PSCR

Public Safety Communications Research

Public Safety 700 MHz Demonstration Network

Network Identifier Guidelines

Version 1.1

(This page is intentionally blank.)

Table of Contents

List of Tables

List of Figures

1 Overview

The primary audience for this guidelines document is Public Safety Communications Research (PSCR) program technical staff tasked with implementing network identifiers for the PSCR Public Safety 700 MHz Demonstration Network, which is based on 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) technology.

The intent of the network identifier guidelines described here is to, as best as possible:

- Replicate the network identifier architecture required for a nationwide public safety network.

- Take into account current waiver deployments.

- Test various guideline recommendations to provide feedback to Demonstration Network stakeholders.

The guidelines described here are subject to change and may change as result of lessons learned from PSCR testing.

1.1 PSCR Demonstration Network

The PSCR program has the only government or independent lab facility in the United States to test and demonstrate public safety 700 MHz broadband networks and applications. Some of the goals of the Demonstration Network are to provide:

- A vendor-neutral place for manufacturers and carriers to test their systems in a multi-vendor environment. This provides integration opportunities.

- A place for public safety to see how these systems will function, specific to their unique needs. Interested agencies can visit the network and get hands-on experience with these systems, as well as run public safety-specific test cases that relate directly to their operational environments.

- A place where early builders can test whether the systems they might procure will work in the eventual nationwide network. The test environment will assist agencies in their procurement process.

1.2 Administration Point of View

In May 2011, the National Telecommunications and Information Administration (NTIA) filed comments on behalf of the Administration (White House, DOC, DOJ, and DHS[1]), to the Federal Communications Commission (FCC) in response to FCC Service Rules for the 698-746, 747-762 and 777–792 MHz Bands for Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band and Amendment of Part 90 of the Commission's Rules.

The NTIA response filed on behalf of the Administration made it clear that, "Intra-public safety network roaming ceases to be a concern in a nationwide network, but remains a significant problem and cause of inefficiencies in a series of regional networks. The Corporation should require only a single Public Land Mobile Network (PLMN) identifier for the purpose of facilitating

---

[1] U.S. Department of Commerce (DOC), U.S. Department of Justice (DOJ), and U.S. Department of Homeland Security (DHS).

roaming among public safety users of a single nationwide public safety broadband network and commercial networks."

1.3 Single Public Land Mobile Network Identifier Advocates

PSCR believes that Public safety LTE systems must comply with 3GPP standards and therefore they must be 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 PLMN ID is the foundation for many LTE network identifiers and these identifiers also require effective coordination and management.

The stance by the Administration provides the initial viewpoint from which the network identifier (network ID) guidelines described here are designed. These guidelines have the overwhelming support from the Administration, Industry and Public Safety Organizations as reinforcement for a single, common PLMN ID.

Figure 1. PLMN ID Contributors
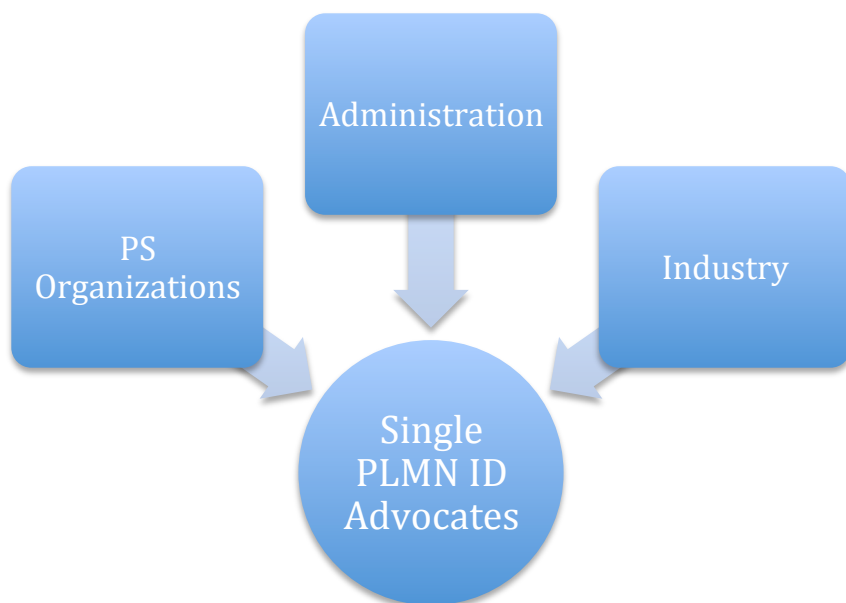
The network examples shown throughout these guidelines have the intent of a single PLMN ID within the concept of a nationwide Public Safety LTE Network. Use of a common, single PLMN ID provides the foundation as the "common denominator" for the remaining LTE network IDs. [2,3,4]

---

[2] August 2011 - ATIS WTSC sent an industry support letter to the IOC for a single PLMN for public safety

[3] May 2011 - NTIA filed comments on behalf of the Administration to the FCC Service Rules for the 698-746, 747-762 and 777-792 MHz Bands

[4] March 2011 – NPSTC board supports single PLMN ID usage – www.npstc.org

September 2011 – APCO board supports single PLMN ID usage – www.apcointl.org

2   Public Land Mobile Network Identifier Structure

A Public Land Mobile Network Identifier or PLMN ID is a five- or six-digit combination of numbers that consists of a three-digit Mobile Country Code and two- or three-digit Mobile Network Code (MNC). The term PLMN is also synonymous with Home Network Identifier (HNI) and Public Mobile Network (PMN).

NOTE: The United States typically implements three-digit MNCs.

The Mobile Station Identification Number (MSIN) is a unique number within a PLMN consisting of 9 or 10 digits. When the MSIN is appended to the PLMN is creates the globally unique International Mobile Subscriber Identifier (IMSI). A unique IMSI is assigned to each user equipment (UE) within a network.

Figure 2. IMSI and PLMN ID Structure
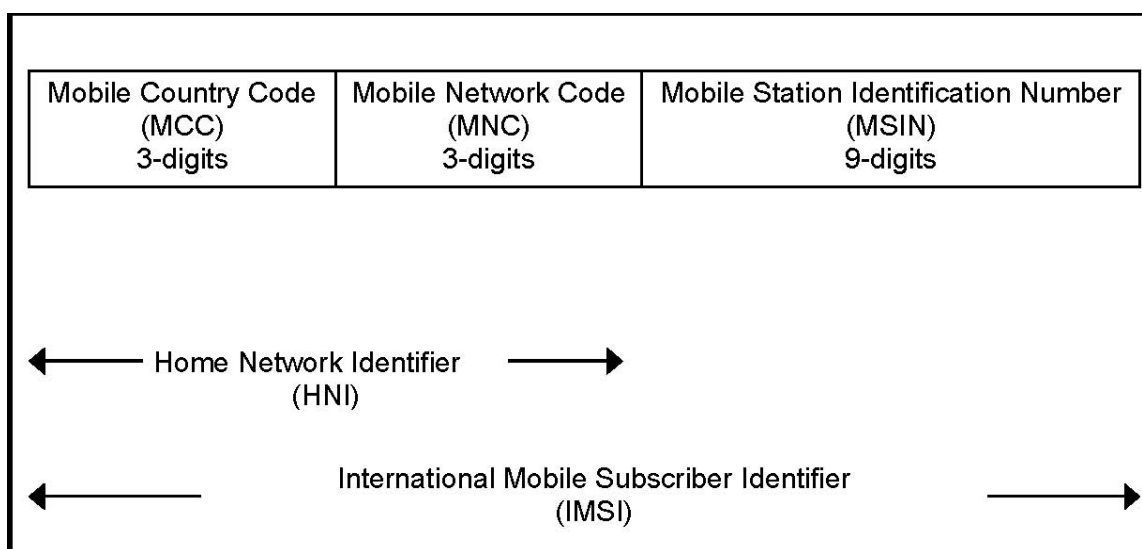
The MCC and MNC are used in the following manner: [5]

- The function of the MCC is to identify the domiciliary country of a mobile terminal/user.

  o By analyzing the MCC, a visited network can determine the country from which the mobile terminal/user originated and in which its home network resides.

- The function of the MNC is to identify the home network, within the country associated with the MCC, of the visiting mobile terminal/user.

  o The visited network uses the MCC-MNC combination to identify and query the home network of the visiting mobile terminal/user that is requesting service.

- The IMSI is used for:

  o Determination of the mobile terminal's/user's home network,

  o Mobile terminal/user identification when information about a specific mobile terminal/user is to be exchanged between visited and home networks,

---

[5] Excerpt taken from IMSI Oversight Committee Guidelines – www.atis.org/ioc/guidelines.asp

- o Mobile station identification on the radio control path for registering a mobile station in a visited wireless network,

- o Mobile station identification for signaling on the radio control path,

- o Identification of the mobile terminal/user to allow for charging and billing of visiting mobile terminals/users, and

- o Subscription management, i.e., retrieving, providing, changing, and updating subscription data for a specific mobile terminal/user.

2.1 Network Identifiers Review

The PSCR program initiated a Network Identifiers Study Item to determine key LTE network parameters governed by the PLMN ID that should be managed throughout the network. Because these parameters have a significant impact on a LTE network, the PSCR program sought comments from all stakeholders during a series of six meetings. Stakeholder input helped inform PSCR on the findings throughout this document and provide a guideline to use in testing these various parameters in the Demonstration Network. Additionally, the results from testing in the Demonstration Network will be used to help inform the Administration and Demonstration Network stakeholders.

