

Table of Contents

1	Document Overview.....	1
2	SV-1 NPSBN Interfaces.....	1
3	Devices Interface (Interface #1)	2
3.1	SV-1 Devices Interface (Interface #1)	3
3.2	StdV-1 Devices Interface (Interface #1)	3
3.3	StdV-2 Devices Interface Roadmap	5
4	RAN to Core Interface (Interface #2)	5
4.1	SV-1 RAN to Core Interface (Interface #2)	6
4.2	StdV-1 RAN to Core Interface (Interface #2)	6
4.3	StdV-2 RAN to Core Interface Roadmap	8
5	Roaming Interface (Interface #3)	8
5.1	SV-1 Roaming Interface (Interface #3).....	9
5.2	StdV-1 Roaming Interface (Interface #3)	9
5.3	StdV-2 Roaming Interface Roadmap.....	11
6	MVNO Interface (Interface #4).....	11
6.1	SV-1 MVNO Interface (Interface #4).....	11
6.2	StdV-1 MVNO Interface (Interface #4)	12
6.3	StdV-2 MVNO Interface Roadmap	13
7	PSTN/ISP Interface (Interface #5).....	13
7.1	SV-1 PSTN/ISP Interface (Interface #5).....	13
7.2	StdV-1 PSTN/ISP Interface (Interface #5).....	14
7.3	StdV-2 PSTN/ISP Interface Roadmap.....	15
8	Applications Ecosystem Interface (Interface #6)	15
8.1	SV-1 Applications Ecosystem Interface (Interface #6).....	16
8.2	StdV-1 Applications Ecosystem Interface (Interface #6)	16
8.3	StdV-2 Applications Ecosystem Interface Roadmap.....	18
9	Public Safety Enterprise Network Interface (Interface #7)	19
9.1	SV-1 Public Safety Enterprise Network Interface (Interface #7)	19
9.2	StdV-1 Public Safety Enterprise Network Interface (Interface #7)	19
9.3	StdV-2 Public Safety Enterprise Network Interface Roadmap.....	22

List of Figures

Figure 1 SV-1 NPSBN Interfaces	2
Figure 2 SV-1 Devices	3
Figure 3 SV-1 RAN(s) to Core	6
Figure 4 SV-1 Roaming Services	9
Figure 5 SV-1 MVNO	12
Figure 6 SV-1 PSTN/ISP	14
Figure 7 SV-1 Applications Ecosystem	16
Figure 8 SV-1 PSEN	19

List of Tables

Table 1 StdV-1 Devices Interface Specifications	4
Table 2 StdV-1 RAN(s) to Core Interface Specifications.....	7
Table 3 StdV-1 Roaming Interface Specifications	9
Table 4 StdV-1 MVNO Interface Specifications.....	12
Table 5 StdV-1 PSTN/ISP Interface Specifications.....	14
Table 6 StdV-1 Applications Ecosystem Interface Specifications	17
Table 7 StdV-1 PSEN Interface Specifications	20
Table 8 StdV-2 PSEN Application and Service Extension Interface Specifications.....	22

1 Document Overview

This document provides views of the interfaces between the First Responder Network Authority's (FirstNet) Core network and other external networks, including each interface's associated technical description, interface standards, and future interface standards required to meet the Final Operational Capability (FOC) milestones that the Contractor will implement as part of its Nationwide Public Safety Broadband Network (NPSBN) offering.

The document details the external interfaces and their relevant standards and specifications necessary for the implementation of the NPSBN. The following interfaces are:

1. Devices Interface
2. Radio Access Network (RAN) (FirstNet- and State-Deployed RANs) to Core Interface
3. Roaming Interface
4. Mobile Virtual Network Operator (MVNO) Interface (if applicable)
5. Public Switched Telephone Network (PSTN)/Internet Service Provider (ISP) Interface
6. Applications Ecosystem Interface
7. Public Safety Enterprise Network Interface

Each interface is described across five planes—transmission, control, security, user, and management. Each plane is a logical or physical layer associated with the overall network architecture, and each carries a different type of traffic.

1. Transmission Plane is the transmission L1 and L2 physical link and data link
2. Control Plane carries signaling, channel control, and L3 routing traffic
3. Security Plane is security access and egress flow control traffic
4. User Plane carries the network user bearer traffic
5. Management Plane carries administrative and operational traffic

The interface sections within this document utilize the following three system and standard views between FirstNet and other external networks:

- **SV-1** – A systems, components, services interface view identifying all interfaces needed during Initial Operational Capability (IOC) through FOC milestones
- **StdV-1** – A technical standards description of each of the identified interfaces during IOC
- **StdV-2** – A technical standards description of each of the identified additional interfaces required at FOC.

These views are not exhaustive and are used as a guideline for the Contractor to identify all standards that are relevant on an interface. The objective is for the Contractor to utilize standard interfaces.

2 SV-1 NPSBN Interfaces

SV-1 (systems view) provides at a high level the NPSBN and its systems/view interfaces. Interface #1 spans both state and commercial RANs to interoperate with the many different types of devices. Interface #2 is a 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) standards-based interface within the network between the Contractor's Core and any RAN. Interfaces #3, #4, and #5 are

3GPP LTE standards-based interfaces with external networks such as MVNOs, roaming partners, and connections for PSTN and ISP access. Interface #6 is with third-party application providers and developers, and interface #7 is with Public Safety Enterprise Networks (PSENs) hosting their local applications and management functions. The interfaces described within this attachment are not an exhaustive list or complete description. Colors are used to identify the organizational owner of a given function:

- **Green** – FirstNet
- **Blue** – PSEN/Local Agency
- **Yellow** – FirstNet Contractor
- **Gray** – Contractor’s roaming partners or integrators

The Contractor shall comply with the current or the latest version of the standard specification specified in the tables contained herein.

