NPSTC 700 MHz Broadband Network Requirements Task Force (Task Force)

Technical Working Group

700 MHz LTE Network Interoperability

Scope

To document the minimum requirements necessary to enable roaming between LTE networks built by multiple, independent public safety organizations and commercial service providers, where roaming users will have initial access to the Internet, <additional applications/services as defined by operations WG>.

This does not prevent organizations from deploying additional applications/services that are available to roaming users, but provides a minimum expectation.

Table of Contents

LTE Network and Device Specifications

Roaming is defined as:

- Roaming minimally requires a device capable of 700 MHz radio network interoperability based on the commercial 3GPP LTE standards.
- In the absence of RF coverage from the home network, the ability for the UE to scan supported bands, perform cell selection and authentication on a visited network
- After authentication on a visited network, the assignment of an IP address, and the ability to communicate with the public Internet, obtain local services as applicable, or access the home network to obtain services supported by the home provider.

Interoperability is defined as:

- The capability to automatically (roam) onto a visited network and have access and share appropriate information/services as authorized.

Based upon discussions with the working group leads, service providers and industry we recommend four categories of roaming for our working group (in order of importance) to focus work on.

1. Roaming between 700 MHz public safety LTE networks – e.g., UE from San Francisco works in NYC. Assumption is that both networks involved in this roaming scenario (visited and home networks) are Evolved Packet Core/System Architecture Evolved (EPC/SAE) networks. This will be defined as intra-network roaming.
2. Roaming between private 700 MHz PS LTE and D block Shared LTE Network – could also be another 3GPP or non-3GPP technology. As defined per current FCC D block plans for regional licensing.
3. Roaming between 700 MHz public safety LTE networks to commercial 700 MHz LTE networks – e.g., UE from San Francisco (home) roams to local Verizon/AT&T (visited) network and roams back.
4. Roaming between 700 MHz public safety LTE networks to commercial and private broadband networks (3GPP and non-3GPP) in other bands. – e.g., UE from San Francisco (home) roams to local AT&T HPSA (visited) network and roams back.

NOTE: Category 1 and 2 may be combined if the D block is reallocated to public safety as recommended by the BBTF, this would include operation over both the D and PSBL blocks .

Categories 2, 3, and 4 can generically be called inter-network roaming and even further defined as inter-RAT (Radio Access Technology) and inter-frequency networks.[1] The initial scope of the group will be to define the minimum set of interfaces required to support intra-network (category 1) roaming. The work for this (similar/common interfaces) can then be applied to the remaining roaming categories. Since the LTE specification was chosen and it is based off of the 3GPP standards – the required interfaces have already or are in process of being defined. This

[1] See NPSTC Broadband Task Force Governance Group Roaming Whitepaper

document will merely reference those interfaces that we deem necessary to fulfill our interoperability needs.

It should be well understood that the LTE standard (3GPP Release 8) is a relatively new standard in which a first draft just accepted in March 2009. Features and performance will grow with each release and iteration of LTE. NOTE: Previous standards work and deployment of existing W-CDMA, WiMAX and EVDO networks often happened 2-5 years after the standards were adopted.

System Identifiers

Several waiver requests from states and cities have been submitted to the FCC to approve the deployment of broadband networks on the PSBL spectrum. The likelihood of having regional networks is very probable – public safety will become a mobile broadband operator. Unanimous consensus was reached in the technical working group based on the fact that a common methodology of identifying public safety networks is required.

In 3GPP networks, the term Public Land Mobile Network (PLMN) is used to describe the Home (HPLMN) or visited (VPLMN) networks for roaming use cases. Standards describe the International Mobile Subscriber Identity (IMSI) that is used by both 3GPP (GSM) and 3GPP2 (CDMA) to uniquely identify every user. In 3GPP networks, every terminal contains a USIM (Universal Subscriber Identity Module) smartcard that permanently stores a unique IMSI and a secret key that is used for authentication. It consists of a 3 digit Mobile Country Code (MCC) and a 2 or 3 digit Mobile Network Code (MNC), this creates the Home Network Identifier (HNI). The addition of a unique 9 digit Mobile Station Identification Number (MSIN) creates the IMSI. Users are identified typically by their PLMN id and more specifically their IMSI.

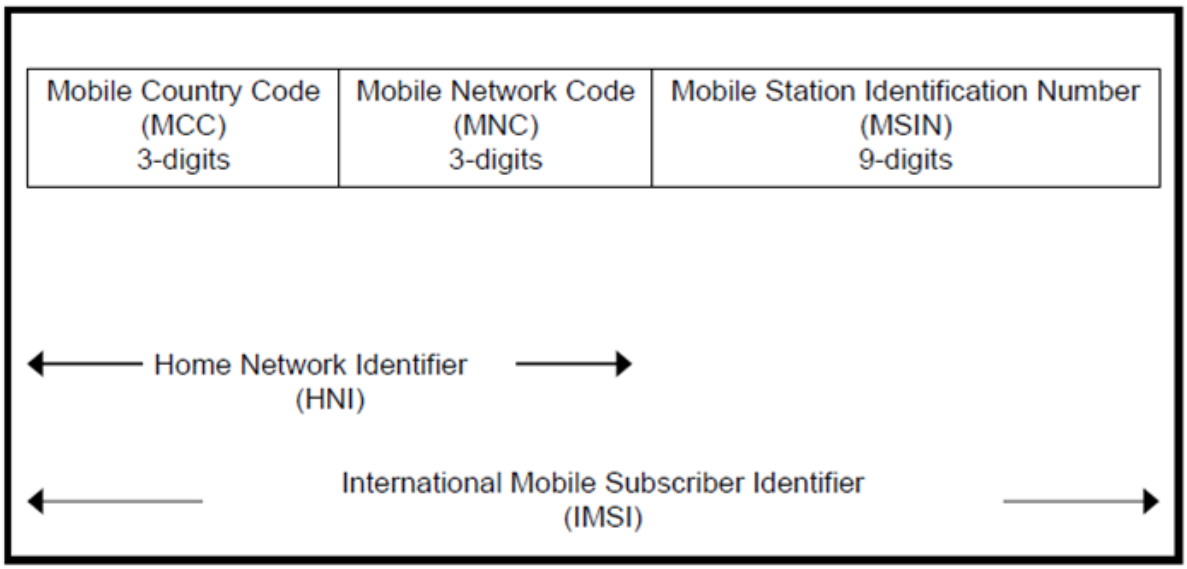


Figure 1: IMSI

In order to differentiate the public safety networks from each other, commercial networks and yet enable them for roaming, a PLMN and IMSI assignment process will be developed for public safety LTE networks. Currently the United States has MCCs 310 – 316, and code 310 has been used to avoid international roaming ambiguities. The MNC is a three digit number (999 possible combinations) that network operators use to differentiate themselves and so that limits the amount available to public safety networks. The Home Network Identifier (HNI), which is a combination of the MCC and MNC is used to identify the PLMN. HNI's are administered by Telcordia according to procedures established by the IMSI Oversight Committee (IOC) which is a committee of the Alliance for Telecommunication Industry Solutions (ATIS). Unique HNI's are required to distinguish between eNodeB's from home and visited networks. The PLMN part of the IMSI (which is stored in the UICC card of the device) is used to determine the proper HSS to query for subscriber information.

ATIS and the IOC have expressed their willingness to work with public safety representatives in assigning PLMN id's. This will be necessary as IOC rules state that to qualify for a HNI, the following must be criteria must be met and the PSBL does not currently meet these.

- Applicants must offer public telecommunications service. Public telecommunications service is defined as a public service, the subscribers to which must be capable of being reached over the PSTN.1
- In the event an applicant is providing network services but is not a public mobile operator, the applicant must be at least an associate member with the GSM Association or other recognized/approved industry governing body, and submit evidence of same.
- Applicants must offer non-discriminatory access of this resource to users. That is, the applicant must offer the availability of services to any end-user customer requesting the service.

These rules are designed for circuit switched services (voice) and not data networks like what is being proposed. The PSBL or whomever the governance group determines is a public safety representative will need to address this issue.

It is unlikely that multiple hundreds of PLMN ids will be assigned for individual public safety networks due to limitations within the IMSI specification. This is an issue that will need to be addressed for early system deployments so that public safety networks can be differentiated from each other and commercial networks.

In order to use LTE systems and devices complying with 3GPP standards, provide for support of the four roaming categories and for early public safety network deployments – they must assigned a PLMN ID. Since PLMN IDs are a limited resource shared by all 3GPP wireless networks worldwide, the use of PLMN IDs should be effectively managed. The Technology Working group has considered two alternatives for assignment of PLMN IDs:

1. Single PLMN id shared by all public safety networks
2. Individual PLMN id for each public safety network

Both implementations have specific considerations and implementation issues as shown in the table below and more detailed information is available in Appendix C.

