



# Appendix C-4

## System and Standard Views (SV-1 and StdV-1)

*Special Notice D15PS00295 – Nationwide Public  
Safety Broadband Network (NPSBN)*

4/27/2015

## Table of Contents

<b>1</b>	<b>Document Overview</b> .....	<b>1</b>
<b>2</b>	<b>RAN-Core</b> .....	<b>2</b>
2.1	SV-1 RAN-Core State Opt-Out.....	3
2.2	StdV-1 RAN-Core Opt-In and Opt-Out .....	3
<b>3</b>	<b>Roaming Interface</b> .....	<b>5</b>
3.1	SV-1 Roaming.....	6
3.2	StdV-1 – Roaming.....	7
<b>4</b>	<b>Application Ecosystem</b> .....	<b>8</b>
4.1	SV-1 Application Ecosystem.....	8
4.2	StdV-1 – Application Ecosystem .....	8
4.2.1	Physical Network Connectivity .....	8
4.2.2	Local Control .....	9
4.2.3	FirstNet Applications.....	9
4.2.4	API, Service Delivery Platform for Network Services.....	9
4.2.5	Application Store .....	10
4.2.6	Application Developers.....	10
4.2.7	Federated Identity Management.....	10
4.2.8	Cloud Services and Applications .....	10
<b>5</b>	<b>Public Safety Entity (PSE)</b> .....	<b>11</b>
5.1	SV-1 PSE .....	12
5.2	StdV-1 PSE.....	13
5.2.1	Transmission .....	13
5.2.2	Security .....	13
5.2.3	Element Management System.....	14
5.2.4	Local Control.....	14
5.2.5	Applications .....	14
<b>6</b>	<b>Device - Network</b> .....	<b>16</b>
6.1	SV-1 Device -Network .....	16
6.2	StdV-1 Device Network.....	17
6.2.1	Air Interface .....	17
6.2.2	Embedded Clients/Applications.....	17
6.2.3	Downloadable Clients/Applications.....	17

## List of Figures

Figure 1	SV-1 NPSBN System Interfaces .....	2
Figure 2	SV-1 RAN-Core (Opt-Out).....	3
Figure 3	SV-1 FirstNet Outbound Roaming.....	6

Figure 4 SV-1 FirstNet Inbound Roaming ..... 7  
Figure 5 SV-1 Application Ecosystem ..... 8  
Figure 6 SV-1 PSE ..... 12  
Figure 7 SV-1 Device: Network..... 16

## List of Tables

Table 1 RAN-Core Interface Specifications ..... 4  
Table 2 Roaming Interface Specification ..... 7  
Table 3 Application Ecosystem - Local Control Interface..... 9  
Table 4 FirstNet Applications – Industry Standards..... 9  
Table 5 API / Service Delivery Platform for Network Services Standards..... 9  
Table 6 Application Store Standards..... 10  
Table 7 Application Developers Standards ..... 10  
Table 8 Federated Identity Management Standards..... 10  
Table 9 Cloud Services and Applications Standards ..... 11  
Table 10 StdV-1 PSE: Transmission ..... 13  
Table 11 StdV-1 PSE: Security ..... 13  
Table 12 StdV-1 PSE: Element Management System..... 14  
Table 13 StdV-1 PSE: Local Control ..... 14  
Table 14 StdV-1 PSE: Applications ..... 15  
Table 15 Device Air Interfaces ..... 17  
Table 16 Embedded Clients/Applications Mandatory Standards..... 17  
Table 17 Downloadable Clients and Applications..... 17

DRAFT

## 1 Document Overview

The document provides two views of the interface between FirstNet's core network and other external interface views and its technical description and details interface requirements and standards that contractors shall meet in their implementation of the nationwide public safety broadband network (NPSBN).

- SV-1: a systems/services interface view identifying all interfaces needed
- StdV-1: a technical standards description of each of the identified interfaces at Initial Operational Capabilities (IOC) 1 – The standards described in the table shall meet the current General Release version at the time of IOC.

The following section of the document provides interfaces and its relevant standards and descriptions of the sub-system within the FirstNet Architecture and aligns with the Operational Architecture.

- RAN – Opt-In and Opt-Out
- Roaming and its interfaces
- Application Ecosystem
- Public Safety Enterprise
- Device – Network