- PSCR determined five initial identifiers (with additional sub-identifiers) that require national management

  - o IMSI – includes PLMN (MCC + MNC) and MSIN

  - o TAI – Tracking area ID

  - o GUTI – Globally Unique Temporary UE ID

  - o ECGI – E-UTRAN (Evolved UMTS (Universal Mobile Telecommunications System) Terrestrial Radio Access Network) Cell Global ID

  - o APN – Access Point Name

- Further research shows that some "permanent" LTE (non-IMS) network identifiers need to be managed or coordinated at some level. These include the evolved packet core (EPC) identifiers (see Appendix C for ID definitions) Table 1 lists.

Table 1. EPC IDs

MMEI	MMEC	MMEGI	IMEI/SV[6]	TAC
ECI	Global eNB ID	eNB ID	IMEI[2]	HA-APN
GUMMEI	TAI List	P-GW ID	MSISDN[7]	*MBMS

In addition to UE and evolved packet system (EPS) parameters, several Radio Access Network (RAN) or RAN-specific IDs (Table 2) are used for such things as managing mobility, identifying specific cell sites, and balancing paging load.

---

[6] Partially out of scope

[7] Includes ENUM and all numbering plan info

Table 2. RAN Identifiers

ECGI	E-UTRAN Cell Global Identifier	Unique cell ID (globally)	PLMN+ECI <= 52 bits
ECI	E-UTRAN Cell Identifier	Unique cell ID (in PLMN)	ECI(28bits)=eNB ID+Cell ID
Global eNB ID	Global eNodeB Identifier	Unique eNodeB ID (globally)	PLMN+eNB ID
eNB ID	eNodeB Identifier	Unique eNB (in PLMN)	20 bits
Cell ID	eNB Cell ID	Unique for each sector of a cell/eNB	8 bits
TAI	Tracking Area Identity	Unique tracking area (globally)	PLMN + TAC
TAC	Tracking Area Code	Unique tracking area (in PLMN) Per cell in eNB	16 bits
TAI List	Tracking Area Identity List	UE can move to cells included in TAI List w/o location update	variable length

2.2 LTE Network ID Diagram

The majority of the network IDs must be programmed into their respective node at the time of commissioning. The IMSI is used in the USIM application on the UICC and is typically programmed at a secure services identity module (SIM) card factory.

Figure 3 shows the delineation of the various IDs, where they are used, and what message flows use them and when they are necessary for network provisioning and commissioning.

Figure 3. Network ID Diagram
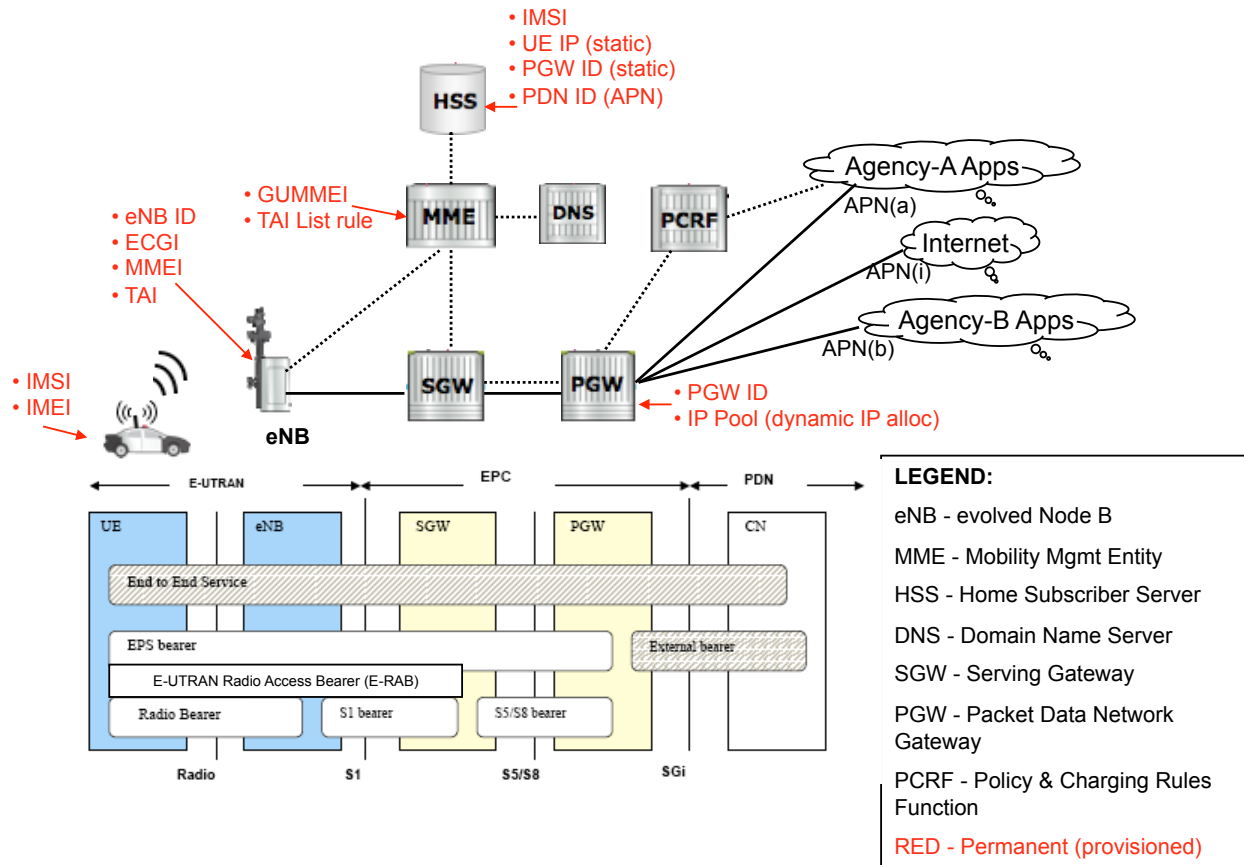
3   LTE Network Identifiers, Parameters, Values

NOTE: Detailed examples for each ID and parameter are shown in the appendices of this guidelines document.

3.1   IMSI Overview

The IMSI is globally unique for each individual user/device. The IMSI is typically stored on the USIM (e.g., "SIM" card) within the UE and also in the Home Subscriber Server (HSS), which is a database that contains all of the user's network access information.

Typically, in a nationwide network, the HSS is physically distributed for geographic redundancy but centralized in functionality (e.g., diameter redirects or mirrored databases). In lieu of pending waiver deployments, the industry-standard way of HSS implementation will need to be modified to support proper interworking between otherwise disparate networks.[8]

Current Diameter Routing Agent (DRA) technologies are capable of multiple contextual routing methods.[9] This includes routing via full IMSI analysis (all digits), partial MSIN analysis, E.164 Number Mapping (ENUM), and several other methodologies. If the signaling network infrastructure is designed properly, then the ability to route on a per UE or IMSI basis is fully supported by current infrastructure vendors. Any demarcations for IMSI blocks is then lessened and would primarily be used for network operator/ID administrator accounting between the various HSSs in the network. Using DRA would mitigate potential issues with MSIN fragmentation.

To facilitate a nationwide network architecture, while supporting waiver deployments, the following assumptions are necessary:

- Nationwide network supporting early waiver deployments – requires that a single network identifier Network operator/ID administrator be used by public safety to allocate, manage and support the approved schema.

- Single or "common" PLMN ID for all Public Safety networks

  For example, MCC=312 MNC=911 PLMN/HNI=312911

- MNC allocation will utilize a three digit number

- Unique MSIN differentiates IMSIs within a PLMN

- MSIN assumption is that nine digits are available for use (~1 Billion device IDs)

  o   Approx. 2~5 million public safety first responders (Roughly 5% of population)

  o   Approx. 24 million potential devices (1st and 2nd responders, M2M, redundancy, future growth, etc.)

