DISPATCH
Internet-Draft
Intended status: Standards Track
Expires: 14 September 2023

S. Gundavelli
M. Grayson
Cisco

13 March 2023

Emergency 911 Services over Wi-Fi
draft-gundavelli-dispatch-e911-wifi-00.txt

Abstract

Proposed is an approach for supporting emergency 911 services over IEEE 802.11 based Wi-Fi access networks. This approach leverages the legal framework and the building blocks of the OpenRoaming federation for extending emergency 911 calling support to already deployed tens of thousands of OpenRoaming Wi-Fi hotspots. The proposal addresses the key issues in emergency calling, around discovery and authentication to access network supporting emergency services, emergency access credentials, location determination of the emergency caller, and delivering emergency voice service configuration to the device and call routing.

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 14 September 2023.

Table of Contents

1. Introduction

The Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC) is drafting a report to Congress regarding use of Wi-Fi technology to access emergency 911 services when there is no mobile coverage. The report will likely detail non-proprietary standards that can support 911 services over IEEE 802.11 based Wi-Fi access technology. Additional commentary suggests that legal and regulatory changes may be needed to address liability, privacy, and security concerns associated with providing public access to 911 over Wi-Fi.

The study looked at the technical feasibility and cost of:

* making telecommunications service provider-owned Wi-Fi access points, and other communications technologies operating on unlicensed spectrum, available to the general public for access to 9-1-1 services, without requiring any login credentials, during times of emergency when mobile service is unavailable;

* the provision by non-telecommunications service provider-owned Wi-Fi access points of public access to 9-1-1 services during times of emergency when mobile service is unavailable; and

* ther alternative means of providing the public with access to 9-1-1 services during times of emergency when mobile service is unavailable."

We have reviewed these requirements and proposed an approach leveraging the OpenRoaming federation of Wi-Fi access providers and Identity Providers for supporting emergency 911 services over unlicensed Wi-Fi access.

2. Conventions and Terminology

2.1. Conventions

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

2.2. Terminology

All the mobility terms used in this document are to be interpreted as defined in the IETF and 3GPP specifications. For convenience, the definitions for some of the terms are provided below.

Subscription Permanent Identifier (SUPI))

A globally unique 5G Subscription Permanent Identifier (SUPI) is allocated to each subscriber in the 5G System. The SUPI value is provisioned in USIM and UDM/UDR function in 5G Core. The structure of SUPI and its privacy is specified [TS23501]

OpenRoaming (OR)

A federation that provides the framework for connecting unprecedented footprint of millions of Wi-Fi hotspots with identity providers.

Identity Provider (IDP)

An entity that manages identity credentials and policies for devices and provides authentications services.

Access Network Provider (ANP)

An entity providing internet connectivity services.

Passpoint Profile

Passpoint is a Wi-Fi Alliance (WFA) protocol that enables mobile devices to discover and authenticate to Wi-Fi hotspots that provide internet access. Profile includes the user's credentials and the access network identifiers.

Roaming Consortium Identifier (RCOI)

It is a 3-octet, or a 5-octet value carried in the 802.11 beacon information element (IE). It is also sent in the ANQP messages. RCOI identifies the groups or identity providers that are supported by the network.

Connectivity Location Function (CLF)

It maintains mappings between the endpoint's dynamically assigned IP address and its physical location. An enhanced CLF maintains the mapping between the devices' access point identifier (BSSID) and the physical location.

Public Safety Answering Point (PSAP)

A PSAP is a facility where emergency calls are received under the responsibility of a public authority.

Route Determination Function (RDF)

It resolves a physical location, either a civic address or a geo-spatial address to the serving PSAP.

E-CSCF

Enhanced Call Session Control Function. It takes the requests from P-CSCF (Proxy CSCF) and routes the emergency sessions to the PSAP based on CLF and RDF queries.

