DISPATCH P. Kyzivat, Ed.
Internet-Draft
Intended status: Informational H. Schulzrinne, Ed.
Expires: January 21, 2017 FCC
July 20, 2016

Interoperability Profile for Relay User Equipment (RUE)
draft-vrs-rue-dispatch-00

Abstract

This document defines and specifies a protocol profile defining an interface between a relay service endpoint used by a deaf or hard-of-hearing user and a relay service.

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 Relay User Equipment (RUE) profile is a profile of the Session Initiation Protocol (SIP) and related media protocols which enables end-user equipment registration and calling for video relay service (VRS) calls. It specifies the minimal set of call flows, 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 document defines a standard interface between a RUE and the services offered by relay service (RS) providers. This document does not enumerate the features that the RUE or relay service provider must support to meet, for example, national regulatory requirements.

3. Terminology

Communication Assistant (CA): The American Sign Language (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 particular form of communication that may be employed by two users, e.g., English voice, Spanish voice, American Sign Language, English lip reading, French real-time-text, or English MSRP instant messaging. Here, one communication modality is assumed to encompass both the language and the manner in which 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 video relay service provider.

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

Dial-around call: A relay call where the subscriber specifies the use of a video relay service provider other than one of the providers the subscriber is registered with. 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") or 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 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 (see: http://nationalnanpa.org)

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

PSTN UE: User equipment (UE) that interfaces with a human being via the PSTN, and mediates communication via voice. A telephone.

PSTN user: An individual using PSTN UE.

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. See [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 communication assistant 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, 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, 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: 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 as the default service for outgoing calls.

Relay user: See 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 which uses hand gestures and body language to convey meaning, including but not limited to American Sign Language (ASL).

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

Telecommunications relay services (TRS): (from the FCC): "Telephone transmission services that provide the ability for an individual who has a hearing or speech disability 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 or speech disability to communicate using voice communication services by wire or radio. Such term includes services that enable two-way communication between an individual who uses a text telephone or other nonvoice terminal device and an individual who does not use such a device, speech-to-speech services, video relay services and non-English relay services."

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. Normative Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

In many portions of this document, the document specifies a required implementation for an optional feature; i.e., that a provider's systems MAY implement a specific feature, and if they do, they MUST implement it in a specific way, in order to implement the functionality provided through this document.

5. General Requirements

All HTTP/HTTPS connections specified throughout this document MUST use HTTPS, and MUST use TLS 1.2 [RFC5246] or later, using a server-side certificate.

During the establishment of a TLS connection 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.

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.

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

6. Initial Selection, Configuration and Registration

6.1. RUE Provider Selection

In order to allow the user to select a relay service, the RUE SHALL obtain, on startup, a list of providers from a publicly accessible URL, e.g., hosted by the national regulatory agency. This provider will be used for outbound calls; the provider chosen for inbound calls is determined by the user's' E.164 number.

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 6.2) and also as the domain to use when targetting one-stage dial-around calls to this provider (as discussed in Section 11.2).

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 which 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"
    }
  ]
}
```


Figure 1: Example of a provider list

6.2. RUE Configuration Service

The RUE uses the following steps to obtain the configuration for each selected provider:

- o The RUE follows the mechanism described in [RFC6011] to construct a Configuration Request URL.

- o The RUE MUST use a "domain" specified in the Provider List as the Configuration Service Domain, taking precedence over other techniques specified in [RFC6011] for discovering the domain.

- o If the HTTPS request to the Configuration Service URL results in an authentication challenge, and the RUE has not cached credentials that satisfy the challenge, then it MUST interact with the VRS user for a userid and password with which to satisfy the challenge. The RUE MAY then cache resulting digest credentials, but MUST NOT cache the password.

This document extends [RFC6011] by describing a format for the configuration data.

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.

(As specified in section 2.3.2.1 of [RFC6011] the query for the configuration includes parameters that identify the RUE. The provider's configuration service MAY use these parameters to select distinct configurations for each RUE the user uses.)

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.

display-name: (Optional) An 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 list of URIs of SIP proxies to be used when sending requests the provider. Multiple URIs identify alternative (redundant) paths to to 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.

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) An array of sets of credentials available for use in responding to SIP, HTTP, 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.

Below is an example configuration payload.

NOTE: For document formatting reasons long quoted strings have been broken into multiple quoted strings separated by whitespace. This is solely for publication reasons - it is not valid JSON syntax.

