Emergency Calling (911/112/*) Services over Wi-Fi

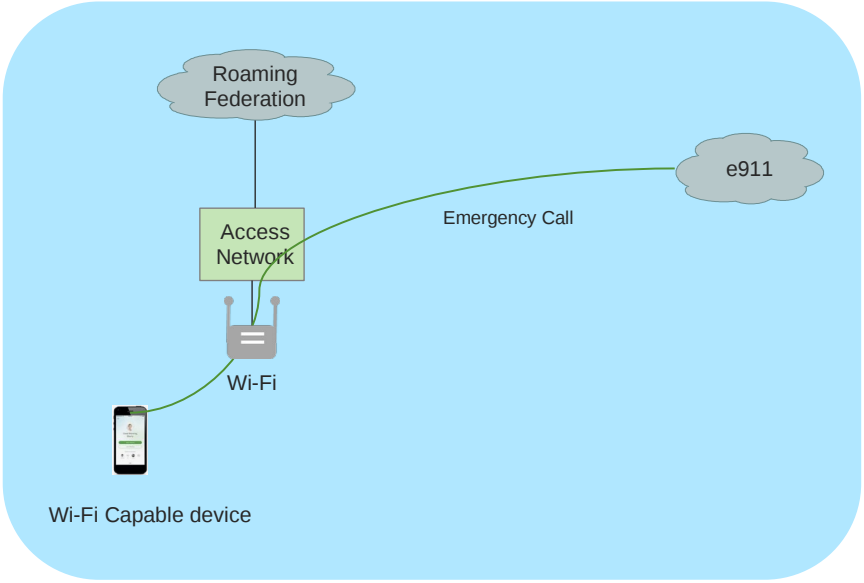
draft-gundavelli-dispatch-e911-wifi

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

IETF 119 Brisbane, March 18th, 2024

User Environments

- The focus is largely on scenarios where there is no availability of a public mobile network. Can a Wi-Fi capable device in such environments, make an emergency call, using the native dialer?



