Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 19 September 2025

C. Wendt
Somos
J. Peterson
Neustar

18 March 2025

SIP Call-Info Parameters for Rich Call Data (RCD)
draft-ietf-sipcore-callinfo-rcd-16

Abstract

This document describes a usage of the SIP Call-Info header field that incorporates Rich Call Data (RCD) associated with the identity of the ~~calling~~ originating party in order to provide to the ~~called~~ terminating party a description of the caller (including ~~or~~ details about the reason for the ~~call~~session).

RCD includes information about the caller beyond the telephone number such as a calling name, ~~or~~ a logo, photo, or jCard object representing the caller, which can help the called party decide ~~whether~~ how to ~~answer~~ handle the ~~phone~~session request. The elements defined for this purpose are intended to be extensible in order to accommodate related information about calls and to be compatible and complementary with the STIR/PASSporT RCD framework.

This document defines three new parameters 'call-reason', 'verified', and 'integrity' for the SIP Call-Info header field and also a new token ("jcard") for the 'purpose' parameter of the Call-Info header field. It also provides guidance on the use of the Call-Info 'purpose' parameter token, "icon".

Commenté [MB1]: Is this specific to the media session?

I would generalize

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 September 2025.

Table of Contents

1. Introduction

Signaling protocols in telephone networks have long supported the delivery of a 'calling name' from the originating side to the terminating side, though in practice, the terminating side is often left to derive a name from the calling-party number by consulting a local address book or an external database. SIP [RFC3261] similarly can carry a 'display-name' in the From header field value from the originating to terminating side, though it is an unsecured field that is not commonly trusted and is often replaced or ignored. The same can be considered true of information in the Call-Info header field in SIP.

To allow ~~calling~~ initiating parties to initiate, and ~~called~~ terminating parties to receive, a more comprehensive, deterministic, and extensible Rich Call Data (RCD) [I-D.ietf-stir-passport-rcd] for incoming ~~calls~~sessions, this document defines a new parameter ('call-reason') for the SIP Call-Info header field [RFC3261] and also a new token ("jcard") for the 'purpose' parameter of the Call-Info header field. For this document and depending on the policies of the communications system, a calling party could be either the end user device (e.g., a SIP user agent (UA)) or a network service as part of a telephone service provider. Similarly, a called party could be an end user device or the network telephone service provider acting on behalf of the recipient of the call.

In order to properly translate and communicate some of the authenticated and trusted properties of 'rcd' claims defined in [I-D.ietf-stir-passport-rcd], this document defines two other new parameters, 'verified' and 'integrity'. These parameters help translate RCD information that had been sent via a SIP network to, for example, a SIP entity on the edge of the network-to-network interface (NNI) that contains a verification service as defined in [RFC8224] and further defined specific to RCD information in [I-D.ietf-stir-passport-rcd]. The verification procedures include ~~the concepts of~~ successful verification of the "rcd" claims and can be correspondingly translated and represented in the Call-Info header field via these new parameters.

Used on its own, this specification assumes that the called party UA can trust the SIP network or the SIP provider to assign, deliver, and protect the correct RCD information as an end-to-end security policy. However, as is true in many interconnected communications services, this end-to-end trust cannot be guaranteed. Therefore, the recommended approach is that the entity inserting the Call-Info header field should also sign the caller information via STIR-defined protocol tools [RFC7340] for SIP [RFC8224] and specifically through the use of RCD or the "rcd" PASSporT defined in [I-D.ietf-stir-passport-rcd].

Commenté [MB2]: Can we remind what the definition of SIP network?

Commenté [MB3]: Can be separate/same

Alternatively, this specification can be utilized in conjunction with the protocols defined in [I-D.ietf-stir-passport-rcd] as part of the communications signaling path, specifically in the trusted UNI device interface at the terminating side as part of an authenticated, network-to-device, trusted signaling where a device may not have the ability to verify the "rcd" PASSporT, but it can receive the RCD information from the Call-Info header field as defined in this specification.

[RFC7852] provides a means of carrying additional data about callers for the purposes of emergency services (especially Section 4.4 (Owner/Subscriber Information) of [RFC7852]). This specification provides an overlapping functionality for non-emergency cases. Rather than overloading its "EmergencyCallData" Call-Info 'purpose' parameter value, this document defines a separate 'purpose' parameter for the more generic delivery of information via jCard [RFC7095]. This document borrows from [RFC7852] the capability to carry a data structure as a body, through the use of the "cid" URI scheme [RFC2392].

Commenté [MB4]: Do we need to say something about co-existence? Any guidance here?

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Overview

~~In t~~This document~~, we~~ provide~~s~~ a framework for the use of Call-Info header field to carry RCD in SIP [RFC3261]. The Call-Info header field (defined in [RFC3261], Section 20.9) defines a 'purpose' parameter. In addition to providing guidance on calling name practices and the use of the existing 'purpose' parameter token, "icon", this document expands on other types of RCD by defining a new 'purpose' token, "jcard", and three new parameters, 'call-reason', 'verified', and 'integrity' for the Call-Info header field to align with RCD as defined in the STIR framework [RFC8224] and with "rcd" PASSporTs defined in [I-D.ietf-stir-passport-rcd].

The 'purpose' parameter token "jcard" is used to associate RCD related to the identity of the calling party in the form of a jCard [RFC7095]. While there is a "card" token defined in [RFC3261] which could be considered to have an overlapping purpose, the "jcard" token is intended to denote the jCard profile defined in this document for use in the Call-Info header field for RCD. The choice of jCard in this specification is guided by two ~~things~~aspects. First, JSON has become the default and is generally the widely accepted, optimally supported format for transmission, parsing, and manipulation of data on IP networks, and jCard represents an extensible method of providing information about a person or business associated with a call. Second, jCard has been defined in [I-D.ietf-stir-passport-rcd] and has been adopted by PASSporT [RFC8225] because of the usage of JSON

a mis en forme : Surlignage

Web Tokens (JWT) [RFC7519].