```
{
      "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"
                  "/export/xcard" ,
      "carddav": "bob@red.example.com" ,
      "ice-servers": [
        "uri": "stun:stun.l.google.com:19302",
        "uri": "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 2: Example RUE configuration JSON object

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, but MUST do so in a cryptographically protected way. The RUE SHOULD retrieve a fresh copy of the configuration before the lifetime expires, or as soon as possible after it expires. However 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 retrieval of a fresh copy of the configuration may be successfully accomplished using digest credentials cached from the prior retrieval. If this is not the case, then it will be necessary to interact with the user to ask her for the user name 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 want to retrieve a new copy of the configuration when it knows the user is present, even when there is still plenty of time before the lifetime expires.

6.3. JSON Schemas

Below are JSON schemas 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)
}
```

Figure 3: 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
      ?"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)
}
```

Figure 4: RUE configuration JSON schema

Figure 5 illustrates the message flow for retrieving a configuration.

```
        ,-.
        `-'
        /|\     ,---.  ,---.  ,------------. ,----------------.  ,---.
         |      |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 |  |   |
        /|\     `-+-'  `-+-'  `-----+------' `--------+-------'  `-+-'
         |
        / \
```

Figure 5: Diagram of RUE automatic configuration using HTTPS Digest authentication

7. RUE SIP Registration

The RUE MUST register with a SIP registrar, following [RFC3261] and [RFC5626] and MUST use SIP-over-TLS. If the configuration 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 URI to be resolved by the RUE for sending the REGISTER request (from "outbound-proxies" if present, else the request-URI) MUST have a domain that is provisioned in DNS with NAPTR records that specify TLS as the preferred transport for SIP. For example a DNS NAPTR query for "sip:p1.red.example.net" 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
IN NAPTR 100 50 "s" "SIP+D2U"  "" _sip._udp.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 MUST authenticate using SIP MD5 digest authentication. The credentials to be used (username and password) MUST be supplied within the credentials section of the configuration, 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.

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.

Multiple simultaneous RUE SIP registrations from different RUE devices with the same SIP URI SHALL be permitted by the VRS 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 when it would cause an active call to be disconnected.

If a provider prematurely terminates a registration in order 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. For example, it could change the registration username/password and revoke cached authorization data so that further attempts by this RUE (or all RUEs) to register with this URI will require the end user of the RUE to re-login before it can fetch a configuration containing the new userid/password.

```
       ,-+-.   ,-+-.  ,------+------.
       |RUE|   |DNS|  |SIP Registrar|
       `-+-'   `-+-'  `------+------'
         |       |           |
   [1] Look up SRV DNS for _sip._tls.red.example.net
         |------>|           |
         |       |           |
   [2] SRV DNS response with red.example.net:5061
         |<------|           |
         |       |           |
   [3] Look up DNS A/CNAME for red.example.net
         |------>|           |
         |       |           |
   [4] IP Address(es) of SIP REGISTRAR Server(s)
         |<------|           |
         |       |           |
   [5] Establish TLS connection to registrar
         |<----------------->|
         |       |           |
   [6] SIP: REGISTER sip:red.example.net
       To: sip:+18135551212@red.example.net;...
       From: sip:+18135551212@red.example.net;...
         |------------------>|
         |       |           |
   [7] SIP: 401 Unauthorized
       WWW-Authenticate Digest realm="read.example.net"
         |  qop="auth,auth-int" nonce=...
         |<------------------|
         |       |           |
   [8] SIP: REGISTER sip_username@sip_domain
       Authorization Digest username="bob" realm="red.example.net"
         |  qop="auth" nonce=... response="..."
         |------------------>|
         |       |           |
   [9] 200 OK    |           |
         |<------------------|
         |       |           |
       ,-+-.   ,-+-.  ,------+------.
       |RUE|   |DNS|  |SIP Registrar|
       `---'   `---'  `-------------'
```

Figure 6: RUE SIP registration message flow

8. NAT Traversal

The RUE SHALL support ICE [RFC5245] and SHALL be able to use STUN [RFC5389] and TURN [RFC5766] servers, when provided, to generate ICE candidates. 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 (see Section 6.2 for configuration). Alternatively, providers MAY use media relaying for all relay and point-to-point calls.