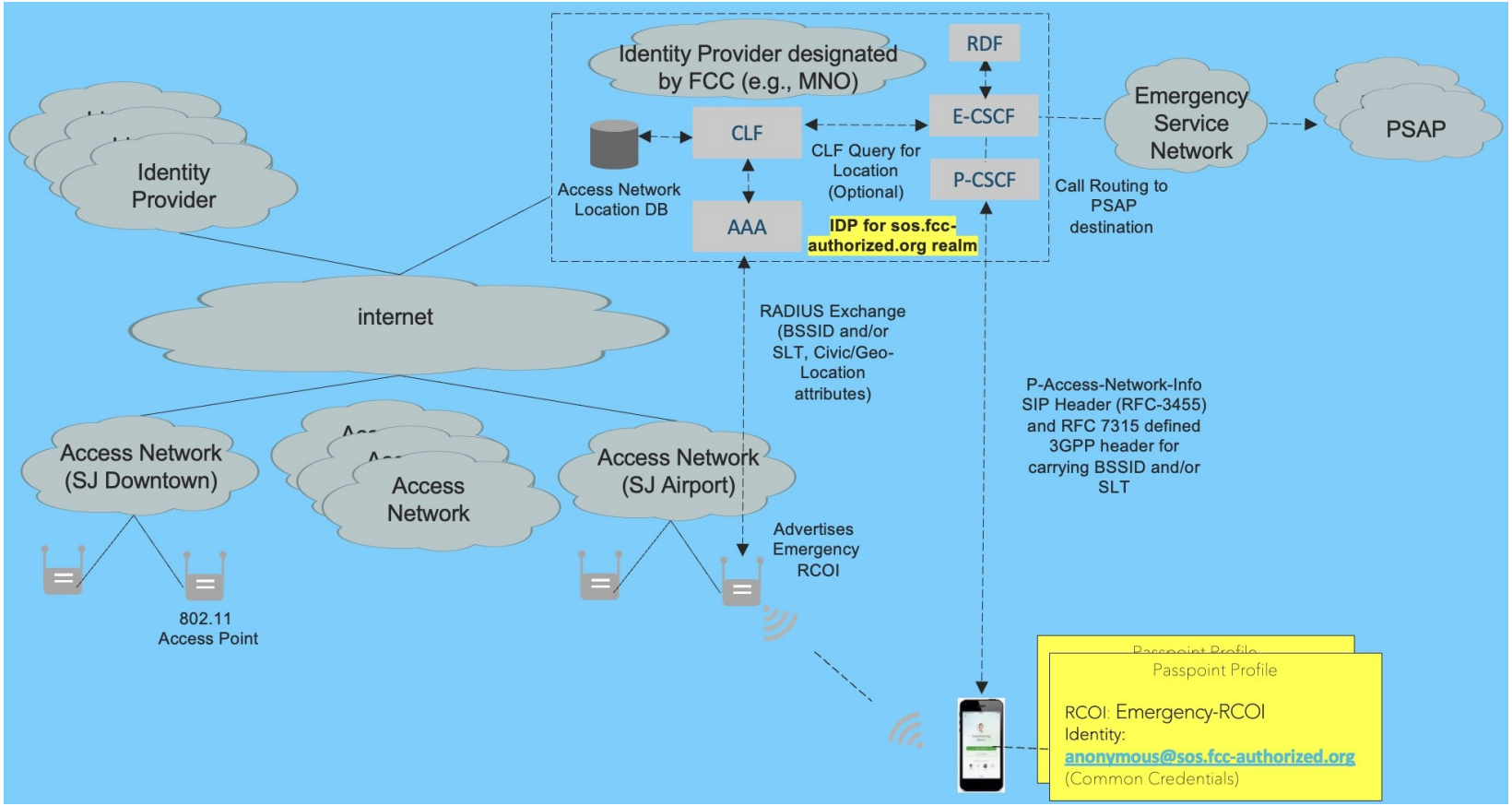
Scenario Description

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.

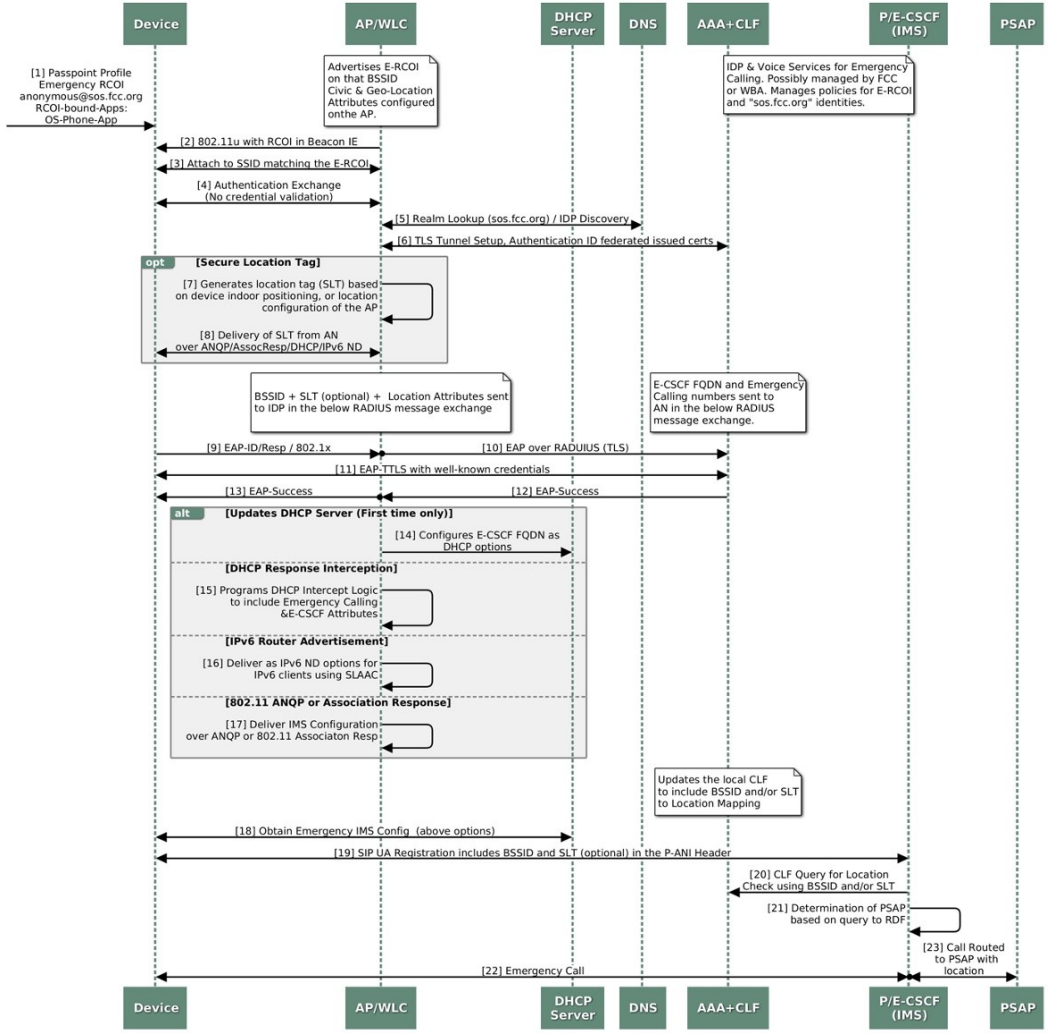
Key Technical Elements

- WLAN Network Identification & Selection
- Passpoint Profiles on Device
- Legal and Regulatory Requirements
- Emergency 911/112/* 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 roaming federation architectures enables a device with an emergency Passpoint profile to make emergency 911 call from any of the Wi-Fi hotspots which is part of the federation.

- These mechanisms 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 911/112/* service.