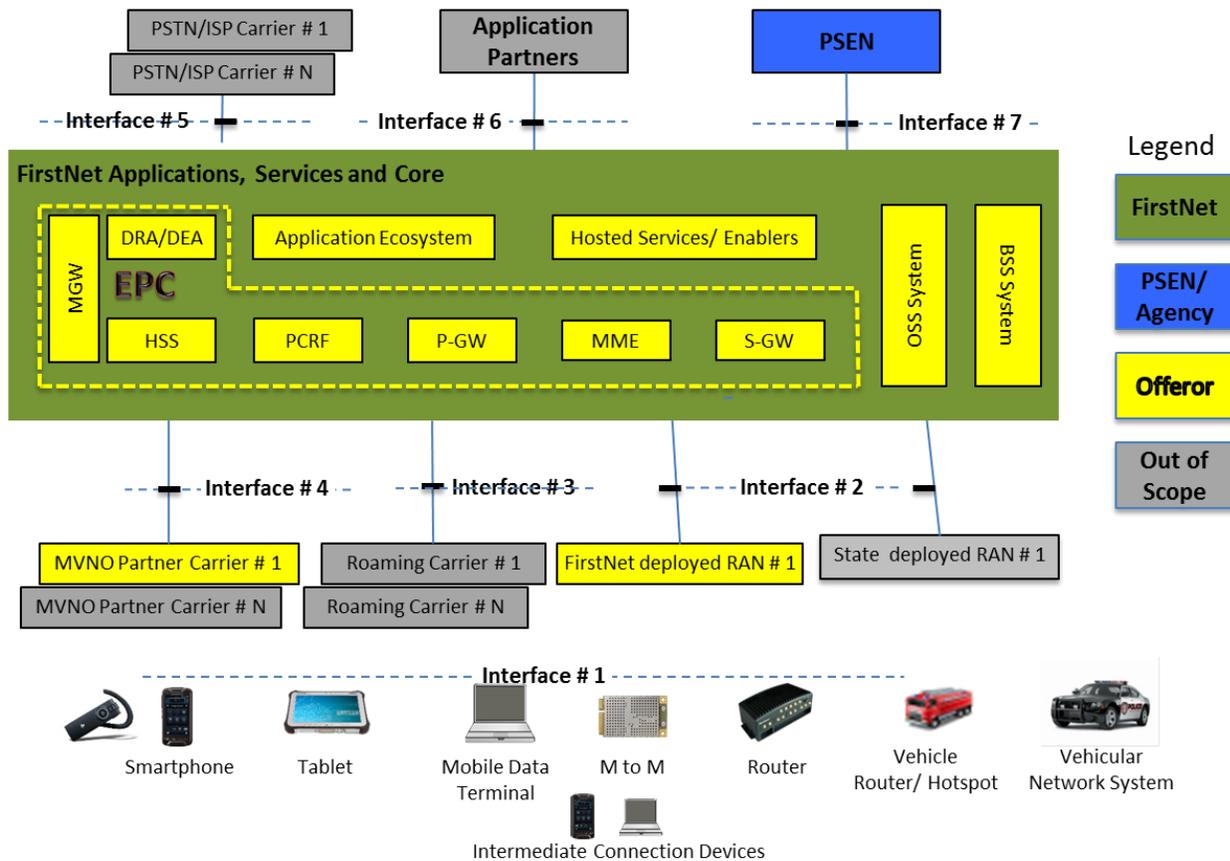


Figure 1 SV-1 NPSBN Interfaces

3 Devices Interface (Interface #1)

The device interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

The devices section covers the system and standard technical views for the interfaces between devices and the NPSBN.

3.1 SV-1 Devices Interface (Interface #1)

The following system view diagram depicts the devices interface.

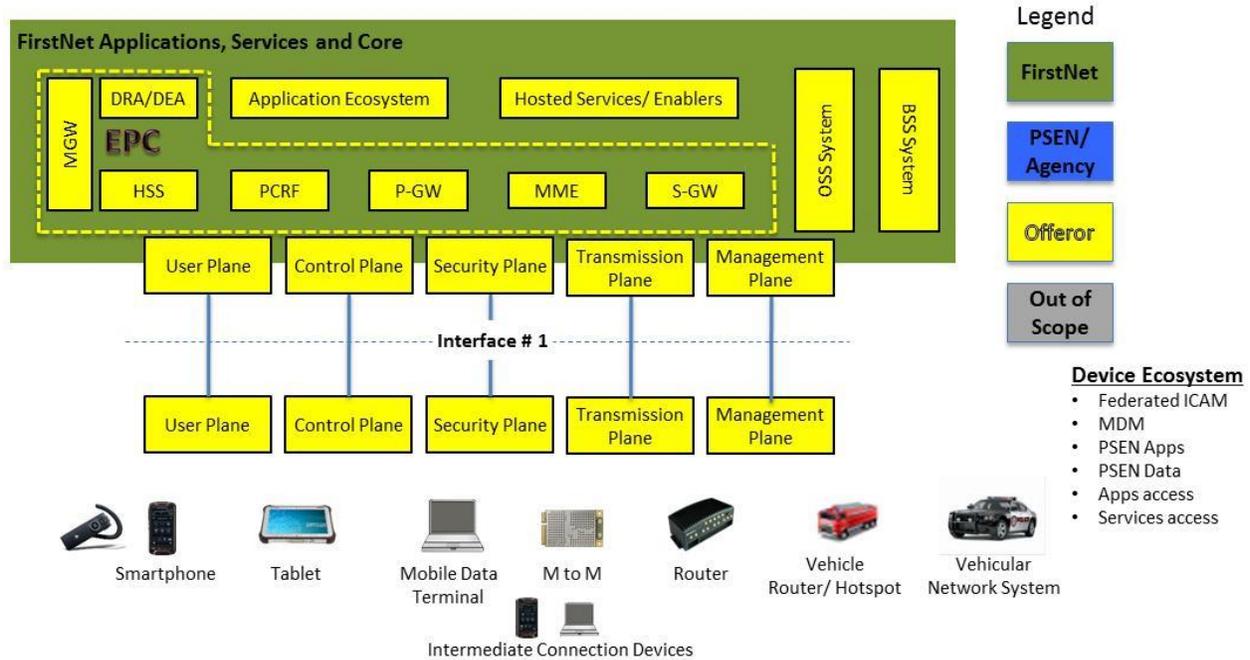


Figure 2 SV-1 Devices

3.2 StdV-1 Devices Interface (Interface #1)

This section defines system-level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on key device capabilities that will be available at IOC and are expected to be operational through FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

This section also covers the coverage and capacity interfaces between the RAN(s) and Core that are applicable to Vehicular Network Systems (VNS). The VNS platform includes the following major components:

- **In-Vehicle Router** – when the VNS is within terrestrial network coverage
- **Satellite modem and antenna** – once the VNS is fully outside of terrestrial network coverage, it can automatically fall back to the satellite modem from the terrestrial network modem(s)
- **Local Enhanced Node Base (eNodeB) station and antenna** – when the VNS is outside of LTE coverage the VNS can automatically act like a remote base station to other users
- **Local Evolved Packet Core (EPC) elements**

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 1 StdV-1 Devices Interface Specifications.

Table 1 StdV-1 Devices Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User, Control, Security, and Transmission	Uu	Utilize existing LTE standard interfaces including but not limited to 3GPP TS: 36.101, 36.104, 36.133, 36.141, 36.201, 36.211, 36.212, 36.213, 36.214, 36.305, 36.314, 36.321, 36.322, 36.323, 36.331, 33.303, 24.301, 24.334, 24.345, 25.301, 25.144, Utilize existing LTE standard interfaces including but not limited to ETSI TS: 102.671, 102.689, 102.690, 102.921
User	VoLTE	GSMA IR92/94
User	MC-PTT	3GPP TS 22.179, TS 23.779
User	eMBMS	3GPP TS 23.246
User	GSCE/SC-PTM	3GPP TS 22.179 3GPP TS 22.468 3GPP TS 36.890 SC-PTM TS 36.890
User	IOPS	3GPP TS 22.346
User	ProSe PC1: Applications to UE PC3: Core Function to UE PC5: UE - UE	3GPP TS 23.703 3GPP TS 23.713 3GPP TS 23.303 3GPP TS 24.333 3GPP TS 24.334 3GPP TS 36.843 3GPP TS 29.345
User	Locations Services	OMA-SUPL v2.0/3.0 OMA – API http://technical.openmobilealliance.org/Technical/technical-information/oma-api-program/oma-api-inventory GSMA OneAPI – http://www.gsma.com/oneapi/
User	Enhanced Messaging	GSMA RCS 5.x
User	Ethernet	100/1000 Mbps RJ45 (Intermediate cabled connection between router platforms to user devices)
User	Wi-Fi	IEEE 802.11 b/g/n 2.4GHz and 5GHz (Intermediate wireless connection between router and Wi-Fi hotspot platforms to user devices)
User	Bluetooth	Bluetooth 4.0 Low Energy (LE) + Enhanced Data Rate (EDR)
User	Satellite data connection	Industry standard satellite IP data connection (VNS satellite fallback for basic internet connectivity when out of cellular coverage.) (Refer to interface 2 information for satellite transmission connectivity SOW operational mode of the VNS platform)
Management	Device Management	OMA-DM v2.0