The RUE MUST support SIP outbound [RFC5626] (also see Section 7).

9. RUE CardDAV Login and Synchronization

A RUE MUST 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]).

Support of CardDAV by providers is OPTIONAL.

The provider MAY include a "carddav" item in the configuration to supply a username and domain identifying a CardDAV server and address book for this account. If no "carddav" item is present, the RUE SHOULD use the "phone-number" and "provider-domain".

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 MAY query the user.

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

Figure 7 shows an example message flow for CardDAV synchronization.

```
      ,-.
      `-'
      /|\
       |      ,---.   ,---.  ,----------------.  ,---.
      / \     |RUE|   |DNS|  |CardDAV Service|  |CRM|
   RUE User   `-+-'   `-+-'  `-------+-------'  `-+-'
      |         |       |            |            |
```

```
   [1] Select a VRS Provider name      |            |
        | ------->|       |            |            |
        |         |       |            |            |
   [2] Lookup SRV _carddavs._tcp.red.example.net    |
        |         |------>|            |            |
        |         |       |            |            |
   [3]  |      SRV carddav.red.example.net:443      |
        |         |<------|            |            |
        |         |       |            |            |
   [4] resolve carddav.red.example.net |            |
        |         |------>|            |            |
        |         |       |            |            |
   [5]        IP Address of CardDAV Server          |
        |         |<------|            |            |
        |         |       |            |            |
   [6] Establish TLS connection to carddav.red.example.net:443
        |         |<------------------>|            |
        |         |       |            |            |
   [7] HTTP: (CardDAV request)         |            |
        |         |------------------->|            |
        |         |       |            |            |
   [8] HTTP: 401 Unauthorized          |            |
       WWW-Authenticate Digest         |            |
       realm="cd.red.example.net"      |            |
       qop="auth,auth-int" nonce=...   |            |
        |         |<-------------------|            |
        |         |       |            |            |
   [9] HTTP: (CardDAV request)         |            |
       Authorization Digest username="bob"          |
       realm="cd.red.example.net" qop="auth"        |
       nonce=... response="..."        |            |
        |         |------------------->|            |
        |         |       |            |            |
        |         |  [10] Sync address book         |
        |         |<.................>|<.........>|
        |         |       |            |            |
     RUE User   ,-+-.   ,-+-.  ,-------+-------.  ,-+-.
        ,-.     |RUE|   |DNS|  |CardDAV Service|  |CRM|
        `-'     `---'   `---'  `---------------'  `---'
        /|\
         |
        / \
```

Figure 7: RUE CardDAV message flow

10. Contacts Export Service

Each provider MUST provide a standard xCard export interface, and RUEs MUST be able to import the list of contacts in xCard [RFC6351] XML format.

The provider MUST supply a URI for access to this service via the "contacts" URI in the configuration. The URL MUST resolve to identify a web server resource that exports contact lists for authorized user.

The RUE MAY retrieve the contact list (address book) by issuing an HTTPS 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 MAY query the user.

