VESTA Router Service NNI Specification

i3 SIP OSPs and Peer NGCS Interface Specification (Network-to-Network Interface)

Version: 2.2

Date: August 07, 2020

TABLE OF CONTENTS

DOCUMENT HISTORY

Author	Date	Version	Description
Steve Mardakis	July 08, 2020	1.0	Initial version.
Steve Mardakis	July 20, 2020	2.0	Adapted to be specific to i3 SIP.
Steve Mardakis	August 04, 2020	2.1	Corrections following review.
Steve Mardakis	August 07, 2020	2.2	Corrections following review.

EXECUTIVE SUMMARY

This document establishes interface specifications for Originating Service Providers (OSPs) and other NG9-1-1 Service Providers interconnecting to the VESTA Router Service for calls handoff and/or calls transfer.

The intention of this document is to provide the interface specification for NG9-1-1 partners, OSPs or other 9-1-1 Service Providers. It is not intended to provide a detailed overview of the functionality of NG9-1-1 or to cover details already specified in existing normative references (e.g., NENA or ATIS standards). Reference to such specifications are made throughout the document, however, unless an alternative has been identified, the NENA i3 standard should be viewed as the default standard.

The scope of the document is to cover both calls exchanged per Alliance for Telecommunication Industry Solutions (ATIS) and NENA standards (i3 SIP).

The National Emergency Number Association (NENA) i3 standard defines how emergency IP-based 9-1-1 calls from OSPs are routed to determine the most appropriate PSAP to receive the call. Every call is routed based on the location that accompanies the call. In addition, the NENA i3 standard defines how different NGCS networks must interconnect in order to allow NG9-1-1 calls to be exchanged between the networks.

OSP related interface standards are defined in two references:

1. The Internet Engineering Task Force (IETF) Best Current Practice for Communications Services in Support of Emergency Calling (RFC6881).
2. The Alliance for Telecommunications Industry Solutions (ATIS) is the normative body responsible for OSPs and has developed to the same best current practice the ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination (ATIS-0700015).

   Note: Emergency calls compliant to the ATIS standard for delivery to an Emergency Services IP Network (ESInet) will conform to NENA's i3 recommendations.

Throughout the document, the reference to OSP is used in a generic way to encompass true Originating Service Providers as well as, depending on the context, peer networks ingressing or transferring calls to the VESTA Router Service.

NOTES

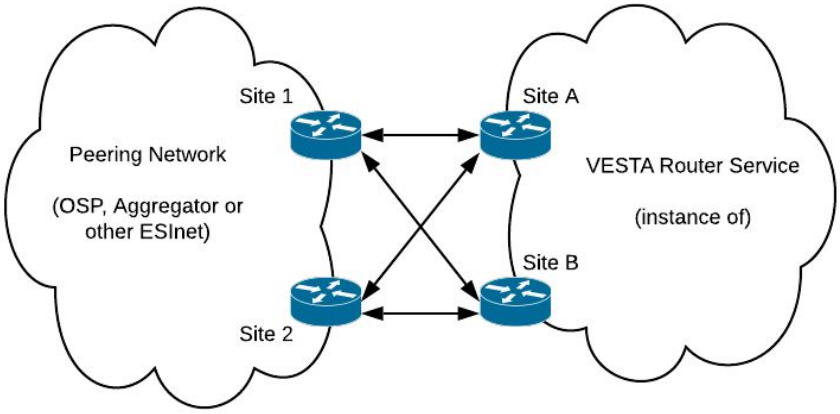
Detailed specifications around DNS support and IPv6 support are the objective guidelines. Currently it is understood that not all cases and deployments are fully compliant.

ARCHITECTURE OVERVIEW

INTERCONNECTION MODEL AND CALL CAPACITY

Interconnection between the Peering Network (OSP, Aggregator or other ESInet) and an instance of VESTA Router Service is a redundant interconnection model as illustrated in the following diagram.

