
March 2023

# COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VIII

# REPORT ON 911 SERVICE OVER WI-FI

DRAFTED BY
WORKING GROUP 4: 911 SERVICE OVER WI-FI

# TABLE OF CONTENTS

Table of Tables and Figures

# 1 Executive Summary

The use of Wi-Fi access to support 911 calling has been a topic of interest in the Federal Communication Commission (FCC or Commission) for several years. On March 23, 2021, the Public Safety and Homeland Security Bureau of the FCC prepared and submitted to Congress a report entitled *Study on Emergency 911 Access to Wi-Fi Access Points and Spectrum for Unlicensed Devices When Mobile Service Is Unavailable* (the "Report to Congress"). The Report to Congress was submitted pursuant to Section 301 of the Repack Airwaves Yielding Better Access for Users of Modern Services (RAY BAUM'S) Act of 2018 (Section 301). Section 4.1.2 of this Report provides a summary of the findings and recommendations of the Commission in their report to Congress. It is important to note the report recognized that "*[b]ased on the information available at this time, we cannot reasonably estimate the costs or benefits of making Wi-Fi access points and spectrum for unlicensed devices available for 911 services when mobile service is unavailable."*

Communications Security, Reliability, and Interoperability Council (CSRIC) VIII recognizes that several years have passed since the publication of the Report to Congress, and the current state of 911 calling utilizing Wi-Fi connections has advanced. This new Report presents up to date information to clarify the current state of 911 Service over Wi-Fi, and recommendations for future advancements.

The FCC specifically directed CSRIC VIII to explore the public safety benefits, technical feasibility, and cost of options for making Wi-Fi access points and/or unlicensed spectrum available to the public to facilitate access to 911 services. The ubiquitous nature of Wi-Fi access suggests that, in the long term, various Wi-Fi solutions could be added to the "toolbox" of 911 connectivity options available to consumers, Public Safety Answering Points (PSAPs)/Emergency Communications Centers (ECCs), and communications providers, and could complement the broader transition to an IP-based Next Generation 911 environment.

CSRIC VIII brought industry stakeholders together to examine a range of technical issues with the goal of promoting consensus in the Wi-Fi ecosystem to support reliable 911 services (voice and text) under normal conditions and when catastrophic events disrupt mobile service. The primary focus was to examine and report on:

- security issues including authentication and access control protocols;
- solutions to automatically activate Wi-Fi Calling on eligible mobile devices when necessary to automatically determine the 911 caller location and address call routing issues;
- 911 call prioritization;
- identification of missing standards; and
- timelines and costs for implementing 911 over Wi-Fi solutions.

The scope of the CSRIC VIII Report addresses the current and future state of 911 and Wi-Fi calling, with consideration given to:

- Device characteristics;
- Wi-Fi access point (AP) characteristics;
- Originating Service Provider (OSP) Interconnecting Network Characteristics;
- Emergency Call Detail Characteristics;
- Caller Location and Call Routing;
- Short Message Service (SMS) and Multimedia Messaging Service (MMS) Text to 911;
- Real Time Text (RTT); and
- Integration into both Legacy and Next Generation 911 Architectures.

Other critical communication modes or features such as placing calls from airplanes, automatic activation of a device for Wi-Fi calling, and future considerations for emergency priority service status during disasters are also included in the Report.

Fundamental to this Report is the identification of use cases which establish the framework for evaluating and documenting the current state and future opportunities associated with Wi-Fi 911 calling. These use cases are analyzed in the context of their ability to support important features of 911 calling, as well as cost considerations associated with critical elements such as cyber security, compatibility of networks, software changes, network elements, operational integration, industry standards, and public education. As a starting point, industry experts reviewed, and came to a consensus in documenting the existing frameworks for 911 access in Wi-Fi environments today. Where scenarios did not support the ability for an end user to reach emergency services, areas for potential enhancement are identified.

PSAPs/ECCs play critical roles in responding to emergency calls. Public Safety's communications criteria important to PSAPs'/ECCs' role in processing and responding to Wi-Fi-based 911 calling was a foundational consideration during the analysis of the Use Cases and is addressed in the Report in Section 3.3.4. Such criteria included:

- Routing the Call to an Appropriate PSAP/ECC;
- Maintaining Connectivity with the Caller;
- Delivery of the Caller's Current Location;
- Call Back Capabilities;
- Authentication of Caller; and
- Identifying that a 911 Call Originated Over Wi-Fi

The above criteria allows for a structured process whereby existing networks were examined and potential opportunities for enhancements are identified as summarized below.

Use Cases #1 - #5 [Section 5.1.2] describe existing functionality that will result in successful 911 calls from a wireless device. Of the first five use cases, only Use Case #5 describes a scenario where the emergency call originates as a Wi-Fi call (because the cellular Radio Access Network (RAN) is not available). These Use Cases are feasible presently and do not have outstanding issues with the initiation and successful completion of emergency calls.

Use Cases #6 - #10 described below are scenarios where the end user may not reach emergency services due to a failure in routing or other issues, such as the inability to connect to a Wi-Fi Access Point (AP).

| | Title | Call Outcome |
|---|---|---|
| Use Case #1 | 911 call over Cellular Network – Home network | Successful |
| Use Case #2 | 911 call over Cellular Network – Domestic and International Roaming (full service) | Successful |
| Use Case #3 | 911 call over Cellular Network – Domestic and International Roaming (limited-service)[1]. | Successful |
| Use Case #4 | 911 call over Cellular Network – NSI Device | Successful |
| Use Case #5 | 911 call over Wi-Fi without cellular coverage | Successful |

[1] A device in a "limited-service" state will be able to make emergency calls but will not be able to make or receive non-emergency calls.

| | Title | Call Outcome |
|---|---|---|
| Use Case #6 | Emergency Access to Nearby Wi-Fi AP | Currently Unsuccessful – Opportunity for improvement |
| Use Case #7 | Automatic Activation of Wi-Fi Calling | Currently Unsuccessful – Opportunity for improvement |
| Use Case #8 | 911 over Wi-Fi from a device with an International subscription | Often Unsuccessful – Opportunity for improvement |
| Use Case #9 | Emergency Access to nearby Wi-Fi AP when cellular RAN, Core and IMS are not available | Currently not supported |
| Use Case #10 | Emergency Access to nearby Wi-Fi AP when cellular RAN, Core and/or IMS are not available using a framework allowing the use of a default Emergency Passpoint profile | Currently not supported |

The detailed technical status of each use case is described in the Report in the various subsections under Section 5.1 and includes critical technical information on background, architecture discussion, assumptions, considerations, ownership, threat analysis, and in some cases regulatory considerations.

Throughout the technical review and development of the Use Cases, CSRIC VIII developed the following recommendations.

**CSRIC Recommendations Intended for the Commission:**

- CSRIC VIII expended significant time attempting to identify the current state of 911 over Wi-Fi capabilities. Maintaining accurate information about the current capabilities will be important for all stakeholders. Thus, the Commission should gather and maintain accurate information about device and network settings related to 911 over Wi-Fi and ensure this information is available to consumers. This information might include a description of the conditions in which a 911 call over Wi-Fi will be supported, addressing the comprehensive set of capabilities and conditions explored in this Report: activation of Wi-Fi calling; authentication; service continuity; prioritization and routing; accuracy of caller location information; etc.
- The Commission should evaluate the applicability of rules for various 911 over Wi-Fi use cases. To encourage the development of technologies and standards identified in this Report, the Commission could consider the need to clarify that entities will not incur new obligations as a function of developing technologies and standards that enable 911 service over Wi-Fi. The Commission could also consider the need for clarification of which entities have obligations to provide 911 service and other obligations such as geolocation and accuracy requirements, when appropriate technologies and standards have been developed and matured.
- The FCC should consult with the Federal Aviation Administration, airlines, Commercial Mobile Radio Service (CMRS) providers, and other stakeholders to consider the need for rules or standards to govern if/when calls/texts to 911 via airplane Wi-Fi should be permitted.
- The FCC should direct a future CSRIC working group to assess the ability for 911 service over Wi-Fi and EPCS NS/EP priority access to coexist and determine if it is necessary to provide more specific recommendations prior to ubiquitous deployment of EPCS.

- CSRIC encourages the FCC to consider opening a proceeding on automatic (phone) device support for Wi-Fi calling for emergency calls when it has not been enabled on the device and cellular service is not available, considering all challenges with respect to routing, caller location, and callback. The length of time that Wi-Fi calling should remain active should be analyzed and recommended as an industry standard.
- If an MNO is not available to allow access to emergency services, the FCC should investigate methods to access emergency services to be designated to handle Wi-Fi-enabled 911 calls, along with an Identity Provider (IDP) function for a new interconnecting network realm dedicated to connecting emergency services from the Internet to emergency services networks.
  Note: To support this new service, consumer devices would need to be configured by OEMs or through established provisioning with a new Passpoint profile, including the emergency Roaming Consortium Organization Identifier (RCOI) (911 RCOI) and a common identity.
- The FCC should consider repealing the requirement to collect Registered Location information for non-fixed interconnected VoIP services at service initialization given the advancements in location determination, and to allow for the automatic enabling of Wi-Fi calling.
- The FCC should consider the need for clarifying the rules to ensure the use of location-based routing and delivery of the best-available location information for 911 calls over Wi-Fi.
- To address roaming issues the FCC should:
  - Determine the current state of VoLTE and VoNR interoperability for emergency calling purposes for devices that are operated in the United States, where feasible;
  - Explore methods to improve access to domestic emergency services for foreign visitors;
  - Determine the feasibility of Wi-Fi calling origination, particularly and specifically in the case of an international visitor's device originating a call over a Wi-Fi connection; and
  - Collaborate with international bodies to harmonize any such rules as described above.

**CSRIC Recommendations Intended for other than the FCC:**

- It is recommended that service providers, Public Safety professionals, and other 911 stakeholders participate in the development of standards-based location spoofing mitigation solutions that will support PSAPs/ECCs in assessing, in real-time, the legitimacy of location information associated with 911 calls, including 911 calls originated over Wi-Fi.
- It is recommended that service providers, Public Safety professionals, and other 911 stakeholders participate in the development of a standards-based solution that will convey a Class of Service (COS) or other designation for 911 calls that originate over Wi-Fi to PSAPs/ECCs.
- Concerning Service Continuity:
  Given the public safety benefits of maintaining a 911 call when a caller moves outside of the serving area of the cell or Wi-Fi access point to which the call is initially connected, CSRIC VIII recommends the following:
  - Industry bodies and individual companies should continue developing and implementing methods for seamless mobility between APs and between APs and cellular networks.
  - Further consideration, including the need for industry standards, should be given by device manufacturers (OEMs) regarding policies and methods for turning on device Wi-Fi and turning off Airplane Mode when a 911 call is made.
- The working group encourages appropriate standards bodies to conduct continued performance modeling and studies to ensure that any future 911 service identification over Wi-Fi and forthcoming EPCS NS/EP priority access can coexist with minimal effect on either service.
- Industry bodies should establish standards and best practices for location-based routing and the provision of location information to complement the current regulatory framework including

those for non-fixed VoIP services.

- If emergency Passpoint profile access to APs (enterprise, residential, public access point) is supported, then AP vendors should support an opt-in capability for such emergency access to the AP, provided that appropriate assurance is made that access is limited to emergency calling.

In conclusion, CSRIC VIII produced a Report that explores the opportunity to leverage the ubiquitous nature of Wi-Fi access points to support 911 connectivity options available to consumers. This Report represents the most comprehensive public documentation to date of the existing capabilities and limitations of 911 service over Wi-Fi, and it analyzes the public safety benefits, technical feasibility, and potential costs associated with improving access to 911 with Wi-Fi access points. CSRIC VIII looks forward to the Commission and other entities acting upon the recommendations detailed in this Report to expand 911 service over Wi-Fi with appropriate consideration of security challenges, technical feasibility, and public safety needs.

It is important to note that the analysis of technological solutions and recommendations were guided by the goal to achieve as much as possible given the current technology, state-of-practice, and potential benefits to public safety. The dedication of many subject matter experts contributed to this report and feel strongly it can serve as a guide for educating Congress, the industry and public safety on the technical opportunities and hurdles involved in advancing 911 Over Wi-Fi in normal and disaster situations.

# 2 Introduction

Access to 911 and emergency services saves lives and property, and safeguards the public. The ability to use Wi-Fi solutions for voice and data communications with emergency communications centers has the potential to expand access to these services and thereby improve public safety overall. When cellular networks are unavailable, such as when out of normal network coverage or during significant disasters in which network infrastructure is damaged or without power, alternative connectivity options (i.e., Wi-Fi) can enable 911 access. The prevalence of Wi-Fi access points in many areas (e.g., offices, homes, enterprises, and venues) suggests that, in the long term, various Wi-Fi solutions could be added to the "toolbox" of 911 connectivity options available to consumers, emergency communications centers, and communications providers, and could complement the broader transition to an IP-based Next Generation 911 environment.

The FCC has previously analyzed the benefits to public safety of certain enhancements to 911 service.[2] Due to a lack of available data, CSRIC VIII was unable to provide a rigorous analysis of the full range of public safety benefits associated with expanding access to 911 over Wi-Fi. For example, it is difficult to define the conditions of a "typical" cellular network outage, or how many additional 911 calls could be completed if various methods of expanding 911 access over Wi-Fi were to be deployed. In general, the group determined that the public safety benefits will be commensurate with the extent and nature of expanded access. Additionally, the group identified key public safety criteria for prioritizing technical enhancements and articulating public safety benefits. As described in Section 3.3.4, these criteria include factors such as the ability to determine the caller's current location, maintain a 911 call, and authenticate the caller's identity, among other factors.

[2] For example, the FCC's 2015 Report and Order on E9-1-1 location accuracy estimated the benefits of improving wireless 9-1-1 location accuracy in terms of the number of lives saved and improvements in patient outcomes due to reduced emergency response times.

In some cases, taking key public safety criteria into account is relevant to mitigating potential risks of expanding 911 access over Wi-Fi. For example, the ability to accurately locate callers, assess the legitimacy of caller identity information delivered with a 911 call, and identify for PSAPs/ECCs that the call is being delivered via voice over Wi-Fi are important tools for dealing with challenges like "swatting." Swatting is a nefarious practice often associated with 911 calls made via voice over IP connections in which a fake call to 911 is placed to trigger a police SWAT team response with a false report of an emergency. Because Voice over Internet Protocol (VoIP) calls make it easier to spoof a caller's identity and location, expanding access to 911 over Wi-Fi poses a risk of increased swatting incidents and other bad actor activities. It is therefore critical to consider public safety impacts that go along with enhancing the public's ability to access 911 over Wi-Fi.

## 2.1 CSRIC Structure

CSRIC VIII was established at the direction of the Chairperson of the FCC in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The purpose of CSRIC VIII is to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of communications systems. CSRIC VIII's recommendations will focus on a range of public safety and homeland security-related communications matters. The FCC created informal subcommittees under CSRIC VIII, known as working groups, to address specific tasks. These working groups must report their activities and recommendations to the Council as a whole, and the Council may only report these recommendations, as modified or ratified, as a whole, to the Chairperson of the FCC.

| Communications Security, Reliability, and Interoperability Council (CSRIC) VIII | | | | | |
|---|---|---|---|---|---|
| CSRIC VIII Working Groups | | | | | |
| Working Group 1: 5G Signaling Protocols Security | Working Group 2: Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment | Working Group 3: Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks | Working Group 4: 911 Service Over Wi-Fi | Working Group 5: Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure | Working Group 6: Leveraging Mobile Device Applications and Firmware to Enhance Wireless Emergency Alerts |
| Co-chairs:<br>Brian Daly, AT&T &<br>Travis Russell, Oracle | Co-chairs:<br>Mike Barnes, Mavenir<br>& George Woodward,<br>RWA | Co-chairs:<br>Micaela Giuhat,<br>Microsoft & John<br>Roese, Dell | Co-chairs:<br>Mary Boyd,<br>Intrado & Mark<br>Reddish, APCO | Co-chairs:<br>Padma Sudarsan,<br>VMWare & Todd<br>Gibson, T-Mobile | Co-chairs:<br>Farrokh Khatibi,<br>Qualcomm &<br>Francisco Sanchez,<br>Small Business |
| FCC Liaison:<br>Ahmed Lahjouji | FCC Liaison:<br>Zenji Nakazawa | FCC Liaison:<br>Jeff Goldthorp | FCC Liaison:<br>Rasoul Safavian | FCC Liaison:<br>Saswat Misra | FCC Liaison:<br>Tara Shostek |

**Table 1 – Working Group Structure**

## 2.2 Working Group 4 Team Members

| Name | Company |
|---|---|
| Brandon Abley | National Emergency Number Association |
| Charles "Peter" Musgrove | AT&T, Inc. |
| Charlie Sasser | National Association of State Technology Directors |
| Chinmay Dhodapkar | Google |
| Craig Hodan | National Weather Service |
| Everett Kaneshige | National Association of Telecommunications Officers & Advisors |
| Fred Frantz | ANDRO Computational Solutions |
| Harold Feld | Public Knowledge |
| James Goerke | Texas 911 Alliance |

| Name | Company |
|---|---|
| Jason Lish | Lumen Technologies |
| Jeanna Green | T-Mobile |
| Jeff Torres | Verizon |
| Jeffrey Wittek | Motorola Solutions |
| Katherine Elkins | National Highway Traffic Safety Administration, 911 Program Office |
| Kevin Green | Somos, Inc. |
| Kirk Burroughs | Apple |
| Malcolm Smith | Cisco Systems, Inc. |
| Mark Annas | City of Riverside Fire Dept., Office of Emergency Mgt |
| Mark Gibson | CommScope |
| Mark Grubb | Cybersecurity & Infrastructure Security Agency, U.S. Dept of Homeland Security |
| Mark Hess | Comcast Corporation |
| Mark Reddish | Association of Public Safety Communications Officials |
| Mary Boyd | Intrado Life & Safety |
| Michael Bergman | Consumer Technology Association |
| Rob Alderfer | Charter Communications |
| Robert Kubik | Samsung Electronics America |
| Sean Scott | SecuLore Solutions |
| Stephen Edge | Qualcomm Technologies, Inc. |
| Steve Watkins | Cox Communications |
| Stuart Strickland | Hewlett Packard Enterprise |
| Susan Miller | Alliance For Telecommunications Industry Solutions |
| Theresa Reese | Ericsson |
| Tim Schram | National Association of Regulatory Utility Commissions |
| Travis Reutter | ACA Connects America's Communications Association |
| Wade Buckner | International Association of Fire Chiefs |
| William "Andy" Leneweaver | Washington State Military Dept |
| William Mikucki | Comtech Telecommunications Corp. |

**Table 2 – List of Working Group Members**

Alternates for members are listed below.

| Name | Company |
|---|---|
| Alison Venable | Association of Public Safety Communications Officials |
| Brian Hurley | ACA Connects |
| Brian Tegtmeyer | National Highway Traffic Safety Administration, U.S. Dept of Transportation, 911 Program |
| Carol Ansley | Cox Communications |
| Chris Anderson | Lumen Technologies, Inc. |
| Christian Militeau | Alliance for Telecommunications Industry Solutions |
| Darrin Morkunas | Intrado Life & Safety |
| J. David Grossman | Consumer Technology Association |
| James Ramsey | National Association of Regulatory Utility Commissioners |
| Justen Davis | Somos, Inc. |
| Matthew Chappell | Cox Communications |
| Megan Stapleton | Comtech Telecommunications Corp. |
| Michael Hooker | T-Mobile |
| Nicholas Garcia | Public Knowledge |
| Peter Thornycroft | Hewlett Packard Enterprise |
| Praveen Srivastave | Charter Communications |
| Scott Blue | Cisco Systems, Inc. |
| Tom Breen | SecuLore Solutions, LLC |

**Table 3 – List of Working Group Alternates**

## 2.3 External Subject Matter Expert Contributors

| Name | Company |
|---|---|
| Mark Grayson | Cisco |
| Pat Welsh | Intelsat |
| Peter Davidson | Intelsat |
| Sri Gundavelli | Cisco |

**Table 4 – List of External Subject Matter Experts**

# 3 Objective, Scope, and Methodology

## 3.1 Objective

The objective of this Report is to present the findings of CSRIC VIII related to 911 Service Over Wi-Fi. Working Group 4 was tasked with exploring the public safety benefits, technical feasibility, and cost of options for making Wi-Fi access points and/or unlicensed spectrum more available to the public to facilitate access to 911 services. The ubiquitous nature of Wi-Fi access points suggests that, in the long term, various Wi-Fi solutions could be added to the "toolbox" of 911 connectivity options available to consumers, Public Safety Answering Points (PSAPs) or Emergency Communications Centers (ECCs), and communications providers, and could complement the broader transition to an IP-based Next Generation 911 environment.

CSRIC VIII WG 4 brought stakeholders together to examine a range of technical issues with the goal of promoting consensus in the Wi-Fi ecosystem to support reliable 911 services (voice and text) under normal conditions and when catastrophic events disrupt mobile service. To support the objective of this Report, the WG examined: security issues, including authentication and access control protocols;

solutions to automatically activate Wi-Fi Calling on eligible mobile devices when necessary; 911 call[3] location and call routing issues; 911 call prioritization; missing standards; and timelines and costs for implementing new 911 over Wi-Fi solutions.

Section 301 of the "RAY BAUM'S" Act of 2018 Directed the Commission to conduct a "network resiliency" study on the technical feasibility, cost and value of expanding public 911 access to emergency response services via Wi-Fi access points, both telecommunications service provider-owned, and non-provider owned.[4] Intuitively, such access would potentially expand the opportunity for the public to "place" a 911 request for emergency services, and thus make the 911 network environment more resilient. In that Report to Congress, the Commission noted that "[b]ased on the information available at this time, we cannot reasonably estimate the costs or benefits of making Wi-Fi access points and spectrum for unlicensed devices available for 911 services when mobile service is unavailable."[5] They acknowledged the "technical and policy challenges" in providing such access, and concluded ". . . as better cost/benefit data becomes available, it will be important to weigh the relative costs and benefits of the specific alternatives discussed in this report against other possible approaches."[6] In March of 2021, the Commission submitted that Report to Congress.

CSRIC VIII acknowledges that there are hurdles to enhancing access to 911 services over Wi-Fi. The analysis documented in this Report starts by considering what can be achieved in the context of 911 calling over Wi-Fi given current technology, state-of-practice, and the potential benefits to public safety. The Report then analyzes the feasibility of enhancing existing solutions to facilitate 911 access over Wi-Fi.

## 3.2 Scope

The scope of this Report examines the current state of 911 and Wi-Fi calling, device characteristics, Wi-Fi access point (AP) characteristics, emergency call details, and location determination options. Public safety criteria for 911 calling, including emergency Wi-Fi calls are addressed, and those criteria are used to analyze the Use Cases presented within this Report.

As part of the scope, CSRIC VIII has included the current state of 911 over Wi-Fi, as it became apparent that current state was not readily known, even among the subject matter experts convened for our membership. The group engaged in detailed discussions to reach consensus on current capabilities so that this Report could serve as an educational resource for stakeholders to understand the current state of 911 and Wi-Fi calling and to appropriately identify areas for potential enhancement. Thus, various technical call flows and Use Cases are also described and analyzed to determine what functionality is working today and what Use Cases need to be addressed / added to ensure emergency calls can be delivered during normal conditions as well as during catastrophic events that may disrupt mobile service.

Based on direction from the Commission, WG4's focus was placed on the analysis and reporting of:

- security issues, including Wi-Fi authentication and access control protocols;

[3] The term "call" is used in this Report to include any form of multi-media content (voice, text, pictures/video), unless otherwise specifically stated.

[4] Repack Airwaves Yielding Better Access for Users of Modern Services (RAY BAUM'S) Act of 2018, Pub. L. 115-141, § 301, 132 Stat. 1080, 1086-87 (2018).

[5] Report to Congress, Study on Emergency 911 Access to Wi-Fi Access Points and Spectrum for Unlicensed Devices When Mobile Service is Unavailable, FCC Public Safety and Homeland Security Bureau, March 23, 2021, p.19. See: https://www.fcc.gov/document/report-congress-911-over-wi-fi

[6] ibid

- solutions to automatically activate 911 Wi-Fi Calling on eligible mobile devices with active subscriptions, when necessary;
- automatic determination of the 911 caller location and discussion of call routing issues;
- 911 call prioritization;
- missing standards; and
- timelines and costs for implementing 911 over Wi-Fi solutions.
- Other Considerations include:
    - Limiting access to *only* 911 service;
    - Turning Wi-Fi Calling *off* after 911 use;
    - Wi-Fi mobility;
    - Dedicated Passpoint Profile for Emergency services;
    - Callback issues; and
    - Power and backhaul issues in cases of natural disasters.

## 3.3 Methodology

CSRIC-VIII followed the methodology described below to efficiently consider the topic at hand.

### 3.3.1 Identify Relevant Use Cases

CSRIC-VIII selected Use Cases that illustrated the issues of concern related to the use of Wi-Fi calling for emergency communications. Some of the Use Cases represent existing functionality that will result in successful 911 calls for users. Others describe scenarios where the end user may not reach emergency services due to a failure in call routing or other issues, and examine possible improvements.

### 3.3.2 Analyze Use Cases for Possible Solutions Including Feasibility (cost, public safety benefit)

The selected Use Cases were then analyzed in the context of their ability to support important features of 911 calling and associated costs. Issues related to technical feasibility, cost and public safety benefits of the selected Use Cases were documented.

### 3.3.3 Identify any outstanding issues preventing Use Cases from becoming feasible

Based on analysis of the selected Use Cases, the outstanding issues preventing desired performance (the successful completion of emergency communications) were identified and potential enhancements were considered.

### 3.3.4 Public Safety Perspective

If Wi-Fi is used to expand the opportunity for a 911 request to be successfully delivered to a PSAP/ECC, then like any other type of 911 call, that delivery needs to provide or support call features essential to emergency response. For example, if the location of the calling party is known, it can be used to route the call to a call center that is responsible for dispatching emergency services to that location. Below is a list of those features or criteria that are important to 911 and used to evaluate the public safety benefits of Wi-Fi 911 call delivery in the context of the various Use Cases examined in this Report. While all of these criteria are important call features that provide potential benefits to public safety, not all are required for the use of Wi-Fi in a particular Use Case.

1. **Connect the 911 call to the appropriate PSAP/ECC**

   This criterion reflects the importance of routing and delivering 911 calls to a PSAP/ECC that is appropriate for the location from which the call was originated. In a 911 environment, 911 calls are routed using a 10-digit key that is representative of the location associated with the caller's device. In an end state NG911 environment, 911 calls are routed based on civic and/or geodetic location, as well as PSAP/ECC policy considerations. Other routing methodologies may exist during the transition to NG911.

2. **Maintain the 911 Call**

   This criterion reflects the importance of maintaining a 911 call when a caller moves outside of the serving area of the cell or Wi-Fi Access Point (AP) to which the call is initially connected. 911 calls established over cellular coverage can be reliably maintained when a caller is mobile. When cellular coverage is unavailable, and the 911 call is established over Wi-Fi, some mobility scenarios are still possible if the caller's device moves away from the Wi-Fi AP that originally served the call. Handovers of 911 calls between Wi-Fi APs within the same Wi-Fi network may be supported. Wi-Fi to cellular and cellular to Wi-Fi handovers are also possible with certain network architectures. While technically feasible, handover from cellular to Wi-Fi is typically not implemented.

3. **Provide the current caller location data**

   Location information is critical to the routing of 911 calls and the dispatch of emergency personnel. Caller location may be in geodetic format (i.e., consisting of x, y, z coordinates with confidence and uncertainty), and/or it may take the form of a civic address (e.g., a dispatchable location provided by the device or a verified registered address). This criterion addresses the ability for a PSAP/ECC to receive current and accurate caller location with a 911 call and to obtain updated caller location when appropriate. See Section 4.5 for further discussion regarding emergency location determination.

4. **Support Callback Capability**

   There may be circumstances where a PSAP/ECC call taker needs to call back an emergency caller (e.g., if the call terminates prematurely, before the call taker can obtain sufficient information about the caller or incident). PSAP/ECC callback is supported if the caller's device has an active registration for regular voice service and a valid callback number has been provided to the PSAP/ECC at the time of the 911 call.

5. **Authentication of Caller Identity Associated with 911 Calls**

   This criterion focuses on the benefits to Public Safety of being able to assess the legitimacy of caller identity information delivered with a 911 call. In an end-state NG911 environment, when caller identity associated with a 911 call is authenticated by an originating network and verified by an Emergency Services IP Network (ESInet) using the Signature-based Handling of Asserted information using toKENs (SHAKEN) mechanism defined in ATIS-1000074[7], attestation level and verification status information can be delivered to the PSAP/ECC with the 911 call. In a legacy 911 or transitional NG911 environment, other ALI-based mechanisms may be used to convey this information to a legacy PSAP/ECC. See ATIS-05000046[8] for further details.