DRAFT

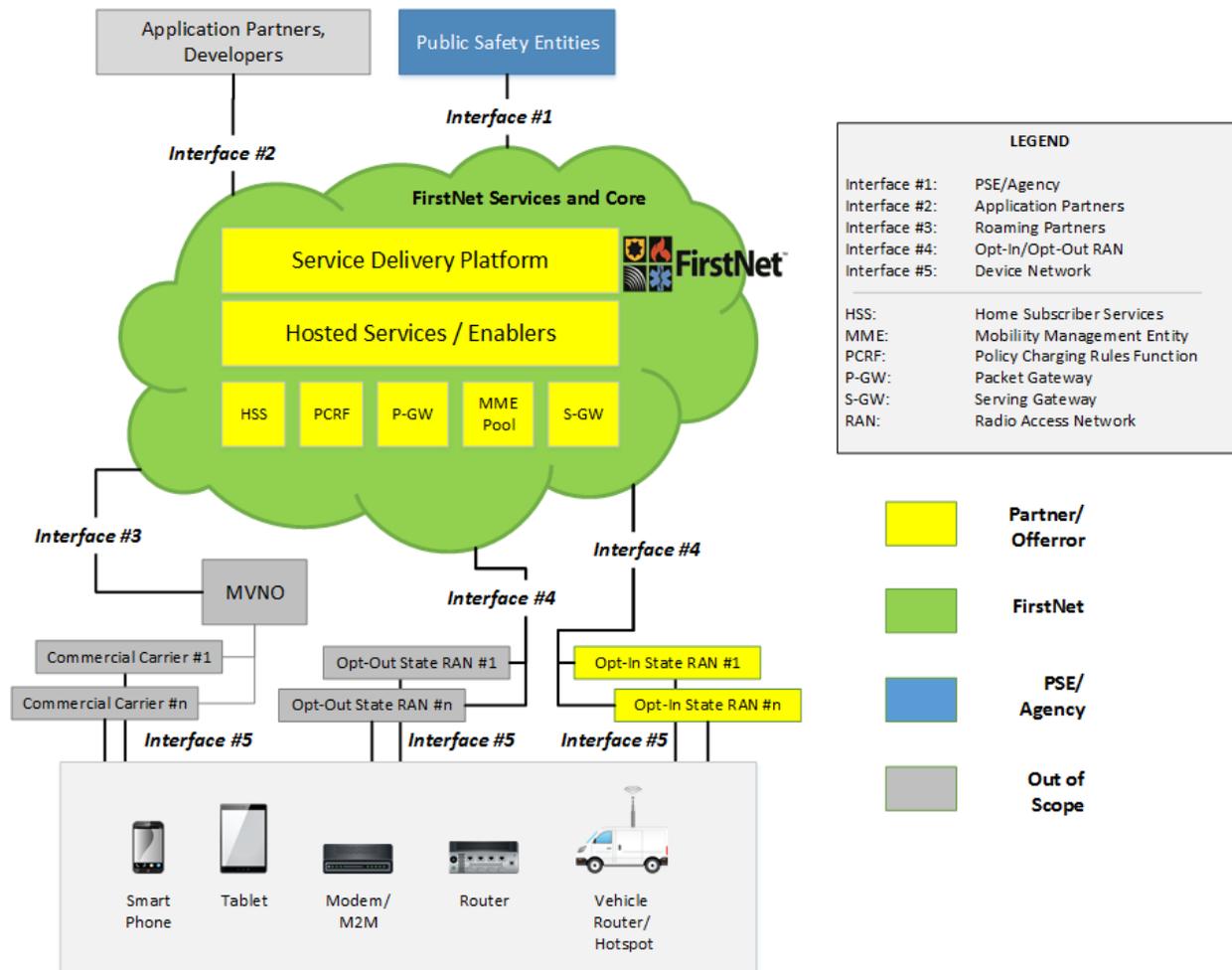


Figure 1 SV-1 NPSBN System Interfaces

Figure 1 SV-1 NPSBN System Interfaces provides at high level the NPSBN and its systems/view interfaces. Interface #2 is with third party application providers and developers, and interface #1 is with Public Safety Entities (PSE) hosting their local applications and management functions. Both interfaces use non-proprietary, open Internet standards. Interfaces #3 and #4 are 3GPP LTE standards-based interfaces with network contractor(s) such as MVNOs and state RANs respectively. Lastly, interface #5 spans both state and commercial RANs to interoperate with the many different types of devices. The interface shown above is not an exhaustive list or complete description. Colors are used to identify the organizational owner of a given function: (Green – FirstNet, Blue – Local Agency/PSEN, Yellow – FirstNet Contractor, Gray – Contractor’s roaming contractors or integrators.) The offeror will comply with the current or the latest version of the standard specification specified in the tables contained herein.

## 2 RAN-Core

This section covers the System View and the Standards Technical View for the RAN-Core Opt-in.