3. Overview

Following are the key aspects in this approach:

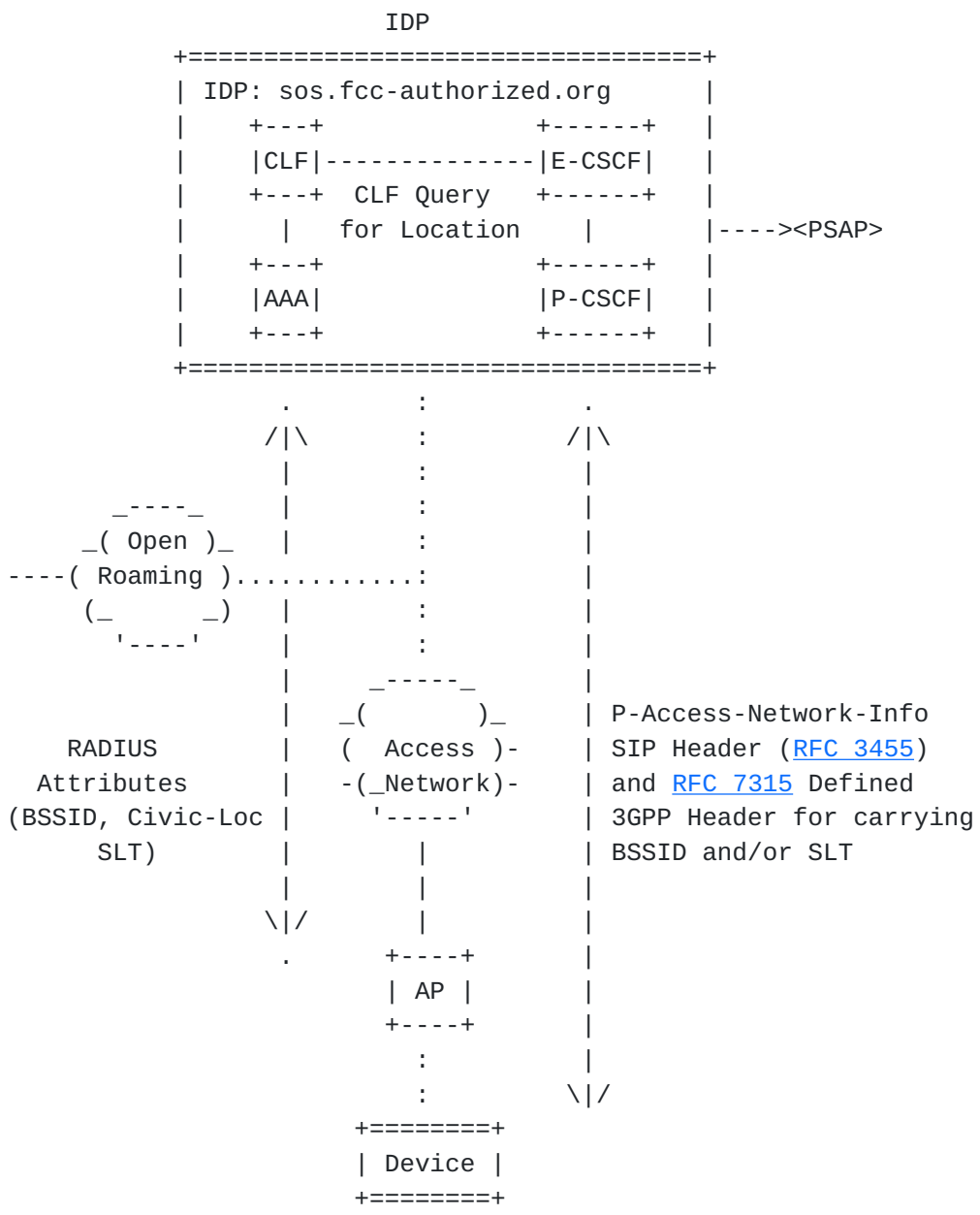


Figure 1: Technical Architecture

There will be a designated Identity Provider (IDP) and designated emergency calling services for supporting emergency 911 service. The AAA server in the IDP supports the realm "@sos.fcc-authorized.org" and the policies for E-911-RCOI (i.e., an E911-specific HotSpot2.0 Roaming Consortium or RCOI). There will also be dedicated P/E-CSCF (Proxy/Emergency Call Services Control Function) for supporting emergency calling services. DNS servers for the realm will be configured to enable ANPs to dynamically discover the designated IDP's AAA servers.