6. **Provide a Wi-Fi calling Designation**

   This criterion focuses on the ability for a PSAP/ECC to identify that an incoming 911 call originated as a Wi-Fi call. The ability to identify a Wi-Fi call may impact how

[7] ATIS-1000074, *Signature-based handling of Asserted information using toKENs (SHAKEN).*

[8] ATIS-0500046, *Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services*.

telecommunicators and other downstream systems (e.g., Geographic Information System [GIS] mapping functions, Computer Aided Dispatch [CAD] systems, dispatch), and emergency response interpret and use other information (e.g., location) associated with the 911 call. While none of the existing legacy Class of Service values uniquely identifies a Wi-Fi emergency call, guidance is provided in NENA-INF-018.1-2017[9] and NENA-STA-015.10-2018[10] regarding the use of the Customer Name/Service field within the Automatic Location Identification (ALI) data delivered to a PSAP/ECC to identify Wi-Fi emergency calls. NG911 supports enhanced call and location type designations using a composite of additional call data and location method tokens (which describe the location determination method used), but updates are needed to convey a specific Wi-Fi calling service designation.

### 3.3.5 Elements for Cost Considerations

Below are suggestions regarding the elements that need to be considered during any/all Use Case development to evaluate cost implications. Use Cases recommending changes to 911 over Wi-Fi capabilities need to consider the following: cyber security; compatibility (backwards / future); education (both for the public and public safety professionals); and operational integration. Further, the process for operational integration can be separated into the processes for standards development and changes in software and hardware.

#### 3.3.5.1 Standards

To ensure interoperability between telecommunications networks (and a uniform experience for consumers), most if not all aspects of 911 over Wi-Fi will require cross-network enhancements. This is made possible through the development and adoption of industry standards. Enhancements to 911 over Wi-Fi may require modification of existing standards and/or the development of new standards by multiple standards bodies. The cost of standards development is difficult to quantify because it primarily entails staff time rather than clear dollar costs. Standards development by its nature can be time-consuming, and some changes will require complex standards work that entails considerable cost to the industry.

#### 3.3.5.2 Software, Hardware – Network, Device

It is anticipated that any changes to 911 over Wi-Fi capabilities would require changes to software and/or hardware for user devices and/or network equipment. In a typical development lifecycle, the following categories will entail costs, in terms of money, time, and other resources.

- Initial Development
- Lab Functional Testing
- Conformance and Interoperability Testing
- Performance Testing
- Operational Integration / Process Documentation
- First Office Application (FOA) / Field Testing
- Deployment
- Life Cycle Testing/Upgrades/Enhancements/etc.
- Incorporation of User Feedback

To the extent practical, the above framework should be applied in each recommendation contained in this Report, regardless of the apparent complexity of the recommendation.

[9] NENA-INF-018.1-2017, *NENA Non-Mobile Wireless Service Interaction Information Document*.
[10] NENA-STA-015.10-2018, *NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping*.

# 4 Current state of 911 Over Wi-Fi

The current state of 911 calling utilizing Wi-Fi connections has advanced since the last FCC Report was made to Congress in March 2021. This section presents information to clarify the current state of 911 calling over Wi-Fi.

## 4.1 Summaries of Prior Reports on 911 Over Wi-Fi

### 4.1.1 Summary of ATIS Wi-Fi Emergency Calling Landscape Assessment

"ATIS-I-0000053, Wi-Fi Emergency Calling Landscape Assessment (September, 2016)", contains a comprehensive survey of the state of Wi-Fi emergency calling as of 2016, identifies gaps in standards that support Wi-Fi emergency calling, and recommends the identification of potential future improvements to the capabilities of Wi-Fi emergency calling to match the capabilities of Voice over Long Term Evolution (VoLTE) emergency calling with respect to location accuracy, redundancy, availability, voice quality, access availability (e.g., which Wi-Fi networks should be accessible), and Non-Service Initialized (NSI) device support.

The ATIS Landscape report includes applicable federal regulations (mostly in the area of VoIP regulations), current emergency calling features, Wi-Fi emergency calling Use Cases including voice calls and Real-Time Text (RTT) calls, mapping of the identified Use Cases to existing standards, existing deployments, and standards under development. The ATIS Landscape report also contains information regarding security and privacy considerations for Wi-Fi emergency calls.
Note that some material in the ATIS Landscape report continues to be relevant in 2023, but some material is out-of-date (e.g., references to the National Emergency Address Database [NEAD]).

### 4.1.2 Summary of FCC Report to Congress

On March 23, 2021, the Public Safety and Homeland Security Bureau of the FCC prepared and submitted to Congress a Report entitled *Study on Emergency 911 Access to Wi-Fi Access Points and Spectrum for Unlicensed Devices When Mobile Service Is Unavailable* (the "Report to Congress"). The Report to Congress was submitted pursuant to Section 301 of the Repack Airwaves Yielding Better Access for Users of Modern Services (RAY BAUM'S) Act of 2018 (Section 301).

The objective of the Report to Congress was to explore the public safety benefits, technical feasibility, and cost of options for providing the public with access to 911 services using Wi-Fi access points and other alternative means during times of emergency when other mobile service is unavailable. It observed that the ubiquitous nature of Wi-Fi access points suggested that, in the long-term, Wi-Fi based solutions could be added to the "toolbox" of 911 connectivity options available to consumers, PSAPs/ECCs, and communications providers, and could complement the broader transition to an IP-based Next Generation 911 environment.

The Report to Congress commenced its analysis by examining the technical feasibility of 911 access to Wi-Fi access points. It reviewed various issues associated with current technology limitations of Wi-Fi calling including, but not limited to:

- Differences between the delivery of a 911 call over a mobile network and delivery of the call over Wi-Fi
- Wi-Fi 911 call flow
- Mobile device authentication and roaming
- Limits on Activating Wi-Fi Access During Times of Emergency
- 911 call prioritization
- 911 call routing and location
- 911 callback
- Text-to-911

- Power and backhaul
- Non-Telecommunications service providers

The Report to Congress next identified technical improvements to Wi-Fi calling needed to support 911, including, but not limited to:

- Automatic Log-On to Wi-Fi Access Points
- Mobile Core Access and Authentication (e.g., Trusted Access/Service Set Identifier/Guest Networks)
- Limiting Access to 911 Services Only
- Insertion of location information in the Session Initiated Protocol (SIP) INVITE

Finally, the Report to Congress reviewed certain policy issues related to making 911 services available over Wi-Fi access points, including, but not limited to:

- Industry coordination
- Privacy/Collection of personally identifiable Information
- Security/Cybersecurity vulnerability
- Consumer education
- Liability protection for service providers and operators
- Alternate means of 911 access/Improving resiliency of existing networks.

In light of the above, the Report to Congress concluded:
*Based on the information available at this time, we cannot reasonably estimate the costs or benefits of making Wi-Fi access points and spectrum for unlicensed devices available for 911 services when mobile service is unavailable. As discussed above, the record indicates that there are significant technical and policy challenges to providing emergency 911 access over Wi-Fi access points and networks, which could be costly to address. In addition, while enhancing Wi-Fi access points to make 911 more reliable and accessible provides clear public benefits, requiring the provision of emergency 911 access over Wi-Fi access points and unlicensed spectrum may yield less benefit at greater cost than other alternatives, such as investing in making mobile networks that already support 911 more resilient and reliable – and therefore more likely to remain available in emergencies. Thus, as better cost/benefit data becomes available, it will be important to weigh the relative costs and benefits of the specific alternatives discussed in this report against other possible approaches.*

## 4.2 Equipment Characteristics

### 4.2.1 Device (UE) Characteristics

The following table lists common Wi-Fi client devices in the market and their capabilities/ characteristics relevant to 911 event creation.

Not all of these device types are addressed in Use Cases within this Report.

| **Device (UE)** | **Wi-Fi Capable** | **Wi-Fi-Calling Capable** | **Mobility** |
|---|---|---|---|
| Smartphone | Yes | Client integrated into native dialer<br><br>Dependent on manufacture of device/software and carrier | Fully mobile |
| Feature Phone | Yes | No | Fully mobile |
| Tablet | Yes | Over The Top (OTT) Client using web browser or application<br><br>Dependent on manufacture of | May be fully mobile w/ cellular or mobile with Wi-Fi service availability |

| | | | |
|---|---|---|---|
| | | device/software | |
| Personal Computer | Yes | OTT Client using web browser or application<br><br>Dependent on manufacture of device/software | May be mobile with Wi-Fi service availability |
| Laptop | Yes | OTT Client using web browser or application<br><br>Dependent on manufacture of device/software | May be fully mobile w/ cellular or mobile with Wi-Fi service availability |
| Wearable Devices | Yes | Client integrated into native dialer to operate in standalone mode or connectivity to a smartphone required<br><br>Dependent on manufacture of device/software and carrier | Fully mobile w/ cellular or mobile with Wi-Fi service availability |
| Smart Home Devices and/or Smart Home Controllers | Yes | Dependent on manufacture of device/software | Depending upon device configuration, may be mobile |
| Music Players/ Smart Speakers | Possible | Dependent on manufacture of device/software | Depending upon device configuration, may be mobile |

Implied by these characteristics is the assumption that the UE has the capability to *participate* in Wi-Fi calling provided that network access is available via Wi-Fi to the Wide Area Network (WAN), and that the 911 application on the UE/device has access to location data. These capabilities may require both software (application) support and operating system support.

### 4.2.2 Wi-Fi Access Point (AP) Characteristics

Within the context of this Report, an Access Point (AP) acts as a bridge to provide wireless devices access to a Local Area Network (LAN) which is typically wired. Devices 'associate' with an AP to gain access to the LAN, which typically also provides access to the Internet and/or a WAN. For associated devices, an access point serves as the focal point for communications, allowing those devices to access the Internet or WAN to originate an emergency call over Wi-Fi.

Access Point (AP) ecosystems can vary widely across enterprise, small business and residential deployments. Residential and small business deployments can be further separated into operator-managed deployments and consumer-managed units.

Enterprise APs are typically managed as a group by a single authority. Example enterprise deployments can include stadiums or arenas, large office buildings, or factories. AP placement and channel assignment is planned for optimal coverage and throughput. A controller system configures and manages the individual access points, which may have limited processing resources of their own. The backhaul network connecting the APs to the controller is most often powered Ethernet. These systems often provide support for certificate-based roaming standards, such as Passpoint or Hotspot 2.0, though the enterprise may or may not have enabled those services.

Residential and small business deployments of APs by broadband system operators are perhaps the largest category of access points in the US. The residential APs are placed in the home by the broadband system operator to support distribution of data service. Sometimes, extender APs or repeaters are deployed in a subscriber's residence to expand Wi-Fi coverage past the initial AP. Small business

deployments are different from enterprise deployments. Both residential and Small Business APs are managed by the deploying operator to varying degrees. The subscriber can often control the channel used, as well as other characteristics. These APs are sometimes integrated with the residence's broadband modem (such as a cable modem or Digital Subscriber Line (DSL) modem), and in other architectures are standalone units. AP gateways tend to be stationary within the home since a broadband connection is also required. These systems sometimes provide support for certificate-based roaming standards, such as Passpoint or Hotspot 2.0, though the operator may or may not have enabled those services.

Residential and small business deployments of retail APs are a third category of AP deployment. These units are usually managed directly by the person who installed them. They may move from room to room in the residence or business location, and even move from building to building if the end user needs Wi-Fi in a certain place. Retail equipment providers often have this equipment self-configure to ease the installation for a non-technical buyer. These systems seldom provide support for certificate-based roaming standards, such as Passpoint or Hotspot 2.0, and the owners rarely have the technical background or business connections to enable these services.

APs installed in non-stationary environments, such as vehicles and airplanes, create an additional challenge as the AP's location can be in motion at the time a device connects for 911 services. This Report recognizes but does not address the challenges of these connections.

The relevant AP characteristics for 911 calls are limited to the following:

- Authentication method(s) to associate with the AP
- Quality of service support in the AP

Authentication methods are relevant if a device seeking to make a 911 call needs to associate and authenticate with the AP. A variety of methods are available for a device to authenticate itself with an AP. Authentication method options are discussed in detail in Use Case #6.

#### 4.2.2.1 Wi-Fi Quality of Service

The IEEE 802.11 standard defines Quality of Service (QoS) mechanisms for over-the-air transmission of traffic when enabled. The most commonly implemented mechanism in networks today is Enhanced Distributed Channel Access (EDCA). EDCA allows Wi-Fi traffic to be prioritized based on standard defined user priorities. These user priorities are then mapped to one of four access categories. These categories are Voice, Video, Best Effort, and Background. The access categories are listed in descending order of priority. Traffic is placed into one of four separate transmit queues based on the access category assigned.

The queues are emptied based on priority. As transmission opportunities become available, the highest priority queue, Voice, is transmitted first until the Voice queue is empty followed by the Video queue, etc.

In addition to prioritized queuing for transmit, a device with traffic to transmit waits a random amount of time after the end of the last transmission to attempt a new transmission. Prioritized traffic is given a statistically higher chance to access the Wi-Fi medium through the use of favorable backoff timer settings. This advantage varies by access category with voice being given the highest statistical chance to access the Wi-Fi medium.

There is no specific prioritization for emergency calls in Wi-Fi QoS. In the case of EDCA, if all systems were configured and performing properly, an emergency Wi-Fi call would get priority over non-voice queue traffic, but only equal priority to other voice tagged traffic. Any prioritization beyond the AP is a separate issue that should be addressed in other industry standards.

## 4.3 OSP Interconnecting Network Characteristics

### 4.3.1 IMS-based Networks

ATIS has defined an architecture to support the interconnection of IP Multimedia Subsystem (IMS) originating networks with legacy Emergency Services Networks, as well as with NENA i3 Emergency Services IP Networks (ESInets), to facilitate the delivery of emergency calls/session requests from various types of devices (i.e., fixed, nomadic, mobile) to legacy and i3 PSAPs/ECCs. ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*, defines the functions and interfaces supported by the elements of an IMS originating network, as depicted in Figure **1**, to process emergency calls and to deliver them to the appropriate Emergency Services Network.

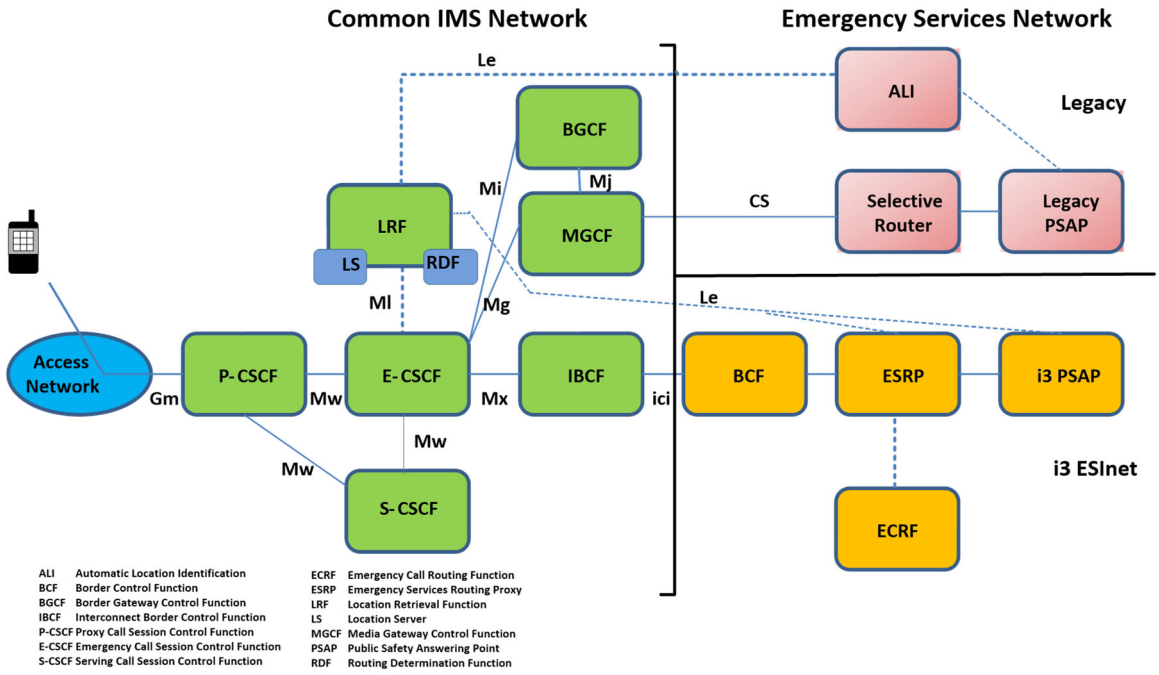



**Figure 1: ATIS-0700015 IMS Interconnection Architecture**

This architecture assumes that, when an emergency call is initiated by a UE, it will be sent to a Proxy Call Session Control Function (P-CSCF). To support 911 calling using Wi-Fi access to a 4G core network[11], the UE will set up a secure tunnel to connect to an Evolved Packet Data Gateway (ePDG) over a Wi-Fi/internet connection. The ePDG routes the emergency call to the P-CSCF in the local IMS network via a Packet Data Network Gateway (not pictured)[12].

Upon detecting that the call is an emergency call, the P-CSCF forwards the call to an Emergency Call Session Control Function (E-CSCF) in the same (originating) network. The E-CSCF forwards the call to the Location Retrieval Function (LRF) to obtain location and/or routing information for the emergency call.

UE location information (or an approximation of it) is needed to help drive the routing mechanism provided by the Routing Determination Function (RDF) in response to a query from the LRF. If a location value has been provided by the UE with the emergency call from the E-CSCF, the LRF need not invoke location retrieval functionality prior to invoking routing determination functionality. If UE

[11] 9-1-1 calling using Wi-Fi access to a 5G core network is supported using the same elements and procedures at the IMS level and as shown in Figure **1** which is also valid for 5G.

[12] See Appendix C for further details regarding architectures that include an ePDG and Packet Data Network Gateway.

location is not available in the session request forwarded by the E-CSCF, the LRF will use a location acquisition technique that is appropriate for the call type to obtain the needed location information. For example:

- If the signaling associated with the emergency call received by the LRF contains a "telephone number" (and no location-by-value or location-by-reference), the LRF will consult a Location Server (LS) that is appropriate for the call type (i.e., based on information received in the SIP signaling associated with the call) to obtain location information associated with the call. For example, for a call from a fixed device, the LRF will query an LS that contains pre-provisioned mappings from telephone numbers to fixed locations.
- If the signaling associated with the emergency call received by the LRF contains a Mobile Station International Subscriber Directory Number (MSISDN)/Mobile Directory Number (MDN) and cell site information, the LRF will consult with an appropriate LS (e.g., a GMLC) to initiate location determination. (Note that ATIS-0700015 assumes that pre-provisioned location information mapped from the cell information [referred to as an "Associated Location"] will be used in the initial routing of the call.)

Having obtained a routing location for the call, the LRF interacts with the RDF, using the location information and a service identifier (i.e., Uniform Resource Name [URN]) as input to the route determination process.[13] Note that, in the case of wireless originations, the LRF will query the RDF with a routing location (i.e., an Associated Location) that will result in the RDF returning routing information that reflects bilateral agreements between PSAPs/ECCs regarding who should receive particular types of calls from specific geographic areas.

The RDF returns routing information (e.g., a Route Uniform Resource Identifier [URI]) that will cause the call to be directed either toward an i3 ESInet or toward a legacy Emergency Services Network.

Based on the information that the LRF received from the E-CSCF with the emergency call/session request, and the emergency services network toward which the emergency call/session is to be directed (as determined based on the Route URI received from the RDF), the LRF will determine whether a Reference Identifier (e.g., a 10-digit number in the form of a URI or an HTTP Enabled Location Delivery [HELD] location URI[14]) needs to be associated with the call, and what information should be returned to the E-CSCF.

If the call is destined for a legacy Emergency Services Network, the information returned by the LRF to the E-CSCF must be appropriate for the path (i.e., trunk group) over which the call will be delivered by the Media Gateway Control Function (MGCF) to the legacy Selective Router (SR). Calls may be delivered to legacy Selective Routers either with a single10-digit number (i.e., a Reference Identifier **or** a callback number), or with two 10-digit numbers (i.e., a Reference Identifier **and** a callback number), based on the outgoing trunk group. If the LRF determines that a Reference Identifier is required, it will create one in the form of a 10-digit number, and associate it with the call. If a callback number is expected by the SR, the LRF may either include the callback number in its response to the E-CSCF, or the E-CSCF may just use the telephone number that was received in the signaling associated with the initial emergency call. The LRF will always return a Route URI to the E-CSCF and it will either return a Reference Identifier, a callback number, both, or neither (for the case where no Reference Identifier is required and the E-CSCF is expected to use the telephone number received with the emergency call). The E-CSCF will forward the call (via a Breakout Gateway Control Function [BGCF]) to an MGCF for delivery to a legacy SR. The MGCF will be responsible for interworking the incoming SIP signaling to

[13] 3GPP TS 23.167 allows the RDF to either be internal or external to the LRF. If the RDF is external to the LRF, ATIS-0700015 defines the interface between the LRF and the RDF to use the Location to Service Translation (LoST) protocol, as defined in RFC 5222.
[14] See IETF RFC 6753, "A Location Deference Protocol Using HTTP-Enabled Location Delivery (HELD)," for further details regarding the use of location URIs.

Signaling System 7 (SS7) or Multi-Frequency (MF) signaling, as appropriate for the outgoing trunk group to the legacy SR.

If the call is to be routed via an i3 ESInet, the signaling associated with the original call contained a telephone number, and the LRF, through its interactions with a LS, identified static location information associated with the call, the LRF will not associate a Reference Identifier with the call. Instead, the LRF will return the static location (as a location-by-value) to the E-CSCF, along with the Route URI. The E-CSCF will send the emergency call forward to the ESInet with the Route URI, the location-by-value, and whatever callback information was received with the origination emergency call/session request.

If the call is to be routed via an i3 ESInet and cell-related information (mapped by the LRF to an "Associated Location") was used by the RDF in routing the call, the LRF will allocate a Reference Identifier (e.g., a HELD location reference URI) to the call and return the Reference Identifier and the Route URI to the E-CSCF. The E-CSCF will send the emergency call forward to the ESInet with the Route URI, the Reference Identifier allocated by the LRF, and whatever callback information was received in the signaling associated with the original emergency call.

When a PSAP/ECC receives an emergency call that has been routed via a legacy Emergency Services Network, it will use the 10-digit key received in incoming signaling to query the Automatic Location Identification (ALI) database for location information. Upon receiving the 10-digit key from the PSAP/ECC, the ALI will consult "steering" data to determine whether the LRF must be queried to obtain location information. If the key is not present in the steering data, the ALI will retrieve static location information from its internal database, and return it to the PSAP/ECC. If the 10-digit key is contained in the steering data, the ALI will generate an E2 or Mobile Location Protocol (MLP) query to the system identified in the steering data (i.e., the LRF) to obtain location information.

When an i3 PSAP/ECC receives an emergency call/session request that has been routed via an i3 ESInet, and the session request includes a location-by-value, it will use the location-by-value received in incoming signaling as the location associated with the call. When an i3 PSAP/ECC receives an emergency call/session request that has been routed via an i3 ESInet and contains a location URI, the PSAP/ECC will de-reference the location URI to obtain location information from the LRF.

For legacy PSAPs/ECCs interconnected to i3 ESInets via Legacy PSAP Gateways (LPGs), the legacy PSAP/ECC will receive a 10-digit key created by the LPG and will use it to query the LPG for location information using the same signaling as it would use to query a legacy ALI database. If the LPG received location-by-value in incoming signaling from the Emergency Service Routing Proxy (ESRP) in the i3 ESInet, it will deliver this location information to the legacy PSAP/ECC, formatting it the same way as location information returned by an ALI database would be formatted. If the LPG received a location URI in incoming signaling from the ESRP, it will de-reference the location URI with the LRF and return the location information formatted the same way as it would be formatted if returned by an ALI database.

In support of 3rd Generation Partnership Project (3GPP)-defined Multimedia Emergency Services (MMES), ATIS-0700015 addresses the simultaneous delivery of text, voice, pictures and video on emergency originations from IMS subscribers. While ATIS-0700015 supports the termination of emergency calls originated by IMS subscribers to both i3 ESInets and legacy Emergency Services Networks, the standard recognizes that there will be limitations with regard to terminating MMES calls to legacy Selective Routers. Only MMES voice calls and some text scenarios (i.e., where the text is converted to Teletypewriter [TTY]) can be handled by a legacy Selective Router/PSAP/ECC. If location-based routing identifies a legacy Selective Router as the target for an MMES call that includes media other than voice or text, the MGCF between the IMS originating network and the legacy Selective Router will not accept any media other than voice or text. ATIS-0700015 also addresses mechanisms for adding and dropping media to/from an existing voice call (e.g., adding a picture or video clip) that has been established with an i3 PSAP/ECC.

ATIS-0700015 also addresses the impacts on the IMS interconnection architecture and signaling associated with the application of Signature-based Handling of Asserted Information Using toKENs

(SHAKEN) call authentication mechanisms to emergency (i.e., 911) calls that are routed via i3 ESInets, and PSAP/ECC callback calls made to emergency callers. ATIS-0700015 addresses the interactions between IMS functional elements in the ATIS-0700015 architecture (e.g., Interconnection Border Control Functions [IBCFs]) and the SHAKEN infrastructure to support caller identity assertion and verification associated with emergency calls.

Interactions with the SHAKEN architecture and procedures to support verification of call authentication information in the context of callback calls that are routed via a Next Generation Emergency Services Network toward the emergency caller are also addressed. In the context of emergency services, caller authentication associated with callback calls must ensure that the callback calls receive the desired call treatment and provide the best chance of being answered by the intended party. In addition to caller identity authentication, ATIS-0700015 also addresses the signing and verification of other key pieces of information that are signaled with 911 calls and callback calls, such as the Resource-Priority header, to mitigate spoofing of this information.

### 4.3.2 Non-IMS Networks

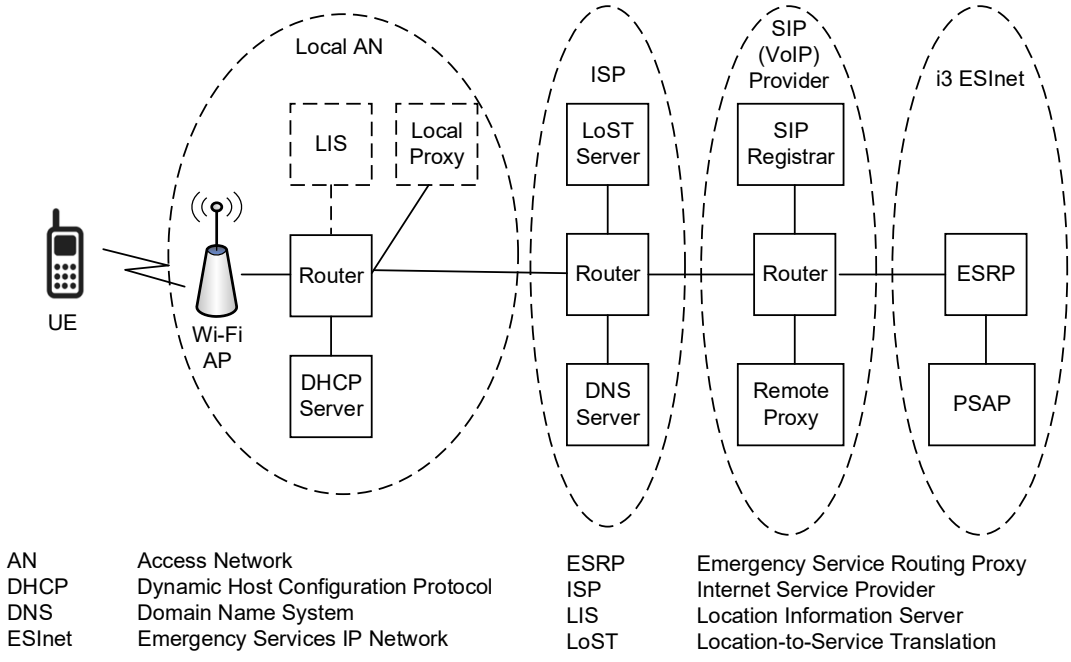



**Figure 2: NG911 Service Architecture without IMS Support (IETF Solution)**

A 911 call via a Wi-Fi AP may potentially be setup without IMS support using an architecture, procedures and signaling defined in IETF RFC 6443 ("Framework for Emergency Calling Using Internet Multimedia") published in December 2011. Although this IETF-based architecture has been defined for more than a decade, there are no known commercial implementations of emergency calling (voice as well as SMS/MMS text) using this method. It is likely that the IETF specifications would need to be updated based on advances in emergency calling that have occurred over more than a decade since their publication. Pertinent regulatory items that have advanced in the last decade include SMS/MMS text-to-911 support as well as RTT support, and design for these services would need to be taken into account. One example of the architecture is shown in Figure 2 which includes the following elements.

| **Legend for Figure** 2 | |
|---|---|
| UE | the device making a 911 call |
| AN | a local access network to the Internet for the UE which includes one or more Wi-Fi APs |
| LIS | Location Information Server - a location server supported by the local AN which is optional |
| LoST Server | A server which may be maintained by the emergency services side which provides PSAP routing information |
| SIP Registrar | Entity in a SIP (e.g., VoIP) service provider supporting callback for the UE |
| ESRP | Emergency Services Routing Proxy - Initial SIP Proxy in an i3 ESInet |
| Proxy | SIP proxy for the UE which may be local or remote |
| PSAP | the destination endpoint of the 911 call |

To establish a 911 call, the different elements in Figure 2 perform certain actions prior to a 911 call and after a 911 call is dialed. These actions are summarized below.

