



Appendix C-5

FirstNet FOC - Features

Standards Forecast

(StdV-2)

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

4/27/2015

Table of Contents

1	Document Overview	1
2	StdV-2 Features Roadmap	1
3	StdV-2 ProSe	1
4	StdV-2 Group Communication System Enablers (GCSE)	4
5	StdV-2 Enhanced Location Services	5
6	StdV-2 Multimedia Broadcast Multi-Cast Services	5
7	StdV-2 Identity Management	7
8	StdV-2 Public Safety Enterprise (PSEN)	10
8.1	Transmission	11
8.2	Security	11
8.3	Applications	11
8.4	Element Management System.....	12
9	StdV-2 Mobile Control Unit (MCU)	12
10	StdV-2 Data Sharing of Local Agencies	14

List of Figures

Figure 1	Proximity Services	2
Figure 2	StdV-2 for Group Communication System Enablers	4
Figure 3	StdV-2 Multimedia Broadcast Multi-Cast Services	6
Figure 4	StdV-2 PSE	10

List of Tables

Table 1	Proximity Services Mandatory Standards	3
Table 2	Group Communication System Enablers Mandatory Standards	5
Table 3	Multimedia Broadcast Multi-Cast Services Mandatory Standards (MBMS)	7
Table 4	Identity Management Mandatory Standards	9
Table 5	Transmission Mandatory Standards	11
Table 6	Security Mandatory Standards.....	11
Table 7	Applications Mandatory Standards.....	11
Table 8	Element Management System Mandatory Standards	12
Table 9	MCU Mandatory Standards.....	13
Table 10	Data Sharing for Local Agencies Standards.....	14

1 Document Overview

This document defines system level interfaces, functionality, and standards, which are expected at final operating capability (FOC). The focus is on key features that are not available at initial operating capability (IOC) but are expected to be operational at FOC. It also identifies those areas that may impact the interface between the Nationwide Public Safety Broadband Network (NPSBN) and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

2 StdV-2 Features Roadmap

The following are the features and functionalities that are required in the FOC timeline:

1. Proximity Services (ProSe)
2. Group Communication System Enablers (GCSE)
3. Enhanced Location Services eMBMS Services
4. Identity, Credential and Access Management (ICAM)
5. Public Safety Enterprise Network (PSEN)
6. Mobile Communications Unit (MCU)
7. Data Sharing of Local Agencies with FirstNet

3 StdV-2 ProSe

Direct Mode has been available for Land Mobile Radio (LMR) for years allowing first responders to be able to communicate with their nearby colleagues directly with no network and will be supported by the LTE components of ProSe and GCSE.

Public safety user equipment (UE) uses ProSe and GCSE to communicate with each other even though they belong to different Home Public Land Mobile Network (HPLMNs).

A public safety can automatically use ProSe when E-UTRAN coverage is not available, or the user can manually set the user equipment to use direct discovery and communication even when E-UTRAN coverage is available.

In addition, the following assumptions are made for public safety ProSe:

- All public safety users utilize ProSe-enabled UEs
- ProSe supports both UE discovery and UE communication

If UEs are in proximity to each other, they may be able to use a direct mode or locally-routed path.

For example, in 3GPP LTE spectrum, the operator can move the data path (user plane) off the access and core networks onto direct links between the UEs. This direct data path is shown in Figure 1 Proximity Services.

