Government of Canada Gouvernement du Canada

700TAG – Technical Advisory Note #6

Impact of Network Identifiers on the Governance of a Nation-Wide Public Safety Mobile Broadband Network

700 MHz Mobile Broadband for Public Safety - Technology Advisory Group

Public Security Science and Technology **V.3** **Jan. 31, 2012**

Partners: The Technology Advisory Group for 700 MHz Public Safety Spectrum (700TAG) is composed of a collaborative group of technical experts led by Centre for Security Science and includes scientific authorities from the Communications Research Centre and technical experts from Federal, Provincial, Territorial, and Municipal agencies.

Objectives

Network identifiers comprise a set of unique characters used in identifying and referencing each network resource in a mobile radio access network, the core network, and the gateways between mobile and other networks. In the event that Canada allocates spectrum for a 700 MHz public safety mobile broadband network, a schema of network identifiers will need to be developed. The objective of this Technical Advisory Note (TAN) is to inform the Canadian public safety community on how network identifiers can be applied to the mobile broadband network and the implications of the identifier schemes on governance of the network at the national and regional levels. Two approaches are reviewed and compared: (i) a single numbering base for the entire nation-wide network, and (ii) multiple numbering bases - one for each regional public safety network.

Purpose of Network Identifiers

Network identifiers in a mobile cellular network are used to uniquely identify each and every mobile subscriber on a publicly accessible network, as well as every device that processes information that is carried on the network or controls users' access to the network. A tiered structure of network identifiers allows for locating mobile users rapidly and to hand-off sessions from one cell to another with minimal impact on the delivered service. They are used for the following purposes [1]:

a) determination of the home network of a visiting mobile terminal or mobile user;

b) determination of the visited network in which a visiting mobile terminal or mobile user is registered;

c) identification of mobile terminal or mobile user when information about a specific mobile terminal or mobile user is to be exchanged between networks offering mobility services;

d) identification of mobile terminal for registering a mobile terminal in a visited network;

e) identification of mobile terminal for signaling;

f) identification of mobile terminal or mobile user for charging and billing purposes;

g) identification of subscribers and management of subscriptions, e.g. for retrieving, providing, changing and updating of subscription data for a specific mobile terminal or mobile user; and

h) identification of a mobile user during the user authentication procedure to identify a roaming user.

Network identifiers can also be used to delineate the logical boundaries between different jurisdictional entities belonging to the same network as well as delineating domains for application data ownership. In the case where multiple operators share the same radio access network, they can be used to distinguish which users belong to which operator.

Structure of Network Identifiers

Network identifiers adhere to international conventions [1,2]. This TAN provides a high level overview of some of the network identifiers for the 3rd Generation Partnership Project (3GPP)* networks, specifically Long Term Evolution (LTE). A complete list of LTE network identifiers can be found in reference [8]. The following network identifiers are examined from the viewpoint of how they impact the architecture and the governance of the network.

a) Public Land Mobile Network Identifier (PLMN ID),

b) International Mobile Subscriber Identifier (IMSI),

c) E-UTRAN Cell Global Identifier (ECGI),

d) Mobility Management Identifiers (MMEI, MMEC, MMEGI),

* www.3gpp.org

e) Tracking Area Identifiers (TAI, TAC).

The Network Identifier (PLMN ID)

The PLMN ID is the basic identifier used to distinguish one public mobile network from all others in the world. The structure of the PLMN ID is shown in Figure 1 and a partial list of PLMN IDs assigned to Canadian wireless operators is given in Table 1. The PLMN ID comprises a 3-digit (decimal) Mobile Country Code (MCC) and a 3-digit Mobile Network Code (MNC). The Telecommunications Standardization Bureau of the International Telecommunication Union assigns MCCs for public networks. Canada is assigned MCC = 302 [3]. In Canada, the MNC is administered by the Canadian Numbering Administrator [†] by authority of the Canadian Radio-television and Telecommunications Commission (CRTC).

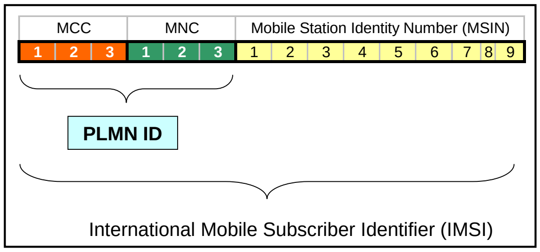

MCC
MNC
Mobile Station Identity Number (MSIN)
1 2 3
1 2 3
1 2 3 4 5 6 7 8 9
PLMN ID
International Mobile Subscriber Identifier (IMSI)

Figure 1: Structure of the PLMN ID and IMSI for LTE networks.

