Internet Engineering Task Force   B. Rosen
Internet-Draft
Intended status: Standards Track   J. Malloy
Expires: August 5, 2019   B. Henderson
                                                  The MITRE Corporation
                                                       February 1, 2019

Interoperability Profile for Relay User Equipment
draft-rosen-rue-00

Abstract

   This document identifies a minimum set of standards and requirements
   that must be supported by a Video Relay Service (VRS) Video Access
   Technology Reference Platform (VATRP)-compliant client and United
   States Telecommunications Relay Service providers required to be
   VATRP compliant. This Relay User Equipment specification only
   specifies a minimum set of requirements. It does not prohibit VRS
   providers or endpoint developers from developing or deploying
   additional capabilities, provided that doing so will not prevent
   compliance with the requirements specified here.

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 https://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 August 5, 2019.

publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction

   Video Relay Service (VRS) is a form of Telecommunications Relay
   Service (TRS) that enables persons with hearing disabilities who use
   sign language, such as American Sign Language (ASL), to communicate
   with voice telephone users through video equipment. These services
   also enable communication between such individuals directly in
   suitable modalities, including any combination of sign language via
   video, real-time text (RTT), and speech.

   This Interoperability Profile for Relay User Equipment (RUE) is a
   profile of the Session Initiation Protocol (SIP) and related media
   protocols that enables end-user equipment registration and calling
   for VRS calls. It specifies the minimal set of call flows, Internet
   Engineering Task Force (IETF) and ITU-T standards that must be
   supported, provides guidance where the standards leave multiple
   implementation options, and specifies minimal and extended
   capabilities for RUE calls.

   This RUE profile supports the requirements of relay services in the
   United States, as described in 47 CFR 64.601 et seq., but may be
   applicable to similar uses elsewhere.

2. Scope

   This RUE Specification documents the standards and controls
   associated with the Video Access Technology Reference Platform
   (VATRP). This RUE specification identifies the minimum set of
   standards for the interface between the VATRP and Providers' networks
   to which the VATRP adheres. This RUE Specification does not prohibit
   the implementation of additional features or functionality by any
   Provider. It also contains some Provider-optional features. If a
   Provider offers the feature described by the optional specification
   on at least one endpoint, the Provider MUST supply the standardized
   interface described in this document for that feature. This edition
   of the RUE specification does not address Provider-to-Provider
   communication (covered in the US VRS Provider Interface Profile) or
   the user interface to the RUE.

3. Terminology

   Communication Assistant (CA): The ASL interpreter stationed in a TRS-
   registered call center working for a VRS Provider, acting as part of
   the wire of a call to provide functionally equivalent phone service.

Communication modality (modality): A specific form of communication that may be employed by two users, e.g., English voice, Spanish voice, American Sign Language, English lip-reading, or French real-time-text. Here, one communication modality is assumed to encompass both the language and the way that language is exchanged. For example, English voice and French voice are two different communication modalities.

Default video relay service: The video relay service operated by a subscriber's default VRS provider.

Default video relay service Provider (default Provider): The VRS provider that registers, and assigns a telephone number to, a specific subscriber. A subscriber's default Provider provides the VRS that handles incoming relay calls to the user. The default Provider also handles outgoing relay calls by default.

Dial-around call: A relay call where the subscriber specifies the use of a VRS provider other than one of the Providers with whom the subscriber is registered. This can be accomplished by the user dialing a "front-door" number for a VRS provider and signing or texting a phone number to call ("two-stage"). Alternatively, this can be accomplished by the user's RUE software instructing the server of its default VRS provider to automatically route the call through the alternate Provider to the desired public switched telephone network (PSTN) directory number ("one-stage").

Full Intra Request (FIR): A request to a media sender, requiring that media sender to send a Decoder Refresh Point at the earliest opportunity. FIR is sometimes known as "instantaneous decoder refresh request", "video fast update request", or "fast update request".

NANP: North America Numbering Plan (please refer to: http://nationalnanpa.org).

Point-to-Point Call (P2P Call): A call between two RUEs, without including a CA.

Relay call: A call that allows persons with hearing or speech disabilities to use a RUE to talk to users of traditional voice services with the aid of a communication assistant (CA) to relay the communication. Please refer to FCC-VRS-GUIDE.

Relay number database (RND): The iTRS Relay Number Database (RND) functions as a 10-digit NANP phone number lookup for SIP and H.323 URLs for TRS subscribers.

Relay-to-relay call: A call between two subscribers each using different forms of relay (video relay, IP relay, TTY), each with a separate CA to assist in relaying the conversation.

Relay service (RS): A service that allow a registered subscriber to use a RUE to make and receive relay calls, point-to-point calls, and relay-to-relay calls. The functions provided by the relay service include the provision of media links supporting the communication modalities used by the caller and callee, and user registration and validation, authentication, authorization, automatic call distributor (ACD) platform functions, routing (including emergency call routing), call setup, mapping, call features (such as call forwarding and video mail), and assignment of CAs to relay calls.

Relay service Provider (Provider): An organization that operates a relay service. A subscriber selects a relay service Provider to assign and register a telephone number for their use, to register with for receipt of incoming calls, and to provide the default service for outgoing calls.

Relay user: Please refer to "subscriber".

Relay user E.164 Number (user E.164): The telephone number assigned to the RUE in ITU-T E.164 format.

Relay user equipment (RUE): A SIP user agent (UA) enhanced with extra features to support a subscriber in requesting and using relay calls. A RUE may take many forms, including a stand-alone device; an application running on a general-purpose computing device such as a laptop, tablet or smart phone; or proprietary equipment connected to a server that provides the RUE interface.

Sign language: A language that uses hand gestures and body language to convey meaning including, but not limited to, American Sign Language (ASL).

Subscriber: An individual who has registered with a Provider and who obtains service by using relay user equipment. This is the traditional telecom term for an end-user customer, which in our case is a relay user.

Telecommunications relay services (TRS): Telephone transmission services that provide the ability for an individual who has a hearing impairment or speech impairment to engage in communication by wire or radio with a hearing individual in a manner that is functionally equivalent to the ability of an individual who does not have a hearing impairment or speech impairment to communicate using voice communication services by wire or radio. TRS includes services that

enable two-way communication between an individual who uses a
Telecommunications Device for the Deaf (TDD) or other non-voice
terminal device and an individual who does not use such a device.