- Diameter Routing Agent (DRA) required between all HSSs in network

- DRA will be required to perform IMSI range or full MSIN analysis for HSS routing

---

[8] Current waiver RFPs all utilized separate HSS nodes and have no direct connection to each other

[9] See vendor DRA presentations at
www.pscr.gov/highlights/700mhz_demo_net_122011/winter_2011_technical_workshop.php

3.2 MSIN Allocation Guidelines

1) Divide the entire 1 billion MSIN allocation into ten equal segments

   a) Each segment contains 100 million (100,000,000) contiguous MSINs

2) Utilize ~50% of initial MSIN allocation under single PLMN = 500,000,000 MSINs

   a) Future growth can then be allocated in 100M MSIN segments

   b) ID administrator will allocate new 100M MSIN segment once overall usage of a segment is at 70%

3) Partition and allocate the first 100M segment with contiguous blocks of MSINs for support of non-geographic based remote/cloud EPC systems

4) Partition and allocate the next 400M MSINs according to population density for remaining regions

5) Subdivide each MSIN segment into 50,000 MSIN block sizes = 10,000 50K Blocks

   a) Allocate 50K blocks based at a regional level

       i) Allow for state or sub-regional block allocations from regional allocation

       ii) Sub-allocations must be overseen by Network operator/ID administrator

   b) Partition contiguous blocks of MSINs for each region[10] – this is key to ensure proper routing.

   c) Allocate large "buffer zones" for each regional block that can be used for future growth (e.g., built-in MSIN reserve)[11]

   d) MSIN Blocks cannot be "split" between multiple HSSs

       i) For example, waiver has two HSSs in region and splits MSIN block between them

       ii) Entire block(s) must be implemented within the HSS

   e) Allocate more blocks out of regional buffer zone for once 70% of previous allotment is used by network operator

6) MSIN Segment 1 would have multiple allocations and rules for the following:

   a) Cloud/Remote EPC Allocations and Federal User Allocations

       i) MSIN 50K blocks would be combined in groups of 5 to create 250K Groups

       ii) Each Cloud/Remote EPC would get an entire contiguous Group assigned for their HSS. (5 MSIN Blocks)

       iii) Once utilization of 70% is achieved within the Group, the Administrator would assign another Group of 250K MSINs (i.e., 5 Blocks)

---

[10] The term "region" is used extensively throughout this document and is notional in nature. For context purposes the use of DHS/FEMA regions is used to delineate specific geographic areas and is not meant as a final determination of a specific region. Other regional designations include but are not limited to the four Region/nine Division Census Bureau and OMB Circular A-105 definitions.

[11] Based on assumption of 5 million public safety users, a 500 million allocation represents a 100-fold increase in the amount of potential users – 10,000% buffer zone.

b) Secondary Responders

    i) For example, public utilities, as approved by the public safety Network Operator/Corporation and Administrator

    ii) 50K MSIN blocks and similar rules for regional allocations would be used

c) Remaining MSIN Blocks reserved for Testing and Buffer Zones

(This page is intentionally blank.)

4 Mobility Management Entity Identifiers

Each Mobility Management Entity (MME) within a network must have a specific, unique identifier that is managed and coordinated nationally. Mobility management is typically performed locally/regionally (East, Central, West).

The components that provide access to the Internet or require high-speed access might be at a sub-regional level (i.e., state or sub-state) to reduce transport costs (e.g., Packet Data Network (PDN) Gateway (P-GW), Serving Gateway (S-GW)). This regional and sub-regional breakdown ensures that traffic is managed appropriately and that devices are paged and tracked accordingly.

There are two specific parameters that define the MME and the group that the MME belongs too.

- MMEC – The MME Code identifies and is assigned to a specific MME. The MMEC is 8 bits (FF) and allows up to 256 unique values per MME Group.

- MMEGI – The MME Group ID [16 bits (FFFF)] is used to identify a group of MMEs. These MMEs are distinguished through the use of the MMEC

The MMEC and the MMEGI in addition to the PLMN ID create a number of derived identifiers that are used continually throughout the LTE system. These are depicted in Figure 4.

- MMEI – MME ID unique within a PLMN = MMEGI + MMEC, 24 bits

- GUMMEI – Globally Unique MME ID = PLMN + MMEI, 48 bits

- GUTI – Globally Unique Temporary UE ID = GUMMEI + M-TMSI, 80 bits

Figure 4. GUTI Structure
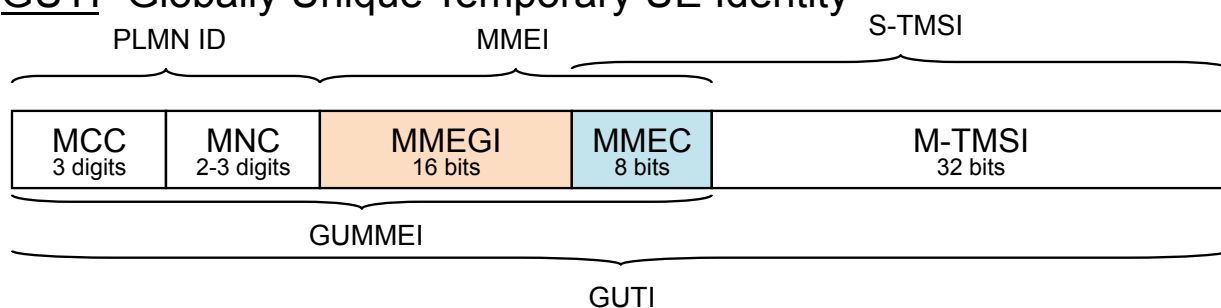
4.1 MME ID Allocation Guidelines

Creating a nationwide public safety broadband network will require that MMEs be combined across states or regions to form MME pools. MME pools as defined by the MMEGI, allow multiple MMEs to act as one MME sub-system. This in-turn provides multiple redundancies and load sharing and capacity that a single MME cannot achieve.

If too many MMEGIs are created, then potentially the MMEs within an older MMEGI will need to be reprogrammed with the national MMEGI scheme, causing system outages. Remote/hosted EPC services must also be accounted for and supported.

Figure 5. MME IDs

Regional MME ID Allocations & Ranges

Region	National MMEGI	Cloud MMEGI	Regional MMEGI	MMEC Range
TOTAL FEMA I	1000	0080	00FF	00 - FF
TOTAL FEMA II	1000	0180	01FF	00 - FF
TOTAL FEMA III	1000	0280	02FF	00 - FF
TOTAL FEMA IV	1000	0380	03FF	00 - FF
TOTAL FEMA V	1000	0480	04FF	00 - FF
TOTAL FEMA VI	1000	0580	05FF	00 - FF
TOTAL FEMA VII	1000	0680	06FF	00 - FF
TOTAL FEMA VIII	1000	0780	07FF	00 - FF
TOTAL FEMA IX	1000	0880	08FF	00 - FF
TOTAL FEMA X	1000	0980	09FF	00 - FF

Sub-regional Allocation

California	Regional MMEGI	MMEC Range
Bay-RICS	07EF	00 - FF
LA-RICS	07FF	00 - FF

- **Two Waivers are located within a single region.**
- **Each system gets a MMEGI assigned to it from the regional pool (1byte offset)**

Following are guidelines for allocating MME IDs:

1) Do not specifically lock MMEGI to specific state or region

    a) Notionally assign one MMEGI per region and provinces. The MMEGI can span multiple states/regions pending on overlapping coverage and approval from network operator/ID administrator

    b) If there is more than one waiver recipient in a DHS region then each waiver network within that region should receive a single unique MMEGI, as in, one unique MMEGI per waiver recipient within region

    c) Additionally, each DHS region should get a MMEGI assigned for remote EPC/hosted solutions

2) Allocate MMEGI on an as needed basis after pending specific implementation guidelines are met, for example:

    a) Scale to MME performance criteria (vendor specific)

      i)   Number of cells served, i.e., 3000 cells

      ii)   Number of subscribers served, i.e., 250,000 subs

   b) Ensure no overlap of areas with other MMEGI

   c) Ensure each MMEGI is unique per given area

3) Develop strict guidelines for assigning more MMEGIs beyond initial allocation

4) Assign static MMEGIs for *potential* future pooling, secondary use and Gateway Core Network (GWCN) network sharing configurations

   a) Regional MMEGI - common one for all regions (nationwide)

5) MMEC – MME Code that is unique in a MME Group ID, 8 bits (FF)

   a) Provision each MME within a regional MMEGI with a *unique* MMEC – this will need to be assigned by the Administrator with the MMEGI

      i)   Allocate as necessary for MME deployments

      ii)   For example, allocate as needed for deployments (Max up to 255 per MMEGI)

   b) Assign MMEC ranges to MMEGI to prevent overlap of IDs

      i)   Allocate enough practical MMEGI and MMEC IDs for public safety deployment

      ii)   May help facilitate future integration of network from waiver to nationwide network

   c) MMECs within a MMEGI are not required to join into a pool

6) FQDN required for MME routing – local DNS managed, for example:

   a) mmec<**MMEC**>.mmegi<**MMEGI**>.mme.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

   b) mmec**255**.mmegi**4095**.mme.epc.mnc911.mcc312.3gppnetwork.org

7) FQDN required for MME pooling – local and root DNS managed, for example:

   a) mmegi<**MMEGI**>.mme.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

   b) mmegi**4095**.mme.epc.mnc911.mcc312.3gppnetwork.org

4.2 MME ID Testing

Phase 3, Part I and Part 2 of the public safety broadband Demonstration Network testing will encompass multiple MME testing based on:

- MSF2009.003 LTE IOT test plan from MSF

- MSF2011.048.03 LTE EPC Certification Program

GUMMEI iterations tested will be based on this Study Item. Tests will tentatively include multi-vendor MME pooling (interoperability).

(This page is intentionally blank.)