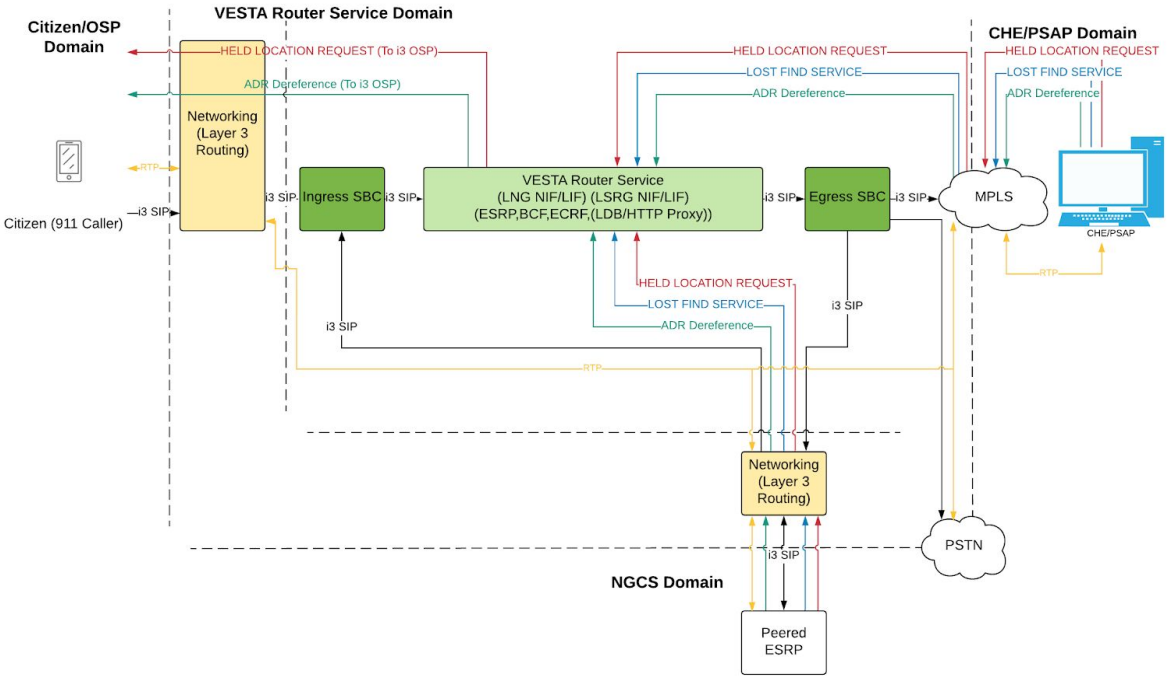
Fully Redundant Interconnection Model



Capacity, or number of simultaneous calls, between the Peering Network and the VESTA Router Service instance is determined by mutual agreement. There is currently no programmatic method to enforce a call volume limit (other than the receiving entity responding with a SIP messaging to reject calls above some threshold) and it is expected each entity will cooperatively use the facilities per agreements. Denial of Service (DOS) attacks or similar network scenarios will be handled according to the entities network management functions.

DIAGRAM

This diagram is showing the different types of calls that can be received and handled by the VESTA Router service as they were described in the previous section.



DEMARCATION POINTS

For the scope of this document, the pertinent demarcation points are the borders between the VESTA Router Service domain and the Citizen/OSP and Peer NGCS domains as represented in the diagram above.

CONNECTION REQUIREMENTS

NETWORK PROTOCOLS

SIP interconnection allows OSPs to deliver 9-1-1 calls via IP to the VESTA Router Service network, which will then result in the call being routed to the appropriate answering point. VESTA Router Service presently supports only IPv4.

VESTA Router Service implementation of SIP is based on RFC-3261 (SIP: Session Initiation Protocol) and RTP implementation is based on RFC-3550 (RTP: A Transport Protocol for Real-Time Applications). The VESTA Router Service also supports many other RFCs listed in the annexe section.

If the need arises to support services and protocols such as 183 - early media or provisional ACKs, these specifics can be negotiated.

PHYSICAL CONNECTIVITY

Vesta Router Service requires each SIP OSP (or OSP aggregator) to deliver their 9-1-1 originated calls via dedicated IP circuits to each of the specified VESTA Router Service Points of Interconnect (POI) for the service area.

Vesta Router Service preference is for a copper Ethernet handoff via a standard RJ-45 connector. Vesta Router Service can also support Ethernet over single mode fiber optic media with LC connectors. The OSP is responsible for establishing a cross connect to the VESTA Router Service demarc.

SIP is expected to use the standard port of 5060. RTP will use a UDP port range determined by the OSP and agreed upon by Vesta Router Service. OSPs connecting to Vesta Router Service via SIP should expect to see these ports advertised from Vesta Router Service SBCs.

The OSPs will implement a SIP failover design to each of Vesta Router Service geographically diverse data centers. This ensures any 9-1-1 call can be delivered to Vesta Router Service, even in the event of a disruption to one OSP connection to a Vesta Router Service data center.

Per NENA's recommendation for i3, circuits should be correctly sized to provide the equivalent of the P.01 grade of service.

NETWORK REDUNDANCY

The VESTA Router Service ESInet is a completely redundant, geo-diverse environment. It is expected that Originating Service Providers (OSPs) and other NG9-1-1 Service Providers are connecting to the VESTA Router Service NG9-1-1 network at a minimum of two of its POI locations and that each connection is capable of supporting the entire volume of 9-1-1 calls.

TRANSPORT DESIGN

1. The transport protocol for SIP shall be TCP. TLS with connection reuse (RFC 5923) shall be used in the future. Certificates management guidelines will be defined in a future version of the document.
2. RTP media packets are transported with UDP.
3. Elements ingressing calls may use either one TLS connection for all the dialogs or a separate TLS connection per each dialog (preferred solution).
4. The VESTA Router Service shall reuse the TLS connection(s) for all SIP responses and new SIP requests in the same dialog.
5. In case of a connection failure:
    a. VESTA Router Service shall establish a new TLS connection towards an Elements ingressing calls using the connection parameters advertised by the Elements ingressing calls in SIP headers (Via or Contact).
    b. Elements ingressing calls shall establish a new TLS connection towards the VESTA Router Service using the VESTA Router Service FQDN and SRV records.

IP ROUTING DESIGN

ADDRESSING

Both IPv4 and IPv6 support is required. IPv6 support can be limited to the edges/boundaries of the VESTA Router Service network. End to end IPv6 support within the VESTA Router Service network is a guideline that should be aimed for.

MTU

Network infrastructure supports MTU of 1500 bytes which has been defined as the standard MTU by the NENA specifications for Next-Generation 9-1-1 services.

QoS REQUIREMENTS

GENERAL

The VESTA Router Service is implementing QoS policies (including traffic DSCP marking) to meet specific Service Level Agreements (SLA). This service level is composed of multiple categories, one of them being adequate packet delivery measured in terms of Jitter, Latency and Packet Loss.