PLMN ID						
MCC			MNC			Name of Operator
3	0	2	6	1	0	Bell Mobility
3	0	2	6	4	0	Bell Mobility
3	0	2	2	2	0	Telus Mobility
3	0	2	2	2	1	Telus Mobility
3	0	2	8	6	0	Telus Mobility
3	0	2	3	6	0	Telus Mobility
3	0	2	7	2	0	Rogers Wireless
3	0	2	4	9	0	Globalive Wireless
3	0	2	6	6	0	MTS Mobility
3	0	2	7	8	0	SaskTel Mobility

Table 1: Partial list of PLMN IDs assigned to Canadian wireless operators.

Subscriber Identifiers (IMSI)

The 15-digit (decimal) IMSI is programmed into the Universal Subscriber Identity Module (USIM) resident on User Equipment (UE). The 9-digit MSIN is assigned by the wireless operator which means that an operator can support up to one billion unique devices on its network. For public safety applications MSIN numbers would be assigned to USIMs used by first responders as well as sensors and other machine-to-machine devices such as automatic vehicle location trackers.

Figure 2 shows an example of a USIM. The USIM contains the Home PLMN ID to which the UE belongs as well as permitted PLMN IDs and prohibited PLMN IDs. The permitted PLMN IDs represent the operators with whom the home network operator has established roaming agreements. The forbidden PLMN IDs are programmed into the USIM by the home network operator. There is also the possibility to identify which operators are preferred among the permitted operators.

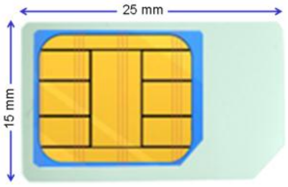


Figure 2: Example of a USIM.

Base Station Identifiers (ECGI)

The LTE base stations, also known as eNB, are uniquely identified down to their individual sectors (also referred to as cells) by the ECGI. The structure of the ECGI is shown in Figure 3.

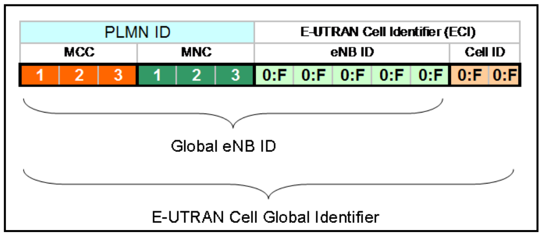


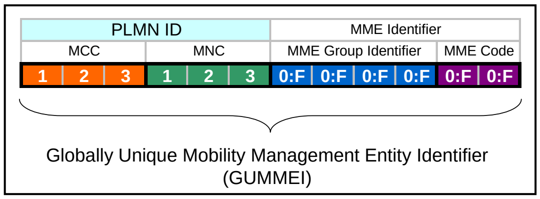
Figure 3: Structure of the ECGI for the LTE cell.

Note that the PLMN ID is part of the ECGI, thus the ECGI is globally unique. The eNB ID is a 5-digit (hexadecimal) number and is assigned by the wireless operator. There are 1,048,576 possibilities. The 2-digit (hexadecimal) Cell ID has 256 combinations and identifies the specific sector within the eNB. The ECGI is programmed into the eNB as part of configuring the equipment.

[†] www.cnac.ca

Mobility Management (MMEI, MMEC, MMEGI)

The Mobility Management Entity (MME) is the key control-node for the LTE access-network. It is responsible for idle mode UE tracking and paging procedure. It is involved in the radio resource assignment for applications (session activation and deactivation). The MME checks the authorization of the UE to register onto the service provider's mobile network and enforces UE roaming restrictions. Lawful interception of signaling is also supported by the MME. It provides the control plane function for mobility between LTE and non-LTE access networks. The MME is identified by a globally unique identifier, GUMMEI, whose structure is shown in Figure 4. There can be a maximum of 16,777,216 MMEs in an operator's network (MMEGI+MMEC = 6 hexadecimal digits). Typically, an MME could support up to 3,000 eNBs or 250,000 subscribers, whichever is more constraining for any particular deployment. So the public safety communities of many Canadian metropolitan areas would likely be fully served by one MME for each metropolitan area.



PLMN ID		MME Identifier	
MCC	MNC	MME Group Identifier	MME Code
1 2 3	1 2 3	0:F 0:F 0:F 0:F	0:F 0:F

Globally Unique Mobility Management Entity Identifier (GUMMEI)

Figure 4: Structure of the GUMMEI.