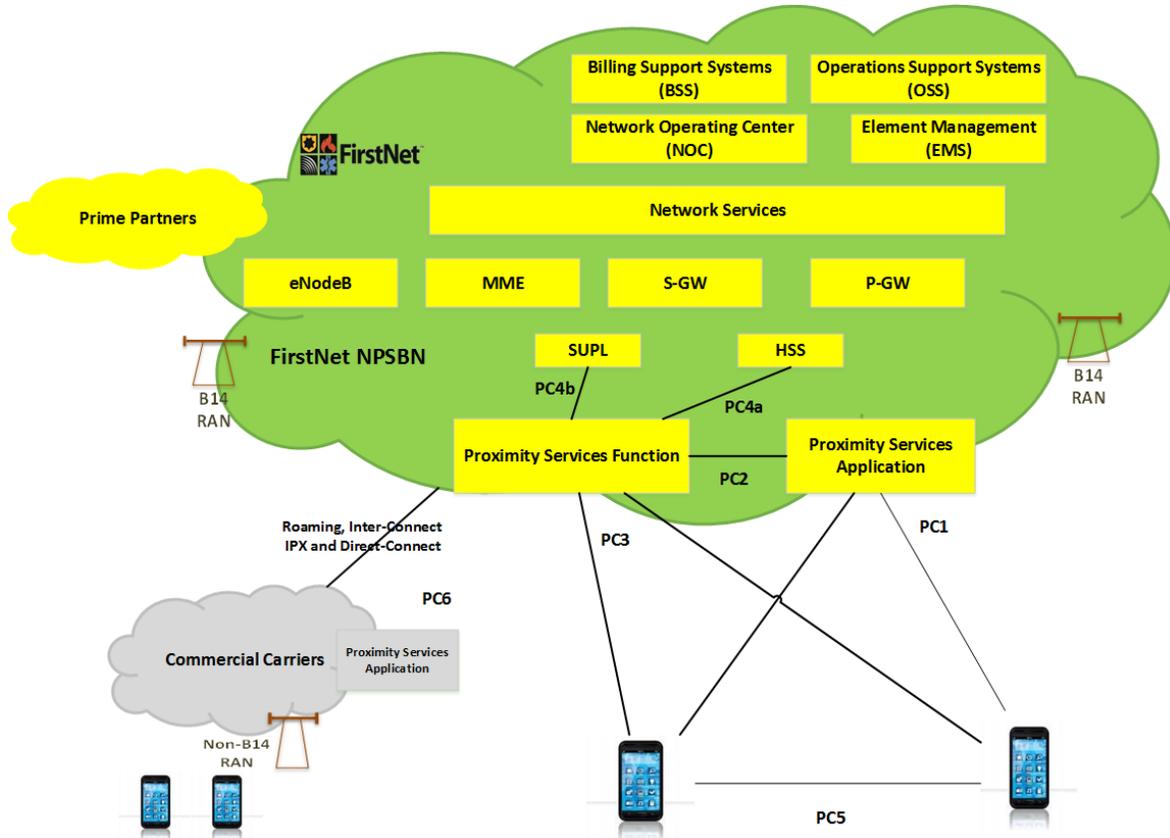


Figure 1 Proximity Services

DRAFT

Table 1 Proximity Services Mandatory Standards

Service Area	Description	Mandatory Standard Document
Proximity Services	ProSe Discovery: a process that identifies that a UE is in proximity of another, using E-UTRA.	
	ProSe Communication: a communication between two UEs in proximity by means of an E-UTRAN communication path established between the UEs. The communication path could for example be established directly between the UEs or routed via local eNB(s).	
	ProSe-enabled UE: a UE that supports ProSe Discovery and/or ProSe Communication. Unless explicitly stated otherwise in this TR, a UE refers to a ProSe-enabled UE.	SA1 <ul style="list-style-type: none"> • TR 22.803 “Feasibility study for ProSe” • TS 22.278 “Service requirements for the Evolved Packet System (EPS)” • TS 22.115 “Service aspects; Charging and billing” • TS 21.905 “Vocabulary for 3GPP Specifications”
	ProSe-enabled Network: a network that supports ProSe Discovery and/or ProSe Communication. Unless explicitly stated otherwise in this TR, a network refers to a ProSe-enabled network.	SA2 <ul style="list-style-type: none"> • TR 23.703 “Study on architecture enhancements to support ProSe (Release 12)” • TS 23.303 “ProSe based services; Stage 2 (Release 12)”
	Open ProSe Discovery: is ProSe Discovery without explicit permission from the UE being discovered.	SA3 <ul style="list-style-type: none"> • TR 33.833 “Study on security issues to support ProSe”
	ProSe Group Communication: a one-to-many ProSe Communication, between two or more UEs in proximity, by means of a common communication path established between the UEs.	RAN1 and RAN2 <ul style="list-style-type: none"> • TR 36.843 “Study on LTE Device to Device ProSe - Radio Aspects”
ProSe UE-to-Network Relay: is a form of relay in which a ProSe-enabled Public Safety UE acts as a communication relay between a ProSe-enabled Public Safety UE and the network using E-UTRA	CT1 <ul style="list-style-type: none"> • TS 24.333 “ProSe Management Object (MO)” • TS 24.334 “ProSe UE to ProSe Function aspects (PC3); Stage 3” 	