These QoS policies are detailed in the VESTA Router MSI ESInet QoS Standards. They slightly differ from the NENA recommendations since they reflect the latest industry standards, learnings and experiences from MSI. These guidelines (especially DSCP marking) are not a mandatory part of this interface specification (NNI) since each party inter-connecting using that NNI can decide on its own scheme and re-mark packets on its edge as long as the intention in terms of quality of service is met.

In order to support interoperability, the ESInet shall only support G.711 uLaw codec with a 20ms packetization rate. Networks supporting emergency services shall not use silence suppression. It is desired by the Public Safety community to hear as much background noise as possible.

PACKET LOSS

As per NENA specifications, an overall (end-to-end) packet loss budget for maintaining intelligible voice transmission is about 5%. VESTA Router Service is putting more stringent specifications in place. They can be found in the VESTA Router MSI ESInet QoS Standards. Out of that packet loss budget, approximately ½ of the packet loss should be allocated for ESInets, so origination service providers are required to maintain a packet loss of less than ½ of the packet loss total budget.

JITTER

As per NENA specifications, jitter should not exceed 20 ms. VESTA Router Service is putting more stringent specifications in place.Specifications can be found in the VESTA Router MSI ESInet QoS Standards.

LATENCY

As per NENA specifications, the one-way transit delay (i.e., end to end, mouth to ear) for real-time media packets should not exceed 150 milliseconds (ITU-T-G.114). VESTA Router Service is putting more stringent specifications in place. They can be found in the VESTA Router MSI ESInet QoS Standards.

SECURITY

ESInets should comply with the NENA-STA-010.2. It is a best practice to ensure that the following Security elements are considered when securing an ESInet:

- SBCs for NNI with NGCS provider network to provide firewall-like security for call signaling and call media streams.
- Firewall in parallel with the SBC in order to be able to process all the different types of traffic.

Encryption of specific communications protocols:

- SIPS (SIP messages over a Transport Layer Security-encrypted channel (SIP RFC 3261))
    - The certificates must be CA signed (either issued by PCA (PSAP Credentialing Agency) or a 3rd party CA).
    - Key exchange algorithms must support PFS (Perfect Forward Secrecy).
    - Both Elements ingressing calls and VESTA Router Service shall support certificate revocation.
    - Certificates issuing, deployment and renewal process is to be defined.
- SRTP (Secure Real-time Transport Protocol (RFC 3711)) (Future)
- HTTPS (Hypertext Transfer Protocol Secure or HTTP/TLS (RFC 2818))
- DNSSEC (Domain Name Security Extensions (RFCs 4033, 4034, 4035))

DNS

NENA-STA-010 prescribes the use of FQDNs instead of using IP addresses in URIs. VESTA Router Service will be supporting these guidelines. DNS will be required to resolve domain names to IP addresses as well as to discover resources, internal and external to a domain.

Note: Some existing deployments may not follow these guidelines. In some situations, dual specific IPs are provided by each party interconnecting. As mentioned earlier in the document, support of DNS throughout the VESTA Router Service is a guideline that should be aimed for moving forward.

The Originating Network is required to provide its own DNS to resolve their respective domain names to routable IP addresses which will be assigned by the Origination Networks for their NG9-1-1 service nodes. These IP addresses will only be routable over private dedicated connections and must not be reachable from the Internet.

Finally, from NENA-STA-010.2: “DNS servers must be highly redundant, and resolvers must be able to use cached records even if they have expired if they lose connections to authoritative DNS servers to resolve names”.

MEDIA INTERFACE

SPECIFICATIONS

1. Media interface shall use RTP protocol (RFC 3550) over UDP.

   Note: SRTP is not yet supported, but will be in the future.

2. Elements ingressing calls must offer its RTP media connection endpoint in SDP which is reachable by VESTA Router Service (not NAT'ed).
3. Elements ingressing calls shall support RTCP on media interface.
4. The vocoder supported shall be G.711U (PCMU).
5. Silence suppression is not supported and must not be used.
6. Loss of RTP shall trigger termination of the session.
7. Loss of RTP detection - the Elements ingressing calls should detect RTP loss and send a re-INVITE (preferably) or send BYE after (TBD, e.g. 30 seconds) seconds of RTP gap.
8. Both parties shall anchor the media.

GENERAL INFORMATION

Audio received on an ESInet is typically forwarded unmodified in a transparent manner. Endpoints responsible to generate audio streams (OSPs and PSAPs) have the mandate to respect some criteria which are listed below. ESInets shall be engineered in a manner that they will not degrade the audio streams from these characteristics point of view:

- Media speech power: The average speech power level of media transmitted from the OSP to ESInet shall not exceed -9 dBm0 for any interval of 3 seconds or greater. It is also expected that media will not have been previously clamped at a maximum level, regardless of the average power level at the NNI. Typical average speech power should be -15 to -25 dBm0.
- Media speech level loss across the OSP: 0 dB is typical. 3 dB is possible. Never greater than 6 dB.
- Echo from OSP into the ESInet: There should never be any echo from the OSP back into the ESInet that is greater than 300 ms in delay. Echo into ESInet that is between 50–300 ms should be at a minimum 55 dB lower than the source signal into the OSP (i.e., Echo Return Loss (ERL) > 55 dB). For echoes less than 50 ms, ERL > 30 dB.