5 eNodeB Identifiers

5.1 E-UTRAN Cell Global Identifier Allocation Guidelines

Within the nationwide network and for each waiver deployment, every eNodeB (cell site), also known as eNB, and cell (sector) needs to be uniquely identified. The E-UTRAN Cell Global Identifier (ECGI) parameter provides this globally unique identifier and consists of two separate IDs:

- eNB ID used to identify an individual eNodeB – does not necessarily need to be contiguous within network

  20 bits = FFFFF = 1,048,575 (7 digits)

- Use Cell ID 01-06 range to define specific cell (**cell = sector**) of eNB ID

  8 bits = FF = 255 (3 digits)

The ECGI is required at every eNodeB for commissioning and requires a FQDN for the Global eNB ID. For example, *enb<eNodeB-ID>.enb.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.*

Figure 6. ECGI Structure
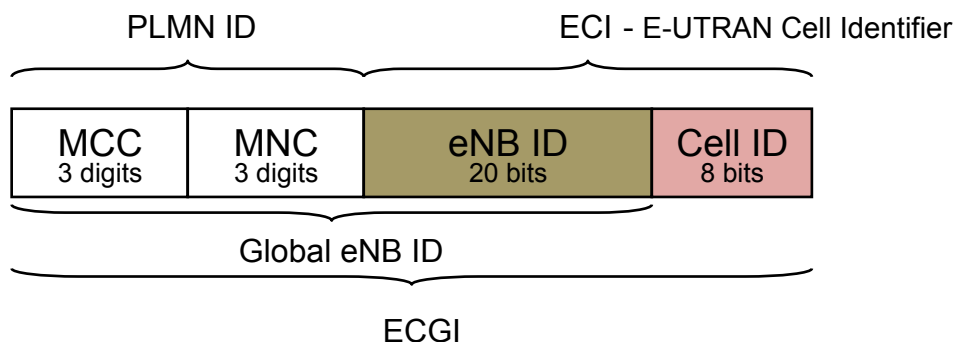
Following are guidelines for allocating ECGIs:

1) An ECGI is required for every public safety eNodeB:

   a) Must be *unique* for each eNB (macro, femto, pico)

   b) The eNB ID should be allocated by the network operator/ID administrator to the network operator

   c) The Cell ID is implemented by the network operator:

      i) It is the responsibility of the network operator to send all Cell ID information to the administrator regularly.

      ii) Network operator/ID administrator database should reflect entire ECGI, i.e., match eNB and Cell IDs within a network.

2) Allocate 10% of eNB IDs for nationwide coverage:

   a) Leave remaining in reserve for future use, femto/pico deployments

b)   1,048,575 x 10% ~ **104,857 eNB IDs[12]**

3)   Subdivide eNB IDs into 128 size blocks

   a)   Allows build out for networks in manageable size

   b)   Allocate eNB IDs per percent of population coverage in each region

   c)   Once eNB block usage hits 90%, allocate individual blocks as necessary from reserve

4)   Use Cell ID 001-006 range to define specific cell (sector) of eNB ID – every sector must be identified within a cell by the network operator – this information is sent back to the Administrator

   a)   Append 8 bits to right of eNB ID, for example:

      i)   Cell 1 (alpha sector) = 001, cell 2 (beta sector) = 002…cell 6 = 006

   b)   Allow remaining digits to be used for future Home eNB or Femto/Pico cell use, if necessary

   c)   *FQDN for each Global eNB ID = enb<eNodeB-ID>.enb.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org*

      i)   For example, FQDN = enb063FC.enb.epc.mnc911.mcc312.3gppnetwork.org

5.2 Tracking Area Identity Allocation Guidelines

The Tracking Area Identity (TAI) is provisioned in the eNodeB at commissioning and is necessary for Tracking Area Update (TAU), e.g., handover (active and idle). The TAI list is used in the MME and is important for mobility if location updates are not working or updating in the MME properly. The TAI allows the UE to move to cells in its list without location update and is globally unique. The allocation of TAIs is really at the discretion of the network design for a specific area and, therefore, should not be assigned on a purely region or population.

The TAI must be managed and engineered carefully. If it is too large (i.e., contains too many eNodeBs) it may lead to excessive overhead messaging in high-traffic cells. If the TAI is too small (i.e., does not contain enough eNodeBs) it may lead to unnecessary retries of messaging to adjacent TAIs.

The TAI contains the globally unique PLMN ID and the Tracking Area Code (TAC). The TAC contains 16 bits (FFFF) = 65,535 (5 digits) and is split into upper and lower bytes. Each eNodeB cell (sector) can only be part of one TAC, meaning multiple eNodeBs are part of a TAC.

---

[12] *NOTE: Approximately 40,000 – 55,000 macro cell sites are required for 98% population coverage (estimates on Verizon and AT&T network deployments). CTIA estimates 256,920 total cell sites in the U.S. (www.ctia.org, June 2011)*

Figure 7. TAI Structure

PLMN ID

| MCC
3 digits | MNC
2-3 digits | TAC
16 bits |

TAI
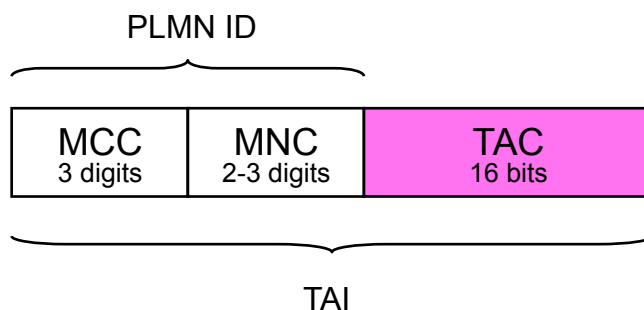
The TACs do not need to be contiguous and are not subject to the same block allocations as MSINs. For accounting purposes though, the TACs should be distributed regionally.

Table 3. Cell ID Examples

Region	Upper Byte TAC Range	Lower Byte TAC Range	Total TAC Allocations	# of eNB ID Allocations	# of eNB ID 128 Blocks	ECI Ranges
TOTAL FEMA I	00-03	00-FF	1024	4823	38	1-4823
TOTAL FEMA II	04-09	00-FF	1536	10695	84	4824-15519
TOTAL FEMA III	0A-0F	00-FF	1536	10066	79	15520-25586
TOTAL FEMA IV	10-19	00-FF	2560	19922	156	25587-45509
TOTAL FEMA V	1A-21	00-FF	2048	17406	136	45510-62916
TOTAL FEMA VI	22-27	00-FF	1536	12897	101	62917-75814
TOTAL FEMA VII	28-29	00-FF	512	4508	35	75815-80323
TOTAL FEMA VIII	2A-2B	00-FF	512	3670	29	80324-83994
TOTAL FEMA IX	2C-33	00-FF	2048	16043	125	83995-100038
TOTAL FEMA X	34-35	00-FF	512	4299	34	100039-104338

Following are guidelines for allocating TAI:

1) Allocate both upper and lower bytes of TAC to create unique TAC
   a) Ease of integration to nationwide network
   b) Simplify DNS entries
      i) Allocate Upper byte as national ID
      ii) Allocate Lower byte as regional ID
2) Allow maximum flexibility in allocation and reallocation of tracking areas
   a) Public safety LTE data usage unknown (active versus idle users, i.e., Tracking Area Updates)
   b) Public safety LTE coverage footprint will change over time. Performance impacts may be seen and require changes to balance paging load
   c) Typically TAC planning based on mobility management requirement and capacity consideration of the network – public safety LTE may require more granular updates or use TAC for jurisdictional boundaries
3) Considerations for TAC design should include
   a) End user device type – M2M (always on sensor), smartphone

b) Applications used

c) Paging capacity considerations, e.g., placing multiple TACs in high density areas

4) Initially allocate up to 20% of TAC pool - leave remaining for growth, larger TAC areas for nationwide area

    a) 16 bits = FFFF = 65,535 x 20% = 13,107 available TACs[13] (3333)

    b) Allocate regionally but allow liberal usage policy by network performance requirements

    c) Authorize and use only initial 10%, i.e., 6,554 (199A) – leave remaining in contiguous blocks for each regions reserve

    d) Once utilization hits 70% from the initial pool, allocate an additional 20% of TACs as needed from reserve pool

5) FQDN = tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

    a) For DNS architecture simplicity - align TAC high-byte boundaries (i.e., 0-255)

        i) Each region is assigned a pool of one or more unique low-byte range of values

        ii) Nationally the high-byte is managed and assigned per region as dictated by site density and traffic patterns

---

[13] Assuming approximately 50,000 eNodeBs are required for 98% population coverage and you put 10 eNodeBs per TAC, having 6,554 TAC zones should more than suffice for the initial rollout. However, each cell (sector) of a eNodeB can potentially (not likely) be in a separate zone

6 Access Point Name

The Access Point Name (APN) is a unique parameter to identify specific packet data networks that an application and/or UE can access. The APN contains unique identifiers that must be managed and coordinated nationally. Management will help to insure uniqueness in the naming so the correct Packet Data Network (PDN) is chosen (from a UE via the P-GW) for a specific application.

The APN name is defined by two specific components:

- Network Identifier (NI) – network that you are connecting to

  o Typically use multiple APNs to utilize different services

  o For example, Verizon (VZW) vzwims – voice and video, vzwadmin – test, vzwinternet – Internet and browsing, vzwapp – internal VZW apps

- Operator Identifier (OI) – consists of the PLMN ID (e.g., PLMN = 312911)

  APN OI = apn.epc.mnc911.mcc312.gprs (resolves to 3gppnetwork.org)

The OI will be a fixed/permanent identifier based upon the single PLMN ID that public safety uses.

