in the Real Time Transport Protocol (RTP) [RFC3550]. It is needed for devices behind NAT, and the specification is required by ICE.

OUTBOUND, Managing Client Initiated Connections through SIP (S): [OUTBOUND], also known as SIP outbound, defines important changes to the SIP registration mechanism that enable delivery of SIP messages towards a UA when it is behind a NAT.

RFC 3581, An Extension to SIP for Symmetric Response Routing (S): [RFC3581] defines the rport parameter of the Via header. It allows SIP responses to traverse NAT.

GRUU, Obtaining and Using Globally Routable User Agent Identifiers (GRUU) in SIP (S): [GRUU] defines a mechanism for directing requests towards a specific UA instance. GRUU is essential for features like transfer and provides another piece of the SIP NAT traversal story.

7. Call Control Primitives

Numerous SIP extensions provide a toolkit of dialog- and call-management techniques. These techniques have been combined together to build many SIP-based services.

RFC 3515, The REFER Method (S): REFER [RFC3515] defines a mechanism for asking a user agent to send a SIP request. It's a form of SIP remote control, and is the primary tool used for call transfer in SIP. Beware that not all potential uses of REFER (neither for all methods nor for all URI schemes) are well defined. Implementors should only use the well-defined ones, and should not second guess or freely assume behavior for the others to avoid unexpected behavior of remote UAs, interoperability issues, and other bad surprises.

RFC 3725, Best Current Practices for Third Party Call Control (3pcc) (B): [RFC3725] defines a number of different call flows that allow one SIP entity, called the controller, to create SIP sessions amongst other SIP user agents.

RFC 3911, The SIP Join Header Field (S): [RFC3911] defines the Join header field. When sent in an INVITE, it causes the recipient to join the resulting dialog into a conference with another dialog in progress.

RFC 3891, The SIP Replaces Header (S): [RFC3891] defines a mechanism that allows a new dialog to replace an existing dialog. It is useful for certain advanced transfer services.

RFC 3892, The SIP Referred-By Mechanism (S): [RFC3892] defines the Referred-By header field. It is used in requests triggered by REFER, and provides the identity of the referring party to the referred-to party.

RFC 4117, Transcoding Services Invocation in SIP Using Third Party Call Control (I): [RFC4117] defines how to use 3pcc for the purposes of invoking transcoding services for a call.

8. Event Framework

RFC 3265, SIP-Specific Event Notification (S): [RFC3265] defines the SUBSCRIBE and NOTIFY methods. These two methods provide a general event notification framework for SIP. To actually use the framework, extensions need to be defined for specific event packages. An event package defines a schema for the event data and describes other aspects of event processing specific to that schema. An RFC 3265 implementation is required when any event package is used.

RFC 3903, SIP Extension for Event State Publication (S): [RFC3903] defines the PUBLISH method. It is not an event package, but is used by all event packages as a mechanism for pushing an event into the system.

RFC 4662, A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists (S): [RFC4662] defines an extension to RFC 3265 that allows a client to subscribe to a list of resources using a single subscription. The server, called a Resource List Server (RLS), will "expand" the subscription and subscribe to each individual member of the list. It has found applicability primarily in the area of presence, but can be used with any event package.

SUBNOT-ETAGS, An Extension to Session Initiation Protocol (SIP) Events for Conditional Event Notification (S): [SUBNOT-ETAGS] defines an extension to RFC 3265 to optimize the performance of notifications. When a client subscribes, it can indicate what version of a document it has so that the server can skip sending a notification if the client is up-to-date. It is applicable to any event package.

9. Event Packages

These are event packages defined to utilize the SIP events framework. Many of these are also listed elsewhere in their respective areas.

RFC 3680, A SIP Event Package for Registrations (S): [RFC3680] defines an event package for finding out about changes in registration state.

GRUU-REG (S): [GRUU-REG] is an extension to the registration event package [RFC3680] that allows user agents to learn about their GRUUs. It is particularly useful in helping to synchronize a client and its registrar with their currently valid temporary GRUU.

RFC 3842, A Message Summary and Message Waiting Indication Event Package for SIP (S): [RFC3842] defines a way for a user agent to find out about voicemails and other messages that are waiting for it. Its primary purpose is to enable the voicemail waiting lamp on most business telephones.

RFC 3856, A Presence Event Package for SIP (S): [RFC3856] defines an event package for indicating user presence through SIP.

RFC 3857, A Watcher Information Event Template Package for SIP (S): [RFC3857], also known as winfo, provides a mechanism for a user agent to find out what subscriptions are in place for a particular event package. Its primary usage is with presence, but it can be used with any event package.

RFC 4235, An INVITE-Initiated Dialog Event Package for SIP (S): [RFC4235] defines an event package for learning the state of the dialogs in progress at a user agent, and is one of several RFCs starting with the important number 42 [HGTTG].

RFC 4575, A SIP Event Package for Conference State (S): [RFC4575] defines a mechanism for learning about changes in conference state, including conference membership.