The new Call-Info header field parameter 'call-reason' ~~provides a string or other object that~~ conveys the caller's intent or reason for calling to help the called party understand the context and intent of the call and why they may want to answer the call.

The new Call-Info header field parameter 'verified' provides an indication, with the value "true", to represent the results of the verification procedures that were performed by the sender of the Call-Info header field. The new Call-Info header field parameter 'integrity' provides a mechanism to associate an integrity hash string, as defined in Section 8.2 of [I-D.ietf-stir-passport-rcd] ~~in Section 8.2~~, that is associated with the content of the resource referenced by the URI represented in the Call-Info header field.

4. A Call-Info Framework for Carrying Rich Call Data

This specification extends the Call-Info header field to be compatible and complimentary to the RCD framework defined in [I-D.ietf-stir-passport-rcd]. Typically, a SIP-based ~~call~~ session involves multiple hops through different trusted and untrusted networks. The STIR framework [RFC7340] addresses the protection of the carriage of call information and identities over untrusted networks, which wasn't addressed in the core SIP specifications. Section 20.9 of [RFC3261]~~, Section 20.9~~ defines the Call-Info header field as the mechanism for carrying call- and caller-related information and also provides procedures for defining new 'purpose' parameter tokens. This document discusses the use of existing tokens and defines a new 'purpose' token to correspond to the RCD framework.

There are a number of RCD information types that can be transmitted in the Call-Info header field of a SIP request. The STIR RCD specification [I-D.ietf-stir-passport-rcd] defines calling name, a logo or icon associated with the caller, and a call reason string. It also discusses an extensible way of carrying caller information using jCard [RFC7095]. It may be that future specifications extend information types and, similar to how this document extends the Call-Info header field to provide corresponding functionality to STIR RCD, it is RECOMMENDED that future specifications also provide corresponding Call-Info extensions.

Commenté [MB5]: How we enforce this?

The RCD framework defined both in this document as well as in [I-D.ietf-stir-passport-rcd] carries call-specific information. The insertion of RCD is intended to be singular in that the receiving party should not be required to make any call-specific decisions based on redundant, duplicate, or conflicting RCD. The RCD information is either intended to be added by a party that is authoritative over that information or to have been translated from a verified STIR RCD PASSporT and unmodified once in a trusted domain. Any additional parties involved in the call path MUST NOT modify the Call-Info header field or add additional Call-Info header fields related to RCD. The insertion of the RCD Call-Info header field should be considered a trusted action based on trusted information,

Commenté [MB6]: How misbehaving intermediate nodes are detected?

and the information MUST NOT be considered modifiable representing the best practice of determining the final representation of the caller RCD to the user.

As discussed in [I-D.ietf-stir-passport-rcd], the calling name uses the display-name value of the From header field [RFC3261] of the request. Alternatively, for some calls, the calling name may come from the P-Asserted-ID header field [RFC3325]. While this is out of scope for Call-Info header field in terms of the representation of the display-name value, this document does discuss the representation of the verification of this value using the 'verified' parameter.

For logos or icons that can represent the calling party, the 'purpose' token "icon" [RFC3261] is used to indicate a URI for an image resource that can be displayed to the user receiving the SIP request. For the purpose of this document and the transmission of RCD, the "icon" 'purpose' token should be used as defined. Section 8.2 provides high-level guidance on image formatting and related information.

This document defines 'call-reason' as a new parameter for the Call-Info header field. This parameter carries a string indicating the reason for the call.

jCard is a comprehensive and extensible mechanism defined in the STIR RCD framework. While [RFC3261] specifies a "card" 'purpose' token, the intent of defining a new "jcard" 'purpose' token is to use the JSON jCard format [RFC7095] and to provide guidance for the use and non-use of jCard attributes to describe the calling party in a communications session as well to provide some security considerations around that information. These topics are covered in the next sections.

5. "jcard" Call-Info 'purpose' Token

The Call-Info 'purpose' token "jcard" indicates support of RCD associated with the identity of a calling party in a SIP call [RFC3261], Section 20.9. The format of a Call-Info header field when using the "jcard" token is as follows.

The Call-Info header field is defined to include a URI that points to a resource that is a jCard JSON object [RFC7095]. The media type for the JSON text MUST be set as application/json with a default encoding of UTF-8 [RFC8259]. This MAY be carried directly in the Call-Info header field URI using the "data" URI scheme. A jCard also MAY be carried in the body of the SIP request bearing this Call-Info header field via the "cid" URI scheme [RFC2392]. Alternatively, the URI MUST define the use HTTPS or a transport that can validate the integrity of the source of the resource as well as the transport channel through which the resource is retrieved. If, in the specific deployment environment of SIP, the source or integrity of the RCD

Commenté [MB7]: I don't parse this

information cannot be trusted, then the use of the STIR RCD framework defined in [I-D.ietf-stir-passport-rcd] should be considered.

A call and its corresponding single RCD-related Call-Info header field MUST only contain a single jCard object represented by an array with two elements. The array MUST only include a single first element with the string "vcard", and the second element is an array of jCard properties corresponding to the single entity jCard object.

The fields like "fn", "photo", or "logo" if used with the use of "icon" calling name in From or P-Asserted-ID header field or purpose token, as described in the previous section, MUST either match or be avoided to allow the called party to clearly determine the intended calling name or icon.