4 StdV-2 Group Communication System Enablers (GCSE)

Currently group communications are available on the LMR network and also non-mission critical Push to Talk (PTT) solution providers use group communication capability on wireless network (LTE, RevA) by using the Open Mobile Alliance (OMA) standards and proprietary application enablers.

The 3GPP specification describes how a Group Communications Service (GCS) Application Server (GCS AS) may use the enablers offered by the 3GPP system for providing a GCS. These enablers are denoted as GCSE.

IP Multimedia Subsystems (IMS) and OMA-XML Document Management Group services related to presence, voice over LTE (VoLTE) and other radio communications services for group are available at the 3GPP specification.

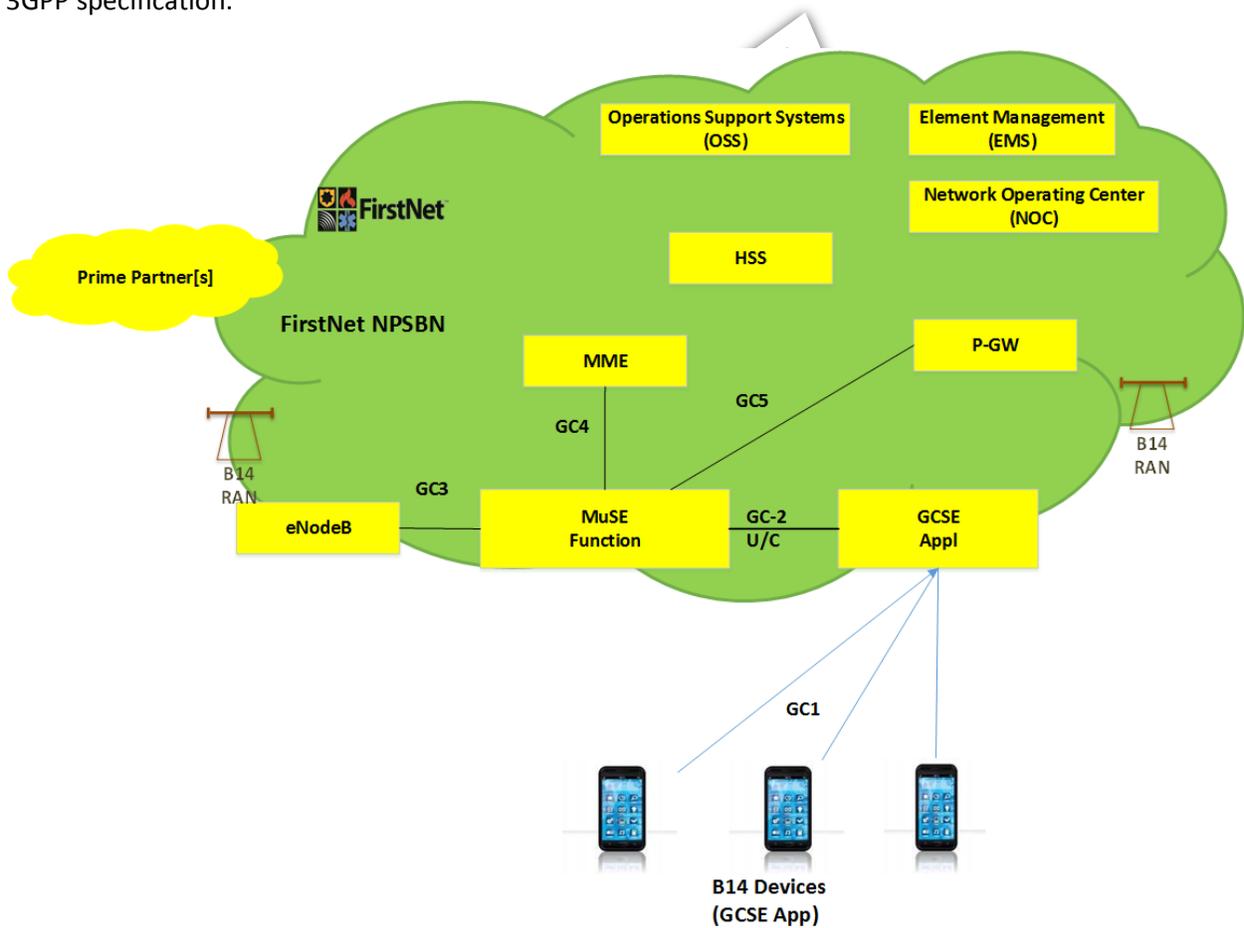


Figure 2 StdV-2 for Group Communication System Enablers

Table 2 Group Communication System Enablers Mandatory Standards

Service Area	Subset	Mandatory Standard Document
GCSE	GCS – Application Server	3GPP TS 23.468
	GCS – Enabled Client	3GPP TS 23.246
	GCS – LTE Core Interface Requirements	
IMS Group Management	Group Management of IMS services	3GPP TS 22.250
		3GPP TS 22.340
		3GPP TS 22.141

5 StdV-2 Enhanced Location Services

The Federal Communications Commission (FCC) has proposed and requested specific measures to improve the accuracy of the location of the E911 calls to the Public Safety Access Points (PSAPS) in PS Docket No. 07-114 to the industry on February 21, 2014. The FCC proposal includes both near- and long-term components. In the near term, FCC proposes to establish interim indoor accuracy metrics that will provide approximate location information sufficient to identify the building for most indoor calls. Contractor shall implement enhanced location services when the FCC and 3GPP finalizes the definitions.

6 StdV-2 Multimedia Broadcast Multi-Cast Services

Multimedia Broadcast Multi-Cast Services (MBMS) is a point-to-multipoint service in which data is transmitted from a single source entity to multiple recipients. Transmitting the same data to multiple recipients allows network resources to be shared. MBMS architecture enables the efficient usage of radio-network and core-network resources, with an emphasis on radio interface efficiency.

MBMS is realized by the addition of a number of new capabilities to existing functional entities of the 3GPP architecture and by addition of a number of new functional entities.

The MBMS bearer service offers two modes:

- Broadcast Mode
- Multicast Mode

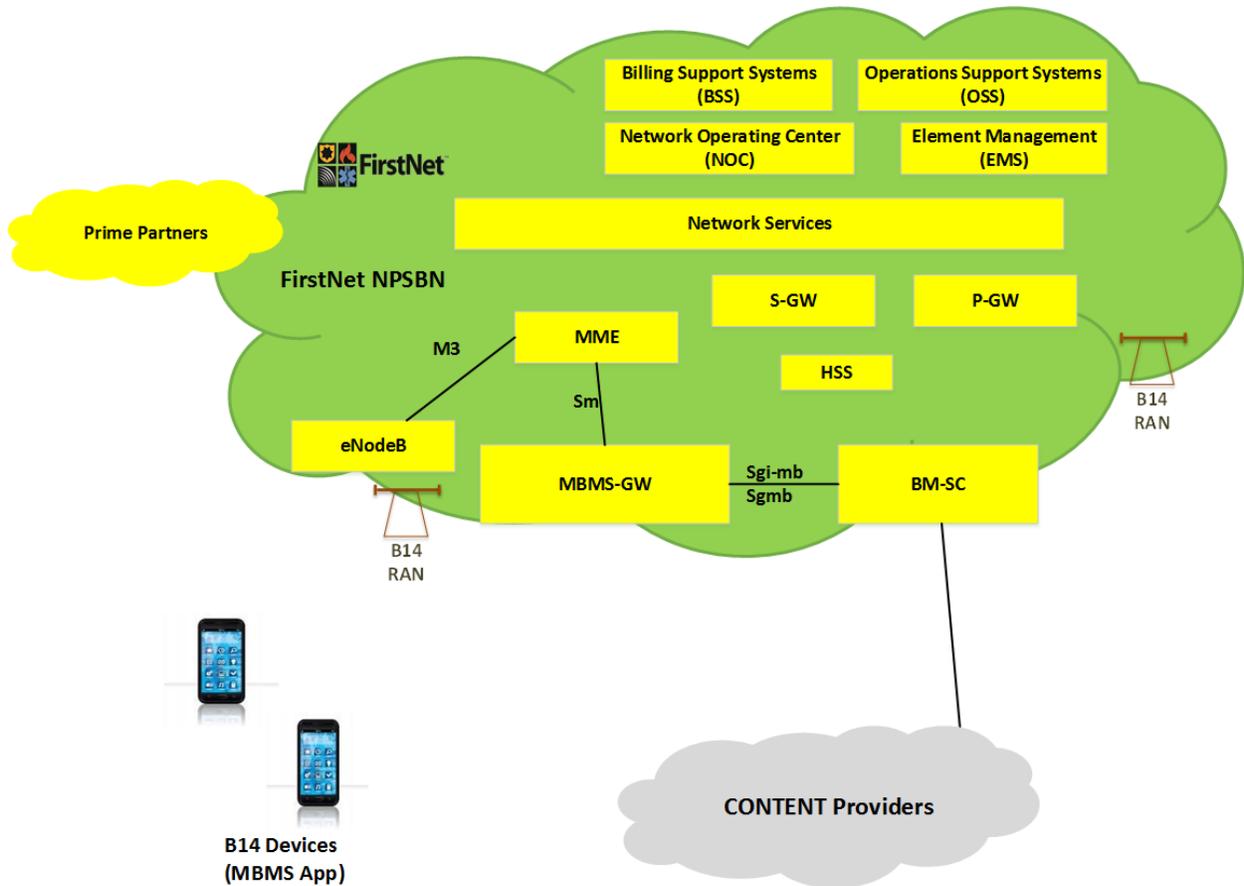


Figure 3 StdV-2 Multimedia Broadcast Multi-Cast Services

The MBMS service shall be supported when the user roams into another network and falls back to 3G. Figure 3 StdV-2 Multimedia Broadcast Multi-Cast Services identifies the MBMS service is available on LTE and 3G Networks.

Table 3 Multimedia Broadcast Multi-Cast Services Mandatory Standards (MBMS)

Service Area	Subset	Mandatory Standard Document
Enhanced MBMS service	M1: It is the reference point between MBMS GW and E-UTRAN/UTRAN for MBMS data delivery	<ul style="list-style-type: none"> • 3GPP TS 23.246 • 3GPP TS 22.146 • 3GPP TS 33.246 • 3GPP TS 22.246
	Multicast is used on this interface to forward data	<ul style="list-style-type: none"> • 3GPP TS 26.346 • 3GPP TS 25.346 • 3GPP TS 25.446
	M3: It is the reference point for the control plane between MME and E-UTRAN	
	Sm: It is the reference point for the control plane between MME and MBMS GW	
	Sn: It is the reference point between MBMS GW and SGSN (S4 based) for the control plane and for MBMS data delivery. Point-to-point mode is used on this interface to forward data	
	SGi-mb: It is the reference point between BM-SC and MBMS GW function for MBMS data delivery	
	SGmb: It is the reference point for the control plane between BM-SC and MBMS GW	

7 StdV-2 Identity Management

In an increasingly mobile and networked world, users of wireless communications expect real-time access to services and applications. Having access to what they need, when they need it, is essential to the user experience and consumer satisfaction with wireless services. A network that provides such access must have the capability to authenticate user identities in order to authorize the services and applications for use.