Figure 8. Access Point Name Structure
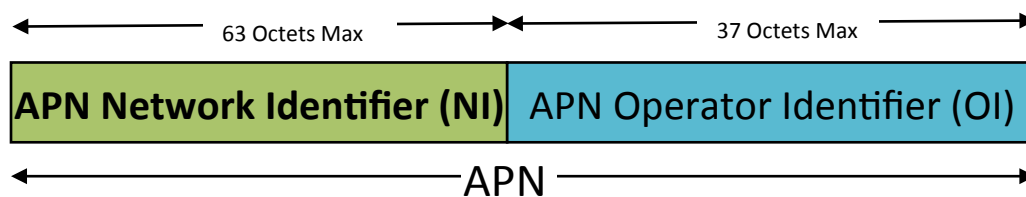
6.1 Nationwide APNs

All public safety users nationwide will require specific common applications and services. To facilitate delivery of these applications in a common manner, with a proper Quality of Experience (QoE) the use of universal, national APNs in all UEs will be required. These common APNs will provide services mutually to all users in the network.

- **<Home APN name>.publicsafety** – custom APN for the region (can be multiple) that connects into specific user's data center for secure and generic (e.g., VPN) access to data services and access to national crime information databases

  FQDN=<local Home APN name>.publicsafety.apn.epc.mnc911.mcc312.3gppnetwork.org

- **ims.publicsafety** – VoLTE telephony voice, SMS/MMS services, Standardized Video services and SIP related messages routed via Mw interface

  FQDN=ims.publicsafety.apn.epc.mnc911.mcc312.3gppnetwork.org

- **mcvoice.publicsafety** – mission critical voice (over-the-top), e.g., push-to-talk (PTT), group call

  FQDN=mcvoice.publicsafety.apn.epc.mnc911.mcc312.3gppnetwork.org

- **<mgmt entity>.publicsafety** – custom APN for the region to be used only for LTE device management using OMA-DM and supervisory/OAM functions that involve the UE

  FQDN=<mgmt entity>.publicsafety.apn.epc.mnc911.mcc312.3gppnetwork.org

- **local.publicsafety** – Standardized APN , when accessing the Public Safety Broadband (PSBB) network by users from same or other jurisdictions for mutual aid and emergency situations to gain efficient access to local servers, i.e., Incident Command System (ICS), "Status/Info Home Page", etc.

  FQDN=local.publicsafety.apn.epc.mnc911.mcc312.3gppnetwork.org

6.2 Custom APN Identifiers Guidelines

In addition to the universal or common APNs, each jurisdiction may have specific services, databases or access they want to enable for their users. Custom APNs can be implemented for jurisdictions that want specific APNs to access their data and applications. However, this will require specific assignment rules and management at the nationwide level to ensure uniqueness in naming the APNs.

The custom APN schema should implement the following rules:

- Allow multiple APN naming assignments for additional national services, local, state and Federal public safety

- Two label scope classes: National (e.g., Federal) scope and Sub-national (e.g., regional) scope

  o National scope label (i.e., the right-most label) of the APN-NI field is assigned by the network operator/ID administrator to insure uniqueness, limit to 8 characters, leaving 55 characters for sub-national assignment.

     For example, **<…>.national.<APN-OI>, <…>.dhs .<APN-OI>, <…>.fema6 .<APN-OI>, <…>.ilstate.<APN-OI>**

  o Local entities (sub-national) would be required to coordinate with the national Network operator/ID administrator to insure unique label names[14]

     For example, **ims**.national, **securityalerts**.dhs, **adamsco.police.co**.fema8, **police.chi.cookco**.ilstate

     FQDN = adamsco.police.co.fema8.apn.epc.mnc911.mcc312.3gppnetwork.org

- Network operator/ID administrator would create and manage secure registration database for public safety APNs:

  o Ensures uniqueness in APNs and prevents routing conflicts

  o Single point of reference for DNS and UE programming

  o Creates common methodology for integrating new APNs

---

[14] Other public safety organizations like APCO or NPSTC could also serve in this role.

The scheme ensures uniqueness of one label field, which thereby ensures uniqueness across the nationwide network. In addition to uniqueness, common APNs can be controlled and managed via the "Shared App Networks" field. The one unique label field is the "Domain Segment" field as Figure 9 illustrates:

Figure 9. Custom Access Point Name
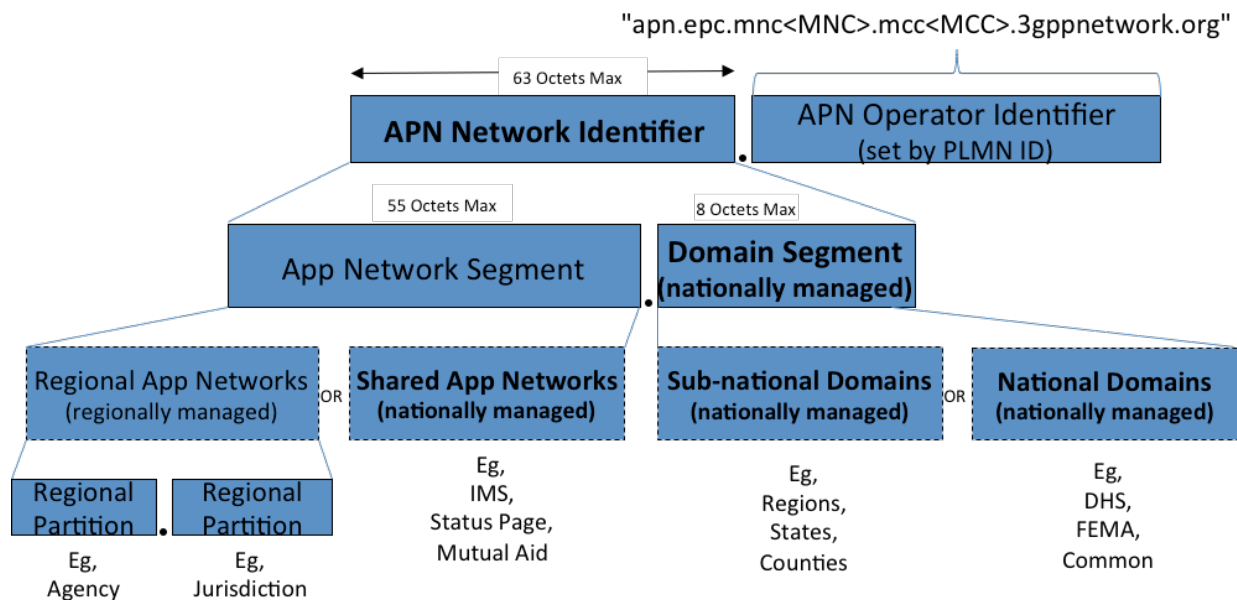
It should be noted that careful and unified planning is necessary upfront for any common/national/default APNs to prevent unnecessary outages due to reconfigurations within the UE and EPC (HSS, S/P-GW). Additionally, local APN changes will incur changes to the users in that particular waiver network. This likely will be service affecting and require reprogramming of all UEs.

The implementation of a standardized process for APN allocation will also help facilitate potential future use of UE management via Open Mobile Alliance (OMA) Device Management (DM). Although out of scope for these guidelines, OMA-DM will allow for easier migration to a nationwide network and provide common procedures to be developed in the waivers (i.e., operations support system (OSS) management). This should be a notional goal of all the waiver deployments as they become interconnected to create the nationwide network.

(This page is intentionally blank.)

7 Future Study Item Work

The public safety broadband Demonstration Network will plan to implement e.164 Electronic Numbering (ENUM) Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) for subscribers.

- Study Item needs to define a common format for public safety networks that the project can utilize, for example, +13035551212@ps.boulder.co.gov

- Action: Provide inputs on ENUM and IMSI implementations that can/should be performed in the demo network. Work with the National Emergency Number Association (NENA) on a plan for public safety

Investigate use cases for Multi Operator Core Network (MOCN) for public safety

- May allow for use of Equivalent PLMN (E-PLMN) ID to be used simultaneously for Federal/DOD users, e.g., Customs and Border Protection (CBP) network on the borders

- Develop use cases for public safety, e.g., public safety eNodeB transmits public safety Home Public Land Mobile Network (H-PLMN) and Equivalent Public Land Mobile Network (E-PLMN) simultaneously but E-PLMN is routed to a separate EPC (shared RAN) for DHS CBP

- Investigate standards effort versus equipment implementation (3GPP TS 23.251….R10+)

- Investigate concerns about quality of service (QoS), loading, etc.

(This page is intentionally blank.)

Appendix A   Network Identifiers Study Item Group

PSCR study item group meetings for the Public Safety 700-MHz Demonstration Network are open and public. The intent of study item group meetings is to obtain information and viewpoints from individual attendees. No consensus or recommendations are sought from the group as a collective. PSCR uses individual inputs to guide any final decision-making.

PSCR is the primary lead for each group, hosts the web portal, and hosts the meetings of the groups. Stakeholders are divided into two categories:

- Collaborators – stakeholders who submit verbal or written comments

- Participants – those who attend meetings for informational purposes

PSCR reserves the right to work with Cooperative Research And Development Agreement (CRADA) partners, collaborators or participants for specific study item deliverables.