RFC 4730, A SIP Event Package for Key Press Stimulus (KPML) (S): [RFC4730] defines a way for an application in the network to subscribe to the set of key presses made on the keypad of a traditional telephone. It, along with RFC 4733 [RFC4733], are the two mechanisms defined for handling DTMF. RFC 4730 is a signaling-path solution, and RFC 4733 is a media-path solution.

RTCP-SUM, SIP Event Package for Voice Quality Reporting (S): [RTCP-SUM] defines a SIP event package that enables the collection and reporting of metrics that measure the quality for Voice over Internet Protocol (VoIP) sessions.

SESSION-POLICY, A Framework for Session Initiation Protocol (SIP) Session Policies (S): [SESSION-POLICY] defines a framework for session policies. In this framework, policy servers are used to tell user agents about the media characteristics required for a particular session. The session policy framework has not been widely implemented.

POLICY-PACK, A Session Initiation Protocol (SIP) Event Package for Session-Specific Session Policies (S): [POLICY-PACK] defines a SIP event package used in conjunction with the session policy framework [SESSION-POLICY].

RFC 5362, The Session Initiation Protocol (SIP) Pending Additions Event Package (S): [RFC5362] defines a SIP event package that allows a UA to learn whether consent has been given for the addition of an address to a SIP "mailing list". It is used in conjunction with the SIP framework for consent [RFC5360].

10. Quality of Service

Several specifications concern themselves with the interactions of SIP with network Quality of Service (QoS) mechanisms.

RFC 3312, Integration of Resource Management and SIP (S): [RFC3312], updated by [RFC4032], defines a way to make sure that the phone of the called party doesn't ring until a QoS reservation has been installed in the network. It does so by defining a general preconditions framework, which defines conditions that must be true in order for a SIP session to proceed.

QoS-ID, Quality of Service (QoS) Mechanism Selection in the Session Description Protocol (SDP) (S): [QoS-ID] defines a way for user agents to negotiate what type of end-to-end QoS mechanism to use for a session. At this time, there are two that can be used: the Resource Reservation Protocol (RSVP) and Next Steps in Signaling (NSIS). This negotiation is done through an SDP extension. Due to limited deployment of RSVP and even more limited deployment of NSIS, this extension has not been widely used.

RFC 3313, Private SIP Extensions for Media Authorization (I): [RFC3313] defines a P-header that provides a mechanism for passing an authorization token between SIP and a network QoS reservation protocol like RSVP. Its purpose is to make sure network QoS is

only granted if a client has made a SIP call through the same provider's network. This specification is sometimes referred to as the SIP walled-garden specification by the truly paranoid androids in the SIP community. This is because it requires coupling of signaling and the underlying IP network.

RFC 3524, Mapping of Media Streams to Resource Reservation Flows (S): [RFC3524] defines a usage of the SDP grouping framework for indicating that a set of media streams should be handled by a single resource reservation.

11. Operations and Management

Several specifications have been defined to support operations and management of SIP systems. These include mechanisms for configuration and network diagnostics.

CONFIG-FRAME, A Framework for SIP User Agent Profile Delivery (S): [CONFIG-FRAME] defines a mechanism that allows a SIP user agent to bootstrap its configuration from the network and receive updates to its configuration, should it change. This is considered an essential piece of deploying a usable SIP network.

RTCP-SUM, SIP Event Package for Voice Quality Reporting (S): [RTCP-SUM] defines a SIP event package that enables the collection and reporting of metrics that measure the quality for Voice over Internet Protocol (VoIP) sessions.

12. SIP Compression

Sigcomp [RFC3320] [RFC4896] was defined to allow compression of SIP messages over low bandwidth links. Sigcomp is not formally part of SIP. However, usage of Sigcomp with SIP has required extensions to SIP.

RFC 3486, Compressing SIP (S): [RFC3486] defines a SIP URI parameter that can be used to indicate that a SIP server supports Sigcomp.

RFC 5049, Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP) (S): [RFC5049] defines how to apply Sigcomp to SIP.

13. SIP Service URIs

Several extensions define well-known services that can be invoked by constructing requests with specific structures for the Request URI, resulting in specific behaviors at the User Agent Server (UAS).

RFC 3087, Control of Service Context using Request URI (I): [RFC3087] introduced the context of using Request URIs, encoded appropriately, to invoke services.

RFC 4662, A SIP Event Notification Extension for Resource Lists (S): [RFC4662] defines a resource called a Resource List Server (RLS). A client can send a subscribe to this server. The server will generate a series of subscriptions, compile the resulting information, and send it back to the subscriber. The set of resources that the RLS will subscribe to is a property of the request URI in the SUBSCRIBE request.

RFC 5363, Framework and Security Considerations for Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)-List Services (S): [RFC5363] defines the framework for list services in SIP. In this framework, a UA can include an XML list object in the body of various requests and the server will provide list-oriented services as a consequence. For example, a SUBSCRIBE with a list subscribes to the URI in the list.

RFC 5367, Subscriptions To Request-Contained Resource Lists in SIP (S): [RFC5367] uses the URI-list framework [RFC5363] and allows a client to subscribe to a resource called a Resource List Server. This server will generate subscriptions to the URI in the list, compile the resulting information, and send it back to the subscriber.