HELD & ADDITIONAL DATA

It is expected that OSPs, Originating/Intermediate ESRPs and Split Rate Centers ESRPs as well as i3 peer NGCS networks may need to support interfaces to dereference (client & server sides depending on the context) location and additional data. These operations are supported in compliance with the NENA and RFC specifications. Examples are provided in the document.

SIP INTERFACE STANDARD FOR EMERGENCY CALL ACCEPTANCE

i3 SUPPORTING STANDARDS

The Emergency calls originating from Originating Service Providers (OSP) should conform to ATIS-0700015. The OSP's Routing Determination Function (RDF) may query the NGCS' ECRF servers, specifying in the findService request the service urn:service:sos, to determine where to address the emergency calls (ECRF query URL(s) to be provided separately). If unable to contact the ECRF servers (by configuration or at run time), the OSP may statically address the emergency call to the ESRP's default ingress queue.

It is of significance that the i3 protocol requires a location object to be included in call presentation messaging (e.g., SIP INVITE message). In i3 SIP, caller's location information is conveyed by either Location by Value (LbV) and/or Location by Reference (LBR).

i3 SIP (Applicable to OSPs, Originating/Intermediate ESRPs and Split Rate Centers ESRPs)

Emergency calls compliant to ATIS-0700015 (which are referred to as i3 SIP) must have to adhere to the following:

- Request URI must be urn:service:sos.
- Topmost Route: header must specify the SIP(S) URI where the call is addressed.
- INVITE must include both a From header and a P-Asserted-Identity: header which is the callback number of the calling device.
- INVITE must include at least one Geolocation: header as defined in RFC6442.
- INVITE must include a Geolocation-Routing header as defined in RFC6442 with its value set to true.
- If more than one Geolocation header is specified, the first entry will be used for routing.
- INVITE must include a Call-Info: header of purpose EmergencyCallData.ProviderInfo as defined in RFC7852.
- INVITE must include a Call-Info: header of purpose EmergencyCallData.ServiceInfo as defined in RFC7852.
- INVITE may include a Call-Info: header of purpose EmergencyCallData.SubscriberInfo as defined in RFC7852 if information is known.
- INVITE may include a Call-Info: header of purpose nena-CallId as specified in section 3.1.6 of the NENA i3 standard.
- INVITE may include a Call-Info: header of purpose nena-IncidentId as specified in section 3.1.7 of the NENA i3 standard.

i3 PEER NGCS NETWORKS (Applicable to calls being transferred)

Emergency calls originating from a peer NGCS network are expected to be fully i3 compliant and triggered by a PSAP located on the peer network requesting a conference/transfer. Such calls are expected to specify an Emergency Incident Data Object (EIDO) which will carry information on the 9-1-1 call and related incident. Calls from a peer NGCS network compliant to i3 (which are also referred to as i3 SIP) have to adhere to the following:

- Request URI must be urn:service:sos.
- Topmost Route: header must specify the SIP(S) URI where the call is addressed.
- INVITE must include a From: header and may include a P-Asserted-Identity: header which is the identity of the element or agent placing the call.
- INVITE must include a Call-Info: header of purpose eido which either points to an EIDO structure found in the body of the INVITE or a reference to be used to obtain the EIDO as illustrated in section 5.8 of the i3 standard.
- INVITE must include a Call-Info: header of purpose nena-CallId as specified in section 3.1.6 of the NENA i3 standard.
- INVITE must include a Call-Info: header of purpose nena-IncidentId as specified in section 3.1.7 of the NENA i3 standard.

ASSUMPTIONS

1. SIP Back-to-Back User Agent (B2BUA) functions can be used in support of network interconnection.
2. SIP is used for call control signaling. The SIP messages can contain a multi-part MIME body. This might cause the SIP message to exceed the 1300 byte recommendation for UDP messages. Fragmented UDP or TCP is supported for these messages.
3. RTP is used for voice transport. RTP uses UDP.
4. RTP is used for Real-Time Text (RTT) transport, RTP uses UDP.
5. TCP is used for Message Session Relay Protocol (MSRP) transport.
6. G.711 uLaw encoding at 20ms packetization is used within the ESInet. No silence suppression is allowed due to PSAP requirements.
7. It is expected that DTMF tones are transported as RTP Events (following RFC-4733 which replaces RFC-2833). DTMF will be transported using RTP Events if generated by the originating entity. DTMF tones embedded within the RTP audio stream will not be detected and converted to RTP Events by VESTA Router Service.
    a. Ingress I3 SIP (Receiving RTP packets): Originating networks should provide DTMF as RTP Events. VESTA Router will not convert in band DTMF tones to RTP Events.
    b. PSAP to NGCS (VESTA Router Service UNI): PSAP must support receiving DTMF tones both as RTP Events and as in band DTMF (as per SDP negotiation).
8. The i3 SIP calls to the VESTA Router Service ESRP must have Location by Value (LbyV) or Location by Reference (LbyR). For LbyR, the HTTPS URL must be reachable over the same IP interconnect points used to facilitate SIP signalling and may be globally routable.
9. The i3 SIP calls to the ESRP can have Additional Data by Value or by Reference . If by Reference, the HTTPS URL must be reachable over the same IP interconnect points used to facilitate i3 SIP signalling and may be globally routable.
10. Elements ingressing calls shall allow configuration of the SIP Timer_B (Call Setup Time). Due to the emergency nature of provided call service, default SIP call timers are not satisfactory (i.e. users cannot wait 30 seconds for a ringtone.).
11. Elements ingressing calls shall support “SIP 302 Moved Temporarily” message according to RFC 3261.
12. Elements ingressing calls shall maintain the connection via heartbeat mechanism using SIP OPTIONS (during periods of inactivity).
13. Elements ingressing calls shall use SIP re-INVITE messages for SIP session keep-alive according to RFC 4028.
14. Elements ingressing calls will be provided with VESTA Router Service FQDN which must be resolved using DNS SRV records when sending SIP requests/responses. Elements ingressing calls shall try

each address found in SRV records until a VESTA Router Service is contacted (according to RFC 3261 and RFC 3263).