**ACTIONS AT THE UE**

**A. Prior to a 911 Call**

1. Register with the SIP Registrar
2. Discover a LoST Server using one of DHCP, local configuration in the UE or a DNS Server query
3. Discover a LIS using DHCP (this step is optional and depends on support of a LIS by the Local AN)
4. Obtain the UE location – using one of local UE means (e.g., Global Navigation Satellite System [GNSS]), the LIS or DHCP
5. Query the LoST server and include the UE location from step 4 and receive back a PSAP URI and local emergency dial string(s) valid for the UE location

NOTE 1: The PSAP URI could be the URI of an ESRP and not the URI of the PSAP

**B. Subsequent to a 911 Call**

6. User dials "911"
   UE verifies its location and PSAP URI (if there is time) by repeating steps 4 and 5
   a. As an option to improve privacy, step 5 can be omitted and the UE only queries the LoST server after a 911 call is dialed using a current or last known UE location
7. The UE assembles a SIP INVITE message with the following SIP headers
   a. Geolocation header – includes the UE location from step 4 or step 6
   b. Request URI – this contains an sos service URN (e.g., "urn:service:sos")
   c. Route header – contains the PSAP URI received in step 5 or step 6
   d. Contact header – contains a global URI for the UE (which is valid long term)
   e. From header – contains a local callback URI for the UE (which is valid short term)

   NOTE 2: The callback URI could contain a telephone number (tel URI) if the UE has a telephone number or might be a SIP URI if the UE can only receive SIP VoIP calls but not calls over the Public Switched Telephone Network (PSTN)
8. The UE sends the SIP INVITE to the Proxy (a local Proxy if there is one or a remote Proxy)
9. After receiving a SIP 200 OK response from the PSAP, the UE sets up media stream(s) with the PSAP – e.g., for voice
10. The user and PSAP operator communicate using the established 911 call media stream(s)
11. The UE expects the PSAP to terminate the call

**ACTIONS AT THE PROXY SUBSEQUENT TO A 911 CALL**

1. Receive the SIP INVITE sent by the UE
2. Query a LoST server for a PSAP URI if the UE did not include a PSAP URI in the SIP INVITE
3. Route the SIP INVITE to the ESRP based on the PSAP URI

**ACTIONS AT THE ESRP SUBSEQUENT TO A 911 CALL**

1. Receive the SIP INVITE forwarded by the Proxy
2. Query a LoST server for a PSAP URI
3. Add a PSAP URI to the SIP INVITE if the UE or Proxy only included the URI of the ESRP in the SIP INVITE
4. Route the SIP INVITE to the PSAP based on the PSAP URI

**ACTIONS AT THE LoST SERVER**

1. Respond to a UE (or Proxy) query that carries a UE location by returning a PSAP (or ESRP) URI and dialstring(s) that are valid for the UE location

Possible use cases for this solution include the following.

1. The user of the UE has no subscription to a CMRS carrier but is subscribed to a VoIP provider like Skype, MS Teams, Zoom etc. in the home country which supports the solution in RFC 6443.
2. The UE belongs to an Enterprise and the Enterprise supports SIP Proxy and SIP Registrar functions and the solution in RFC 6443.

The solution in RFC 6443 as summarized above was determined to have a number of dependencies and risks as follows.

1. Means to obtain a location (e.g., using GNSS or a LIS) needs to be available to a UE locally.
2. Validation of the UE location is needed (e.g., via a second independent location solution).
3. A VoIP service provider with a local SIP Proxy and SIP Registrar is needed.
4. Availability of a LoST server is required.
5. User privacy might be at greater risk if a query containing the UE location is always sent to a LoST server prior to a 911 call (e.g., whenever a UE attaches to a new AN).
6. Availability of a LIS server is required when the UE has no location capability of its own.

## 4.4 Emergency Call Detailed Characteristics

### 4.4.1 Legacy Enhanced 911 (911) Service Architectures

A key characteristic of 911 Service is Selective Routing. Selective Routing allows 911 calls to be routed to the appropriate PSAP/ECC based on the calling number/Automatic Number Identification (ANI), or other location information (in the form of a pseudo-ANI [pANI] or location key) that may be provided with the call. A fundamental element in a 911 Service architecture is the Selective Router (SR) (also referred to as an 911 tandem). An SR is a specially equipped Time Division Multiplexing (TDM) switch that controls the delivery of voice calls to PSAPs/ECCs with ANI information. In a 911 environment, an SR typically receives emergency calls over dedicated MF or SS7-supported trunk groups from wireline end offices and Mobile Switching Centers (MSCs). To support selective routing, an SR will interact with a Selective Routing Database (SRDB). The SR provides the calling number/ANI or location key to the SRDB, and the SRDB returns an Emergency Service Number (ESN). An ESN is a three- to five-digit number representing a unique combination of emergency service agencies (law enforcement, fire, and Emergency Medical Service [EMS]) designated to serve a specific range of addresses within a particular

geographical area referred to as an Emergency Service Zone (ESZ). The SR uses the ESN to select the path to the destination PSAP/ECC for the emergency call. The SR delivers the emergency call to the PSAP/ECC, typically over traditional Centralized Automatic Message Accounting (CAMA)-like (i.e., Traditional MF) or Enhanced MF (E-MF) interfaces. Traditional MF is still in use in certain areas today, and supports the delivery of a 7-digit number, along with a single Numbering Plan Digit (NPD) that can be used to derive the Numbering Plan Area (NPA) and to indicate whether the Automatic Number Identification (ANI) information should be displayed using a steady or flashing display. A flashing display is intended to alert the PSAP/ECC call-taker of special conditions related to call treatment. E-MF is a Feature Group D-like signaling scheme that is more commonly used between SRs and PSAPs/ECCs. It supports the delivery of either one or two 10-digit numbers to the PSAP/ECC with the voice call, along with an ANI II value that tells the PSAP/ECC Customer Premises Equipment (CPE) whether to display the information using a steady or flashing display. The MF signaling stream includes a key that the PSAP/ECC will use to query an Automatic Location Identification (ALI) system for the caller's location information via a separate data interface. In the case of wireline emergency callers, the ALI database contains static telephone number-to-street address mappings. In support of emergency calls from wireless callers, the ALI system typically contains mappings from a location key to steering data that triggers the ALI system to query a Mobile Positioning Center (MPC)/Gateway Mobile Location Center (GMLC) in the legacy wireless originating network to obtain location associated with the emergency caller. The PSAP/ECC uses location information returned to it by the ALI system to support the dispatch of emergency personnel.

### 4.4.2 Transitional Next Generation 911 (NG911) Service Architectures

Although end-state NG911 is defined to utilize an end-to-end IP architecture, there will continue to be legacy wireline and wireless (circuit switched) originating networks deployed after emergency service networks and a significant number of PSAPs/ECCs have evolved to support NG911 functionality. Likewise, NG911 Emergency Services Networks will be required to support the delivery of emergency calls to legacy PSAPs/ECCs. Since any PSAPs/ECCs served by NG911 Emergency Services Networks will need to be able to receive emergency calls from Next Generation (SIP/IP enabled) or legacy originating networks, gateway functionality will be a required component of transitional NG911 Service Architectures.

To support emergency calls that originate in legacy networks, the NENA i3 architecture, as specified in NENA-STA-010.3, includes the Legacy Network Gateway (LNG) functional element. As described in NENA-STA-010.3, the LNG is a signaling and media interconnection point between callers in legacy wireline/wireless originating networks and the i3 architecture. The LNG logically resides between the originating network and the NG911 Emergency Services Network and allows PSAPs/ECCs served by the NG911 Emergency Services Network to receive emergency calls from legacy originating networks. The LNG provides protocol interworking from the SS7 or MF signaling that it receives from a legacy originating network to the SIP signaling used in the NG911 Emergency Services Network. In addition, the LNG is responsible for routing emergency calls to the appropriate element in the appropriate NG911 Emergency Services Network. To support this routing function, the LNG applies NG911-specific interworking functionality to legacy emergency calls that allows the information provided in the call setup signaling by the wireline switch or MSC (e.g., calling number/ANI, Emergency Services Routing Key [ESRK], Emergency Services Routing Digits [ESRD]) to be used as input to the retrieval of a routing location (in the form of a street address or geo coordinate location) from an associated location server/database. The LNG uses this location information to query a call routing function (i.e., an Emergency Call Routing Function [ECRF]) to obtain routing information for the call. The LNG will then forward the emergency call to a routing element in the NG911 Emergency Services Network (e.g., an i3 Emergency Service Routing Proxy [ESRP]), based on the routing information provided. The LNG will

include callback and location information in the outgoing SIP signaling associated with the emergency call.

To support routing functionality within the NG911 Emergency Services Network, the LNG must be capable of processing dereference requests for routing location generated by routing elements within the NG911 Emergency Services Network. In addition to identifying the location to be used for emergency call routing, the LNG is also responsible for providing caller location to PSAPs/ECCs for emergency calls that originate in legacy networks. To support this functionality, the LNG must also be capable of receiving and processing location dereference requests from NG911 PSAPs/ECCs and Legacy PSAP Gateways (LPGs). The mechanisms used by an LNG to access caller location are comparable to those used by an ALI system to provide caller location to a PSAP/ECC in an E9 1 1 environment (i.e., by accessing provisioned data, then steering queries to MPC/GMLCs in wireless originating networks, as appropriate).

In addition to supporting the delivery of emergency calls to NG911 PSAPs/ECCs, NG911 Emergency Services Networks are required to support the delivery of emergency calls to legacy PSAPs/ECCs. To support the delivery of emergency calls that are routed via NG911 Emergency Services Networks to legacy PSAPs/ECCs, transitional NG911 Service Architectures may include a Legacy PSAP Gateway (LPG) that serves as the signaling and media interconnection point between the NG911 Emergency Services Network and the legacy PSAP/ECC. The LPG is expected to provide special processing of the information received in incoming (SIP-based) call setup signaling to facilitate call delivery to legacy PSAPs/ECCs, to assist legacy PSAPs/ECCs in obtaining the callback and location information necessary to process the emergency call and support the dispatch of emergency personnel, and to support feature functionality currently available to legacy PSAPs/ECCs, such as call transfer. The SIP signaling delivered to an LPG by an NG911 Emergency Services Network will contain the same information as the SIP signaling that is delivered to an NG911 PSAP/ECC, including location information (by reference or by value) and callback information. The LPG will be responsible for interworking the SIP signaling to the Traditional MF or E-MF signaling that is appropriate for the interface over which the call will be delivered to the legacy PSAP/ECC. In that sense, the LPG will look like an SR to the legacy PSAP/ECC. Traditional MF and E-MF interfaces to legacy PSAPs/ECCs assume that callback information signaled to a PSAP/ECC will be in the form of a 7/10-digit North American Numbering Plan (NANP) number. It is possible that the callback information delivered to an LPG with an emergency call (e.g., associated with a VoIP origination) will not be in the form of (or easily converted to) a 10-digit NANP number. If a PSAP/ECC is expecting to receive callback information delivered with the call in call setup signaling, and the callback information received by the LPG is not in the form of (or easily converted to) a 10-digit NANP number with an NPA that is appropriate for the target PSAP/ECC (i.e., consisting of one of four NPAs supported by a legacy PSAP/ECC that supports a Traditional MF interface), the LPG will perform a mapping from the callback information to a locally significant digit string that can be delivered to the legacy PSAP/ECC via Traditional MF or E-MF signaling (as appropriate for the PSAP/ECC). Note that, like emergency calls from non-initialized mobile devices, legacy PSAPs/ECCs will not be able to initiate a callback call if the callback information associated with the emergency call is not in the form of a dialable NANP number.

Location information received by the LPG will be provided to the legacy PSAP/ECC outside of the call setup process via a legacy ALI interface. The LPG will look to the legacy PSAP/ECC like an ALI system and the legacy PSAP/ECC will query the LPG using the same interface as it would use to query an ALI database. Like an ALI system, when an LPG is queried with an ALI location key (i.e., callback number and/or pANI), the LPG will respond with the location and other non-location information, as appropriate for the query protocol used by the legacy PSAP/ECC.

If the PSAP/ECC expects to receive location information (i.e., a location key) delivered with the emergency call, the LPG will generate a 10-digit key (pANI) and associate it with the location and other call information that was provided in the incoming SIP signaling from the NG911 Emergency Services Network. This pANI will be passed to the PSAP/ECC via the Traditional MF or E-MF interface (as appropriate for the PSAP/ECC) and will be used by the PSAP/ECC in the ALI query that it generates.

During the transition period while the Emergency Services infrastructure migrates toward IP and PSAPs/ECCs evolve to support i3/NG911 functionality, wireline and wireless callers and PSAPs/ECCs that are served by SRs will need to be supported. Likewise, transitional architectures must support emergency calls that are routed via an NG911 Emergency Services Network and are destined for legacy PSAPs/ECCs that are still connected to legacy SRs. A Legacy Selective Router Gateway (LSRG) will provide the needed functionality to facilitate emergency call handling in transitional architectures where legacy SRs and ALIs are still present. The LSRG is a signaling and media connection point between a legacy SR and an NG911 Emergency Services Network. An ingress LSRG allows emergency originations routed via a legacy SR to terminate on an NG911 PSAP/ECC that is served by an NG911 Emergency Services Network, as well as allowing calls routed via an NG911 Emergency Services Network to terminate to a legacy PSAP/ECC that is served by an LPG or egress LSRG. An egress LSRG allows emergency calls that are routed via an NG911 Emergency Services Network to be delivered to a legacy PSAP/ECC that is connected to a legacy SR. The LSRG also facilitates transfers of calls between PSAPs/ECCs that are served by legacy SRs and PSAPs/ECCs that are served by NG911 Emergency Services Networks, regardless of the type of network from which the call originated.

Calls originating in legacy end offices or MSCs that are routed via a legacy SR must undergo signaling interworking to convert the incoming SS7 signaling used by the SR to the SIP signaling supported by the NG911 Emergency Services Network. An LSRG on the ingress side of the NG911 Emergency Services Network supports an SS7 interface toward the SR, and a SIP interface toward the NG911 Emergency Services Network. To the SR, the LSRG looks like another SR, interconnected via an SS7 tandem-to-tandem trunk group. The LSRG must support functionality to interwork the SS7 signaling that it receives from the SR with the SIP signaling used in the NG9 1 1 Emergency Services Network.

The LSRG is also responsible for routing emergency calls that originate in a network that is connected to the SR to the appropriate (routing) element in the NG911 Emergency Services Network. To support this routing, the LSRG must apply service-specific interworking functionality to legacy emergency calls to allow the information provided by the wireline switch or MSC (e.g., calling number/ANI, ESRK, ESRD) in the call setup signaling, and passed to the LSRG through the SR, to be used as input to the retrieval of routing and caller location. The LSRG obtains caller location information by querying a legacy ALI database using the "key" (i.e., calling number/ANI, ESRK, ESRD) provided in call setup signaling. To the ALI system, the LSRG looks like a PSAP/ECC. The LSRG obtains routing location either from the ALI database (e.g., for wireline originations) or by mapping the received ESRK/ESRD to a location that will result in the call being routed to the target PSAP/ECC. The LSRG uses the routing location to query a call routing function (e.g., an ECRF) to obtain routing information for the call. The LSRG will then forward the emergency call/session request to the appropriate element in the NG911 Emergency Services Network, based on routing information provided by the routing function. The LSRG includes callback and location information in the outgoing SIP signaling sent to the NG911 Emergency Services Network. Like an LNG, to support routing functionality within the NG911 Emergency Services Network, the LSRG must be capable of processing dereference requests for routing location generated by routing elements within the NG911 Emergency Services Network. The LSRG must also be capable of receiving and processing location dereference requests from i3 PSAPs/ECCs, LPGs and egress LSRGs for caller

location.[15] When an ingress LSRG receives a dereference request for caller location information, it will query the ALI system, and the ALI system will typically steer the query to an MPC/GMLC in the wireless network.

As described above, an emergency call that is routed via an NG911 Emergency Services Network and is destined for a legacy PSAP/ECC that is connected to an SR must traverse an LSRG on the egress side of the NG911 Emergency Services Network. Upon receiving an emergency session request from an NG911 Emergency Services Network, the LSRG will analyze the signaled information and apply service-specific processing to identify the outgoing trunk group over which the call will be delivered to the interconnected legacy SR, and to ensure that the information delivered to the legacy SR is in an acceptable format. The LSRG will select the outgoing route to the SR based on the destination PSAP/ECC telephone number/address provided in the incoming SIP signaling from the NG911 Emergency Services Network. The LSRG will then deliver the emergency call to the SR over an SS7-supported tandem-to-tandem trunk group. SS7 tandem-to-tandem interfaces between legacy SRs assume that the PSAP/ECC telephone number and the callback information and/or location keys (i.e., pANIs) signaled to the legacy SR will be in the form of a 10-digit NANP number. If callback information is to be delivered to the SR (i.e., in the SS7 Calling Party Number parameter) and it is not in the form of (or easily converted to) a 10-digit NANP number, the LSRG will perform a mapping from the non-NANP callback information to a pseudo callback number that is appropriate for the destination PSAP/ECC.

The LSRG will also need to be able to pass a key to the location information associated with the emergency call to the SR, either by itself or in addition to the callback information. An egress LSRG must therefore also generate a 10-digit pANI to associate with the location information received in incoming signaling from the NG911 Emergency Services Network. (Note that the same digit string can be used to represent both the callback and location information.)

If the SR receives both a callback number (or pseudo callback number) and a pANI (associated with the location information), it will use per-PSAP/ECC provisioning to determine what will be signaled forward to the PSAP/ECC. The PSAP/ECC will use the information received in incoming signaling to query an ALI system to obtain caller location for the call. The ALI will steer the location query back to the LSRG in the same way as it would steer a location query to an MPC/GMLC in a wireless originating network. The location key used in the query to the LSRG will be the pANI (possibly in combination with the callback number/pseudo callback number) created by the LSRG for the emergency call. If the location information received from the NG911 Emergency Services Network is in the form of a location-by-value, the LSRG will be responsible for returning that location information, as well as the callback number and other non-location information, in the response to the ALI system. If the location information is in the form of a civic location/street address, the LSRG must ensure that location returned in the ALI response is in a format that is acceptable to the ALI system/PSAP/ECC. If the location information received from the NG911 Emergency Services Network is in the form of a location-by-reference, the LSRG will first have to dereference the location reference to obtain the location value to be returned in the response to the ALI system. If the location value that is received is in the form of a civic location/street address, the LSRG will have to ensure that location returned in the ALI response is in an acceptable format.

Legacy PSAPs/ECCs may also receive 911 calls from SRs that interconnect with a Media Gateway Control Function (MGCF)/Media Gateway (MGW) in an IP Multimedia Subsystem (IMS) originating network. In that case, the 911 call will be delivered to the SR over an SS7 or MF trunk group, with signaling that includes a pANI created by the IMS originating network. This pANI will be delivered to

[15] Location deference requests will typically be associated with legacy wireless originations. Location information associated with legacy wireline originations will typically be signaled forward “by value”.

the legacy PSAP/ECC over an existing MF or E-MF interface, and will be used by the legacy PSAP/ECC to query the ALI system. The ALI system will use the pANI to interact with a Location Retrieval Function (LRF) in the IMS originating network, as if it were an MPC/GMLC, to obtain location information associated with the emergency call. (See Section 4.3.1 for further details related to 911 call processing in IMS originating networks.)

### 4.4.3 End-State Next Generation 911 (NG911) Service Architectures

The end-state NG911 service architecture assumes that the originating network supports IP connectivity and NG911 call and data processing functionality, an NG911 emergency services network is in place, and legacy PSAPs/ECCs have evolved to become i3-capable, which includes being able to process multimedia communications from emergency callers, as well as location and other data associated with 911 originations, to support the dispatch of emergency personnel and the conveyance of critical incident data to first responders.

Where the architecture includes an IMS originating network, an emergency call/session initiated by User Equipment (UE) will be sent to a Proxy Call Session Control Function (P-CSCF). The P-CSCF then forwards the emergency call/session request to an Emergency Call Session Control Function (E-CSCF) in the same (originating) network. The E-CSCF forwards the request to the Location Retrieval Function (LRF) to obtain location and/or routing information for that call/session.

UE location information (or an approximation of it) is needed to help drive the routing mechanism provided by the Routing Determination Function (RDF) element in response to a query from the LRF. If a location-by-value has been provided in the session request from the E-CSCF, the LRF may not invoke location retrieval functionality prior to invoking routing determination functionality. If UE location is not available in the session request forwarded by the E-CSCF, the LRF will use a location acquisition technique that is appropriate for the call type to obtain the needed location information.

Having obtained a routing location for the call, the LRF will interact with the RDF, using the location information and a service identifier (i.e., Uniform Resource Name [URN]) as input to the route determination process. Based on existing standards documented in ATIS-0700015, the routing location used by an LRF to query the RDF for wireless originations may be an Associated Location determined by the LRF. An Associated Location is used in some wireless routing scenarios where the cell address or cell centroid cannot be used to route an emergency call. In those scenarios, an LRF will map the cell ID received in the SIP INVITE message to a routing location that is designated for the appropriate PSAP/ECC for that cell (i.e., a location that will result in the RDF returning routing information that reflects bilateral agreements between PSAPs/ECCs regarding who should receive particular types of calls from specific geographic areas). The RDF will return routing information (e.g., a Route URI) that will cause the call to be directed either toward an NG911 Emergency Services Network or toward an SR in a legacy Emergency Services Network.

The LRF returns location and routing information it has obtained to the E-CSCF. In an end-state NG911 environment, the E-CSCF will route the call along with callback and location information (by value and/or by reference) via an exit Interconnection Border Control Function (IBCF) on the egress side of the IMS originating network and a Border Control Function (BCF) on the ingress side of the NG911 Emergency Services Network to a routing element (e.g., ESRP) in the Emergency Services IP Network (ESInet). The routing element uses the location information received in incoming SIP signaling (location-by-value) or obtained by dereferencing a location-by-reference to query a Geographic Information System (GIS)-based routing database (e.g., an ECRF). The routing response contains the address of the "next hop" in the call path. Call routing may also be influenced by policy routing rules accessed by the

routing element. The routing element forwards the emergency call/session request (with the same callback and location information as it received in incoming SIP signaling) to the "next hop" element based on the address received in the response from the routing database and any applicable routing policy. The "next hop" element may be a PSAP/ECC or it may be another routing element in the call path, depending on the way the NG911 Service Architecture is implemented. Ultimately the emergency call is delivered to PSAP/ECC with the same callback and location information that was initially delivered to the routing element.

The PSAP/ECC will use the information received in signaling, as well as information received via media and through interactions with the emergency caller, to determine the type of emergency response required and the location to which the response should be directed. The PSAP/ECC will assess the availability of emergency response resources required and dispatch the appropriate emergency personnel. In an end-state NG911 environment, critical incident data will be shared between affected agencies and with first responders using standard data formats and conveyance mechanisms.

### 4.4.4 Text to 911

The ability to communicate with PSAPs/ECCs via text is critical to allowing members of the community who are deaf, deafblind, hard of hearing as well as those with speech disabilities, and any 911 caller who needs assistance and for whom a voice call to 911 might result in an escalation of an emergency situation, to obtain emergency services. Different technologies may be used to support texting to 911, including Teletypewriter for the Deaf (TTY), Short Message Service (SMS), and Real Time Text (RTT). Each technology may require specific network, service, and equipment functionality.

TTY is a technology for text transmission in the analog telephone network, character by character, as typed. It uses a modem and character codes and other transmission conventions standardized in TIA 825A, as well as in ITU-T Recommendation V.18 Annex A. Implementation of TTY text telephone technology using the TIA 825A standard is mandatory in all 911 PSAPs/ECCs in U.S. However, there are a number of limitations characteristic of TTY communications. For example, transmission can only take place in one direction at a time (half-duplex). While the TTY device is transmitting, it cannot receive. If someone tries to transmit at the same time, the characters may be garbled or lost. Therefore, users are expected to take turns typing, and give turn by using specific text tokens. While the TTY device handles text, voice cannot be transmitted. Alternating between audio and text can be done during the same call but must be formally signaled between the users. TTY devices can only transmit between 3 and 6 characters per second, typically slower than many people can type, which can cause a backlog in communication. There are limitations in the character set supported by TTY devices, and only upper or lower case characters can be used, not both. In addition, the display area on user devices is very limited (i.e., one or two lines), making long texts inconvenient to read.

In a Report and Order issued by the FCC in December 2016[16], the FCC discussed the "transition from text telephone (TTY) technology to real-time text (RTT) as a reliable and interoperable universal text solution over wireless Internet protocol (IP) enabled networks for people who are deaf, hard of hearing, deaf-blind, or have a speech disability." In light of the benefits of RTT, the FCC adopted rules permitting IP-based wireless providers and manufacturers to support RTT in lieu of supporting TTY technology. With RTT, text is transmitted instantly while being typed (i.e., character by character). An RTT-capable receiving party can immediately read the text as it is written, without waiting for the person to finish typing and press "send" or waiting for the network to deliver the message, as is the case with

[16] FCC 16-169, FCC Report and Order and Further Notice of Proposed Rulemaking in the Matter of Transition from TTY to Real-Time Text Technology; December 15, 2016.

SMS. If the sender is unable to complete a message, the receiving party will still be able to see the portion of the message the sender began, allowing a call taker to interrupt or insert conversation. RTT provides a way for consumers to incorporate conversational text along with audio (voice) simultaneously during the call. RTT uses the same architecture as IP-based voice to support emergency communications with PSAPs/ECCs via NG911 or legacy Emergency Services Networks. As described in NENA-INF-042.1, an emergency session is initiated from a user on a wireless carrier network and that session is expected to provide support for simultaneous voice and RTT text media. While both media paths are established, the PSAP/ECC may not receive both audio and RTT text media. For example, a caller that is unable to speak may only communicate via RTT. As with voice calls to 911, the RTT "call" will enter the originating IMS Network via the P-CSCF and be routed to an E-CSCF in the same network. The LRF will determine the routing location information associated with the call and will use that information to interact with the RDF. Based upon the location of the caller (or the cell site location receiving the 911 call), the call may be routed to a legacy emergency services network via an MGCF or it may be routed to an NG911 Emergency Services Network. If the call is routed to a legacy emergency services network, the Media Gateway (MGW) will convert the RTT plus audio to TTY Baudot tones plus potentially other audio (e.g., background noise, etc.). If the call is routed to an NG911 Emergency Services Network through a BCF, the media will continue to be RTT plus audio. A routing element (e.g., ESRP) in the NG911 Emergency Services Network will route the call to the PSAP/ECC. If the target PSAP/ECC is a legacy PSAP/ECC that is supported by an LPG, the LPG will have to convert the RTT to Baudot tones.

SMS text to 911 is different from RTT in that it supports the transmission of only text in block mode (i.e., the user composes an entire message and must press "send" at which point the entire message is transmitted). Like RTT, SMS supports two-way simultaneous transmission; however unlike RTT, SMS is a store-and-forward service, which means that SMS messages may be received and presented out of order. SMS text to 911 will be available on existing and new SMS-capable mobile devices that have a valid two-way text messaging subscription at the time of the initiation of SMS text to 911 text message and that can support the three digit "911" short code. SMS text to 911 relies on a different architecture than voice and RTT calls to 911.