3.3 StdV-2 Devices Interface Roadmap

The Contractor shall comply with any future and evolving 3GPP standard interface specification requirements as well as transitioning any proprietary services to an industry standard based solution for any mission-critical service device extensions including:

- **Mission-critical video and data** – Mission-critical video and mission-critical data are 3GPP Release 14 features. Currently, use cases and requirements are being developed. The Contractors need to provide the mission-critical video and data services for the public safety operations. The services should utilize the functions in Group Communication System Enablers (GCSE), Proximity Services (ProSe), and Isolated E-UTRAN Operation for Public Safety (IOPS), and interwork with the Mission-Critical Push-to-Talk (MC-PTT) service.
- **MC-PTT enhancements** – The Contractor needs to incorporate enhanced features specified after 3GPP Release 13, including but not limited to priority, MC-PTT user and group identification, floor control, and group communications and management.
- **Group communications enhancements** – The Contractor needs to incorporate enhanced features specified after 3GPP Release 13, including but not limited to the enhancements to Single Cell Point-to-Multipoint (SC-PTM) transmission and Evolved Multimedia Broadcast Multicast Service (eMBMS) to allow flexible eMBMS bearers establishment, congestion handling, eMBMS roaming, and MC-PTT applications.
- **Proximity service enhancements** – The Contractor needs to incorporate enhanced features specified after 3GPP Release 13, including but not limited to the enhancements to system architecture, direct discovery, direction communication, relay, service authorization, EPC level discovery, LTE-WLAN direct communication, service continuity, and ProSe identity.
- **Location capabilities enhancements for indoor and outdoor emergency communications**

4 RAN to Core Interface (Interface #2)

The RAN to Core interface for both FirstNet-deployed RAN and state-deployed RAN interfaces will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

This section provides three views of the interface between FirstNet’s Core network and FirstNet-deployed RANs and state-deployed RANs.

This section covers the system view and the standards technical view for the coverage and capacity interfaces between the RAN(s) and Core that are applicable to both FirstNet and state-deployed RAN states and territories. Element or entity diagrams are logical and FirstNet equipment and responsibilities may be physically located within FirstNet-deployed RAN state borders.

4.1 SV-1 RAN to Core Interface (Interface #2)

The following system view diagram depicts the RAN(s) to Core interface.

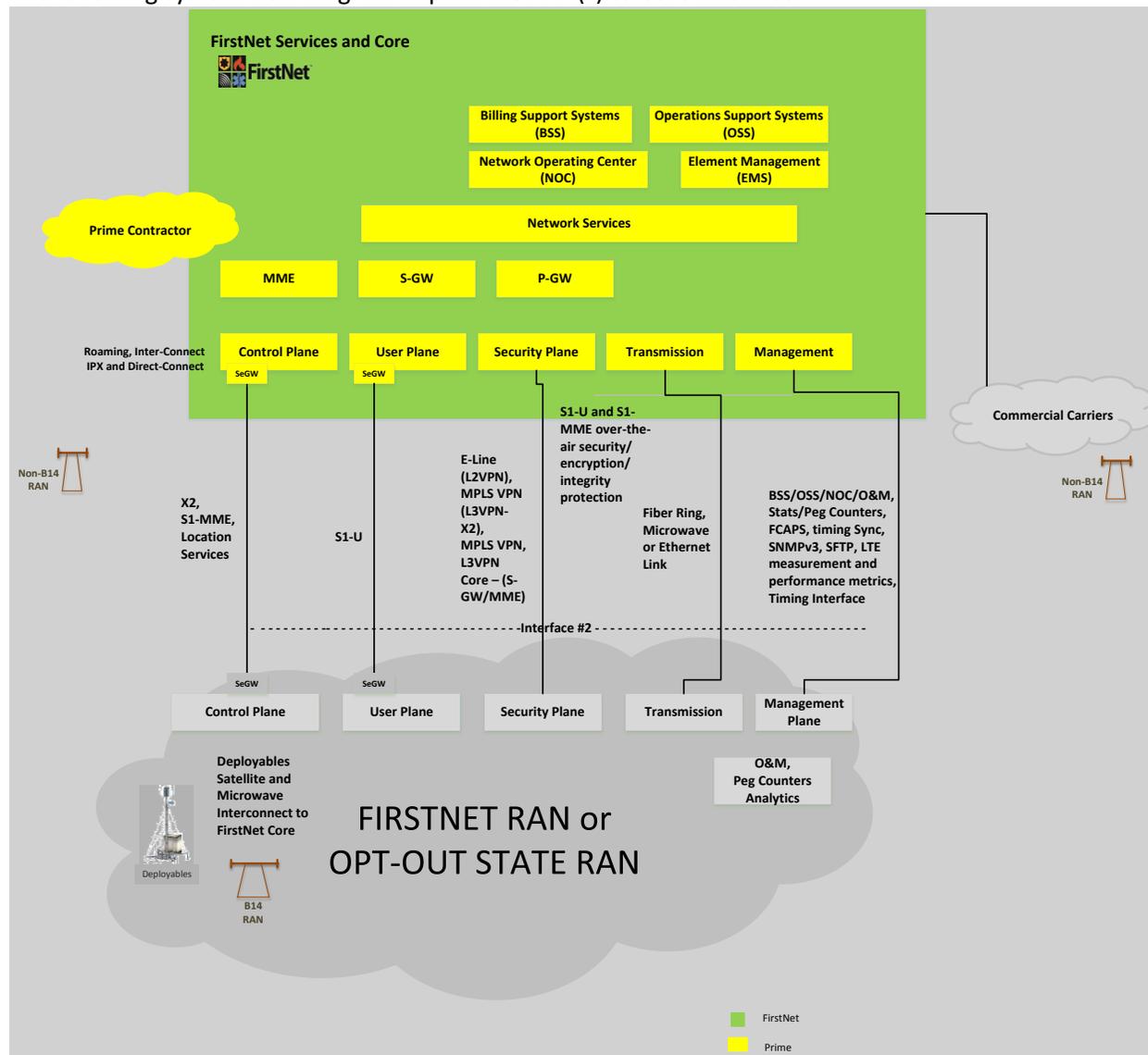


Figure 3 SV-1 RAN(s) to Core

4.2 StdV-1 RAN to Core Interface (Interface #2)

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 2 StdV-1 RAN(s) to Core Interface Specifications. FirstNet foresees that there will be a range of types of deployable units that connect to the FirstNet Core via Interface #2. FirstNet-deployed RANs will utilize, at a minimum, the same interface(s) as the state-deployed RAN interfaces listed below to be fully interoperable.