## 2.1 SV-1 RAN-Core State Opt-Out

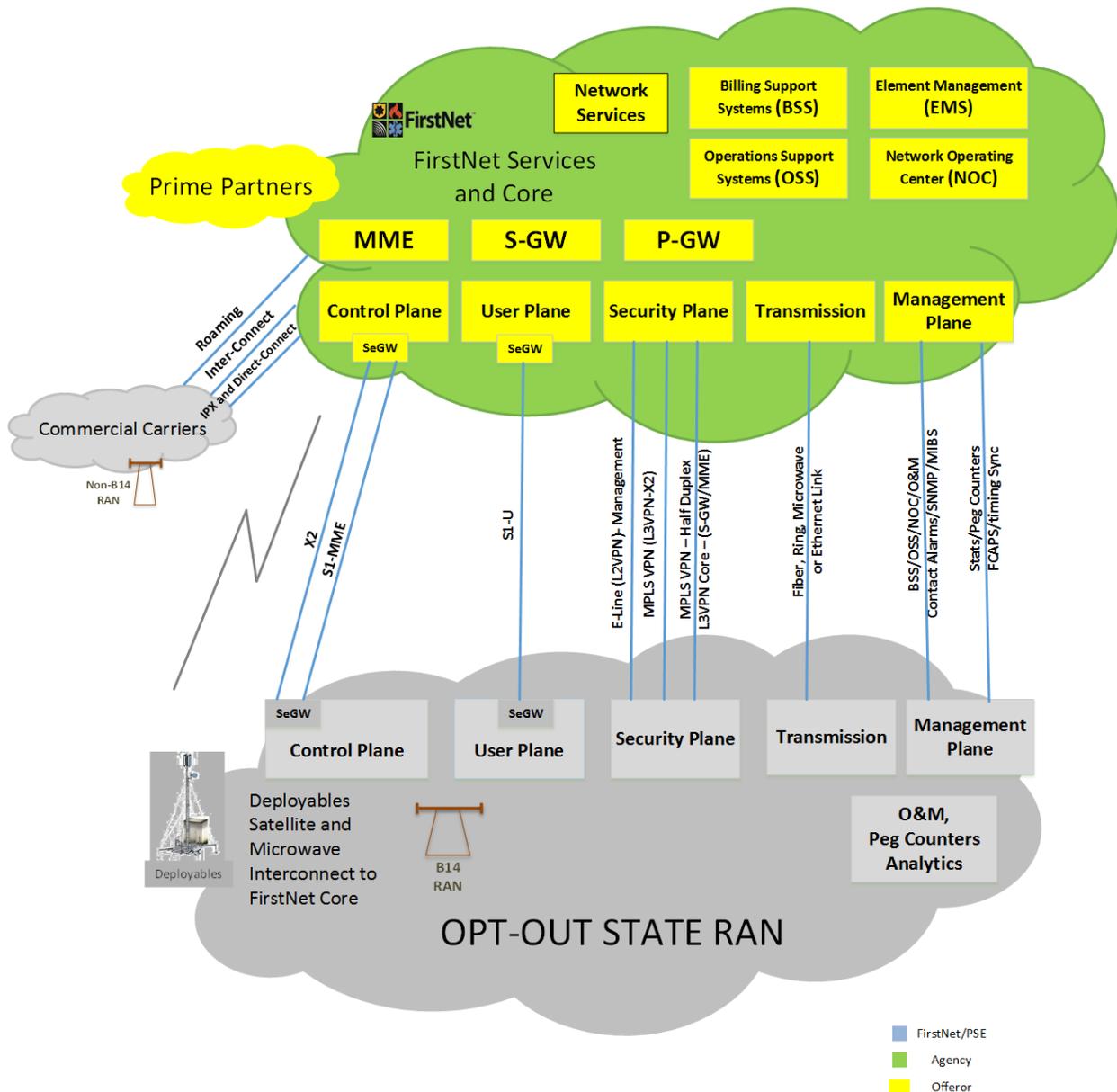


Figure 2 SV-1 RAN-Core (Opt-Out)

## 2.2 StdV-1 RAN-Core Opt-In and Opt-Out

The contractor shall comply with the mandatory standards interface specification requirements for interoperability with the National Public Safety Broadband Network (NPSBN) found in Table 1 RAN-Core Interface Specifications.

Table 1 RAN-Core Interface Specifications

Service Area	Description	Mandatory Standard and Source Document
<b>Security</b>	IPSec	RFC 2401 (Security Architecture for the Internet Protocol), AH and ESP
<b>Transmission</b>	Microwave, Fiber Ethernet to (MME, S/P-GW)	Industry standard best practice.
<b>eNodeB</b>	S1-MME Interface	3GPP TS 23.122, 24.301, 36.410, 36.411, 36.412, 36.413, 33.210, 33.310 MOCN, GWCN 3GPP TS 23.236 3GPP TS 23.251
	S1-U Interface	3GPP TS 23.122, 24.301, 36.410, 36.411, 36.414, 33.210, 33.310 MOCN, GWCN - 3GPP TS 23.236 3GPP TS 23.251
	S1 -U Security/Encryption	3GPP 33.210
	S1- MME Security/Encryption	3GPP 33.310
	X-2	3GPP TS 36.420, 36.421, 36.422, 36.423, 36.424
	LTE-Uu	3GPP release (e.g. R-9 or R-10)
	LTE measurements and performance metrics	3GPP 36.214, 36.314, 36.133, and 32.425
	Timing Interface	GPS and external 2.048 MHz synchronization and transmission synchronization. The transmission synchronization includes time division multiplexing (TDM), Synchronous Ethernet (SyncE) from ITU G.8262, and Timing over Packet (IEEE 1588). eICIC, CoMP requires +/- 1.5 to 5 $\mu$ s. ITU-T G.8272 defines requirements for a Primary Reference Time Clock (PRTC).
	Voice Services	VoLTE IR.92 version 6

Service Area	Description	Mandatory Standard and Source Document
	Location Services - LTE Positioning Protocol A (LPPa)	3GPP TS 23.271 3GPP 36.355, 36.305, 36.331 3GPP TS 36.355 (LTE positioning protocol) Secure User Plane Location protocol as specified in: OMA-RD-SUPL-V3_0 (requirements) OMA-AD-SUPL-V3 (architecture) OMA-ERELD-SUPL-V3_0 (enablers) OMA-TS-ULP-V3_0 (user plane protocol) Mobile Location Protocol services as specified in: OMA-RD-MLS-V1_3 (requirements) OMA-AD-MLS-V1_3 (architecture) OMA-ERELD-MLP-V3_1 (enablers) OMA-LIF-MLP-V3_3 (mobile location protocol) OMA-TS-LPPe-V1_1 (LPP extensions)  User Plane: (For reference only) OMA-TS-LPPe v1.1 OMA-SUPL v1., v.20, v3.0 OMA-SUPCS v1.0
<b>SLA Management</b>	Performance and Audit Monitoring	SNMP v3, sftp

### 3 Roaming Interface

This section covers the System View (SV-1) and the Standards Technical View (StdV-1) that the contractor shall implement in support of roaming.