When an SMS text to 911 message is initiated by a user on a wireless carrier network, that SMS message will be forwarded to a Short Message Service Center (SMSC). The SMSC is the network element in the wireless operator network that is responsible for distributing SMS messages. Upon recognizing the short code "911", the SMSC sends the SMS message to the Text Control Center (TCC) using the Short Message Peer to Peer Protocol (SMPP). As described in J-STD-110, the TCC is responsible for: (1) converting various protocols and acting as a gateway; (2) requesting location that may be used for routing; (3) requesting routing instructions; and (4) initiating a dialogue with the PSAP/ECC (possibly via an interconnecting emergency services network) through the appropriate interworking function of the TCC. When the TCC receives an initial text message, it obtains location from the Location Server (LS). The LS may determine a coarse location by obtaining cell site location information, or the LS may obtain the mobile device's location using commercial Location-Based Services (LBS) supported by the serving network. When queried by the TCC, the LS will invoke processes to obtain the location and return that location to the TCC for routing. The TCC uses the location information returned by the LS to interact with a Routing Server (RS). The RS supports a mechanism by which location information (either civic address or geo-coordinates) and a Service URN (urn:service:sos) serve as input to a mapping function that returns a URI used to route a text message toward the appropriate PSAP/ECC based upon the location provided by the LS. The TCC converts the text message to an appropriate protocol and initiates a dialogue with the PSAP/ECC. The TCC supports three different egress protocols. One interface provides a TTY connection to a Selective Router (SR) in a legacy emergency services network and requires that SMS text messages be converted to TTY as Baudot tones. The second interface is a proprietary Web

Services interface that supports delivery of SMS texts to transitional PSAPs/ECCs using a HyperText Transfer Protocol (HTTP) interface from the TCC. The third interface supports Message Session Relay Protocol (MSRP) and requires that the TCC convert SMS text messages to MSRP for delivery via an NG911 Emergency Services Network to an NG911 PSAP/ECC or to a legacy PSAP/ECC that is connected to the NG911 Emergency Services Network via an LPG.

In addition to delivering SMS text to 911 messages, the TCC must also be capable of processing requests for location information from ALI systems, routing elements in NG911 Emergency Services Networks, NG911 PSAPs/ECCs, LPGs, and other TCCs.

The architecture that supports SMS text to 911 messages has been extended to support the delivery of plain text Multimedia Messaging Service (MMS) messages to 911. MMS is a standard way of sending messages that include multimedia content to and from mobile phones. MMS extends SMS to allow the exchange of messages that are longer than 160 characters. One popular use of MMS is to send messages to multiple recipients. Support for MMS text messages to 911 required that the SMS to 911 architecture be expanded to include two new functional elements, namely the Multimedia Messaging Service Center (MMSC) and the MMS Interworking Function (MMS IWF), as well as the interface between them. The MMSC is a functional element in the service provider network that distributes MMS messages. The MMS-IWF resides in the TCC and receives incoming MMS messages from the MMSC. The interface between the MMSC and the MMS IWF is a unidirectional interface that allows a user-initiated MMS message to be transported from the MMSC to the MMS IWF. When a PSAP/ECC responds to an MMS text message, the TCC converts it to an SMS message and sends it via the interface to the SMSC.

If an MMSC receives an MMS message with multiple recipients, and one of the recipients is “911”, the MMSC will only include “911” in the recipient address field of the message sent to the MMS IWF in the TCC, and will remove “911” from the recipient address field of the message sent to the other recipients. If the TCC receives an MMS message that contains plain text media and additional media types, it will pass the plain text media type to the PSAP/ECC and will respond back to the mobile device with a courtesy message stating that only the text was forwarded to 911. The TCC will also provide a courtesy message to the PSAP/ECC indicating that additional media was received but not forwarded. If the TCC receives an MMS message that only contains media types other than plain text media, it will respond back to the mobile device with a courtesy message stating that multimedia content is not supported and that the user should make a voice call to 911.

### 4.4.5 Background On Roaming

Cellular networks in the United States will allow any voice-capable device that is either provided voice service to the PSTN or is in limited-service state the ability to place an emergency call with or without a roaming agreement as required under the Commission’s rules. However, there are edge cases where the combination of a lack of roaming voice service or limited service and an active Wi-Fi connection may negatively affect an international visitors’ ability to place an emergency call.

Once circuit-switched voice services including 3GPP Global Standard for Mobile Communications (GSM), 3GPP Universal Mobile Telecommunications System (UMTS), and 3GPP2 Code-Division Multiple Access (CDMA) 2000 services are shut down, very old devices that do not support VoLTE/Voice over New Radio (VoNR) will no longer receive any cellular voice service. Whenever an international roaming user has an active connection and their device supports standard VoLTE/VoNR, they will be able to place an emergency call.

Generally, where "911" is used in the context of this discussion, the number dialed may be "112" or any other provisioned emergency number on the device, Subscriber Identity Module (SIM)/Universal Subscriber Identity Module (USIM) or network. Use Cases included in this Report describe an international visitor that has an emergency. All devices and networks that follow standards process an emergency call similarly regardless of the emergency number dialed.

The ability to support callbacks in a legacy 911 environment is impacted by ALI data/processing limitations and some other practical concerns. Many countries use telephone numbers that are longer than those defined by the North American Numbering Plan, and in those cases the caller's telephone number will be truncated as ALI configurations typically allow exactly 10 digits. In the case that the number is shorter than 10 digits, the ALI display may not be populated properly or in an intelligible way, or an error may be displayed since the caller's telephone number is not a 10-digit number as expected. In either case, the country code is not included in ALI data, as ALI configurations assume the country code "1" for North America. The telecommunicator will not know the caller's country code, unless the caller informs them of their full telephone number, or the telecommunicator looks up this information based on their nationality. Finally, the telecommunicator's equipment may not be configured to make a call outside of the user's home country.

These limitations do not apply to end-to-end NG911 originated and terminated calls.

The home network VoLTE capability of international roamers visiting the US is the primary factor limiting VoLTE roaming agreements domestically with US carriers, even when their devices are VoLTE capable. Where a visiting user has an established roaming agreement and compatible device, they will have regular voice service and will be able to originate a 911 call normally. Even so, VoLTE roaming agreements are not required for international roamers to make VoLTE emergency calls from VoLTE capable devices to US PSAPs/ECCs, though these devices will be in limited-service mode.

Home networks are responsible for the devices they certify and what networks they are allowed to roam on for voice service, and are also responsible for how they treat home-routed calls over Wi-Fi Calling. Visited networks domestically in the US are responsible for VoLTE interoperability with devices when they follow the GSMA IR.92 (GSMA, IMS Profile for Voice and SMS, 2020).

That said, VoLTE interoperability globally is in the collective best interest to continue providing roaming services as legacy circuit switch networks become less available. Industry alignment on network support for IPv4/Ipv6 VoLTE would expand VoLTE interoperability for both international and domestic roaming (especially during cellular outages), and reduce the likelihood of emergency calls over Wi-Fi Calling as a last resort. Devices and/or visiting service users that do not have VoLTE interoperability will not have service at all, and will not be able to place an emergency call over cellular.

Novel approaches to purely Wi-Fi-based origination may mitigate some of the issues described in the scenarios above, as the emergency call may be originated directly through Wi-Fi, though limitations may apply as described in Section 5.1.

Eventually many of these issues will be functionally eliminated in an NG911 environment. For example, the routing architecture for NG911 calls defined in North American and European Standards provide a framework where the location provided to the NG911 or NG112 network will be able to route globally to the correct NG911 PSAP/ECC, regardless of the circumstances of the user's home or visited network, or even whether or not the user has cellular coverage or only has Wi-Fi service. Additionally, there are not the same issues with callback information in an NG911 environment. A SIP URI is globally addressable regardless of circumstances, provided there is mutual network connectivity (either through interconnection or as secured traffic over the public internet). As both continents work towards a unified next-generation emergency calling architecture, the caller's roaming status and whether they have cellular or WiFi connectivity should not matter.

## 4.5 Location Determination (UE/AP)

The table below summarizes different options for obtaining the location of UE that is initiating a 911 call over WiFi. Techniques using a combination of the methods below are commonly implemented in wireless devices that have Wi-Fi interfaces. The locations determined by these devices may be used in location-based routing that has begun being deployed in the nation's mobile networks and may be provided to a PSAP to support dispatch.

| NAME | DESCRIPTION | CHARACTERISTICS |
|---|---|---|
| DBH | Device-based hybrid (DBH) location is an estimation method that typically utilizes either a selection or a combination of location methods available to the handset in an environment, including crowd-sourced Wi-Fi, A-GNSS, and possibly other handset-based sensors. It also includes an associated uncertainty estimate reflective of the quality of the returned location. | DBH solutions such as Android Fused Location Provider (FLP) and iOS Hybridized Emergency Location (HELO) are widely available on consumer smartphones and capable of generating high accuracy, low latency coordinate-based information often sufficient to identify the caller's horizontal and vertical location.<br><br>Available for 911 calls over both cellular and Wi-Fi networks.<br><br>Accurate and reliable in a variety of environments both indoor and outdoor for both location-based routing and dispatch, but not always available. |
| Registered Location | This uses the most recent customer provided information obtained by the Wi-Fi Calling service provider that identifies the physical address of an end user's device. | 911 caller must be verified to be at a Registered Location for it to be used for routing and/or dispatch.<br><br>Registered Location is permitted to be automatically obtained with or without the user's input. |
| Global Positioning System (GPS)/GNSS Location | Location is obtained by the UE or a Public Land Mobile Network (PLMN) location server | Accurate and reliable for a UE outdoors<br>Often unavailable indoors |
| Local UE IP Address | The IP address is assigned by a WLAN AP or Local PLMN. Higher order bits in the IP address may be associated with a known approximate location. | Very coarse location granularity (e.g., identifies a town or city) |
| Media Access Control (MAC) Address of associated Wi-Fi AP | The MAC address is obtained by the UE or by a PLMN for a trusted Wi-Fi AP owned by the PLMN | Requires a database with manually preconfigured locations of Wi-Fi APs, which is not available nor feasible. |

| NAME | DESCRIPTION | CHARACTERISTICS |
|---|---|---|
| MAC Addresses of nearby Wi-Fi APs | The MAC addresses are obtained by the UE | Requires a database with manually preconfigured locations of Wi-Fi APs, which is not available nor feasible |
| Local Wi-Fi determined location | Location is determined by the UE or local Wi-Fi Network (or AP) based on local Wi-Fi measurements and known locations of local Wi-Fi APs | Applicable to an Enterprise (e.g., shopping mall, hotel, commercial company, airport, convention center) which has Wi-Fi location capability and possibly a local location server |
| Cellular-based location | Location is obtained by the UE or PLMN based on existing standards for 4G (LTE) or 5G (NR) | Very unlikely to be available for 911 over Wi-Fi as cellular should then be used for the 911 call |
| Wi-Fi AP location broadcast | The Wi-Fi AP is manually configured with its own location (geodetic and/or civic) which is broadcast using IEEE 802.11 signaling<br>Location is obtained by the UE and forwarded to the PLMN or PSAP/ECC | Reliability would be highly suspect due to possible misconfiguration or moving a Wi-Fi AP without changing its configured location<br>There may be Wi-Fi AP user privacy issues<br>Not available or feasible. |
| Last Known UE Location | Obtained by the UE, stored, and possibly updated over time using inertial sensors | Accuracy would be suspect unless the last known location is very recent |

### 4.5.1 Location Spoofing Mitigation

Just as there is value in applying caller identity authentication and verification services and associated protocols to 911 calls, Public Safety would benefit from being able to determine the legitimacy of the location information associated with the 911 calls that they receive. For example, the ability to recognize spoofed location information can provide Public Safety with a critical tool to support the detection and mitigation of swatting attacks which have been a growing problem in recent months. Swatting attacks put innocent people at risk. Location that is spoofed by bad actors can negatively impact the routing and processing of 911 calls, as well as the dispatch of emergency personnel. Ideally, a call taker at a PSAP/ECC should be able to assess, in real time, the level of trust that can be placed in the location information provided with a call.

There is ongoing industry activity within ATIS and NENA focused on developing tools that will allow a PSAP/ECC to assess the legitimacy of the caller location that they receive. An emergency location spoofing mitigation solution could leverage the SHAKEN infrastructure used to sign caller identity information to support the signing of location information associated with a 911 call by the Originating Service Provider (OSP) and the verification of that information by the Next Generation 911 (NG911) System Service Provider. Further study is needed to assess the standards impacts, as well as architecture and signaling impacts and Public Safety operations impacts, associated with a location spoofing mitigation solution.

## 4.6 Service Continuity

The following conclusions were reached regarding 911 over Wi-Fi and caller mobility that can allow a 911 call to continue without disruption of the voice or other media connection between the user and PSAP/ECC operator when a UE moves out of coverage of a Wi-Fi AP.

- Wi-Fi to Cellular
  - Wi-Fi to cellular handovers are possible when the ePDG (or corresponding 5G network elements) used to support a call over Wi-Fi and the cellular network that the device would connect to belong to the same PLMN.
- Cellular to Wi-Fi
  - There is support in standards for a call established via cellular to hand off to Wi-Fi for both 4G LTE and 5G NR. Implementation of this for 911 calls is believed to be limited so far because cellular coverage is considered the most reliable method for supporting a 911 call to the PSAP/ECC through the serving emergency services network and keeping a 911 call connected.
- Wi-Fi to Wi-Fi
  - When a 911 call is established over Wi-Fi, some mobility scenarios are possible where the UE moves away from the Wi-Fi AP that originally served the call. Each WLAN needs a unique Wi-Fi network name also known as the service set ID (SSID) of the network. Handovers between Wi-Fi APs with the same SSID are supported. Additionally, industry efforts are increasing the feasibility of seamless mobility between APs.[17]

## 4.7 Airplane Mode

Airplane Mode is a device setting in which smartphone connectivity to a RAN is deactivated but connectivity to a Wi-Fi access point may remain active. Historically, when a device in Airplane Mode called 911, OS settings may have kept the device in Airplane Mode, making it possible that a 911 call was delivered over Wi-Fi even though delivery over the CMRS network was not possible. Modern OS settings often do not maintain Airplane Mode when a 911 call is made. Instead, Airplane Mode would automatically be turned off or the user would be prompted to exit Airplane Mode on the native dialer so that the call could be delivered over the CMRS network rather than over Wi-Fi.

[17] For example, Mobile Wi-Fi is a technology that would increase seamless mobility between APs without requiring UE changes. https://www.lightreading.com/broadband/cablelabs-aims-to-bring-mobility-to-wi-fi-/d/d-id/781328

## 4.8 Automatic Activation of Device Wi-Fi

Devices allow users to toggle Wi-Fi connectivity on and off. 911 calls over Wi-Fi can only be completed if the device Wi-Fi is turned on. Some users prefer to keep Wi-Fi off, only activating Wi-Fi as-needed (e.g., for data-intensive applications; while on an airplane; etc.). When a user calls 911, iOS and Android devices turn on Wi-Fi automatically. Thus, setting aside other constraints (enabling Wi-Fi calling; accessibility through the access point; etc.), dialing 911 with Wi-Fi turned off would not prevent the call from being completed over Wi-Fi.

## 4.9 Future Consideration for Emergency Preparedness Priority Service over Wi-Fi

National Security and Emergency Preparedness (NS/EP) personnel require prioritized communications during emergency events when communications networks may be congested, degraded or damaged. Wireless NS/EP priority access is based on Multimedia Priority Service (MPS) as defined in the 3rd Generation Partnership Project (3GPP) Technical Specification (TS) 22.153 and is deployed on domestic wireless service provider networks as Wireless Priority Service (WPS). Previously, there were no standardized MPS features for Wi-Fi access networks, however in 2022 efforts were initiated to specify MPS features as part of the emerging IEEE 802.11be standard as Emergency Preparedness Communication Service (EPCS)[18]. Certification for EPCS features is not yet available.

EPCS includes features for discovery, authorization verification, invocation/revocation, and priority to NS/EP traffic. Priority treatment to NS/EP signaling and user traffic is enabled via leveraging Enhanced Distributed Channel Access (EDCA) parameters. Normally, a Wi-Fi Access Point (AP) provides EDCA parameters to associated devices that control the ability of those devices to contend for the wireless medium. EDCA parameters control the behavior of devices when they try to access the wireless medium to allow certain traffic to experience statistically improved behavior. If EPCS is activated on an AP, the AP will provide degraded EDCA parameters (i.e., longer contention window limits and arbitration inter-frame spacing) to non-EPCS devices thus providing priority to devices with EPCS enabled. EPCS can be activated on an AP by a previously authenticated device's request for EPCS activation or by the AP itself through other means not specified in the standard. An initial performance study has been conducted which demonstrates that priority, as specified in IEEE 802.11be, can be provided to NS/EP voice calls with minimal effect on the number of other non-priority voice calls that can be supported.[19]Additional studies are needed to further explore future multimedia service interactions, including concurrent voice, data and video communications.

An active EPCS prioritization session may interact with 911 calls over Wi-Fi. CSRIC VIII has identified that serious consideration should be given to potential interactions so that 911 services, in particular, can co-exist with EPCS prioritization. In current Wi-Fi standards, 911 calls are not readily identified, making coexistence challenging. If 911 calls can be identified, then methods may be developed to advance coexistence between 911 calls and EPCS communications.

## 4.10 911 Service via Airplane Wi-Fi

Making a 911 communication over airplane Wi-Fi with satellite backhaul presents some unique challenges. While calls and texts to 911 are technically feasible over an aircraft Wi-Fi connection, several factors differentiate 911 access via aircraft Wi-Fi from other types of Wi-Fi access:

[18] IEEE P802.11be/D2.0, "Draft Standard for Information Technology — Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks — Specific Requirements, Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2022
[19] Das, Subir et al., "Multimedia Priority Service over Wi-Fi Networks" IEEE Communications Standards Magazine, June 2022.

- Airplane Wi-Fi might have access protocols that are different from other types of Wi-Fi. When a consumer first enables Wi-Fi on a plane, they are in an "unauthorized" Wi-Fi state, and each airline determines the protocols to authorize Wi-Fi access. Similar to a 911 caller who needs to access a restricted terrestrial Wi-Fi access point, the user must either go through the usual association steps or some sort of alternative automated association must take place.
- In-flight Wi-Fi configurations typically disallow all voice calls, including 911 calls. These are limitations as a matter of airline Wi-Fi service[20] and CMRS provider[21] policy, not technical infeasibility. Texts, however, are typically permitted to go through assuming the Mobile Network Operators (MNO) support Wi-Fi calling, the phone has "Wi-Fi Calling" enabled and the user/passenger has a session.
- To the extent that calls or texts from airplane Wi-Fi are permitted, routing the communication to the correct PSAP presents unique difficulties for a caller/device that may be travelling more than 500 miles per hour and may not land for thousands of miles from their current location.

It should be noted that there are multiple other communication paths from an airplane to the ground to seek assistance between the flight crew and resources on the ground (e.g., satellite, High Frequency [HF] radio, Very High Frequency [VHF] radio, etc.) that would handle most in-flight emergencies, diluting the benefits in a cost-benefit calculation for 911 over airplane Wi-Fi. It is also worth noting that it may be possible for a device on an aircraft to connect to a cellular network and successfully complete a 911 call, particularly at lower altitudes and airspeeds. For example, on 9/11/2001, the FBI noted a passenger onboard flight 93 successfully made a 70-second call to the Westmoreland County 911 Center.[22]

# 5 Analysis, Findings, and Recommendations

## 5.1 Analysis

Using the analysis methodology detailed in Section 3.3, the following sections examine Use Cases and analyze potential opportunities for improvement.

### 5.1.1 Summary List of Use Cases

To organize the analysis of different aspects of 911 over Wi-Fi, Use Cases have been identified. The initial five Use Cases describe the current means to place an emergency call from a wireless device. The remainder of the Use Cases describe scenarios where the end user may not reach emergency services due to a failure in call routing or other issues, and analyze possible improvements.

---

[20] For example, **Intelsat Wi-Fi Onboard documentation states: "No Voice Applications.** You will not use any type of voice application (including, without limitation, voice over Internet protocol) without receiving prior written permission from Wi-Fi Onboard, in its discretion. Prior written permission may be denied in Wi-Fi Onboard's discretion for a variety of reasons, including, but not limited to, restrictions under applicable law and the policies of the applicable airline. Calls when the plane is airborne are also restricted by our agreements with the airlines. If you would like to seek written permission from Wi-Fi Onboard to use a voice application, please contact Wi-Fi Onboard Customer Care by email at support@wifionboard.com (US; Canada)."

[21] For example, T-Mobile service (supported by Intelsat) allows texting and streaming (no voice service support) on airlines where the service is activated. The service requires: Wi-Fi calling is enabled on the device, completion of 911 address registration, and making at least 1 call using Wi-Fi calling with that device and SIM card. The service expressly states that it does not support emergency services: (911 via text or voice). T-Mobile's webpage states that all messages are billed as if the user is on a Wi-Fi network in a domestic location, regardless of where the flight travels.

[22] See https://www.nps.gov/flni/learn/historyculture/phone-calls-from-flight-93.htm

| | Title | Call Outcome |
|---|---|---|
| Use Case #1 | 911 call over Cellular Network – Home network | Successful |
| Use Case #2 | 911 call over Cellular Network – Domestic and International Roaming (full service) | Successful |
| Use Case #3 | 911 call over Cellular Network – Domestic and International Roaming (limited-service)[23]. | Successful |
| Use Case #4 | 911 call over Cellular Network – NSI Device | Successful |
| Use Case #5 | 911 call over Wi-Fi without cellular coverage | Successful |
| Use Case #6 | Emergency Access to Nearby Wi-Fi AP | Currently Unsuccessful – Opportunity for improvement |
| Use Case #7 | Automatic Activation of Wi-Fi Calling | Currently Unsuccessful – Opportunity for improvement |
| Use Case #8 | 911 over Wi-Fi from a device with an International subscription | Often Unsuccessful – Opportunity for improvement |
| Use Case #9 | Emergency Access to nearby Wi-Fi AP when cellular RAN, Core and IMS are not available | Currently not supported |
| Use Case #10 | Emergency Access to nearby Wi-Fi AP when cellular RAN, Core and/or IMS are not available using a framework allowing the use of a default Emergency Passpoint profile | Currently not supported |

### 5.1.2 Use Cases for Existing Functionality (1-5)

#### 5.1.2.1 Use Case Descriptions

The first five (5) Use Cases in the table above represent existing functionality that will result in successful 911 calls for users. Within these 5 Use Cases, if the cellular Radio Access Network (RAN) and core network are available, a device will always default to using the RAN versus Wi-Fi, even if Wi-Fi Calling is enabled. If the RAN is not available, a device with Wi-Fi Calling enabled can still make successful emergency calls over Wi-Fi using the core network. (See Appendix B for call flow examples illustrating these Use Cases.) In the later Use Cases, additional situations are discussed where one or more of the conditions necessary for successful Wi-Fi calls are absent.

Since the first five Use Cases default to existing emergency call processing by the cellular RAN and core network, most of the criteria described in Section 3.3.4 that are important to 911 and provide benefits to

[23] A device in a "limited-service" state will be able to make emergency calls but will not be able to make or receive non-emergency calls.

Public Safety are met. Routing mechanisms built into the cellular core network and the Emergency Services Network support the routing of 911 calls to the appropriate PSAP/ECC, with callback information (or non-dialable callback information in the case of an NSI call) and location information in geodetic and/or civic format. Existing implementations also support the ability for a PSAP/ECC to obtain updated location information associated with an emergency call when the PSAP/ECC determines it is appropriate to do so. Future enhancements to cellular originating (core) networks and Emergency Services Networks may include support for mechanisms that will provide the PSAP/ECC with an assessment of the legitimacy of the callback and location information that is associated with a 911 call. The application of Signature-based Handling of Asserted information using toKENs (SHAKEN) caller identity authentication and verification procedures to emergency calls in originating and Emergency Services Networks has been addressed in industry standards, is being developed and tested, but has not yet been deployed. When applied to 911 calls, SHAKEN authentication and verification allow attestation level and verification status information, indicating the trustworthiness of the caller identification information associated with the 911 call, to be delivered to PSAP/ECC along with the callback number. Regardless of the attestation level and verification status, SHAKEN procedures should not result in the blocking of 911 calls. Standard Operating Procedures (SOPs) will specify how attestation level and verification status information may influence call handling and/or support post-processing associated with emergency calls, as determined by the jurisdiction. For example, SOPs will clearly define how caller authentication information (e.g., attestation level) will be displayed to PSAP/ECC call takers and describe how that information should be used in the course of handling an emergency call. SOPs should also provide guidance with respect to how an agency will prioritize and handle calls of different attestation levels relative to other calls occurring around the same time.

As described in Section 4.5.1, activities in ATIS and NENA are currently underway to develop a mechanism that will allow a PSAP/ECC to assess the legitimacy of the caller location information associated with a 911 call.

Originating network standards and implementations applicable to the first five Use Cases support handover of emergency calls (e.g., when a device moves from one serving cell to another) and continuity of associated location information. In addition, the architectures supporting Use Cases 1, 2, and 5 allow a PSAP/ECC to call back an emergency caller, should the PSAP/ECC determine it is necessary to do so. In Use Cases 3 and 4, callback is not available due to limited-service or origination from an NSI device.

The criteria described in Section 3.3.4 identify the desirability of providing an indication to the PSAP/ECC that a call originated as a Voice over Wi-Fi call. Such an indication may provide a PSAP/ECC with more context to assist them in handling the emergency call. In an end-state NG911 environment (where end-to-end IP connectivity is available), Additional Data delivered with an emergency call may be used to indicate a call that was originated using Wi-Fi access. In a legacy 911 or transitional NG911 environment, while there are Position Source codes that can be used to identify emergency calls that were originated using Wi-Fi access, there is no standard Class of Service value that can be used to identify a Wi-Fi originated call to a PSAP/ECC call taker. There are, however, existing implementations that use other Automatic Location Identification (ALI) data fields (e.g., the Customer Name/Service field) to convey to the PSAP/ECC the fact that the emergency call originated as a Wi-Fi call. Note that, of the first five Use Cases, the criterion related to the ability to convey an indication that an emergency call originated as a Wi-Fi call is only applicable to Use Case #5.

Location determination is provided through traditional cellular network means for Use Cases #1 through #4. Location determination for Wi-Fi calls, as applicable to Use Case #5, was originally based on the location that a user provided when they first enabled Wi-Fi calling. This location is referred to as the ‘registered location’. Location-based routing allows the device to provide information about its current location directly. Device-provided location information is added to the SIP messages used in Wi-Fi calling.

### 5.1.2.2 Feasibility Discussion and Outstanding Issues

The Use Cases discussed in this section are feasible presently and do not have outstanding issues with the initiation and successful completion of emergency calls.

***Use Case #1*** **911 call over Cellular Network – Home network**

| | |
|---|---|
| *Device* | Smart Phone with cellular subscription |
| *Cellular Network connectivity* | Device connected to Home Public Land Mobile Network (H-PLMN) cellular |
| *Wi-Fi Access* | Device may or may not be associated with a Wi-Fi access point |
| *Wi-Fi Calling Feature* | Wi-Fi Calling may or may not be enabled |
| *Description* | User dials 911 on native dialer<br>Emergency call originated over cellular radio<br>Emergency call over cellular H-PLMN routed to carrier IMS<br>(Out of Scope for Wi-Fi Calling) |

***Use Case #2*** **911 call over Cellular Network – – Domestic and International Roaming (full service)**

| | |
|---|---|
| *Device* | Smart Phone with cellular subscription |
| *Cellular Network connectivity* | Device connected to Visited Public Land Mobile Network (V-PLMN) cellular (full service) |
| *Wi-Fi Access* | Device may or may not be connected to Wi-Fi access point |
| *Wi-Fi Calling Feature* | Wi-Fi Calling may or may not be enabled |
| *Description* | User dials 911 on native dialer<br>Emergency call originated over cellular radio<br>Emergency call over V-PLMN routed to carrier IMS<br>(Out of Scope for Wi-Fi Calling) |

***Use Case #3*** **911 call over Cellular Network – – Domestic and International Roaming (limited-service)**

| | |
|---|---|
| *Device* | Smart Phone with cellular subscription |
| *Cellular Network connectivity* | Device connected to V-PLMN cellular (limited-service) |
| *Wi-Fi Access* | Device may or may not be connected to Wi-Fi access point |
| *Wi-Fi Calling Feature* | Wi-Fi Calling is not enabled |
| *Description* | User dials 911 on native dialer<br>Emergency call originated over cellular radio<br>NSI Emergency call over V-PLMN routed to carrier IMS<br>(Out of Scope for Wi-Fi Calling) |

***Use Case #4*** **911 call over Cellular Network – NSI Device**

| | |
|---|---|
| *Device* | Smart Phone with no subscription |
| *Cellular Network connectivity* | Device connected to V-PLMN cellular (limited-service) |
| *Wi-Fi Access* | Device may or may not be connected to Wi-Fi access point |
| *Wi-Fi Calling Feature* | Wi-Fi Calling is not enabled |
| *Description* | User dials 911 on native dialer<br>Emergency call originated over cellular radio<br>NSI Emergency call over V-PLMN routed to carrier IMS<br>(Out of Scope for Wi-Fi Calling) |

***Use Case #5*** **911 call using Wi-Fi Calling Feature without cellular coverage**

| | |
|---|---|
| *Device* | Smart Phone with cellular subscription |
| *Cellular Network connectivity* | Device not connected to H-PLMN cellular, and V-PLMN is not available (including for limited-service mode) H-PLMN IMS services are operational (RANs are not reachable). |
| *Wi-Fi Access* | Device is connected to a Wi-Fi access point |
| *Wi-Fi Calling Feature* | Wi-Fi Calling is enabled |
| *Description* | User dials 911 on native dialer<br>Emergency call originated over Wi-Fi radio<br>Emergency call over Wi-Fi is interconnected to the H-PLMN IMS network that is associated with the subscriber |

### 5.1.3 Emergency Access Needed to Nearby Wi-Fi AP (Use Case #6)

| ***Use Case #6*** | **Emergency Access Needed to Nearby Wi-Fi AP** |
|---|---|
| *Device* | Smart Phone with cellular subscription |
| *Cellular Network connectivity* | Device not connected to H-PLMN cellular, and V-PLMN is not available (including for limited-service mode) H-PLMN IMS services are operational (RANs are not reachable). |
| *Wi-Fi Access* | Device is not associated with a Wi-Fi access point |
| *Wi-Fi Calling Feature* | Wi-Fi Calling is enabled |
| *Description* | User dials 911 on native dialer<br>Current – Emergency call fails<br>Possible Future – Emergency Access granted to a nearby AP for the duration of the emergency call<br>- Emergency call originated over Wi-Fi radio<br>- Emergency call over Wi-Fi is home routed to carrier IMS<br>- Needs to ensure call goes to appropriate PSAP/ECC and has best known location. |

#### 5.1.3.1 Use Case #6 Description

A person enters a building without cellular coverage, but with good Wi-Fi coverage, carrying a phone and has previously enabled Wi-Fi Calling for that phone. The person does not have credentials for the Wi-Fi network. The caller's current location is not the location provided when registering for Wi-Fi Calling, and no GPS signal is visible in the building. A local emergency has occurred, but has not disrupted operation of the person's service provider's core cellular network. The person requires emergency assistance.