SIP HEADER REQUIREMENTS

For i3 SIP, the Request Line must contain a service URN. The service URN must be urn:service:sos as defined in RFC 5031.

Example: INVITE urn:service:sos SIP/2.0

SIP Headers

Header	i3 SIP	Reference	Details
Accept	Optional	RFC 3261 Section 20.1	Example: Allow: INVITE, ACK, OPTIONS, PRAC, BYE
Allow	Optional	RFC 3261 Section 20.5	Shall be present in the initial INVITE and its associated 200-OK response. Example: Allow: INVITE, ACK, OPTIONS, PRAC, BYE
Call-ID	Mandatory	RFC 3261 Section 20.8	Example: Call-ID: cb03a0b53
Call-Info	Mandatory	RFC 3261 Section 20.8	Must include NENA Call Tracking and Incident Identifiers and additional data about the call and caller or reference to an Emergency Incident Data Object (EIDO). Example: Call-Info:https://www.example.com/23sed de3; purpose="EmergencyCallData.ProviderInfo"
Contact	Mandatory	RFC 3261 Section 20.10	If the originator of the call is capable of processing conference-related REFER requests then isfocus must be specified. The Parties will mutually agree upon implementation of this i3 SIP function. Example: Contact:<sip:3125551234@carrier.example .com>
ContentLength	Conditional	RFC 3261 Section 20.14	Must be present if there is a SIP body. Example: 256
Content-Type	Conditional	RFC 3261 Section 20.15	Must be present if there is a SIP body with a MIME type.

			Example: Content-Type: multipart/mixed; boundary=boundary1
CSEQ	Mandatory	RFC 3261 Section 20.16	Example: CSEQ: 127 INVITE
From	Mandatory	RFC 3261 Section 20.20	Must contain ANI (wireline) or pANI (wireless). Examples: From:<sip:3125551234@carrier.example.com;user=phone>;tag=171828 From:<tel:3125551234>;tag=171828
Geolocation	Mandatory	RFC 6442 Section 4.1	Provides location by value or by reference. The Geolocation header will either contain a location reference URI, or it will contain a Content-ID (CID) that points to the location in the message body where the location value is found. For LbyR, the ESInet supports HTTP and HTTPS as pointers to the Location Object. Example of location-by-reference: Geolocation:<https:lrf.lrfprovider.net/9xkei90z> Example of location-by-value: Geolocation: <cid:target123@someoperator.example.com>
GeolocationRouting	Mandatory	RFC 6442 Section 4.2	Define if location can be used for routing and should be set to yes.
History-Info	Passthrough	RFC 4244	Except if the call is alternate routed, a History-Info header will be added if it exists.

Max-Forwards	Mandatory	RFC 3261 Section 20.22	Example: Max-Forwards: 70
MIME-Version	Optional	RFC 3261 Section 20.24	Present if there is a SIP body with a MIME type. If none, version 1 will be assumed. Example: MIME-Version: 1.0
P-Access-Network-Info	Passthrough	RFC 3455	May indicate cell site. Example: P-Access-Network-Info:3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=0AE212345608A41F9
P-Asserted-Identity	Conditional	RFC 3325	The P-Asserted-Identity must represent the TN, MDN, or MSISDN of the caller that can be used to call the caller back. In the case signaling includes both a pANI and a callback number, the P-Asserted-Identity field must be the callback number of the call. Example: P-Asserted-Identity:<sip:+13125551234@carrier.example.net;user=phone>
P-ChargingVector	Passthrough	RFC 3455	May identify the originating carrier. Example: P-Charging-Vector:icid=34c23c445902;idid-generatedat=ecscf.carrier.example.net;orig-ioi=carrier.example.net
P-PreferredIdentity	Passthrough	RFC 3325	Example: P-Preferred-Identity:<sip:+13125551234@carrier.example.net;user=phone>
Record-Route	Optional	RFC 3261 Section 20.30	Example: Record-Route:<sip:sbc.carrier.example.com;lr>

Route	Mandatory	RFC 3261 Section 20.34	The top-most Route header must contain the target of the call. Example: Route: <sip:sos@psap.example.com>
Supported	Optional	RFC 3261 Section 20.37	Example: Supported: geolocation
To	Mandatory	RFC 3261 Section 20.39	The To header must be urn:service:sos Example: To: urn:service:sos
Unsupported	Optional	RFC 3261 Section 20.40	Example: Unsupported: geolocation
Via	Mandatory	RFC 3261 Section 20.42	Example: Via:SIP/2.0/UDP[aaa:bbb:ccc:ddd]:1357;branch=z9hG4bKnashds7

EXAMPLES

As the title mentions, these messages are provided as examples (Some of the additional data examples are coming from RFC-7852) and the implementations may not contain all fields described in those examples. One example of where this note is applicable is the vcard schema.