Consideration	**Single PLMN id shared by all PS networks**	**Individual PLMN id for each network**
Coordination for Non-overlapping IMSI	PS agencies must coordinate usage of MSIN to avoid overlapping IMSI	Unique PLMN id for each PS agency assures non-overlapping IMSI
Identifying the HSS containing HSS subscriber data	If multiple HSS are used (one for each regional PS network or a few regions pool their resources to buy and maintain an HSS but it is still not national) a Diameter Redirect or Proxy Agent as described in TS 29.272 is required. The Diameter Agent must be operated as a shared entity for all regional PS networks. The Diameter Agent must use info from MSIN to identify the correct HSS. An alternative is to share a single HSS among all regional PS networks	Unique PLMN id can be used to identify the correct HSS in both the roaming and non-roaming cases.
Determining the home network for usage records for roaming	May require an additional centralized process to accept usage records from roamed networks and forward to correct regional PS network based on additional information beyond just the PLMN id However in some cases the roaming user may be accessing local services, in which case the visited network needs to generate records to send to the user's home network for purposes of charging. This should not be any different in public safety networks and may not be difficult to implement.	Follows industry practice of sorting by PLMN id
Cell ID transmitted by LTE cells contains the PLMN id. Cell ID is used by mobile device to determine on which network to register and is a factor in eNodeB handover decisions	Cell reselection, which will trigger PLMN selection, is controlled via specific parameters. A potential problem is when a Ue with home network coverage may attempt to roam on a visited network if the signal strength is stronger than the home network cell. Ideally a user moving out of coverage will have its device look for other networks based on a specific threshold and hence move to that network. When coming back to its own network, the device still searches for cells and when it finds its "home" PLMN it jumps back to that cell. There is also the possibility of manual PLMN selection when a user can request the device to scan for available PLMNs and order the device to select one.	Having each regional PS network have its own PLMN id follows standard industry practice

Users roaming on a visited network will have the same PLMN ids as home users. PS assumptions state that visiting users should be assigned lower priority than home users	MME must make decisions to lower priority based on something other than PLMN id – APN for example. In this case the priority is not determined by the PLMN of the user but rather the subscription of the user. Can potentially be done statically where roaming users always get lower priority after restrictions apply May be more difficult provisioning task since APNs change more frequently than PLMN ids	MME can make decisions to lower the priority of visiting users based on PLMN id. This is a relatively simple extension of data already present in the MME to control which customers are allowed to roam using PLMN ids. Follows industry practice

Table 1 - PLMN ID

The following are recommendations for public safety PLMN id allocation and implementation:

1. A common schema should be used to identify public safety users and public safety regional LTE networks (intra-network – category 1 roaming).
    a. Which PLMN id scheme should be implemented?
    b. Schema for intra-network (category 2, 3, 4) will not be explicitly defined with the exception of specific network interfaces
2. PSBL will apply for dedicated PLMN id (MCC/MNC/HNI) from the IOC
3. Use an existing MCC as determined by ATIS and IOC.
4. USIM is provisioned by the home network administrator with
    a. Home IMSI (HPLMN)
    b. Prioritized list of permitted VPLMNs
    c. Forbidden PLMNs list
5. For voice, MMS, SMS and PSTN support, the PSBL and/or public safety representatives should coordinate and manage MSIN - ITU-T E.169 PSTN number allocations

Frequency Spectrum

The waiver requests and the likely intent of the FCC are to grant spectrum in the public safety band only and not the adjacent D Block (this is all subject to change – as with NYC latest filing).

This creates a possible issue with how 3GPP defines band classes. 3GPP TS 36.101 v8.6.0 defines band class 14 is for 10 MHz wide channels using Frequency Division Duplex (FDD). This band class includes both the D-Block and public safety band as one contiguous band class. The public safety specific band is defined for operations in 763-768 MHz and 793-798 MHz range. 3GPP/LTE supports multiple and scalable bandwidths. Within band class 14, 5 MHz channels sizes are supported and can therefore accommodate public safety 5 MHz allocations.

Recommendation is that networks and devices deployed for public safety have the minimum capability to support 3GPP TS 36.101 v8.6.0 band class 14 and make band classes 12, 13 and 17 optional. Pending the waiver grants, operationally the network and devices may initially only use the upper 5 MHz, public safety band only – again this is subject to change pending.

E-UTRA Operating Band	Downlink (DL) operating band BS transmit UE receive	Uplink (UL) operating band BS receive UE transmit	Duplex Mode	Channel bandwidth $BW_{Channel}$ [MHz]	Transmission bandwidth configuration N_{RB}
14	758 – 768 MHz	788 – 798 MHz	FDD	10	50
14 - PS	763 – 768 MHz	793 – 798 MHz	FDD	5	25
14 – D	758 – 763 MHz	788 – 793 MHz	FDD	5	25

Table 2 - Band Class– Note that 3GPP only defines band 14, the –PS and –D suffixes are for a more detailed Public Safety definition of the sub band characteristics.

The use of full duplex, FDD will be the primary access method used in public safety LTE networks. The use of half-duplex FDD will not be supported by public safety due to issues with time to market, data throughput loss, lack of supporting Ue and eNodeB equipment.

Network Interfaces

The LTE/SAE/EPC architecture has several defined interfaces for interoperating with the network. These interfaces will allow users to roam into networks via these interfaces. In discussions with the working group leads, vendors, service providers and public safety the ***initial*** goal for network roaming and interoperability is defined as allowing users who leave their home network and authenticate automatically (roam) unto a visited network and have access to:

1. Public internet access
2. Best effort data
3. VPN access to their home network

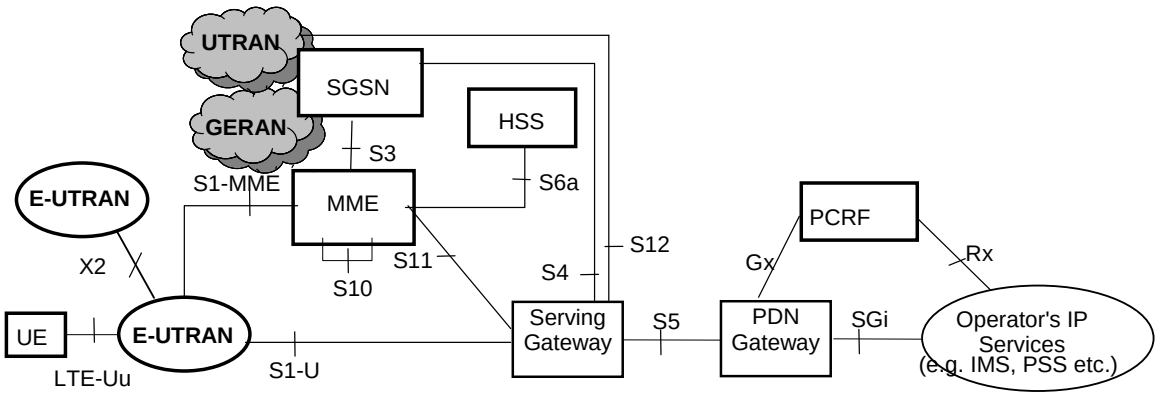
LTE, EPC and IMS are maturing technologies and as new features and capabilities are added, public safety will be able to utilize these. Optional features within an LTE network are Quality of Service (QoS), Priority and Pre-emption. These are essential features to many future public safety applications and may be implemented in future regional networks. Having those features follow a user when they roam into another network is not within the scope of this initial document. The amount of complexity, application service delivery, availability of equipment and overall timeline for this work group do not allow us to address this fully. However, it is fully understood that these features are key to a public safety network and we will continue to research the best possible implementations.

As network and application functionality increases, public safety enhancing features such as QoS, multicast/broadcast (MBMS – Release 9 target) and priority can be added to the roaming capabilities. This may require that supplementary roaming agreements be allowed between agencies and commercial service providers.

It is assumed that each network built out be a 3GPP Evolved Packet Core (EPC) network. We will define the system interfaces and the roaming cases necessary to support intra-network roaming (Category 1).

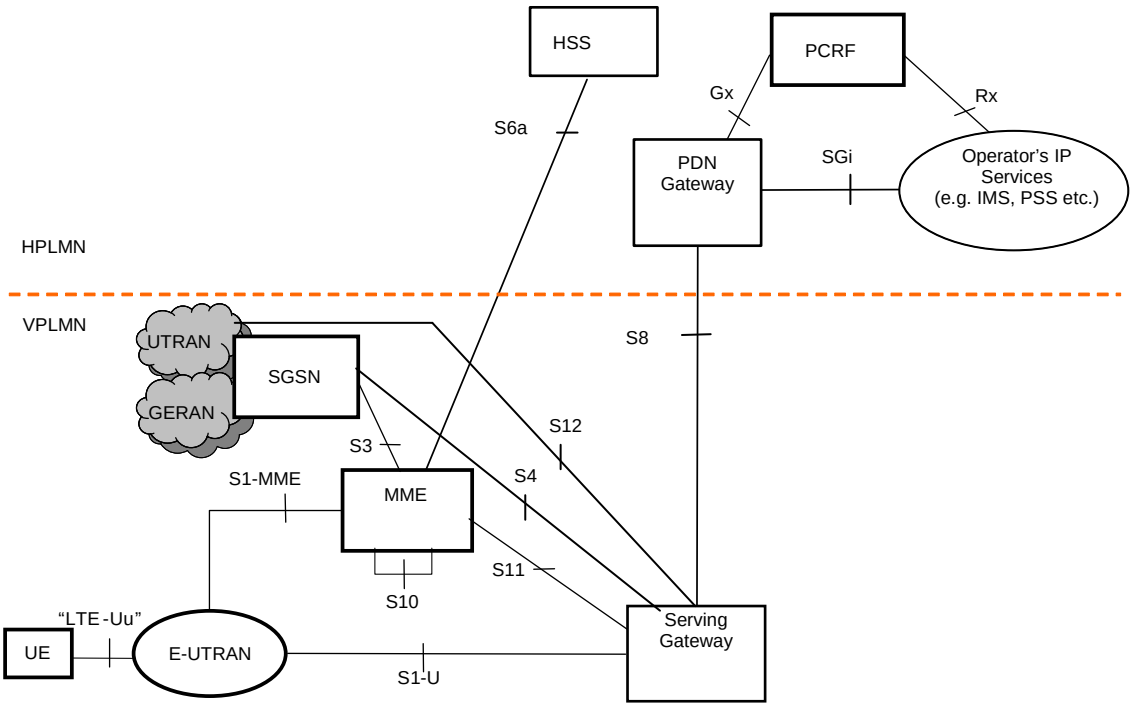
In general the network should support initially support LTE to LTE handovers (Category 1 & 2) as per 3GPP Release 8 Specifications (March 2009). See Appendix D for more detailed information regarding the specific 3GPP documents.

The following section uses multiple diagrams and network information from 3GPP TR 23.882, 23.401 and 23.402.