### 3.1 SV-1 Roaming

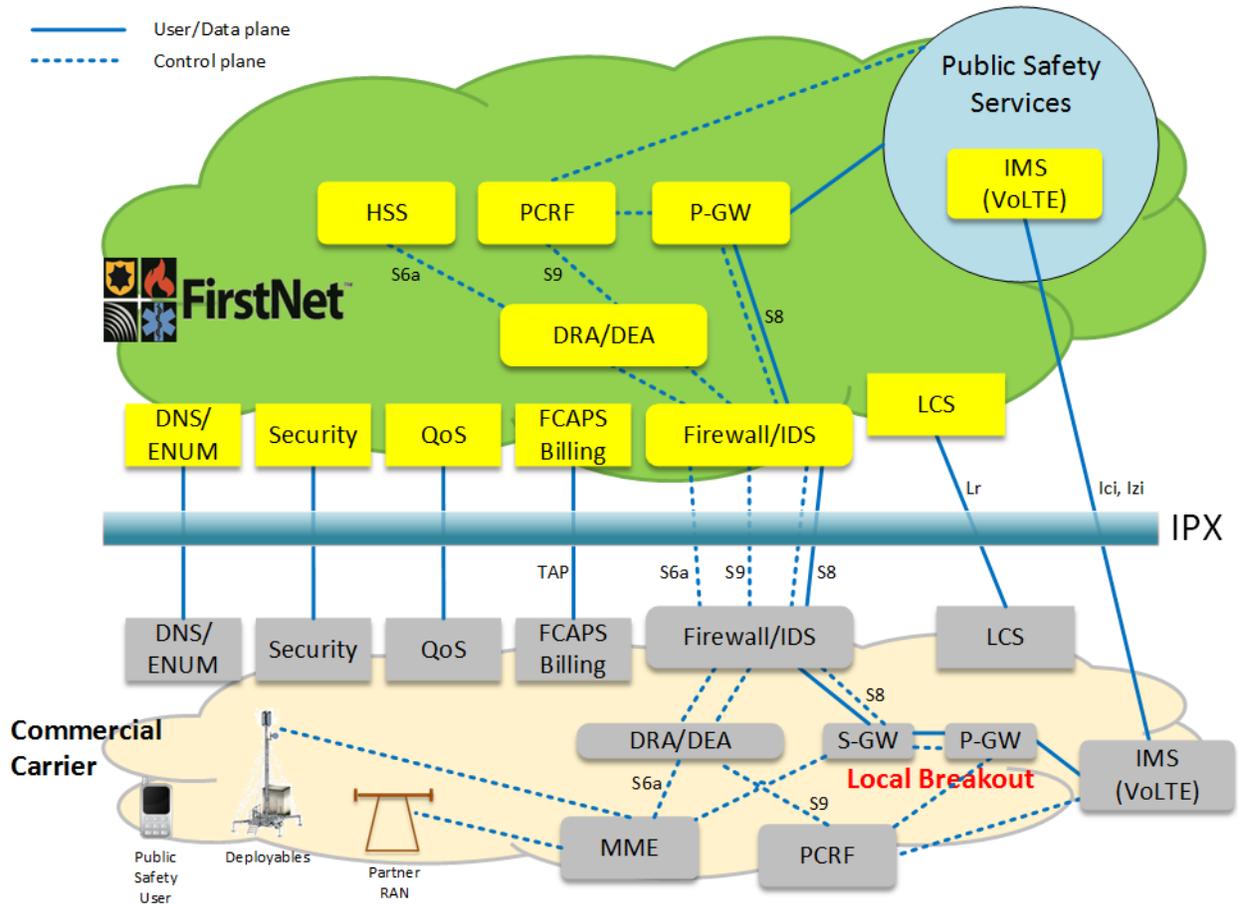


Figure 3 SV-1 FirstNet Outbound Roaming

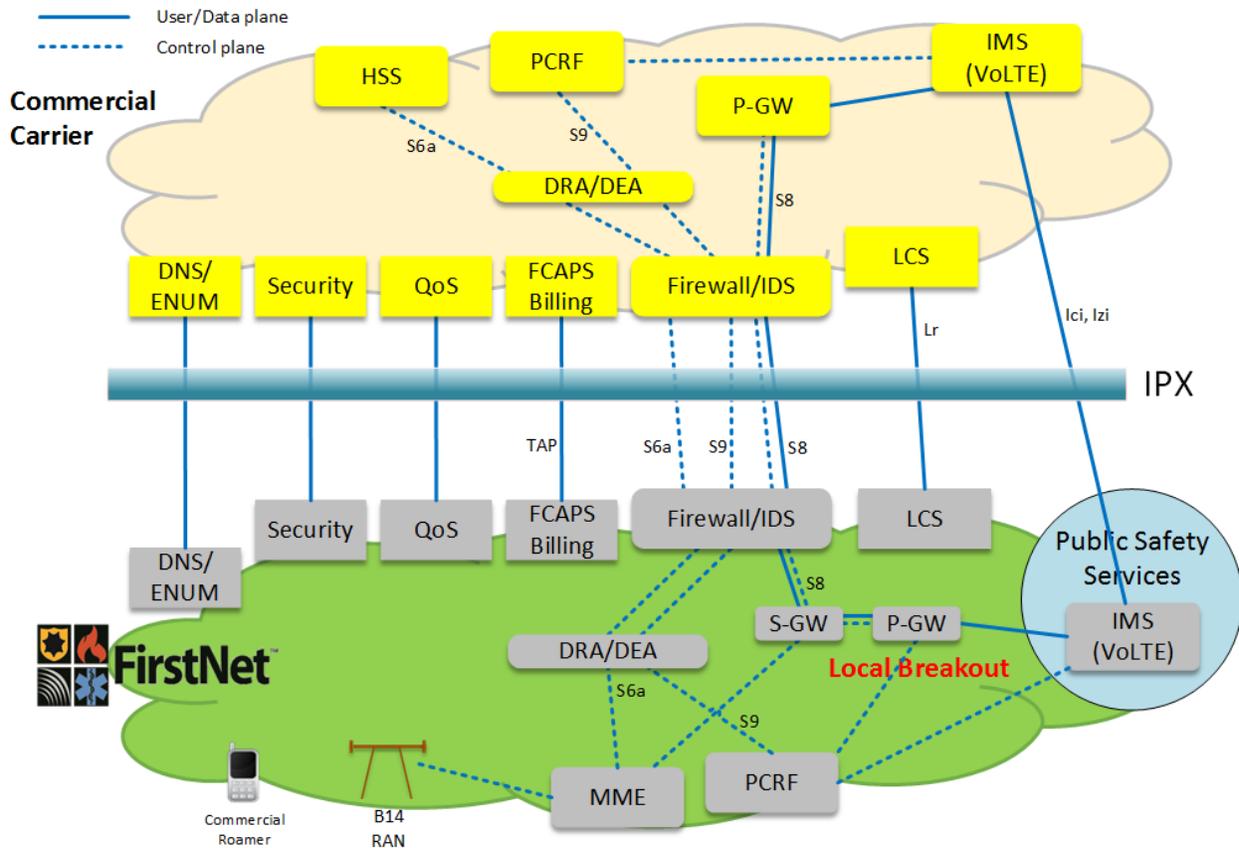


Figure 4 SV-1 FirstNet Inbound Roaming

### 3.2 StdV-1 - Roaming

The contractor shall comply with the 3GPP roaming interface specifications outlined in Table 2 Roaming Interface Specification.