RFC 5365, Multiple-Recipient MESSAGE Requests in SIP (S): [RFC5365] uses the URI-list framework [RFC5363] and allows a client to send a MESSAGE to a number of recipients.

RFC 5366, Conference Establishment Using Request-Contained Lists in SIP (S): [RFC5366] uses the URI-list framework [RFC5363]. It allows a client to ask the server to act as a conference focus and send an invitation to each recipient in the list.

RFC 4240, Basic Network Media Services with SIP (I): [RFC4240] defines a way for SIP application servers to invoke announcement and conferencing services from a media server. This is accomplished through a set of defined URI parameters that tell the media server what to do, such as what file to play and what language to render it in.

RFC 4458, Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR) (I): [RFC4458] defines a way to invoke voicemail and IVR services by using a SIP URI constructed in a particular way.

14. Minor Extensions

These SIP extensions don't fit easily into a single specific use case. They have somewhat general applicability, but they solve a relatively small problem or provide an optimization.

RFC 4488, Suppression of the SIP REFER Implicit Subscription (S): [RFC4488] defines an enhancement to REFER. REFER normally creates an implicit subscription to the target of the REFER. This subscription is used to pass back updates on the progress of the referral. This extension allows that implicit subscription to be bypassed as an optimization.

RFC 4538, Request Authorization through Dialog Identification in SIP (S): [RFC4538] provides a mechanism that allows a UAS to authorize a request because the requestor proves it knows a dialog that is in progress with the UAS. The specification is useful in conjunction with the SIP application interaction framework [INTERACT-FRAME].

RFC 4508, Conveying Feature Tags with the REFER Method in SIP (S): [RFC4508] defines a mechanism for carrying RFC 3840 feature tags in REFER. It is useful for informing the target of the REFER about the characteristics of the intended target of the referred request.

RFC 5373, Requesting Answer Modes for SIP (S): [RFC5373] defines an extension for indicating to the called party whether or not the phone should ring and/or be answered immediately. This is useful for push-to-talk and for diagnostic applications.

RFC 5079, Rejecting Anonymous Requests in SIP (S): [RFC5079] defines a mechanism for a called party to indicate to the calling party that a call was rejected since the caller was anonymous. This is needed for implementation of the Anonymous Call Rejection (ACR) feature in SIP.

RFC 5368, Referring to Multiple Resources in SIP (S): [RFC5368] allows a UA sending a REFER to ask the recipient of the REFER to generate multiple SIP requests, not just one. This is useful for conferencing, where a client would like to ask a conference server to eject multiple users.

RFC 4483, A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages (S): [RFC4483] defines a mechanism for content indirection. Instead of carrying an object within a SIP body, a URL reference is carried instead, and the recipient dereferences the URL to obtain the object. The specification has potential applicability for sending large instant messages, but

has yet to find much actual use.

RFC 3890, A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP) (S): [RFC3890] specifies an SDP extension that allows for the description of the bandwidth for a media session that is independent of the underlying transport mechanism.

RFC 4583, Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams (S): [RFC4583] defines a mechanism in SDP to signal floor control streams that use BFCP. It is used for push-to-talk and conference floor control.

CONNECT-PRECON, Connectivity Preconditions for Session Description Protocol Media Streams (S): [CONNECT-PRECON] defines a usage of the precondition framework [RFC3312]. The connectivity precondition makes sure that the session doesn't get established until actual packet connectivity is checked.

RFC 4796, The SDP (Session Description Protocol) Content Attribute (S): [RFC4796] defines an SDP attribute for describing the purpose of a media stream. Examples include a slide view, the speaker, a sign language feed, and so on.

IPv6-TRANS, IPv6 Transition in the Session Initiation Protocol (SIP) (S): [IPv6-TRANS] defines practices for interworking between IPv6 and IPv6 user agents. This is done through multi-homed proxies that interwork IPv4 and IPv6, along with ICE [ICE] for media traversal. The specification includes some minor extensions and clarifications to SDP in order to cover some additional cases.

CONNECT-REUSE, Connection Reuse in the Session Initiation Protocol (SIP) (S): [CONNECT-REUSE] defines an extension to SIP that allows a Transport Layer Security (TLS) connection between servers to be reused for requests in both directions. Normally, two connections are set up between a pair of servers, one for requests in each direction.

15. Security Mechanisms

Several extensions provide additional security features to SIP.

RFC 4474, Enhancements for Authenticated Identity Management in SIP (S): [RFC4474] defines a mechanism for providing a cryptographically verifiable identity of the calling party in a SIP request. Known as "SIP Identity", this mechanism provides an alternative to RFC 3325. It has seen little deployment so far, but its importance as a key construct for anti-spam techniques and new security mechanisms makes it a core part of the SIP specifications.

RFC 4916, Connected Identity in the Session Initiation Protocol (SIP) (S): [RFC4916] formally updates RFC 3261. It defines an extension to SIP that allows a calling user to determine the identity of the final called user (connected party). Due to forwarding and retargeting services, this may not be the same as the user that the caller was originally trying to reach. The mechanism works in tandem with the SIP identity specification [RFC4474] to provide signatures over the connected party identity. It can also be used if a party identity changes mid call due to third party call control actions or PSTN behavior.