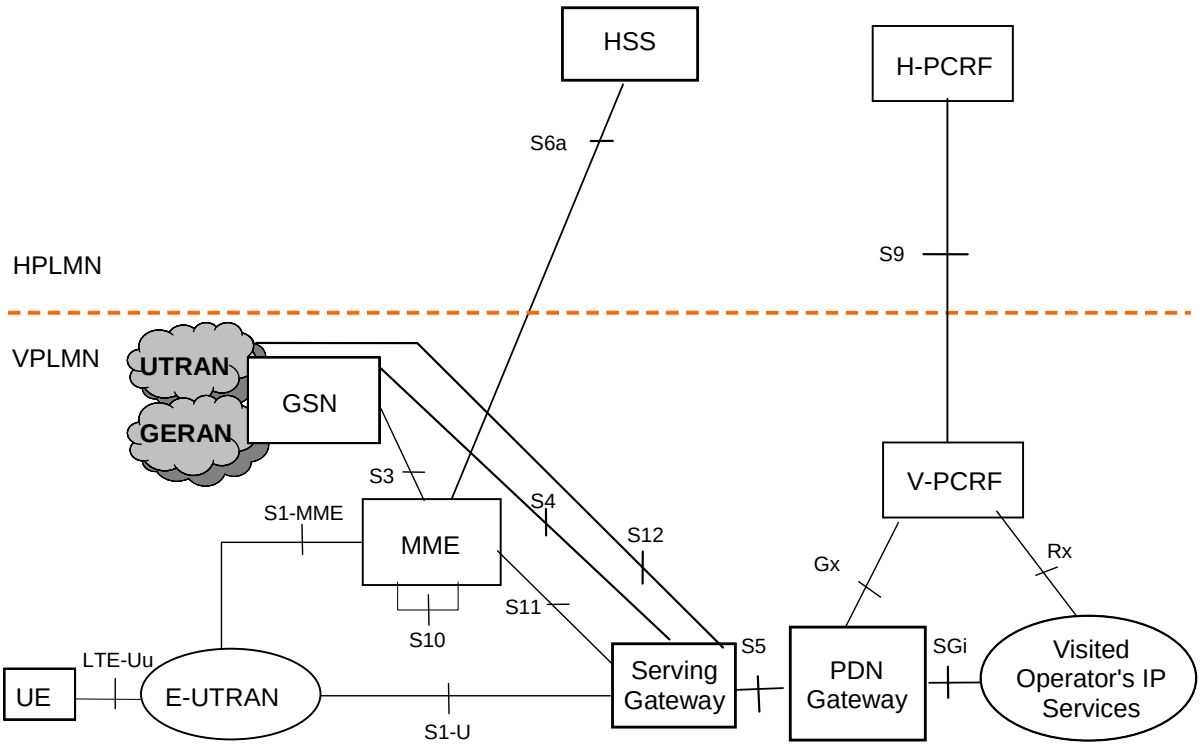


The general system diagram (PLMN) shows several new interfaces. What we need to determine is what interfaces are required to support our roaming scenario's and when they will be available from the vendors.

To support the four categories of roaming, it may be necessary to support roaming traffic that is homed to both the Home PLMN (HPLMN) and the Visited PLMN (HPLMN). An example would be web access while roaming; the UE would not be required to route traffic through the VPLMN to the HPLMN but instead utilize the internet access via the VPLMN. In the instance that you use a VPN to get email or database access, then payload traffic would flow from VLPMN to Internet to Home internet portal (VPN), then to local applications.



EPC Roaming architecture – Home routed traffic



EPC Roaming architecture – Local Breakout

To support initial network build outs that support roaming for category 1 networks the following interfaces are required:

1. Uu – LTE Air Interface
2. S6a – Visited MME to Home HSS - Diameter signalling

The following interfaces are highly recommended to fully support category 1, 2 and 3 networks:

3. S8 – Visited SGW to Home PGW
4. S9 – Visited PCRF to Home PCRF for dynamic policy arbitration. The S9 is primarily used for QoS functionality from the PCRF but its inclusion will allow easier migration to a QoS enabled network.
    a. Gx – PGW to PCRF interconnection required if S9 is implemented
5. Multi-vendor interoperability (IOT) supported on the S1-MME and S1-U interface between the eNb and the EPC
6. X2 – Intra-network eNodeB connection shall be required within a homogeneous public safety 700 MHz regional network – this does not include geographically adjacent systems
    a. IOT required for multi-vendor support

Category 4 roaming and network diagrams are covered in Appendix B.

Mobility and Handover Implications

Handover is the process that happens when a UE moves from coverage of one cell to the coverage area of another cell. (The assumption is that the UE is in the RCC connected state, else if the UE is in the idle state, it is a cell reselection per the RRC state machine.) LTE supports the use of two types of handover delivery mechanisms called seamless and lossless handover. How each of these handover delivery mechanisms are applied is dependent on the QoS assigned to the radio bearer. Ue active session handover is accomplished via the S1 or X2 interface.

Handover requirements will be as follows:

- Handover of active sessions on geographically adjacent public safety 700 MHz LTE networks. Intra-network handover for data session between home and visited networks is required. This is defined as intra-RAT handover.
    - These types of handovers will be subject to pre-arranged roaming agreement(s).
- Handover of active sessions between home and visited networks is not required when a visited network is using another RAT such as 3GPP2 or another release of 3GPP (e.g. Release 7). This is defined as inter-RAT handover.
- After handover from the 700 MHz public safety LTE network to a commercial carrier (inter-RAT), the user may come back (idle and active) into the coverage area of their home network. The cell search mechanisms should support the ability to identify and public safety LTE neighbor cells.

- Public safety networks should be the primary networks for cell reselection. As such the white-list maintained on the Ue, PLMN ids or the equivalent of the neighbor cell list (NCL) should be programmed to facilitate public safety LTE networks as the primary choice.

Pending the outcome of the waiver requests and the potential addition of voice capability or if the FCC requires this by rule, the implementation of lawful intercept (CALEA) may be required on the public safety LTE network. The MME, PGW and SGW have the necessary interfaces to support this functionality and public safety LTE networks should use 3GPP TS 33.107 v8.8 (or later) as a reference on how to support this functionality.

Inter-network Authentication and Connectivity

In order for roaming and more specifically authentication to be enabled, there must be several interfaces that are connected between each home and visited network. To support this, multiple leased lines would be required, thus putting a large technical and financial burden on the public safety network. Commercial service providers traditionally use 3rd party clearing houses to provide their roaming authentication and interworking functionality. This allows inter-RAT roaming such as CDMA and GSM to interwork with each other (e.g. GPRS Roaming Exchange (GRX) and CDMA Roaming Exchange (CRX)), number portability, SMS/MMS/IM and many other functionalities that follow users as they roam. In addition, roaming fraud has been a serious problem for operators. To combat this growing problem, the GSMA has implemented Near Real Time Roaming Data Exchange (NRTRDE).

Public safety should utilize similar methodologies for roaming to enable them the most flexibility and cost savings. A 3rd party commercial interworking provider can support a common authentication scheme for all public safety networks, thus supporting both inter- and intra-network roaming.

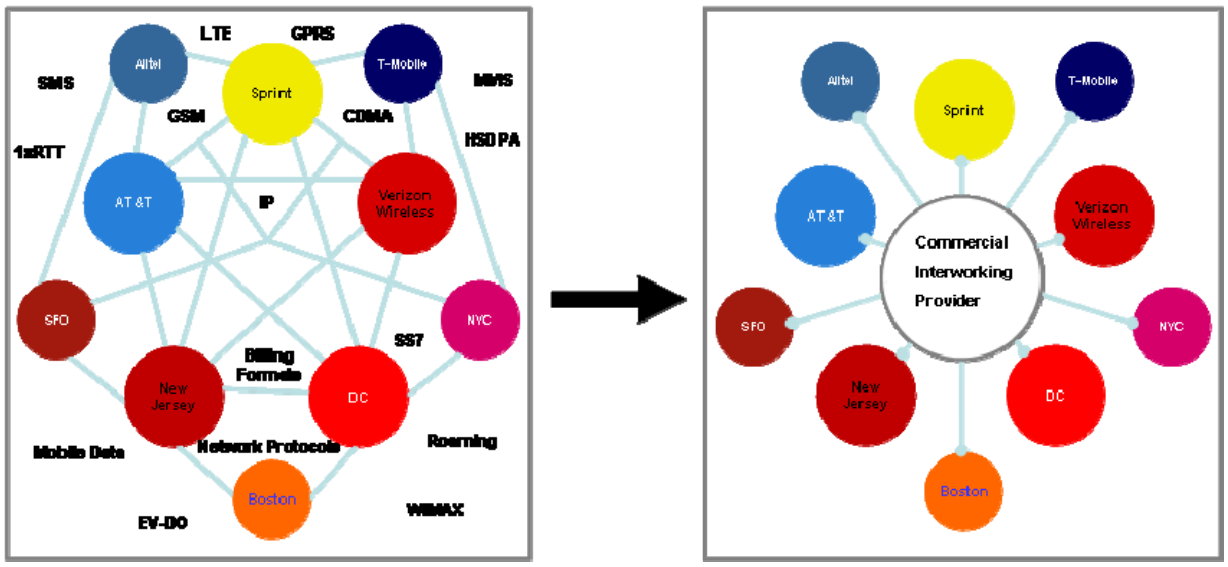


Figure 2: 3rd Party Interworking

Interwork Connectivity Recommendations

1. A common/single 3rd party clearing house should be utilized by public safety
    a. PSBL and/or public safety representative will determine specifications based upon bi-lateral roaming agreements
2. All 700 MHz public safety LTE networks will utilize a similar authentication scheme
    a. Implementation of Near Real Time Roaming Data Exchange (NRTRDE) between public safety networks and between public safety and commercial networks to combat fraud and facilitate the exchange of roaming data.
3. Provisions should be allowed to directly interconnect geographically close 700 MHz public safety LTE networks to each other.
    a. Directly connected networks will need to ensure to PSBL and/or public safety representatives that all proper authentication credentials are processed accordingly
4. Redundant, geographically separate 3rd party clearing house centers will need to be supported to address disaster scenario's
    a. Backup solution will need to be available to authenticate roaming users when 3rd party network isn't available and mutual aide is required from roamers