INVITE for an ATIS-0700015 Wireless Call Example

```
INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/UDP 10.255.192.2:5060; branch=z9hG4bK73aa7b525e2609022cde98487416cd9;rport
Max-Forward: 70
From: <sip:8195551212@osp.com>;tag=7ce596dd83f28456882cc41e7c896714
To: <urn:service:sos>
P-Asserted-Identity: <sip:8195551212@osp.com>
Route: sip:sos@esrpab.ng911.ca
Geolocation: <https://lrf.osp.com/getlocation?tn=8195551212>
Geolocation-Routing: yes
Call-ID: 6-70736@10.255.194.202
CSeq: 200 INVITE
Contact: < sip:8195551212@osp.com >
Expires: 300
User-Agent: IMS-15.3.6
Call-Info: <https://lrf.osp.com/getprovider?tn=8195551212>;
purpose=EmergencyCallData.ProviderInfo
Call-Info: <https://lrf.osp.com/getservice?tn=8195551212>;
purpose=EmergencyCallData.ServiceInfo
Call-Info: <https://lrf.osp.com/getsubscriber?tn=8195551212>;
purpose=EmergencyCallData.SubscriberInfo
Content-Length:207
Content-Type: application/sdp
v=0
o=user1 53655765 2353687637 IN IP4 10.255.194.202
s=-
c=IN IP4 10.255.194.202
t=0 0
m=audio 6000 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

INVITE for an inter-NGCS i3 call Example

```
INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/UDP 10.255.192.2:5060; branch=z9hG4bK73aa7b525e2609022cde98487416cd9;rport
Max-Forward: 70
From: <sip:AgentJohnSmith@primaryPSAP.com>;tag=7ce596dd83f28456882cc41e7c896715
To: <urn:service:sos>
P-Asserted-Identity: < sip:AgentJohnSmith@primaryPSAP.com >
Route: sip:sos@secondaryPSAP.com
Call-ID: 7-70737@10.255.194.202
CSeq: 200 INVITE
Contact: <827tdah@10.255.192.2:5060>;isfocus
Expires: 300
User-Agent: VESTARouter-2.0.346
Call-Info: <urn:nena:uid:callid:jq3atrfab2jczi7:inbcf.VESTARouter.com>; purpose=nena-CallId
Call-Info: <urn:nena:uid:incidentid:7dldqzvuw6hx17e:inbcf:VESTARouter.com>;
purpose=nena-IncidentId
Call-Info: <https://eidd.primarypsap.com/geteidd?callid=jq3atrfab2jczi7:inbcf.VESTARouter.com
>;
purpose=eido
Content-Length:207
Content-Type: application/sdp


v=0
o=user1 53655765 2353687637 IN IP4 10.255.194.202
s=-
c=IN IP4 10.255.194.202
t=0 0
m=audio 6000 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

HELD locationResponse Example

```
<?xml version="1.0" encoding="utf-8"?>
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
       <presence xmlns="urn:ietf:params:xml:ns:pidf"
        entity="pres:3650n87934c@ls.example.com">
         <tuple id="b650sf789nd">
          <status>
           <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
            <location-info>
             <Point xmlns="http://www.opengis.net/gml" srsName="urn:ogc:def:crs:EPSG::4326">
              <pos>-34.407 150.88001</pos>
             </Point>
            </location-info>
            <usage-rules
             xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy">
             <gbp:retention-expiry>2018-09-11T03:42:28+00:00
             </gbp:retention-expiry>
            </usage-rules>
            <method>GPS</method>
           </geopriv>
          </status>
         <timestamp>2006-01-10T03:42:28+00:00</timestamp>
         </tuple>
        </presence>
      </locationResponse>
```

ADR Response – Provider Info Example

```
<?xml version="1.0" encoding="UTF-8"?>
   <ad:EmergencyCallData.ProviderInfo
       xmlns:ad="urn:ietf:params:xml:ns:EmergencyCallData:ProviderInfo">
       <ad:DataProviderReference>string0987654321@example.org
       </ad:DataProviderReference>
       <ad:DataProviderString>Example VoIP Provider
       </ad:DataProviderString>
       <ad:ProviderID>urn:nena:companyid:ID123</ad:ProviderID>
       <ad:ProviderIDSeries>NENA</ad:ProviderIDSeries>
       <ad:TypeOfProvider>Telecom Provider</ad:TypeOfProvider>
       <ad:ContactURI>tel:+1-201-555-0123</ad:ContactURI>
       <ad:Language>en</ad:Language>
       <ad:DataProviderContact
           xmlns="urn:ietf:params:xml:ns:vcard-4.0">
                   <vcard>
                       <fn><text>Hannes Tschofenig</text></fn>
                       <n>
                           <surname>Hannes</surname>
                           <given>Tschofenig</given>
                           <additional/>
                           <prefix/>
                           <suffix>Dipl. Ing.</suffix>
                       </n>
                       <bday><date>--0203</date></bday>
                       <anniversary>
                           <date-time>20090808T1430-0500</date-time>
                       </anniversary>
```

```
<gender><sex>M</sex></gender>
<lang>
    <parameters><pref><integer>1</integer></pref>
    </parameters>
    <language-tag>de</language-tag>
</lang>
<lang>
    <parameters><pref><integer>2</integer></pref>
    </parameters>
    <language-tag>en</language-tag>
</lang>
<org>
    <parameters><type><text>work</text></type>
    </parameters>
    <text>Example VoIP Provider</text>
</org>
<adr>
    <parameters>
        <type><text>work</text></type>
        <label><text>Hannes Tschofenig
            Linnoitustie 6
            Espoo , Finland
            02600</text></label>
    </parameters>
    <pobox/>
    <ext/>
    <street>Linnoitustie 6</street>
    <locality>Espoo</locality>
    <region>Uusimaa</region>
    <code>02600</code>
    <country>Finland</country>
</adr>
<tel>
    <parameters>
        <type>
            <text>work</text>
            <text>voice</text>
        </type>
    </parameters>
    <uri>tel:+358 50 4871445</uri>
</tel>
<tel>
    <parameters>
        <type>
            <text>work</text>
            <text>main-number</text>
            <text>voice</text>
        </type>
    </parameters>
    <uri>tel:+358 50 5050505</uri>
</tel>
<email>
    <parameters><type><text>work</text></type>
    </parameters>
    <text>hannes.tschofenig@nsn.com</text>
</email>
<geo>
    <parameters><type><text>work</text></type>
    </parameters>
```

```
                        <uri>geo:60.210796,24.812924</uri>
                    </geo>
                    <key>
                        <parameters><type><text>home</text></type>
                        </parameters>
                        <uri>
                          http://www.example.com/key.asc
                        </uri>
                    </key>
                    <tz><text>Finland/Helsinki</text></tz>
                    <url>
                        <parameters><type><text>home</text></type>
                        </parameters>
                        <uri>http://www.tschofenig.priv.at</uri>
                    </url>
                </vcard>
        </ad:DataProviderContact>
    </ad:EmergencyCallData.ProviderInfo>
```