The devices are pre-configured with a HotSpot2.0/Passpoint profile, which includes the emergency RCOI (E-911-RCOI), and a common identity, e.g., anonymous@sos.fcc-athorized.org. Device eco-systems vendors can pre-configure this profile into every device at the time of manufacturing or push an updated profile using established carrier-bundle based provisioning. This anonymous profile will be common for all devices. This allows the device to discover Wi-Fi access networks that support emergency 911 services. Furthermore, the SIP User Agent in the mobile device will be able to use P/E-CSCF configuration obtained from the Wi-Fi access network.

Wi-Fi access networks that are part of the OpenRoaming federation and willing to support emergency 911 services will configure the emergency RCOI on their WLAN equipment. WLAN OEM suppliers can augment existing OpenRoaming provisioning interfaces with emergency RCOI settings. These networks allow any devices without access credentials to connect to the network for emergency calling. The Wi-Fi access network will recover the realm from the identity and use DNS system to discover the designated IDP's AAA servers.

OpenRoaming already requires access networks to provide their Civic Location and/or Geo-spatial coordinates in the IDP signaling messages. The location information may be manually configured or can be obtained from a reliable source. The device will also be able to discover emergency voice services (CSCF) and the related configuration from the access network or from a cloud entity. This allows device to be able to use the emergency e911 services when connected to access networks that are not part of the OpenRoaming federation. NOTE that this assumes that the device has basic internet connectivity and can initiate emergency calls without requiring emergency calling support from the access network. The device can include location elements, obtained either from the access network or from a cloud function, and include them in the SIP signaling using the Geolocation header fields defined in RFC 6442. The E-CSCF function will retrieve the location elements from the signaling messages from the device.

For supporting the architecture based on this approach, we need the following updates to the WBA OpenRoaming architecture. Cisco has discussed such change request with WBA that includes:

* enhancement to WBA OpenRoaming technical framework to include use of emergency RCOI.

* enhancements to OpenRoaming templated legal terms for access network providers on use of emergency RCOI and associated requirements, e.g., related to use of existing defined RFC 5580 location attributes.

* updates to WBA WRIX offered-service VSA to include new string for "openroaming-emergency" service definition.

* definition of policies required to be enforced by ANP when filter-id attribute mirrors the "openroaming-emergency" tag.

4. Key Service Requirements

Emergency service considerations for supporting this emergency 911 service.

An emergency call handling service shall be designated to handle Wi-Fi-enabled 9-1-1 calls, along with an IDP function for the realm e.g., "sos.fcc-authorized.org", where an existing MNO cannot (non-provisioned device or MNO core is unavailable). This should consider third-party providers such as IDPaaS/MNO/Voice Service Providers to host these services.

Broadband service providers and HotSpot venue operators shall provide the Civic-Location and or the Geo-spatial coordinates of the venue, and the emergency voice service configuration to the device in the IP address configuration procedures.

Consumer devices should be pre-configured by OEMs or through established carrier-bundle based provisioning with a HotSpot2.0/ Passpoint profile, including the emergency RCOI (E-911-RCOI) and a common identity such as "anonymous@sos.fcc-authorized.org.".

5. Access Network Location

Location of the caller is a key element in the emergency-service workflow. Emergency response centers must be able to determine the location of the caller before service is dispatched. A caller may be too young, frightened or confused to provide the location of emergency, therefore automatic location determination by PSAP is an essential requirement.

The device making the emergency call must be able to obtain the Civic and/or Geo-spatial coordinates for inclusion in SIP Registration messages. Reliance on GPS is not an option for most indoor environments.