An example of a Call-Info header field is:

Call-Info: <https://example.com/qbranch.json>;purpose=jcard

An example of the contents of a URL-linked jCard JSON file is shown as follows:

```
["vcard",
  [
    ["version",{},"text","4.0"],
    ["fn",{},"text","Q Branch"],
    ["org",{},"text","MI6;Q Branch Spy Gadgets"],
    ["photo",{},"uri","https://example.com/photos/q-256x256.png"],
    ["logo",{},"uri","https://example.com/logos/mi6-256x256.jpg"],
    ["logo",{},"uri","https://example.com/logos/mi6-64x64.jpg"]
  ]
]
```

An example SIP INVITE using the "data" URI scheme is as follows:

```
INVITE sip:alice@example.com SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKnashds8
To: Alice <sip:alice@example.com>
From: Bob <sip:12155551000@example.com;user=phone>;tag=1928301774>
Call-ID: a84b4c76e66710
Call-Info: <data:application/json,["vcard",[["version",{},"text",
 "4.0"],["fn",{},"text","Q Branch"],["org",{},"text","MI6;Q Branch
 Spy Gadgets"],["photo",{},"uri","https://example.com/photos/quart
 ermaster-256x256.png"],["logo",{},"uri","https://example.com/log
 os/mi6-256x256.jpg"],["logo",{},"uri","https://example.com/logos/
 mi6-64x64.jpg"]]]\>;purpose=jcard;call-reason="Rendezvous for
 Little Nellie"
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Fri, 25 Sep 2015 19:12:25 GMT
Contact: <sip:12155551000@gateway.example.com>
Content-Type: application/sdp

v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
s=Session SDP
```

Commenté [MB8]: What is the behavior at the terminating side when more are present?

Commenté [MB9]: I smell this was grabbed from other RFCs, but updating the date to match the publication date would make sense.

```
c=IN IP4 pc33.atlanta.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

An example SIP INVITE using the "cid" URI scheme is as follows:

```
INVITE sip:alice@example.com SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKnashds8
To: Alice <sip:alice@example.com>
From: Bob <sip:12155551000@example.com;user=phone>;tag=1928301774>
Call-ID: a84b4c76e66710
Call-Info: <cid:12155551000@example.com>;purpose=jcard;
 call-reason="Rendezvous for Little Nellie"
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Fri, 25 Sep 2015 19:12:25 GMT
Contact: <sip:12155551000@gateway.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...

--boundary1

Content-Type: application/sdp

v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
s=Session SDP
c=IN IP4 pc33.atlanta.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

--boundary1

Content-Type: application/json
Content-ID: <12155551000@example.com>

["vcard",[["version",{},"text","4.0"],["fn",{},"text","Q Branch"],
 ["org",{},"text","MI6;Q Branch Spy Gadgets"],["photo",{},"uri","
 https://example.com/photos/quartermaster-256x256.png"],["logo",
 {},"uri","https://example.com/logos/mi6-256x256.jpg"],["logo",{},
 "uri","https://example.com/logos/mi6-64x64.jpg"]]]
```

6. 'call-reason' Call-Info Parameter

This specification defines a new parameter that extends the overall content of the RCD-related Call-Info header field. As other parameters may be defined in the future, this parameter is intended to be separate and distinct from the other URI and 'purpose' tokens

that may proceed these parameters.

This new parameter of the Call-Info header field is called 'call-reason'. The 'call-reason' parameter is intended to convey a short textual message suitable for display to an end user during call alerting. As a general guideline, this message SHOULD be no longer than 64 characters; displays that support this specification may be forced to truncate messages that cannot fit onto a screen. This message conveys the caller's intention in contacting the callee. It is an optional parameter, and the sender of a SIP request cannot guarantee that its display will be supported by the terminating endpoint. The manner in which this reason is set by the caller is outside the scope of this specification.

Commenté [MB10]: Is there a chance that this can be a clickable text? If so, can we say that the display should not be clickable, by default?

An alternative approach would have been to use the value of Subject header field [RFC3261] to convey the reason for the call. However, because the Subject header field has seen little historical use in SIP implementations and its specification describes its potential use in filtering, it seemed prudent to define a new means of carrying a call reason indication.

An example of a Call-Info header field value with the "call-reason" parameter follows:

```
Call-Info: <https://example.com/jbond.json>;purpose=jcard;
 call-reason="For your ears only"
```

In the case that there is only a 'call-reason' or 'verified' parameter or any future parameters that may be defined and no need for a purpose parameter with no associated URI the null data URI, "data:" is used as the URI. The purpose parameter "jcard", defined in this document, is used to avoid any conflicts or confusion with existing implementations and previously defined purpose parameters. As an example:

```
Call-Info: <data:>;purpose=jcard;
 call-reason="For your ears only"
```

7. 'verified' Call-Info Parameter

~~This specification defines an additional new parameter, t~~The 'verified' parameter, that extends and complements the content conveyed by the RCD-related Call-Info header field. This parameter ~~is to be used to~~ indicates to the recipient that the information contained in the Call-Info header field has been verified by verification procedures for claims defined in Section 8 of [I-D.ietf-stir-passport-rcd] ~~Section 8~~. The presence of a 'verified' parameter on a Call-Info header field should be considered specific to the information for that Call-Info header field only. If there is a Call-Info header field corresponding to information defined in this specification that doesn't contain a 'verified' parameter, the recipient should assume that information was not received and verified corresponding to the verification procedures defined in Section 8 of [I-D.ietf-stir-passport-rcd] ~~Section 8~~.

There is a single valid value associated with the 'verified' parameter of 'true'. The value 'true' indicates to the recipient

that the party that included the Call-Info header field performed a successful verification of the information represented. As a general principle of Call-Info header field information, the recipients ability to trust the 'verified' parameter is based on the trusted relationship of whom they are receiving the SIP request.

Example where the parameter verified="true" is used to represent that a verification procedure has been performed within a trust domain to indicate the 'icon' URL has been successfully verified:

```
Call-Info: <https://example.com/jbond.png>;purpose=icon;
 verified="true"
```

In addition to the use of the indication of successful verification of RCD information, an important usage of the 'verified' parameter is for the indication of verified "display-name" information, sometimes referred to as calling name or CNAM.

In the following example, a call was delivered via an NNI ~~network relationship~~ to a terminating provider with the following STIR RCD PASSporT.