This issue is magnified for the nation’s first responders who often require immediate access to networks for communications and information sharing. Identity, Credential, and Access Management (ICAM) refers to the technology and governance of providing access to a network. Through ICAM, first responders are “identity proofed” by their local agencies and issued credentials that verify their identity and provide access to the resources they need.

ICAM is an important consideration in FirstNet’s planning for a NPSBN. Contractor shall support ICAM and the unique challenges from those faced by commercial providers. For instance, first responders use devices that may be shared by multiple users who work different shifts, or in cases of mutual aid while responding to an incident. As such, in addition to recognizing the device, the NPSBN is required to verify the identity of the user of that device in order to deliver authorized services.

Furthermore, given that public safety agencies locally control identity and credential management, Contractor shall consider ICAM for a diverse set of tens of thousands of public safety agencies. Additionally, access to applications, and the priority of those applications, can be highly dynamic based upon the role of the user and the user’s involvement in an incident. For these and other reasons, ICAM is critical for innovative and cost-effective solutions.

DRAFT

Table 4 Identity Management Mandatory Standards

Service Area	Description	Mandatory Standard Document
Federal Agency Access (Identity Management)	<p>Access to the national database (DB) (CJIS, NEMSIS etc.) through FirstNet core.</p> <p>PSE shall authenticate, authorize the local agency services/applications for visited PS users.</p> <p>The opt-out state and its local PSE shall provision and maintain their own users' credentials and identity in their own network and act as the identity provider.</p>	<p>Some of the evolving standards on ICAM are shown below:</p> <p>GFIPM: Global Federated Identity and Privilege Management</p> <p>Trustmark: National Strategy for Trusted Identities in Cyberspace (NSTIC)</p> <p>SICAM: State Identity, Credential Access Management</p> <p>NIEF: National Identity Exchange Federation (NIEF)</p> <p>PIV-I: Personal Identification Verification-Inter-operability.</p> <p>NSTIC: National Strategy for Trusted Identities in Cyberspace.</p> <p>NISTIR-8014 – NIST document on Identity framework.</p> <ol style="list-style-type: none"> 1. NIST 800-63, 2. NIST 800-53, 3. NIST 800- 157 4. NIST 800 – 161 5. NIST 7981 <p>FIDO: Fast Identity Online IJIS Institute (http://ijis.org)</p> <p>SAML and Open ID Connect are some of the Federated Identity protocols where the ICAM framework uses The Local agency federated access is transparent.</p> <p>ATIS Standard: IDAM</p> <ol style="list-style-type: none"> 1. ATIS-1000044.2011 2. ATIS-1000045.2012

8 StdV-2 Public Safety Enterprise (PSEN)

At FOC, the following interface specifications may change or be required to be supported.

