Emergency e911 Services over Wi-Fi

draft-gundavelli-dispatch-e911-wifi

Authors: Sri Gundavelli (Cisco) & Mark Grayson (Cisco)

IETF 116 Yokohoma, March 26th, 2023

Background

- The mission of the FCC Communications Security, Reliability, and Interoperability Council (FCC CSRIC VIII) is to make recommendations to the Commission to promote the security, reliability, and resiliency of the Nation's communications systems.
  - https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-1

WG4: https://www.fcc.gov/file/23814/download

- **Working Group 4: 911 Service Over Wi-Fi**

- *Co-chairs: Mary Boyd, Intrado & Mark Reddish, APCO*
- *FCC Liaison: Rasoul Safavian*

- The Chairwoman of the FCC directs 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 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), and communications providers, and could complement the broader transition to an IP-based Next Generation 911 environment.

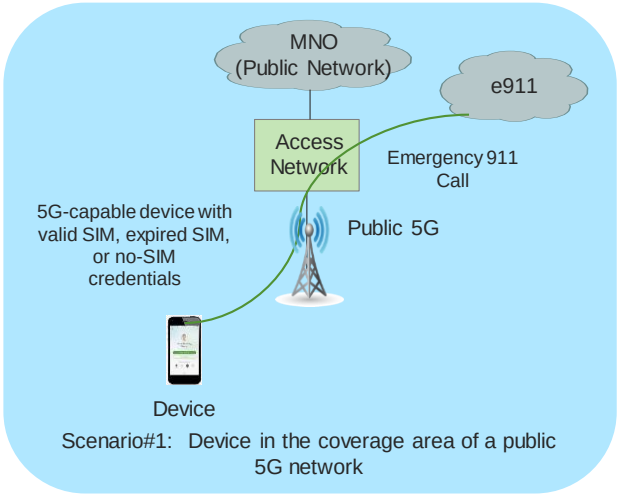
- CSRIC VIII will bring industry stakeholders together to examine a range of technical issues with the goal of promoting consensus in the Wi-Fi ecosystem to support reliable 911 services (voice and text) under normal conditions and when catastrophic events disrupt mobile service. The primary focus will be 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, automatically determining the 911 caller location and call routing issues, 911 call prioritization, identifying missing standards, and timelines and costs for implementing 911 over Wi-Fi solutions.

  - ***Milestones**:*

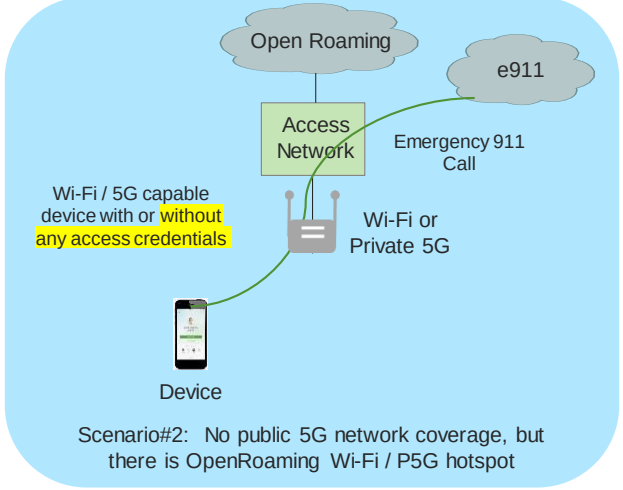
- Report on 911 Service over Wi-Fi, ***March 2023***

User Environments

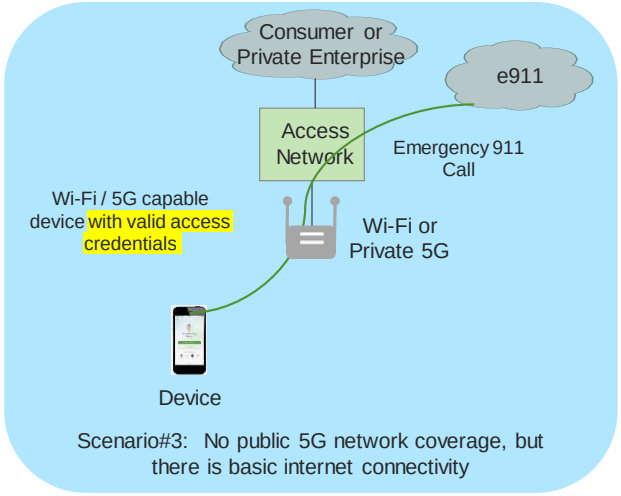
- The focus is largely on scenarios where there is no availability of a public mobile network. There is an explicit assumption that the device is Wi-Fi capable and is in proximity of a Wi-Fi hotspot.