```
Protected Header
{
  "alg":"ES256",
  "typ":"passport",
  "ppt":"rcd",
  "x5u":"https://cert.example.org/passport.pem"
}
Payload
{
  "dest":{"tn":["12025551001"]},
  "iat":1443208345,
  "orig":{"tn":"12025551000"},
  "rcd":{"nam":"James Bond","icn":"https://example.com/jbond.png"}
}
```

The terminating provider receives a SIP INVITE with an identity header containing the STIR RCD PASSporT is verified through a verification service. The provider then wants to deliver the call to an end device in the trusted and authenticated UNI network. The provider uses local policies to determine the information desired to present to the end device. The following example SIP INVITE could be used to represent the RCD information using two Call-Info header fields. Because the verification of both the icon and calling name passed, a Call-Info header for the 'icon' is added with a verified="true" parameter, and the use of Call-Info with a null data URI is used, as discussed in the "call-reason" section above. This document defines the convention that when a Call-Info header field with a null data URI, "data:", a default purpose of "jcard" and adding a verified="true" indicates that the display-name information in either the From and/or P-Asserted-ID header field has been verified via RCD verification procedures.

Example SIP INVITE described above:

```
INVITE sip:qbranch@example.com SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKnashds8
```

```
To: "QBranch" <sip:qbranch@example.com>
From: "James Bond" <sip:12155551000@example.com;user=phone>;
 tag=1928>
Call-ID: a84b4c76e66710
Call-Info: <https://example.com/jbond.png>;purpose=icon;
 verified="true"
Call-Info: <data:>;purpose=jcard;verified="true"
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Fri, 25 Sep 2025 19:12:25 GMT
Contact: <sip:12155551000@gateway.example.com>
Content-Type: application/sdp

v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
s=Session SDP
c=IN IP4 pc33.atlanta.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

8. 'integrity' Call-Info Parameter

~~This specification defines an additional new parameter, t~~he 'integrity' parameter~~, that~~ extends and complements the integrity information conveyed specifically by the 'rcdi' claim in the RCD-related Call-Info header field. This parameter is ~~intended to be~~ used to indicate, for a URI represented in the Call-Info header field, the resource referenced by that URI has an associated integrity hash value. Section 6.1 of [I-D.ietf-stir-passport-rcd] describes the creation of the digest value including the hash algorithm indicator a '-' separator and the hash value as a string. The JSON pointer object container described as the container of the 'rcdi' hashes is not necessary since each hash value should only correspond to a single URI.

Typically, this hash value, assuming the URI and the resource pointed to the URI don't change between the STIR RCD PASSporT and the Call-Info URI value, the integrity value can be directly used as the same corresponding string in both the 'rcdi' claim and the 'integrity' parameter string value.

Example STIR RCD PASSporT:

```
Protected Header
{
  "alg":"ES256",
  "typ":"passport",
  "ppt":"rcd",
  "x5u":"https://cert.example.org/passport.pem"
}
Payload
{
  "crn": "Rendezvous for Little Nellie",
  "dest": {"tn": ["12155551001"]},
  "iat": 1443208345,
  "orig": {"tn": "12025551000"},
  "rcd": {
```

```
        "nam": "Q Branch Spy Gadgets",
        "icn": "https://example.com/photos/q-256x256.png"
      },
      "rcdi": {
        "/icn": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4"
      }
    }
```

Example corresponding SIP INVITE with Call-Info information derived from RCD information above:

```
   INVITE sip:qbranch@example.com SIP/2.0
   Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKnashds8
   To: "James Bond" <sip:12155551001@example.com;user=phone>
   From: "Q Branch Spy Gadgets" <sip:12025551000@example.com;
    user=phone>;tag=1928>
   Call-ID: a84b4c76e66710
   Call-Info: <https://example.com/photos/q-256x256.png>;purpose=
    icon;verified="true";integrity="sha256-RojgWwU6xUtI4q82+kHPyHm
    1JKbm7+663bMvzymhkl4"
   Call-Info: <data:>;purpose=jcard;call-reason="Rendezvous for
    Little Nellie";verified="true"
   Call-Info: <data:>;purpose=jcard;verified="true"
   CSeq: 314159 INVITE
   Max-Forwards: 70
   Date: Fri, 25 Sep 2025 19:12:25 GMT
   Contact: <sip:12155551000@gateway.example.com>
   Content-Type: application/sdp

   v=0
   o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
   s=Session SDP
   c=IN IP4 pc33.atlanta.example.com
   t=0 0
   m=audio 49172 RTP/AVP 0
   a=rtpmap:0 PCMU/8000
```

9. Usage and an Example of Call-Info for RCD

The procedures for the usage of URIs and 'purpose' parameter tokens should generally follow the procedures defined in [RFC3261]. The following example provides both the STIR RCD PASSporT and the corresponding set of Call-Info header fields shows the use of multiple 'purpose' parameters to indicate a jCard and an icon and also a 'call-reason' parameter:

Example STIR RCD PASSporT:

```
   Protected Header
   {
      "alg":"ES256",
      "typ":"passport",
      "ppt":"rcd",
```

Commenté [MB11]: Is there any provisioning requires to make use of the extensions? Are there logs for session that were rejected because the reason does not match, etc.?