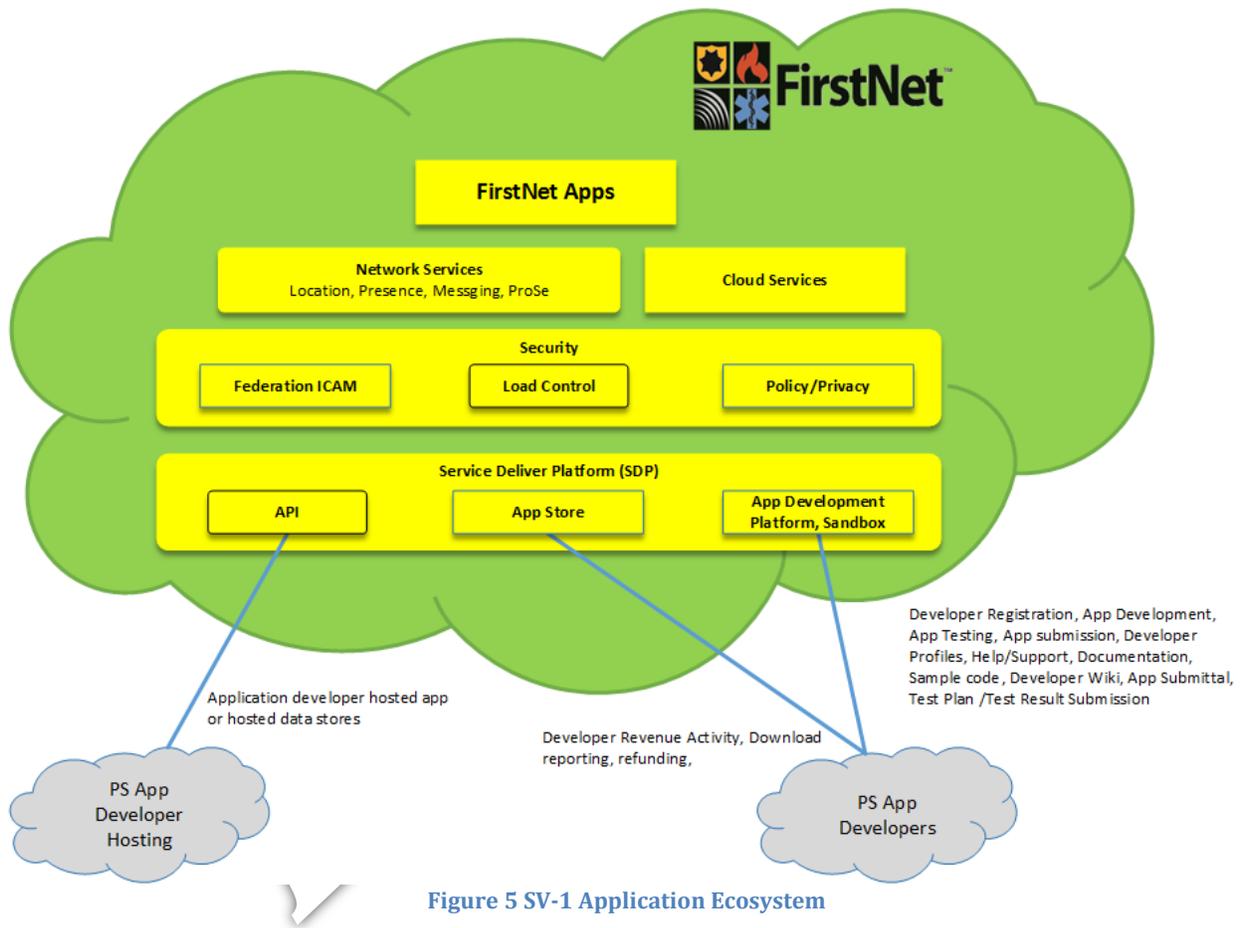
Table 2 Roaming Interface Specification

Service Area	Subset	Mandatory Standard and Source Document
<b>Roaming Guidelines</b>		GSMA PRD IR.88(53),GSMA PRD IR.67(52) GSMA PRD IR.65, 3GPP TS 23.401
<b>IMS/HSS</b>	DNS/ENUM	GSMA PRD IR.67 [52]
	DRA/DEA	defined by IETF RFC 3588 [59] and utilized by GSMA PRD IR.88 [53],
	Ici/Izi	3GPP TS 29.165 [24], GSMA PRD IR.65
	S9	3GPP TS 23.203
	S6a	3GPP TS 29.272 [30]
	VoLTE	3GPP TS 23.002 [1].
<b>Location</b>	RLP (Roaming Location Protocol)	3GPP TS 23.271 OMA-TS-RLP-V1_2-20120529-C
<b>EPC</b>	S5/S8	Control plane protocol (GTPv2-C) is defined in 3GPP TS 29.274 [31] and the user plane protocol (GTPv1-U) is defined in 3GPP TS 29.281 [32].

Service Area	Subset	Mandatory Standard and Source Document
<b>Security</b>	IPSec, Firewall	RFC 2401 (Security Architecture for the Internet Protocol), AH and ESP RFC 2401 – Firewall Enhancement Protocol (FEP)
<b>Transmission</b>	Fiber to MME and S/P-GW	Industry standard best practice.

## 4 Application Ecosystem

### 4.1 SV-1 Application Ecosystem



### 4.2 StdV-1 – Application Ecosystem

#### 4.2.1 Physical Network Connectivity

Contractor shall ensure that transmission links between a FirstNet application ecosystem and its application development contractors will be via public internet links and are encrypted. Links between the FirstNet application ecosystem and any production level third party hosting facilities must be both encrypted and fully redundant and served by at least two (2) separate and unique physical paths from different providers.

#### 4.2.2 Local Control

Local control is a web interface to provision users, manage the devices and applications, view billing, and monitor the performance of the local network for the PSEN. The Service Delivery Platform (SDP) will broker the web interface and apply all security based standards and policies.