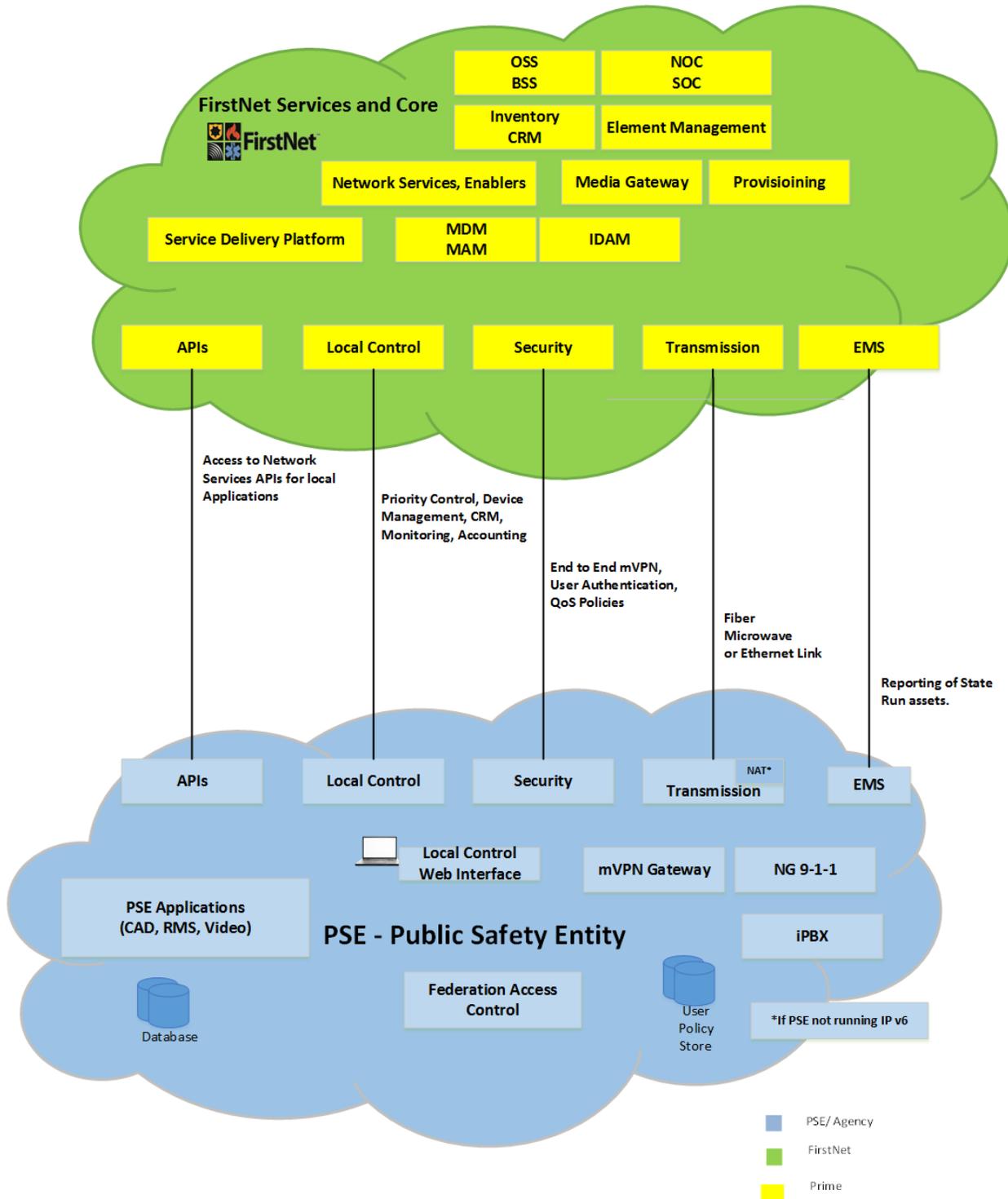


Figure 4 StdV-2 PSE

8.1 Transmission

The transmission link between FirstNet and the PSEN shall support IPsec to secure access to multiple interfaces that are centralized such as operations, provisioning, and centrally hosted or PSEN hosted applications. For example, access to federal applications and databases (CJIS, NLETS) will become centralized as opposed to each agency currently having its own access. The secured connections will need to be certified by the respective federal agency. The change to StdV-1 therefore is as follows.