Figure 8 shows an example message flow for contact list retrieval.

```
     ,-.
     `-'
     /|\
      |       ,---.   ,---.  ,--------------------------.  ,---.
     / \      |RUE|   |DNS|  |Contacts Export Web Service|  |CRM|
   RUE User   `-+-'   `-+-'  `-------------+-------------'  `-+-'
     |          |       |                  |                  |
[1] Select a VRS Provider name             |                  |
     | ------->|       |                   |                  |
     |          |       |                  |                  |
[2] resolve red.example.net                |                  |
     |          |------>|                  |                  |
     |          |       |                  |                  |
[3] IP Address of Web Server               |                  |
     |          |<------|                  |                  |
     |          |       |                  |                  |
[4] Establish TLS web connection to red.example.net           |
     |          |<------------------------>|                  |
     |          |       |                  |                  |
[5] HTTP: GET /contacts/export/xcard       |                  |
     |          |------------------------->|                  |
     |          |       |                  |                  |
[6] HTTP: 401 Unauthorized                 |                  |
    WWW-Authenticate Digest                |                  |
    realm="cd.red.example.net"             |                  |
    qop="auth,auth-int" nonce=...          |                  |
     |          |<-------------------------|                  |
     |          |       |                  |                  |
```

```
   [7] HTTP: GET /contacts/export/xcard      |                  |
       Authorization Digest username="bob"   |                  |
       realm="cd.red.example.net" qop="auth" |                  |
       nonce=... response="..."              |                  |
        |         |------------------------->|                  |
        |         |       |                  |                  |
        |         | [8] Find contacts for username="bob"        |
        |         |       |                  |----------------->|
        |         |       |                  |                  |
        |         | [9] Contacts list in xCard format           |
        |         |      (application/vcard+xml)                |
        |         |       |                  |<-----------------|
        |         |       |                  |                  |
        |         | [10] 200 OK              |                  |
        |         |<-------------------------|                  |
        |         |       |                  |                  |
     RUE User   ,-+-.   ,-+-.  ,-------------+-------------.  ,-+-.
        ,-.     |RUE|   |DNS|  |Contacts Export Web Service|  |CRM|
        `-'     `---'   `---'  `---------------------------'  `---'
        /|\
         |
        / \
```

Figure 8: Message flow for RUE contacts retrieval using xCard

11. SIP Session Establishment

11.1. RUE Normal Call Origination

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

The RUE SHALL route all calls through the outbound proxy of the default provider. INVITE requests used to initiate calls SHOULD NOT contain route headers except that one route header which addresses the outbound proxy MAY be added. The SIP URIs in the To field and the Request-URI MUST be formatted as specified in Section 13 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 From-URI MUST be formatted as specified in Section 13, using the phone-number and "provider-domain" from the configuration. It SHOULD also contain the display-name from the configuration, when present. (See Section 6.2.)

Negotiated media MUST follow the guidelines specified in Section 14 of this document.

11.2. Dial-Around

Only relay calls use dial around. If the dialed number is in the iTRS RND, the call is a point-to-point call and follows the procedures in Section 11.1.

For one-stage dial-around the RUE MUST follow the procedures in Section 11.1 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 6.1.

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>
```

Figure 9: Example of one-stage dial around call

11.3. RUE Normal Call Termination

After initial SIP registration, the RUE SHALL be reachable via their telephone number.

As per SIP [RFC3261] basic call flows, as shown in [RFC3665], in-bound SIP INVITEs SHALL be forwarded to the SIP-registered RUE.

All SIP registered RUE with the same SIP URI should receive the same parallel forked SIP INVITE so that they ring at the same time. The first RUE to reply with a 200 OK answers the call, and the other call branches should be CANCELed.

If no RUE has an active SIP registration or none of the RUE respond to the call during the ring period chosen by the provider, and a videomail service is available, the in-bound SIP INVITE SHALL be forwarded to the videomail service, as in, sip:+18135551212@vm.red.example.net.

11.4. Emergency Calls

RUEs MUST comply with [RFC6881] for handling of emergency calls, with the following exception:

- o location information MUST be conveyed with a "geo:" URI in a Geolocation header field, as defined in [RFC5870].

  (While section 4.1 of [RFC6442] prohibits this usage, the reasons for doing so do not apply to 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;

Other behavior not specified by [RFC6881] is specified by Section 11.

```
       ,-+-.         ,----+----.
       |RUE|         |Default  |
       |   |         |Provider |
       `-+-'         `----+----'
         |                |
         | [1] INVITE     |
         |--------------->|
         |                |
```

Message Details:

[1] INVITE Rue -> Default Provider

```
INVITE urn:service:sos SIP/2.0
Via: ...
Max-Forwards: ...
To: <urn:service:sos>
From: "Bob Smith" <sip:+18135551212@red.example.net;user=phone>
Call-ID: ...
Geolocation: <geo:40.6777,-111.915;u=0>
Geolocation-Routing: yes
Accept: application/sdp, application/pidf+xml
CSeq: ...
Contact: ...
Content-Type: application/sdp
Content-Length: ...