SIPS-URI, The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP) (S): [SIPS-URI] is intended to update RFC 3261. It revises the processing of the SIPS URI, originally defined in RFC 3261, to fix many errors and problems that have been encountered with that mechanism.

DOMAIN-CERTS, Domain Certificates in the Session Initiation Protocol (SIP) (B): [DOMAIN-CERTS] clarifies the usage of SIP over TLS with regards to certificate handling, and defines additional procedures needed for interoperability.

RFC 3323, A Privacy Mechanism for the Session Initiation Protocol (SIP) (S): [RFC3323] defines the Privacy header field, used by clients to request anonymity for their requests. Though it defines several privacy services, the only one broadly used is the one that supports privacy of the P-Asserted-Identity header field [RFC3325].

RFC 4567, Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP) (S): [RFC4567] defines extensions to SDP that allow tunneling of a key management protocol, namely MIKEY [RFC3830], through offer/answer exchanges. This mechanism is one of three Secure Realtime Transport Protocol (SRTP) keying techniques specified for SIP, with Datagram Transport Layer Security (DTLS)-SRTP [SRTP-FRAME] having been selected as the final solution.

RFC 4568, Session Description Protocol (SDP) Security Descriptions for Media Streams (S): [RFC4568] defines extensions to SDP that allow for the negotiation of keying material directly through offer/answer, without a separate key management protocol. This mechanism, sometimes called sdescriptions, has the drawback that the media keys are available to any entity that has visibility to the SDP. It is one of three SRTP keying techniques specified for SIP, with DTLS-SRTP [SRTP-FRAME] having been selected as the final solution.

SRTP-FRAME, Framework for Establishing an SRTP Security Context using DTLS (S): [SRTP-FRAME] defines the overall framework and SDP and SIP processing required to perform key management for RTP using Datagram TLS (DTLS) [RFC4347] directly between endpoints, over the media path. It is one of three SRTP keying techniques specified for SIP, with DTLS-SRTP [SRTP-FRAME] having been selected as the final solution.

RFC 3853, S/MIME Advanced Encryption Standard (AES) Requirement for SIP (S): [RFC3853] formally updates RFC 3261. It is a brief specification that updates the cryptography mechanisms used in SIP S/MIME. However, SIP S/MIME has seen very little deployment.

CERTS, Certificate Management Service for the Session Initiation Protocol (SIP) (S): [CERTS] defines a certificate service for SIP whose purpose is to facilitate the deployment of S/MIME. The certificate service allows clients to store and retrieve their own certificates, in addition to obtaining the certificates for other users.

RFC 3893, Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format (S): [RFC3893] defines a SIP message fragment that can be signed in order to provide an authenticated identity over a request. It was an early predecessor to [RFC4474], and consequently AIB has seen no deployment.

SAML, SIP SAML Profile and Binding (S): [SAML] defines the usage of the Security Assertion Markup Language (SAML) within SIP, and describes how to use it in conjunction with SIP identity [RFC4474] to provide authenticated assertions about a user’s role or attributes.

RFC 5360, A Framework for Consent-Based Communications in the Session Initiation Protocol (SIP) (S): [RFC5360] defines several extensions to SIP, including the Trigger-Consent and Permission-Missing header fields. These header fields, in addition to the other procedures defined in the document, define a way to manage membership on "SIP mailing lists" used for instant messaging or conferencing. In particular, it helps avoid the problem of using such amplification services for the purposes of an attack on the network by making sure a user authorizes the addition of their address onto such a service.

RFC 5361, A Document Format for Requesting Consent (S): [RFC5361] defines an XML object used by the consent framework. Consent documents are sent from SIP "mailing list servers" to users to allow them to manage their membership on lists.

RFC 5362, The Session Initiation Protocol (SIP) Pending Additions Event Package (S): [RFC5362] defines a SIP event package that allows a UA to learn whether consent has been given for the addition of an address to a SIP "mailing list". It is used in conjunction with the SIP framework for consent [RFC5360].

RFC 3329, Security Mechanism Agreement for SIP (S): [RFC3329] defines a mechanism to prevent bid-down attacks in conjunction with SIP authentication. The mechanism has seen very limited deployment. It was defined as part of the 3GPP IP Multimedia Subsystem (IMS) specification suite [3GPP.24.229], and is needed only when there is a multiplicity of security mechanisms deployed at a particular server. In practice, this has not been the case.

RFC 4572, Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP) (S): [RFC4572] specifies a mechanism for signaling TLS-based media streams between endpoints. It expands the TCP-based media signaling parameters defined in [RFC4145] to include fingerprint information for TLS streams so that TLS can operate between end hosts using self-signed certificates.

RFC 5027, Security Preconditions for Session Description Protocol Media Streams (S): [RFC5027] defines a precondition for use with the preconditions framework [RFC3312]. The security precondition prevents a session from being established until a security media stream is set up.