Table 2 StdV-1 RAN(s) to Core Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	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
User	Enhanced Messaging Location Services - LTE Positioning Protocol A (LPPa)	3GPP TS 23.271 3GPP TS 36.355 3GPP TS 36.305 3GPP TS 36.331 3GPP TS 36.455 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 v1.0, v2.0, v3.0 OMA-SUPCS v1.0
Control	S1-MME Interface X2	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 3GPP TS 36.420, 36.421, 36.422, 36.423, 36.424
Control	Timing Interface	GPS and external 2.048 MHz synchronization and transmission synchronization. The transmission synchronization includes Synchronous Ethernet (SyncE) from ITU G.8262, and Timing over Packet (IEEE 1588). eICIC, CoMP requires +/- 1.5 to 5 μs. ITU-T G.8272 defines requirements for a Primary Reference Time Clock (PRTC).

Service Area (Plane)	Description	Standard and Source Document
Security	IPSec S1 –U Security/Encryption S1- MME Security/Encryption L3VPN	RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP 3GPP 33.210 3GPP 33.310 Section J, Attachment J-10, Cybersecurity
Transmission	Terrestrial or Deployable Copper, Microwave, Fiber, Satellite utilizing standard IP connectivity to (MME, S/P-GW)	Industry standard best practice
Management	LTE measurements and performance metrics Terrestrial or Deployable Copper, Microwave, Fiber, Satellite utilizing standard IP connectivity to (MME, S/P-GW)	Industry standard best practice
Management	SLA Management Performance and Audit Monitoring LTE measurements and performance metrics	3GPP 36.214, 36.314, 36.133, and 32.425
Management	SLA Management Performance and Audit Monitoring EMS to NMS	Industry standard best practice SNMP v3 – RFC 2571 Architecture for SNMP Frameworks, RFC 3411 User- based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) SFTP

4.3 StdV-2 RAN to Core Interface Roadmap

The RAN to Core interface (Interface #2) at FOC shall be compliant with the then-current 3GPP release standards.

5 Roaming Interface (Interface #3)

The roaming interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

This section defines the system view, functionality, and standards that are expected to be deployed during IOC and available at FOC for the Core network. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

This section provides three views of the interface between FirstNet’s Core network and roaming partners.

5.1 SV-1 Roaming Interface (Interface #3)

The following system view diagram depicts the roaming interface.

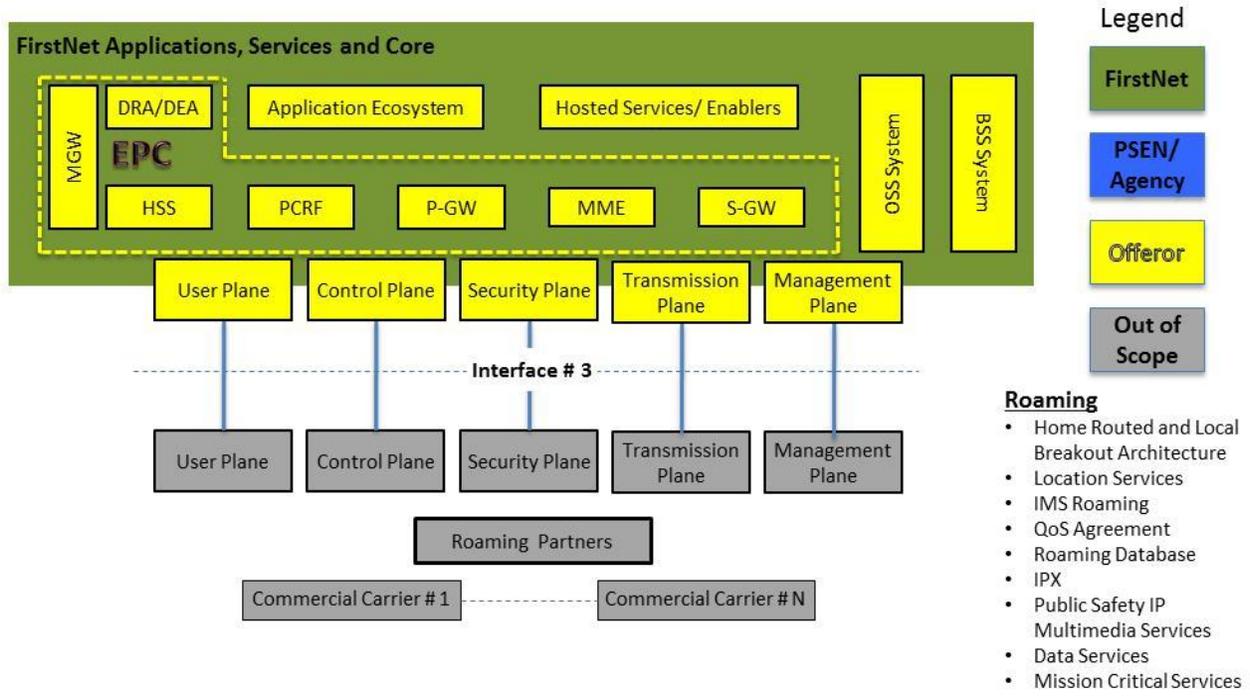


Figure 4 SV-1 Roaming Services

5.2 StdV-1 Roaming Interface (Interface #3)

This section defines system-level interfaces, functionality, and standards that are expected to be deployed during IOC and available at FOC. The focus is on key roaming capabilities that will be available at IOC and are expected to be operational through FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 3 StdV-1 Roaming Interface Specifications.

Table 3 StdV-1 Roaming Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	S8, GTPv1-U	3GPP TS 29.281 [32]
User	IMS Emergency Session	3GPP TS 23.167
User	IMS Profile for Voice and SMS	GSMA IR92
User	Locations Services, RLP	3GPP TS 23.271 OMA-TS-RLP-V1_2-20120529-C

Service Area (Plane)	Description	Standard and Source Document
Control	S8, GTPv2-C	3G PP TS 29.274 [31]
Control	Roaming Architecture	GSMA IR.88 [53]
Control	Local Breakout Architecture	GSMA IR.88 [53]
Control	QoS Control	3GPP TS 23.203
Control	DNS/ENUM	3GPP TS 29.303, GSMA PRD IR.67 [52]
Control	DRA/DEA	Defined by IETF RFC 3588 [59] and utilized by GSMA PRD IR.88 [53]
Control	IMS Roaming, Ici/Izi	3GPP TS 29.165 [24], GSMA PRD IR.65
Control	S9	3GPP TS 23.203
Control	Stream Control Transmission Protocol	IETF RFC 4960
Control	S6a, Diameter	3GPP TS 29.272 [30], IETF RFC 3588/3589
Control	Numbering, Addressing, and Identification	3GPP TS 23.003
Control	EPC Architecture	3GPP TS 23.401
Control	Network Architecture	3GPP TS 23.002 [1]
Security	Security Architecture	3GPP TS 33.401 Section J, Attachment J-10, Cybersecurity
Security	IP Network Layer Security	3GPP TS 33.210
Security	IKE with certificates	3GPP TS 33.310
Security	IPSec, Firewall	RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP RFC 4301- Firewall Enhancement Protocol (FEP)
Security	Inter-operator IP Backbone Security Requirements	GSMA IR.77
Security	Roaming Guidelines	GSMA IR.88
Transmission	Standard IP connectivity	Industry standard best practice (Public peering, private peering, or point-to-point connections utilizing Ethernet, VPLS, MPLS, based routing options with appropriate security measures and redundancy to meet objectives)
Transmission	IPX - Secure Roaming / interworking network	GSMA IR.34
Management	Telecommunications Management	3GPP TS 32.101, 3GPP TS 32.102, GSMA IR.88, 3GPP TS 103.260 Part 1 3GPP TS 103.260 Part 2
Management	Roaming Database	GSMA IR.21