**Table 3 Application Ecosystem - Local Control Interface**

Service Area	Description	Mandatory Standard and Source Document
<b>FirstNet Web Portal</b>	The PSE administrator is able to manage devices, applications, performance of its users	Web Portal Access from FirstNet to the secured portal of local agency. (JSON, XML) Support SSL, TLS

#### 4.2.3 FirstNet Applications

**Table 4 FirstNet Applications - Industry Standards**

Service Area	Description	Mandatory Standard and Source Document
<b>Client Server Applications</b>	Any server based applications available in FirstNet application ecosystem infrastructure	SOAP or RESTful using WSDL, JSON, XML Or industry standard best practice software methods
<b>Home Web Page for PSE (if needed)</b>	Based on PSE needs of their local status information of incidents gathered from multiple sources	HTML pages and JSON data (json.org) OpenData (Socradata framework) W3C - CORS and JSONP HTML5 based applications

#### 4.2.4 API, Service Delivery Platform for Network Services

**Table 5 API / Service Delivery Platform for Network Services Standards**

Service Area	Description	Mandatory Standard and Source Document
<b>APIs</b>	APIs useful for network services access and consumption	SOAP or RESTful using WSDL, JSON, XML Or industry standard best practice software methods
<b>Network Services API</b>	Messaging, location, voice, RCS, video, payment network services	SOAP or RESTful using WSDL,JSON,XML Or industry standard best practice software methods
<b>Payment API</b>	All paid application download and in-app purchasing	SOAP or RESTful using WSDL, JSON, XML. Or industry standard best practice software methods

#### 4.2.5 Application Store

Table 6 Application Store Standards

Service Area	Description	Mandatory Standard and Source Document
<b>FirstNet App Store</b>	<p>The public safety community users can discover, browse, download, and rate the public safety application.</p> <p>Different types of applications are available on the FirstNet App Store.</p> <p>Device only – Downloadable application Client (Device) and Server Based application. Server based application</p>	<p>HTML pages and JSON data (json.org) OpenData framework W3C – CORS and JSONP. SOAP or RESTful using WSDL, JSON, XML. Or industry standard best practice software methods</p>

#### 4.2.6 Application Developers

Table 7 Application Developers Standards

Service Area	Description	Mandatory Standard and Source Document
<b>App Developers</b>	<p>Third party public safety developers can access, register, develop and test the application on FirstNet Sandbox environment.</p>	<p>SDK, API and development tools available..</p>

#### 4.2.7 Federated Identity Management

Table 8 Federated Identity Management Standards

Service Area	Description	Mandatory Standard and Source Document
<b>Federation of ICAM</b>	<p>Access to the external database</p> <p>The hosted application or application in the cloud services will use the identity federation.</p> <p>PSE shall authenticate, authorize the local agency services/applications for visited PS users. The PSE also has its own legacy access to federal data or Big data directly.</p>	<p>SAML and Open ID Connect are some of the federated identity protocols that the ICAM framework uses.</p>

#### 4.2.8 Cloud Services and Applications

The contractor(s) shall provide cloud services and its associated services and applications further detailed in Table 9 Cloud Services and Applications Standards.

Table 9 Cloud Services and Applications Standards

Service Area	Description	Mandatory Standard and Source Document
<b>APIs for Cloud Services</b>	APIs useful for local applications used by PSE for SaaS, PaaS, IaaS capability.	SOAP or RESTful using WSDL, JSON, XML. Or industry standard best practice software methods
<b>Application Hosting or Service Subscription</b>	Small PSE providers can use for their application hosting or Big Data Analytics, identity service subscription.	SOAP or RESTful using WSDL, JSON, XML. Or industry standard best practice software methods

## 5 Public Safety Entity (PSE)

This section provides two views of the interface between FirstNet's core network and a Public Safety Enterprise Network (PSEN):

- SV-1: a systems/services interface view identifying all interfaces needed
- StdV-1: a technical standards description of each of the identified interfaces at IOC 1

The specification defines the interface and relevant standards between the PSE and FirstNet domains enabling secure access by first responders to the databases and applications that are hosted by the PSE.