Scenario#1: Device in the coverage area of a public 5G network



Scenario#2: No public 5G network coverage, but there is OpenRoaming Wi-Fi / P5G hotspot



Scenario#3: No public 5G network coverage, but there is basic internet connectivity

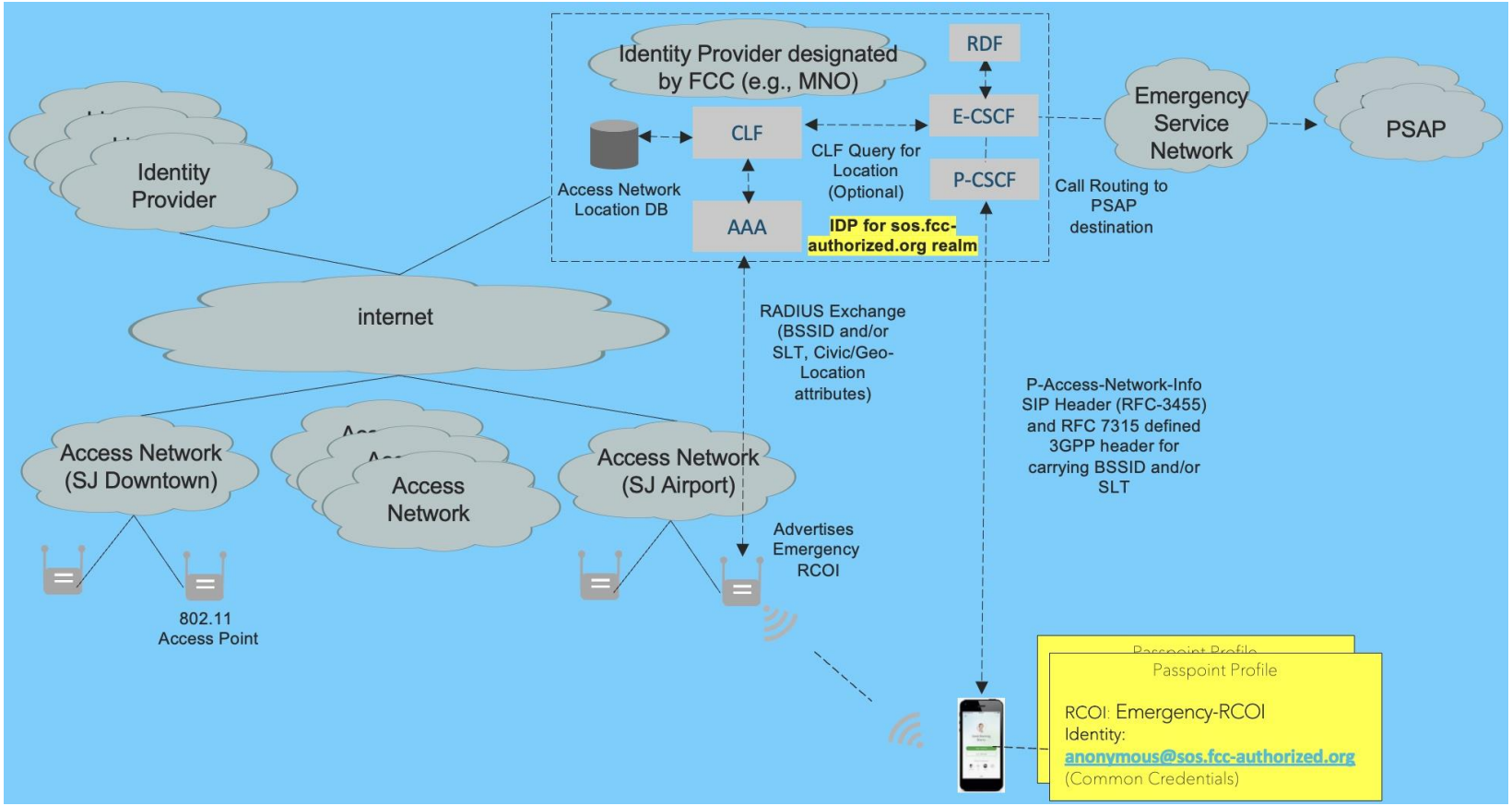
Scenario Description

Device	The use case applies to devices with • Wi-Fi interface and (optional) SIM • Wi-Fi interface is available Device is pre-configured with the default emergency passpoint profile. This may have been installed as part of the carrier-bundle upgrade, time of manufacturing at the OEM, part of enterprise software upgrade, or by the end user.
Cellular Network connectivity	H-PLMN and V-PLMN RAN unavailable; H-PLMN Core and IMS unavailable.