Service Area (Plane)	Description	Standard and Source Document
Management	Roaming Charging Aspect	3GPP TS 32.849
Management	Policy and Charging Control	3GPP TS 29.212, 3GPP TS 29.214, 3GPP TS 29.215
Management	SNMP v3 Architecture User-based Security Model for SNMPv3	RFC 2571 RFC 3411 Best practice industry standard specifications for operational support

5.3 StdV-2 Roaming Interface Roadmap

The Contractor shall comply with any future and evolving 3GPP standard interface specification requirements as well as transitioning any proprietary services to an industry standard based solution for any roaming services including these specific public safety mission-critical services:

- Mission-critical video and data
- MC-PTT
- Group communications
- Proximity service
- Enhance location capabilities for indoor and outdoor emergency communications

6 MVNO Interface (Interface #4)

This interface applies if a Contractor proposes to include any MVNO functionality. MVNO interfaces will support existing service, feature, and applications as specified in 3GPP releases in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline for all user, control, security, transmission, and management planes.

When using an MVNO, the NPSBN will maintain its core network, service platforms, Operational Support Systems (OSS), and Business Support Systems (BSS), as well as have its own International Mobile Subscriber Identity (IMSI) codes, Subscriber Identity Module (SIM) cards, numbering space and interconnections. The Contractor will work with FirstNet to innovate and develop leading-edge public safety services and maintain full control of its policies and charging. The NPSBN will interface with its host Mobile Network Operator (MNO) using well-defined standard interfaces in a pseudo-roaming scenario, allowing it to connect to multiple MNOs through the discovery and selection process. In this situation, the NPSBN will operate effectively like a MNO without its own RAN.

6.1 SV-1 MVNO Interface (Interface #4)

The following system view diagram depicts the MVNO interface.

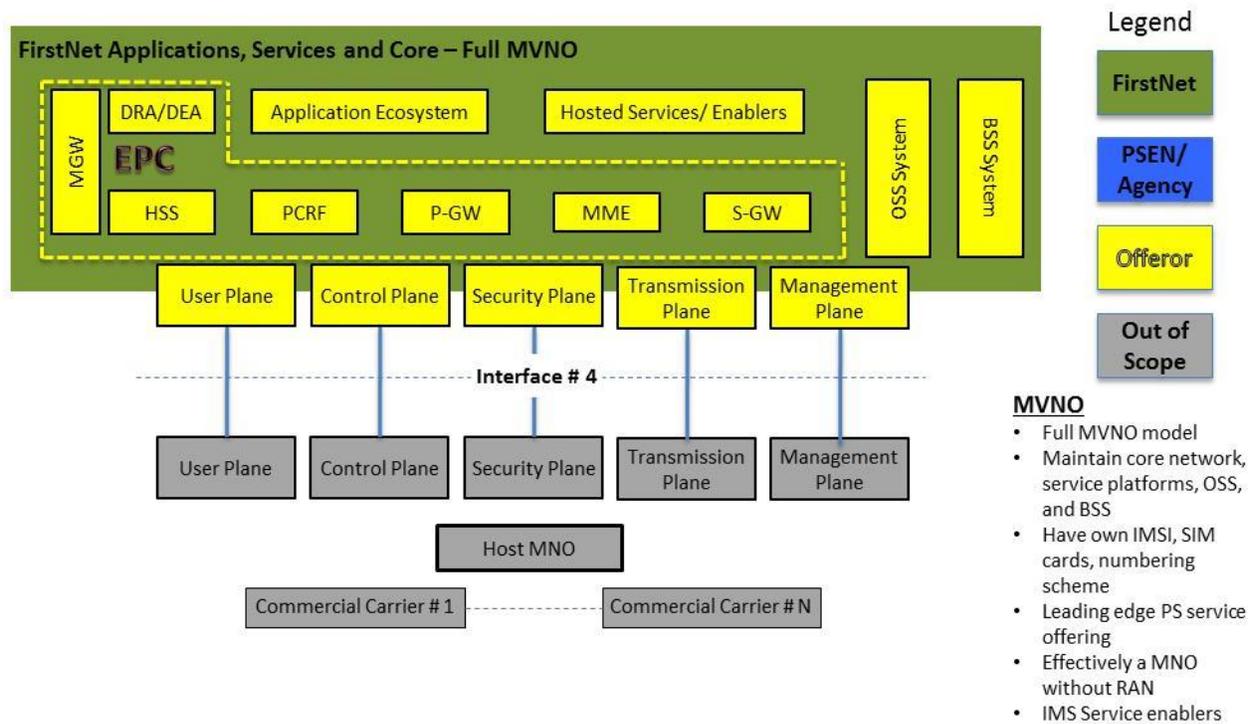


Figure 5 SV-1 MVNO

6.2 StdV-1 MVNO Interface (Interface #4)

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in MVNO Interface Specifications in Table 4 StdV-1 MVNO Interface Specifications. MVNO interfaces will utilize existing service, feature and application interfaces as specified in up to and including 3GPP Releases 13 in accordance with IOC/FOC for all user, control, security, transmission, and management planes.

This section defines system level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on key MVNO capabilities that will be available at IOC and are expected to be operational through FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

Table 4 StdV-1 MVNO Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	S5/S8, GTPv1-U	3GPP TS 29.281
User	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

Service Area (Plane)	Description	Standard and Source Document
User	IMS Profile for Voice and SMS	GSMA IR92
User	Locations Services, RLP	3GPP TS 23.271 OMA-TS-RLP-V1_2-20120529-C
Control	S1-MME Interface X-2	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 3GPP TS 36.420, 36.421, 36.422, 36.423, 36.424
Control	Roaming Architecture	GSMA IR.88
Control	Local Breakout Architecture	GSMA IR.88
Control	QoS Control	3GPP TS 23.203
Control	DNS/ENUM	3GPP TS 29.303, GSMA PRD IR.67
Control	DRA/DEA	defined by IETF RFC 3588 and utilized by GSMA PRD IR.88,
Control	IMS Roaming, Ici/Izi	3GPP TS 29.165, GSMA PRD IR.65
Control	S9	3GPP TS 23.203
Control	Stream Control Transmission Protocol	IETF RFC 4960
Control	S6a, Diameter	3GPP TS 29.272, IETF RFC 3588/3589

6.3 StdV-2 MVNO Interface Roadmap

The Contractor shall comply with the mandatory standards interface specification requirements for the full MVNO model in providing mission-critical services, including:

- Mission-critical video and data
- MC-PTT
- Group communications
- Proximity service
- Enhance location capabilities for indoor and outdoor emergency communications

7 PSTN/ISP Interface (Interface #5)

The PSTN/ISP interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

7.1 SV-1 PSTN/ISP Interface (Interface #5)

The following system view diagram depicts the PSTN/ISP interface.