Devices

Public safety LTE devices will initially share or be the same as commercially available devices. Initial devices for the LTE market in the US will consist of PCI Express and USB dongle configurations. Smart phone and phone type devices will likely follow on in the 2011 timeframe. The minimum requirements and specifications, but not limited to, for a public safety device are the following:

1. Band class 14 should be supported for 5 and 10 MHz channel sizes in Frequency Division Duplex (FDD) mode as per 3GPP TS 36.101 v8.6.0
2. USIM should be unlocked to allow public safety users to switch out UICC cards between multiple devices

Optional requirements and specifications

1. IMS authentication and services via support of the ISIM as per 3GPP TS 31.103: *Characteristics of the IP Multimedia Services Identity Module (ISIM)*
2. Multi-mode support of 3GPP Rel. 7 HSPA and/or 3GPP2 EVDO Rev. A
3. Multi-band support for 3GPP & 3GPP2 commercial 700, 850 and 1900 MHz bands

Standards Testing

LTE has been selected as the wireless broadband standard for public safety. There is already a very robust test methodology in place due to the fact that LTE is being adopted by commercial service providers worldwide. The conformance-test standards are split into two documents: the three-part TS 36.521 deals with all the transmitter and receiver tests and RMM (radio resource management) while 36.523 deals with the signaling (protocol) tests. Within 3GPP RAN WG1 – WG4 they are working on system level tests and RAN WG5 are working on UE related tests. (ETSI/3GPP have over 400 mandated tests already.)

3GPP Special Task Force 160 (STF 160) is working on using TTCN3 as the test language for LTE and have all leading manufacturers working in that group. ETSI and 3GPP are working closely with the Global Certification Forum (GCF) Ltd and the PCS Type Certification Board (PTCRB) to select a certain number of test cases and define how many test cases must be passed to certify the device under test. These test cases are then executed by accredited test labs such as Cetecom and 7 Layers.

The minimum requirements and specifications, but not limited to, for a public safety 700 MHz LTE Standards testing are the following:

1. Minimally, public safety 700 MHz LTE infrastructure and subscriber equipment will need to have been tested and certified by the aforementioned 3GPP test suites that the GCF is overseeing.
2. If GCF testing is not available within the timeframe of network deployment the vendors and public safety network operators should have the option to perform specific testing as determined by the PSBL and/or public safety network representative.

Applications and Quality of Service

Within the Evolved Packet System (EPS), IP connectivity is provided between the UE and the PLMN external packet network e.g., Public Internet Access, this is called PDN Connectivity Service. As defined by the scope of this working group, the primary application for users who are roaming will be internet access. Specific applications as defined by the Operations Working Group include but are not limited to the following:

1. Internet access
2. VPN access to home networks
3. Visited network home page
    a. Intra-network roaming users will have a common webpage, text message or delivered information on applications and services offered by the visited network and relevant alerts.
4. Text messaging
    a. Application level SMS over IP will be allowed but recommend the use of a common SMS delivery system as described in 3GPP TS 23.204 V8.4.0 and 3GPP TS 24.341 V8.1.0
        i. *NOTE: Inclusion of this specification may require the use of the IP Multimedia Subsystem (IMS)
    b. Current SMS capability is supported via media gateways that are designed for control plane/circuit switched networks. Legacy SMS support is tentatively scheduled for 3GPP Release 9 (or 10 depending on the delivery platform).
        i. Will follow 3GPP development and industry trends for supporting legacy SMS
5. Location identification
    a. Location Based Services will require user plane interfaces as opposed to current circuit switched PDE type implementations.
        i. Under investigation by technical working group for solutions and will track industry trends
        ii. Will require unified support from chipset, subscriber and infrastructure vendors
    b. User and control plane support for LBS targeted for 3GPP Release 9
6. LMR gateway interconnection
    a. Use of the latest Bridging Systems Interface Specification (BSI) is the recommended LMR gateway interconnect

Desired Applications – These requirements are under continuing investigation by the technical working group

1. LAN bridging to broadband networks
    a. This will likely require the use of wireless router and need to utilize QoS to prevent overloading the cell.
2. One-to-many communications across all media
    a. Multimedia Broadcast Multicast Service (MBMS & E-MBMS) for LTE is scheduled for 3GPP Release 9
        i. Further investigation on requirements is necessary to determine system impacts and implementations
3. Commercial Mobile Alert System (Public Warning System)
    a. Defined by the FCC under Part 10 rules, to handle broadcast of geo-targeted imminent threat to life or property emergency alerts distributed by the Federal Government though a CMAS aggregation function under the FEMA iPAWS program.
        i. This includes deployment of a CMSP Gateway in the public safety network to receive the alerts from the FEMA Federal Alert Gateway, and

distribution of those alerts in the LTE network via a Cell Broadcast Center.
   ii. ATIS and TIA, in conjunction with FEMA, have defined the interface between the Federal Alert Gateway and the CMSP Gateway, and ATIS is developing specifications for supporting CMAS on LTE.
   iii. PWS, which includes CMAS support, is scheduled for 3GPP Release 9.
b. Support for CMAS functionality in the mobile devices consistent with the Joint ATIS/TIA CMAS Mobile Device Behavior Specification (J-STD-100, January 30, 2009).
   i. Public safety mobile devices should give consideration for support of the Required Monthly Test (which do not go to consumer devices).

4. E-911 support for part 90 systems
   a. Investigate the necessity to support E-911 for initial data only public safety LTE network
   b. Also address FCC requirement based upon PSTN voice capability added to public safety LTE network
   c. Investigate control plan implementation impact for IMS based emergency calls

Quality of Service (QoS), priority and pre-emptive access are all important features to public safety networks. Within 3GPP Release 8, QoS is defined in TS 23.401 and in TS 23.203. Public Safety Networks should utilize QoS as defined in these documents.

The EPS uses logical channel bearers (bearer), pre-defined QoS values, Uplink Traffic Flow Templates (TFT) and Downlink TFT to enable QoS. Many other parameters such as the APN-AMBR, UE-AMBR, QCI, ARP, GBR, MBR and several others need to be defined. These parameters must then be mapped across the network, mapped to the roaming networks (commercial and public safety) and even to 3G networks. The goal of standardizing these interfaces and parameters is to ensure that the services and applications mapped to a QoS class receive the same minimum level of QoS when roaming or within a multi-vendor deployment. Needless to say this is a complicated and important aspect to designing networks that enable QoS. Continuing work will be required to create templates for public safety applications and services. It should be noted that the use of dynamic policy control (PCRF) used within LTE will minimally require the Rx and Gx interfaces.

LTE Security

For network and subscriber security it is recommended that common 3GPP authentication and security is used for public safety networks.

3GPP LTE supports the Authentication and Key Agreement (AKA) scheme as defined in TS 33.401. The credentials that are exchanged are the IMSI, and the permitted network service capabilities are fetched from the Home Subscriber Server (HSS). The Packet Data Convergence Protocol (PDCP) layer processes the security functions for the radio bearer. These security functions include:

- User Plane - integrity protection and verification of data
- Control/User Plane – ciphering/deciphering of data

These security features are never deactivated in a LTE network and will be used in public safety LTE networks. Possible exceptions would be an emergency call without a USIM.

The Radio Resource Control (RRC – TS 36.311) protocol layer may optionally implement LTE signalling layer security features. The Network Access Stratum (NAS – TS 24.301) protocol layer may optionally implement EPC signalling layer security features. The Packet Data Convergence Sublayer (PDCP – TS 36.323) protocol layer may optionally implement user data plane security features. For public safety LTE networks, these optional security layer features specified in 3GPP TS 33.401 should be implemented.

The use of network layer virtual private networks (VPN) will be allowed on public safety LTE networks. VPNs provide secure communication tunnels to home servers/applications and can support (e.g. NCIC/CJIS, AES and HIPPA) public safety security requirements. Coordination of ports and QoS will need to be determined as necessary between home and visited networks.

Continued research and requirements can be fed into 3GPP Release 10 where a study on new Encryption & Integrity EPS security algorithms, which could include public safety specific requirements, is being done.

Appendix A - Definitions

The following are LTE Interfaces: (Ref: TS 23.401 v 841)

- **S1-MME** :- Reference point for the control plane protocol between E-UTRAN and MME.
- **S1-U**:- Reference point between E-UTRAN and Serving GW for the per bearer user plane tunneling and inter eNodeB path switching during handover.
- **S3**:- It enables user and bearer information exchange for inter 3GPP access network mobility in idle and/or active state.
- **S4**:- It provides related control and mobility support between GPRS Core and the 3GPP Anchor function of Serving GW. In addition, if Direct Tunnel is not established, it provides the user plane tunneling.
- **S5**:- It provides user plane tunneling and tunnel management between Serving GW and PDN GW. It is used for Serving GW relocation due to UE mobility and if the Serving GW needs to connect to a non-collocated PDN GW for the required PDN connectivity.
- **S6a**:- It enables transfer of subscription and authentication data for authenticating/authorizing user access to the evolved system (AAA interface) between MME and HSS.
- **Gx**:- It provides transfer of (QoS) policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PDN GW.
    - **Gxa:-** Allows PCRF to subscribe to appropriate event triggers in the Bearer Binding and Event Reporting Function (BBERF) located in a trusted non-3GPP access gateway, as defined in 29.212
    - **Gxc**:- Allows PCRF to subscribe to appropriate event triggers in the Bearer Binding and Event Reporting Function (BBERF) located in the S-GW, as defined in 29.212.
- **S8**:- Inter-PLMN reference point providing user and control plane between the Serving GW in the VPLMN and the PDN GW in the HPLMN. S8 is the inter PLMN variant of S5.
- **S9**:- It provides transfer of (QoS) policy and charging control information between the Home PCRF and the Visited PCRF in order to support local breakout function.
- **S10**:- Reference point between MMEs for MME relocation and MME to MME information transfer.
- **S11**:- Reference point between MME and Serving GW.
- **S12**:- Reference point between UTRAN and Serving GW for user plane tunnelling when Direct Tunnel is established. It is based on the Iu-u/Gn-u reference point using the GTP-U protocol as defined between SGSN and UTRAN or respectively between SGSN and GGSN. Usage of S12 is an operator configuration option.
- **S13**:- It enables UE identity check procedure between MME and EIR.
- **SGi**:- It is the reference point between the PDN GW and the packet data network. Packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provision of IMS services. This reference point corresponds to Gi for 3GPP accesses.