...Session Description Protocol (SDP) goes here
```

Figure 10: Example of emergency call set-up with geo URI

12. RUE Videomail

12.1. Mail Waiting Indicator (MWI)

If the provider includes an MWI URI in the configuration (see Section 6.2) then it MUST process a subscription to "message-summary" events [RFC3842] at that URI.

To subscribe to MWI the RUE SHOULD attempt to subscribe to "message-summary" events at the URI provided by configuration. If there is no URI in the configuration the RUE SHOULD NOT attempt to subscribe to "message-summary" events. (This differs from the default behavior implied in [RFC3842].)

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

12.2. Videomail Retrieval

To retrieve videomail, the RUE establishes a SIP session to the "videomail" URI in the configuration. (See Section 6.2.) The user interaction required to select messages to view is at the discretion of the provider; the provider MAY also offer other means, such as a web page, to view video mail.

13. 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. The 'hostport' [RFC3261] in the URI depends upon the provider's setup.

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

14. Media

14.1. Text-Based Communication

The RUE MUST support real-time text ([RFC4102],[RFC4103] and [RFC5194]) via T.140 media.

One original and two redundant generations SHALL be transmitted and supported, with a 300 ms transmission interval.

14.2. Video Codecs

The RUE must implement the video/H.264 [RFC6184] Constrained Baseline Profile, Level 1.3, packetization mode 1.

14.3. Audio Codecs

Both RUEs and providers MUST support G.711 mu-law and they SHOULD support G.722. In addition, G.722.1 and/or G.722.2 MAY also be supported.

14.4. DTMF Digits

The RUE and providers MUST offer and accept offers of the "audio/telephone-event" [RFC4733] media type. They MUST support conveying event codes 0 through 15 (DTMF digits "0"-"9", "A"-"D","*","#") defined in Table 7 of [RFC4733]. Handling of other tones is OPTIONAL.

15. RTP & RTCP

All media streams between the RUE and another endpoint or relay provider MUST be exchanged using the real-time transport protocol (RTP) as described in [RFC3550]. All RTP and RTCP traffic over UDP MUST use symmetric RTP [RFC4961]. Receivers of RTP traffic MUST be capable of processing RTP packets with a different packetization rate than the rate used for sending.

15.1. Bandwidth Negotiation Flow Control and Media Performance

During a call, codec control messages SHOULD be used as described in [RFC5104] 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 doesn't support CCM TMMBR, INVITE messages MAY be used during a call to renegotiate the use of bandwidth. Automatic bit rate control SHALL be applied on video for the purpose of enabling transmission of at least 30 frames of video per second with low latency and good video quality.

15.2. RTP / AVPF Profile for RTCP Feedback

Implementations SHOULD support the RTP/AVPF profile per [RFC4585] for RTCP feedback support, but MUST signal "RTP/AVP" in the SDP m-line for compatibility. Supporting the RTP/AVPF 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 AVPF messages MUST be declared by RTCP Feedback attributes. Since implementations convey media streams from RUEs of varying background, there may be situations when no AVPF attributes are supported in a session.

For complete support of both AVPF and AVP, it is recommended to make an initial INVITE with "AVPF". 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.

15.3. Negative Acknowledgement, Packet Loss Indicator, Full Intraframe Request

For calls with more than two parties, negative acknowledgement mode (NACK) SHOULD be used. With only two parties, NACK MAY be used if the round-trip latency time is low enough to allow it.

Signaling picture lossses 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 draft-ietf-avt-avpf-ccm-10 [draft-ietf-avt-avpf-ccm-10] section 4.3.1.2

If the above have not been negotiated because either side of the call cannot support it, SIP INFO messages MAY be used to send XML encoded Picture Fast Update messages according to [RFC5168].

16. IANA Considerations

This memo includes no request to IANA.

17. Security Considerations

The RUE is required to communicate with a number of servers on public IP addresses and specific ports in order to perform its required functions. If it is necessary for a subscriber to operate the client software on a corporate or other network which operates a default-deny firewall between the RUE and these services, the user will have to 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 RS provider. Because the VRS providers may use different ports for different services, these port numbers may be different from provider to provider.

18. Contributors

Contributions to this document have been made by:

Jay Ashworth, Grant Beckmann, Lorenzo Benoni, Ian Blenke, Scot Brooksby, Byron Caswell, Eugene Christensen, Brandon Dopf, Dennis Episkopos, Kadian Ferguson, Brendan Foley, James Hamlin, Dustin Laun, George Lee, John Martin, Bruce Mattie, Adam Montero, Andrew Mulitz, Tom Murillo, Jose Pereira, Peter Preinitz, Isaac Roach, Zarko Roganovic, Lydia Runnels, Steve Saunders, Ed Sayers, Jeremy Shaffner, Joshua Shaffner, Roger Slusser, Mike Strecker, Antonio Sweet, Kyle Vaught, Claudio Villalobos.

The completion of the document was facilitated by MITRE staff.

19. vCard Example