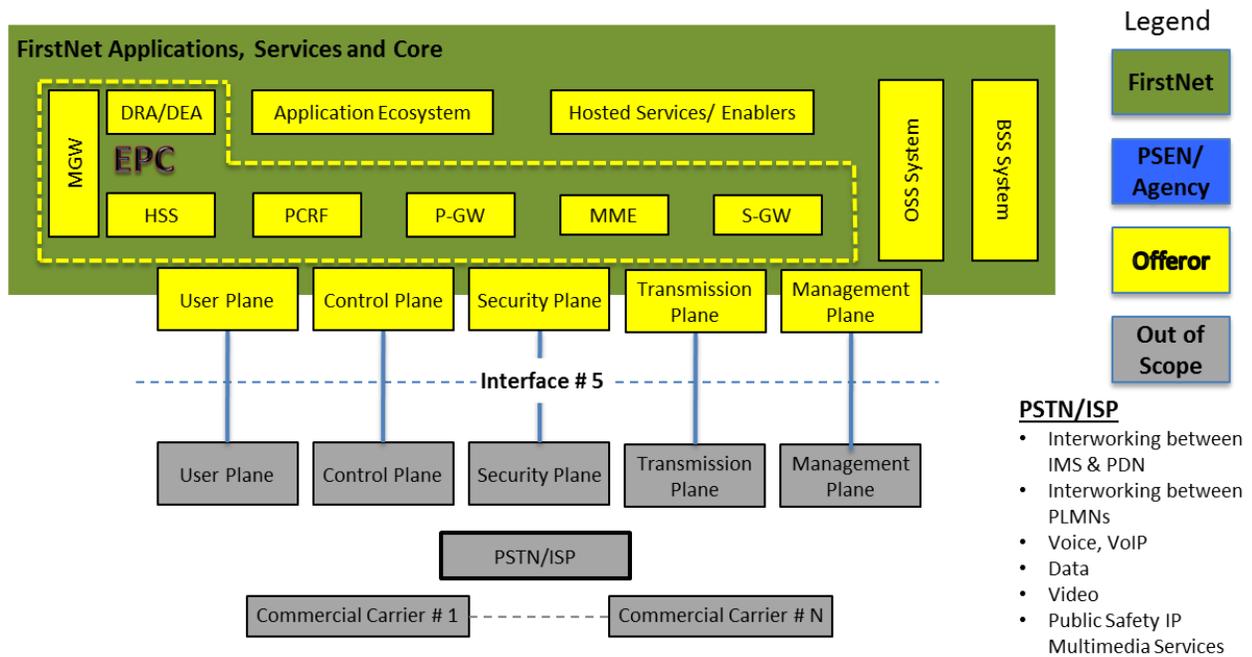


Figure 6 SV-1 PSTN/ISP

7.2 StdV-1 PSTN/ISP Interface (Interface #5)

This section defines system-level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on key PSTN/ISP interfaces that may not be available at IOC but are expected to be operational at FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 5 StdV-1 PSTN/ISP Interface Specifications.

Table 5 StdV-1 PSTN/ISP Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	S14 – ANDSF	3GPP TS 24.312
User	Sgi – Interworking between PLMN supporting PDN	3GPP TS 29.061
User	Pulse code modulation (PCM)	ITU-T Recommendation G.711
User	Packet switched conversational multimedia	3GPP TS 26.235
User	Mb – Interworking between the IMS and IP networks	3GPP TS 29.162

Service Area (Plane)	Description	Standard and Source Document
Control	Mb – Interworking between the IMS and IP networks	3GPP TS 29.162
Control	SIGTRAN	IETF RFC 2719
Control	Stream Control Transmission Protocol (SCTP)	IETF RFC 2960
Security	Security Architecture	Utilize existing 3GPP standard interfaces 3GPP TS 33.401
Security	IP Network Layer Security	Utilize existing 3GPP standard interfaces 3GPP TS 33.210
Security	Session Border Controller - based SIP Interconnection	Utilize existing 3GPP standard TS 29.238 and IETF RFC 5853
Security	IKE with certificates	Utilize existing 3GPP standard interfaces 3GPP TS 33.310
Security	IPSec, Firewall	RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP RFC 4301- Firewall Enhancement Protocol (FEP)
Transmission	Standard connectivity	Industry standard best practice with appropriate security measures and redundancy to meet objectives
Management	Telecommunications Management	Utilize existing 3GPP standard interfaces 3GPP TS 32.101, 3GPP TS 32.102, GSMA IR.88

7.3 StdV-2 PSTN/ISP Interface Roadmap

The Contractor shall comply with the standards in its PSTN/ISP Interface roadmap to support mission-critical communication services that are required in the FOC timeline:

- Mission-critical video and data
- MC-PTT enhancements
- ProSe enhancements
- GCSE enhancements
- Enhanced location services for indoor and outdoor emergency communications

8 Applications Ecosystem Interface (Interface #6)

The applications ecosystem interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

The key interfaces of the application ecosystem in the NPSBN are:

1. The public safety app developers, partners, and their applications
2. The device ecosystem and its applications
3. The Public Safety Entity, their network and the applications

The Contractor shall comply with the interface specification standard and security policies outlined in Section J, Attachment J-10, Cybersecurity, for the applications ecosystem.

8.1 SV-1 Applications Ecosystem Interface (Interface #6)

The following system view diagram depicts the applications ecosystem interface.