### 5.1 SV-1 PSE

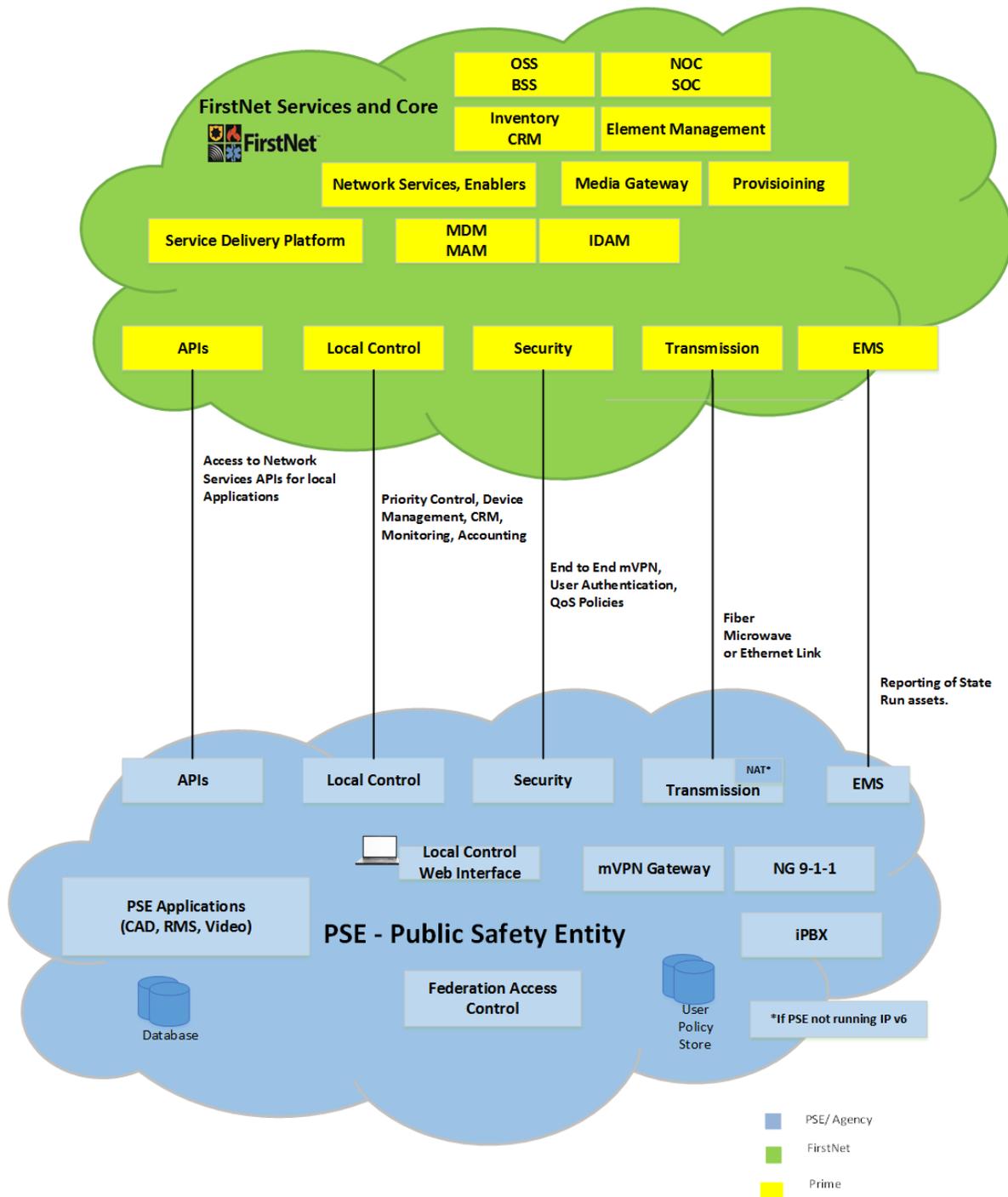


Figure 6 SV-1 PSE

## 5.2 StdV-1 PSE

### 5.2.1 Transmission

Contractor shall ensure that the transmission links between a PSE and FirstNet are redundant and geographically diverse transmission facilities. The transmission facilities can be provided by one or more service providers. The connections at a single datacenter and the equipment racks must be physically diverse and must have at least 25 feet of separation. Some PSEs will have two datacenters that are already set up as redundant datacenters. In this instance, each datacenter can connect with a single link into separate physically diverse FirstNet core nodes.

**Table 10 StdV-1 PSE: Transmission**

Item	Mandatory Standard and Source Document
<b>Physical Layer (1)</b>	Fiber, microwave Bandwidth specified based on PSE needs.
<b>Data Link Layer (2)</b>	Ethernet CIR <sup>1</sup> Firewall Policy Implementation (Port, QoS mapping) MAC address/VLAN <sup>2</sup>
<b>Network Layer (3)</b>	MPLS (Domain and Label Switching) Trusted vs Untrusted Network Diffserv DSCP IPv6 (responsibility of PSE to provide NAT, if necessary)

### 5.2.2 Security

First responders require secure, reliable, remote access to their PSEN databases and applications. Contractor shall employ end-to-end mobile VPN that supports Federal Information Processing Standards Publication (FIPS) 140-2, Security Requirements for Cryptographic Modules, compliant encryption, and two-factor authentication. The interface must also support federated access to local databases and applications (under the control of the local administrator) for visiting first responders working outside of their jurisdiction.

**Table 11 StdV-1 PSE: Security**

Item	Description	Mandatory Standard and Source Document
<b>Certificates</b>	Identification of endpoints, users, and devices	PKI X.509 v3
<b>Mobile VPN<sup>3</sup></b>	End-to-end (device to PSEN) encryption of data in transit	FIPS140-2, levels 2 and 3 (Suite B)
	Authentication of users	Radius/ PKI for smartcards, user certificates (such as PIV-I) and biometric systems. Radius-EAP protocol with Active Directory.
	QoS and access policies	Web interface/ HTTP(S)

<sup>1</sup> CIR: Committed Information Rate

<sup>2</sup> Separate VLANs for Element Management System, local control, and applications traffic on firewall.

<sup>3</sup> Must employ compatible mVPN client on devices with over-the-air updates.

### 5.2.3 Element Management System

Contractor shall ensure that reporting of the health of network elements is reported back to the Element Management System for the FirstNet Network Operations Center (NOC) using the following interfaces:

**Table 12 StdV-1 PSE: Element Management System**

Service Area	Mandatory Standard and Source Document
<b>FCAPS</b>	SNMP v3, FTP, sftp

### 5.2.4 Local Control

Contractor shall utilize web interfaces, as noted below, to provision users, manage the devices and applications, view billing, and monitor the performance of the local network for the PSE. The description in Table 13 StdV-1 PSE: Local Control, below refers to some of the use case documents related to Devices, Local Control and Operations.

**Table 13 StdV-1 PSE: Local Control**

Service Area	Description	Mandatory Standard and Source Document
<b>Device Management (includes applications)</b>	Activate/ de-activate device Lock and wipe device Manage device applications Manage agency policies Inventory reporting Device log collection	Web interface/ HTTP(S) to multi-tenant OMA-DM v2.0 compliant system
<b>CRM</b>	User experience monitoring Integrated subscriber provisioning	Web interface/ HTTP(S)
<b>Monitoring, SLAs</b>	Dispatch view of coverage and faults Security monitoring FM, CM, PM logging and forensics <sup>4</sup> Maintenance request and approval	Web interface/ HTTP(S)
<b>Accounting</b>	Charging and billing views	Web interface/ HTTP(S)
<b>Priority and Quality of Service</b>	User priority provisioning CAD interface for priority control QoS Proxy for VPN and applications	Web portal access from FirstNet to the secured portal of PSE. (JSON,XML) Supports SSL, TLS

### 5.2.5 Applications

Information from application servers or databases hosted by the PSE can be in-application or browser-based. Some of the applications hosted by the PSE may take advantage of Application Program Interfaces (APIs) offered by the FirstNet's service delivery platform, for example, a CAD application prioritizing applications of some of the first responders of an agency during a local incident. The

<sup>4</sup> Fault, Configuration, and Performance Management

description in the Table below refers to some of the use case document related to Network Services, Devices, Local Control, and Operation

**Table 14 StdV-1 PSE: Applications**

Service Area	Description	Mandatory Standard and Source Document
<b>APIs</b>	APIs useful for local applications, for example, QPP.	SOAP or RESTful using WSDL, JSON, XML or industry standard best practice software methods.
<b>Home Web Page</b>	Local status information of incidents gathered from multiple sources	HTML pages and JSON data (json.org) OpenData framework W3C – CORS and JSONP