Video relay service (VRS): A relay service for people with hearing or
speech disabilities who use sign language to communicate using video
equipment (video RUE) with other people in real time. The video link
allows the CA to view and interpret the subscriber's signed
conversation and relay the conversation back and forth with the other
party.

4. Requirements Language

The keywords "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]

5. General Requirements

All HTTP/HTTPS connections specified throughout this document MUST
use HTTPS. Both HTTPS and all SIP Transactions MUST use TLS 1.2
[RFC5246] or later, using a server-side certificate issued by a well-
known Certificate Agency. The minimum cipher suite to be supported
is TLS_RSA_WITH_AES_256_CBC_SHA25.
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 support is RECOMMENDED.

During the establishment of secure connections with a provider, the
RUE MAY be asked by the server for a client certificate. In that
case it SHOULD provide a client certificate. Providers MAY reject
requests that fail to provide a recognized certificate.

All text data payloads not otherwise constrained by a specification
in another standards document MUST be encoded as Unicode UTF/8.

6. SIP Signaling

The RUE and Providers MUST conform to the following core SIP
standards [RFC3261] (Base SIP) [RFC3263] (Locating SIP Servers),
[RFC3264] (Offer/Answer), [RFC3840] (User Agent Capabilities),
[RFC5626] (Outbound), [RFC4566] (Session Description Protocol),
[RFC3323] (Privacy), [RFC3605] (RTCP Attribute in SDP), [RFC6665]
(SIP Events), [RFC3311] (UPDATE Method), [RFC5393] (Loop-Fix),
[RFC5658] (Record Route fix), [RFC5954] (ABNF fix), [RFC3960] (Early
Media), and [RFC6442] (Geolocation Header).

In addition, the RUE MUST, and Providers MAY, conform to [RFC3327]
(Path), [RFC5245] (ICE), [RFC3326] (Reason header), [RFC3515] (REFER
Method), [RFC3891] (Replaces Header), [RFC3892] (Referred-By).

RUEs MUST include a "User-Agent" header field uniquely identifying
the RUE application, platform, and version in all SIP requests, and
MUST include a "Server" header field with the same content in SIP
responses.

6.1. Registration

The RUE MUST register with a SIP registrar, following [RFC3261] and
[RFC5626]. If the configuration (please refer to Section 11)
contains multiple "outbound-proxies", then the RUE MUST use them as
specified in [RFC5626] to establish multiple flows.

The request-URI for the REGISTER request MUST contain the "provider-
domain" from the configuration. The To-URI and From-URI MUST be
identical URIs, formatted as specified in Section 13, using the
"phone-number" and "provider-domain" from the configuration.

The RUE determines the URI to resolve by initially determining if an
outbound proxy is configured. If it is, the URI will be that of the
outbound proxy. If no outbound proxy is configured, the URI will be
the Request-URI from the REGISTER request. The RUE extracts the
domain from that URI and consults the DNS record for that domain.
The DNS entry MUST contain NAPTR records conforming to RFC3263. One
of those NAPTR records MUST specify TLS as the preferred transport
for SIP. For example, a DNS NAPTR query for "sip:
p1.red.example.netv" could return:

```
    IN NAPTR 50  50 "s" "SIPS+D2T" "" _sips._tcp.p1.red.example.net
    IN NAPTR 90  50 "s" "SIP+D2T"  "" _sip._tcp.p1.red.example.net
```

If the RUE receives a 439 (First Hop Lacks Outbound Support) response
to a REGISTER request, it MUST re-attempt registration without using
the outbound mechanism.

The registrar MAY authenticate using SIP MD5 digest authentication.
The credentials to be used (username and password) MUST be supplied
within the credentials section of the configuration and identified by
the realm the registrar uses in a digest challenge. This username/
password combination SHOULD NOT be the same as that used for other
purposes, such as retrieving the RUE configuration or logging into
the Provider's customer service portal. Because MD5 is considered
insecure, [I-D.yusef-sipcore-digest-scheme] SHOULD be implemented by
both the RUE and Providers and SHA-based digest algorithms SHOULD be
used for digest authentication.

If the registration request fails with an indication that credentials
from the configuration are invalid, then the RUE SHOULD retrieve a
fresh version of the configuration. If credentials from a freshly

retrieved configuration are found to be invalid, then the RUE MUST
cease attempts to register and SHOULD inform the RUE User of the
problem.

Support for multiple simultaneous registrations by Providers is
OPTIONAL, as described in Section 2.

Multiple simultaneous RUE SIP registrations from different RUE
devices with the same SIP URI SHOULD be permitted by the Provider.
The Provider MAY limit the total number of simultaneous
registrations. When a new registration request is received that
results in exceeding the limit on simultaneous registrations, the
Provider MAY then prematurely terminate another registration;
however, it SHOULD NOT do this if it would disconnect an active call.

If a Provider prematurely terminates a registration to reduce the
total number of concurrent registrations with the same URI, it SHOULD
take some action to prevent the affected RUE from automatically re-
registering and re-triggering the condition.

6.2. Session Establishment

6.2.1. Normal Call Origination

After initial SIP registration, the RUE adheres to SIP [RFC3261]
basic call flows, as documented in [RFC3665].

The RUE MUST route all calls through the outbound proxy of the
default Provider.

INVITE requests used to initiate calls SHOULD NOT contain Route
headers. Route headers MAY be included in one-stage dial-around
calls and emergency calls. The SIP URIs in the To field and the
Request-URI MUST be formatted as specified in subsection 6.4 using
the destination phone number. The domain field of the URIs SHOULD be
the "provider-domain" from the configuration (e.g.,
sip:+13115552368@red.example.com;user=phone). The same exceptions
apply, including anonymous calls.

Anonymous calls MUST be supported by both the RUE and Providers. An
anonymous call is signaled per [RFC3323].

The From-URI MUST be formatted as specified in Section 6.4, using the
phone-number and "provider-domain" from the configuration. It SHOULD
also contain the display-name from the configuration when present.
(Please refer to Section 11.2.)

Negotiated media MUST follow the guidelines specified in Section 7 of this document.

To allow time to timeout an unanswered call and direct it to a videomail server, the User Agent Client MUST NOT impose a time limit less than the default SIP Invite transaction timeout of 3 minutes.