If the person tries to dial 911 (or some other emergency assistance code), she will experience several obstacles:

No cellular signal available
No credentials to access the visible Wi-Fi network
Current location may be unknown and does not match registered Wi-Fi Calling address

#### 5.1.3.2 Use Case #6 Feasibility Discussion and Outstanding Issues

There are 2 high level feasibility topics:

1. Wi-Fi network access
2. Location determination

#### 5.1.3.3 Wi-Fi Network Access Discussion

Use Case #6, Emergency Access Needed to Nearby Wi-Fi AP, contemplates credential-less access to an AP. It should be noted that while this unsecured access would support the intent of making 911 service available in as many situations as possible, the trade-off is in the impact on security.

The NIST Cybersecurity Framework (v1.1) "Core" has the following element in the Protect category:

> **Identity Management, Authentication and Access Control (PR.AC):**
> **PR.AC-1**: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

This risk assessment element is supported by citations from standards from various standards bodies including ISO/IEC, ISA and NIST itself. PR.AC-1 does not imply that credential-less access is strictly forbidden; it instead informs the Cybersecurity Framework (CSF) user to assess the risk involved.

And there is a risk; open, unprotected access to network services may lead to denial-of-service attacks or other threats. This risk factor should be evaluated and mitigated.

Note that a user may already have appropriate credentials to access one or more Wi-Fi networks but this Use Case assumes that the user does not have appropriate credentials. Several methods could be used to overcome this obstacle and are discussed in the following subsections.

#### 5.1.3.3.1 An unencrypted open public SSID could be configured on the local Wi-Fi network

This would allow a phone without local credentials to associate with the Wi-Fi network. However, the user would still need to find and manually select the appropriate SSID. Since open networks expose users and the local infrastructure to security risks, most administrators will not configure them. Because of the security risks, this option should be avoided. Further, open public Wi-Fi networks may not be a reliable means for legitimate users to access 911.

#### 5.1.3.3.2 The local Wi-Fi network and the client device could support Opportunistic Wireless Encryption (OWE)

To mitigate some of the security issues associated with open SSIDs, the AP and client could use OWE (Opportunistic Wireless Encryption) defined by IETF RFC 8110 and standardized by the Wi-Fi Alliance under the "Wi-Fi Certified Open" certification program. This allows devices lacking local credentials to establish a secure connection between the AP and client, but still requires the user to find and manually select the appropriate SSID and is only supported in a minority of the most recently released networks and client devices.

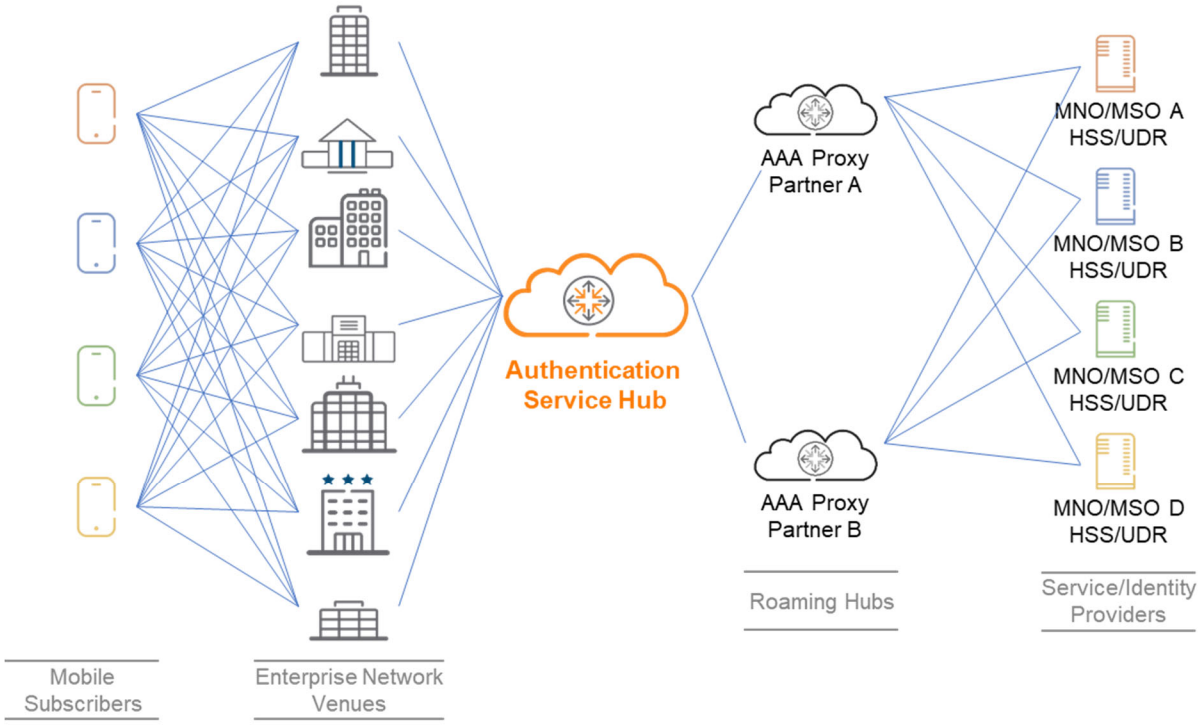
The use of this option to enable a successful Use Case requires significant effort with regard to upgrading the installed base of AP hardware and new device software (to auto-select the OWE AP in an emergency call situation). A thorough evaluation of the feasibility of this option would require more in-depth study and could lead to additional standards activity.

#### 5.1.3.3.3 The local Wi-Fi network, the client device, and cellular service provider could support Passpoint$^{tm}$, with new Emergency Calling addition

The *Passpoint* standard allows a client device with cellular credentials to automatically and securely authenticate itself, with no user intervention, on a participating Wi-Fi network. The *Passpoint* standard has been supported in all client and network equipment for many years. All major US mobile network operators support *Passpoint* and push the necessary *Passpoint* profiles to their subscribers' devices. Local support for *Passpoint* would require a secure tunnel between the local network and the mobile network

operator's authentication server and an agreement between the operator and the local Wi-Fi network to allow it to advertise the operator's PLMN over Wi-Fi. This method is not currently available to most subscribers of mobile network services outside the U.S., thus their phones will not generally support this feature.

The diagram below illustrates an example network supporting *Passpoint* authentication of devices (shown at far left). Mobile subscribers attempt to connect to enterprise venues. Those venues may have existing connections with an authentication service hub, which may also involve commercial arrangements. The authentication service hub routes individual authentication requests to the appropriate MNO(s) for approval. Proxy partners may also be involved acting as clearing houses to direct the authentication requests.




Additional feature work within *Passpoint* would be needed to provide support for differentiated priority for emergency calls. Current *Passpoint* service generally provides the same level of service to all devices that successfully authenticate. Proprietary features may exist that already support this functionality.

#### 5.1.3.3.4 The local Wi-Fi network and the client device could support 802.11u™ Emergency Access

An existing 802.11 feature allows a client device to request access to an AP for the purposes of an emergency call and to provide a method for an AP to advertise this emergency call support. This feature remains optional, and as a result has rarely been implemented, and provides no security for the emergency call traffic over the air.

Similar methods could be defined to allow a client device to request access for emergency communications, but use of the current 802.11u feature set should be avoided due to the lack of security.

### 5.1.3.4 Internet Access

Assuming the device successfully associates with the Wi-Fi network, the local network must not block internet access or prevent the mobile phone from establishing a secure tunnel to the core mobile network

required by Wi-Fi Calling. Any network that supports *Passpoint* should also support Wi-Fi Calling. However, some network systems exist only to provide local communications within a smaller group of devices, notably in an industrial or factory setting. In those cases, the network is purposefully not connected to the Internet. If Access Network Query Protocol (ANQP) is implemented on the AP, this limitation could be indicated to help mitigate the risk of connecting to a network that lacks internet connectivity. A recommendation to avoid a smartphone user wasting time in an emergency situation is that any Wi-Fi deployments that do not provide Internet access should implement the Emergency Service Support ANQP elements and not indicate that emergency services are reachable using this AP. A change could be proposed with IEEE 802.11 to add an option that affirmatively indicates that emergency services are not reachable through that AP.
Note also that the Emergency Call Number ANQP-element, when correctly provisioned, can provide one or more emergency phone numbers to a requesting device that will direct an emergency call toward a PSAP/ECC in the local geographic area of the device.
Some systems funnel traffic back to centralized firewalled gateways. Even if a client device was able to connect to a local Wi-Fi network, its traffic might still be blocked by a firewall in the network if the device is not recognized as authorized to traverse the firewall to reach the Internet. Methods should be developed to ensure that any device accessing the network to initiate an emergency call be assigned to a role or profile that supports Wi-Fi Calling.

#### 5.1.3.5 Wi-Fi Network Access Outstanding Issues

The following outstanding issues exist for Wi-Fi network access:

1. Open public SSIDs are insecure and avoided by enterprises as well as residential users of Wi-Fi.
2. OWE is not supported by most access points, enterprise systems and client devices.
3. *Passpoint* profiles are rarely provided to enterprise Wi-Fi systems and are not provided to residential retail AP devices. *Passpoint* profiles are not generally provided to international client devices. Definition of a new emergency calling indication and associated profile would be desirable.
4. Emergency Access using 802.11u is insecure and not supported by most APs or client devices.

To enable an entirely new option for users without Wi-Fi network credentials would require substantial new standards development.

Alternatively, more extensive support for *Passpoint* may provide a faster improvement for people who have currently active devices. It is important to note that it will not improve performance for NSI devices, or international roamers absent broader international adoption.

#### 5.1.3.6 Location Determination Discussion and Outstanding Issues

Accurate determination of the phone's location is important for call routing, and to dispatch emergency services. The recently updated rules for non-fixed interconnected VoIP services require the provision of dispatchable location with each 911 call if it is technically feasible, and if it is not feasible, the provision of verified Registered Location information (with or without additional action by the caller) or Alternative Location information, or the call is to be routed to a national emergency call center.

Implementations of low latency device-based hybrid (DBH) location technologies for wireless emergency calls allow wireless devices that have access to information on their current location to present that information to the networks that are processing the call, e.g., the originating network. This location information enables the originating network to route the incoming emergency call to the most appropriate emergency services network for routing to the appropriate PSAP/ECC, and for the PSAP/ECC to dispatch emergency responders to the calling device's location.

Despite the progress with 911 location accuracy and location-based routing for wireless 911 calls,

consumer access to Wi-Fi Calling service still relies on the availability of user Registered Location - address information inputted to the carrier's system prior to Wi-Fi Calling service initialization.

This has multiple challenges:

1. Due to previous regulatory requirements, current carrier implementations require a Registered Location from the customer where the service will first be used and must provide a means of updating that location at will and in a timely manner. Existing implementations and the regulatory framework that drove them must be considered along with the efforts to make Wi-Fi Calling to 911 more broadly available to callers without an associated Registered Location.

2. The accuracy of the Registered Location for the purpose of 911 call handing is dependent on the device owner updating their address.

3. At the time of the 911 call, service providers are required by FCC rules derived from the RAY BAUM'S ACT to identify whether the service is being used to call 911 from a different location other than the Registered Location and if so, either
    a. Prompt the customer to provide a new Registered Location; or
    b. Update the Registered Location without requiring additional action by the customer.

When Registered Location verification is not achieved, accurate Alternative Location information sourced from the device or other sources may be used when available for location-based routing and for emergency dispatch. Routing calls to a national emergency call center is permitted, after a "good-faith" effort to obtain location data from all available location sources.

The broad availability of DBH location technologies combined with the deployment of location-based routing has led to improvements in location information for 911 over Wi-Fi over supporting networks, reducing the reliance upon a user-inputted Registered Location and associated challenges.

### 5.1.4 Automatic Activation of Wi-Fi Calling Feature (Use Case #7)

| ***Use Case #7*** | **Automatic Activation of Wi-Fi Calling** |
|---|---|
| *Device* | Smart Phone with cellular subscription |
| *Cellular Network connectivity* | Device not connected to H-PLMN cellular, and V-PLMN is not available (including for limited-service mode). H-PLMN IMS services are operational (RANs are not reachable). |
| *Wi-Fi Access* | Device is associated with a Wi-Fi access point |
| *Wi-Fi Calling Feature* | Wi-Fi Calling is not enabled |
| *Description* | User dials 911 on native dialer<br>Current – Emergency call fails<br>Possible Future – Wi-Fi Calling Feature is activated for the duration of the emergency call<br>- Emergency call originated over Wi-Fi radio<br>- Emergency call over Wi-Fi is home routed to carrier IMS |

#### 5.1.4.1 Use Case #7 Description

A person enters a building without cellular coverage, but with good Wi-Fi coverage. She is carrying a smartphone with a cellular subscription, but has not enabled Wi-Fi Calling. She has credentials for the Wi-Fi network and the smartphone is currently associated with the nearest AP. A local emergency has occurred, but has not disrupted operation of her service provider's core cellular network. She requires

emergency assistance.

If she tries to dial 911 (or some other emergency assistance code), her emergency call will fail even though the relevant networking entities for an emergency call over Wi-Fi are available because the Wi-Fi Calling feature has not been activated.

#### 5.1.4.2 Use Case #7 Feasibility Discussion and Outstanding Issues

The current interconnected VoIP calling regulatory framework has resulted in Wi-Fi Calling feature implementations that require the user to affirmatively activate Wi-Fi Calling and provides a registered location for emergency service purposes as part of service initialization. In cases such as the one discussed in this Use Case, the technology has the capability of providing emergency calling services and the reception and routing of such a call is entirely feasible, but in many wireless operator and mobile device feature implementations, the network and the mobile device may not provide such a service.

It may be feasible to support an emergency call attempt in the context of this Use Case by modifying device implementations to support some form(s) of automatic Wi-Fi Calling enablement, and enhancing network implementations to address issues related to location availability, emergency call routing, etc., as described below. One potential mechanism for addressing scenarios where a cellular network radio connection is unavailable is to have the device override device settings to allow temporary support for Wi-Fi Calling when (only) an emergency call attempt is made on a device that supports Wi-Fi access.

Alternatively, the underlying operation of Wi-Fi capable devices could be changed to always allow emergency calling over Wi-Fi when the cellular network RAN is not accessible and a Wi-Fi association is active, regardless of whether the user has chosen to activate the Wi-Fi calling feature.

Assuming support for the enhancements described above, routing of the emergency call will be impacted by the availability and accuracy of emergency location information. In either of the scenarios described above, the device may be able to provide a location estimate in call establishment signaling associated with the emergency call that is sufficient to allow the call to be routed to the appropriate PSAP. Under current practices, where the RAN is not available, the IMS core network will not perform a proximity check of the device-based location by comparing it to a cell-based or other network-determined location Although Registered Location may be available to the IMS core network due to a previous Wi-Fi Calling activation, that Registered Location may not reflect the caller's current location and, without the availability of the RAN, cannot be verified prior to using it for emergency call routing.

If neither device-based location nor a verified Registered Location is available, the emergency call may be default-routed to a national emergency call center as a last resort, consistent with operator, regulatory, and PSAP policy, and provided that a good faith effort has been made to obtain location data from all available alternative location sources. This assumes that the device can determine a path to the IMS core network.

If Wi-Fi Calling is automatically activated because the caller has dialed 911, some implementations may be limited in their ability to determine a serving ePDG and provide location information for call routing and dispatch. In these cases, the device may not be able to attach to the IMS core network.

This is another scenario where emergency calls could be routed to a national call center that is designated to handle such calls; however, in this case, the device, upon recognizing that the emergency call is to use Wi-Fi access, would need to be able to identify a path to that call center.

For any of the scenarios discussed in the context of this Use Case, an important question for investigation is the proper length of the call-back time and associated call features. Section 3.3.4 identifies support for PSAP callback as an important feature of 911, however, discussions within the CSRIC group suggest that

the length of time within which a PSAP may attempt to call back the emergency caller is unclear. If the emergency caller returns to cellular coverage, then callback is not an issue. If Wi-Fi Calling that has been automatically activated remains active for some period of time after the emergency call has terminated to allow for receipt of PSAP callbacks, further investigation is needed to determine whether incoming non-emergency calls would or could be blocked, or the emergency caller would be allowed to initiate non-emergency calls during the time that Wi-Fi Calling remains active.

Section 3.3.4 identifies the importance of maintaining a 911 call when a caller moves outside of the serving area of the cell or Wi-Fi Access Point (AP) to which the call is initially connected. See Section 4.6 for further discussion of handovers between Wi-Fi APs, as well as Wi-Fi to cellular handovers, that may be applicable to this Use Case.

The criteria described in Section 3.3.4 identifies the desirability of providing an indication to the PSAP that a call originated as a Voice over Wi-Fi call. As described in Section 5.1.2.1, Additional Data delivered with an emergency call may be used to indicate that the call originated using Wi-Fi access. In a legacy 911 or transitional NG911 environment, existing implementations use ALI data fields, such as the Customer Name/Service field, to convey to the PSAP the fact that the emergency call originated as a Wi-Fi call. Since this Use Case describes a scenario where an emergency call is routed using Wi-Fi access to an IMS core network, it can be assumed that the IMS core network will populate the relevant information in the Additional Data that it creates.

Since this Use Case assumes that the caller has a cellular subscription and that 911 calls are routed via an IMS core network, SHAKEN functionality supported by the IMS core network can provide caller identity authentication for 911 calls in the context of this Use Case. As described in Section 3.3.4, this will allow Public Safety to assess the legitimacy of caller identity information delivered with those 911 calls.

#### 5.1.4.3 Automatic Activation of Wi-Fi Calling Outstanding Issues

Under the current interconnected VoIP calling regulatory framework, affirmative user action is required to enable Wi-Fi Calling on a device. Users who have not activated the Wi-Fi Calling feature on their phone may not realize that they are reducing the number of situations in which they can successfully make emergency calls. The users may not want to enable Wi-Fi Calling for other reasons.

Possible improvements to the current situation include:

- It is possible the cellular service providers encourage users to activate Wi-Fi Calling by emphasizing the improved emergency calling options.
- It may be feasible for cellular service providers to automatically enable Emergency Calling Over Wi-Fi as a new feature. Similar to the current emergency calling behavior that uses a cellular connection for 911 calls even if the user has enabled Wi-Fi calling, an additional feature could be defined that will allow a 911 call attempt to automatically go over Wi-Fi if the cellular network is not available. The current requirement to collect a registered customer location before enabling service is an impediment.
- Alternatively, it may be feasible for implementations to allow an emergency call attempt to activate the Wi-Fi Calling feature on a device that does not already have Wi-Fi Calling enabled, without user interaction, when the cellular network is unavailable.

The use of auto-enablement of Wi-Fi calling for emergency calls when the cellular network is not available will need careful investigation to determine whether, once activated, it is limited to emergency calling and PSAP/ECC calling or if non-emergency calls should also be available. PSAP/ECC callbacks should be supported for some period of time. (See RFC7090 and RFC6881 for further discussion.)

### 5.1.5 911 over Wi-Fi from a device with an International subscription (Use Case #8)

| ***Use Case #8*** | **911 over Wi-Fi from a device with an International subscription** |
|---|---|
| *Device* | Smart phone with an international cellular subscription located in the United States |
| *Cellular Network connectivity* | Device not connected to V-PLMN (including for limited-service mode). H-PLMN and V-PLMN IMS services are operational (RANs are not reachable). |
| *Wi-Fi Access* | Device is associated with a Wi-Fi access point |
| *Wi-Fi Calling Feature* | Wi-Fi Calling is enabled |
| *Description* | User dials 911 (or any recognized emergency number) on native dialer<br>Current – The emergency call is originated over Wi-Fi and is interconnected to the H-PLMN IMS network in the home country configured on the SIM card<br>Possible Future – Emergency call over Wi-Fi is interconnected to a V-PLMN IMS network |

#### 5.1.5.1 Use Case 8 Description

A person with cellular roaming coverage enters a building with good Wi-Fi coverage. The caller is carrying a smartphone with a subscription to a service provider located in their home country and has Wi-Fi Calling enabled. A local catastrophic event occurs causing all the cellular radios in the vicinity to become unavailable but has not impacted the Wi-Fi infrastructure to which her device is connected, Wi-Fi Calling service through her home service provider, or the IMS core networks of potential roaming service providers. The caller requires emergency assistance.

If the caller tries to dial 911 (or any recognized emergency number) that emergency call would originate over Wi-Fi over the established home ePDG connection and home route to the caller's service provider's IMS network for call processing even though there are roaming IMS networks available for Local Breakout (LBO) directly to the local PSAP/ECC. This presents significant operational concerns as the ability of the home IMS network to transfer the emergency call and associated data internationally to the PSAP/ECC in the United States could be limited.

As an alternative to interconnecting with the home network, the call could instead be interconnected with a visited network in the US if there is a roaming agreement with such a network. This alternative is supported in international 3GPP standards but is not commonly implemented. This would avoid international PSAP routing problems and would be very similar to support of a 911 call over a Cellular Network for International Roaming (Use Case #2) at an IMS level.

#### 5.1.5.2 Use Case #8 Feasibility Discussion

In scenarios such as the one discussed in this Use Case, the technology may have the capability to leverage the 3GPP LBO roaming architecture for providing emergency Wi-Fi Calling service directly to the local PSAP/ECC. It may be feasible to support 3GPP LBO for Wi-Fi Calling with device and network enhancements that would allow for the on-demand selection of a VPLMN ePDG for emergency services. The emergency ePDG section procedure would require devices to determine the country it is located in and store a list of potential supporting VPLMNs. When a device determines to be located in a country other than its home country, it may query a Domain Name System (DNS) with a Fully Qualified Domain Name (FQDN) containing VPLMN information for location-specific emergency ePDG selection within the roaming partner's PLMN. The roaming PLMN could return a list of geographically diverse ePDGs that service the local area but remain available due to their remoteness to the catastrophic event.

#### 5.1.5.3 Use Case #8 Outstanding Issues

The addition of Wi-Fi roaming for emergency services would likely need to be added to commercial cellular roaming agreements to support reciprocal roaming capability for US travelers abroad and to ensure interoperability between the devices and VPLMN IMS networks.

The device must be able to reliably convey location information using standards-based signaling at call setup for a VPLMN IMS core network to deliver the emergency call directly to the appropriate PSAP/ECC. When device location is unavailable, the emergency call should be routed to a national call center to assist the caller with accessing local emergency services. A dedicated national call center capable of supporting a large influx of emergency calls from multiple service providers should be considered for handling these calls.

If the call is IMS-originated, device-provided location can populate the Presence Information Data Format – Location Object (PIDF-LO) in the SIP INVITE with the user's true location. In end-state NG911 this allows the call to be recursively routed via ECRFs and Forest Guides to the correct PSAP/ECC. In transitional NG911 (when not all elements are NG911 conformant end-to-end), device-provided PIDF-LO location information can make international call transfer take less time as the true location of the caller is already known.

The call may also be routed to a call triage center to assist the caller with accessing local emergency services. The call may also present a recorded announcement instructing the caller to provide information about contacting local emergency services, or that the service is not available. This is the responsibility of the home operator.

### 5.1.6 Emergency Access to Nearby Wi-Fi AP When Cellular RAN, Core and IMS are Not Available (Use Case #9)

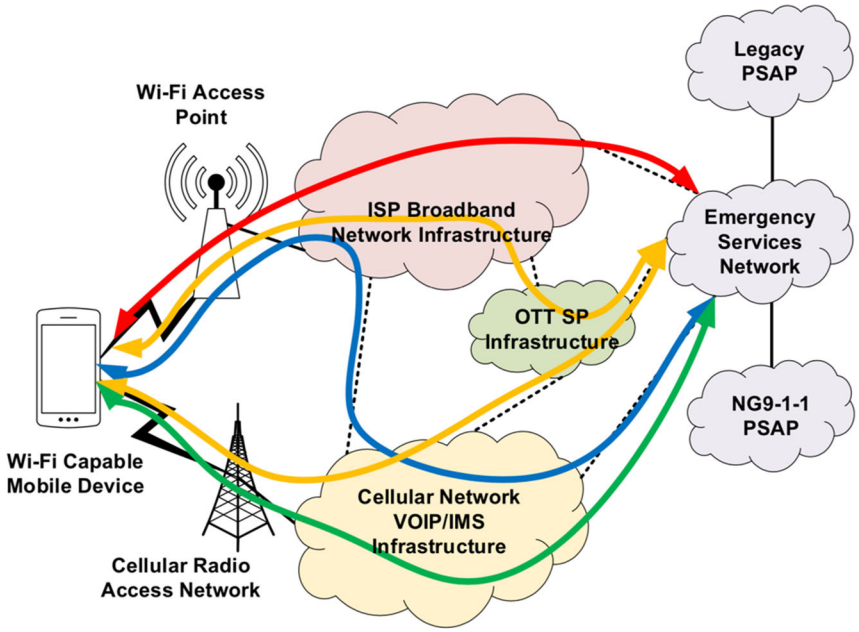
This Use Case is associated with Figure 7: 911 Origination - No Access to Cellular Network - Modified IETF Solution.

*Use Case #9* Emergency Access to nearby Wi-Fi AP when cellular RAN, Core and IMS is not available

| | |
|---|---|
| Device | The Use Case applies to devices with<br>• Wi-Fi-only interface and no SIM<br>• Both cellular and W-Fi interfaces |
| Cellular Network connectivity | Home or visiting cellular RAN, Core and IMS connectivity are not available |
| VoIP Service Provider | There is a common VoIP service provider who supports the modified IETF solution. |
| Wi-Fi Access | Device is associated with a Wi-Fi Access Point. |
| Wi-Fi Calling Feature | Wi-Fi Calling is enabled |
| Description | User dials 911 on native dialer<br>Current – Emergency call fails for there are no known communications servers to route the 911 calls<br><br>Possible Future – A designated entity deploys and operates communications servers to receive and route 911 calls in this corner case. It is assumed that the devices are pre-provisioned with these communications servers' information. |

### 5.1.6.1 Background

The following diagram titled *Figure 7.1: Potential Paths for Emergency Call from Mobile Device to Emergency Services* included within in *ATIS-I-0000053, Wi-Fi Emergency Calling Landscape Assessment, September 2016*, identifies several scenarios in which 911 call support is required. The Use Case in this section focuses on the red arrow, which shows a connection between the calling device and PSAP/ECC, through the Internet Service Provider (ISP) broadband network and with a common VoIP Service Provider (SP who supports the modified IETF solution but requires no subscription.




### 5.1.6.2 Use Case #9 Description

The caller is currently in a natural disaster area and wants to make an emergency voice call. Unfortunately, the tornado took down several nearby cellular towers, and the power failure at the nearby data center also impacted the cellular IP Multimedia System (IMS) and core infrastructure. Fortunately, a nearby Wi-Fi network with internet access is accessible to the caller. The caller associates their device with the Wi-Fi network. Upon joining the Wi-Fi network, the caller dials 911 on the device's native dialer.

