rum
Internet-Draft
Intended status: Standards Track
Expires: 26 February 2021

B. Rosen
25 August 2020

Interoperability Profile for Relay User Equipment
draft-ietf-rum-rue-03

Abstract

Video Relay Service (VRS) is a term used to describe a method by which a hearing persons can communicate with deaf/Hard of Hearing user using an interpreter ("Communications Assistant") connected via a videophone to the deaf/HoH user and an audio telephone call to the hearing user. The CA interprets using sign language on the videophone link and voice on the telephone link. Often the interpreters may be supplied by a company or agency termed a "provider" in this document. The provider also provides a video service that allows users to connect video devices to their service, and subsequently to CAs and other dead/HoH users. It is desirable that the videophones used by the deaf/HoH/H-I user conform to a standard so that any device may be used with any provider and that video calls direct between deaf/HoH users work. This document describes the interface between a videophone and a provider.

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.

Both deaf/HoH to provider (interpreted) and direct deaf/HoH to deaf/HoH calls are supported on this interface. While there are some accommodations in this document to maximize backwards compatibility with devices and services that conform to this document, backwards compatibility is not a requirement, and some interwork may be required to allow direct video calls to older devices. This document only describes the interface between the device and the provider, and not any other interface the provider may have.

2. 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". 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-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.

RUE Interface: the SIP interface between a RUE and the provider who supports it

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.

3. 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]

4. General Requirements

All HTTP/HTTPS connections specified throughout this document MUST use HTTPS. Both HTTPS and all SIP connections MUST use TLS conforming to at least [RFC7525] and must support [RFC8446]

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

5. SIP Signaling

Implementations of the RUE Interface 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 the above documents the RUE device conforms to the requirements of a SIP user Agent, and the provider conforms to the requirements of Registrar and Proxy Server where the document specifies different behavior for different roles. The only requirement on providers for RFC6655 (Events) is support for the Message Waiting Indicator (See Section Section 8), which is optional and providers not supporting MWI need not support RFC6665.

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

Implementations 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.

5.1. Registration

The RUE MUST register with a SIP registrar, following [RFC3261] and [RFC5626] at a provider it has an account with. 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 all implementations 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 is OPTIONAL.

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.

5.2. Session Establishment

5.2.1. Normal Call Origination

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

A RUE device MUST routes all outbound calls through an outbound proxy if configured.

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 all implementations. An anonymous call is signaled per [RFC3323].

The From-URI MUST be formatted as specified in Section 5.4, 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 9.2.)

Negotiated media MUST follow the guidelines specified in Section 6 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.

5.2.2. One-Stage Dial-Around Origination

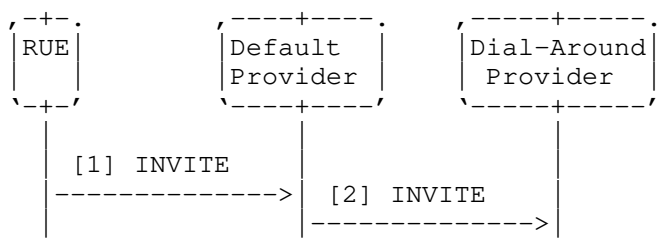
Outbound dial-around calls allow a RUE user to select any Provider to provide interpreting services for any call. "Two-stage" dial-around calls involve the RUE calling a telephone number that reaches the dial-around Provider and using signing or DTMF to provide the called party telephone number. In two-stage 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 5.2.1 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 9.1.

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:

One Stage Dial-Around



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
```

Figure 1

5.2.3. 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 a jCard [RFC7095]. 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").

5.2.4. 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.

5.2.5. Emergency Calls

Implementations MUST conform to [RFC6881] for handling of emergency calls, except that if the device is unable to determine its own location, it MAY send the emergency call without a Geolocation header and without a Route header (since it would be unable to query the LoST server for a route per RFC6881). If an emergency call arrives at the provider without a Geolocation header, the provider MUST supply location by adding the Geolocation header, and MUST supply the route by querying the LoST server with that location.

If the emergency call is to be handled using existing country specific procedures, the Provider is responsible for modifying the INVITE to conform to the country-specific requirements. In this case, location MAY be extracted from the RFC6881 conformant INVITE and used to propagate it to the appropriate country-specific entities. Because the RUE may have a more accurate and timely location of the device than the a manual entry location for nomadic RUE devices, but country-specific procedures require the location to be pre-loaded in some entity prior to placing an emergency call, implementations of a RUE device MAY send a Geolocation header containing its location in the REGISTER request if the configuration specifies it. That information MAY be used to populate the location to appropriate country-specific entities.

Implementations MUST implement Additional Data, [RFC7852]. RUE devices MUST implement Data Provider, Device Implementation and Owner/Subscriber Information blocks. Providers MUST implement Data Provider and Service Information blocks as the call is forwarded to the PSAP.

5.3. Mid Call Signaling

Implementations MUST support re-INVITE to renegotiate media session parameters (among other uses). Per Section 6.1, implementations MUST, be able to support an INFO request for full frame refresh for devices that do not support RTCP mechanisms (please refer to Section 6.8). Implementations MUST support an in-dialog REFER ([RFC3515] updated by [RFC7647] and including support for norefersub per [RFC4488]) with the Replaces header [RFC3891] to enable call transfer.

5.4. 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.

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

5.5. Transport

Implementations MUST conform to [I-D.ietf-rtcweb-transports] except that that this specification does not use the WebRTC data channel. See Section Section 6.2 for how RUE supports real time text without the data channel.

Implementations MUST support SIP outbound [RFC5626] (please also refer to Section 5.1).

6. Media

This specification adopts the media specifications for WebRTC ([I-D.ietf-rtcweb-overview]). Where WebRTC defines how interactive media communications may be established using a browser as a client, this specification assumes a normal SIP call. The RTP, RTCP, SDP and specific media requirements specified for WebRTC are adopted for this document. The RUE is a WebRTC non-browser" endpoint, except as noted expressly below.

The following sections specify the WebRTC documents to which conformance is required. "Mandatory to Implement" means a conforming implementation must implement the specified capability. It does not mean that the capability must be used in every session. For example, OPUS is a mandatory to implement audio codec, and all conforming implementations must support OPUS. However, implementation presenting a call across the RUE Interface where the call originates

in the Public Switched Telephone Network, or an older, non-RUE-compatible device, which only offers G.711 audio, does not need to include the OPUS codec in the offer, since it cannot be used with that call.

6.1. SRTP and SRTCP

Implementations MUST support [I-D.ietf-rtcweb-rtp-usage] except that MediaStreamTracks are not used. Implementations MUST conform to Section 6.4 of [I-D.ietf-rtcweb-security-arch].

6.2. Text-Based Communication

Implementations MUST 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. Note that this is not how real time text is transmitted in WebRTC and some form of transcoder would be required to interwork real time text in the data channel of WebRTC to RFC4103 real time text.

6.3. Video

Implementations MUST conform to [RFC7742] with the exception that, since backwards compatibility is desirable and older devices do not support VP8, that only H.264, as specified in [RFC7742] is Mandatory to Implement and VPB support is OPTIONAL at both the device and providers.

6.4. Audio

Implementations MUST conform to [RFC7874].

6.5. DTMF Digits

Implementations 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.

6.6. Session Description Protocol

The SDP offers and answers MUST conform [I-D.ietf-rtcweb-jsep] except that the RUE Interface uses SIP transport for SDP.

6.7. 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].

6.8. 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, implementations MUST implement SIP INFO messages to send and receive XML encoded Picture Fast Update messages according to [RFC5168].

7. Contacts

7.1. CardDAV Login and Synchronization

Support of CardDAV by Providers is OPTIONAL.

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.

7.2. Contacts Import/Export Service

Implementations MUST be able to export/import the list of contacts in jCard [RFC7095] json 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.

8. Mail Waiting Indicator (MWI)

Support of MWI by Providers is OPTIONAL

Implementations MUST support subscriptions to "message-summary" events [RFC3842] to the URI specified in the configuration.

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

9. Provisioning and Provider Selection

To simplify how users interact with RUE devices, the RUE interface defines a provisioning mechanism which consist of files stored on server that are retrieved by the RUE device. Two files are supported: one provides a directory of providers so that a user interface that allows easy provider selection either for registering or for dial-around. The other file provides configuration data for the device. The RUE device would retrieve these files at boot time. No mechanism for creating the files are specified. Each of the files contains a single json object. The retrieval mechanism is HTTPS download of that object from a provisioned location.

9.1. 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. This file is MAY be a single file per country, containing all the providers authorized in that country, but MAY be any collection of providers.

The provider list, formatted as JSON, contains:

* 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.

* 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 9.2) and as the domain to use when targeting one-stage dial-around calls to this Provider (as discussed in Section 5.2.2).

  - 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.

Example of a Provider list JSON object