The WLANs supporting emergency 911 services should be capable of providing the Civic Location or the Geo-Spatial coordinates of the caller, or of the access point. An OpenRoaming access point must be manually configured with the Civic and/or the Geo-Spatial coordinates or able to derive location through other means. For example, an access point operating in 6 GHz Standard Power mode is required to

include its geo-location in the spectrum grant requests sent to the AFC. In some environments, the access point can learn the location information from a connected ethernet switch, or from a broadband service provider network. Furthermore, any access points supporting indoor localization services will be able to meet the location requirement.

It is proposed to re-use the definition of location signaling in OpenRoaming, enabling the access point to provide the Civic address and/or the Geo-spatial coordinates of the device or of the access point to the IDP for CLF population. A confidence-level indicator is also optionally included in the reported location-data, based on RFC 7459 considerations. This parameter is indicative of the uncertainity and the confidence level of the reported location.

6. WLAN Network Identification and Selection

The OpenRoaming federation makes extensive use of Passpoint specified Roaming Consortium Organization Identifiers (RCOIs) for defining polices that are supported by particular access network providers (ANPs) and those policies supported by individual identity providers (IDPs). The supported RCOIs are provisioned in WLAN equipment by the ANPs and configured in the Passpoint profile of devices managed by IDPs. Only when there is a match of RCOIs between WLAN and Passpoint profile will an authentication exchange be triggered. It is proposed to define the use of an emergency-RCOI for use in the systems to support E911 only service.

7. Legal and Regulatory Requirements

The OpenRoaming federation has a foundation in a legal framework, whereby the Wireless Broadband Alliance (WBA) as the federation's policy authority is responsible for defining the framework under which the federation operates. WBA defines the privacy policy that providers are required to comply with as well as end-user terms and conditions. In addition, WBA defines the legal templated terms that are used between OpenRoaming brokers and OpenRoaming providers, defining immutable terms that all OpenRoaming providers need to agree to. Finally, WBA agrees legal terms directly with OpenRoaming brokers, including terms that require OpenRoaming brokers to use the WBA templated terms in their agreements with providers. It is proposed that these legal agreements be amended with terms that cover operation of E911 service and allow provisions to indemnify ANPs against any liabilities resulting from e911 call failures.

8. Authentication on the emergency RCOI WLAN

The requirements include being able to support emergency calls for users without valid credentials to fully authenticate to the WLAN, in this case a credential that has been issued by a specific OpenRoaming IDP designated to support users without a full credential. 3GPP has defined an approach that uses a 3GPP defined vendor specific EAP method called EAP-3GPP-LimitedService for supporting devices without credentials. However, this vendor specific EAP method is not widely supported. Instead, this use-case leverages the well supported EAP-TTLS method with a common set of credentials used by all users wanting to access on the emergency-RCOI WLAN. The EAP-Identity shall be specified as anonymous@sos.fcc-authorized.org with common credentials being used in the inner method.

9. Authentication using the sos.fcc-authorized.org realm

OpenRoaming dynamically discovers the signaling peers used to authenticate end-users using DNS. The same approaches are re-used by ANPs to discover the signaling systems used to support the EAP-server for the sos.fcc-authorized.org realm. The EAP-server will use the common credentials to authenticate users without valid OpenRoaming credentials onto the WLAN. OpenRoaming defines the RADIUS messages exchanged between ANP and IDP. These include the "offered-service" vendor specific attribute as well as RFC 5580 defined location attributes. It is proposed to define a new value for the offered service, e.g., "openroaming-emergency" to unambiguously indicate that the authentication has come from a WLAN configured with the emergency RCOI.