ADR Response – Service Info Example

```
<?xml version="1.0" encoding="UTF-8"?>
       <svc:EmergencyCallData.ServiceInfo
              xmlns:svc="urn:ietf:params:xml:ns:EmergencyCallData:ServiceInfo">
              <svc:DataProviderReference>lrf@osp.com
              </svc:DataProviderReference>
              <svc:ServiceEnvironment>Business</svc:ServiceEnvironment>
              <svc:ServiceType>POTS</svc:ServiceType>
              <svc:ServiceMobility>Fixed</svc:ServiceMobility>
       </svc:EmergencyCallData.ServiceInfo>
```

ADR Response – Device Info Example

```
<?xml version="1.0" encoding="UTF-8"?>
   <dev:EmergencyCallData.DeviceInfo
       xmlns:dev="urn:ietf:params:xml:ns:EmergencyCallData:DeviceInfo">
       <dev:DataProviderReference>d4b3072df.201409182208075@example.org
       </dev:DataProviderReference>
       <dev:DeviceClassification>fixed</dev:DeviceClassification>
       <dev:DeviceMfgr>Nokia</dev:DeviceMfgr>
       <dev:DeviceModelNr>Lumia 800</dev:DeviceModelNr>
       <dev:UniqueDeviceID TypeOfDeviceID="IMEI">35788104
       </dev:UniqueDeviceID>
   </dev:EmergencyCallData.DeviceInfo>
```

ADR Response – Comment Example

```
<?xml version="1.0" encoding="UTF-8"?>
   <com:EmergencyCallData.Comment
        xmlns:com="urn:ietf:params:xml:ns:EmergencyCallData:Comment">
      <com:DataProviderReference>string0987654321@example.org
      </com:DataProviderReference>
      <com:Comment xml:lang="en">This is an example text.</com:Comment>
   </com:EmergencyCallData.Comment>
```

ADR Response – Subscriber Info Example

```
<?xml version="1.0" encoding="UTF-8"?>
   <sub:EmergencyCallData.SubscriberInfo
        xmlns:sub=
            "urn:ietf:params:xml:ns:EmergencyCallData:SubscriberInfo"
        privacyRequested="false">
       <sub:DataProviderReference>FEABFECD901@example.org
       </sub:DataProviderReference>
       <sub:SubscriberData xmlns="urn:ietf:params:xml:ns:vcard-4.0">
            <vcard>
                  <fn><text>Simon Perreault</text></fn>
                  <n>
                      <surname>Perreault</surname>
                      <given>Simon</given>
                      <additional/>
                      <prefix/>
                      <suffix>ing. jr</suffix>
                      <suffix>M.Sc.</suffix>
                  </n>
                  <bday><date>--0203</date></bday>
                  <anniversary>
                      <date-time>20090808T1430-0500</date-time>
                  </anniversary>
                  <gender><sex>M</sex></gender>
                  <lang>
                      <parameters><pref><integer>1</integer></pref>
                      </parameters>
                      <language-tag>fr</language-tag>
                  </lang>
                  <lang>
                      <parameters><pref><integer>2</integer></pref>
                      </parameters>
                      <language-tag>en</language-tag>
                  </lang>
                  <org>
                      <parameters><type><text>work</text></type>
                      </parameters>
                      <text>Viagenie</text>
                  </org>
                  <adr>
                      <parameters>
                          <type><text>work</text></type>
                          <label><text>Simon Perreault
```

```
            2875 boul. Laurier, suite D2-630
            Quebec, QC, Canada
            G1V 2M2</text></label>
    </parameters>
    <pobox/>
    <ext/>
    <street>2875 boul. Laurier,
            suite D2-630</street>
    <locality>Quebec</locality>
    <region>QC</region>
    <code>G1V 2M2</code>
    <country>Canada</country>
</adr>
<tel>
    <parameters>
        <type>
            <text>work</text>
            <text>voice</text>
        </type>
    </parameters>
    <uri>tel:+1-418-656-9254;ext=102</uri>
</tel>
<tel>
    <parameters>
        <type>
            <text>work</text>
            <text>voice</text>
            <text>main-number</text>
        </type>
    </parameters>
    <uri>tel:+1-418-555-0000</uri>
</tel>
<tel>
    <parameters>
        <type>
            <text>work</text>
            <text>text</text>
            <text>voice</text>
            <text>cell</text>
            <text>video</text>
        </type>
    </parameters>
    <uri>tel:+1-418-262-6501</uri>
</tel>
<email>
    <parameters><type><text>work</text></type>
    </parameters>
    <text>simon.perreault@viagenie.ca</text>
</email>
<geo>
    <parameters><type><text>work</text></type>
    </parameters>
    <uri>geo:46.766336,-71.28955</uri>
</geo>
<key>
    <parameters><type><text>work</text></type>
    </parameters>
    <uri>
    http://www.viagenie.ca/simon.perreault/simon.asc
```

```
                    </uri>
                </key>
                <tz><text>America/Montreal</text></tz>
                <url>
                    <parameters><type><text>home</text></type>
                    </parameters>
                    <uri>http://nomis80.org</uri>
                </url>
        </vcard>
    </sub:SubscriberData>
</sub:EmergencyCallData.SubscriberInfo>
```