A.1 Scope of Work

The goal of the Network Identifiers study item group is to help develop requirements for a single nationwide public safety 700-MHz PLMN. Tasks include:

- Develop network identifier requirements for a single nationwide PLMN for public safety (700 MHz) and the support test cases to evaluate the requirements:
  - Multiple jurisdictions with local control of infrastructure
  - Multiple regional redundant EPC data centers
  - Multiple eNodeB and EPC vendors
  - Evaluate Network ID usage and deployment options:

    Consider how to integrate waiver recipient networks into a national network

    Define technical requirements and dependencies for determining/choosing network identifiers that can be used by TBD governance organization

- In Phase 1, consider:
  - Single band (Public Safety Broadband Licensee (PSBL) Band 14)
  - Common APN naming scheme with local/regional flexibility
  - "Splitting" network identifiers under one PLMN
  - Solutions for user identity to HSS resolution
  - DNS and sub-domain naming between EPC data centers

- In Phase 2 consider:
  - Commercial carrier roaming; regional subscription zones
  - Inter-PLMN handovers (intra-RAT, inter-RAT)
  - ENUM, IMS, IPX (IP eXchange) interconnect options, etc.

A.2 Study Item Deliverables

Deliverables for the Network Identifiers study item group include:

- Focus initial phase of study on 33 network identifiers (21 of 33 are "Permanent")

  - Validate feasibility of single PLMN ID for multiple jurisdictions nationwide; show model architecture of a nationwide network and use cases

  - Identify key issues to be solved (e.g., user ID to HSS resolution, subdomains, commercial roaming, etc.)

  - Identify which parameters need or should be "managed"

- Develop use cases and requirements for key issues (e.g., split IMSIs, TAIs, Diameter proxy agent, Operations and Management (O&M), etc.)

- Identify relevant 3GPP and Global System for Mobile communications Association (GSMA) technical specification references and requirements.

  Determine what GSMA IR.21 information is required for carrier roaming – may feed directly into Roaming and Clearing Study Item

- During first phase, identify additional network identifiers for second phase of study (e.g., ENUM, IMS, regional subscription zones, base station identity and color code, etc.)

Appendix B   Nationwide Network Architecture

Figure 10 provides a diagram of the nationwide network.

Figure 10. Nationwide Public Safety Broadband Network
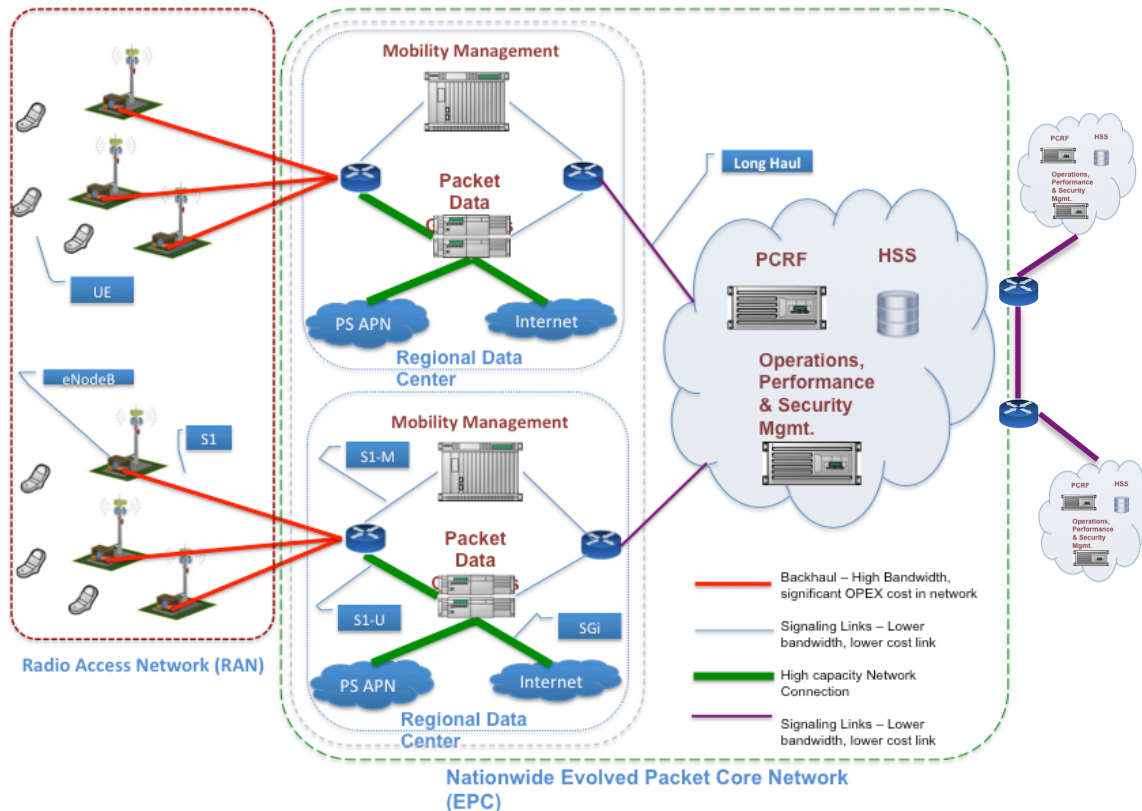
B.1 Key Architecture Points

Following are key architecture points of the nationwide public safety broadband network:

- Network Architecture would be managed nationwide and have an architected core network with:

  o A nationwide RAN using one PLMN-ID (network identifier)

  o *Does not imply a single vendor*

  o Centrally managed subscriber database, authentication, security – with local control for provisioning/management as required

- Interoperability of multiple vendors equipment within the nationwide network would be tested before network/equipment deployment

- No roaming between public safety agencies within the nationwide PSBN (all in the same network)

- Roaming in this context means PSBN users accessing commercial networks (3G/4G)

- Governance/Administration would mean a single nationwide network operator with some local flexibility and regional operations

B.2 Distributed Core Network Element Points

Some functions of the core network will be centralized and others will be distributed. For example:

- The database that contains all of the users, policy control for QoS on the system may be centralized in functionality (geographically redundant), e.g., HSS, Subscription Locator Function (SLF), Policy and Charging Rules Function (PCRF)

- Mobility management might be done locally/regionally (East, Central, West), e.g., MME

- The components that provide access to the Internet or require high-speed access might be at a sub-regional level (i.e., state or sub-state) to reduce transport costs. e.g., P-GW, S-GW

Appendix C   Glossary of Evolved Packet Core Identifiers

	Identifier	Title	Purpose	Structure	Perm / Temp	3GPP Reference
1	IMSI	International Mobile Subscriber Identity	Unique ID of LTE subscriber	PLMN+MSIN <= 15 digits	P	TS 23.003 2.1-2.3
2	PLMN ID	Public Land Mobile Network Identifier	Unique ID of PLMN	MCC+MNC <= 6 digits	P	TS 23.003 2.2-2.3
3	MCC	Mobile Country Code	Assigned by ITU	3 digits	P	TS 23.003 2.2
4	MNC	Mobile Network Code	Assigned by National Authority	2-3 digits	P	TS 23.003 2.2
5	MSIN	Mobile Subscriber Indentification Number	Assigned by Operator	9-10 digits	P	TS 23.003 2.2
6	MSISDN	Mobile Subscriber Int'l ISDN Number	Country Code, Nat'l Dest. Code, Subsc. Number (SCCP routing)	ITU-T E.164 CC, NDC, SN	P	TS 23.003 3.1-3.3
7	GUMMEI	Globally Unique MME Identifier	Unique ID of MME (globally)	PLMN+MMEI	P	TS 23.003 2.8.1
8	MMEI	MME Identifier	Unique ID of MME (in PLMN) Commissioned at eNB	MMEGI+ MMEC	P	TS 23.003 2.8.1
9	MMEGI	MME Group Identifier	Unique group ID within a PLMN	16 bits	P	TS 23.003 2.8.1
10	MMEC	MME Code	Unique ID within MME Group	8 bits	P	TS 23.003 2.8.1
11	GUTI	Globally Unique Temporary UE Identity	Alias for IMSI between UE and MME for security reasons	GUMMEI+ M-TMSI	T	TS 23.003 2.8.1
12	TIN	Temporary Identity Used in Next Update	Indicates which temporary ID will be used in next update	=GUTI	T	TS 23.401 4.3.5.6
13	S-TMSI	SAE Temporary Mobile Subscriber Identity	Temp short UE ID unique in MME Pool	MMEC+ M-TMSI	T	TS 23.003 2.8.1
14	M-TMSI	MME Mobile Subscriber Identity	Unique UE ID within MME	32 bits	T	TS 23.003 2.8.1
15	C-RNTI	Cell-Radio Network Temporary Identifier	Unique UE ID for UE with a radio resource connection within a cell	0x0001-0xFFF3	T	TS 25.331
16	eNB S1AP UE ID	eNB S1 Application Protocol UE Identifier	Unique UE ID on S1-MME interface in eNB	32-bit integer	T	TS 23.401 5.2.4
17	MME S1AP UE ID	MME S1 Application Protocol UE Identifier	Unique UE ID on S1-MME interface in MME	32-bit integer	T	TS 23.401 5.2.5
18	IMEI	International Mobile Equipment Identity	Unique mobile equipment ID	TAC+SNR+CD 15 digits	P	TS 23.003 6.2.1, 6.3
19	IMEI/SV	IMEI / Software Version	IMEI software version	TAC+SNR+SVN 16 digits	P	TS 23.003 6.2.2, 6.3
20	ECGI	E-UTRAN Cell Global Identifier	Unique cell ID (globally)	PLMN+ECI <= 52 bits	P	TS 36.413 9.2.1.38
21	ECI	E-UTRAN Cell Identifier	Unique cell ID (in PLMN)	ECI(28bits)= eNB ID+Cell ID	P	TS 36.413 9.2.1.38
22	Global eNB ID	Global eNodeB Identifier	Unique eNodeB ID (globally)	PLMN+eNB ID	P	TS 36.413 9.2.1.37
23	eNB ID	eNodeB Identifier	Unique eNB (in PLMN)	20 bits	P	TS 36.413 9.2.1.37
24	PGW ID	PDN Gateway Identity	Identifies PDN gateway HSS assigns PGW for UE context	IP Addr(4bytes) or, FQDN	P	TS 23.003, 19.1 19.2, 19.4, Anx E
25	TAI	Tracking Area Identity	Unique tracking area (globally)	PLMN + TAC	P	TS 23.003 19.4.2.3
26	TAC	Tracking Area Code	Unique tracking area (in PLMN) Per cell in eNB	16 bits	P	TS 23.003 19.4.2.3
27	TAI List	Tracking Area Identity List	UE can move to cells included in TAI List w/o location update	variable length	P	TS 24.301 9.9.3.33
28	PDN ID	Packet Data Network Identity	Access Point Name; determines PGW and PDN point of connection	APN.NI+APN.OI variable length	P	TS 23.003 9.1
29	EPS Bearer ID	Evolved Packet System Bearer Identity	Identifies EPS bearer per UE (default or dedicated)	4 bits	T	TS 23.401 5.2.1
30	E-RAB ID	E-UTRAN Radio Access Bearer Identity	Identifies E-RAB per UE	4 bits	T	TS 23.401 5.2.1
31	DRB ID	Data Radio Bearer Identifier	Identifies D-RAB pwer UE	4 bits	T	TS 36.331 4.4, 6.3.2
32	LBI	Linked EPS Bearer Identifier	IDs default bearer associated with dedicated EPS bearer	4 bits	T	TS 23.401 5.4.1 5.4.5, 5.5.1.2.2
33	TEID	Tunnel End Point Identifier	Identifies end point of GTP tunnel when it is established	32 bits	T	TS 29.060 3.1