10. Emergency CSCF operation for end-users using sos.fcc-authorized.org credentials

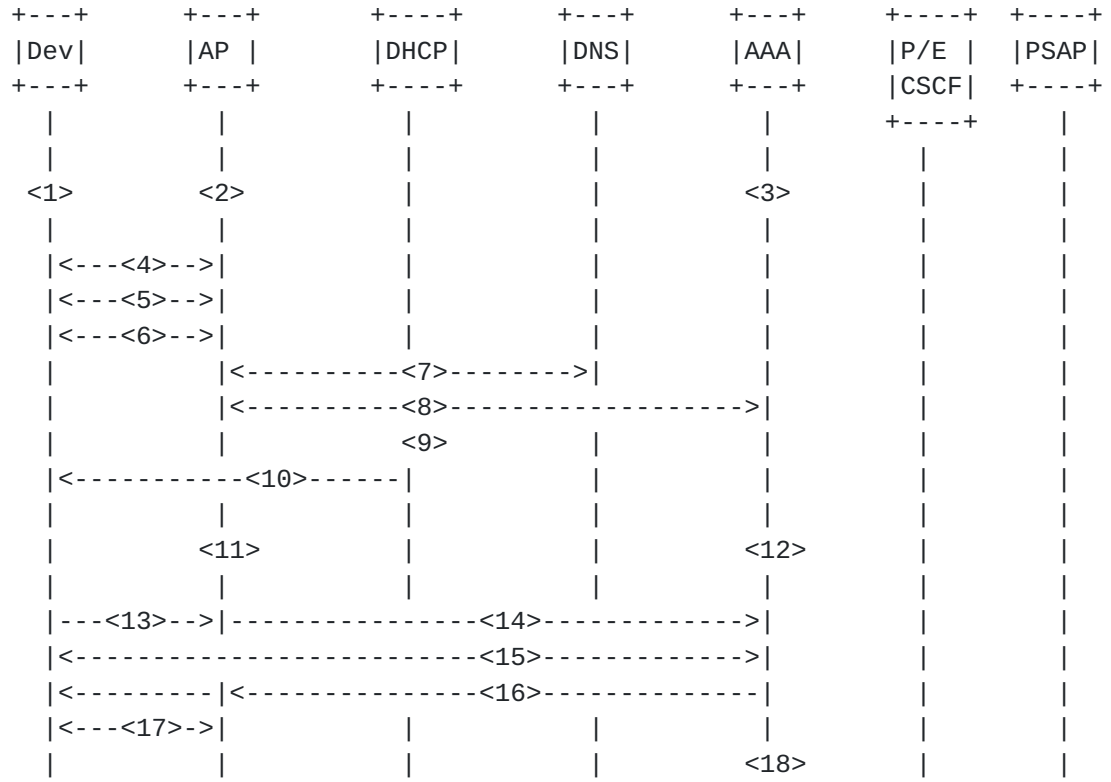
Whereas 3GPP defines the E-CSCF as always operating in the access network, in this use-case the E-CSCF is a common function that can be leveraged by all OpenRoaming ANPs that have configured the emergency-RCOI. This means that the E-CSCF isn't coupled to the access network by which it can recover network provided location information. Instead, in this use-case we leverage the existing OpenRoaming specifications that define the signaling of civic and geo-spatial location in the RADIUS exchange between ANP and IDP. Unlike in cellular networks, users on WLAN systems will frequently be allocated private IP addresses. This IP address information can be included in the RADIUS exchange between ANP and IDP, but because it will frequently represent a private address, it cannot be used to uniquely identify a user. Instead, it is proposed to enhance the Connectivity Location Function (CLF) to allow querying based on Basic Service Set ID (BSSID) which represents the MAC address of the WLAN radio

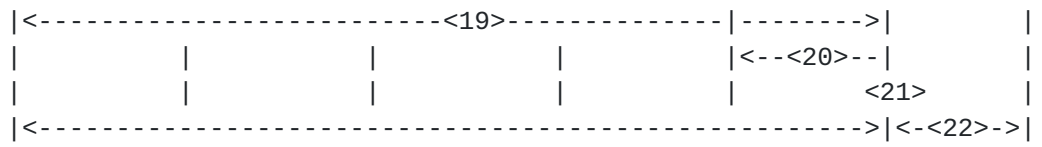
interface that is serving a user, and optionally a Secure Location Tag (SLT) which the WLAN system will deliver it to the device. The BSSID and/or the SLT will be included in the P-ANI SIP header sent by the device as well as being included in the ANP to IDP RADIUS signaling. It's proposed that the definition of the IDP hosting the sos.fcc-authorized.org realm includes support for enhanced CLF capability that enables the IDP to be queried by an E-CSCF based on BSSID and/or SLT. The IDP can then match the BSSID and/or SLT with that received in RADIUS messages originated from individual ANPs and return the corresponding location information to the E-CSCF.