- **Rf/Gz** - PCEF to Offline Charging System (OFCS) Interface as specified in 3GPP TS 32.240.
- **Ro/Gy** - PCEF to Online Charging System (OCS) Interface as specified in 3GPP TS 32.240.
- **Rx**:- The Rx reference point resides between the AF and the PCRF in the TS 23.203 [6].
- **SBc**:- Reference point between CBC and MME for warning message delivery and control functions.

Protocol assumption:
- The S1-U is based on GTP-U protocol;
- The S3 is based on GTP protocol;
- The S4 is based on GTP protocol;
- The S5 is based on GTP protocol. PMIP variant of S5 is described in TS 23.402 [2];
- The S8 is based on GTP protocol. PMIP variant of S8 is described in TS 23.402 [2].
- S3, S4, S5, S8, S10 and S11 interfaces are designed to manage EPS bearers

LTE Network elements

E-UTRAN

E-UTRAN is described in more detail in TS 36.300 [5].

In addition to the E-UTRAN functions described in TS 36.300 [5], E-UTRAN functions include:
- Header compression and user plane ciphering;
- MME selection when no routeing to an MME can be determined from the information provided by the UE;
- UL bearer level rate enforcement based on UE-AMBR and MBR via means of uplink scheduling(e.g. by limiting the amount of UL resources granted per UE over time);
- DL bearer level rate enforcement based on UE-AMBR;
- UL and DL bearer level admission control;
- Transport level packet marking in the uplink, e.g. setting the DiffServ Code Point, based on the QCI of the associated EPS bearer.

MME

MME functions include:
- NAS signaling;
- NAS signaling security;
- Inter CN node signaling for mobility between 3GPP access networks (terminating S3);
- UE Reachability in ECM-IDLE state (including control and execution of paging retransmission); - Tracking Area list management;
- PDN GW and Serving GW selection;
- MME selection for handovers with MME change;
- SGSN selection for handovers to 2G or 3G 3GPP access networks;
- Roaming (S6a towards home HSS);
- Authentication;
- Bearer management functions including dedicated bearer establishment.
- Lawful Interception of signaling traffic.
- Warning message transfer function (including selection of appropriate eNB).
- UE Reachability procedures.

NOTE: The Serving GW and the MME may be implemented in one physical node or separated

physical nodes.

Gateway General

Two logical Gateways exist:

- Serving GW (S-GW);
- PDN GW (P-GW).

NOTE: The PDN GW and the Serving GW may be implemented in one physical node or separated physical nodes.

Serving GW

The Serving GW is the gateway which terminates the interface towards E-UTRAN.

For each UE associated with the EPS, at a given point of time, there is a single Serving GW.

The functions of the Serving GW, for both the GTP-based and the PMIP-based S5/S8, include:

- the local Mobility Anchor point for inter-eNodeB handover;
- sending of one or more “end marker” to the source eNodeB, source SGSN or source RNC immediately after switching the path during inter-eNodeB and inter-RAT handover, especially to assist the reordering function in eNodeB.
- Mobility anchoring for inter-3GPP mobility (terminating S4 and relaying the traffic between 2G/3G system and PDN GW);
- ECM-IDLE mode downlink packet buffering and initiation of network triggered service request procedure;
- Lawful Interception;
- Packet routing and forwarding;
- Transport level packet marking in the uplink and the downlink, e.g. setting the DiffServ Code Point, based on the QCI of the associated EPS bearer;
- Accounting on user and QCI granularity for inter-operator charging;
- UL and DL charging per UE, PDN, and QCI(e.g. for roaming with home routed traffic).
- Interfacing OFCS according to charging principles and through reference points specified in TS 32.240 [51].

Additional Serving GW functions for the PMIP-based S5/S8 are captured in TS 23.402 [2].

Connectivity to a GGSN is not supported.

PDN GW

The PDN GW is the gateway which terminates the SGi interface towards the PDN.

If a UE is accessing multiple PDNs, there may be more than one PDN GW for that UE, however a mix of S5/S8 connectivity and Gn/Gp connectivity is not supported for that UE simultaneously.

PDN GW functions include for both the GTP-based and the PMIP-based S5/S8:

- Per-user based packet filtering (by e.g. deep packet inspection);
- Lawful Interception;
- UE IP address allocation;
- Transport level packet marking in the uplink and downlink, e.g. setting the DiffServ Code Point, based on the QCI of the associated EPS bearer;
- UL and DL service level charging as defined in TS 23.203 6;
- Interfacing OFCS through according to charging principles and through reference points specified in TS 32.240 [51].
- UL and DL service level gating control as defined in TS 23.203 [6];
- UL and DL service level rate enforcement as defined in TS 23.203 6;
- UL and DL rate enforcement based on APN-AMBR(e.g. by rate policing/shaping per aggregate of traffic of all SDFs of the same APN that are associated with Non-GBR QCIs);

- DL rate enforcement based on the accumulated MBRs of the aggregate of SDFs with the same GBR QCI(e.g. by rate policing/shaping);
- DHCPv4 (server and client) and DHCPv6 (client and server) functions;
- The network does not support PPP bearer type in this version of the specification. Pre-Release 8 PPP functionality of a GGSN may be implemented in the PDN GW;
- packet screening.

Additionally the PDN GW includes the following functions for the GTP-based S5/S8:

- UL and DL bearer binding as defined in TS 23.203 [6];
- UL bearer binding verification as defined in TS 23.203 [6];
- Functionality as defined in RFC 4861 [32].

The P-GW provides PDN connectivity to both GERAN/UTRAN only UEs and E-UTRAN capable UEs using any of E-UTRAN, GERAN or UTRAN. The P-GW provides PDN connectivity to E-UTRAN capable UEs using E-UTRAN only over the S5/S8 interface.

SGSN

In addition to the functions described in TS 23.060 [7], SGSN functions include:

- Inter EPC node signaling for mobility between 2G/3G and E-UTRAN 3GPP access networks;
- PDN and Serving GW selection: the selection of S-GW/P-GW by the SGSN is as specified for the MME;
- MME selection for handovers to E-UTRAN 3GPP access network.

GERAN

GERAN is described in more detail in TS 43.051 [15].

UTRAN

UTRAN is described in more detail in TS 25.401 [16].

PCRF

General

PCRF is the policy and charging control element. PCRF functions are described in more detail in TS 23.203 [6].

In non-roaming scenario, there is only a single PCRF in the HPLMN associated with one UE's IP-CAN session. The PCRF terminates the Rx interface and the Gx interface.

In a roaming scenario with local breakout of traffic there may be two PCRFs associated with one UE's IP-CAN session:

- H-PCRF that resides within the H-PLMN;
- V-PCRF that resides within the V-PLMN.

Home PCRF (H-PCRF)

The functions of the H-PCRF include:

- terminates the Rx reference point for home network services;
- terminates the S9 reference point for roaming with local breakout;
- associates the sessions established over the multiple reference points (S9, Rx), for the same UE's IP-CAN session (PCC session binding).

The functionality of H-PCRF is described in TS 23.203 [6].

Visited PCRF (V-PCRF)

The functions of the V-PCRF include:

- terminates the Gx and S9 reference points for roaming with local breakout;
- terminates Rx for roaming with local breakout and visited operator's Application Function.

The functionality of V-PCRF is described in TS 23.203 [6].

PDN GW's associated AAA Server

The PDN Gateway may interact with a AAA server over the SGi interface. This AAA Server may maintain information associated with UE access to the EPC and provide authorization and other network services. This AAA Server could be a RADIUS or Diameter Server in an external PDN network, as defined in TS 29.061 [38]. This AAA Server is logically separate from the HSS and the 3GPP AAA Server.

PSTN - is composed of all transmission and switching facilities and signal processors supplied and operated by all telecommunications common carriers for use by the public. Every station on the PSTN is capable of being accessed from every other station on the PSTN via the use of NANP E.164 numbers.

UE - user equipment (UE) a.k.a cell phone, subscriber unit, air card is any device used directly by an end-user to communicate to the LTE network. The UE connects to the eNb via the UU.

USIM - Universal Subscriber Identity Module is the logical entity on a UICC smart card running on a 3G mobile phone. It can store subscriber, authentication, phone contact and SMS information

UICC - Universal Integrated Circuit Card is the smart card used in the UE on a LTE network

Appendix B – Commercial and non-3GPP roaming

As stated within 3GPP TS 23.401 and TS 23.402 the EPS supports the use of both 3GPP based and non-3GPP IP access networks to access the EPC. The EPS enables the concept of trusted and non-trusted non-3GPP networks. Interworking between WiMAX IEEE 802.16e and CDMA 2000 EVDO networks are considered trusted non-3GPP networks and these will be the likely targets for roaming. An example of a non-trusted network would be a 802.11 Wi-Fi network.

- The EPS supports IETF-based network-based mobility management mechanism (e.g., PMIP) and host-based mobility management mechanism (e.g., MIP) over S2 reference points.
- The EPS supports IETF-based network-based mobility management mechanism (e.g., PMIP) over S5, and S8 reference points.