Commenté [MB12]: Are there cases where this is not followed?

```
      "x5u":"https://cert.example.org/passport.pem"
   }
   Payload
   {
      "crn":"For your ears only",
      "dest":{"tn":["12025551001"]},
      "iat":1443208345,
      "orig":{"tn":"12025551000"},
      "rcd":{
        "jcl":"https://example.com/qbranch.json",
        "icn":"https://example.com/jbond.png"
      },
      "rcdi": {
        "/jcl": "sha256-yHm1JKbm7+663bMvzymhkl4RojgWwU6xUtI4q82+kHP"
        "/icn": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4"
      }
   }
```

Example Call-Info header fields:

```
   Call-Info: <data:>;purpose=jcard;verified="true"
   Call-Info: <https://example.com/jbond.json>;purpose=jcard;verified
    =true;integrity="sha256-yHm1JKbm7+663bMvzymhkl4RojgWwU6xUtI4q82
    +kHP"
   Call-Info: <https://example.com/jbond.png>;purpose=icon;
    call-reason="For your ears only";verified=true;integrity=
    "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4"
```

10. Usage of jCard and Property-Specific Usage

Beyond the definition of the specific properties or JSON arrays associated with each property, this specification defines a few rules above and beyond [RFC7095] that are specific to the use of jCard for Call-Info and RCD to ensure there is a minimum level of supported properties to which every implementation of this specification should adhere. This includes support for interpreting the value of these properties and the ability to render in some appropriate form the display capabilities of common telephone devices as well as applications, and also includes requirements specific to textual and graphics-capable displays.

10.1. Usage of URIs in jCard

When one or more URIs are used in a jCard, it is important to note that any URI-referenced data, with the exception of the top-level usage of "jcl" as a URI to the jCard itself (unless updated by any future extensions of this specification) MUST NOT contain any URI references. In other words, the jCard can have URI references as defined in the jCard specification and this document, but the content referenced by those URIs MUST NOT have any URIs, and therefore MUST be enforced by the client to not follow those URI references or not render that content to the user if any URI are present in that specific URI linked content. The purpose of this is to control the security and more specifically to align with the content-integrity mechanism defined in [I-D.ietf-stir-passport-rcd]. The authors do not believe there is a scenario for which deeper URI references would be required or even supported by the typical use of current jCard

properties. However, because jCard is extensible, this rule is set to restrict further extension without the proper consideration of security and integrity properties of both Call-Info usage as well as the RCD and STIR signing of the data [I-D.ietf-stir-passport-rcd] [RFC8224].

10.2. Usage of Multimedia Data in jCard or with Icon

For the use of the 'purpose' token "icon" or for the cases where the jCard either incorporates URIs or includes digital images and sounds directly via Base64 encoding, ~~we~~ this document provides recommendations to facilitate the successful decoding and rendering of these images and media formats.

Commenté [MB13]: Consider add a ref

For images, such as for the "photo" and "logo" properties, the default image formats SHOULD be PNG [ISOPNG] or JPEG [ITUJPEG], as these files are commonly used to support 24-bit RGB images. Supporting older telephone devices that only support bitmap (BMP) images [RFC7903] with a lower bit range (e.g., ~~16~~ 16-bit, ~~8~~ 8-bit, or 1 bit), or grayscale, or 1-bit black and white color displays, should be considered optional or even not recommended because, at the time of writing, they are becoming increasingly rare (i.e., typically, devices either have color or color-aware graphical displays that support PNG or JPEG formats or they are exclusively textual displays).

In addition, vector images are increasingly popular to use for icons because they support scalable images without having to send multiple resolutions. The SVG format has gained wide support as of this writing as a common format for vector images. At a minimum, the SVG Tiny 1.2 specification [W3C-SVGTiny1.2] SHOULD be supported as an additional default format for devices.

For the cases where image files are referenced by URIs as file resources, this document defines a character string that SHOULD be concatenated onto the end of a file name, but before the file extension, that signals the height and width of the image to the end device for the convenience of determining the appropriate resolution to retrieve without the need to retrieve all the image files. It is also recommended that images have a square aspect ratio with equal height and width and with a power of two value for the number of pixels (e.g., 32x32, 128x128, 512x512). The format of the string should be "filename-HxW", where "filename" is a unique string representing the file, "H" represents the height in pixels, and "W" represents the width in pixels.

It is appropriate and useful to include multiple versions of images or sounds so that endpoints that cannot support all formats or resolutions can select the format they do support. The convention that is RECOMMENDED is that files that refer to the same content should use the same filename portion. If the image format has a specific resolution, the HxW portion of the filename should correspond to the pixel resolution. The file extension should reference the file type (e.g., filename.png, filename.svg, or filename.jpg) or (e.g., filename-32x32.png, filename-64x64.png, filename.svg, filename-32x32.jpg, or filename-64x64.jpg).

Because this is a complex and often debated topic that has evolved over the many years of advances in image coding and display technologies, we suggest relying on either future specifications or industry forum specifications that might correspond to supporting particular classes of devices to further define how URIs can reference appropriate image formats and files.

For audio files, the recommendation is to provide mp3, m4a or mp4, or wav files [RFC2361], although the usage of sound (for example, a special ring tone for a particular caller) is not well defined in this specification. Future documents should consider both usage and potential security risks of playing sounds that are not specifically authorized by a device user.

10.3. Cardinality

Property cardinalities are indicated, for convenience, using the following notation and follow the guidance of jCard [RFC7095] and vCard [RFC6350], which is based on ABNF (see [RFC5234], Section 3.6):

Cardinality	Meaning
1	Exactly one instance per jCard MUST be present.
*1	Exactly one instance per jCard MAY be present.
1*	One or more instances per jCard MUST be present.
*	One or more instances per jCard MAY be present.

10.4. Identification Properties

The following properties, initially defined in [RFC6350], hold the identity information of the entity associated with the jCard. This subset of properties selected for this document are relevant to telephone and messaging applications. jCard is an extensible object; therefore, there may be future specifications that extend the set of properties relevant to the applications that implement this specification.

Commenté [MB14]: simplify

10.4.1. "fn" Property

The "fn" property provides a formatted text corresponding to the name of the object the jCard represents. Reference: [RFC6350], Section 6.2.1.