11. Emergency calling by OpenRoaming subscribers on MNOs

End users who have been provisioned with a full OpenRoaming profile will successfully authenticate onto the OpenRoaming ANP using their standard profile and standard OpenRoaming RCOI. As an OpenRoaming IDP, the MNO is able to similarly match the civic-location and/or geospatial location of authentication requests with the BSSID and/or the SLT signaled by the ANP. The MNO operating the CSCF is able to recover the BSSID and/or the SLT from the P-ANI header and determine the location of their own users.

12. Call Flows





1. **Passpoint Profile with Emergency-RCOI, ananonymous@sos.fcc-authorized.org.**
2. **Advertises E-RCOI on that BSSID, Civic & Geo-Location Attributes configured on the AP.**
3. **IDP & Voice Services for Emergency Calling. Possibly managed by FCC or WBA. Manages policies for E-RCOI\nand "sos.fcc.org" identities.**
4. **802.11u with RCOI in Beacon IE**
5. **Attach to SSID matching the E-RCOI**
6. **Authentication Exchange (No credential validation)**
7. **Realm Lookup (sos.fcc.org) / IDP Discovery**
8. **TLS Tunnel Setup, Authentication ID federated issued certs**
9. **Generates location tag (SLT) based\non device indoor positioning, or location configuration of the AP**
10. **Delivery of SLT from AN over ANQP/AssocResp/DHCP/IPv6 ND**
11. **BSSID + SLT (optional) +** Location Attributes sent to IDP in the below RADIUS message exchange
12. **E-CSCF FQDN and Emergency\nCalling numbers sent to AN in the below RADIUS message exchange**
13. **EAP-ID/Resp / 802.1x**
14. **EAP over RADUIUS (TLS)**
15. **EAP-TTLS with well-known credentials**
16. **EAP-Success**
17. **Delivers IMS Configuration over 802.11, DHCP, or IPv6 ND**
18. **Updates the local CLF to include BSSID and/or SLT to Location Mapping**
19. **SIP UA Registration includes BSSID and SLT (optional) in the P-ANI Header**
20. **CLF Query for Location Check using BSSID and/or SLT**
21. **Determination of PSAP based on query to RDF**
22. **Emergency Call Routed to PSAP with location**

Figure 2: Emergency e911 Services over Wi-Fi Access

Following is some additional text explaining above interactions.

* The device is pre-configured with the emergency passpoint profile, which includes the emergency RCOI, and a common identity, "anonymous@sos.fcc.org". This allows the device to discover access networks that support emergency 911 services.

* An 802.11 access network supporting EAP-based authentication method and is part of the OpenRoaming federation is either configured with the Civic-Location and/or the Geo Spatial coordinates of the access point or has the ability to derive location coordinates through other means.

* The access network for supporting emergency 911 services will advertise the emergency RCOI in the 802.11 Beacon messages, and furthermore will respond to any ANQP queries on the supported services.

* A device that is in coverage of a WLAN but without any valid conventional access-network credentials may use the UI interaction to trigger the selection of the profile containing the emergency RCOI. The end user's selection of an emergency calling application, or interaction with the default phone application (e.g., by selecting the emergency call option in the UI or by dialing an emergency phone number) may trigger the selection of the Passport profile with the emergency RCOI, resulting in the device performing a network-attach for emergency-call access.

* The device will use the default identity, "anonymous@sos.fcc.org" from passpoint profile in the initial authentication message exchange, allowing the access network to discover the AAA server / IDP for EAP authentication.

* The access network using the realm portion of the identity, "sos.fcc.org." will perform a DNS lookup the AAA server for the IDP supporting the emergency RCOI and the realm.

* The access network and the AAA server will establish a secure TLS tunnel for securing the 802.1x/EAP traffic between the device and the IDP. The authentication of the peers will be based on the OpenRoaming federation issued X.509 certificates.