6.2.2. One-Stage Dial-Around Origination

Outbound dial-around calls allow a RUE user to select any Provider to provide interpreting services for any call. "Two-stage" dial-around calls involve the RUE calling a telephone number that reaches the dial-around Provider and using signing or DTMF to provide the called party telephone number. In two-stage dial-around, the To URI is the URI of the dial-around Provider and the domain of the URI is the Provider domain from the configuration.

One-stage dial-around is a method where the called party telephone number is provided in the To URI and the Request-URI, using the domain of the dial-around Provider.

For one-stage dial-around, the RUE MUST follow the procedures in Section 6.2.1 with the following exception: the domain part of the SIP URIs in the To field and the Request-URI MUST be the domain of the dial-around Provider, discovered according to Section 11.1.

The following is a partial example of a one-stage dial-around call from VRS user +1-555-222-0001 hosted by red.example.com to a hearing user +1-555-123-4567 using dial-around to green.example.com for the relay service. Only important details of the messages are shown and many header fields have been omitted:

```
    ,-+-.          ,----+----.     ,-----+-----.
   |RUE|          |Default  |     |Dial-Around|
   |   |          |Provider |     | Provider  |
    `-+-'          `----+----'     `-----+-----'
     |                  |                |
     | [1] INVITE       |                |
     |------------->| [2] INVITE    |
     |                  |------------->|
```
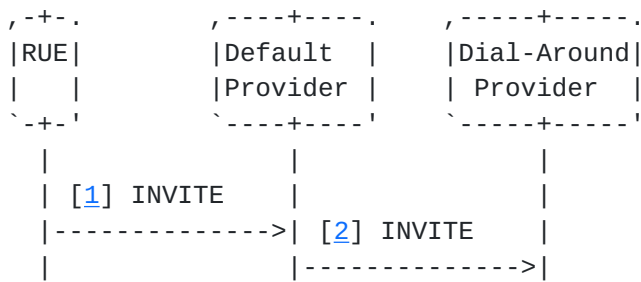
   Message Details:

   [1] INVITE Rue -> Default Provider

   INVITE sip:+15551234567@green.example.net;user=phone SIP/2.0
   To: <sip:+15551234567@green.example.net;user=phone>
   From: "Bob Smith" <sip:+18135551212@red.example.net;user=phone>
   Route: sip:green.example.net

   [2] INVITE Default Provider -> Dial-Around Provider

   INVITE sip:+15551234567@green.example.net;user=phone SIP/2.0
   To: <sip:+15551234567@green.example.net;user=phone>
   From: "Bob Smith" sip:+18135551212@red.example.net;user=phone
   P-Asserted-Identity: sip:+18135551212@red.example.net

                      One Stage Dial-Around

6.2.3. RUE Contact Information

   To identify the owner of a RUE, the initial INVITE for a call from a
   RUE, or the 200 OK accepting a call by a RUE, identifies the owner by
   sending a Call-Info header with a purpose parameter of "rue-owner".
   The URI MAY be an HTTPS URI or Content-Indirect URL. The latter is
   defined by [RFC2392] to locate message body parts. This URI type is
   present in a SIP message to convey the RUE ownership information as a
   MIME body. The form of the RUE ownership information is an xCard.
   Please refer to [RFC6442] for an example of using Content-Indirect
   URLs in SIP messages. Note that use of the Content-Indirect URL
   usually implies multiple message bodies ("mime/multipart").

6.2.4. Incoming Calls

   The RUE MUST accept inbound calls sent to it by the proxy mentioned
   in the configuration.

   If Multiple simultaneous RUE SIP registrations from different RUE
   devices with the same SIP URI exist, the Provider MUST parallel fork

the call to all registered RUEs so that they ring at the same time.
The first RUE to reply with a 200 OK answers the call and the
Provider MUST CANCEL other call branches.

6.2.5. Emergency Calls

The RUE MUST comply with [RFC6881] for handling of emergency calls.

Providers MAY comply with RFC6881 for handling of emergency calls.
In addition, they MUST:

o Accept RUE emergency calls complying with the specifications in
   this document;

o Recognize such calls as emergency calls and properly handle them
   as such;

o Address other behavior not specified by RFC6881 as specified in
   Section 6.2.

Specifically, if the emergency call is to be handled using E9-1-1
(VPC) procedures, the Provider is responsible for modifying the
INVITE to conform to the VPC requirements. In this case, location
MAY be extracted from the RFC6881 conformant INVITE and used to
propagate it to the VPC where possible with the emergency call.
Because the RUE may have a more accurate and timely location of the
device than the typical manual entry location for nomadic RUE
devices, the RUE MUST send a Geolocation header containing its
location in the REGISTER request if the configuration specifies it.
The Provider MAY use that information to populate the location of the
device in the VPC before any emergency call.

6.3. Mid Call Signaling

The RUE and Providers MUST support re-INVITE to renegotiate media
session parameters (among other uses). Per Section 8, the RUE MUST,
and providers SHOULD, be able to support an INFO request for full
frame refresh for devices in a call with the RUE that do not support
RTCP mechanisms (please refer to Section 8.3). The RUE MUST support
REFER to enable call transfer.

6.4. URI Representation of Phone Numbers

SIP URIs constructed from non-URI sources (dial strings) and sent to
SIP proxies by the RUE MUST be represented as follows, depending on
whether they can be represented as an E.164 number.

A dial string that can be written as an E.164 formatted phone number
MUST be represented as a SIP URI with a URI ";user=phone" tag. The
user part of the URI MUST be in conformance with 'global-number'
defined in [RFC3966]. The user part MUST NOT contain any 'visual-
separator' characters.

Dial strings that cannot be written as E.164 numbers MUST be
represented as dialstring URIs, as specified by [RFC4967], e.g.,
sip:411@red.example.net;user=dialstring.

Relay Service URIs and User Address of Records (AoR) MUST resolve (in
accord with [RFC3263]) to globally routable IPv4 addresses. The AoRs
MAY also resolve to IPv6 addresses.

6.5. NAT Traversal

The RUE MUST support ICE [RFC5245] and MUST be able to use STUN
[RFC5389] and TURN [RFC5766] servers, when specified in the
configuration. If a STUN or TURN server issues a challenge for
digest credentials, the RUE MUST attempt to continue using matching
credentials from the configuration.