Table 5 Transmission Mandatory Standards

Item	Mandatory Standard and Source Document
Data Link Layer (2)	Firewall Policy Implementation (VPN)

8.2 Security

A newer encryption standard will be adopted moving from FIPS140-2 to FIPS140-3 (currently in draft). The Contractor shall support additional authentication technologies including SAML2.0 and Open ID Connect, if not supported already, as well as derived PIV-I credentials. The change to StdV-1 therefore is as follows:

Table 6 Security Mandatory Standards

Item	Description	Mandatory Standard and Source Document
Mobile VPN ¹	Encryption of data in transit	FIPS140-2, (FIPS 140-3 when it becomes available)
	Authentication of users	SAML2.0 or Open ID Connect tokens Derived PIV-I, NIST SP 800-157

8.3 Applications

With NG911, there will need to be an IMS peering interface between FirstNet and the PSEN for multimedia services. The change to StdV-1 therefore is as follows:

Table 7 Applications Mandatory Standards

Service Area	Description	Mandatory Standard and Source Document
NG9-1-1	IMS peering for NG911 Multimedia Services	3GPP TS23.167, Emergency Services IP Network Design for NG9-1-1 Information Document (www.nena.org/?IP_Network_NG911)
Certificates	Identification of endpoints, users, and devices	PKI X.509 v3

¹ Must employ compatible mVPN client on devices with over-the-air updates.

Service Area	Description	Mandatory Standard and Source Document
	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, and biometric systems. Radius-EAP protocol with active directory.
	QoS and access policies	Web interface/ HTTP(S)

8.4 Element Management System

The Next Generation Management Interface shall be integrated with FirstNet NOC using the following interface.

Table 8 Element Management System Mandatory Standards

Service Area	Mandatory Standard and Source Document
NGN-Management	3GPP TS 32.102

9 StdV-2 Mobile Control Unit (MCU)

Deployables are traditionally used for large scale incidents or events where the coverage is localized but there is a need for concentrated capacity. Most large-scale public safety events are somewhat localized leading to large concentrations of users, several hundred users in less than one square mile. This coverage and capacity are needed during times that task traditional networks such as major events, large-scale disasters, and during extended periods without available commercial power. Commercial networks are not generally designed for these extreme demands on coverage or capacity requirements.

To tackle the diverse types of incidents, a deployable strategy for public safety shall provide a portfolio of products comprising cells on wheels (COWs) and systems on wheels (SOWs) that commercial operators use today to provide localized capacity at events and longer duration incidents, portable communications for incidents in remote areas inaccessible by vehicles, and lastly a mobile, fast response, low capacity solution able to manage short duration, smaller incidents (which account for 95% of all incidents) and to take control of the larger incidents until more resources can arrive.

Table 9 MCU Mandatory Standards

Service Area	Subset	Mandatory Standard Document
MCU	<p>A MCU shall support a hybrid network solution comprising 3G/ LTE terrestrial and satellite networks as backhaul options.</p> <p>The hybrid network operation shall provide a seamless handover between terrestrial and satellite networks for an end-user to maintain seamless communications</p> <p>The satellite network shall be able to transport both LTE and LMR traffic back to FirstNet's Evolved Packet Core (EPC) as well as from the MCU back to the FirstNet's core and/or at least one commercial LTE/3G network.</p> <p>The deployable solution shall work seamlessly in coverage, network or satellite, or out-of-coverage without the intervention of the first responder.</p> <p>The MCU SHALL support band 14, at least one commercial 3G/LTE network, and satellite as backhaul options to FirstNet's EPC.</p>	<p>3GPP specification on proximity services, GCSE, MBMS is applicable other than generic LTE standards interface.</p> <p>The 3GPP IOPS (isolated operations) specifications.</p>

10 StdV-2 Data Sharing of Local Agencies

Table 10 Data Sharing for Local Agencies Standards

Service Area	Subset	Standard Document
Interoperability with other state PSEs	CAD application and other data apps sharing with FirstNet	U.S. DoJ Document. https://it.ojp.gov/documents/LEITSC_Law_Enforcement_CAD_Systems.pdf
ISE - Information Sharing Environment	Information sharing between agencies and its framework	DHS-ISE: Information Sharing Environment National Strategy for Information Sharing and Safeguarding (NSISS)

DRAFT