RFC 3310, Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (S): [RFC3310] defines an extension to digest authentication to allow it to work with the credentials stored in cell phones. Though technically it is an extension to HTTP digest, its primary application is SIP. This extension is useful primarily to implementors of IMS.

RFC 4169, Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2 (S): [RFC4169] is an enhancement to [RFC3310] that further improves security of the authentication.

16. Conferencing

Numerous SIP and SDP extensions are aimed at conferencing as their primary application.

RFC 4574, The SDP (Session Description Protocol) Label Attribute (S): [RFC4574] defines an SDP attribute for providing an opaque label for media streams. These labels can be referred to by external documents, and in particular, by conference policy documents. This allows a UA to tie together documents it may obtain through conferencing mechanisms to media streams to which they refer.

RFC 3911, The SIP Join Header Field (S): [RFC3911] defines the Join header field. When sent in an INVITE, it causes the recipient to join the resulting dialog into a conference with another dialog in progress.

RFC 4575, A SIP Event Package for Conference State (S): [RFC4575] defines a mechanism for learning about changes in conference state, including conference membership.

RFC 5368, Referring to Multiple Resources in SIP (S): [RFC5368] allows a UA sending a REFER to ask the recipient of the REFER to generate multiple SIP requests, not just one. This is useful for conferencing, where a client would like to ask a conference server to eject multiple users.

RFC 5366, Conference Establishment Using Request-Contained Lists in SIP (S): [RFC5366] is similar to [RFC5367]. However, instead of subscribing to the resource, an INVITE request is sent to the resource, and it will act as a conference focus and generate an invitation to each recipient in the list.

RFC4579, Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents (B): [RFC4579] defines best practice procedures and call flows for conferencing. This includes conference creation, joining, and dial out, amongst other capabilities.

RFC 4583, Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams (S): [RFC4583] defines a mechanism in SDP to signal floor control streams that use BFCP. It is used for push-to-talk and conference floor control.

17. Instant Messaging, Presence, and Multimedia

SIP provides extensions for instant messaging, presence, and multimedia.

RFC 3428, SIP Extension for Instant Messaging (S): [RFC3428] defines the MESSAGE method, used for sending an instant message without setting up a session (sometimes called "page mode").

RFC 3856, A Presence Event Package for SIP (S): [RFC3856] defines an event package for indicating user presence through SIP.

RFC 3857, A Watcher Information Event Template Package for SIP (S): [RFC3857], also known as winfo, provides a mechanism for a user agent to find out what subscriptions are in place for a particular event package. Its primary usage is with presence, but it can be used with any event package.

TRANSFER-MECH, A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer (S): [TRANSFER-MECH] defines a mechanism for signaling a file transfer session with SIP.

18. Emergency Services

Emergency services include preemption features, which allow authorized individuals to gain access to network resources in time of emergency, along with traditional emergency calling.

RFC 4411, Extending the SIP Reason Header for Preemption Events (S): [RFC4411] defines an extension to the Reason header, allowing a UA to know that its dialog was torn down because a higher priority session came through.

RFC 4412, Communications Resource Priority for SIP (S): [RFC4412] defines a new header field, Resource-Priority, that allows a session to get priority treatment from the network.

LOCATION, Location Conveyance for the Session Initiation Protocol (S): [LOCATION] defines a mechanism for carrying location objects in SIP messages. This is used to convey location from a UA to an emergency call taker.

19. Security Considerations

This specification is an overview of existing specifications and does not introduce any security considerations on its own. Of course, the world would be far more secure if everyone would follow one simple rule: "Don't Panic!" [HGTTG].

20. Acknowledgements

The author would like to thank Spencer Dawkins, Brian Stucker, Keith Drage, John Elwell, and Avshalom Houri for their comments on this

document.

21. Informative References

[3GPP.24.229] 3GPP, "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", 3GPP TS 24.229 5.22.0, September 2008.

[ABNF-FIX] Gurbani, V. and B. Carpenter, "Essential correction for IPv6 ABNF in RFC3261", Work in Progress, November 2007.

[BODY-HANDLING] Camarillo, G., "Message Body Handling in the Session Initiation Protocol (SIP)", Work in Progress, November 2008.

[CERTS] Jennings, C. and J. Fischl, "Certificate Management Service for The Session Initiation Protocol (SIP)", Work in Progress, November 2008.

[CONFIG-FRAME] Channabasappa, S., "A Framework for Session Initiation Protocol User Agent Profile Delivery", Work in Progress, February 2008.

[CONNECT-PRECON] Andreasen, F., Camarillo, G., Oran, D., and D. Wing, "Connectivity Preconditions for Session Description Protocol Media Streams", Work in Progress, October 2008.

[CONNECT-REUSE] Gurbani, V., Mahy, R., and B. Tate, "Connection Reuse in the Session Initiation Protocol (SIP)", Work in Progress, October 2008.

[DOMAIN-CERTS] Gurbani, V., Lawrence, S., and B. Laboratories, "Domain Certificates in the Session Initiation Protocol (SIP)", Work in Progress, October 2008.

[ECRIT-FRAME] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia", Work in Progress, July 2008.

[GRUU] Rosenberg, J., "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)", Work in Progress, October 2007.