Providers MAY operate STUN and TURN servers for RUEs to use (please
refer to Section 11.2 for configuration). Alternatively, providers
MAY use Back to Back User Agents to modify media end points to
achieve NAT traversal. This may involve media relays.

The RUE and providers MUST support SIP outbound [RFC5626] (please
also refer to Section 6.1).

7. Media

7.1. Text-Based Communication

Real-time text support by Providers is OPTIONAL as described in
Section 2.

The RUE MUST and Providers SHOULD support real-time text ([RFC4102]
and [RFC4103]) via T.140 media. One original and two redundant
generations MUST be transmitted and supported, with a 300 ms
transmission interval.

7.2. Video Codecs

The RUE and Providers MUST implement the video/H.264 [RFC6184]
Constrained Baseline Profile, Level 1.3, packetization mode 1. H.265
Main Profile, Level 2.1 or better MAY be supported.

7.3. **Audio Codecs**

   The RUE and Providers MUST support G.711 mu-law. Providers SHOULD,
   and the RUE MUST, support G.722. In addition, G.722.1 and/or G.722.2
   MAY also be supported.

7.4. **DTMF Digits**

   The RUE and Providers MUST support the "audio/telephone-event"
   [RFC4733] media type. They MUST support conveying event codes 0
   through 11 (DTMF digits "0"-"9", "*","#") defined in Table 7 of
   [RFC4733]. Handling of other tones is OPTIONAL.

7.5. **Session Description Protocol**

   The SDP offers and answers MUST conform to the Offer/Answer
   Section of the VRS US Provider Profile [pip] document.

7.6. **Privacy**

   The RUE MUST be able to control privacy of the user by implementing a
   one-way mute of audio and or video, without signaling, locally, but
   MUST maintain any NAT bindings by periodically sending media packets
   on all active media sessions containing silence/comfort noise/black
   screen/etc. per [RFC6263].

8. **SRTP and SRTCP**

   All media streams between the RUE and another endpoint or relay
   Provider MUST be exchanged using the secure real-time transport
   protocol (SRTP) [RFC3550] using DTLS [RFC5763], [RFC5764], except
   that for backwards compatibility with older video endpoints, RTP MAY
   be negotiated if SRTP negotiation fails. All SRTP/RTP and SRTCP/RTCP
   traffic over UDP MUST use symmetric RTP [RFC4961]. Receivers of
   SRTP/RTP traffic MUST be capable of processing SRTP/RTP packets with
   a different packetization rate than the rate used for sending.

8.1. **Bandwidth Negotiation Flow Control and Media Performance**

   The RUE and Providers MUST support codec control messages as
   described in [RFC5104]. During a call, codec control messages SHOULD
   be used to negotiate maximum bitrate. Specifically, Temporary
   Maximum Media Stream Bit Rate Request (TMMBR) SHOULD be used where
   endpoints have detected the need to decrease or increase the bit
   rate. Where either side of a session does not support CCM TMMBR, re-
   INVITE messages MAY be used during a call to renegotiate the use of
   bandwidth.

8.2. **SRTP / SAVPF Profile for SRTCP Feedback**

   The RUE and Providers MUST support the SRTP/SAVPF profile per
   [RFC4585] for SRTCP feedback support. Supporting the SRTP/SAVPF
   profile allows implementations to use advanced RTCP mechanisms, like
   indicating packet loss, requesting intra frame, and temporary bitrate
   change indication, which are essential for video streams.

   Supported SAVPF messages MUST be declared by RTCP Feedback
   attributes. Because implementations convey media streams from RUEs
   of varying background, there may be situations when no SAVPF
   attributes are supported in a session.

   For calls to devices that do not support SAVPF, it is recommended to
   make an initial INVITE with "SAVPF". If some media are not accepted
   with that profile, then a re-INVITE SHOULD be made with AVP
   declaration on the non-accepted media and the other media unchanged.
   The only combinations required are SAVPF and AVP.

8.3. **Negative Acknowledgment, Packet Loss Indicator, and Full
       Intraframe Request Features**

   NACK SHOULD be used when negotiated and conditions warrant its use.
   Signaling picture losses as Packet Loss Indicator (PLI) SHOULD be
   preferred, as described in [RFC5104].

   FIR SHOULD be used only in situations where not sending a decoder
   refresh point would render the video unusable for the users, as per
   RFC5104 subsection 4.3.1.2.

   For backwards compatibility with calling devices that do not support
   the foregoing methods, the RUE MUST implement and use SIP INFO
   messages to send and receive XML encoded Picture Fast Update messages
   according to [RFC5168].

9. **Contacts**

9.1. **CardDAV Login and Synchronization**

   Support of CardDAV by Providers is OPTIONAL, as described in
   Section 2.

   The RUE MUST and Providers MAY be able to synchronize the user's
   contact directory between the RUE endpoint and one maintained by the
   user's VRS provider using CardDAV ([RFC6352] and [RFC6764]).

   The configuration MAY supply a username and domain identifying a
   CardDAV server and address book for this account.

To access the CardDAV server and address book, the RUE MUST follow
[Section 6 of RFC6764](), using the chosen username and domain in place
of an email address. If the request triggers a challenge for digest
authentication credentials, the RUE MUST attempt to continue using
matching "credentials" from the configuration. If no matching
credentials are configured, the RUE MUST use the SIP credentials from
the configuration. If the SIP credentials fail, the RUE MUST query
the user.

Synchronization using CardDAV MUST be a two-way synchronization
service, with proper handling of asynchronous adds, changes, and
deletes at either end of the transport channel.

9.2. Contacts Import/Export Service

Each Provider MUST supply a standard xCard import/export interface
and the RUE MUST be able to export/import the list of contacts in
xCard [RFC6351] XML format.

The RUE accesses this service via the "contacts" URI in the
configuration. The URL MUST resolve to identify a web server
resource that imports/exports contact lists for authorized users.

The RUE stores/retrieves the contact list (address book) by issuing
an HTTPS POST or GET request. If the request triggers a challenge
for digest authentication credentials, the RUE MUST attempt to
continue using matching "credentials" from the configuration. If no
credentials are configured, the RUE MUST query the user.