```
<vcards xmlns="urn:ietf:params:xml:ns:vcard-4.0">
<vcard>
  <fn><text>Billy Boberson</text></fn>
  <n>
    <surname>Boberson</surname>
    <given>Billy</given>
    <additional/>
    <prefix/>
    <suffix>ing. jr</suffix>
    <suffix>M.Sc.</suffix>
  </n>
  <lang>
    <parameters><pref><integer>1</integer></pref></parameters>
    <language-tag>en</language-tag>
  </lang>
  <tel>
    <parameters>
      <type>
        <text>work</text>
        <text>voice</text>
      </type>
    </parameters>
    <uri>tel:+1-206-656-9254;ext=102</uri>
  </tel>
  <tel>
    <parameters>
      <type>
        <text>work</text>
        <text>voice</text>
        <text>cell</text>
        <text>video</text>
      </type>
    </parameters>
    <uri>tel:+1-253-262-6501</uri>
  </tel>
</vcard>
</vcards>
```

Figure 11: vCard example

20. Normative References

[JCR] Newton, A. and P. Cordell, "A Language for Rules Describing JSON Content", draft-newton-json-content-rules-06 (work in progress), March 2016, <https://tools.ietf.org/html/draft-newton-json-content-rules-06>.

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

[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, <http://www.rfc-editor.org/info/rfc3261>.

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

[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, <http://www.rfc-editor.org/info/rfc3550>.

[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, <http://www.rfc-editor.org/info/rfc3665>.

[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, <http://www.rfc-editor.org/info/rfc3842>.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, DOI 10.17487/RFC3966, December 2004, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc4103>.

[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, <http://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, <http://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, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc5168>.

[RFC5194] van Wijk, A., Ed. and G. Gybels, Ed., "Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)", RFC 5194, DOI 10.17487/RFC5194, June 2008, <http://www.rfc-editor.org/info/rfc5194>.

[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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc5389>.

[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, <http://www.rfc-editor.org/info/rfc5626>.

[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, <http://www.rfc-editor.org/info/rfc5766>.

[RFC5870] Mayrhofer, A. and C. Spanring, "A Uniform Resource Identifier for Geographic Locations ('geo' URI)", RFC 5870, DOI 10.17487/RFC5870, June 2010, <http://www.rfc-editor.org/info/rfc5870>.

[RFC6011] Lawrence, S., Ed. and J. Elwell, "Session Initiation Protocol (SIP) User Agent Configuration", RFC 6011, DOI 10.17487/RFC6011, October 2010, <http://www.rfc-editor.org/info/rfc6011>.

[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, <http://www.rfc-editor.org/info/rfc6184>.

[RFC6351] Perreault, S., "xCard: vCard XML Representation", RFC 6351, DOI 10.17487/RFC6351, August 2011, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc6442>.

[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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc7159>.

Authors' Addresses

Paul Kyzivat (editor)

Email: pkyzivat@alum.mit.edu

Henning Schulzrinne (editor)
FCC
450 12th Street SW
Washington, DC 20554
US

Email: schulzrinne@cs.columbia.edu