### 5.1.6.3 911 Communications Server Proposal

This proposal envisions a handful of 911 communications call routing servers serving all of the United States. Their only job is to receive 911 calls for the above Use Case and route them to the correct PSAP/ECC based on the location information supplied by the handset in the signaling messages. The service should be capable of Location Based Routing (LBR).
The idea of an entity, other than the communications service provider (e.g., CMRS provider) with whom the end user has no direct relationship, communicating directly with the end-user handset for 911 call routing will require new specification development and interoperability testing for the 911 calls to work seamlessly and reliably. There are several IETF RFCs that can provide foundational technology but a separate document will be needed to describe the end-to-end working of the proposed system.

**Assumptions and considerations**:

- The handset is capable of determining its geolocation (e.g., using onboard GPS) and reporting it to the 911 communications servers in the signaling messages (e.g., using the SIP geolocation header)

- No Use Case-specific assistance from the Wi-Fi network operator, or CMRS provider, or ISP is necessary
- An existing or new entity could host and operate these 911 call-routing servers.
- Existing communications call-routing servers and proxies may agree to perform the 911 call routing function in case of emergencies described in the Use Case.

#### 5.1.6.4 Identity Discussion

The user's device may have several options to choose from when registering with the network for the 911 call. For example, the device can potentially use:

1. SIM Card Integrated Circuit Card Identification (ICCID) if registering to the service provider with which the device has a subscription
2. Other unique IDs made available to the device
3. Pre-provisioned certificate (e.g., Passpoint profile)

**Assumptions and considerations:**

- This identity should be globally unique and routable for the purpose of 911 callback
- PSAPs/ECCs may be able to receive an emergency call with identities other than a phone number

#### 5.1.6.5 Communications Server Discovery Discussion

As one option, the device manufacturers or the service provider (e.g., CMRS provider) may pre-provision the device with a generic 911 communications server address (e.g., 911.communicationsserver.InPublicService.org). The server at that address could redirect the device's communications based on a location disclosed by the device.

A DNS Service (SRV) record or DHCP could also be utilized for finding these servers.

#### 5.1.6.6 Callback Discussion

Upon successfully connecting to the PSAP/ECC, if the caller's handset disconnects, how does the PSAP/ECC execute the required "call back"?
It is envisioned that the signaling message sent to the PSAP/ECC includes the routable contact for the device and the 911 communications server for the PSAP/ECC to use to route the call back to the caller.

RFC 6443 proposed using SIP Contact and From headers, which is another possible solution for 911 callback in this Use Case.

### 5.1.7 Emergency Access to nearby Wi-Fi AP when cellular RAN, Core and/or IMS is not available using a framework allowing the use of a default Emergency Passpoint profile (Use Case #10)

*Use Case #10* Emergency Access to nearby Wi-Fi AP when cellular RAN, Core and/or IMS is not available using a framework allowing the use of a default Emergency Passpoint profile

| | |
|---|---|
| Device | The Use Case applies to devices with<br>• Wi-Fi interface and (optional) SIM<br>• Wi-Fi interface is available<br>• Device is pre-configured with the default Emergency Passpoint profile. |
| Cellular Network connectivity | H-PLMN and V-PLMN RAN are unavailable; H-PLMN Core and IMS are unavailable. |
| Wi-Fi Access | Wi-Fi network participating in a framework that defines technical interworking for Passpoint-based authentication as well as legal obligations on the Wi-Fi network provider, allowing use of a proposed Emergency Passpoint profile in the location. The Wi-Fi network may or may not have any direct business relationship with the device's MNO but offers network access to any device with an Emergency Passpoint profile for making 911 calls. |
| Wi-Fi Calling Feature | Wi-Fi calling is enabled |
| Description | User dials 911 on native dialer<br><br>Current – Emergency call fails because device has no Wi-Fi access network credentials and therefore cannot connect to the network. Even assuming Wi-Fi access, the call still fails because there are no mobile core and/or IMS servers to route the 911 call.<br><br>Possible Future – Leveraging a framework allowing the use of an Emergency Passpoint profile, many more devices would be able to automatically associate with Wi-Fi access points that may also provide network location to the emergency service. This solution requires the devices are pre-provisioned with a proposed Emergency Passpoint profile. This solution may also require that the AP signal its location. |

### 5.1.7.1 Technical Architecture

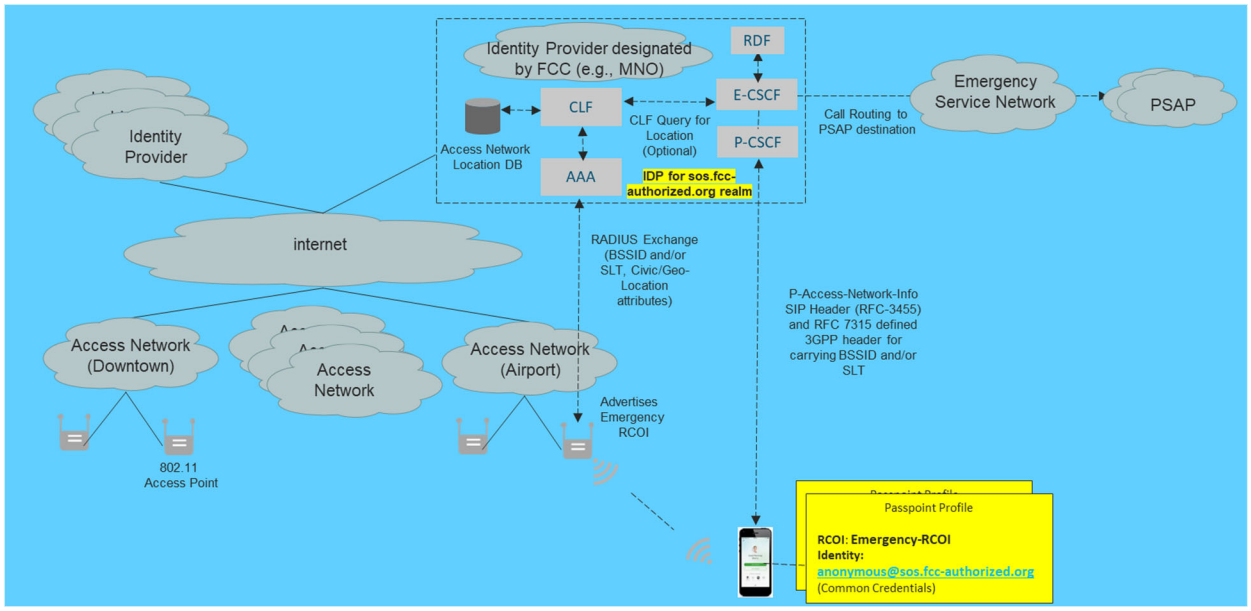



**Figure 3: Internet-based Framework for 911 Calling**

The following are the key aspects in this use-case.

A designated IDP and designated emergency calling services are proposed to support emergency 911 service. An Authentication Authorization and Accounting (AAA) server in the IDP could support a new realm for authentication of 911 callers (e.g., an FCC-sponsored realm such as "sos.fcc-authorized.org") and associated policies. A dedicated P/E-CSCF (Proxy/Emergency Call Session Control Function) would also be required to support emergency calling services.

The user devices would need to be pre-configured with an Emergency Passpoint profile, including an emergency RCOI, and a common identity for emergency services. Device eco-system vendors might pre-configure this profile in a device at the time of manufacturing or an updated profile might be pushed onto the device later using established carrier-bundle based provisioning if carriers supported this profile.

This profile would be common for all devices so that a device could discover Wi-Fi access networks that support emergency 911 services.

Wi-Fi access networks that participate in the framework and are willing to support emergency 911 services could configure the emergency RCOI on their Wi-Fi equipment. Wi-Fi OEM suppliers may augment existing Passpoint provisioning interfaces with emergency RCOI settings. These networks would then be able to allow any devices with the Emergency Passpoint profile but without access credentials to connect to those networks for at least emergency calling.

The designated entity hosting the voice service function can deploy either the 3GPP-defined IMS core, or an implementation of the SIP Proxy function designed specifically to support emergency calling, either of which would be able to terminate call signaling from an RFC-3261-compatible Wi-Fi calling client.

#### 5.1.7.2 WLAN Network Identification and Selection

An emergency RCOI may be provisioned in WLAN equipment by the local Wi-Fi network and configured in the Passpoint profile of devices. Only when there is a match of RCOIs between Wi-Fi infrastructure and Emergency 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 911-only service.

#### 5.1.7.3 Framework Requirements

A legal framework whereby responsibility and terms under which local Wi-Fi networks participate in authenticating devices with Emergency Passpoint profiles is required. These legal agreements need to include terms that cover operation of the 911 service and allow provisions to indemnify local Wi-Fi network and network providers against any liabilities resulting from 911 call failures. A regulatory rulemaking may be required to provide terms and conditions associated with the use of the Emergency Passpoint profile and a mandate to install the Emergency Passpoint profiles in devices.

#### 5.1.7.4 Authentication With The Emergency RCOI

The requirements include being able to support emergency calls for users without valid credentials for any of the local Wi-Fi networks. 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 Extensible Authentication Protocol (EAP) method is not widely supported. Instead, this use-case could leverage the well supported EAP-TTLS method with a common set of credentials used by all users wanting to initiate emergency communications using the emergency-RCOI.

#### 5.1.7.5 Access Point Location

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. It is proposed to re-use the RFC-5580 definition for location in RADIUS signaling to IDP, enabling the access point to provide the location of the device or of the access point to the IDP for Connectivity Location Function (CLF) population.

#### 5.1.7.6 Emergency CSCF Operation For End-Users Using Proposed Emergency Communications Credentials

Whereas 3GPP defines the E-CSCF as always operating in the access network, in this use case the E-CSCF could be a common function leveraged by all participating local Wi-Fi networks that have configured the emergency RCOI realm. 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 existing technical frameworks could be leveraged that define the use of IETF specifications for signaling of civic and geo-spatial location in the RADIUS exchange. Unlike in cellular networks, users on WLAN systems may frequently be allocated private IP addresses. This IP address information can be included in the RADIUS exchange, 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 proposed Secure Location Tag (SLT) which the WLAN system could deliver to the user's device. The BSSID and/or the SLT will be included in the P-Access Network Information (P-ANI) SIP header sent by the device as well as being included in the RADIUS signaling. The E-CSCF may query the IDP for the local Wi-Fi network location.

#### 5.1.7.7 Threat Analysis

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.

### 5.1.8 Network Selection, Prioritization, and Fallback

In some scenarios, there may be several alternative access types and alternative procedures allowing a 911 call to be established. When this happens, only one of the Use Cases above will normally be applicable via an implicit prioritization defined by their assumptions. However, should the 911 call attempt fail using the highest priority alternative, then a UE is expected to attempt the 911 call using other available alternatives. This means that Use Cases above may be invoked when not all of their assumptions apply.

Standards bodies have defined fallback chains for some Use Cases, and new Use Cases can be considered by Standards bodies in the future. In those fallback chains, a 911 call over Wi-Fi must be included if Wi-Fi access is available to a UE according to the Use Cases defined above.

## 5.2 Findings

### 5.2.1 Findings related to Cellular Enabled Devices

Cellular enabled devices with Wi-Fi calling enabled can generally place 911 calls over Wi-Fi successfully. Recent advances in Location Based technologies have improved the usefulness of Wi-Fi calls over Wi-Fi by increasing the confidence that a device can be successfully located and the call routed toward the appropriate PSAP.

### 5.2.2 Findings related to Wi-Fi Calling Configuration

Cellular enabled devices without Wi-Fi Calling enabled present an opportunity for improvement over the status quo. Improvements in this area are less dependent upon the development of new standards and more dependent on feature activation decisions within the industry.

### 5.2.3 Findings related to Non-Cellular Enabled Devices

The potential public safety benefits of expanding 911 access from non-cellular enabled devices were not significant enough to outweigh the apparent risks and technical challenges of expanding access from such devices. Therefore, this subject was viewed as a lower priority that could be considered at a future date.

### 5.2.4 Findings related to Wi-Fi Activation on Devices

Devices that support Wi-Fi Calling, but have Wi-Fi access disabled, may present an opportunity for improvement over the status quo. Improvements in this area may depend upon analysis of the relative value of overriding a user's choice to deactivate Wi-Fi or enter Airplane mode to enable an emergency call to be placed over Wi-Fi versus allowing the emergency call to fail.

### 5.2.5 Findings related to Wi-Fi Access by Devices making Emergency Calls

Several possible options were found that could improve Wi-Fi access for devices seeking to make an emergency call without cellular RAN access. Improvements in this area require additional analysis due to the intersection of legal and regulatory considerations.

### 5.2.6 Findings related to Roaming Devices

Devices that are roaming away from their established cellular networks present opportunities for improvement. Improving the treatment of international visitors roaming was particularly identified as presenting an opportunity for improvement as 3G networks are disabled in most parts of the U.S. Improvements in this area require additional analysis due to the intersection of legal and regulatory considerations.

### 5.2.7 Findings related to Handling of Text Emergency Calls With Wi-Fi Calling

Emergency text methods supported by wireless operators include SMS to 911, MMS text to 911, and RTT. All of these methods are supported over Wi-Fi calling, and the Use Cases described in this Report apply to voice emergency calls as well as to these emergency text methods. The IP-based connection afforded by Wi-Fi calling facilitates the conveyance of location data used for both routing and dispatch purposes for emergency texting using Wi-Fi calling.

## 5.3 Recommendations

### 5.3.1 The following CSRIC Recommendations are Intended for the Commission:

- CSRIC VIII expended significant time attempting to identify the current state of 911 over Wi-Fi capabilities. Maintaining accurate information about the current capabilities will be important for all stakeholders. Thus, the Commission should gather and maintain accurate information about device and network settings related to 911 over Wi-Fi and ensure this information is available to consumers. This information might include a description of the conditions in which a 911 call over Wi-Fi will be supported, addressing the comprehensive set of capabilities and conditions explored in this Report: activation of Wi-Fi calling; authentication; service continuity; prioritization and routing; accuracy of caller location information; etc.
- The Commission should evaluate the applicability of rules for various 911 over Wi-Fi use cases. To encourage the development of technologies and standards identified in this Report, the Commission could consider the need to clarify that entities will not incur new obligations as a function of developing technologies and standards that enable 911 service over Wi-Fi. The Commission could also consider the need for clarification of which entities have obligations to

provide 911 service and other obligations such as geolocation and accuracy requirements, when appropriate technologies and standards have been developed and matured.

- The FCC should consult with the Federal Aviation Administration, airlines, Commercial Mobile Radio Service (CMRS) providers, and other stakeholders to consider the need for rules or standards to govern if/when calls/texts to 911 via airplane Wi-Fi should be permitted.
- The FCC should direct a future CSRIC working group to assess the ability for 911 service over Wi-Fi and EPCS NS/EP priority access to coexist and determine if it is necessary to provide more specific recommendations prior to ubiquitous deployment of EPCS.
- CSRIC encourages the FCC to consider opening a proceeding on automatic (phone) device support for Wi-Fi calling for emergency calls when it has not been enabled on the device and cellular service is not available, considering all challenges with respect to routing, caller location, and callback. The length of time that Wi-Fi calling should remain active should be analyzed and recommended as an industry standard.
- If an MNO is not available to allow access to emergency services, the FCC should investigate methods to access emergency services to be designated to handle Wi-Fi-enabled 911 calls, along with an IDP function for a new interconnecting network realm dedicated to connecting emergency services from the Internet to emergency services networks.
  Note: To support this new service, consumer devices would need to be configured by OEMs or through established provisioning with a new Passpoint profile, including the emergency RCOI (911 RCOI) and a common identity.
- The FCC should consider repealing the requirement to collect Registered Location information for non-fixed interconnected VoIP services at service initialization given the advancements in location determination, and to allow for the automatic enabling of Wi-Fi calling.
- The FCC should consider the need for clarifying the rules to ensure the use of location-based routing and delivery of the best-available location information for 911 calls over Wi-Fi.
- To address roaming issues the FCC should:
  - Determine the current state of VoLTE and VoNR interoperability for emergency calling purposes for devices that are operated in the United States, where feasible;
  - Explore methods to improve access to domestic emergency services for foreign visitors;
  - Determine the feasibility of Wi-Fi calling origination, particularly and specifically in the case of an international visitor's device originating a call over a Wi-Fi connection; and
  - Collaborate with international bodies to harmonize any such rules as described above.

### 5.3.2 The following CSRIC Recommendations are Intended for Other than the FCC:

- It is recommended that service providers, Public Safety professionals, and other 911 stakeholders participate in the development of standards-based location spoofing mitigation solutions that will support PSAPs/ECCs in assessing, in real-time, the legitimacy of location information associated with 911 calls, including 911 calls originated over Wi-Fi.
- It is recommended that service providers, Public Safety professionals, and other 911 stakeholders participate in the development of a standards-based solution that will convey a Class of Service (COS) or other designation for 911 calls that originate over Wi-Fi to PSAPs/ECCs.
- Concerning Service Continuity:
  Given the public safety benefits of maintaining a 911 call when a caller moves outside of the serving area of the cell or Wi-Fi access point to which the call is initially connected, CSRIC VIII recommends the following:

  - Industry bodies and individual companies should continue developing and implementing methods for seamless mobility between APs and between APs and cellular networks.
  - Further consideration, including the need for industry standards, should be given by device manufacturers (OEMs) regarding policies and methods for turning on device Wi-Fi and turning off Airplane Mode when a 911 call is made.
- The working group encourages appropriate standards bodies to conduct continued performance modeling and studies to ensure that any future 911 service identification over Wi-Fi and forthcoming EPCS NS/EP priority access can coexist with minimal effect on either service.
- Industry bodies should establish standards and best practices for location-based routing and the provision of location information to complement the current regulatory framework including those for non-fixed VoIP services.
- If emergency Passpoint profile access to APs (enterprise, residential, public access point) is supported, then AP vendors should support an opt-in capability for such emergency access to the AP, provided that appropriate assurance is made that access is limited to emergency calling.

# 6 Conclusions

In conclusion, CSRIC VIII produced a report that explores the opportunity to leverage the ubiquitous nature of Wi-Fi access points to support 911 connectivity options available to consumers. This report represents the most comprehensive public documentation to date of the existing capabilities and limitations of 911 service over Wi-Fi, and it analyzes the public safety benefits, technical feasibility, and potential costs associated with improving access to 911 with Wi-Fi access points. CSRIC VIII looks forward to the Commission and other entities acting upon the recommendations detailed in this report to expand 911 service over Wi-Fi with appropriate consideration of security challenges, technical feasibility, and public safety needs.

# 7 Appendix A – Glossary

| Term | Description |
|---|---|
| 3GPP GSM | GSM (Global Standard for Mobile Communications) is an international standard digital radio interface utilized by some North American wireless carriers. |
| 3GPP UMTS | UMTS (Universal Mobile Telecommunications System) is a third-generation mobile cellular system for networks based on the GSM standard. |
| 3GPP2 CDMA 2000 | CDMA2000 (also known as C2K or IMT Multi-Carrier (IMT-MC)) is a family of 3G mobile technology standards for sending voice, data, and signaling data between mobile phones and cell sites. |
| A-GNSS | Assisted-Global Navigation Satellite System |
| ALI | Automatic Location Identification is the automatic display at the PSAP of the caller's telephone number, the address/location of the telephone and supplementary emergency services information of the location from which a call originates. |
| ANI or pANI | Automatic Number Identification is the telephone number associated with the call origination, originally associated with the access line of the caller. |
| pANI | Pseudo Automatic Number Identification), Routing Number<br>A telephone number used to support routing of wireless 911 calls. It may identify a wireless cell, cell sector or PSAP to which the call should be routed. |
| ANP | An Access Network Provider is an entity providing internet connectivity services. |
| AP | An Access Point is an entity that contains one station (STA) and provides access to the distribution system services, via the wireless medium (WM) for associated STAs. An AP comprises a STA and a distribution system access function (DSAF). |
| ATIS | The Alliance for Telecommunications Solutions is a U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. |
| BSSID | Basic Service Set Identifier, where a BSS is a set of stations (STAs) that have successfully synchronized. |
| CLF | The Connectivity Location Function maintains mappings between the endpoints' 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. |
| CSRIC | Communications Security, Reliability, And Interoperability Council is an advisory body of the FCC, formerly known as NRIC (Network Reliability and Interoperability Council), which provides recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety. |

| Term | Description |
|---|---|
| DBH | Device-based hybrid is a location technology that uses a mix of location methods available to the device including crowd-sourced Wi-Fi, Assisted Global Navigation Satellite System (A-GNSS), and handset-based sensors. It also includes an associated uncertainty estimate reflective of the quality of the returned location. [24] |
| ECC | **Emergency Communications Center**<br>A facility that—<br>(I) is designated to receive a 9–1–1 request for emergency assistance; and<br>(II) performs one or more of the functions described below; or a Public Safety Answering Point, as defined in section 222 of the Communications Act of 1934 (47 U.S.C. 222).<br>FUNCTIONS DESCRIBED<br>(i) Processing and analyzing 9–1–1 requests for emergency assistance and information and data related to such requests.<br>(ii) Dispatching appropriate emergency response providers.<br>(iii) Transferring or exchanging 9–1–1 requests for emergency assistance and information and data related to such requests with one or more other emergency communications centers and emergency response providers.<br>(iv) Analyzing any communications received from emergency response providers.<br>(v) Supporting incident command functions. |
| ECRF | Emergency Call Routing Function is a functional element in NGCS (Next Generation Core Services) which is a LoST (Location-to-Service Translation) protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller's location or towards a responder agency. |
| E-CSCF | An Emergency Call Session Control Function takes the requests from P-CSCF (Proxy CSCF) and routes the emergency sessions to the PSAP based on CLF and RDF queries. |
| EDCA | Enhanced Distributed Channel Access is the prioritized carrier sense multiple access with collision avoidance (CSMA/CA) access mechanism used by quality-of-service (QoS) stations (STAs) in a QoS basic service set (BSS) and STAs operating outside the context of a BSS. This access mechanism is also used by the QoS access point (AP) and operates concurrently with hybrid coordination function (HCF) controlled channel access (HCCA). |

[24] © Alliance for Telecommunications Industry Solutions. This document may be obtained from the ATIS website at: Glossary – ATIS Telecom Glossary.

| Term | Description |
|---|---|
| ESInet | An Emergency Services IP Network is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG911 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks). The term ESInet designates the network, not the services that ride on the network.<br>https://nenawiki.org/wiki/Main_Page |
| ePDG | Evolved Packet Data Gateway |
| ESN | An Emergency Service Number is a 3-5 digit number that represents one or more ESZs (Emergency Service Zone), stored as a 3-5 character numeric string in a GIS database. |
| ESRK | An Emergency Services Routing Key is a 10-digit North American Numbering Plan number that uniquely identifies a wireless emergency call, is used to route the call through the network, and used to retrieve the associated ALI data. |
| FCC | Federal Communications Commission (aka: the Commission) |
| GPS | The Global Positioning System is a space-based navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. |
| HELD | HTTP Enabled Location Delivery is a protocol that can be used to acquire Location Information (LI) from a LIS (Location Information Server) within an access network as defined in IETF RFC 5985. |
| HELO | Hybridized Emergency Location |
| IDP | Identity Provider is an entity that manages identity credentials and policies for devices and provides authentications services. |
| IETF | The Internet Engineering Task Force is the lead standard-setting authority for Internet protocols. |
| IMS | The IP Multimedia Subsystem is a reference architecture defined by 3GPP that comprises all 3GPP/3GPP2 core network elements providing IP multimedia services that support audio, video, text, pictures alone or in combination, delivered over a packet switched domain. |
| LAN | A Local Area Network is a transmission network encompassing a limited area, such as a single building or several buildings in close proximity. |
| LNG | A Legacy Network Gateway is an NG911 Functional Element that provides an interface between a non-IP originating network and a Next Generation Core Services (NGCS) enabled network. |

| Term | Description |
|---|---|
| LPG | A Legacy PSAP Gateway is a signaling and media interconnection point between an ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and NG911 PSAPs. The Legacy PSAP Gateway supports an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced MF interface (comparable to the interface between a traditional Selective Router and a legacy PSAP) on the other. |
| LRF | The Location Retrieval Function is the IMS-associated functional entity that handles the retrieval of location information for the emergency caller including, where required, interim location information, initial location information and updated location information. |
| LS | A Location Server is General term for the entity responsible for obtaining the location of the User Equipment (UE). See 3GPP TS 23.167 |
| LSRG | The Legacy Selective Router Gateway provides an interface between a 911 Selective Router and an ESInet, enabling calls to be routed and/or transferred between Legacy and NG networks. |
| MAC Address | Media/Medium Access Control Address provides an identifier associated with a device that is commonly used for addressing. |
| MDN | A Mobile Directory Number is the telephone number dialed to reach a wireless telephone. |
| MGCF | The Media Gateway Control Function is an IMS element that facilitates call control, interfacing the Packet Switched domain to the Circuit Switched domain, when interworking between the IMS and PSTN is required. |
| MMES | Multimedia Emergency Services |
| MMS | Multimedia Services is a standard way to send messages that extends the core SMS (Short Message Service) capability to include multimedia content to and from a mobile phone over a cellular network. |
| MMSC | Multimedia Message Service Center |
| MMS-IWF | Multimedia Services-Interworking |
| MPC/GMLC | The Mobile Positioning Center (MPC)/Gateway Mobile Location Center (GMLC) is a Functional Entity that provides an interface between the wireless originating network and the Emergency Services Network. The MPC/GMLC retrieves, forwards, stores and controls position data within the location services network. |
| MSC | A Mobile Switching Center is the wireless equivalent of a Central Office, which provides switching functions for wireless calls. |
| NANP | The North American Numbering Plan is an integrated telephone numbering plan serving 20 North American countries that share its resources and are in the +1 country code. NANP numbers are ten-digit numbers consisting of a three-digit Numbering Plan Area (NPA) code, commonly called an area code, followed by a seven-digit local number. The format is usually represented as NXX-NXX-XXXX where N is any digit from 2 through 9 and X is any digit from 0 through 9. |

| Term | Description |
|---|---|
| NENA (The 911 Association) | NENA serves the public safety community as the only professional organization solely focused on 911 policy, technology, operations, and education issues. With more than 12,000 members in 48 chapters across North America and around the globe, NENA promotes the implementation and awareness of 911 and international three-digit emergency communications systems. See http://www.nena.org/page/aboutfaq2017 for more details. |
| NPA | Numbering Plan Area is encoded numerically with a three-digit telephone number prefix, commonly called the area code. |
| NPD | Numbering Plan Digit is a component of the traditional 8-digit 911 signaling protocol between the Enhanced 911 Control Office and the PSAP CPE. Identifies 1 of 4 possible area codes. |
| NSI | Non-Service Initialized refers to a mobile device for which there is no valid service contract with any CMRS provider. As such, NSI devices have no associated subscriber name and address, do not provide a call-back number, and may not provide location. |
| OTT | Over The Top (signaling) is a technology that bypasses traditional network distribution approaches and runs over, or on top of, core Internet networks. |
| 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. A Passpoint Profile includes the user's credentials and the access network identifiers. |
| P-CSCF | Proxy Call Session Control Function |
| PLMN | Public Land Mobile Network is a network that is established and operated by an administration or by a recognized operating agency (ROA) for the specific purpose of providing land mobile telecommunications services to the public. *Note:* A PLMN may be considered as an extension of a fixed network, *e.g.,* the Public Switched Telephone Network (PSTN) or as an integral part of the PSTN. 24 |
| PSAP/ECC (Public Safety Answering Point) | **PSAP (Public Safety Answering Point)**<br>As defined in 47 USC 222, "Public safety answering point or PSAP":<br><br>A facility that has been designated to receive emergency calls and route them to emergency service personnel. |
| PSTN | The Public Switched Telephone Network is the network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America. |
| RDF | The Routing Determination Function resolves a physical location, either a civic address or a geo-spatial address to the serving PSAP. |
| RADIUS | Remote Authentication Dial-In User Service |
| RCOI | A Roaming Consortium Organization Identifier 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. |
| RTT | Real Time Text is a text transmission that is character at a time, as in TTY. Technology that allows consumers to send and receive Internet Engineering Task Force (IETF) RFC 4103 text characters, as they are typed, as well as audio simultaneously. |

| Term | Description |
|---|---|
| SHAKEN | Signature-based Handling of Asserted information using toKENs (SHAKEN) is an industry framework for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an Internet Protocol (IP)-based service provider voice network. |
| SIM/USIM | Subscriber Identity Module/Universal Subscriber Identity Module |
| SIP | Session Initiation Protocol is a protocol specified by the IETF (RFC 3261) that defines a method for establishing multimedia sessions over the Internet. |
| SLT | Secure Location Tag |
| SMSC | Short Message Service Center |
| SR | The Selective Router is the Central Office that provides the tandem switching of 911 calls. It controls delivery of the voice call with ANI to the PSAP and provides Selective Routing, Speed Calling, Selective Transfer, Fixed Transfer, and certain maintenance functions for each PSAP. |
| SRDB | A Selective Routing Database is the routing table that contains telephone number to ESN relationships which determines the routing of 911 calls. |
| SS7 | Signaling System 7 is an out-of-band signaling system used to provide basic routing information, call set-up and other call termination functions. Signaling is removed from the voice channel itself and put on a separate data network. |
| SWAT | Special Weapons And Tactics |
| TCC | Text Control Center |
| TTY | A Teletypewriter is a device or application used to send or receive character by character communication using Baudot signaling. |
| UE | User Equipment |
| URI | A Uniform Resource Identifier is an identifier consisting of a sequence of characters matching the syntax rule that is named <URI> in RFC 3986. It enables uniform identification of resources via a set of naming schemes. |
| URN | A Uniform Resource Name is a type of URI. The URNs are intended to serve as persistent, location-independent, resource identifiers and are designed to make it easy to map other namespaces (which share the properties of URNs) into URN-space.<br>An example of a URN is urn:service:sos. |
| VoLTE | Voice over LTE (Long Term Evolution) |
| VoNR | Voice over New Radio |
| WAN | A Wide Area Network is a computer network that spans a relatively large geographical area and consists of two or more interconnected local area networks (LANs). |
| WLAN | Wireless Local Area Network comprises the portion of a Local Area Network (see above) that is provided over a wireless medium. |

# 8 Appendix B – High-Level Call Flows

This appendix provides example call flows illustrating different call scenarios. The first call flow

example assumes that an emergency call is originated using a smartphone that has Wi-Fi Calling enabled in an area where both Wi-Fi coverage and cellular coverage are available. This call flow describes a typical scenario where even though Wi-Fi access is available and Wi-Fi calling is enabled on the device, an emergency call is routed via a cellular network because the cellular RAN and core networks are available. This call flow assumes that the originating network is an IMS network and that the call is routed via an i3 ESInet to an i3 PSAP/ECC.