Value type: A single text value.

Cardinality: 1*

Example:

```
["fn", {}, "text", "Mr. John Q. Public\, Esq."]
```

Commenté [MB15]: Are other languages supported in the text part?

10.4.2. "n" Property

The "n" property provides the components of the name of the object the jCard represents. Reference: [RFC6350], Section 6.2.2.

Value type: A single structured text value. Each component can have multiple values.

Cardinality: *1

Example:
```
["n", {}, "text", "Public;John;Quinlan;Mr.;Esq."]
["n", {}, "text", "Stevenson;John;Philip,Paul;Dr.;Jr.,M.D.,A.C.P."]
```

10.4.3. "nickname" Property

The "nickname" property provides the text corresponding to the nickname of the object the jCard represents. Reference: [RFC6350], Section 6.2.3.

Value type: One or more text values separated by a COMMA character (U+002C).

Cardinality: *

Example:
```
["nickname", {}, "text", "Robbie"]
["nickname", {}, "text", "Jim,Jimmie"]
["nickname", {}, "text", "TYPE=work:Boss"]
```

Commenté [MB16]: Idem for the language

10.4.4. "photo" Property

The "photo" property provides image or photograph information that annotates some aspect of the object the jCard represents. Reference: [RFC6350], Section 6.2.4.

In addition to the definition of jCard, and to promote interoperability and proper formatting and rendering of images, the photo SHOULD correspond to a square image with the size of 128x128, 256x256, 512x512, or 1024x1024 pixels.

Value type: A single URI.

Cardinality: *

Example:
```
["photo", {}, "uri", "http://www.example.com/jqpublic-256x256.png"]
```

10.5. Delivery Addressing Properties

This property is concerned with information related to the delivery address of the jCard object.

10.5.1. "adr" Property

The "adr" property provides the delivery address of the object the jCard represents. Reference: [RFC6350], Section 6.3.1.

Value type: A single structured text value separated by the SEMICOLON character (U+003B).

Cardinality: *

Example:

```
["adr", {"type":"work"}, "text",
  ["", "", "3100 Massachusetts Avenue NW", "Washington", "DC",
    "20008", "U.S.A."]
]
```

"adr" also allows a structured value element that itself has multiple values. In this case, the element of the array describing the structured value is itself an array with one element for each of the component's multiple values. The following example shows alternate values for the address string.

Example:

```
["adr", {"type":"work"}, "text",
  ["", "", ["3100 Massachusetts Avenue NW","Embassy of the
    United Kingdom"], "Washington", "DC", "20008", "U.S.A."]
]
```

10.6. Communications Properties

These properties describe how to communicate with the object that the jCard represents.

10.6.1. "tel" Property

The "tel" property provides the telephone number for the object the jCard represents. Reference: [RFC6350], Section 6.4.1.

Relative to the SIP From header field value, this information may provide an alternate telephone number or other related telephone numbers for other uses.

It is important to note that any of the potential instances of the "tel" property should not be considered part of the authentication or verification part of STIR [RFC8224] or required to match the "orig" claim in the PASSporT [RFC8225]. These telephone numbers can be for contact, fax, or other purposes aligned with the general usage of jCard and vCard, but the potential confusion of the callee when provided with multiple telephone numbers versus the actual, verified telephone number should be considered from a general policy point of view.

Value type: By default, it is a single free-form text value (for backward compatibility with vCard 3), but it SHOULD be reset to a URI value. It is expected that the URI scheme will be "tel", as specified in [RFC3966], but other schemes MAY be used.

Cardinality: *

Example:

```
["tel", { "type": ["voice", "text", "cell"], "pref": "1" }, "uri",
 "tel:+1-202-555-1000"]
["tel", { "type": ["fax"] }, "uri", "tel:+1-202-555-1001"]
```

10.6.2. "email" Property

The "email" property provides the electronic mail address of the object the jCard represents. Reference: [RFC6350], Section 6.4.2.

Value type: A single text value.

Cardinality: *

Example:

```
["email", {"type":"work"}, "text", "jqpublic@xyz.example.com"]
["email", {"pref":"1"}, "text", "jane_doe@example.com"]
```

10.6.3. "lang" Property

The "lang" property provides the language(s) that may be used for communicating with the object the jCard represents. Reference: [RFC6350], Section 6.4.4.

Value type: A single language-tag value.

Cardinality: *

Example:

```
["lang", {"type":"work", "pref":"1"}, "language-tag", "en"]
["lang", {"type":"work", "pref":"2"}, "language-tag", "fr"]
["lang", {"type":"home"}, "language-tag", "fr"]
```

10.7. Geographical Properties

These properties provide geographical information associated with the object the jCard represents.

10.7.1. "tz" Property

The "tz" property provides the time zone of the object the jCard represents. Reference: [RFC6350], Section 6.5.1.

Note: the reference for time-zone names is https://www.iana.org/time-zones.

Value type: The default is a single text value. It can also be reset to a single URI or a UTC-offset value.

Cardinality: *

Example:

```
["tz", {}, "text", "Raleigh/North America"]
```

10.7.2. "geo" Property

The "geo" property provides the global positioning of the object the jCard represents. Reference: [RFC6350], Section 6.5.2.

Value type: A single URI.

Cardinality: *

Example:
  ["geo", {}, "uri", "geo:37.386013,-122.082932"]

10.8. Organizational Properties

These properties are concerned with information associated with characteristics of the organization or organizational units of the object that the jCard represents.

10.8.1. "title" Property

The "title" property has the intent of providing the position or job of the object the jCard represents. Reference [RFC6350], Section 6.6.1.

Value type: A single text value.

Cardinality: *

Example:
  ["title", {}, "text", "Research Scientist"]

10.8.2. "role" Property

The "role" property has the intent of providing the position or job of the object the jCard represents. Reference [RFC6350], Section 6.6.2.