Wi-Fi Access	OpenRoaming federation Wi-Fi network is available in the location. The hotspot is configured to enable access to users with emergency passpoint profiles.
Wi-Fi Calling Feature	Wi-Fi Calling is enabled
Description	User dials 911 on native dialer Device discovers and attaches to the OpenRoaming hotspot supporting emergency services. Temporary access is granted to the device for making the emergency calls. Device obtains the voice service configuration from the access network. User's call is routed to the emergency voice server. The call is routed to the nearest PSAP.

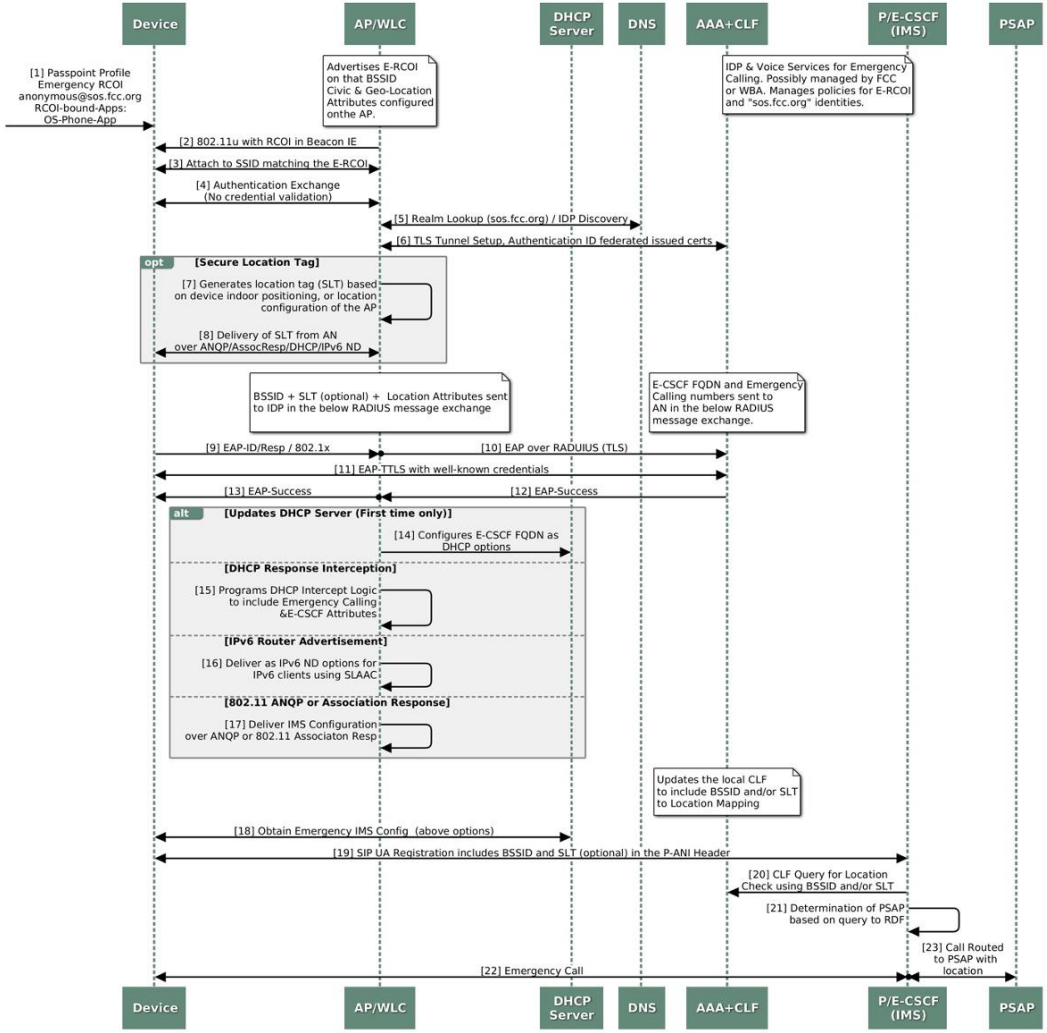
Key Technical Elements

- WLAN Network Identification & Selection
- Passpoint Profiles on Device
- Legal and Regulatory Requirements
- Emergency 911 Service Configuration Delivery
- Signaling of Access Network Location
- Detecting Rogue Caller & Location Spoofing