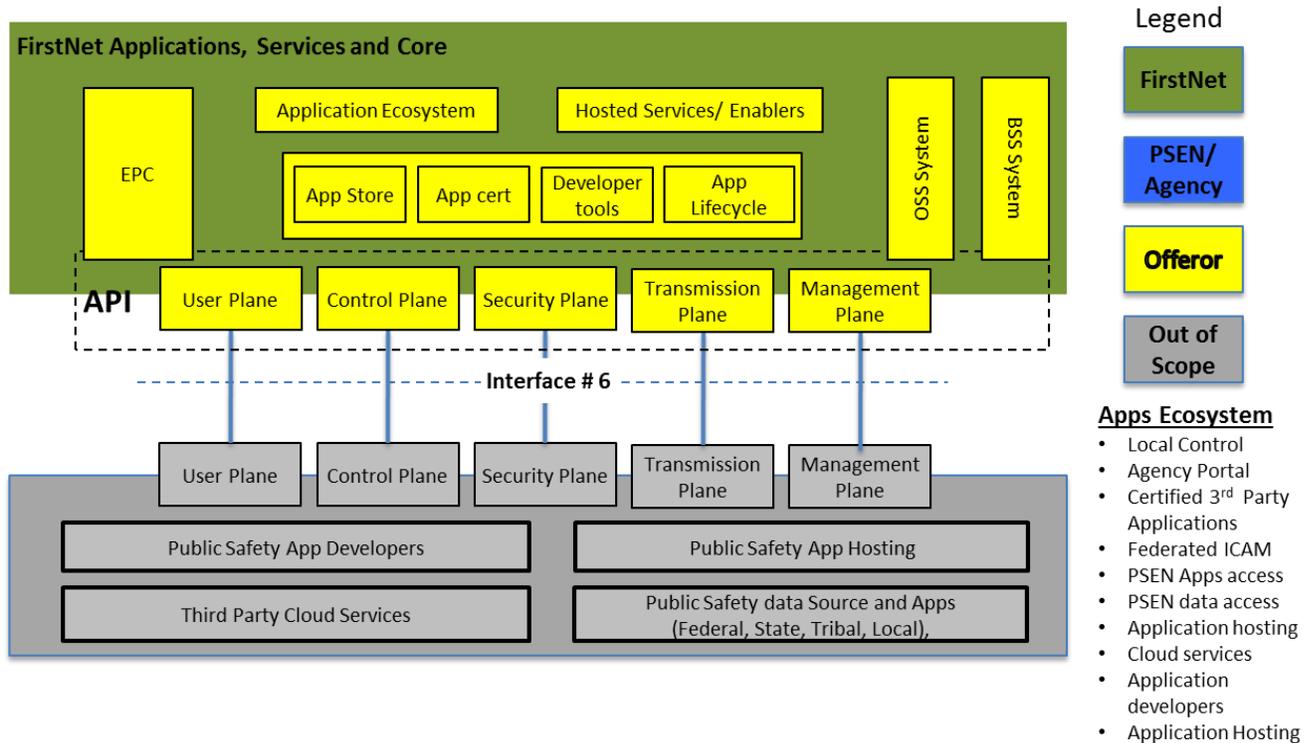


Figure 7 SV-1 Applications Ecosystem

8.2 StdV-1 Applications Ecosystem Interface (Interface #6)

The standards and the source document defined in the tables below for the interface provides minimum guidance to the Contractors.

The Contractor shall comply with the interface specification standard, security policy outlined in Section J, Attachment J-10, Cybersecurity, for the application ecosystem.

This section defines system-level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on application interfaces that may not be available at IOC but are expected to be operational at FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 6 StdV-1 Applications Ecosystem Interface Specifications.

Table 6 StdV-1 Applications Ecosystem Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	Federated ICAM Credentials and Credentialing. Authentication and SSO Authorization and ABAC	Utilize industry standard best practices. Some of the minimum Federated ICAM standards and best practice are: GFIPM: Global Federated Identity and Privilege Management NIEF: National Identity Exchange Federation FICAM: Federal Identity, Credential and Access Management SICAM: State Identity, Credential and Access Management. OASIS SAML 2.0 Open ID Connect (http://openid.net/connect/) Kantara Initiative (https://kantarainitiative.org/) NISTIR – 8014 ATIS-1000044.2011 ATIS-1000045.2012 FIPS 201-2 NIST SP 800-157 NIST SP 800-78-4 NIST SP 800-73-4 NIST SP 800-76-2 NIST SP 800-63-2 FIDO: Fast Identity Online NIST SP 800-79-2 NSIT SP 1800-3 (Draft)
User	Third-Party Apps (FirstNet-certified)	Utilize industry standard best practices.
User	Offeror-Provided App (Local Control, PSE home page)	Utilize industry standard best practices.
User	APIs	Utilize industry standard best practices for network, device, OSS, BSS, and cloud services.
User	App Store	Utilize industry standard best practices

Service Area (Plane)	Description	Standard and Source Document
User	App Developer App certification and tools. App Life-cycle	Utilize industry standard best practices. SDK, API, plugins, and development tools available for native, hybrid, web, desktop applications for all of the device types in the device ecosystem. OWASP NIST-SP-163 NIST NVD Static, Dynamic, Interactive analysis test tools for applications and its security (SAST, DAST, IAST) following industry standard best practice and methods Utilize industry standard best practices
User	App Security	Section J, Attachment J-10, Cybersecurity, app security guidelines. Utilize industry standard best practices.
User	ProSe PC1 – App server to UE PC2 – Core to App server	Utilize existing 3GPP standard interfaces or industry best practices. 3GPP TS 23.303 3GPP TS 24.333 3GPP TS 24.334 3GPP TS 36.843 3GPP TS 29.345
User	Locations Services Ir RLP	3GPP TS 23.271 OMA-TS-RLP-V1_2-20120529-C
Control	ICS and Rx	Utilize existing 3GPP standard interfaces or industry best practices
Security		Utilize existing 3GPP standard interfaces
Security	IPsec, Firewall	Section J, Attachment J-10, Cybersecurity RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP RFC 4301– Firewall Enhancement Protocol (FEP)
Security	Federated ICAM	Refer ICAM user plane standards related to security guidelines and utilize industry standard best practice.
Transmission		Utilize industry standard best practices
Management	Local Control System and component Management Tools	Utilize existing 3GPP standard interfaces or industry best practices Industry standard best practice for data collection

8.3 StdV-2 Applications Ecosystem Interface Roadmap

The applications ecosystem interface at FOC shall be compliant with the then-current 3GPP release standards.

9 Public Safety Enterprise Network Interface (Interface #7)

The PSEN interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

The specification defines the interface and relevant standards between a PSEN and FirstNet domains, enabling secure access by first responders to the databases, services, and applications that are hosted by the PSEN, as well as interworking with FirstNet functions, applications, and services.

FirstNet’s intent is not to be prescriptive in how the logical interfaces displayed are implemented. FirstNet’s intention is to work with the Contractor to solidify key PSEN interface requirements to ensure proper connectivity, services, application, security, and functionality objectives of each PSEN interface are met.

9.1 SV-1 Public Safety Enterprise Network Interface (Interface #7)

The following system view diagram depicts the PSEN interface.