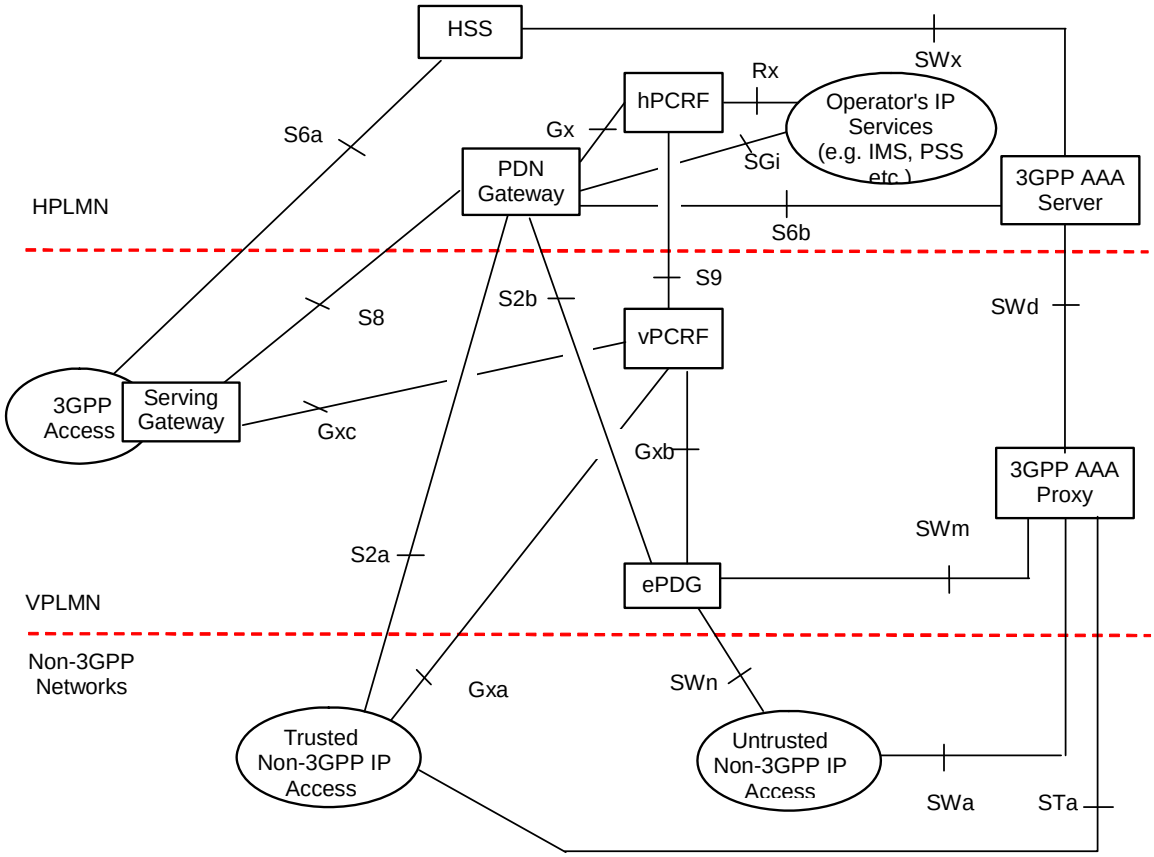
Several new interfaces can be utilized as roaming interfaces and within 3GPP there are several supported variations.

UTRAN – EPS Networks

- S12 – UTRAN to SGW
- S4 – SGSN to SGW
- S3 – SGSN to MME
- SWx and SWz – HSS and AAA

Trusted Non-3GPP – EPS Networks (Interfaces from the non-3GPP IP Access Network to EPS nodes)

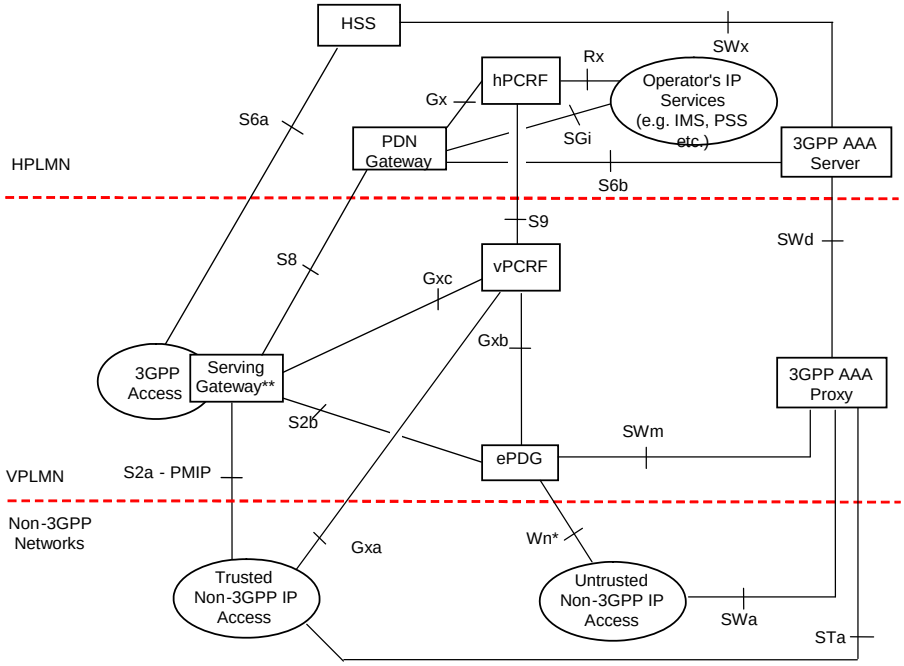
- S2a – PGW
- Gxa – vPCRF
- STa – AAA
- S2aPMIP – SGW
- S2c – UE to PGW
- S101 – MME to HRPD
- S103 – SGW to HSGW