10. Mail Waiting Indicator (MWI)

Support of MWI by Providers is OPTIONAL, as described in [Section 2]()

The RUE MUST and Providers SHOULD support subscriptions to "message-
summary" events [RFC3842] to the URI specified in the configuration
if the Provider supports message waiting indicator on any endpoint.

In notification bodies, videomail messages SHOULD be reported using
"message-context-class multimedia-message" defined in [RFC3458].

11. Provisioning and Provider Selection

11.1. RUE Provider Selection

To allow the user to select a relay service, the RUE MAY obtain, on
startup, a list of Providers from a configured accessible URL.

The provider list, formatted as JSON, contains:

   o Version: Specifies the version number of the Provider list format.
      A new version number SHOULD only be used if the new version is not
      backwards-compatible with the older version. A new version number
      is not needed if new elements are optional and can be ignored by
      older implementations.

   o Providers: An array where each entry describes one Provider. Each
      entry consists of the following items:

      * name: This parameter contains the text label identifying the
         Provider and is meant to be displayed to the human VRS user.

      * domain: The domain parameter is used for configuration purposes
         by the RUE (as discussed in Section 11.2) and as the domain to
         use when targeting one-stage dial-around calls to this Provider
         (as discussed in Section 6.2.2).

      * operator: (OPTIONAL) The operator parameter is a SIP URL that
         identifies the operator "front-door" that VRS users may contact
         for manual (two-stage) dial-around calls.

   The VRS user interacts with the RUE to select from the Provider list
   one or more Providers with whom the user has already established an
   account.

```
  {
    "version": 1,
    "providers": [
      {
        "name": "Red",
        "domain": "red.example.net",
        "operator": "sip:operator@red.example.net"
      },
      {
        "name": "Green",
        "domain": "green.example.net",
        "operator": "sip:+18885550123@green.example.net;user=phone"
      },
      {
        "name": "Blue",
        "domain": "blue.example.net"
      }
    ]
  }
```

                    Example of a Provider list JSON object

11.2. **RUE Configuration Service**

   The RUE is provisioned with one or more URIs that may be queried for
   configuration with HTTPS.

   The data returned will include a set of key/value configuration
   parameters to be used by the RUE, formatted as a JSON object and
   identified by the associated [RFC7159] "application/json" MIME type,
   to allow for other formats in the future.

   The configuration data payload includes the following data items.
   Items not noted as (OPTIONAL) are REQUIRED. If other unexpected
   items are found, they MUST be ignored.

   o version: Identifies the version of the configuration data format.
      A new version number SHOULD only be used if the new version is not
      backwards-compatible with the older version. A new version number
      is not needed if new elements are optional and can be ignored by
      older implementations.

   o lifetime: Specifies how long (in seconds) the RUE MAY cache the
      configuration values.

   o display-name: (OPTIONAL) A user-friendly name to identify the
      subscriber when originating calls.

   o phone-number: The telephone number (in E.164 format) assigned to
      this subscriber. This becomes the user portion of the SIP URI
      identifying the subscriber.

   o provider-domain: The DNS domain name of the default Provider
      servicing this subscriber.

   o outbound-proxies: (OPTIONAL) A list of URIs of SIP proxies to be
      used when sending requests to the Provider. Multiple URIs
      identify alternative (redundant) paths to the Provider.

   o mwi: (OPTIONAL) A URI identifying a SIP event server that
      generates "message-summary" events for this subscriber.

   o videomail: (OPTIONAL) A SIP URI that can be called to retrieve
      videomail messages.

   o contacts: An HTTPS URI that may be used to export (retrieve) the
      subscriber's complete contact list managed by the Provider.

   o carddav: (OPTIONAL) A username and domain name (separated by
      ""@"") identifying a "CardDAV" server and user name that can be

used to synchronize the RUE's contact list with the contact list
managed by the Provider.

o sendLocationWithRegistration: True if the RUE should send a
   Geolocation Header with REGISTER, false if it should not.
   Defaults to false if not present.

o ice-servers: (OPTIONAL) An array of URLs identifying STUN and TURN
   servers available for use by the RUE for establishing media
   streams in calls via the Provider.

o credentials: (OPTIONAL) An array of sets of credentials available
   for use in responding to SIP, HTTP, contacts, cardDAV, STUN, and
   TURN digest authentication challenges from specified realms. Each
   set consists of the following items:

   * realm: The realm to which this set of credentials applies.

   * username: The username field to be used in responding to a
      challenge.

   * password: The password to use in generating the response to the
      challenge.

```
{
  "version": 1,
  "lifetime": 86400,
  "display-name" : "Bob Smith",
  "phone-number": "+18135551212",
  "provider-domain": "red.example.net",
  "outbound-proxies": [
    "sip:p1.red.example.net",
    "sip:p2.red.example.net"
    ],
  "mwi": "sip:+18135551212@red.example.net",
  "videomail": "sip:+18135551212@vm.red.example.net",
  "contacts": "https://red.example.net:443/contacts/1dess45awd"
  "carddav": "bob@red.example.com" ,
  "sendLocationWithRegistration": false,
  "ice-servers": [
     {"stun:stun.l.google.com:19302" },
     {"turn:turn.red.example.net:3478"}
  ],
  "credentials": [
    {
      "realm": "red.example.net",
      "username": "bob",
      "password": "reg-pw"
```

```
      },
      {
        "realm": "proxies.red.example.net",
        "username": "bob",
        "password": "proxy-pw"
      },
      {
        "realm": "cd.red.example.net",
        "username": "bob",
        "password": "cd-pw"
      },
      {
        "realm": "vm.red.example.net",
        "username": "bob",
        "password": "vm-pw"
      },
      {
        "realm": "stun-turn.red.example.net",
        "username": "bob",
        "password": "stun-turn-pw"
      }
    ]
    }
```

                    Example JSON configuration payload

   The wire format of the data is in keeping with the standard JSON
   description in RFC7159.

   The "lifetime" parameter in the configuration indicates how long the
   RUE MAY cache the configuration values. If the RUE caches
   configuration values, it MUST cryptographically protect them. The
   RUE SHOULD retrieve a fresh copy of the configuration before the
   lifetime expires or as soon as possible after it expires. The
   lifetime is not guaranteed: the configuration may change before the
   lifetime value expires. In that case, the Provider MAY indicate this
   by generating authorization challenges to requests and/or prematurely
   terminating a registration.