The second call flow example illustrates a scenario where an emergency call is originated by a device that has Wi-Fi Calling enabled, and has successfully associated with a Wi-Fi network. The device establishes a secure tunnel to an Evolved Packet Data Gateway (ePDG) and routes the Wi-Fi emergency call via the ePDG and a Packet Data Network Gateway (PGW) to a local IMS core network. The local IMS core network uses location information provided by the device to route the emergency call to an NG911 Emergency Services Network, which subsequently routes the call to an i3 PSAP/ECC.

The third call flow example assumes an emergency call handling architecture that is based on RFC 6443. The IETF emergency call architecture prefers that endpoints learn their location and supply it when establishing an emergency call. In this call flow example, the device interacts with a Location Information Server (LIS) to obtain its location. RFC 6443 specifies that location should be obtained at the time an emergency call is detected, but suggests that mobile devices determine location at network attachment time and periodically thereafter as a backup in case location determination at the time of the call does not work. In this call flow example, the device also interacts with a LoST server to obtain routing information for the emergency call. RFC 6443 specifies that a device may interact with a LoST server prior to an emergency call being originated to obtain the local emergency dial string(s) and a "PSAP/ECC URI" that it can cache for use if the LoST query fails during an emergency call. Consistent with RFC 6443, this call flow example assumes that the call is routed via a proxy in an originating network to an ESRP in an i3 ESInet. As in the first call flow example, the ESRP also interacts with a LoST server, referred to as an ECRF, using the routing location provided with the call. The ESRP also applies whatever policy routing is appropriate and delivers the call to the i3 PSAP/ECC with location and callback information. While consistent with IETF RFCs, this call flow example is not widely implemented; mobile devices typically do not support interactions with LISs or LoST servers.

The fourth call flow example is a variation on the second call flow example where the device determines its own location without interacting with a LIS, and upon detecting a request for an emergency call, includes its location and an appropriate service URN in outgoing signaling to a Call Server/proxy in an originating network. In this call flow example, the Call Server/proxy uses the location received in incoming SIP signaling from the device to interact with a LoST server/ECRF to obtain routing information associated with an ESRP in an i3 ESInet. The ESRP then processes the emergency call in the same way as in the previous call flow examples and delivers the emergency call with location and callback information to an i3 PSAP/ECC. While this call flow does not require the device to interact with a LIS or LoST server, the routing of emergency calls to VoIP Service Provider networks is not typical of arrangements supported by some mobile devices today. In the more typical architecture, mobile devices route emergency calls via cellular carrier networks.

## 8.1 911 Origination - Cellular Network Available - Using IMS Originating Network

A person enters a building where both cellular coverage (i.e., both the cellular RAN and core network) and good Wi-Fi coverage is available. He is carrying a smartphone that knows its location and that has Wi-Fi Calling enabled. A situation occurs that requires him to call 911 to request emergency assistance.

The call flow illustrated in Figure 4 shows one example of how a standard NG911 architecture may be used to support this Use Case. Specifically, this call flow assumes that the 911 call is processed by an IMS originating network. It further assumes that location information is delivered by-value by the device to the Proxy Call Session Control Function (P-CSCF) in the IMS originating network in the SIP INVITE associated with the emergency origination. The P-CSCF passes the SIP INVITE message to the

Emergency Call Session Control Function (E-CSCF) which forwards it to the Location Retrieval Function (LRF). The LRF interacts with a Location Server (LS) to obtain initial (Phase I) location information and to trigger (Phase II) position determination. The LRF interacts with a Routing Determination Function (RDF) to determine how to route the emergency call. Location-based routing performed by the RDF determines that the emergency call is to be routed via an Emergency Service Routing Proxy (ESRP) in an i3 Emergency Services IP Network (ESInet). The LRF generates a location-by-reference and may contain both the device-provided location-by-value and a location-by-reference, along with the routing information, in the 300 Multiple Choices message returned to the E-CSCF. The E-CSCF passes the SIP INVITE to the exit Interconnection Border Control Function (IBCF). The exit IBCF in the IMS originating network forwards the SIP INVITE message via an ingress Border Control Function (BCF) to an ESRP in the i3 ESInet. Call processing continues with the ESRP interacting with an Emergency Call Routing Function (ECRF), where location-based routing is performed. The ESRP will also apply policy-based routing to the emergency call, as appropriate. The ESRP determines the target Public Safety Answering Point (PSAP/ECC) or an Emergency Communications Center (ECC) for the emergency call and forwards the SIP INVITE message with the caller identity (callback number) as well as location information to that PSAP/ECC.

Note that the call flow illustrated in Figure 4 does not include procedures related to SHAKEN caller identity authentication/verification, RPH signing/verification or consistency checking of device-provided location information.

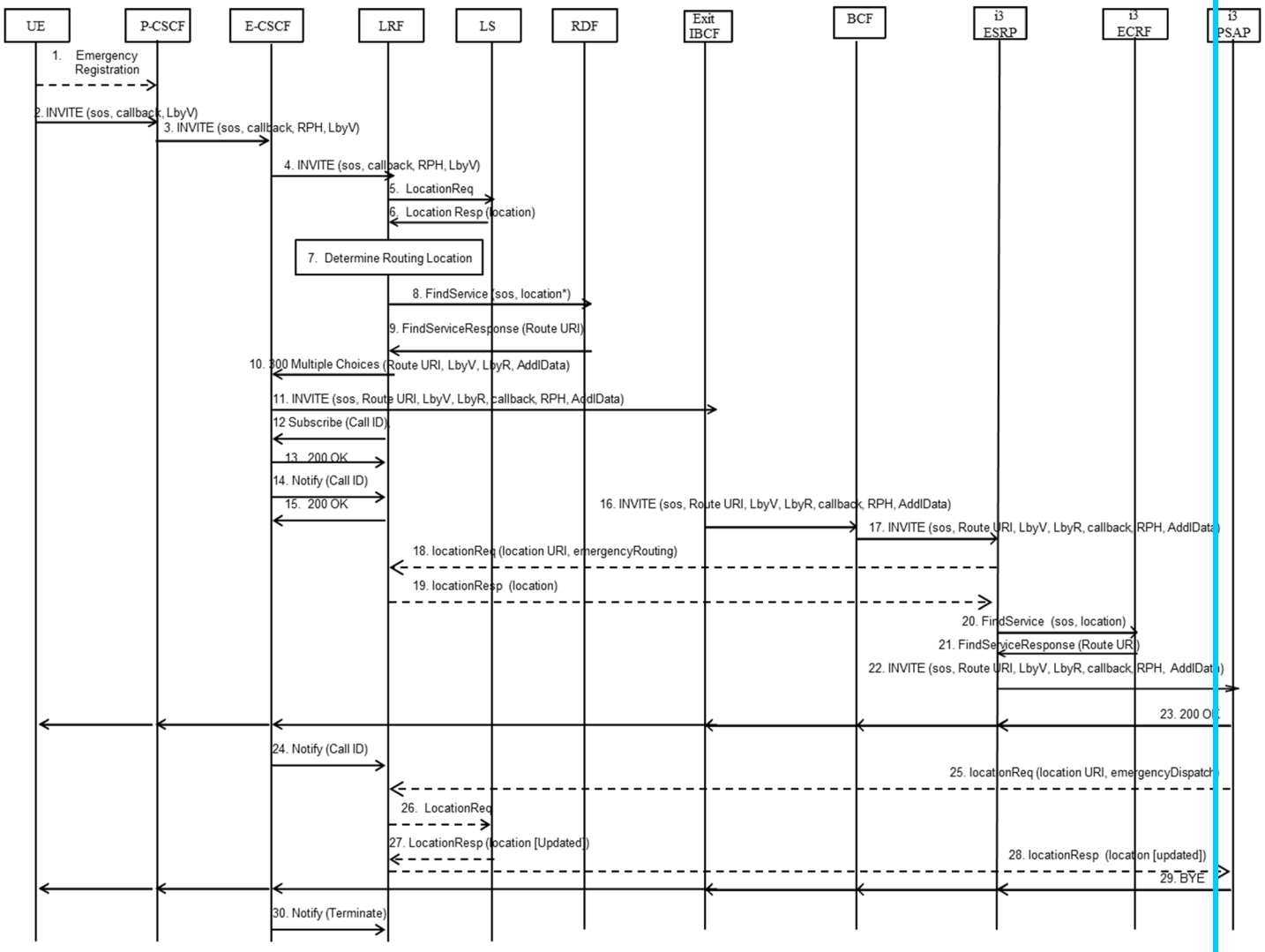


**Figure 4: 911 Origination - Cellular Network Available - IMS Originating Network**

**Step 1.** (Conditional) Emergency registration occurs (if not already emergency registered and the UE has credentials).

**Step 2.** The originating SIP UE (i.e., the smartphone), which is authenticated to the P-CSCF, creates a SIP INVITE that includes a callback number (i.e., a telephone number identity), an sos service URN in the Request URI, and location information in the form of a Presence Information Data Format Location Object (PIDF-LO) in the body of the message (i.e., location-by-value).

**Step 3.** The P-CSCF in the originating network adds a P-Asserted-Identity header field asserting the callback number/caller identity of the originating SIP UE and a Resource-Priority Header (RPH) with a value of "esnet.1" to the SIP INVITE. The P-CSCF passes the SIP INVITE to the E-CSCF.

**Step 4.** The E-CSCF passes the SIP INVITE message to the LRF to obtain location and routing information for the emergency call.

**Step 5.** The LRF interacts with an LS to acquire initial (Phase I) location and to initiate position determination.

**Step 6.** The LS responds with the initial location information.

**Step 7.** The LRF determines the routing location for the call. Whether the LRF uses the device-based location or an "Associated Location" as input to the routing process is left to local policy. [25]

**Step 8.** The LRF queries the RDF using the routing location. (Based on ATIS-0700015, the LRF will use the Location to Service Translation (LoST) protocol (as defined in RFC 5222) to query the RDF. The RDF will determine routing based on the routing location and an 'sos' service URN).

**Step 9.** The RDF returns a Route URI. In this example, the Route URI is associated with an ESRP in an i3 ESInet.

**Step 10.** The LRF redirects the call back to the E-CSCF by returning a 300 Multiple Choices message that may contain the location-by-value received from the device, as well as a location URI that it created, a Route URI that directs the call toward the i3 ESInet, and Additional Data.

**Step 11.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information it received in the initial SIP INVITE message, and forwards it to the exit IBCF. In this example the SIP INVITE includes the sos service URN, a Route URI, location-by-value[26], location-by-reference, the callback number, the RPH, and Additional Data.

[25] For emergency calls originated by mobile devices, ATIS-0700015 defines an "Associated Location" as a location (civic, geodetic, or polygon) within the designated PSAP/ECC jurisdiction that may be used to route the call toward the designated PSAP/ECC. An LRF determines an Associated Location by mapping a cell ID to a routing location that is associated with the PSAP/ECC which, based on pre-existing agreements, is supposed to receive the call.

[26] Feedback from Public Safety received as part of recent activity in ATIS and NENA related to location spoofing mitigation has indicated a desire to receive device-based location-by-value only if an indication that a consistency check was performed and an indication of the results of that check are also provided.

**Step 12.** The LRF sends a SIP SUBSCRIBE to the E-CSCF to be informed of call state. (Alternatively, the Subscriptions may be done at the system start-up and be applicable to all calls [not shown].)

**Step 13.** The E-CSCF responds to the SUBSCRIBE request with a 200 OK message.

**Step 14.** The E-CSCF sends the initial state NOTIFY message to the LRF.

**Step 15.** The LRF responds to the NOTIFY message by returning a 200 OK message to the E-CSCF.

**Step 16.** The exit IBCF routes the SIP INVITE over the NNI to a BCF on the ingress side of the i3 ESInet using standard inter-domain routing resolution.

**Step 17.** The ingress BCF forwards the SIP INVITE to the ESRP.

**Step 18.** Since, in this example, both location-by-value and location-by-reference are provided in the SIP INVITE associated with the emergency call, the ESRP will determine which location to use for routing based on policy.[27] If the ESRP determines that the location-by-reference is to be used, it will query the LRF (as identified in the location URI) for routing location. (This call flow illustrates the use of HELD as a location de-reference protocol. The value of the responseTime parameter in the HELD locationRequest message is set to "emergencyRouting".)

**Step 19.** (Conditional on Step 18) The LRF supplies routing location to the ESRP.

**Step 20.** The ESRP queries the ECRF using the LoST protocol, including the routing location and an 'sos" service URN in the query message.

**Step 21.** The ECRF performs location-based routing and replies to the ESRP with a Route URI (i.e., PSAP/ECC URI).

**Step 22.** The ESRP applies policy-based routing, as applicable, and passes the SIP INVITE message to the i3 PSAP/ECC. In this example the SIP INVITE includes the sos service URN, a Route URI (associated with the i3 PSAP/ECC), location-by-value, location-by reference, the callback number, the RPH, and Additional Data.

**Step 23.** The PSAP/ECC indicates the call has been answered by returning a SIP 200 OK to the ESRP. The 200 OK gets propagated back to the UE.

**Step 24.** The E-CSCF sends a notification to the LRF updating the call state.

**Step 25.** (Optional) The PSAP/ECC queries the LRF (as identified in the location URI) for updated location information (responseTime parameter="emergencyDispatch" in this example). (Note that Steps 25-28 can occur prior to Steps 23 and 24.)

**Step 26.** (Conditional on Step 25) The LRF queries the LS for updated location information. (Note that the value of the responseTime parameter [emergencyDispatch or a specific time value] will be used by the LRF to determine whether to query the LS).

**Step 27.** (Conditional on Step 26) The LS returns updated UE location information to the LRF.

**Step 28.** (Conditional on Step 25) The LRF supplies updated UE location to the PSAP/ECC.

[27] Note that, following RFC 6442 which states that a SIP intermediary that adds a locationValue MUST position the new locationValue as the last locationValue within the Geolocation header field of the SIP request, Clause 3.2 of NENA-STA-010.3 advises that Originating Networks providing multiple locations in the original INVITE associated with an emergency call do so by making the top entry the preferred location to use for routing and putting the other location information after.

**Step 29.** When the PSAP/ECC determines that the call can be terminated, the PSAP/ECC sends a SIP BYE to the ESRP. The BYE message gets propagated back to the UE. (Note that the BYE may instead be initiated by the UE.)

**Step 30.** The E-CSCF sends a termination SIP NOTIFY to the LRF to allow it to release resources associated with the emergency call.

## 8.2 911 Origination - Wi-Fi Access - IMS Core Network Available and Used

A person enters a building where good Wi-Fi coverage is available. He is carrying a smartphone that knows its location, has Wi-Fi Calling enabled, and has successfully associated with a Wi-Fi network. A situation occurs that requires him to call 911 to request emergency assistance. An IMS core network is available to support emergency call routing to an NG911 Emergency Services Network. The device discovers the Evolved Packet Data Gateway (ePDG) node at the border of the IMS core network using a Domain Name System (DNS) lookup. The ePDG, acts like a gateway between the public internet and the rest of the operator's core network. The device sets up a secure (e.g., IPsec) tunnel to connect to the ePDG over a Wi-Fi/internet connection. The ePDG routes the emergency call to the local IMS network via the Packet Data Network Gateway (PGW).

The call flow illustrated in Figure 5 shows a SIP INVITE message associated with an emergency call being generated by the calling UE. The INVITE includes location information (i.e., a location-by-value). The INVITE is passed from the ePDG via the PGW to the Proxy Call Session Control Function (P-CSCF) in the IMS core network. The P-CSCF passes a SIP INVITE message that includes the location-by-value and a Resource-Priority Header (RPH) to the Emergency Call Session Control Function (E-CSCF) which forwards it to the Location Retrieval Function (LRF). The LRF interacts with a Routing Determination Function (RDF) to determine how to route the emergency call. Location-based routing performed by the RDF determines that the emergency call is to be routed via an Emergency Service Routing Proxy (ESRP) in an i3 Emergency Services IP Network (ESInet). The LRF returns a 300 Multiple Choices message to the E-CSCF that may contain the device-provided location-by-value and Additional Data (by value), along with the routing information. The E-CSCF passes the SIP INVITE to the exit Interconnection Border Control Function (IBCF). The exit IBCF in the IMS originating network forwards the SIP INVITE message via an ingress Border Control Function (BCF) to an ESRP in the i3 ESInet. Call processing continues with the ESRP using the received location-by-value to interact with an Emergency Call Routing Function (ECRF), where location-based routing is performed. The ESRP will also apply policy-based routing to the emergency call, as appropriate. The ESRP determines the target Public Safety Answering Point (PSAP/ECC) or an Emergency Communications Center (ECC)for the emergency call and forwards the SIP INVITE message with the caller identity (callback number) as well as the device-provided location-by-value to that PSAP/ECC.

Note that the call flow illustrated in Figure 5 does not include procedures related to SHAKEN caller identity authentication/verification, RPH signing/verification, or consistency checking of device-provided location information. It also does not illustrate a mechanism by which updated location can be acquired by the PSAP/ECC.

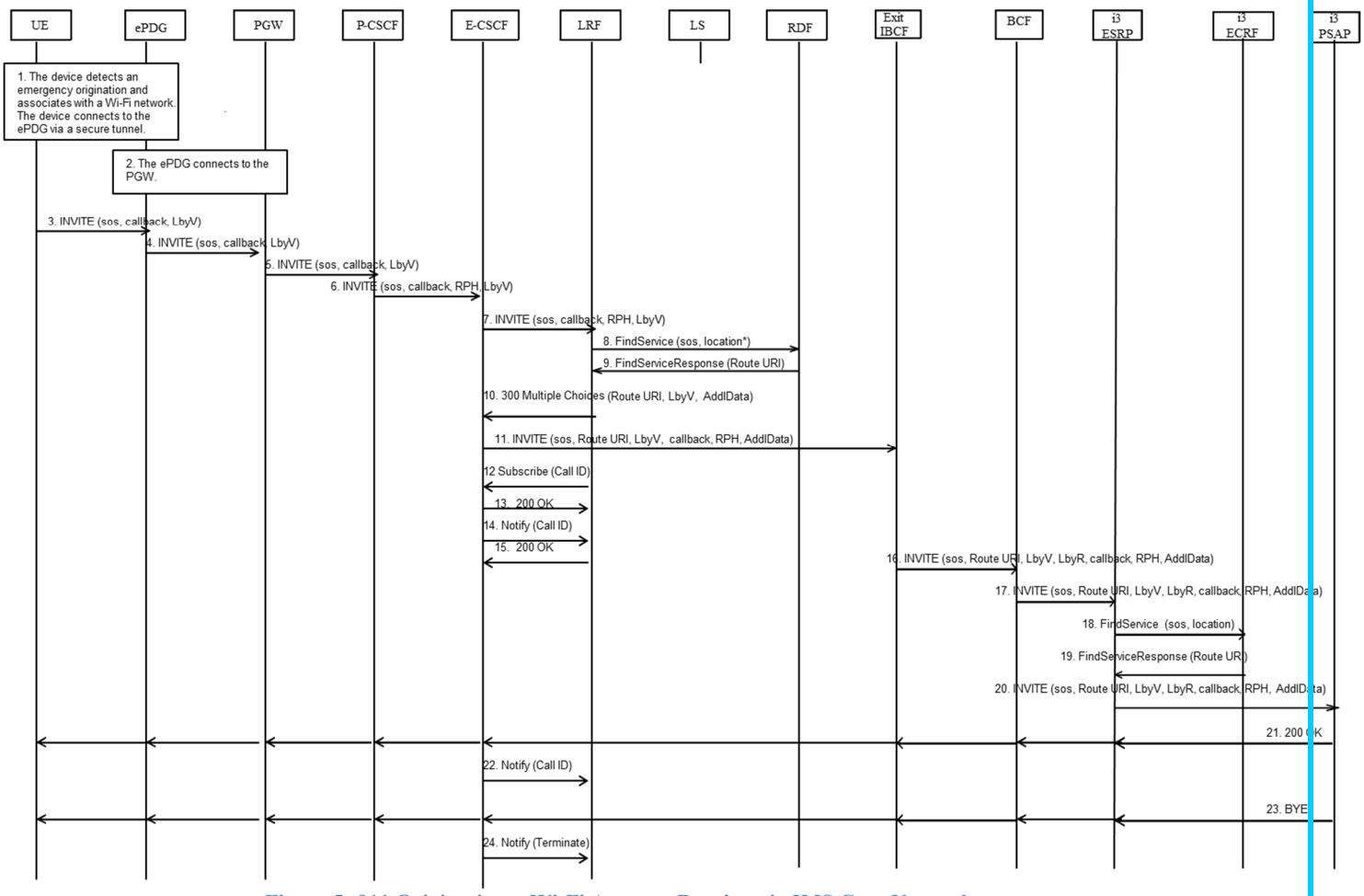



**Figure 5: 911 Origination - Wi-Fi Access - Routing via IMS Core Network**

**Step 1.** The device detects an emergency origination and associates with a Wi-Fi network. The device connects to the ePDG via a secure tunnel.

**Step 2.** The ePDG connects to the PGW through which the call-related signaling will be passed to the IMS core network.

**Step 3.** The originating SIP UE (i.e., the smartphone), which is authenticated to the P-CSCF, creates a SIP INVITE that includes a callback number (i.e., a telephone number identity), an sos service URN in the Request URI, and location information in the form of a Presence Information Data Format Location Object (PIDF-LO) in the body of the message (i.e., location-by-value). The UE passes the INVITE to the ePDG.

**Step 4.** The ePDG passes the SIP INVITE to the PGW.

**Step 5.** The PGW passes the SIP INVITE to the P-CSCF in the IMS core network.

**Step 6.** The P-CSCF in the core network adds a P-Asserted-Identity header field asserting the callback number/caller identity of the originating SIP UE and a Resource-Priority Header (RPH) with a value of "esnet.1" to the SIP INVITE. The P-CSCF passes the SIP INVITE to the E-CSCF.

**Step 7.** The E-CSCF passes the SIP INVITE message to the LRF to obtain location and routing information for the emergency call.

**Step 8.** The LRF queries the RDF using the device-provided location-by-value as the routing location. (Based on ATIS-0700015, the LRF will use the Location to Service Translation (LoST) protocol (as defined in RFC 5222) to query the RDF. The RDF will determine routing based on the routing location and an 'sos' service URN).

**Step 9.** The RDF returns a Route URI. In this example, the Route URI is associated with an ESRP in an i3 ESInet.

**Step 10.** The LRF redirects the call back to the E-CSCF by returning a 300 Multiple Choices message that contains the location-by-value received from the device, a Route URI that directs the call toward the i3 ESInet, and Additional Data (by value).

**Step 11.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information it received in the initial SIP INVITE message, and forwards it to the exit IBCF. In this example the SIP INVITE includes the sos service URN, a Route URI, location-by-value[28], the callback number, the RPH, and Additional Data.

**Step 12.** The LRF sends a SIP SUBSCRIBE to the E-CSCF to be informed of call state. (Alternatively, the Subscriptions may be done at the system start-up and be applicable to all calls [not shown].)

**Step 13.** The E-CSCF responds to the SUBSCRIBE request with a 200 OK message.

**Step 14.** The E-CSCF sends the initial state NOTIFY message to the LRF.

**Step 15.** The LRF responds to the NOTIFY message by returning a 200 OK message to the E-CSCF.

**Step 16.** The exit IBCF routes the SIP INVITE over the NNI to a BCF on the ingress side of the i3 ESInet using standard inter-domain routing resolution.

**Step 17.** The ingress BCF forwards the SIP INVITE to the ESRP.

**Step 18.** Since, in this example, only location-by-value is provided in the SIP INVITE associated with the emergency call, the ESRP will query the ECRF using the LoST protocol, including the location-by-value and an 'sos" service URN in the query message.

**Step 19.** The ECRF performs location-based routing and replies to the ESRP with a Route URI (i.e., PSAP/ECC URI).

**Step 20.** The ESRP applies policy-based routing, as applicable, and passes the SIP INVITE message to the i3 PSAP/ECC. In this example the SIP INVITE includes the sos service URN, a Route URI (associated with the i3 PSAP/ECC), location-by-value, location-by reference, the callback number, the RPH, and Additional Data.

**Step 21.** The PSAP/ECC indicates the call has been answered by returning a SIP 200 OK to the ESRP. The 200 OK gets propagated back to the UE.

**Step 22.** The E-CSCF sends a notification to the LRF updating the call state.

**Step 23.** When the PSAP/ECC determines that the call can be terminated, the PSAP/ECC sends a SIP BYE to the ESRP. The BYE message gets propagated back to the UE. (Note that the BYE may instead be initiated by the UE.)

[28] Feedback from Public Safety received as part of recent activity in ATIS and NENA related to location spoofing mitigation has indicated a desire to receive device-based location-by-value only if an indication that a consistency check was performed and an indication of the results of that check are also provided.

**Step 24.** The E-CSCF sends a termination SIP NOTIFY to the LRF to allow it to release resources associated with the emergency call.

## 8.3 911 Origination – IETF-based Solution

This call flow describes a scenario where the IETF solution (as summarized in clause 4.3.2) plays a role in routing a Wi-Fi emergency call. In this example, the emergency caller is not subscribed or does not have access to a CMRS network but does have a subscription with a VoIP Service Provider that supports the IETF solution.

The call flow provided in Figure 6 illustrates a scenario where an emergency call is delivered by a non-IMS VoIP Service Provider network to an i3 ESInet with location-by-value. This call flow assumes that, upon detecting an emergency origination, the calling device requests location by querying a Location Information Server (LIS) in the access network, using the HELD protocol. The HELD locationRequest contains an identifier associated with the calling device and appropriate credentials. It also contains an indication of the form that the provided location information should take. In this example call flow, the device requests a civic or geodetic location. The LIS responds with location information (i.e., location-by-value [LbyV]). The device uses the location information returned in the HELD locationResponse to query an Emergency Call Routing Function (ECRF) (or other LoST server) for routing information.[29] The ECRF returns a URI associated with an ESRP in an i3 ESInet. The device forwards the emergency session request to a Call Server/Proxy in its serving (non-IMS i3-compliant) originating VoIP network. The SIP INVITE message signaled by the device to the Call Server/Proxy includes a Route header that contains the URI of an ESRP in an i3 ESInet, an emergency services service URN (urn:service:sos) in the Request-URI, callback information in the From header, and a location-by-value in the message body. (A Geolocation header that contains a Content-ID [cid] pointing to the PIDF-LO in the message body, a Geolocation-Routing header set to “yes”, and other SIP headers will also be included in the SIP INVITE message, but are not specifically illustrated in Figure 6.) The Call Server/Proxy adds a P-Asserted-Identity header containing callback information, and Additional Data “by value” to the body of the SIP INVITE message, along with a Call-Info header that contains a cid pointing to the Additional Data in the message body, and forwards the SIP INVITE to a BCF on the ingress side of the i3 ESInet. The BCF adds a Resource-Priority Header set to “esnet.1” to the INVITE (if not already present) and forwards the SIP INVITE to the ESRP. The ESRP uses the location-by-value to query the i3 ECRF. In this example call flow, the Route URI that is returned by the ECRF is associated with an i3 PSAP/ECC. Figure 6 shows the emergency call then being delivered to the i3 PSAP/ECC with the same location-by-value as was received by the i3 ESInet in incoming signaling from the non-IMS originating network, as well as the Additional Data (by value).