```
{
  "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"
    }
  ]
}
```

Figure 2

9.2. RUE Configuration Service

A RUE device may retrieve a configuration from a provisioned URL using HTTPs.

The data returned will include a set of key/value configuration parameters to be used by the RUE, formatted as a single 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.

* 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.

* lifetime: Specifies how long (in seconds) the RUE MAY cache the configuration values. Values may not be valid when lifetime expires. Emergency Calls MUST continue to work.

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

* 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.

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

* outbound-proxies: (OPTIONAL) A URI of a SIP proxy to be used when sending requests to the Provider.

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

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

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

* 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.

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

* 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.

* credentials: (OPTIONAL) TBD

Example JSON configuration payload

```
{
  "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"
    }
  ]
  }
```

Figure 3

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.

9.3. Schemas

The following JSON schemas are for the Provider List and the RUE Configuration.

Provider List JSON Schema

```
{
    "$schema": "http://json-schema.org/draft-07/schema",
    "type": "object",
    "title": "Providers schema",
    "description": "List of Providers",
    "required": [
        "version",
        "providers"
    ],
    "properties": {
        "version": {
            "type": "number",
            "description": "Version of this schema",
        },
        "providers": {
            "type": "array",
            "description": "provider list as an array.",
            "items": {
                "required": [
                   "name",
                   "domain"
                ],
                "properties": {
                    "name": {
                       "type": "string",
                       "description": "Display Name",
                    },
                    "domain": {
                       "type": "string",
                       "description":
                          "domain name used with config file",
                   },
                   "operator": {
                      "type": "string",
                      "description":
                         "SIP URI for dial-around",
                   }
                }
            }
        }
    }
 }
```

Figure 4

RUE Configuration JSON Schema