   Note: In some cases, the RUE may successfully retrieve a fresh copy
   of the configuration using digest credentials cached from the prior
   retrieval. If this is not successful, then the RUE will need to ask
   the user for the username and password. Unfortunately, this
   authentication step might occur when the user is not present,
   preventing SIP registration and thus incoming calls. To avoid this
   situation, the RUE MAY retrieve a new copy of the configuration when
   it knows the user is present, even if there is time before the
   lifetime expires.

11.3. Schemas

The following JSON schemas are for the Provider List and the RUE
Configuration. These are represented using the JSON Content Rules
[JCR] schema notation.

```
{
  "version": 1,
  "providers": [
    1*
      {
       "name": string,
       "domain": fqdn,
       ?"operator":            ; "front-door" access to provider
           uri,                ; (sip uri)
           * /^.*$/ : any        ; (allow future extensions)
      }
    ] ,
    * /^.*$/ : any             ; (allow future extensions)
}
```

                    Provider List JSON Schema

```
  {
    "version": 1,             ; Interface version
    "lifetime": integer,      ; Deadline (in seconds) for
                              ; refreshing this config without
                              ; user input.
    "phone-number": /^\+[0-9]+$/ , ; E.164 phone number
                              ; for this user
    ?"display-name" : string,; display name for From: header
    "provider-domain": fqdn, ; SHOULD match that in Provider List
    ?"outbound-proxies": [ 1* : uri ], ; sip URIs
    ?"mwi": uri ,             ; sip URI for MWI subscriptions
    ?"videomail": uri ,       ; sip URI for videomail retrieval
    "contacts": uri ,         ; https URI for contact list retrieval
    ?"carddav": /^[^@]+@[^@]+$/ , ; for contact list synch
    ?"sendLocationWithRegistration": boolean , ; send location y/n
    ?"ice-servers":           ; (Required for ICE use)
       [ 1* : uri ],          ; (stun[s] & turn[s] URIs
    ?"credentials":           ; for digest authentication
      [ 1* {
        "realm": string,
        "username": string,
        "password": string
        } ],
    * /^.*$/ : any            ; (allow future extensions)
  }
```

                    RUE Configuration JSON Schema

   The following illustrates the message flow for retrieving a RUE
   automatic configuration using HTTPS Digest Authentication:

     ,¯.
     `_'
     /|\   ,---. ,---. ,-----------. ,----------------. ,---.
      | |RUE| |DNS| |HTTPS Server| | Provider | |CRM|
     / \ | | | | | | |Global Settings | | |
   RUE User `-+-'  `-+-' `-----+-----' `--------+-------' `-+-'
      | | | | | |
   [1] Select a VRS Provider name | | |
      | ------->| | | | |
      | | | | | |
   [2] NAPTR "SFUA.CFG" red.example.net | |
      | |----->| | | |
      | | | | | |
   [3] NAPTR "!.*!https://server.red.example.net/!" | |
      | |<-----| | | |
      | | | | | |
   [4] If NAPTR found, query DNS server.red.example.net |
```

```
      |           |----->|          |            |           |
      |           |      |          |            |           |
    [5] If NXDOMAIN, query DNS config.red.example.net   |       |
      |           | - - >|          |            |           |
      |           |      |          |            |           |
    [6] IP Address of Config Server   |          |           |
      |           |<-----|          |            |           |
      |           |      |          |            |           |
    [7] Establish TLS connection     |          |           |
      |           |<--------------->|            |           |
      |           |      |          |            |           |
    [8] HTTP: https://config.red.example.net/v1  |           |
      |           |--------------->|             |           |
      |           |      |          |            |           |
    [9] HTTP: 401 Unauthorized       |          |           |
        WWW-Authenticate Digest realm="Y" qop="auth,auth-int" nonce=|
      |           |<---------------|            |           |
      |           |      |          |            |           |
    [10] Query for userid/pw         |          |           |
      |<--------|        |          |            |           |
      |         |        |          |            |           |
    [11] User="bob", pw="bob's global provider pw"  |         |
      |-------->|        |          |            |           |
      |         |        |          |            |           |
    [12] HTTP: https://config.red.example.net/v1      |       |
      | Authorization Digest username="bob" realm="Y" qop="auth" |
      | nonce=... response="..." ...            |           |
      |           |--------------->|            |           |
      |           |      |          |            |           |
      |      [13] Find subscriber information for username="bob"  |
      |         |        |          |------------------------------>|
      |         |        |          |            |           |
      |      [14] Subscriber specific configuration information  |
      |         |        |          |<------------------------------|
      |         |        |          |            |           |
      |      [15] Retrieve provider specific settings    |       |
      |         |        |          |--------------->|       |
      |         |        |          |            |           |
      |      [16] Provider configuration information  |       |
      |         |        |          |<---------------|       |
      |         |        |          |            |           |
    [17] 200 OK + JSON merge subscriber + provider configs   |
      |           |<---------------|            |           |
      |           |      |          |            |           |
      RUE User   ,---.  ,---.  ,-----------. ,----------------.  ,---.
        ,-.      |RUE|  |DNS|  |HTTPS Server| |   Provider    | |CRM|
        `-'      |   |  |   |  |           | |Global Settings |  |   |
        /|\      `-+-'  `-+-'  `-----+------' `--------+-------'  `-+-'
```