(This page is intentionally blank.)

Appendix D   Network Identifier Examples

The MSIN range for a single PLMN that uses all nine available digits has a maximum allowable range of 1,000,000,000 unique MSINs. The initial allocation for public safety would be 500,000,000 contiguous MSINs. The remaining 500M MSINs would be subdivided into 100M segments. Once the initial 500M allocations reach 70% utilization, another segment would be allocated for use under the same allocation rules as the initial allocation.

The initial 500M and subsequent segments will be subdivided into contiguous 50,000 MSIN size blocks. Each of these 50K blocks will be made up of contiguous MSINs and multiple, contiguous 50K blocks will be assigned to each region based on population.

The first 100M segment will be used for cloud/remote EPC services, Federal users and support of the remaining US territories (e.g., Guam, Virgin Islands). Groups of five 50K contiguous blocks, 250,000 MSINs, will be allocated for each (instead of individual 50K blocks) of the networks.

D.1 Regional MSIN Allocation and Implementation Example

- PLMN = 312 911

- IMSI Range = 312911 000000000 – 312911 499999999

- Start regional implementation at second MSIN segment (leave segment 1 for testing, cloud/remote, secondary users, etc.)

  Segment 2 = 312911 100000000 – 312911 499999999

- HSS supports multiple regions

  Assign entire block(s) into HSS

- Sub-Regional allocations could go to local municipal systems (i.e., county, parish, city)

  o   Sub-regional allocations are controlled by the Network operator/ID administrator in negotiation with the public safety network operator

  o   Once the MSIN threshold is reached, another MSIN block is assigned.

Figure 11. Regional MSIN Allocation and Implementation Example

Regional Allocations
50K MSIN Block Allocations based on Regional Population Density

Region	MSIN Block Allocations
TOTAL FEMA I	370
TOTAL FEMA II	816
TOTAL FEMA III	764
TOTAL FEMA IV	1564
TOTAL FEMA V	1324
TOTAL FEMA VI	983
TOTAL FEMA VII	351
TOTAL FEMA VIII	278
TOTAL FEMA IX	1222
TOTAL FEMA X	329

- Administrator will allocate contiguous blocks to each region
- Blocks include built in reserve/zone buffers

Sub-Regional Allocations
States & Provinces

State	50K Block Allocations
New Jersey	225
New York	496
Puerto Rico	95

MSIN Block Start	MSIN Block End	State	Region	Block #	MSIN Threshold
118450000	118499999	New Jersey	2	370	118485000
118500000	118549999	New Jersey	2	371	118535000
118550000	118599999	New Jersey	2	372	118585000
118600000	118649999	New Jersey	2	373	118635000
118650000	118699999	New Jersey	2	374	118685000
118700000	118749999	New Jersey	2	375	118735000
118750000	118799999	New Jersey	2	376	118785000
118800000	118849999	New Jersey	2	377	118835000
118850000	118899999	New Jersey	2	378	118885000
118900000	118949999	New Jersey	2	379	118935000
↓	↓	↓	↓	↓	↓
129600000	129649999	New Jersey	2	594	129635000

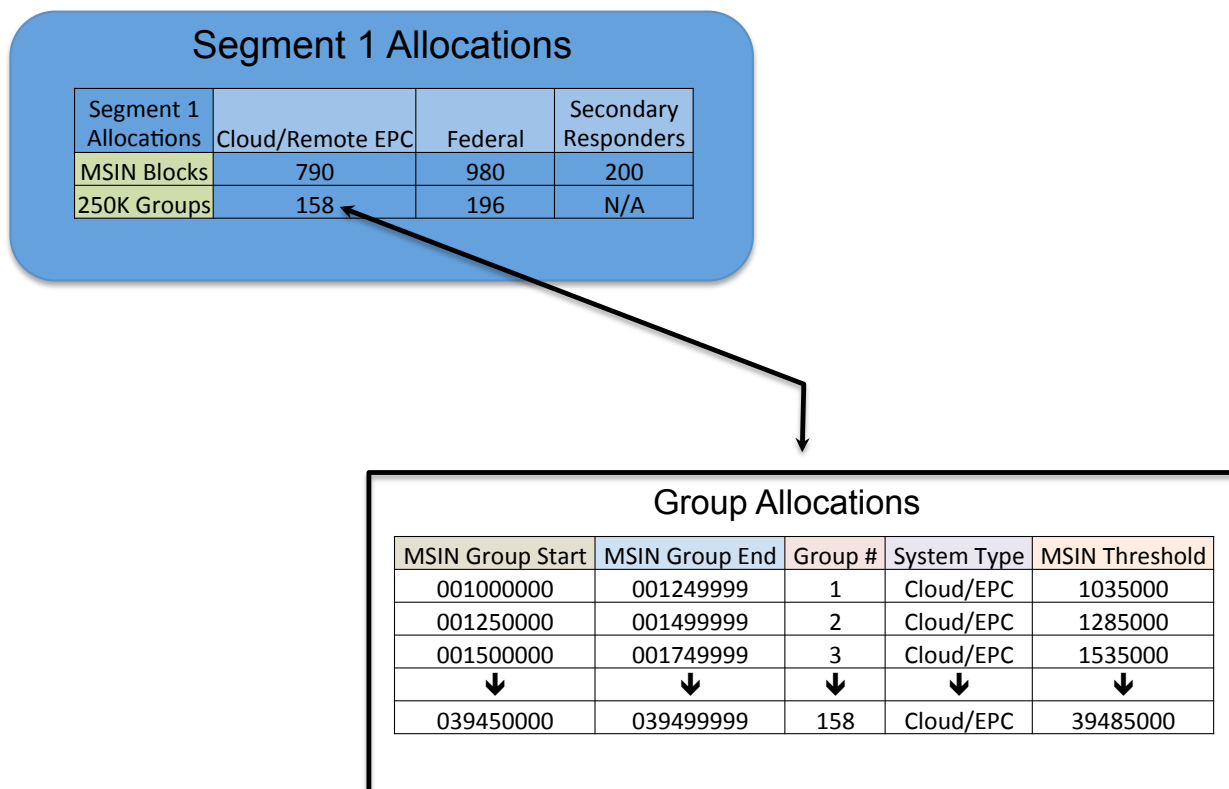**Sub-Regional MSIN Block Allocation Detail**

D.2 Segment 1 MSIN Allocation and Implementation Example

MSIN Segment 1 would have multiple allocations and rules for the following:

- Cloud/Remote EPC Allocations and Federal MSIN Allocations

    o   MSIN 50K blocks would be combined in groups of five for 250K Groups

    o   Each Cloud/Remote EPC would get an entire contiguous Group assigned for their HSS.

    o   Once utilization of 70% is achieved within the Group, another Group would be assigned by the Administrator

- Secondary Responders (e.g., Public Utilities) as approved the public safety Network Operator/Corporation and Administrator

    50K MSIN blocks and rules for regional allocations would be used

- Remaining MSIN Blocks reserved for Testing and Buffer Zones

Figure 12 highlights MSIN example allocations.