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

DRAFT

## 6 Device - Network

### 6.1 SV-1 Device -Network

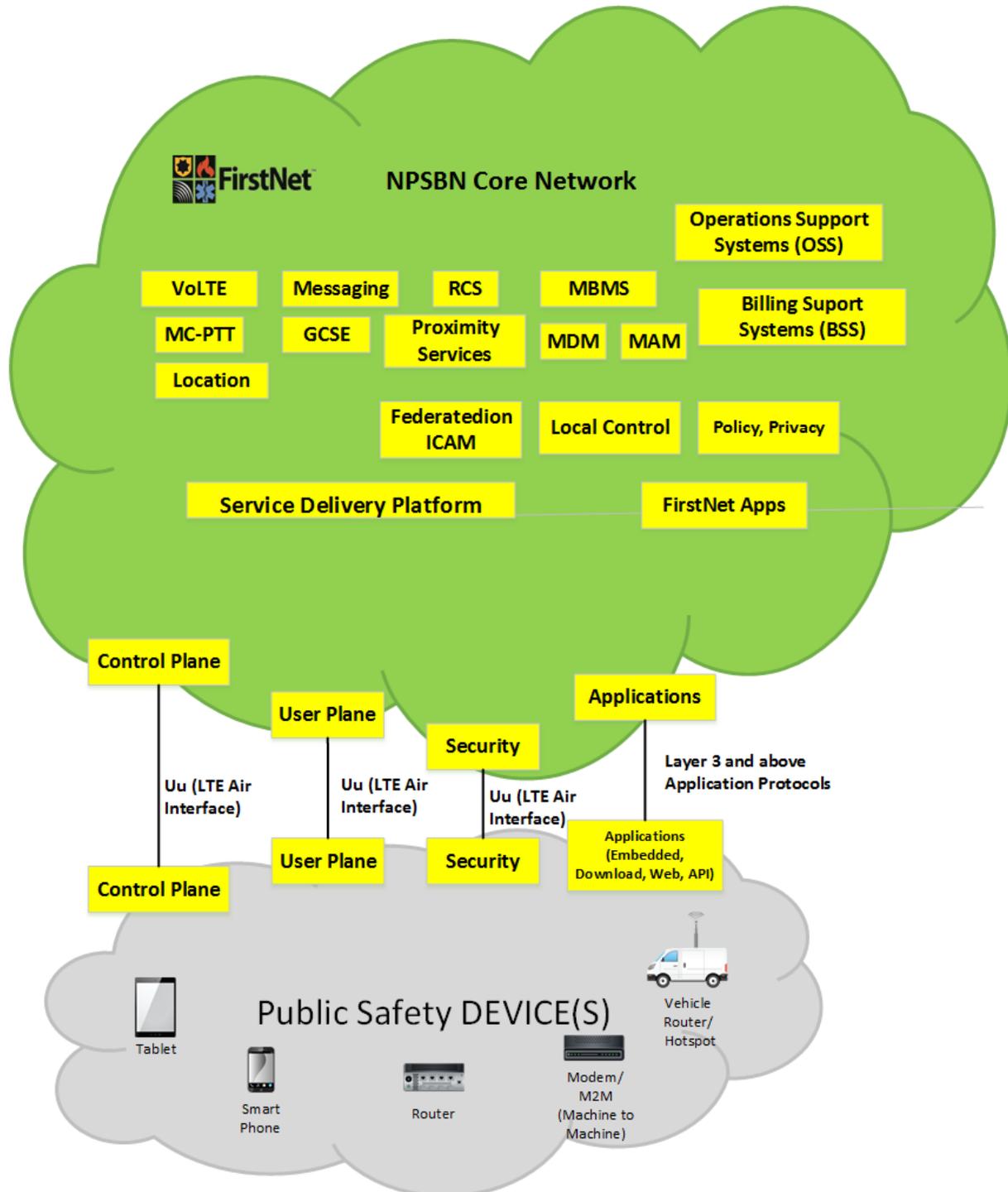


Figure 7 SV-1 Device: Network

## 6.2 StdV-1 Device Network

### 6.2.1 Air Interface

Table 15 Device Air Interfaces

Service Area	Subset	Mandatory Standard and Source Document
<b>Air Interface (Uu)</b>		3GPP TS 25.301, 3GPP TS 36.305, 3GPP TS 25.144, 3GPP 36.211
<b>Ub, Ua (Optional)</b>	Bootstrap Interface Network Application	3GPP TS 24.109

### 6.2.2 Embedded Clients/Applications

Table 16 Embedded Clients/Applications Mandatory Standards is a list of clients and applications that contain their own protocols. Contractor shall ensure their implementation in the NPSBN.

Table 16 Embedded Clients/Applications Mandatory Standards

Service Area	Subset	Mandatory Standard and Source Document
<b>VoLTE</b>	Voice/SIP	GSMA IR92/IR94
<b>RCS</b>	RCS 5.x	GSMA, RCS Device API
<b>SUPL</b>	Location	OMA-SUPL v2.0/3.0
<b>XDM</b>	Group List	OMA-XDM v2.0, 3GPP TS 24.167
<b>OMA-DM</b>	Device Management	OMA-DM v2.0
<b>GCSE</b>	Group Communications	3GPP TS 22.179, 3GPP 22.468
<b>MBMS</b>	Broadcast/Multicast	3GPP TS 23.246
<b>Proximity Services</b>	Voice/SIP	3GPP TS 23.703, Rel. 12
<b>MC-PTT</b>	Voice/SIP	3GPP TS 22.179

### 6.2.3 Downloadable Clients/Applications

Non-native

Table 17 Downloadable Clients and Applications

Service Area	Subset	Mandatory Standard and Source Document
<b>Software</b>	Software Development tools/Kits	REST, XML
<b>Identity</b>	SSO, Federation, User, device ID mapping	OASIS SAML 2.0, OpenID Connect No specification
<b>Tools</b>	Data collection across services and applications	No standard/specification
<b>HTTP</b>	Web-Based Client	W3C Specification