```
   {
       "$schema": "http://json-schema.org/draft-07/schema",
       "title": "The root schema",
       "description": "RUE Configuration File",
       "required": [
           "version",
           "lifetime",
           "phone-number",
           "provider-domain",
           "carddav",
       ],
       "properties": {
           "version": {
               "type": "number",
               "description": "Version of this schema",
           },
           "lifetime": {
               "type": "integer",
               "description":
                  "how long (in seconds) the RUE MAY cache the configuration valu
es",
           },
           "display-name": {
               "type": "string",
               "description":
                  "A user-friendly name to identify the subscriber when originati
ng calls",
           },
           "phone-number": {
               "type": "string",
               "description":
                  "The telephone number (in E.164 format) assigned to this subscr
iber",
           },
           "provider-domain": {
               "type": "string",
               "description":
                  "The DNS domain name of the default Provider servicing this sub
scriber",
           },
           "outbound-proxies": {
               "type": "array",
               "description":
                  "List of URIs of SIP proxies to be used when sending requests t
o the Provider",
               "items": {
                    "type": "string",
                    "format": "uri"
               }
           },
           "mwi": {
               "type": "string",
               "format": "uri",
```

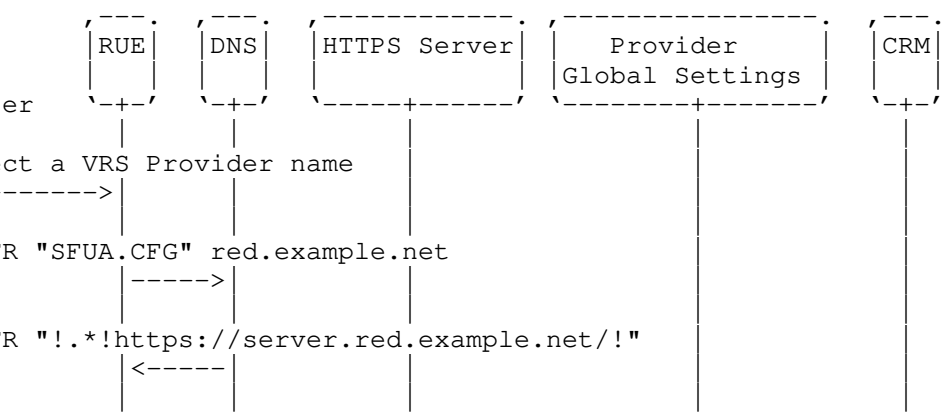
```
                "description":
                   "A URI of a SIP event server that generates message-summary eve
nts",
            },
            "videomail": {
                "type": "string",
                "format": "uri",
                 "description":
                    "A SIP URI that can be called to retrieve videomail messages",
            },
            "contacts": {
                "$id": "#/properties/contacts",
                "type": "string",
                "format": "uri",
                "description":
                   "An HTTPS URI used to manage the subscriber's contact list at t
he Provider.",
             },
            "carddav": {
                "type": "string",
                "description":
                   "A username and domain name (separated by @) identifying a Card
DAV server",
             },
            "sendLocationWithRegistration": {
                "type": "boolean",
                "description":
                   "True if the RUE should send a Geolocation Header with REGISTER
",
                "default": false,
            },
            "ice-servers": {
                "type": "array",
                "description":
                   "An array of URLs identifying STUN and TURN servers available",
                "items": {
                  "type": "object",
                  "properties": {
                    "servertype": {
                       "type": "string"
                    },
                    "url": {
                       "type": "string"
                    }
                  }
                }
            },
            "credentials": {
                "type": "array",
                "description": "registration credentials",
                "additionalItems": true,
                "items": {
```

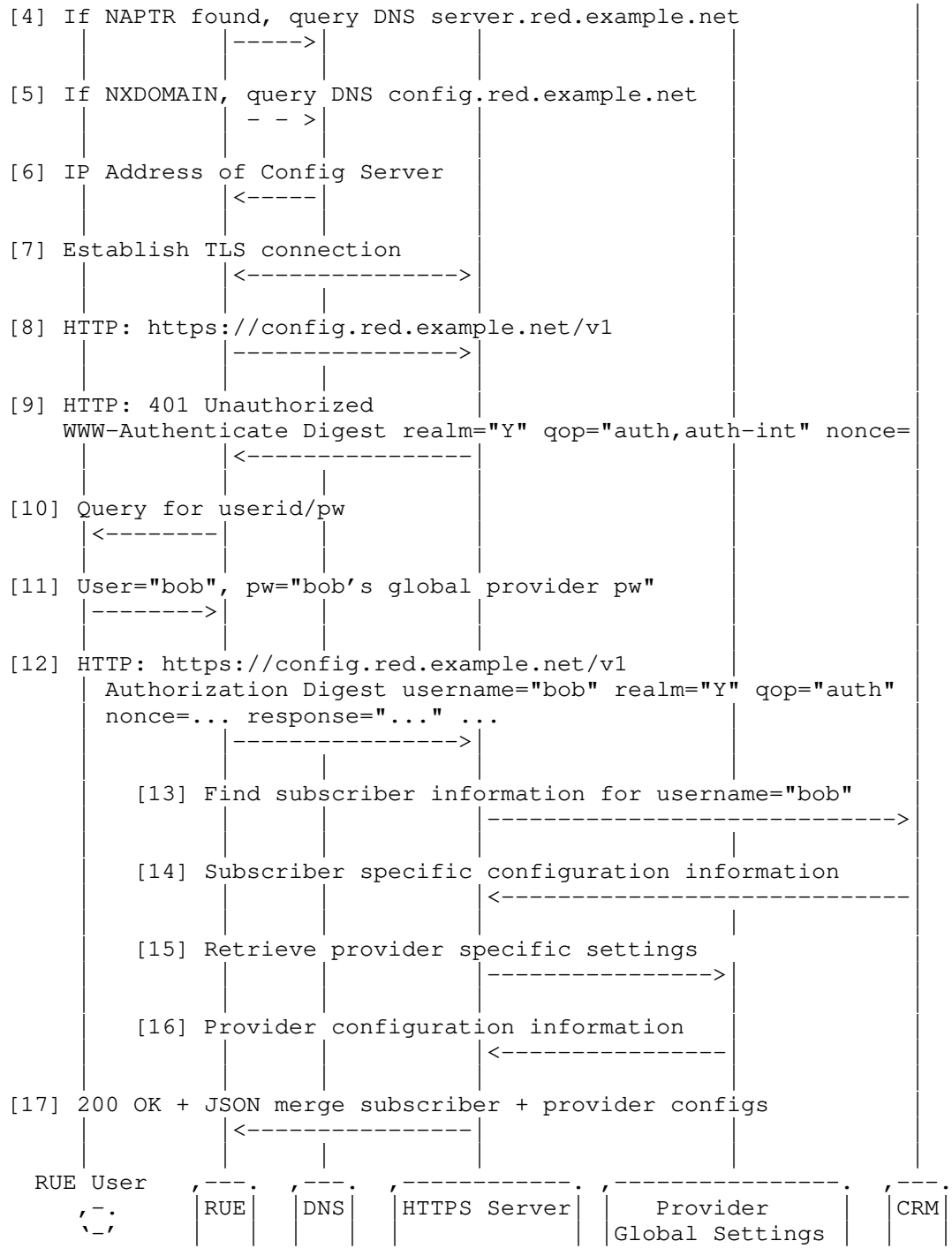
```
                "type": "object",
                "required": [
                   "realm",
                   "username",
                   "password"
                ],
                "properties": {
                   "realm": {
                      "type": "string",
                      "description":
                         "domain of provider matching domain in provider list",
                   },
                   "username": {
                      "type": "string",
                      "description": "username for registration"
                   },
                   "password": {
                      "type": "string",