* The device will complete the EAP authentication using the common credentials from the emergency passpoint profile. The 802.1x/EAP messages are tunneled as RADIUS messages between the access point and the AAA server.

* The access point will generate secure location tag (SLT) for the device. The SLT will be delivered to the device over one of the protocols (ANQP/802.11/DHCP/IPv6 ND). SLT is a tag representative

of the device' location. In another variation, SLT can be a composite object composed of a signed location by the access network or a cloud function, along with the identifiers of the signing entity. Functions such as E-CSCF will be able to verify the location by verifying the signature of the signing entity.

* The access point includes the BSSID of the access point in the Calling-Station-Id attribute (RFC 2865) and/or the SLT in a new attribute to be defined.

* The access point will also include the attributes for carrying the Civic Location and/or the Geo-Spatial coordinates of the access point (RFC 5580).

* The AAA server will send the IMS configuration (E-CSCF FQDN) supporting emergency call routing services to the access point.

* A success EAP transaction between the device and the AAA server will result in the AAA server sending EAP-SUCCESS to the device.

* The AAA server will update the local CLF function with the location of the access point, using BSSID and/or the SLT as location identifiers.

* The access point delivers the IMS configuration to the client over one of the interfaces (802.11/ANQP/DHCP/IPv6 ND). ANP will apply policies which limits the usage of the network over emergency RCOI only for emergency calling. Furthermore, the ANP will apply QoS policies on the emergency session for ensuring the call meets the SLA defined for the emergency service. ANP will prioritize traffic and sessions on emergency RCOI over other RCOIs.

* The IMS client in the device performs registration with the emergency IMS system. The UA inserts the P-Access-Network-Info header field in the SIP message using the 3GPP 24.229 defined fields. It contains the BSSID of the access point (access-type="IEEE-802.11", wlan-node-id="BSSID", and optionally a secure-location-tag=SLT). A new parameter, "secure-location-tag" will be defined.

* The E-CSCF function uses the BSSID and/or the SLT from the P-ANI header for determination of the device's location. It queries the CLF for retrieving the Civic and/or the Geo-spatial coordinates of the access point. The E-CSCF function may query the RDF function for the PSAP destination address.

* The E-CSCF will route the emergency call to the nearest PSAP.

13. IANA Considerations

This document does not requires any IANA actions.

14. Security Considerations

network access identifier [RFC7542]

A rogue user or a compromised device may potentially trigger a volume of emergency calls, including calls spoofing the caller's real location. The value set for the field, "i-wlan-node-id" in the PANI header can potentially be a false BSSID which maps to a different location in the CLF database.

In this use-case, we eliminate this threat with the use of SLT (Secure Location Tag) that the network will generate dynamically and will provide it to the device for inclusion in emergency call signaling.

A trusted OpenRoaming access network signals the same location tag along with the civic and/or geo-spatial coordinates to the IDP. The CSCF function will retrieve the SLT from the call signaling from the device and will look up the civic location and/or geo-spatial coordinates of the device by querying the CLF database populated by the IDP. SLT serves as an index to the real-location and the generated tag is valid for a short duration, thereby eliminating any replay attacks.

A rogue user or a compromised device may also initiate a volume of emergency calls, including a valid caller's location. This threat is not a new threat and exists even in today's emergency services supported over wireline and cellular architectures.

15. Acknowledgements

We had many discussions with the members of FCC CSRIC 8 WG and that feedback greatly us greatly in developing this proposal.

16. References

16.1. Normative References

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

[RFC7542] DeKok, A., "The Network Access Identifier", RFC 7542, DOI 10.17487/RFC7542, May 2015, <https://www.rfc-editor.org/info/rfc7542>.

16.2. Informative References

[TS23501] 23.501, 3. T., "Numbering, addressing and identification", 2021.

Authors' Addresses

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
United States of America
Email: sgundave@cisco.com

Mark Grayson
Cisco
11 New Square Park
Bedfont Lakes
United Kingdom
Email: mgrayson@cisco.com