

Public Safety Broadband Interoperability Recommendations

FCC Interoperability Vendor Meeting



August 17, 2010

Introduction

- Early deployments will play an essential role in further developing recommendations and requirements
 - However, standards compliance of early deployments is essential to allow smooth evolution and interoperability
- We recommend to focus interoperability on the following key areas:
 - Standards compliance of interfaces between LTE elements with a key focus on devices
 - Security options required for Public Safety
 - Roaming between Public Safety LTE networks and between PS LTE networks and commercial networks, both LTE and non-LTE
 - Handover between LTE networks, both PS and commercial
- Other areas that are important for interoperability are:
 - QoS and priority access mechanisms
 - Interface public safety applications can use to influence priority and QoS
 - Status/Information Home Page requirements

Interfaces Between LTE Elements

Alcatel-Lucent believes this is the core set of LTE interfaces that must be certified to ensure interoperability.

Interface	Elements	Associated 3GPP Standards
Uu	UE to eNB	36.211, 36.212, 36.213, 36.214, 36.321, 36.322, 36.323, 36.331
RF/BS	UE to eNB	36.104, 36.141, 36.133
NAS	UE to MME	23.122, 24.301
S1-U	eNB to SGW	36.411, 36.412, 36.414
S1-MME	eNB to MME	36.411, 36.412, 36.413
X2	eNB to eNB	36.420-36.424
S10	MME to MME	29.274
S6a	MME to HSS	29.272
S11	MME to SGW	29.274
S5/S8	SGW to PGW	29.274, 29.281
SGi	PGW to PDN	29.061
Gx	PGW to PCRF	29.212, 29.213
S9	V-PCRF to H-PCRF	29.213, 29.215
Rx	PCRF to Application	29.213, 29.214

Additional interfaces would be of concern when other radio access technologies are considered

Security Requirements for Public Safety

- Follow recommendations provided in NPSTC BBTF report. These include support for:
 - The Radio Resource Control (RRC - TS 36.331) protocol layer should implement LTE signaling layer security features;
 - The Network Access Stratum (NAS - TS 24.301) protocol layer should implement EPC signaling layer security features; and
 - The Packet Data Convergence Sublayer (PDCP - TS 36.323) protocol layer should implement user data plane security features
- Alcatel-Lucent also recommends that all the Authentication and Key Agreement (AKA) procedures described in section 6, 7, and 8 of 3GPP TS 33.401 be implemented
- Standardize on tunnel mode IPsec Encapsulating Security Payload with IKEv2 certificates and allow the use of a Security Gateway on the core side

Device Interoperability

- PS will benefit from work done by commercial service providers
 - Commercial providers drive backwards compatibility for devices
 - 3GPP UE test cases defined in 3GPP 36.508, 36.509, 36.521-x, 36.523-x
- Need to perform basic RAN-level IOT testing
 - Will each public safety network operator require their device vendors to perform IOT with their network equipment vendors (as done by commercial operators) or will there be a single party performing this for all of Public Safety?
 - Additionally, roaming onto commercial networks requires device interoperability with commercial partner network
 - This may require one or more commercial partners depending on local coverage
- What application layer device compatibility is required?
 - Device management (OMA)
 - Sign-on requirements (SAML?)
 - Other clients
 - ...

How Will We Achieve Interoperability?

- The only way to ensure true interoperability is by testing among multiple vendors of all interfaces deemed critical to Public Safety

- Time is of the essence!
 - Need to find a way to achieve this without delaying any deployments while supporting complete interop for PS

- Recommendation:
 - Mandate all Public Safety contracts include a standard set of terms/conditions/requirements regarding interoperability and vendor support for interoperability testing
 - Define an initial set of use cases that will assure interop for functionality important to early deployments
 - Align on 3GPP Release 8, December 2009 as minimal release level
 - Consistent with some major commercial service providers
 - Leverage NIST testbed to execute these use cases between vendors and create a joint test report
 - In parallel put long-term strategy in place

Long-Term Interoperability Strategy

- Establish a test facility to validate interoperability among vendors.
- Act as single party performing device testing for Public Safety
- Define interface specifications/compliance matrices for the 3GPP standards associated with each of the interfaces
 - Sample interface specification supplied by Alcatel-Lucent provides a template
- Define use cases that cover required functionality
 - Will evolve over time as new functionality is added (e.g. PTT, Multimedia Broadcast Multicast Service - MBMS)
 - Use similar approach as followed by Network Vendors IOT (NVIOT) Forum
- Identify the organization that acts as arbiter for failed interface test cases.

Additional Decisions to be Made to Improve Interoperability

- Align on interface between applications and PCRF
 - Is diameter-based Rx interface appropriate, or is a RESTful API required
- Align on MME and SGW pooling as defined by 3GPP to provide geographic redundancy between eNB and EPC
- Align on IMS-based SMS per 3GPP 23.204
- Define Status/Information home page
- Define guidelines for use of priority access while at home and roaming
- OOBE: align on current $43 + 10\log P$ dB for operations in the PSBB Block