```
        |
       / \
```

                        RUE Configuration Retrieval

12. Acknowledgements

13. IANA Considerations

   This memo includes no request to IANA.

14. Security Considerations

   The RUE is required to communicate with servers on public IP
   addresses and specific ports to perform its required functions. If
   it is necessary for the RUE to function on a corporate or other
   network that operates a default-deny firewall between the RUE and
   these services, the user must arrange with their network manager for
   passage of traffic through such a firewall in accordance with the
   protocols and associated SRV records as exposed by the Provider.
   Because VRS providers may use different ports for different services,
   these port numbers may differ from Provider to Provider.

15. Normative References

   [I-D.yusef-sipcore-digest-scheme]
              Shekh-Yusef, R., "The Session Initiation Protocol (SIP)
              Digest Authentication Scheme", draft-yusef-sipcore-digest-
              scheme-06 (work in progress), September 2017.

   [pip]   SIPForum, "VRS US Providers Profile TWG-6-1.0", 2015,
              <https://www.sipforum.org/download/
              vrs-us-providers-profile-twg-6-1-0-pdf/#>.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

   [RFC2392] Levinson, E., "Content-ID and Message-ID Uniform Resource
              Locators", RFC 2392, DOI 10.17487/RFC2392, August 1998,
              <https://www.rfc-editor.org/info/rfc2392>.

   [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston,
              A., Peterson, J., Sparks, R., Handley, M., and E.
              Schooler, "SIP: Session Initiation Protocol", RFC 3261,
              DOI 10.17487/RFC3261, June 2002,
              <https://www.rfc-editor.org/info/rfc3261>.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation
           Protocol (SIP): Locating SIP Servers", RFC 3263,
           DOI 10.17487/RFC3263, June 2002,
           <https://www.rfc-editor.org/info/rfc3263>.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model
           with Session Description Protocol (SDP)", RFC 3264,
           DOI 10.17487/RFC3264, June 2002,
           <https://www.rfc-editor.org/info/rfc3264>.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP)
           UPDATE Method", RFC 3311, DOI 10.17487/RFC3311, October
           2002, <https://www.rfc-editor.org/info/rfc3311>.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session
           Initiation Protocol (SIP)", RFC 3323,
           DOI 10.17487/RFC3323, November 2002,
           <https://www.rfc-editor.org/info/rfc3323>.

[RFC3326] Schulzrinne, H., Oran, D., and G. Camarillo, "The Reason
           Header Field for the Session Initiation Protocol (SIP)",
           RFC 3326, DOI 10.17487/RFC3326, December 2002,
           <https://www.rfc-editor.org/info/rfc3326>.

[RFC3327] Willis, D. and B. Hoeneisen, "Session Initiation Protocol
           (SIP) Extension Header Field for Registering Non-Adjacent
           Contacts", RFC 3327, DOI 10.17487/RFC3327, December 2002,
           <https://www.rfc-editor.org/info/rfc3327>.

[RFC3458] Burger, E., Candell, E., Eliot, C., and G. Klyne, "Message
           Context for Internet Mail", RFC 3458,
           DOI 10.17487/RFC3458, January 2003,
           <https://www.rfc-editor.org/info/rfc3458>.

[RFC3515] Sparks, R., "The Session Initiation Protocol (SIP) Refer
           Method", RFC 3515, DOI 10.17487/RFC3515, April 2003,
           <https://www.rfc-editor.org/info/rfc3515>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V.
           Jacobson, "RTP: A Transport Protocol for Real-Time
           Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550,
           July 2003, <https://www.rfc-editor.org/info/rfc3550>.

[RFC3605] Huitema, C., "Real Time Control Protocol (RTCP) attribute
           in Session Description Protocol (SDP)", RFC 3605,
           DOI 10.17487/RFC3605, October 2003,
           <https://www.rfc-editor.org/info/rfc3605>.

   [RFC3665]   Johnston, A., Donovan, S., Sparks, R., Cunningham, C., and
               K. Summers, "Session Initiation Protocol (SIP) Basic Call
               Flow Examples", BCP 75, RFC 3665, DOI 10.17487/RFC3665,
               December 2003, <https://www.rfc-editor.org/info/rfc3665>.

   [RFC3840]   Rosenberg, J., Schulzrinne, H., and P. Kyzivat,
               "Indicating User Agent Capabilities in the Session
               Initiation Protocol (SIP)", RFC 3840,
               DOI 10.17487/RFC3840, August 2004,
               <https://www.rfc-editor.org/info/rfc3840>.

   [RFC3842]   Mahy, R., "A Message Summary and Message Waiting
               Indication Event Package for the Session Initiation
               Protocol (SIP)", RFC 3842, DOI 10.17487/RFC3842, August
               2004, <https://www.rfc-editor.org/info/rfc3842>.

   [RFC3891]   Mahy, R., Biggs, B., and R. Dean, "The Session Initiation
               Protocol (SIP) "Replaces" Header", RFC 3891,
               DOI 10.17487/RFC3891, September 2004,
               <https://www.rfc-editor.org/info/rfc3891>.

   [RFC3892]   Sparks, R., "The Session Initiation Protocol (SIP)
               Referred-By Mechanism", RFC 3892, DOI 10.17487/RFC3892,
               September 2004, <https://www.rfc-editor.org/info/rfc3892>.

   [RFC3960]   Camarillo, G. and H. Schulzrinne, "Early Media and Ringing
               Tone Generation in the Session Initiation Protocol (SIP)",
               RFC 3960, DOI 10.17487/RFC3960, December 2004,
               <https://www.rfc-editor.org/info/rfc3960>.

   [RFC3966]   Schulzrinne, H., "The tel URI for Telephone Numbers",
               RFC 3966, DOI 10.17487/RFC3966, December 2004,
               <https://www.rfc-editor.org/info/rfc3966>.

   [RFC4102]   Jones, P., "Registration of the text/red MIME Sub-Type",
               RFC 4102, DOI 10.17487/RFC4102, June 2005,
               <https://www.rfc-editor.org/info/rfc4102>.

   [RFC4103]   Hellstrom, G. and P. Jones, "RTP Payload for Text
               Conversation", RFC 4103, DOI 10.17487/RFC4103, June 2005,
               <https://www.rfc-editor.org/info/rfc4103>.

   [RFC4566]   Handley, M., Jacobson, V., and C. Perkins, "SDP: Session
               Description Protocol", RFC 4566, DOI 10.17487/RFC4566,