REFERENCE DOCUMENTS

NENA-STA-010.2 Detailed Functional and Interface Specification for the NENA i3 Solution

ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination (document number ATIS-0700015)

NENA-INF-016.2-2018 Emergency Services IP Network Design (ESIND) Information Document

International Telecommunications Union (ITU) One-way Transmission Time (G.114)

VESTA Router MSI ESInet QoS Standards(Link)

ACRONYMS

Acronym	Definition
ADR	Additional Data Repository
ATIS	Alliance for Telecommunications Industry Solutions
BCF	Border Control Function
CLEC	Competitive Local Exchange Carrier
CO	Central Office
DNS	Domain Name Service
DSCP	Differentiated Services Code Point
ECRF	Emergency Core Routing Function
ESInet	Emergency Services Internetwork
ESRP	Emergency Services Routing Proxy
HELD	HTTP-Enabled Location Delivery
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standards
IT	Information Technology
ITU	International Telecommunication Union
LDB	Legacy Database
LIS	Location Information Service
LRF	Location Retrieval Function
MPLS	Multiprotocol Label Switching
MTU	Message Transfer Unit
NENA	National Emergency Number Association
NGCS	Next Generation Core Services
NIST	National Institute of Standards and Technology
NNI	Network-to-Network Interface

OSP	Originating Service Provider
POI	Point of Interconnection
PRF	Policy Routing Function
PRR	Policy Routing Rules
PSAP	Public Safety Answering Point
QoS	Quality of Service
RDF	Routing Determination Function
RDN	Routing Directory Number / ReDirection Number
RTT	Real-time Text
SBC	Session Border Controller
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier

APPENDIX

APPENDIX 1 : RFC DESCRIPTIONS

RFC-2475: An Architecture for Differentiated Services

RFC-2818: HTTP Over TLS

RFC-2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

RFC-3261: SIP: Session Initiation Protocol

RFC-3262: Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

RFC-3263: Session Initiation Protocol (SIP): Locating SIP Servers

RFC-3264: An Offer/Answer Model with the Session Description Protocol (SDP)

RFC-3311: The Session Initiation Protocol (SIP) UPDATE Method

RFC-3323: A Privacy Mechanism for the Session Initiation Protocol (SIP)

RFC-3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

RFC-3326: The Reason Header Field for the Session Initiation Protocol (SIP)

RFC-3398: Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping

RFC-3455: Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)

RFC-3515: The Session Initiation Protocol (SIP) Refer Method

RFC-3525: Gateway Control Protocol Version 1

RFC-3550: RTP: A Transport Protocol for Real-Time Applications

RFC-3711: The Secure Real-time Transport Protocol (SRTP)

RFC-3761: The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Dyscovery System (DDDS) Application (ENUM)

RFC-3824: Using E.164 numbers with the Session Initiation Protocol (SIP)

RFC-3891: The Session Initiation Protocol (SIP) “Replaces” Header

RFC-4028: Session Timers in the Session Initiation Protocol (SIP)

RFC-4033: DNS Security Introduction and Requirements

RFC-4034: Resource Records for the DNS Security Extensions

RFC-4035: Protocol Modifications for the DNS Security Extensions

RFC-4244: An Extension to the Session Initiation Protocol (SIP) for Request History Information

RFC-4317: Session Description Protocol (SDP) Offer/Answer Examples

RFC-4488: Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription

RFC-4566: SDP: Session Description Protocol

RFC-4694: Number Portability Parameters for the “tel” URI

RFC-4733: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

RFC-4904: Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)

RFC-5031: A Uniform Resource Name (URN) for Emergency and Other Well-Know Services

RFC-5923: Connection Reuse in the Session Initiation Protocol (SIP)

RFC-6442: Location Conveyance for the Session Initiation Protocol

RFC-6665: (Future) SIP-Specific Event Notification

RFC-6881: Best Current Practice for Communicating Services in Support of Emergency Calling

RFC-7852: Additional Data Related to an Emergency Call