Exh. JDW-9
Docket UT-181051
Witness: James D. Webber

BEFORE THE WASHINGTON
UTILITIES AND TRANSPORTATION COMMISSION

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION, **Complainant,** **v.** **CENTURYLINK COMMUNICATIONS, LLC.,** **Respondent.**	**DOCKET UT-181051**

EXHIBIT TO
TESTIMONY OF

JAMES D. WEBBER

ON BEHALF OF STAFF OF
WASHINGTON UTILITIES AND
TRANSPORTATION COMMISSION

National Emergency Number Association Definitions

December 15, 2021

NENA i3 Standard for Next Generation 9-1-1

Abstract: This Standard provides the detailed functional and interface specifications for a post-transition IP (Internet Protocol)-based multimedia telecommunications system, including the Core Services and legacy gateways necessary to support delivery of emergency calls via an IP-based Emergency Services IP network.

NENA i3 Standard for Next Generation 9-1-1

NENA-STA-010.3a-2021
DSC Approval: 05/18/2021
PRC Approval: 07/09/2021
NENA Executive Board Approval: 07/12/2021
ANSI Board of Standards Review Approved: 10/07/2021
Next Scheduled Review Date: 07/12/2024

Prepared by:
National Emergency Number Association (NENA) 911 Core Services Committee, i3 Architecture Working Group

Published by NENA
Printed in USA

as expressed in the retransmission-allowed field. FEs SHOULD honor the "retransmission-allowed" element of the PIDF-LO when laws do not specify privacy is suspended. When laws suspend privacy, FEs SHOULD send location regardless of the value of the "retransmission-allowed" element. When handling non-emergency calls, retransmission-allowed SHOULD be honored.

An entity conforming to this specification that supplies a PIDF-LO for an emergency call MUST use the <provided-by> element to convey its Data Provider Additional Data block, as specified in RFC 7852 [107] Section 4.1. Note that the PIDF-LO supplier's Data Provider block MUST also be conveyed using a Call-Info header field as described in sections 3.1.15 and 4.11, unless the supplier is not in the call path. The <provided-by> element MUST NOT be used to convey any other Additional Data blocks. The "dataProvider" schema [ref3] of the "pidf:geopriv10:dataProvider namespace" [ref4] MUST NOT be used. It is RECOMMENDED that the Data Provider Additional Data block be conveyed by value rather than by reference, to avoid an additional operation to obtain the data.

2.6 xCard/jCard

In many interfaces defined in this and related NG9-1-1 documents, a common need is to provide contact information. For example, in some blocks of Additional Data and in Service/Agency Locator, the identity and contact information is part of the data structure. When contact data is needed, i3 specifies the use of an xCard in eXtensible Markup Language (XML) format per RFC 6351 [113] where the interface must be XML, and a jCard as defined in RFC 7095 [215] when the interface is JSON.

2.7 Emergency Services IP Networks

ESInets are private, managed, and routed IP networks. An ESInet serves a set of PSAPs, a region, a state/province, or a set of states/provinces. ESInets are interconnected to neighboring ESInets so that traffic can be routed from any point in the ESInet to any point in any other ESInet. States/Provinces MAY have a backbone ESInet either directly connecting to all PSAPs in the state/province, or interconnected to all county/parish or regional ESInets. Neighboring states/provinces or regions SHOULD interconnect their ESInets. It is desirable to have a backbone national ESInet in each country to optimize routing of traffic between distant ESInets. Each PSAP MUST be connected to an ESInet, possibly through a Legacy PSAP Gateway.

ESInets MUST accept and route IPv4 and IPv6 packets. All services MUST support IPv4 and IPv6 interfaces. IPv6 is RECOMMENDED for use throughout the ESInet, but cannot be assumed. Within this document there are several interfaces that may require a text representation of an IPv6 address, including in the specification of addresses for media in the Session Description Protocol (SDP). In such interfaces the canonical representation

specified in RFC 5952 [196] MUST be used, including the use of brackets when specifying a port number. Note that originating networks are outside the scope of this document and they may not follow RFC 5952 conventions.

ESInets MUST be accessible from the global Internet, with calls going through the Border Control Function (BCF). This Internet interconnect is RECOMMENDED at the state ESInet level with local or regional ESInets getting Internet connectivity via the state ESInet. Originating networks SHOULD be connected to any ESInet to which they regularly deliver volume traffic via a private connection through the BCF of that ESInet.

An ESInet MUST be capable of withstanding the largest feasible Distributed Denial of Service (DDoS)/Telephone Denial of Service (TDoS) attack. As of this version, that means approximately at least a terabit of mitigation. Network and BCF bandwidth as well as mitigation services may be used to achieve this requirement. DDoS/TDoS mitigation typically requires that traffic be rerouted to a mitigation service. Private connections MUST be able to be so re-routed if mitigation is needed. Connection through the Internet is acceptable, PREFERABLY through a Virtual Private Network (VPN) with the same mitigation caveat.

Note: The effect on emergency calls already in progress when mitigation is enabled will be addressed in a future version of this document.