               July 2006, <https://www.rfc-editor.org/info/rfc4566>.

   [RFC4585] Ott, J., Wenger, S., Sato, N., Burmeister, C., and J. Rey,
              "Extended RTP Profile for Real-time Transport Control
              Protocol (RTCP)-Based Feedback (RTP/AVPF)", RFC 4585,
              DOI 10.17487/RFC4585, July 2006,
              <https://www.rfc-editor.org/info/rfc4585>.

   [RFC4733] Schulzrinne, H. and T. Taylor, "RTP Payload for DTMF
              Digits, Telephony Tones, and Telephony Signals", RFC 4733,
              DOI 10.17487/RFC4733, December 2006,
              <https://www.rfc-editor.org/info/rfc4733>.

   [RFC4961] Wing, D., "Symmetric RTP / RTP Control Protocol (RTCP)",
              BCP 131, RFC 4961, DOI 10.17487/RFC4961, July 2007,
              <https://www.rfc-editor.org/info/rfc4961>.

   [RFC4967] Rosen, B., "Dial String Parameter for the Session
              Initiation Protocol Uniform Resource Identifier",
              RFC 4967, DOI 10.17487/RFC4967, July 2007,
              <https://www.rfc-editor.org/info/rfc4967>.

   [RFC5104] Wenger, S., Chandra, U., Westerlund, M., and B. Burman,
              "Codec Control Messages in the RTP Audio-Visual Profile
              with Feedback (AVPF)", RFC 5104, DOI 10.17487/RFC5104,
              February 2008, <https://www.rfc-editor.org/info/rfc5104>.

   [RFC5168] Levin, O., Even, R., and P. Hagendorf, "XML Schema for
              Media Control", RFC 5168, DOI 10.17487/RFC5168, March
              2008, <https://www.rfc-editor.org/info/rfc5168>.

   [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment
              (ICE): A Protocol for Network Address Translator (NAT)
              Traversal for Offer/Answer Protocols", RFC 5245,
              DOI 10.17487/RFC5245, April 2010,
              <https://www.rfc-editor.org/info/rfc5245>.

   [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security
              (TLS) Protocol Version 1.2", RFC 5246,
              DOI 10.17487/RFC5246, August 2008,
              <https://www.rfc-editor.org/info/rfc5246>.

   [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing,
              "Session Traversal Utilities for NAT (STUN)", RFC 5389,
              DOI 10.17487/RFC5389, October 2008,
              <https://www.rfc-editor.org/info/rfc5389>.

[RFC5393] Sparks, R., Ed., Lawrence, S., Hawrylyshen, A., and B.
           Campen, "Addressing an Amplification Vulnerability in
           Session Initiation Protocol (SIP) Forking Proxies",
           RFC 5393, DOI 10.17487/RFC5393, December 2008,
           <https://www.rfc-editor.org/info/rfc5393>.

[RFC5626] Jennings, C., Ed., Mahy, R., Ed., and F. Audet, Ed.,
           "Managing Client-Initiated Connections in the Session
           Initiation Protocol (SIP)", RFC 5626,
           DOI 10.17487/RFC5626, October 2009,
           <https://www.rfc-editor.org/info/rfc5626>.

[RFC5658] Froment, T., Lebel, C., and B. Bonnaerens, "Addressing
           Record-Route Issues in the Session Initiation Protocol
           (SIP)", RFC 5658, DOI 10.17487/RFC5658, October 2009,
           <https://www.rfc-editor.org/info/rfc5658>.

[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, DOI 10.17487/RFC5763, May
           2010, <https://www.rfc-editor.org/info/rfc5763>.

[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,
           DOI 10.17487/RFC5764, May 2010,
           <https://www.rfc-editor.org/info/rfc5764>.

[RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using
           Relays around NAT (TURN): Relay Extensions to Session
           Traversal Utilities for NAT (STUN)", RFC 5766,
           DOI 10.17487/RFC5766, April 2010,
           <https://www.rfc-editor.org/info/rfc5766>.

[RFC5954] Gurbani, V., Ed., Carpenter, B., Ed., and B. Tate, Ed.,
           "Essential Correction for IPv6 ABNF and URI Comparison in
           RFC 3261", RFC 5954, DOI 10.17487/RFC5954, August 2010,
           <https://www.rfc-editor.org/info/rfc5954>.

[RFC6184] Wang, Y., Even, R., Kristensen, T., and R. Jesup, "RTP
           Payload Format for H.264 Video", RFC 6184,
           DOI 10.17487/RFC6184, May 2011,
           <https://www.rfc-editor.org/info/rfc6184>.

[RFC6263]   Marjou, X. and A. Sollaud, "Application Mechanism for
            Keeping Alive the NAT Mappings Associated with RTP / RTP
            Control Protocol (RTCP) Flows", RFC 6263,
            DOI 10.17487/RFC6263, June 2011,
            <https://www.rfc-editor.org/info/rfc6263>.

[RFC6351]   Perreault, S., "xCard: vCard XML Representation",
            RFC 6351, DOI 10.17487/RFC6351, August 2011,
            <https://www.rfc-editor.org/info/rfc6351>.

[RFC6352]   Daboo, C., "CardDAV: vCard Extensions to Web Distributed
            Authoring and Versioning (WebDAV)", RFC 6352,
            DOI 10.17487/RFC6352, August 2011,
            <https://www.rfc-editor.org/info/rfc6352>.

[RFC6442]   Polk, J., Rosen, B., and J. Peterson, "Location Conveyance
            for the Session Initiation Protocol", RFC 6442,
            DOI 10.17487/RFC6442, December 2011,
            <https://www.rfc-editor.org/info/rfc6442>.

[RFC6665]   Roach, A., "SIP-Specific Event Notification", RFC 6665,
            DOI 10.17487/RFC6665, July 2012,
            <https://www.rfc-editor.org/info/rfc6665>.

[RFC6764]   Daboo, C., "Locating Services for Calendaring Extensions
            to WebDAV (CalDAV) and vCard Extensions to WebDAV
            (CardDAV)", RFC 6764, DOI 10.17487/RFC6764, February 2013,
            <https://www.rfc-editor.org/info/rfc6764>.

[RFC6881]   Rosen, B. and J. Polk, "Best Current Practice for
            Communications Services in Support of Emergency Calling",
            BCP 181, RFC 6881, DOI 10.17487/RFC6881, March 2013,
            <https://www.rfc-editor.org/info/rfc6881>.

[RFC7159]   Bray, T., Ed., "The JavaScript Object Notation (JSON) Data
            Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March
            2014, <https://www.rfc-editor.org/info/rfc7159>.

Authors' Addresses

   Brian Rosen
   Mars, PA
   US

   Phone: +1 724 382 1051
   Email: br@brianrosen.net

Jim Malloy
The MITRE Corporation
McLean, VA
US

Phone: +1 703 983 2835
Email: jmalloy@mitre.org

Brett Henderson
The MITRE Corporation
McLean, VA
US

Phone: +1 619 758 6071
Email: brhenderson@mitre.org