[GRUU-REG] Kyzivat, P., "Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routable User Agent URIs (GRUUs)", Work in Progress, July 2007.

[HGTTG] Adams, D., "The Hitchhiker's Guide to the Galaxy", September 1979.

[ICE] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", Work in Progress, October 2007.

[ICE-TCP] Rosenberg, J., "TCP Candidates with Interactive Connectivity Establishment (ICE)", Work in Progress, July 2008.

[INTERACT-FRAME] Rosenberg, J., "A Framework for Application Interaction in the Session Initiation Protocol (SIP)", Work in Progress, July 2005.

[IPv6-TRANS] Camarillo, G., "IPv6 Transition in the Session Initiation Protocol (SIP)", Work in Progress, August 2007.

[LOCATION] Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol", Work in Progress, November 2008.

[LOOP-FIX] Sparks, R., Lawrence, S., Hawrylyshen, A., and B. Campen, "Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies", Work in Progress, October 2008.

[OPTION-TAG] Rosenberg, J., "Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)", Work in Progress, June 2007.

[OUTBOUND] Jennings, C. and R. Mahy, "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)", Work in Progress, October 2008.

[POLICY-PACK] Hilt, V. and G. Camarillo, "A Session Initiation Protocol (SIP) Event Package for Session-Specific Session Policies.", Work in Progress, July 2008.

[QoS-ID] Polk, J., Dhesikan, S., and G. Camarillo, "Quality

of Service (QoS) Mechanism Selection in the Session Description Protocol (SDP)", Work in Progress, November 2008.

[RECORD-ROUTE] Froment, T., Lebel, C., and B. Bonnaerens, "Addressing Record-Route issues in the Session Initiation Protocol (SIP)", Work in Progress, October 2008.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2543] Handley, M., Schulzrinne, H., Schooler, E., and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, March 1999.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC2848] Petrack, S. and L. Conroy, "The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services", RFC 2848, June 2000.

[RFC2976] Donovan, S., "The SIP INFO Method", RFC 2976, October 2000.

[RFC3087] Campbell, B. and R. Sparks, "Control of Service Context using SIP Request-URI", RFC 3087, April 2001.

[RFC3204] Zimmerer, E., Peterson, J., Vemuri, A., Ong, L., Audet, F., Watson, M., and M. Zonoun, "MIME media types for ISUP and QSIG Objects", RFC 3204, December 2001.

[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.

[RFC3262] Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, June 2002.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[RFC3265] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 2002.

[RFC3310] Niemi, A., Arkko, J., and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, September 2002.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002.

[RFC3312] Camarillo, G., Marshall, W., and J. Rosenberg, "Integration of Resource Management and Session Initiation Protocol (SIP)", RFC 3312, October 2002.

[RFC3313] Marshall, W., "Private Session Initiation Protocol (SIP) Extensions for Media Authorization", RFC 3313, January 2003.

[RFC3320] Price, R., Bormann, C., Christoffersson, J., Hannu, H., Liu, Z., and J. Rosenberg, "Signaling Compression (SigComp)", RFC 3320, January 2003.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[RFC3326] Schulzrinne, H., Oran, D., and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)", RFC 3326, December 2002.

[RFC3327] Willis, D. and B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts", RFC 3327, December 2002.

[RFC3329] Arkko, J., Torvinen, V., Camarillo, G., Niemi, A., and T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", RFC 3329,

January 2003.

[RFC3372] Vemuri, A. and J. Peterson, "Session Initiation Protocol for Telephones (SIP-T): Context and Architectures", BCP 63, RFC 3372, September 2002.

[RFC3388] Camarillo, G., Eriksson, G., Holler, J., and H. Schulzrinne, "Grouping of Media Lines in the Session Description Protocol (SDP)", RFC 3388, December 2002.

[RFC3398] Camarillo, G., Roach, A., Peterson, J., and L. Ong, "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping", RFC 3398, December 2002.

[RFC3401] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS", RFC 3401, October 2002.

[RFC3420] Sparks, R., "Internet Media Type message/sipfrag", RFC 3420, November 2002.

[RFC3427] Mankin, A., Bradner, S., Mahy, R., Willis, D., Ott, J., and B. Rosen, "Change Process for the Session Initiation Protocol (SIP)", BCP 67, RFC 3427, December 2002.

[RFC3428] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[RFC3482] Foster, M., McGarry, T., and J. Yu, "Number Portability in the Global Switched Telephone Network (GSTN): An Overview", RFC 3482, February 2003.

[RFC3486] Camarillo, G., "Compressing the Session Initiation Protocol (SIP)", RFC 3486, February 2003.

[RFC3515] Sparks, R., "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003.

[RFC3524] Camarillo, G. and A. Monrad, "Mapping of Media Streams to Resource Reservation Flows", RFC 3524, April 2003.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3578] Camarillo, G., Roach, A., Peterson, J., and L. Ong, "Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signalling to the Session Initiation Protocol (SIP)", RFC 3578, August 2003.

[RFC3581] Rosenberg, J. and H. Schulzrinne, "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing", RFC 3581, August 2003.