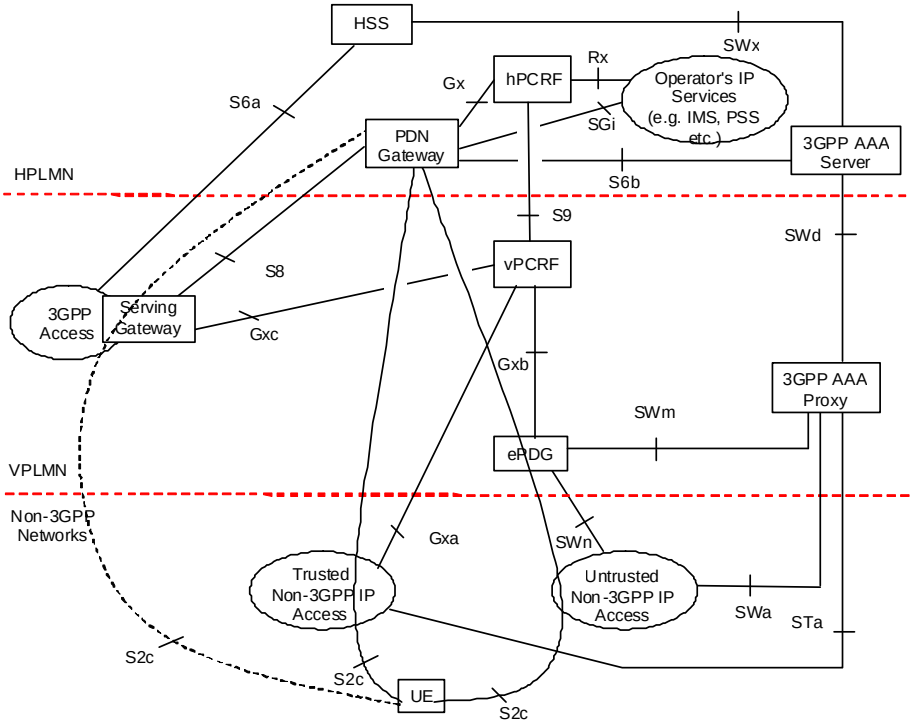
1

2 **Roaming Architecture for EPS using S8, S2a– S2b - Home Routed**

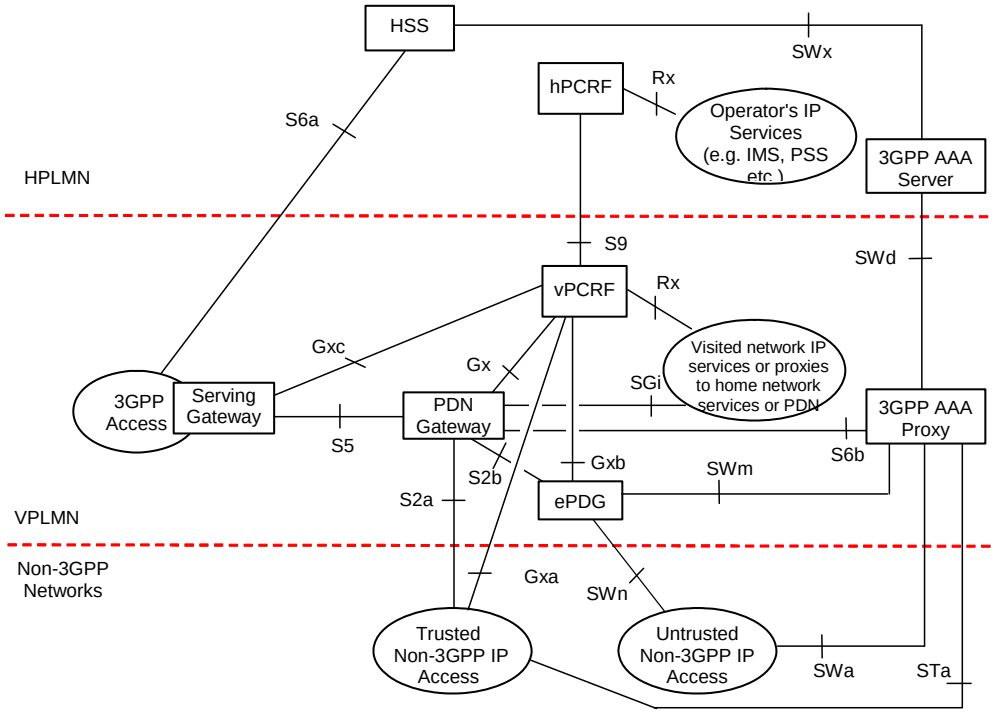
3



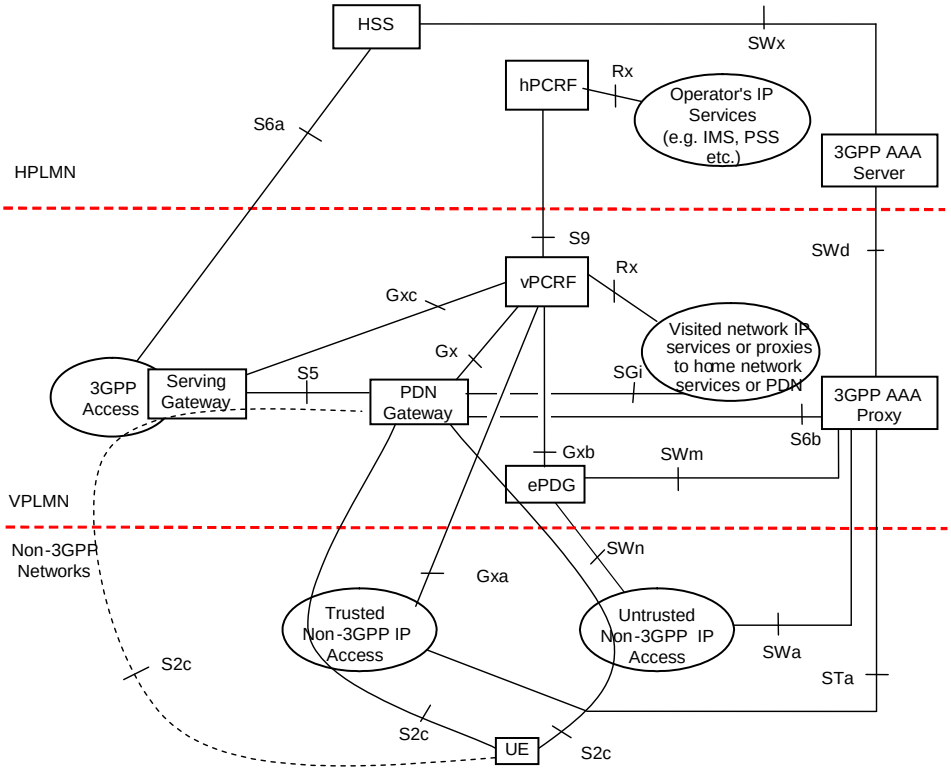
Roaming Architecture for EPS using PMIP-based S8, S2a, S2b (Chained PMIP-based S8-S2a/b) - Home Routed



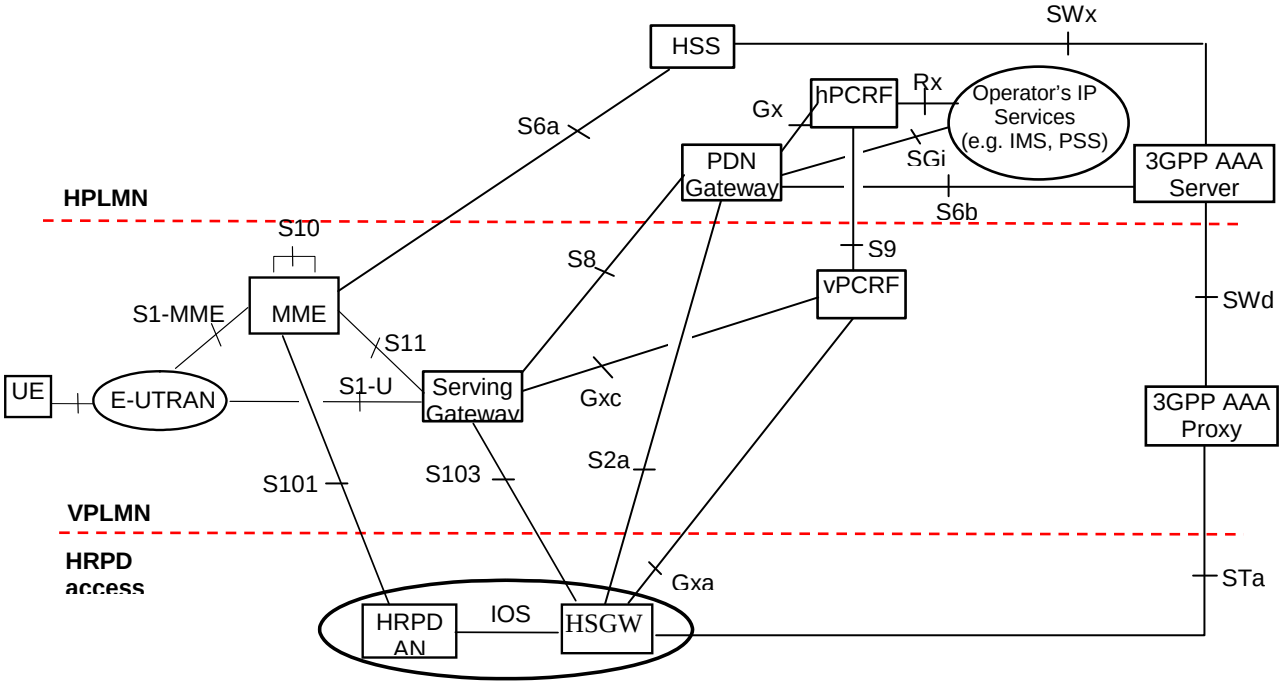
Roaming Architecture for EPS using S8 – S2c - Home Routed



Roaming Architecture for EPS using S5, S2a, S2b – Local Breakout



Roaming Architecture for EPS using S5, S2c – Local Breakout



Architecture for optimised handovers between E-UTRAN access and cdma2000 HRPD access (roaming case; Home routed)

Appendix C – PLMN ID Info

PLMN ID Information and diagrams

PLMN IDs are used in several ways in 3GPP networks:

1. The first digits in the IMSI are the PLMN ID. This assures that IMSIs assigned by different network operators are unique.
2. The PLMN ID in the IMSI is used to identify the Home Subscriber Server (HSS) containing the user's service subscription information. In case of roaming, this allows the visited network to query the HSS in the correct home network.
3. The PLMN ID is part of the Cell ID that is broadcast by each LTE cell. This allows the mobile device to first attempt to camp on a cell from the home network and camp on a visited network cell only if no home network cell is detected. The device is programmed with a list of the PLMN ID of networks that the home network operator has roaming agreements with.
4. The PLMN ID in the IMSI is used by the MME to determine whether a visiting user is allowed to connect as a roaming user. It can also be used to identify visiting users and override the requested QOS and insure that home users receive higher priority and QOS treatment
5. PLMN ID may be used to identify the home network of visiting users for the purpose of aggregating roaming usage for accounting purposes.

APN Attach Info

One very workable solution within LTE and specified in 3GPP 23.401-860 is the use of an attach (address assignment) to the default PDN, that is associated with a fully qualified domain name as the identifier. This could potentially be used as an alternative for LTE to LTE network roaming cases even if the PLMN identifier is the same. This would utilize existing methodologies within the Access Point Name (APN), the Fully Qualified Domain Name (FQDN) stored in the USIM and the Packet Data Network Gateway (PDN-GW). Once a Ue (subscriber device) in LTE attaches to any network it tries to attach to its default APN. The APN is identified by its FQDN and will result in the selection of a specific PDN GW for the default bearer.

An example would be that all networks use MCC 310 and a MNC is assigned (xxx) to the PSBL to identify public safety networks. Each network would then have their own APN, so for NYC users they may get an APN of nyc.ny.emergency-networks.net and the users in San Francisco would be sfo.ca.emergency-networks.net. To support category 1 roaming, when a NY user powers on their device in San Francisco the PLMN will be accepted (Public Safety User) and when setting up the default bearer the network in San Francisco would know to take it back to New York and vice-versa. This is one potential solution that circumvents the limitation of MNC numbering, allows for proper billing/roaming charges,

SLF Info

Another solution would be to use the Home Network Identifier (HNI), which is a combination of the MCC and MNC, to identify the PLMN. Each network would be assigned a HNI by the IMSI

Oversight Committee (IOC) which is a committee of the Alliance for Telecommunication Industry Solutions (ATIS). Unique HNIs are required to distinguish between eNodeb's from home and visited networks. The PLMN part of the IMSI (which is stored in the UICC card of the device) is used to determine the proper HSS to query for subscriber information.

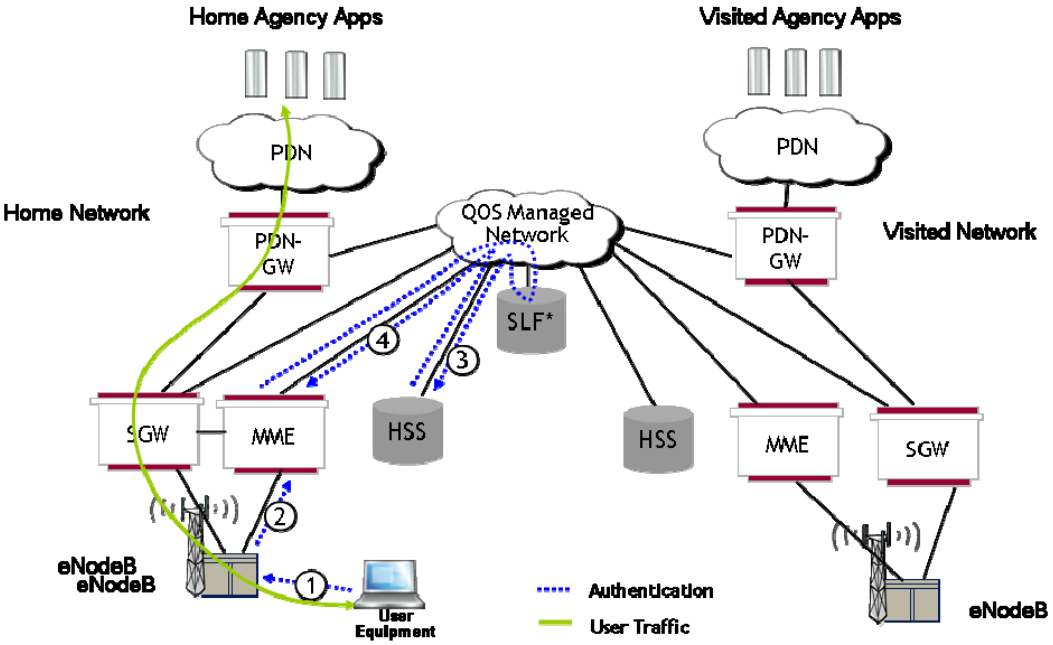
When a user roams into another network the device is programmed to first try to select Home PLMN. If the HPLMN is not available then the device is given a list of Visitor PLMNs that can be used with for roaming. A common or central HSS would be a logical solution but it may not be very practical with multiple, geographically separate systems. This means that in order for the networks by different PS agencies to have separate HSS's they must also have different HNIs. However, a common HSS is not necessarily needed even if each LTE network has the same MCC/MNC. Another possibility is where there is a SLF (Subscriber Location Function) that points to the correct HSS. This SLF could be owned by the PSST and it does not need to contain the entire user information but only the pointer to the HSS. This would work well as there is also a need for a DNS server to translate the domain name to a particular IP address. Instead of having one DNS server per market with duplicate databases there can be a few geographically distributed but logically centralized networks.