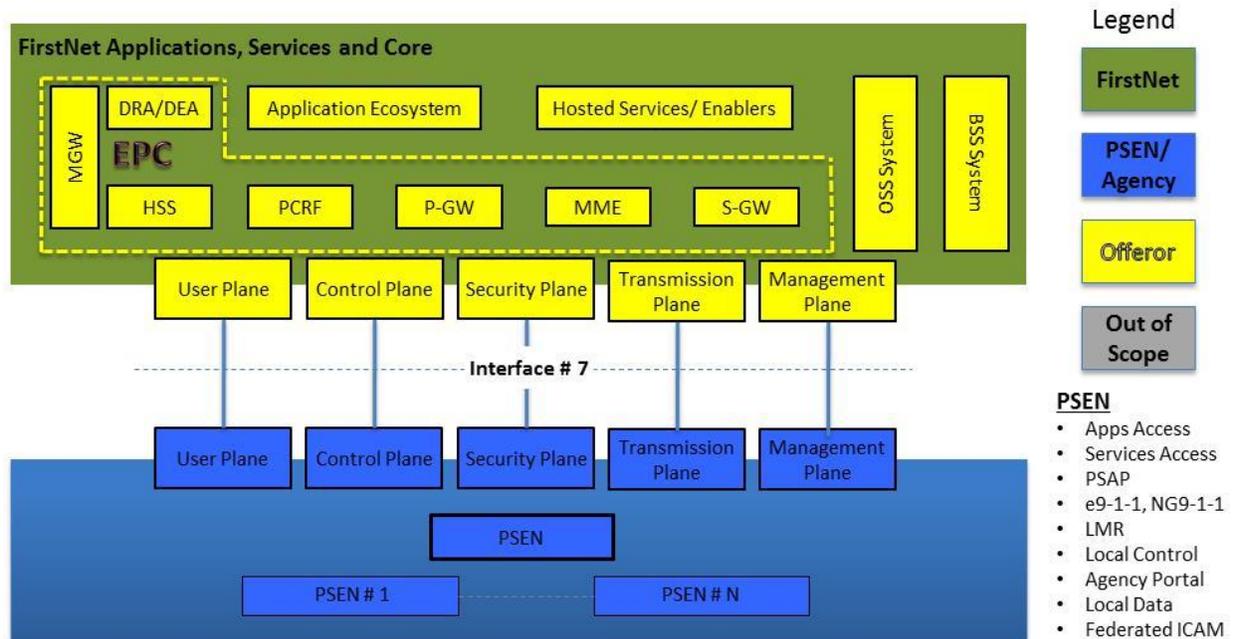


Figure 8 SV-1 PSEN

9.2 StdV-1 Public Safety Enterprise Network Interface (Interface #7)

This section defines system-level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on key PSEN capabilities that will be available at IOC and are expected to be operational through FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 7 StdV-1 PSEN Interface Specifications.

Table 7 StdV-1 PSEN Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	IMS peering for NG911 Multimedia Services	3GPP TS23.167, Emergency Services IP Network Design for NG9-1-1 Information Document (http://www.nena.org/?page=Standards)
User	Third Party Apps (FirstNet certified)	Utilize industry standard best practices.
User	App Security	Section J, Attachment J-10, Cybersecurity, app security guidelines. Utilize industry standard best practices.
User	Federated ICAM Credentials and Credentialing Authentication and SSO Authorization and ABAC	Utilize industry standard best practices. Some of the minimum Federated ICAM standards and best practice are: GFIPM: Global Federated Identity and Privilege Management NIEF: National Identity Exchange Federation FICAM: Federal Identity, Credential, and Access Management SICAM: State Identity, Credential, and Access Management. OASIS SAML 2.0 Open ID Connect Kantara initiative NISTIR – 8014 ATIS-1000044.2011 ATIS-1000045.2012 FIPS 201-2 NIST SP 800-157 NIST SP 800-78-4 NIST SP 800-73-4 NIST SP 800-76-2 NIST SP 800-63-2 FIDO: Fast Identity Online NIST SP 800-79-2 NSIT SP 1800-3 (Draft)
User	VoLTE	VoLTE IR.92 version 6?
User	MC-PTT	3GPP TS 22.179, TS 23.779
User	GSCE/SC-PTM	3GPP TS 22.179 3GPP TS 22.468 3GPP TS 36.890 SC-PTM TS 36.890

Service Area (Plane)	Description	Standard and Source Document
User	ProSe PC1: Applications to UE PC2: Core to App server	3GPP TS 23.703 3GPP TS 23.713 3GPP TS 23.303 3GPP TS 24.333 3GPP TS 24.334 3GPP TS 36.843 3GPP TS 29.345
User	Locations Services Ir RLP	3GPP TS 23.271 OMA-TS-RLP-V1_2-20120529-C
User	Enhanced Messaging	
Control		Utilize existing 3GPP standard interfaces
Control	Ici/Izi	3GPP TS 29.165 [24], GSMA PRD IR.65
Security	IPSec, Firewall	Section J, Attachment J-10, Cybersecurity RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP RFC 4301 – Firewall Enhancement Protocol (FEP) Firewall Policy Implementation (VPN) Utilize existing 3GPP standard interfaces TBD added security standards
Security	ICAM	FIPS140-2, levels 2 and 3 (Suite B)
Security	Authentication of users	SAML2.0 or Open ID Connect tokens Derived PIV-I, NIST SP 800-157
Security	Identification of endpoints, users, and devices	PKI X.509 v3 Radius/ PKI for smartcards, user certificates (such as PIV-I), tokens and biometric systems. Radius-EAP protocol with Active Directory
Transmission	Transmission Point of Presence (POP) for public and private peering and point to point circuits	Utilize existing 3GPP and industry standard interfaces for layers 1, 2 and 3 transmission connectivity such as fiber, copper, microwave and satellite, Ethernet, MPLS, VPLS and appropriate hardening and redundancy mechanisms to separate domains (BGP, OSPF, etc.) as well as isolate and eliminate data storms
Management	Local Control QoS and access policies for provisioning	Utilize existing 3GPP and industry standard interfaces or industry best practices such as Web interface/HTTP(S)
Management	Device Management (includes applications)	Utilize existing industry standard interfaces or industry best practices such as Web interface/HTTP(S) to multi-tenant OMA-DM v2.0 compliant system
Management	CRM	Utilize existing industry standard interfaces or industry best practices such as Web interface/HTTP(S)
Management	Monitoring, SLAs	Utilize existing industry standard interfaces or industry best practices such as Web interface/HTTP(S)

Service Area (Plane)	Description	Standard and Source Document
Management	Accounting	Utilize existing industry standard interfaces or industry best practices such as Web interface/ HTTP(S)
Management	Priority and Quality of Service	Utilize existing 3GPP standard interfaces or industry best practices, TLS
Management	FCAPS, ITIL, NGNMS	Utilize existing 3GPP standard interfaces or industry best practices such as RFC 3411 SNMP v3, FTP, sftp, 3GPP TS 32.102

9.3 StdV-2 Public Safety Enterprise Network Interface Roadmap

The PSEN interface roadmap is the technical standards description of each of the identified additional interfaces required at FOC. The standards described in the table shall meet the current general release version at the time of FOC (standards forecast Release 14 and other standards planned for IOC-4 to FOC time frame).

The following table lists any application and service extensions that may not be available during the IOC time frames. These may include such items as data sharing, computer-aided dispatch (CAD), location, NG9-1-1, and ESINet integration.

Table 8 StdV-2 PSEN Application and Service Extension Interface Specifications

Service Area	Subset	Standard and Source Document
User	CAD application	APCO and IJIS Institute on CAD minimum functional requirements for multi-functional, multi-discipline PSEN https://www.apcointl.org/doc/911-resources/apco-standards/584-11011-2015-multi-functional-multi-discipline-cad/file.html
User	NG9-1-1	Data apps sharing with FirstNet
User	ESINet	Data apps sharing with FirstNet
Security	ESINet	Section J, Attachment J-10, Cybersecurity Future cybersecurity standards
User	Information Sharing Environment (ISE)	DHS-ISE: Information Sharing Environment National Strategy for Information Sharing and Safeguarding (NSISS) https://www.ise.gov