[RFC3605] Huitema, C., "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)", RFC 3605, October 2003.

[RFC3608] Willis, D. and B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration", RFC 3608, October 2003.

[RFC3665] Johnston, A., Donovan, S., Sparks, R., Cunningham, C., and K. Summers, "Session Initiation Protocol (SIP) Basic Call Flow Examples", BCP 75, RFC 3665, December 2003.

[RFC3666] Johnston, A., Donovan, S., Sparks, R., Cunningham, C., and K. Summers, "Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows", BCP 76, RFC 3666, December 2003.

[RFC3680] Rosenberg, J., "A Session Initiation Protocol (SIP) Event Package for Registrations", RFC 3680, March 2004.

[RFC3725] Rosenberg, J., Peterson, J., Schulzrinne, H., and G. Camarillo, "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)", BCP 85, RFC 3725, April 2004.

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

[RFC3840] Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Indicating User Agent Capabilities in the Session

Initiation Protocol (SIP)", RFC 3840, August 2004.

[RFC3841] Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)", RFC 3841, August 2004.

[RFC3842] Mahy, R., "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)", RFC 3842, August 2004.

[RFC3853] Peterson, J., "S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)", RFC 3853, July 2004.

[RFC3856] Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, August 2004.

[RFC3857] Rosenberg, J., "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)", RFC 3857, August 2004.

[RFC3890] Westerlund, M., "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)", RFC 3890, September 2004.

[RFC3891] Mahy, R., Biggs, B., and R. Dean, "The Session Initiation Protocol (SIP) "Replaces" Header", RFC 3891, September 2004.

[RFC3892] Sparks, R., "The Session Initiation Protocol (SIP) Referred-By Mechanism", RFC 3892, September 2004.

[RFC3893] Peterson, J., "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format", RFC 3893, September 2004.

[RFC3903] Niemi, A., "Session Initiation Protocol (SIP) Extension for Event State Publication", RFC 3903, October 2004.

[RFC3910] Gurbani, V., Brusilovsky, A., Faynberg, I., Gato, J., Lu, H., and M. Unmehopa, "The SPIRITS (Services in PSTN requesting Internet Services) Protocol", RFC 3910, October 2004.

[RFC3911] Mahy, R. and D. Petrie, "The Session Initiation Protocol (SIP) "Join" Header", RFC 3911,

October 2004.

[RFC3959] Camarillo, G., "The Early Session Disposition Type for the Session Initiation Protocol (SIP)", RFC 3959, December 2004.

[RFC3960] Camarillo, G. and H. Schulzrinne, "Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)", RFC 3960, December 2004.

[RFC4028] Donovan, S. and J. Rosenberg, "Session Timers in the Session Initiation Protocol (SIP)", RFC 4028, April 2005.

[RFC4032] Camarillo, G. and P. Kyzivat, "Update to the Session Initiation Protocol (SIP) Preconditions Framework", RFC 4032, March 2005.

[RFC4091] Camarillo, G. and J. Rosenberg, "The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework", RFC 4091, June 2005.

[RFC4117] Camarillo, G., Burger, E., Schulzrinne, H., and A. van Wijk, "Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc)", RFC 4117, June 2005.

[RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", RFC 4145, September 2005.

[RFC4168] Rosenberg, J., Schulzrinne, H., and G. Camarillo, "The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)", RFC 4168, October 2005.

[RFC4169] Torvinen, V., Arkko, J., and M. Naslund, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2", RFC 4169, November 2005.

[RFC4235] Rosenberg, J., Schulzrinne, H., and R. Mahy, "An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)", RFC 4235, November 2005.

[RFC4240] Burger, E., Van Dyke, J., and A. Spitzer, "Basic

Network Media Services with SIP", RFC 4240, December 2005.

[RFC4244] Barnes, M., "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, November 2005.

[RFC4320] Sparks, R., "Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction", RFC 4320, January 2006.

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[RFC4411] Polk, J., "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events", RFC 4411, February 2006.

[RFC4412] Schulzrinne, H. and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)", RFC 4412, February 2006.

[RFC4458] Jennings, C., Audet, F., and J. Elwell, "Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)", RFC 4458, April 2006.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC4483] Burger, E., "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages", RFC 4483, May 2006.

[RFC4488] Levin, O., "Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription", RFC 4488, May 2006.

[RFC4497] Elwell, J., Derks, F., Mourot, P., and O. Rousseau, "Interworking between the Session Initiation Protocol (SIP) and QSIG", BCP 117, RFC 4497, May 2006.

[RFC4508] Levin, O. and A. Johnston, "Conveying Feature Tags with the Session Initiation Protocol (SIP) REFER Method", RFC 4508, May 2006.

[RFC4538] Rosenberg, J., "Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP)", RFC 4538, June 2006.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[RFC4567] Arkko, J., Lindholm, F., Naslund, M., Norrman, K., and E. Carrara, "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)", RFC 4567, July 2006.

[RFC4568] Andreasen, F., Baugher, M., and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", RFC 4568, July 2006.

[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, July 2006.