Access to ESInets MUST be controlled. Only public safety agencies and their service providers may be connected directly to the ESInet. Call origination sources, gateways, and similar elements are outside the ESInet and interconnected through the BCF. However, for security reasons, the ESInet SHOULD NOT be assumed to be a "walled garden."

For Quality of Service (QoS) reasons, IP traffic within an ESInet MUST implement DiffServ (RFC 2474 [218] and 2475 [134]). Differentiated Service Code Points (DSCPs) within the ESInet are drawn from pool 2, with the exception of DSCP value "0000 00" which is the default from Pool 1. Routers MUST respect code points: Functional Elements MUST mark packets they create with appropriate code points. The ESInet edge router MUST perform traffic conditioning for packets entering the ESInet. The following code points MUST be used, so that packets transiting more than one ESInet can receive appropriate treatment. The following Per Hop Behaviors (PHB) on ESInets are RECOMMENDED starting points and MAY be changed based on operational experience:

This table specifies ESInet-specific traffic. Other traffic (e.g., DHCP, ICMP, BGP, etc.) should be marked according to industry standards and best practices.

DSCP	Use	PHB
0000 00	Routine Traffic except as specified below	Default (Best Effort)

DSCP	Use	PHB
0000 11	9-1-1 Call (SIP) Signaling (including non-interactive calls) and emergency call related HTTP/S operations, DNS traffic	AF12
0001 11	9-1-1 Text Media (RTT and MSRP)	AF12
0010 11	9-1-1 Audio Media (9-1-1 Calls and admin calls)	EF
0011 11	9-1-1 Video Media	AF11

Interconnected ESInets represent a DS Region as defined in RFC 2475 [134] and connect to other networks which are distinct DS Regions. The ESInet edge routers SHOULD re-mark code points between the interconnected networks and the ESInet to match the traffic classes ("Use") above as closely as possible, within the terms of any interconnect agreements with such networks. An interconnected network might perform the re-marking at its edge routers, in which case the ESInet edge router's re-marking is a null operation.

All elements in an ESInet SHOULD have a publicly addressable IP address. Network Address Translations (NATs) SHOULD NOT be used within an ESInet. Although NAT use within an ESInet is NOT RECOMMENDED, NATs may be needed in specific deployments, and therefore all network elements MUST operate in the presence of NATs.

It is RECOMMENDED that elements connected to the ESInet not be referred to by their IP address but rather through a hostname using DNS. Use of statically assigned IP addresses SHOULD be limited, and SHOULD NOT be used with IPv6 addresses. Dynamic Host Configuration Protocol (DHCP) (RFC 2131) [147] or Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 8415 [233]) must be implemented on all network elements to obtain IP address, gateway, and other services.

There SHALL NOT be any single point of failure for any critical service or function hosted on the ESInet. Certain services designated as non-critical may be exempt from this requirement. These MUST NOT include the BCF, internal ECRF, ESRP, Logging Service, and security services. Services MUST be deployed to survive disasters, deliberate attacks, and massive failures.

2.8 Service Interfaces

In this document, we make use of three kinds of interfaces:

- Web Services, typically using a Simple Object Access Protocol (SOAP) [148] interface or using Representational State Transfer (REST),
- Simple HyperText Transfer Protocol Secure (HTTPS) (RFC 2818) [153] GET (and in some cases, POST) with retrieval of JSON data structures based on a Uniform Resource Identifier (URI), and
- SIP interfaces, including SIP Subscribe/Notify.

Term or Abbreviation (Expansion)	Definition / Description
CAMA (Centralized Automatic Message Accounting)	A type of in-band analog transmission protocol that transmits telephone number via multi-frequency encoding. Originally designed for billing purposes.
CAP (Common Alerting Protocol)	A general format for exchanging emergency alerts, primarily designed as an interoperability standard for use among warning systems and other emergency information systems. Refer to http://docs.oasis-open.org/emergency/cap/
CDR (Call Detail Record)	A record stored in a database recording the details of a received or transmitted call (from NENA-STA-010). The data information sent to the ALI computer by a remote identifying device (PBX, Call Position Identifier, etc)
cid (Content Identifier [Content-ID])	A unique identifier assigned to a body part that allows the body part to be referenced in a SIP header field.
codec (COder/DECoder)	A standardized means for encoding and decoding media, especially audio and video.
CoS (Class of Service)	A designation in E9-1-1 that defines the service category of the telephony service. Examples are residential, business, Centrex, coin, PBX, VoIP, and wireless Phase II (WPH2).
CPE (Customer Premises Equipment)	Communications or terminal equipment located in the customer's facilities – Terminal equipment at a PSAP.
CSRC (Contributing Source)	As specified in RFC 3550, a source of a stream of RTP packets that has contributed to the combined stream produced by an RTP mixer.
Dereference	The act of exchanging a reference to an item by its value. For example, the dereference operation for location uses a protocol such as SIP or HELD to obtain a location value (PIDF-LO).
DES (Data Encryption Standard)	The data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption. Public key cryptography (PKC) uses two keys, (i.e., one for encryption and one for decryption).
DHCP (Dynamic Host Control Protocol (i2); Dynamic Host Configuration Protocol)	A widely used configuration protocol that allows a host to acquire configuration information from a visited network and, in particular, an IP address.