Value type: A single text value.

Cardinality: *

Example:
  ["role", {}, "text", "Project Leader"]

10.8.3. "logo" Property

The "logo" property has the intent of specifying a graphic image of a logo associated with the object the jCard represents. Reference [RFC6350], Section 6.6.3.

Value type: A single URI.

Cardinality: *

Example:
  ["logo", {}, "uri", "http://www.example.com/abccorp-512x512.jpg"]

  ["logo", {}, "uri", "
   AQEEBQAwdzELMAkGA1UEBhMCVVMxLDAqBgNVBAoTI05ldHNjYXBlIENvbW11bm
   ljYXRpb25zIENvcnBvcmF0aW9uMRwwGgYDVQQLExNJbmZvcm1hdGlvbiBTeXN0
   <...the remainder of base64-encoded data...>"]

10.8.4. "org" Property

The "org" property has the intent of specifying the organizational name and units of the object the jCard represents. Reference [RFC6350], Section 6.6.4.

Value type: A single structured text value consisting of components separated by the SEMICOLON character (U+003B).

Cardinality: *

Example:

```
["org", {}, "text", "ABC\, Inc.;North American Division;Marketing"]
```

10.9. Explanatory Properties

These properties provide additional information such as notes or revisions specific to the jCard.

10.9.1. "categories" Property

The "categories" property specifies application category information about the object the jCard represents. Reference: [RFC6350], Section 6.7.1.

Value type: One or more text values separated by a COMMA character (U+002C).

Cardinality: *

Example:

```
["categories", {}, "text", "TRAVEL AGENT"]

["categories", {}, "text", "INTERNET,IETF,INDUSTRY"]
```

10.9.2. "note" Property

The "note" property specifies supplemental information or a comment about the object the jCard represents. Reference: [RFC6350], Section 6.7.2.

Value type: A single text value.

Cardinality: *

Example:

```
["note", {}, "text", "This fax number is operational 0800 to 1715
 EST\, Mon-Fri."]
```

10.9.3. "sound" Property

The "sound" property specifies digital sound content information that annotates some aspect of the object the jCard represents. This property is often used to specify the proper pronunciation of the name property value of the jCard. Reference: [RFC6350], Section 6.7.5.

Value type: A single URI.

Cardinality: *

Example:

```
["sound", {}, "uri", "https://www.example.com/pub/logos
```

```
      /abccorp.mp3"]

     ["sound", {}, "uri", "data:audio/basic;base64,MIICajCCAdOgAwIBA
      gICBEAQEEBQAwdzELMAkGA1UEBhMCVVMxLDAqBgNVBAoTI05ldHNjYXBlIENvb
      W11bmljYXRpb25zIENvcnBvcmF0aW9uMRwwGgYDVQQLExNJbmZvcm1hdGlvbiB
      <...the remainder of base64-encoded data...>"]
```

10.9.4. "uid" Property

The "uid" property specifies a globally unique identifier corresponding to the object the jCard represents. Reference: [RFC6350], Section 6.7.6.

Value type: A single URI value. It MAY also be reset to free-form text.

Cardinality: *1

Example:

```
  ["uid", {}, "uri", "urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"]
```

10.9.5. "url" Property

The "url" property specifies a uniform resource locator associated with the object the jCard represents. Reference: [RFC6350], Section 6.7.8.

There are potential security and privacy implications of providing URLs with telephone calls. The end client receiving a jCard with a "url" property MUST only display the URL and not automatically follow the URL or provide automatic preview of the URL, and generally provide good practices in making it clear to the user it is their choice to follow the URL in a browser context consistent with all of the common browser security and privacy practices available on most consumer OS environments.

Value type: A single uri value.

Cardinality: *

Example:

```
  ["url", {}, "uri", "https://example.org/french-rest/chezchic.html"]
```

10.9.6. "version" Property

The "version" property MUST be included and is intended to specify the version of the vCard specification used to format this vCard. Reference: [RFC6350], Section 6.7.9.

Value type: A single text value.

Cardinality: 1

Example:

```
  ["version", {}, "text", "4.0"]
```

11. Extension of jCard

Part of the intent of using jCard is to leverage its extensibility to define new properties to relay new information related to a caller. This capability is inherently supported as part of standard extensibility. However, usage of those new properties should be published and registered following [RFC7095], Section 3.6 or new specifications.

12. IANA Considerations

12.1. 'jcard' Purpose Parameter Value

This document defines the 'jcard' value for the 'purpose' parameter of the Call-Info header field [RFC3261]. IANA has added this document to the list of references for the 'purpose' value of Call-Info in the "Header Field Parameters and Parameter Values" sub-registry of the "Session Initiation Protocol (SIP) Parameters" registry.

12.2. SIP Call-Info Header Field 'call-reason' Parameter

This document defines the 'call-reason' generic parameter for use as a new parameter in the Call-Info header field in the "Header Field Parameters and Parameter Values" registry defined by [RFC3968]. The parameter's token is "call-reason", and it takes the value of a quoted string.

Header Field	Parameter Name	Predefined Values	Reference
Call-Info	call-reason	No	[this RFC]

12.3. SIP Call-Info Header Field 'verified' Parameter

This document defines the 'verified' generic parameter for use as a new parameter in the Call-Info header field in the "Header Field Parameters and Parameter Values" registry defined by [RFC3968]. The parameter's token is "verified", and it takes the value of a quoted string that can only be "true".

Header Field	Parameter Name	Predefined Values	Reference
Call-Info	verified	Yes	[this RFC]

12.4. SIP Call-Info Header Field 'integrity' Parameter

This document defines the 'integrity' generic parameter for use as a new parameter in the Call-Info header field in the "Header Field Parameters and Parameter Values" registry defined by [RFC3968]. The parameter's token is "integrity", and it takes the value of a quoted string.