                      "description": "password for registration",
                   }
                },
             }
          }
       },
   }
```

Figure 5

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

RUE Configuration Retrieval




[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 Global Settings
CRM

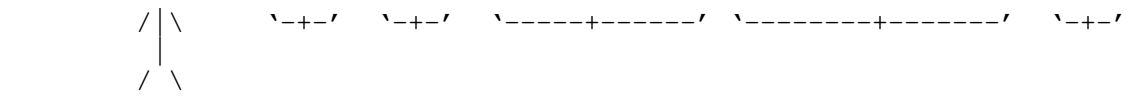


Figure 6

10. Acknowledgements

Brett Henderson and Jim Malloy provided many helpful edits to prior versions of this document.

11. IANA Considerations

This memo includes no request to IANA.

12. 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.

13. Normative References

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

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

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[RFC4488] Levin, O., "Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription", RFC 4488, DOI 10.17487/RFC4488, May 2006, <https://www.rfc-editor.org/info/rfc4488>.

[RFC7647] Sparks, R. and A.B. Roach, "Clarifications for the Use of REFER with RFC 6665", RFC 7647, DOI 10.17487/RFC7647, September 2015, <https://www.rfc-editor.org/info/rfc7647>.

[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>.

[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>.

[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>.

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

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[RFC7095] Kewisch, P., "jCard: The JSON Format for vCard", RFC 7095, DOI 10.17487/RFC7095, January 2014, <https://www.rfc-editor.org/info/rfc7095>.

[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>.

[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>.

[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>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[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>.

[RFC7852] Gellens, R., Rosen, B., Tschofenig, H., Marshall, R., and J. Winterbottom, "Additional Data Related to an Emergency Call", RFC 7852, DOI 10.17487/RFC7852, July 2016, <https://www.rfc-editor.org/info/rfc7852>.

[I-D.ietf-rtcweb-overview]
Alvestrand, H., "Overview: Real Time Protocols for Browser-based Applications", Work in Progress, Internet-Draft, draft-ietf-rtcweb-overview-19, 11 November 2017, <http://www.ietf.org/internet-drafts/draft-ietf-rtcweb-overview-19.txt>.

[I-D.ietf-rtcweb-rtp-usage]
Perkins, C., Westerlund, M., and J. Ott, "Web Real-Time Communication (WebRTC): Media Transport and Use of RTP", Work in Progress, Internet-Draft, draft-ietf-rtcweb-rtp-usage-26, 17 March 2016, <http://www.ietf.org/internet-drafts/draft-ietf-rtcweb-rtp-usage-26.txt>.

[I-D.ietf-rtcweb-jsep]
Uberti, J., Jennings, C., and E. Rescorla, "JavaScript Session Establishment Protocol", Work in Progress, Internet-Draft, draft-ietf-rtcweb-jsep-26, 27 February 2019, <http://www.ietf.org/internet-drafts/draft-ietf-rtcweb-jsep-26.txt>.

[RFC7874] Valin, JM. and C. Bran, "WebRTC Audio Codec and Processing Requirements", RFC 7874, DOI 10.17487/RFC7874, May 2016, <https://www.rfc-editor.org/info/rfc7874>.

[RFC7742] Roach, A.B., "WebRTC Video Processing and Codec Requirements", RFC 7742, DOI 10.17487/RFC7742, March 2016, <https://www.rfc-editor.org/info/rfc7742>.

[I-D.ietf-rtcweb-transports]
Alvestrand, H., "Transports for WebRTC", Work in Progress, Internet-Draft, draft-ietf-rtcweb-transports-17, 26 October 2016, <http://www.ietf.org/internet-drafts/draft-ietf-rtcweb-transports-17.txt>.

[I-D.ietf-rtcweb-security-arch]
Rescorla, E., "WebRTC Security Architecture", Work in Progress, Internet-Draft, draft-ietf-rtcweb-security-arch-20, 22 July 2019, <http://www.ietf.org/internet-drafts/draft-ietf-rtcweb-security-arch-20.txt>.

[I-D.yusef-sipcore-digest-scheme]
Shekh-Yusef, R., "The Session Initiation Protocol (SIP) Digest Authentication Scheme", Work in Progress, Internet-Draft, draft-yusef-sipcore-digest-scheme-07, 1 April 2019, <http://www.ietf.org/internet-drafts/draft-yusef-sipcore-digest-scheme-07.txt>.

[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/#>.

Author's Address

Brian Rosen
470 Conrad Dr
Mars, PA 16046
United States of America

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