End-to-end System View



Call Flow


Device
AP/WLC
DHCP Server
DNS
AAA+CLF
P/E-CSCF (IMS)
PSAP
[1] Passpoint Profile
Emergency RCOI
anonymous@sos.fcc.org
RCOI-bound-Apps:
OS-Phone-App
Advertises E-RCOI on that BSSID
Civic & Geo-Location Attributes configured onthe AP.
IDP & Voice Services for Emergency Calling. Possibly managed by FCC or WBA. Manages policies for E-RCOI and "sos.fcc.org" identities.
[2] 802.11u with RCOI in Beacon IE
[3] Attach to SSID matching the E-RCOI
[4] Authentication Exchange
(No credential validation)
[5] Realm Lookup (sos.fcc.org) / IDP Discovery
[6] TLS Tunnel Setup, Authentication ID federated issued certs
opt
[Secure Location Tag]
[7] Generates location tag (SLT) based on device indoor positioning, or location configuration of the AP
[8] Delivery of SLT from AN over ANQP/AssocResp/DHCP/IPv6 ND
BSSID + SLT (optional) + Location Attributes sent to IDP in the below RADIUS message exchange
E-CSCF FQDN and Emergency Calling numbers sent to AN in the below RADIUS message exchange.
[9] EAP-ID/Resp / 802.1x
[10] EAP over RADUIUS (TLS)
[11] EAP-TTLS with well-known credentials
[13] EAP-Success
[12] EAP-Success
alt
[Updates DHCP Server (First time only)]
[14] Configures E-CSCF FQDN as DHCP options
[DHCP Response Interception]
[15] Programs DHCP Intercept Logic to include Emergency Calling &E-CSCF Attributes
[IPv6 Router Advertisement]
[16] Deliver as IPv6 ND options for IPv6 clients using SLAAC
[802.11 ANQP or Association Response]
[17] Deliver IMS Configuration over ANQP or 802.11 Associaton Resp
Updates the local CLF to include BSSID and/or SLT to Location Mapping
[18] Obtain Emergency IMS Config (above options)
[19] SIP UA Registration includes BSSID and SLT (optional) in the P-ANI Header
[20] CLF Query for Location Check using BSSID and/or SLT
[21] Determination of PSAP based on query to RDF
[23] Call Routed to PSAP with location
[22] Emergency Call
Device
AP/WLC
DHCP Server
DNS
AAA+CLF
P/E-CSCF (IMS)
PSAP

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.

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

- A trusted OpenRoaming access network signals the same location tag along with the civic and/or geo-spatial coordinates to the IDP. The CSCF function will retrieve the SLT from the call signaling from the device and will look up the civic location and/or geo-spatial coordinates of the device by querying the CLF database populated by the IDP.

Next Steps

- The proposed approach based on WBA's OpenRoaming enables a device with an emergency Passpoint profile to make emergency 911 call from any of the OpenRoaming hotspots.

- Authors believe there is tremendous value in improving access to emergency services over Wi-Fi. It can potentially save lives.

- Does the working group agree with this view? Should IETF should document techniques for improving access emergency 911 service.

COMMENTS?

OpenRoaming Primer

Private Wireless Roaming Landscape before OpenRoaming

- Carrier Wi-Fi foundations in place
  - WBA's Wireless Roaming Intermediary Exchange used to support "Carrier Wi-Fi" use cases for paid Wi-Fi
- More than a single deployment model
  - Majority of Wi-Fi deployed by private enterprises and most desire to serve guests/visitors/public but may not require financial payment
- Avoiding intrusive experience due to fragmented legal approaches
  - Today, each access network presents their own terms and privacy policies that need to be agreed, before access permitted
- Based on bi-lateral agreements with carrier legal teams
  - Unable to scale above 10s to 100s of networks

WBA OpenRoaming: A cloud-based roaming federation

- Leverages native device Passpoint capability
- WBA defined common legal framework
- DNS based dynamic discovery of Identity Provider's AAA systems using realm from EAP Identity
- Signalling secured using RadSec (TLS) with WBA public key infrastructure and certificate policy
- RADIUS profile that includes requirements to support RFC 5580 location signalling
- Lowering barriers to adoption for Wi-Fi roaming
  - 1000 live networks across the globe
  - 2 Million Access points
  - 300 Companies, Cities and Enterprises

OpenRoaming Legal Framework