[29] Based on RFC 6443, the endpoint can complete the LoST mapping from its location at boot time, and periodically thereafter. It should attempt to obtain a "fresh" location, and from that a current mapping when it places an emergency call.

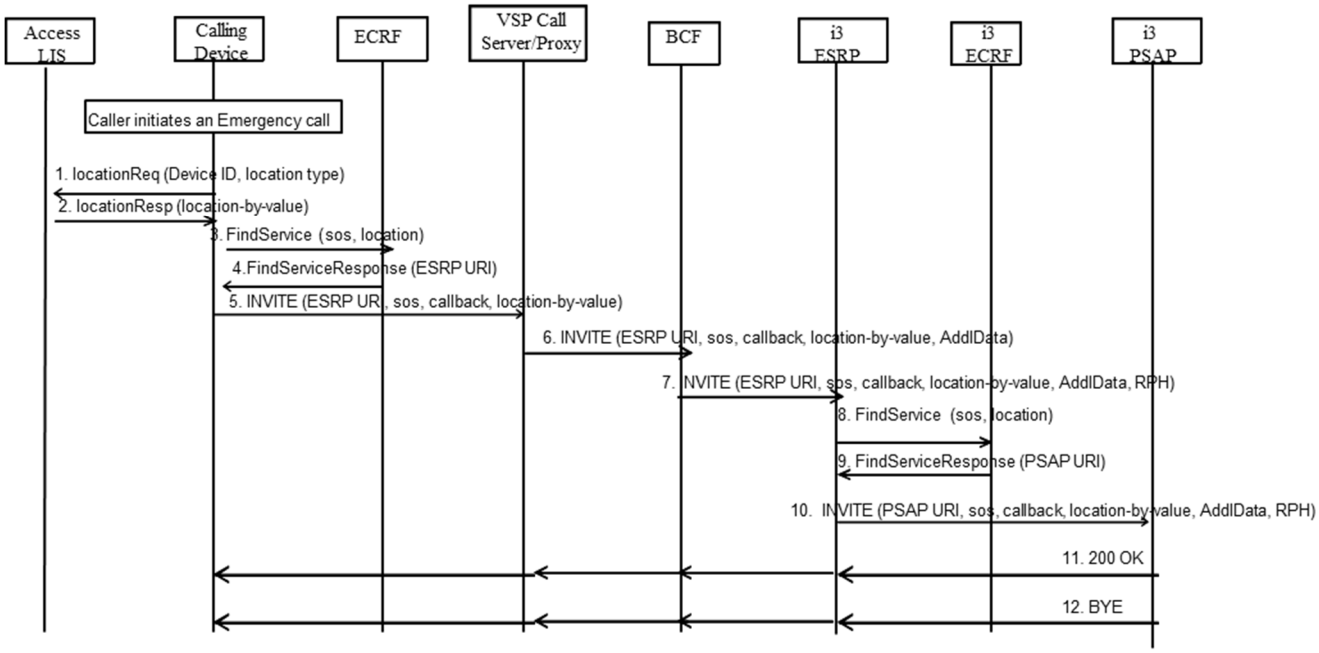



**Figure 6: 911 Origination - No Access to Cellular Network - IETF Solution**

**Step 1.** Upon recognizing a request for emergency service, the calling device requests location by querying the LIS in the access network. (This example illustrates the use of the HELD protocol for the location request.) The locationRequest contains an identifier and appropriate credentials associated with the calling device, as well as an indication of the type of location being requested. In this example, the device requests civic or geodetic location. The locationRequest also includes a responseTime parameter (not shown) indicating how long the device is prepared to wait for a response or the purpose for which the device needs the location.

**Step 2.** The LIS determines the location of the calling device in some way – e.g., based on a known location of the Wi-Fi AP being used by the calling device or by other means. The LIS responds to the location request by returning location information "by-value".

**Step 3.** The device uses the LbyV in the location response from the LIS and the emergency service URN (urn:service:sos) to query an ECRF (or other LoST server) for routing information.

**Step 4.** The ECRF responds by returning a URI associated with an ESRP in an i3 ESInet.

**Step 5.** The device generates a SIP INVITE message that includes a Route header that contains the ESRP URI, an emergency services service URN (urn:service:sos), callback information, and LbyV (i.e., a Geolocation header that contains a cid, a Geolocation-Routing header set to "yes", and a PIDF-LO in the body of the message that contains the LbyV), and sends it to a Call Server/Proxy in its VoIP service provider network.

**Step 6.** The Call Server/Proxy adds a P-Asserted-Identity header containing callback information, and Additional Data "by value" to the received SIP INVITE message by including a Call-Info header that contains a cid pointing to the Additional Data in the message body, and forwards the SIP INVITE message to a BCF on the ingress side of the i3 ESInet.

**Step 7.** The BCF adds an RPH with a value of "esnet.1" to the received INVITE message and forwards it to the ESRP.

**Step 8.** The ESRP queries the ECRF using the location information received in the body of the received SIP INVITE message and the emergency service URN (urn:service:sos).

**Step 9.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP/ECC that is served by the i3 ESInet.

**Step 10.** The ESRP generates an outgoing SIP INVITE message, using the routing information received from the ECRF as well as information received in the initial SIP INVITE message, and forwards it to the i3 PSAP/ECC (via a BCF [not shown]). The SIP INVITE message contains the PSAP/ECC URI in the Route header, the sos service URN in the Request-URI, the callback information in the From header and P-Asserted-Identity header, the RPH, the LbyV in the body (along with a cid in the Geolocation header and a Geolocation-Routing header set to "yes"), and Additional Data (by value) in the body (along with a cid in the Call-Info header).

**Step 11.** The PSAP/ECC indicates the call has been answered by returning a SIP 200 OK to the ESRP. The 200 OK gets propagated back to the calling device.

**Step 12.** At the appropriate time, the PSAP/ECC determines that the call can be terminated and sends a SIP BYE to the ESRP. The BYE message gets propagated back to the calling device. (Note that the BYE may instead be initiated by the calling device.)

## 8.4 911 Origination – Variation on IETF-based Solution

The call flow provided in Figure 7 illustrates an alternative to having the device query the LIS for location, RFC 6443 allows for the device to determine its own location based on measurements (or some other location determination mechanism) rather than interacting with a LIS to obtain it. This call flow assumes that the device determines its own location. It further assumes that the device does not support interactions with a LoST server, and that the Call Server/Proxy in the serving VoIP Service Provider network is responsible for performing that function. The remainder of the call flow is identical to the one described in Section 9.3 above.

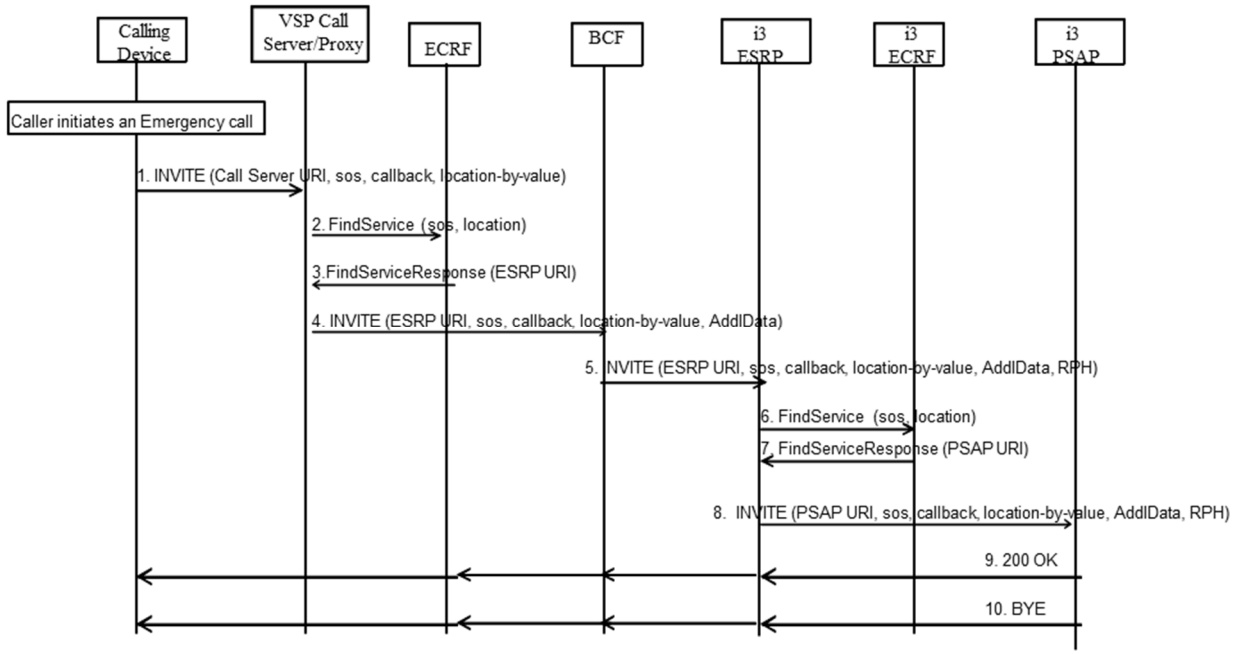



**Figure 7: 911 Origination - No Access to Cellular Network - Modified IETF Solution**

**Step 1.** Upon recognizing a request for emergency service, the calling device generates a SIP INVITE message that includes a Route header that contains the URI of a Call Server/Proxy in a VoIP Service Provider network, an emergency services service URN (urn:service:sos), callback information, and location-by-value (i.e., a Geolocation header that contains a cid, a Geolocation-Routing header set to "yes", and a PIDF-LO in the body of the message that contains the LbyV), and sends it to a Call Server/Proxy in a VoIP service provider network.

**Step 2.** The Call Server/Proxy uses the LbyV and the emergency service URN (urn:service:sos) in the received INVITE message to query an ECRF (or other LoST server) for routing information.

**Step 3.** The ECRF responds by returning a URI associated with an ESRP in an i3 ESInet.

**Step 4.** The Call Server/Proxy generates a SIP INVITE message that includes a Route header that contains the ESRP URI, an emergency services service URN (urn:service:sos), callback information, and LbyV (i.e., a Geolocation header that contains a cid, a Geolocation-Routing header set to "yes", and a PIDF-LO in the body of the message that contains the LbyV), and Additional Data "by value" (i.e., including a Call-Info header that contains a cid pointing to Additional Data in the message body), and forwards the SIP INVITE message to a BCF on the ingress side of the i3 ESInet.

**Step 5.** The BCF adds an RPH with a value of "esnet.1" to the received INVITE message and forwards it to the ESRP.

**Step 6.** The ESRP queries the ECRF using the location information received in the body of the received SIP INVITE message and the emergency service URN (urn:service:sos).

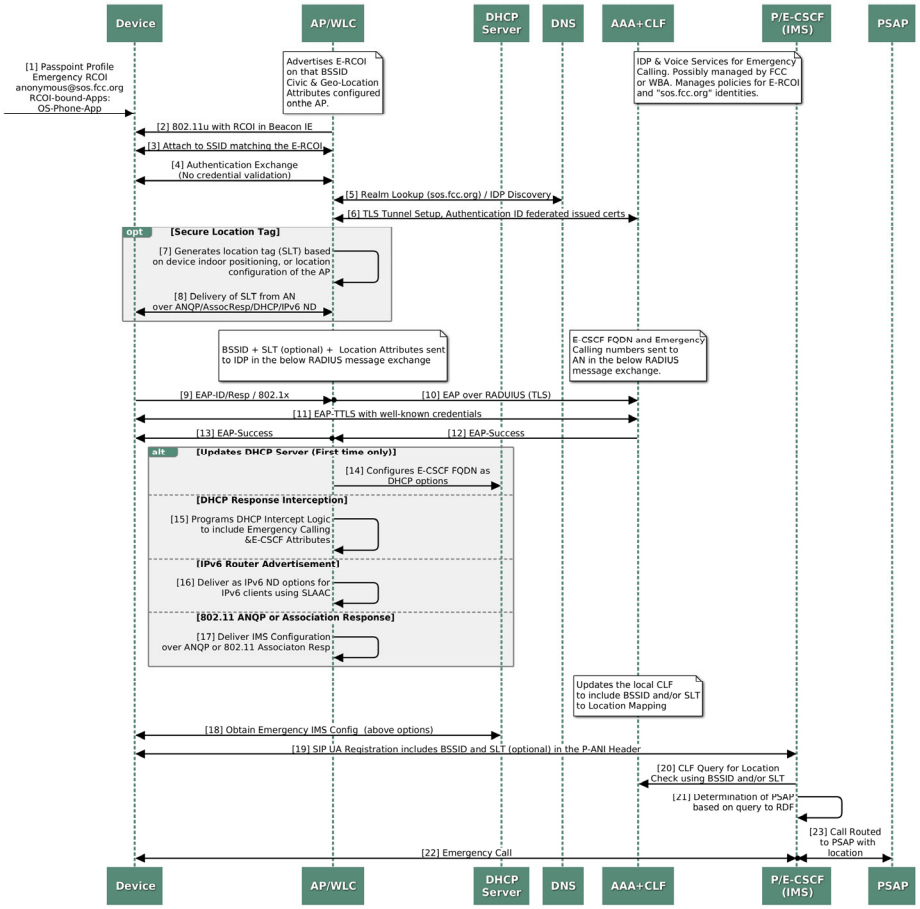
**Step 7.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP/ECC that is served by the i3 ESInet.

**Step 8.** The ESRP generates an outgoing SIP INVITE message, using the routing information received from the ECRF as well as information received in the initial SIP INVITE message, and forwards it to the i3 PSAP/ECC (via a BCF [not shown]). The SIP INVITE message contains the PSAP/ECC URI in the Route header, the sos service URN in the Request-URI, the callback information in the From header and P-Asserted-Identity header, the LbyV in the body (along with a cid in the Geolocation header and a Geolocation-Routing header set to "yes"), and Additional Data (by value) in the body (along with a cid in the Call-Info header).

**Step 9.** The PSAP/ECC indicates the call has been answered by returning a SIP 200 OK to the ESRP. The 200 OK gets propagated back to the calling device.

**Step 10.** At the appropriate time, the PSAP/ECC determines that the call can be terminated and sends a SIP BYE to the ESRP. The BYE message gets propagated back to the calling device. (Note that the BYE may instead be initiated by the calling device.)

## 8.5 Emergency Access to Nearby Wi-Fi AP When Cellular RAN, Core and/or IMS is Not Available Using a Framework Allowing the Use of a Default Emergency Passpoint Profile (Use Case #10)




## Key Steps:

1. The device is pre-configured with the emergency Passpoint profile, which includes the emergency RCOI, and a common identity, "anonymous@sos.fcc-authorized.org". This allows the device to discover access networks that support emergency 911 services.
2. An 802.11 access network supporting EAP-based authentication method 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.
3. 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.
4. 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.
5. The device will use the default identity, "anonymous@sos.fcc-authorized.org" from Passpoint profile in the initial authentication message exchange, allowing the access network to discover the AAA server / IDP for EAP authentication.
6. The access network using the realm portion of the identity, "sos.fcc-authorized.org." will perform a DNS lookup using the AAA server for the IDP supporting the emergency RCOI and the realm.

7. The access network and the AAA server will establish a secure TLS tunnel for securing the 802.1x/EAP traffic. The authentication of the peers will be based on X.509 certificates.
8. 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.
9. 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.
10. 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.
11. 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).
12. The AAA server will send locale-specific IMS configuration (E-CSCF FQDN) supporting emergency call routing services to the access point.
13. A successful EAP transaction between the device and the AAA server will result in the AAA server sending EAP-SUCCESS to the device.
14. 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.
15. 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.
16. 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.
17. 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.

## 8.6 Considerations

- None of the call flows illustrated above take into consideration the application of SHAKEN caller identity authentication/verification, RPH signing/verification, or location spoofing mitigation mechanisms which would include the ability to perform a consistency check on device-provided location, to the 911 call.
- The call flows depicted above do not address mechanisms for obtaining and conveying updated device-based location to PSAPs/ECCs (where the initial location is expected to be provided "by-value") or the ability to perform a consistency check on updated device-provided location.
- The two bullets above do not apply to Use Case #10: Emergency Access to nearby Wi-Fi AP when cellular RAN, Core and/or IMS is not available using a framework allowing the use of a default emergency Passpoint profile.

# 9 Appendix C – 3GPP IMS Reference Architecture

## 9.1 VoLTE and Wi-Fi Calling to 911: Normal State (Use Cases #1 through #4)

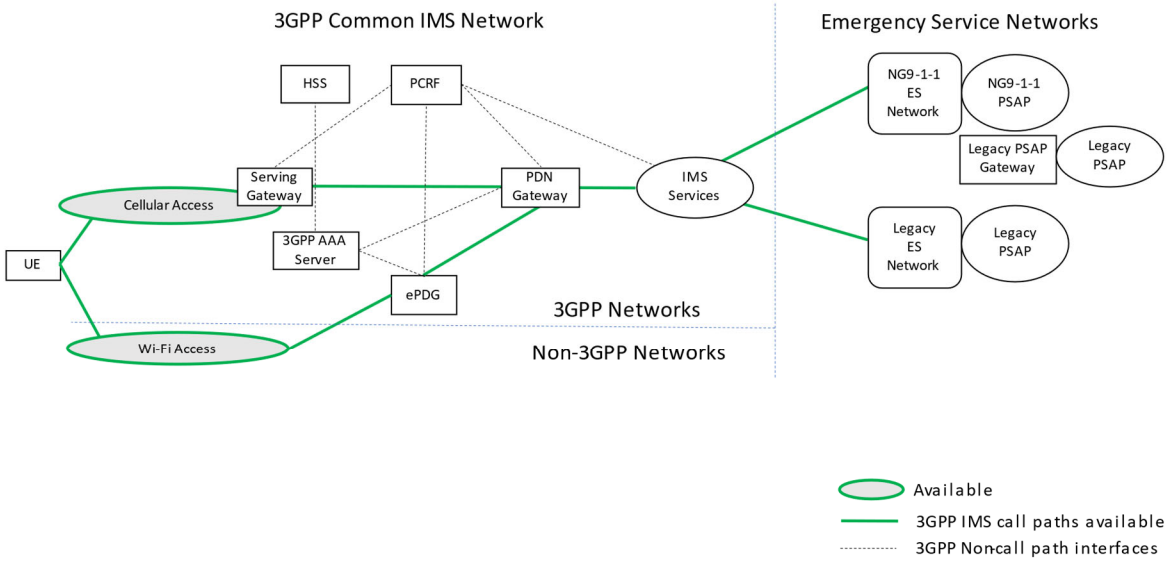



**Figure 8: VoLTE and Wi-Fi Calling to 911: Normal State (Use Cases #1 through #4)**

## 9.2 Cellular Access Network Unavailable: Wi-Fi Calling
**(Working Use Cases #5 (Current), #6 (Future), #7 (Future))**

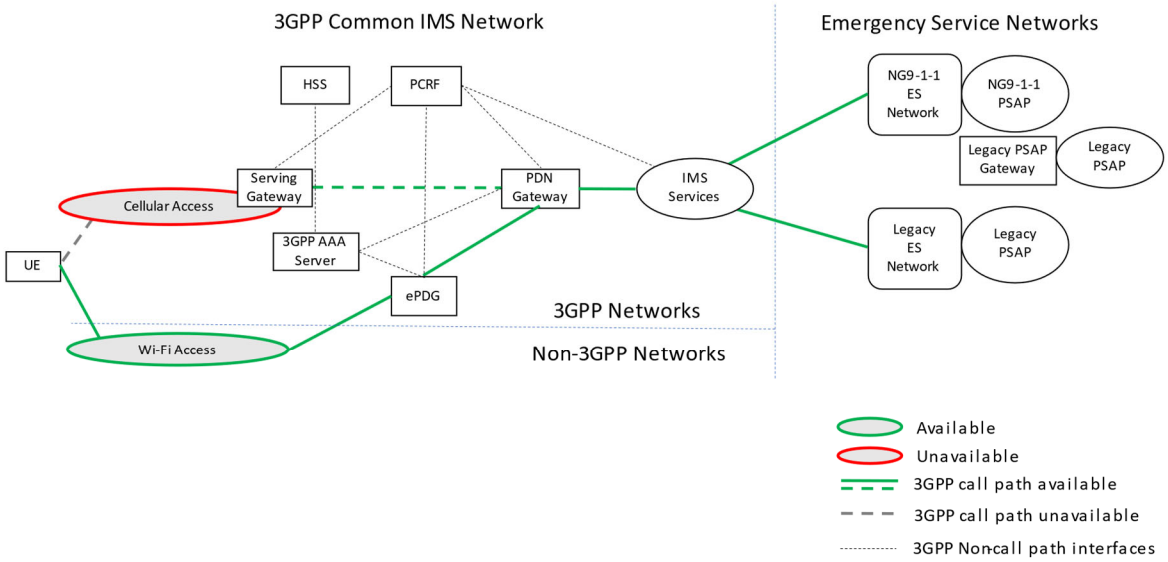



**Figure 9: Cellular Access Network Unavailable**
**(Working Use Cases #5 (Current), #6 (Future), #7 (Future))**

## 9.3 Cellular Access Network Unavailable: Wi-Fi Calling (Use Case #6 Emergency Access to Nearby Wi-Fi AP (Current))

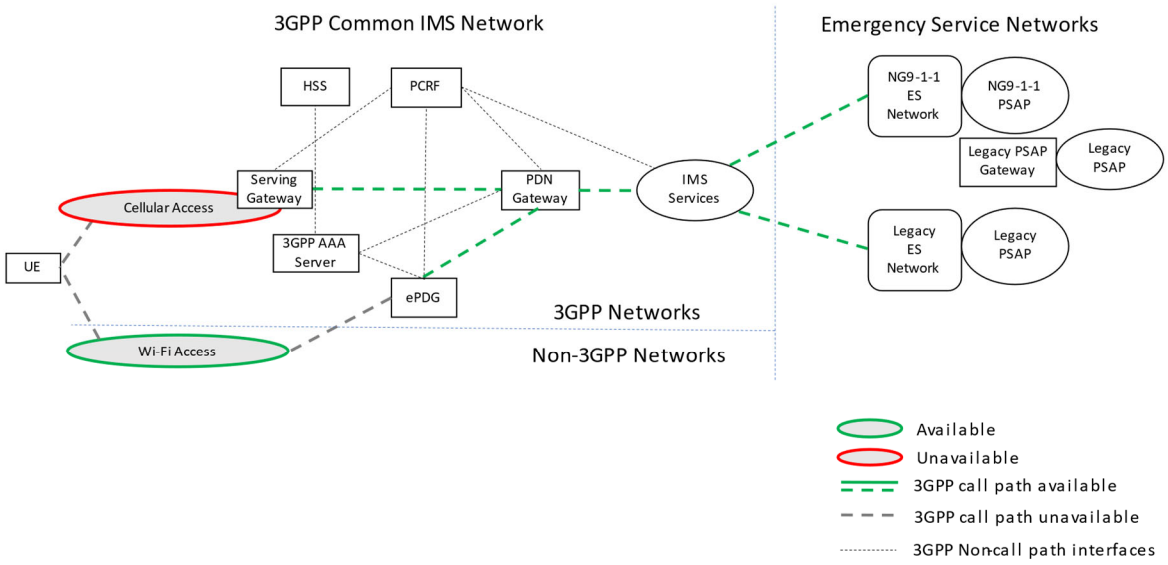



Figure 10: Cellular Access Network Unavailable: Wi-Fi Calling (Use Case #6 Emergency Access to Nearby Wi-Fi AP (Current))

## 9.4 Cellular Access Network Unavailable: Wi-Fi Calling (Use Case #7 Automatic Activation of Wi-Fi Calling (Current))

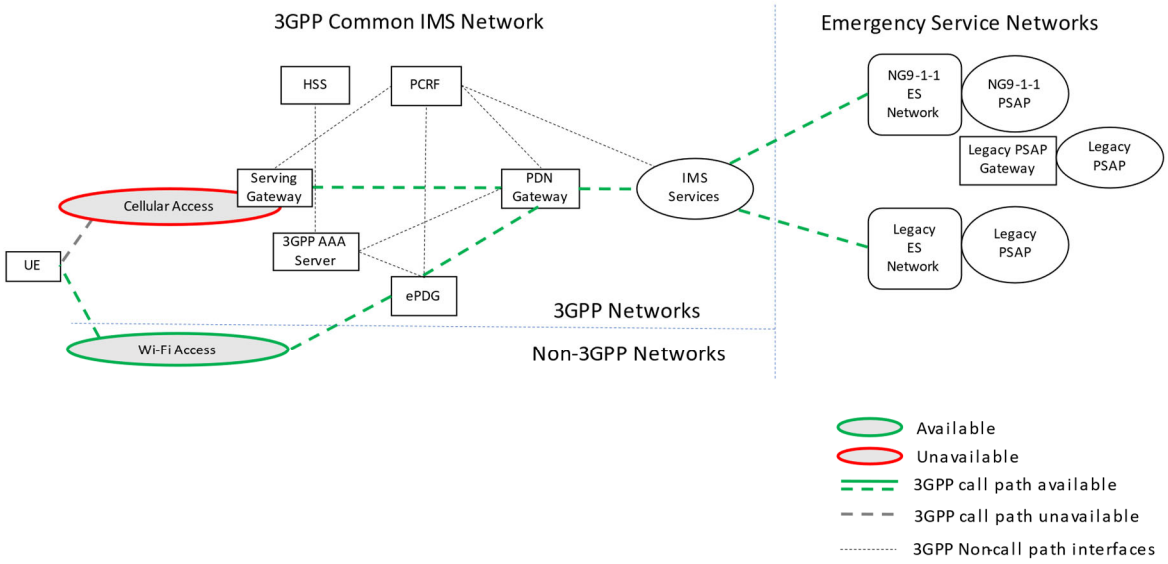



Figure 11: Cellular Access Network Unavailable: Wi-Fi Calling

(Use Case #7 Automatic Activation of Wi-Fi Calling (Current))

## 9.5 Cellular Access Network Unavailable: Wi-Fi Calling Use Case #8 911 over Wi-Fi from a device with an International subscription (Future)

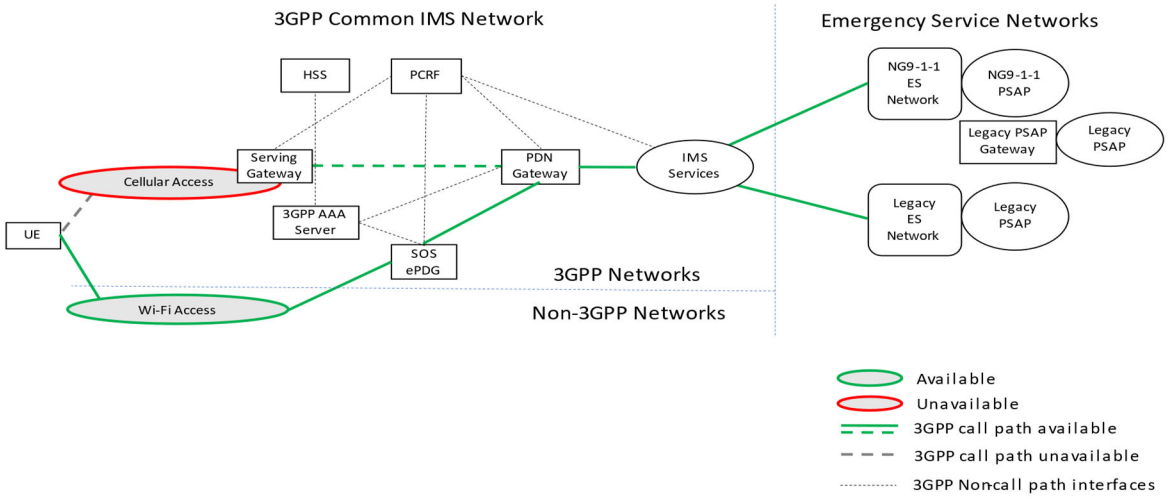



Figure 12: Use Case #8
911 over Wi-Fi from a device with an International subscription (Future)