Header Field	Parameter Name	Predefined Values	Reference

Call-Info	integrity	No	[this RFC]

13. Security Considerations

Revealing information such as the name, location, and affiliation of a person necessarily entails certain privacy risks. The SIP Call-Info header field has no particular confidentiality requirement, as the information sent in SIP is in the clear anyway. Transport-level security can be used to hide information from eavesdroppers, and the same confidentiality mechanisms would protect any Call-Info or jCard information carried or referred to in SIP.

The use of the Call-Info header for transporting Rich Call Data ('rcd') is intended primarily for providing verified information at the termination of a call, where a verification service has a trusted UNI relationship with the user agent. To ensure the integrity and authenticity of this data, the security framework established by STIR, including the use of the 'rcd'PASSporT as defined in [I-D.ietf-stir-passport-rcd], should be followed. This framework enables digital signatures to verify the issuer of assertions related to the calling party's identity, distinguishing persistent identity attributes from transient, per-call details. Implementers should also consider certificate-based constraints to ensure proper binding between caller identity assertions and call-specific metadata while maintaining the integrity of the information throughout transmission. Since Call-Info serves as a means to convey verified caller information to the end user, mechanisms should be in place to validate the authenticity of the assertion, enforce appropriate certificate associations, and preserve the trustworthiness of Rich Call Data from origination to termination.

The SIP framework, defined in [RFC3261] and the various extensions to SIP, which stir [RFC8224] and rich call data [I-D.ietf-stir-passport-rcd] are included, since its existence has provided mechanisms to assert information about the person or entity behind the call. This can be a feature that can be a benefit to the

SIP network that allows users to help identify the calling party behind an abstract telephone number. It can also enable the ability for actors to impersonate a calling party they are not authorized to represent. The core security consideration that either explicitly or implicitly have been acknowledged with any of the SIP and stir specifications is that there is a management and policy layer that validates the participants in the ecosystem and their use of a SIP network with telephone number identifiers and identity related information. The use of this specification should weigh this responsibility and make the appropriate considerations to validate the proper participation and use of these tools follow these larger security, impersonation prevention, and privacy considerations.

The use of this specification with the insertion of meta data related to a caller or the purpose of the call should recognize the risk that this information can be viewed by those network elements and participants in the delivery of the SIP call. The insertion of media directly or via Base64 encoding or using a remote URI that query network resources should be considered as a potential threat vector

to the user or user agent that could potentially allow the parsing of documents crafted to trigger a bug or install a virus. Remote access to URI content should additionally be considered as potentially exposing information about that user or user agent. Some sensitive users may desire the ability to control or disable these mechanisms entirely and methods to restrict or disable these potential concerns should be considered to mitigate these concerns. Largely, any information that is included in rich call data should be considered public and this specification does not define any mechanism to protect this information beyond the security and privacy associated with the SIP signalling itself. This is a property that is consistent with SIP more generally and this specification follows a similar pattern for its use.

This specification contains the ability to include media resources and URI and URL resource references to media resources that could pose a threat when referencing or decoding the content of these media resources similar to threats that web browsers and other media decoding applications must be concerned about. A network specific set of policies or best practices for the use and hosting of media content that is agreed to contain validated media resources that have been evaluated to not pose a security threat to the participants or the devices supported in the ecosystem should be considered.

14. References

14.1. Normative References

[I-D.ietf-stir-passport-rcd]
Wendt, C. and J. Peterson, "PASSporT Extension for Rich Call Data", Work in Progress, Internet-Draft, draft-ietf-stir-passport-rcd-26, 5 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-stir-passport-rcd-26>.

[ISOPNG] ISO/IEC, "Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG), Functional specification, ISO/IEC 15948:2004", March 2004.

[ITUJPEG] ITU-T, "Information technology - Digital compression and coding of continuous-tone still images, JPEG File Interchange Format (JFIF) ITU-T Recommendation T.871, ISO/IEC 10918-5", May 2013.

[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/rfc/rfc2119>.

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

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

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

[RFC3968] Camarillo, G., "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)", BCP 98, RFC 3968, DOI 10.17487/RFC3968, December 2004, <https://www.rfc-editor.org/rfc/rfc3968>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/rfc/rfc5234>.

[RFC6350] Perreault, S., "vCard Format Specification", RFC 6350, DOI 10.17487/RFC6350, August 2011, <https://www.rfc-editor.org/rfc/rfc6350>.

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

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/rfc/rfc7519>.

[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/rfc/rfc7852>.

[RFC7903] Leonard, S., "Windows Image Media Types", RFC 7903, DOI 10.17487/RFC7903, September 2016, <https://www.rfc-editor.org/rfc/rfc7903>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018, <https://www.rfc-editor.org/rfc/rfc8224>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/rfc/rfc8225>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/rfc/rfc8259>.

[W3C-SVGTiny1.2] W3C, "Scalable Vector Graphics (SVG) Tiny 1.2", 22

December 2008, <https://www.w3.org/TR/SVGMobile/>.

14.2. Informative References

[RFC2361] Fleischman, E., "WAVE and AVI Codec Registries", RFC 2361, DOI 10.17487/RFC2361, June 1998, <https://www.rfc-editor.org/rfc/rfc2361>.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, DOI 10.17487/RFC3325, November 2002, <https://www.rfc-editor.org/rfc/rfc3325>.

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <https://www.rfc-editor.org/rfc/rfc7340>.

Acknowledgements

We would like to thank David Hancock, Alec Fenichel, Paul Kyzivat, Yi Jing and other members of the SIPCORE and STIR working groups and ATIS/SIP Forum IPNNI for their helpful suggestions and comments during the creation of this document.

Authors' Addresses

Chris Wendt
Somos
United States of America
Email: chris@appliedbits.com

Jon Peterson
Neustar
United States of America
Email: jon.peterson@neustar.biz