Dual USIM

Another alternative in the short/medium term solution for PS networks operating under waivers is dual-uSIM support in UE's, together with multi-mode, multi-band support for roaming to commercial 3GPP networks (rel 8 and earlier releases). This may make reduce the network integration for PS networks working under waivers.

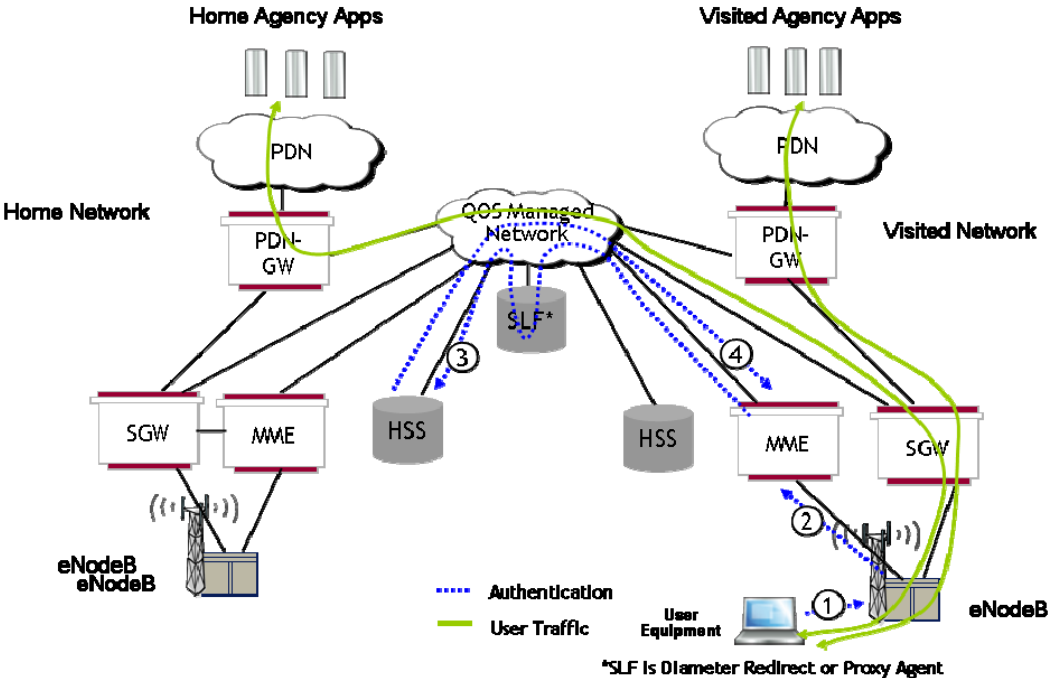
This would allow use of the device on commercial 3GPP networks without requiring a roaming agreement or interconnection between the PS LTE and commercial networks .

Network Interconnection with one PLMN id
Home Network



1
2

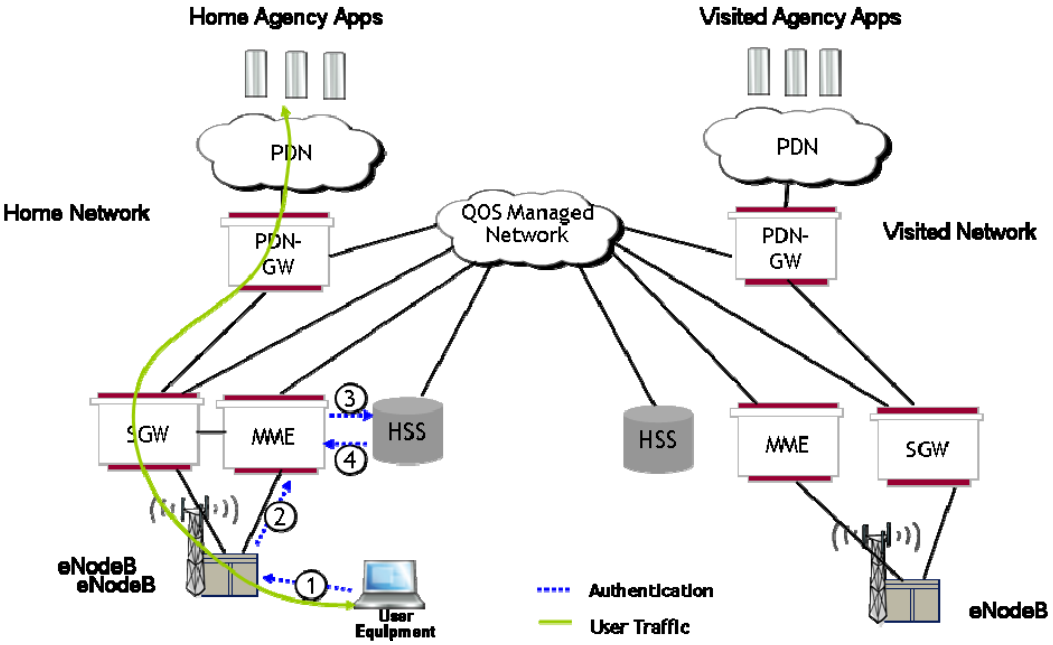
Network Interconnection with one PLMN id
Visited Network



3

4

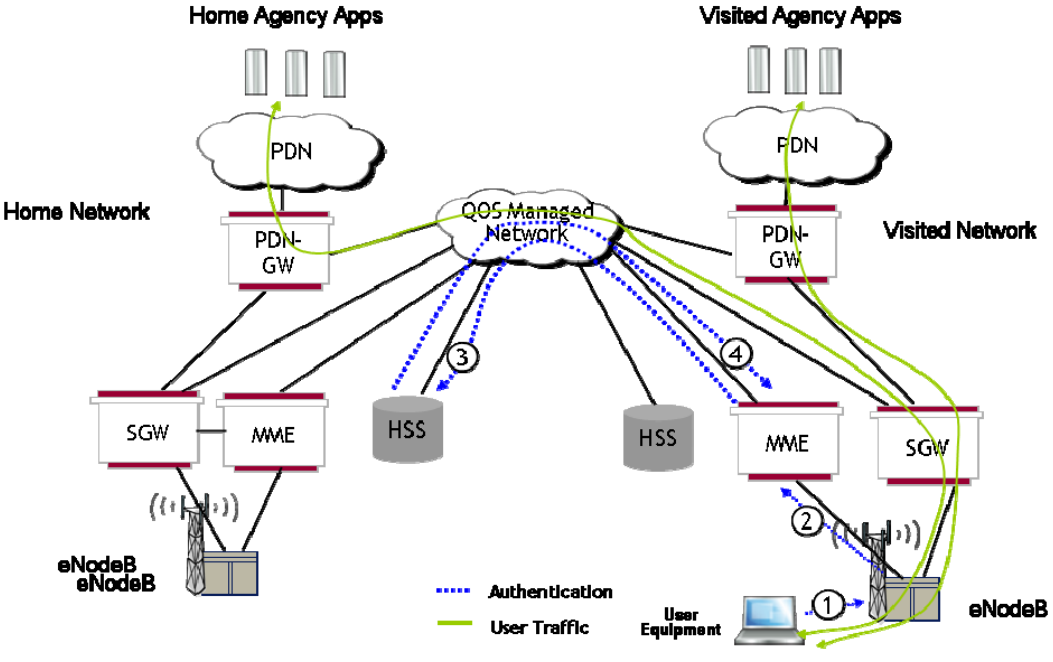
Network Interconnection with separate PLMN id for each network Home Network



1

2

Network Interconnection with separate PLMN id for each network Visited Network



3

4

Appendix D – 3GPP Standards

3GPP Release 8 Specifications (March 2009)

3GPP TS 23.401: *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*

3GPP TS 29.274: *3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3*

3GPP TS 29.275: *Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols*

3GPP Standards Required for LTE (E-UTRA) Physical Layer Interoperability

3GPP TS 36.211 Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation

3GPP TS 36.212 Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding

3GPP TS 36.213 Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures

3GPP TS 36.214 Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer – Measurements

3GPP TS 36.104 Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception

3GPP TS 36.101 Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception

3GPP Standards Required for LTE (E-UTRA) Data Link Layer Interoperability

3GPP TS 36.321 Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification

3GPP TS 36.322 Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification

3GPP Standards Required for LTE (E-UTRA) Network Layer (Access Stratum) Interoperability

3GPP TS 36.323 Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification

3GPP TS 36.331 Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification

3GPP TS 36.304 Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode

3GPP TS 25.304 User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode

3GPP Standards Required for LTE (E-UTRA) Network Layer (Non-Access Stratum) Interoperability

3GPP TS 24.301 Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3

3GPP TS 24.122 Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode

---

3GPP Standards Required for EPC S6a Interface Interoperability

3GPP TS 29.272: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (Release 8)