[RFC4574] Levin, O. and G. Camarillo, "The Session Description Protocol (SDP) Label Attribute", RFC 4574, August 2006.

[RFC4575] Rosenberg, J., Schulzrinne, H., and O. Levin, "A Session Initiation Protocol (SIP) Event Package for Conference State", RFC 4575, August 2006.

[RFC4579] Johnston, A. and O. Levin, "Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents", BCP 119, RFC 4579, August 2006.

[RFC4583] Camarillo, G., "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams", RFC 4583, November 2006.

[RFC4662] Roach, A., Campbell, B., and J. Rosenberg, "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists", RFC 4662, August 2006.

[RFC4730] Burger, E. and M. Dolly, "A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)", RFC 4730, November 2006.

[RFC4733] Schulzrinne, H. and T. Taylor, "RTP Payload for DTMF Digits, Telephony Tones, and Telephony

Signals", RFC 4733, December 2006.

[RFC4796] Hautakorpi, J. and G. Camarillo, "The Session Description Protocol (SDP) Content Attribute", RFC 4796, February 2007.

[RFC4896] Surtees, A., West, M., and A. Roach, "Signaling Compression (SigComp) Corrections and Clarifications", RFC 4896, June 2007.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, June 2007.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

[RFC5027] Andreasen, F. and D. Wing, "Security Preconditions for Session Description Protocol (SDP) Media Streams", RFC 5027, October 2007.

[RFC5049] Bormann, C., Liu, Z., Price, R., and G. Camarillo, "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)", RFC 5049, December 2007.

[RFC5079] Rosenberg, J., "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)", RFC 5079, December 2007.

[RFC5360] Rosenberg, J., Camarillo, G., and D. Willis, "A Framework for Consent-Based Communications in the Session Initiation Protocol (SIP)", RFC 5360, October 2008.

[RFC5361] Camarillo, G., "A Document Format for Requesting Consent", RFC 5361, October 2008.

[RFC5362] Camarillo, G., "The Session Initiation Protocol (SIP) Pending Additions Event Package", RFC 5362, October 2008.

[RFC5363] Camarillo, G. and A. Roach, "Framework and Security Considerations for Session Initiation Protocol (SIP) URI-List Services", RFC 5363, October 2008.

[RFC5365] Garcia-Martin, M. and G. Camarillo, "Multiple-Recipient MESSAGE Requests in the Session Initiation Protocol (SIP)", RFC 5365, October 2008.

[RFC5366] Camarillo, G. and A. Johnston, "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)", RFC 5366, October 2008.

[RFC5367] Camarillo, G., Roach, A., and O. Levin, "Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP)", RFC 5367, October 2008.

[RFC5368] Camarillo, G., Niemi, A., Isomaki, M., Garcia-Martin, M., and H. Khartabil, "Referring to Multiple Resources in the Session Initiation Protocol (SIP)", RFC 5368, October 2008.

[RFC5373] Willis, D. and A. Allen, "Requesting Answering Modes for the Session Initiation Protocol (SIP)", RFC 5373, November 2008.

[RTCP-SUM] Clark, A., Pendleton, A., Johnston, A., and H. Sinnreich, "Session Initiation Protocol Package for Voice Quality Reporting Event", Work in Progress, October 2008.

[SAML] Tschofenig, H., Hodges, J., Peterson, J., Polk, J., and D. Sicker, "SIP SAML Profile and Binding", Work in Progress, November 2008.

[SDP-CAP] Andreasen, F., "SDP Capability Negotiation", Work in Progress, July 2008.

[SDP-MEDIA] Gilman, R., Even, R., and F. Andreasen, "SDP media capabilities Negotiation", Work in Progress, July 2008.

[SESSION-POLICY] Hilt, V., Camarillo, G., and J. Rosenberg, "A Framework for Session Initiation Protocol (SIP) Session Policies", Work in Progress, November 2008.

[SIMPLE] Rosenberg, J., "SIMPLE made Simple: An Overview of the IETF Specifications for Instant Messaging and Presence using the Session Initiation Protocol (SIP)", Work in Progress, October 2008.

[SIPS-URI] Audet, F., "The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)", Work in Progress, November 2008.

[SRTP-FRAME] Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing an SRTP Security Context using DTLS", Work in Progress, October 2008.

[SUBNOT-ETAGS] Niemi, A., "An Extension to Session Initiation Protocol (SIP) Events for Conditional Event Notification", Work in Progress, July 2008.

[TRANSFER-MECH] Garcia, M., Isomaki, M., Camarillo, G., Loreto, S., and P. Kyzivat, "A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer", Work in Progress, November 2008.

[UA-PRIVACY] Munakata, M., Schubert, S., and T. Ohba, "UA-Driven Privacy Mechanism for SIP", Work in Progress, October 2008.

[UPDATE-PAI] Elwell, J., "Updates to Asserted Identity in the Session Initiation Protocol (SIP)", Work in Progress, October 2008.

Author's Address

Jonathan Rosenberg
Cisco
Iselin, NJ
US

EMail: jdrosen@cisco.com
URI: http://www.jdrosen.net

Full Copyright Statement

Intellectual Property