Figure 12. Segment 1 MSIN Allocation and Implementation Example

Segment 1 Allocations

Segment 1 Allocations	Cloud/Remote EPC	Federal	Secondary Responders
MSIN Blocks	790	980	200
250K Groups	158	196	N/A

Group Allocations

MSIN Group Start	MSIN Group End	Group #	System Type	MSIN Threshold
001000000	001249999	1	Cloud/EPC	1035000
001250000	001499999	2	Cloud/EPC	1285000
001500000	001749999	3	Cloud/EPC	1535000
↓	↓	↓	↓	↓
039450000	039499999	158	Cloud/EPC	39485000

D.3 MME Pooling ID Allocation and Implementation Example

Figure 13 provides a diagram of the example.

Figure 13. MME Pooling ID Allocation and Implementation Example

PLMN = 312911
MMEGI = 0x07EF = 4095   MMEC = 0x01 = 001
MMEI = 07EF01   GUMMEI = 3129114095001

MME FQDN: mmec01.mmegi07EF.mme.epc.mnc911.mcc312.3gppnetwork.org
Pool FQDN: mmegi07EF.mme.epc.mnc911.mcc312.3gppnetwork.org

GUMMEI Programmed into each MME (Can support multiple GUMMEI)

MMEC Defines specific MME

MMEGI Defines Which MMEs are in MME Pool

MMEI programmed into each eNodeB (Can support multiple MMEI)
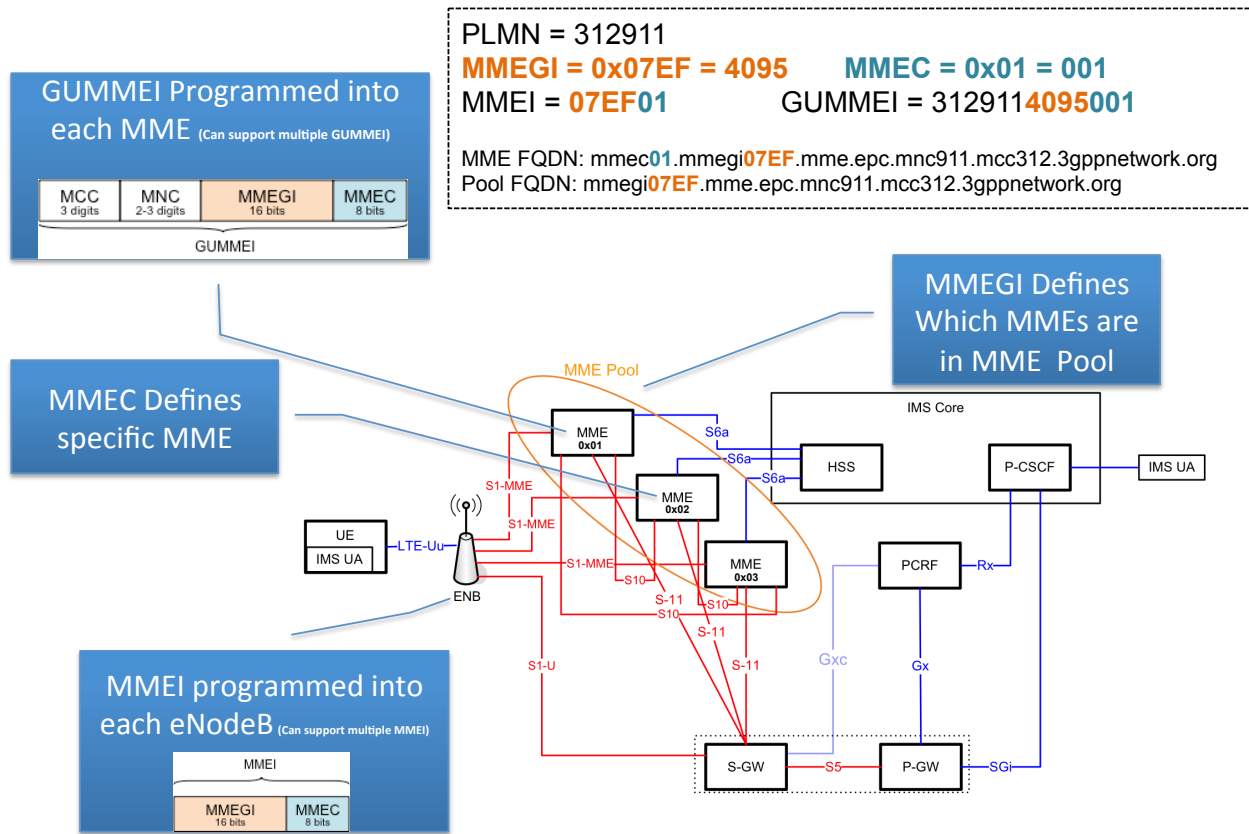
D.4 ECGI and TAI Implementation Example

PLMN = 312911

eNB ID = 03AC0

Cell ID = 001

ECI = **03AC0001**

GeNB ID = 312911**03AC0**

ECGI = 312911**03AC0001**

TAC = 2C01 and 2C03

TAI = 312911**18F8**

eNB FQDN: enb**03AC0**.enb.epc.mnc911.mcc312.3gppnetwork.org

TAC FQDN: tac-lb**F8**.tac-hb**18**.tac.epc.mnc911.mcc312.3gppnetwork.org

Figure 14. ECGI and TAI Implementation Example
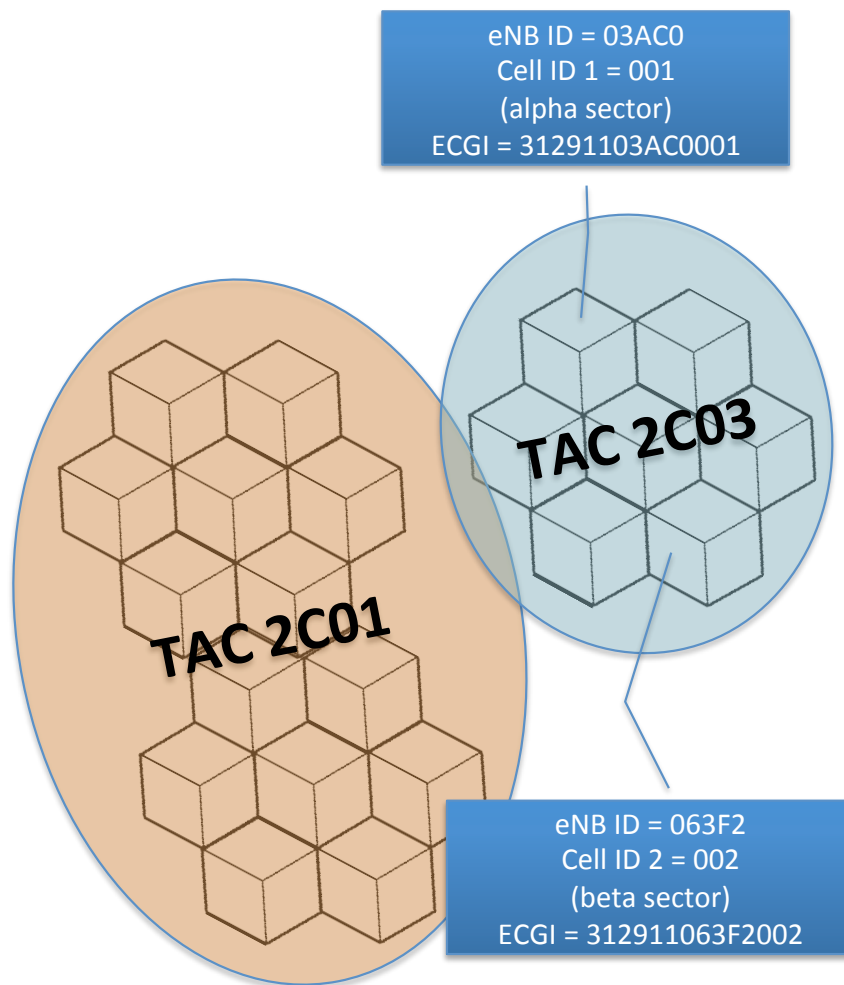
In Table 4, the TAI rule list is programmed into the MME and each UE uses the top 16 in the TAI rule list.

Table 4. TAI Rule List for ECGI and TAI Implementation

Region	Upper Byte TAC Range	Lower Byte TAC Range	Total TAC Allocations	# of eNB ID Allocations	# of eNB ID 128 Blocks	ECI Ranges
TOTAL FEMA I	00-03	00-FF	1024	4823	38	1-4823
TOTAL FEMA II	04-09	00-FF	1536	10695	84	4824-15519
TOTAL FEMA III	0A-0F	00-FF	1536	10066	79	15520-25586
TOTAL FEMA IV	10-19	00-FF	2560	19922	156	25587-45509
TOTAL FEMA V	1A-21	00-FF	2048	17406	136	45510-62916
TOTAL FEMA VI	22-27	00-FF	1536	12897	101	62917-75814
TOTAL FEMA VII	28-29	00-FF	512	4508	35	75815-80323
TOTAL FEMA VIII	2A-2B	00-FF	512	3670	29	80324-83994
TOTAL FEMA IX	2C-33	00-FF	2048	16043	125	83995-100038
TOTAL FEMA X	34-35	00-FF	512	4299	34	100039-104338