Tracking Area Codes (TAI, TAC)

Tracking Area Codes (TAC) are assigned to groups of eNBs and used for idle-state mobility management. This level of partitioning is useful to minimize the frequency of the UE updating its location to the Mobility Management Entity (MME) and thereby conserves idle-state battery power in the UE as it migrates from cell to cell. The notion of Tracking Area also minimizes the amount of signaling traffic sent across the network to UEs by directing paging requests specifically to the Tracking Area where the UE has registered its location. Groups of Tracking Areas can be used to delineate jurisdictional boundaries within the footprint of a larger network. Figure 5 is an illustration of eNBs assigned to an MME and grouped into Tracking Areas. Figure 6 shows the numbering structure for the Tracking Area Identifier (TAI), starting with the PLMN ID which indicates that the TAI is also globally unique. TAC is a 4-digit (hexadecimal) number with 65,536 possibilities.

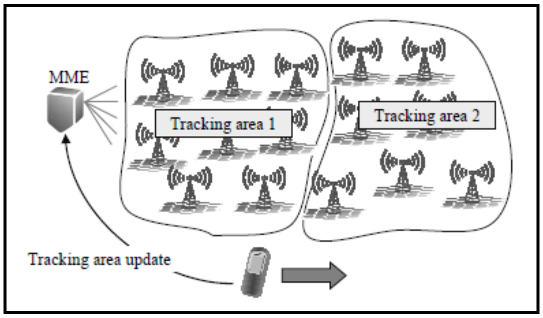
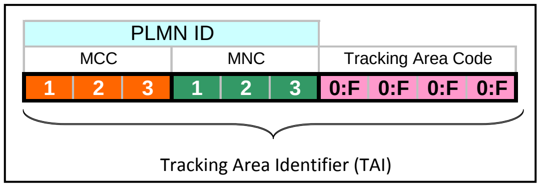


Figure 5: Illustration of grouping eNBs into Tracking Areas [4].



PLMN ID		
MCC	MNC	Tracking Area Code
1 2 3	1 2 3	0:F 0:F 0:F 0:F

Tracking Area Identifier (TAI)

Figure 6: Structure of the globally unique TAI.

One PLMN ID versus multiple PLMN IDs

The 700 MHz mobile broadband network for Canada's public safety community can be implemented with one PLMN ID for the entire nation-wide network, or it could potentially be implemented with each region having its own PLMN ID. Both options are examined from the viewpoint of technical implementation and implications for governance. Ultimately, it will be up to Industry Canada to determine which option will be adopted.

Multiple PLMN IDs

If each region were to have its own PLMN ID then they would essentially be independent network operators, just like any of the wireless operators in Table 1. Federal users with no specific geographically distinguishable regional boundaries (e.g. RCMP) could also be assigned their own PLMN ID and still be able to attach onto any regional network. They could share the infrastructure, to varying degrees, with the regional operators. The 3GPP has specified two ways for independent operators to share physical network elements in order to facilitate the hosting of virtual operators [5]. Operators who choose to share only the Radio Access Networks (eNB) are deemed to operate under the Multi-Operator Core Network (MOCN) configuration. Operators who choose to share eNB and MME are deemed to operate under the Gateway Core Network (GWCN) configuration. In both cases the UEs will be able to attach to any shared eNB. Figure 7 illustrates the MOCN configuration where, regardless of which operator owns the UE, it can attach to the Radio Access Network (RAN) of operator-A while they are in region-A. Figure 8 illustrates the GWCN configuration. Notwithstanding the sharing of infrastructure between the two operators, in order for the users to be able to register onto each other's networks, the two operators will need to establish roaming agreements between them.

The logical construct of the network identifiers for a regional operator could be as shown in Figure 9. Each region would operate its own Home Subscriber Server (HSS) and Evolved Packet Core (EPC) LTE network. The latter could be a hosted service. With roaming agreements between all regional operators, all users would be able to attach to any public safety network nation-wide. An operator representing federal users could share the infrastructure with regional operators as a Mobile Virtual Network Operator (MVNO), having its own PLMN ID. Alternatively, federal users could be covered under a logical network and roam across all regional networks.

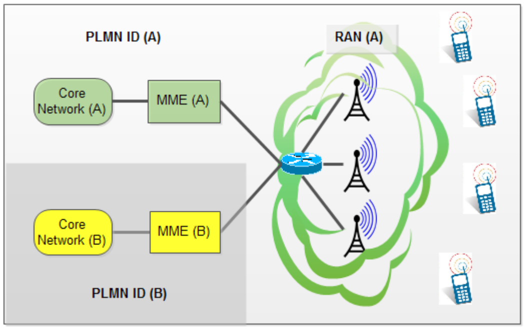


Figure 7: Multi-Operator Core Network (MOCN)

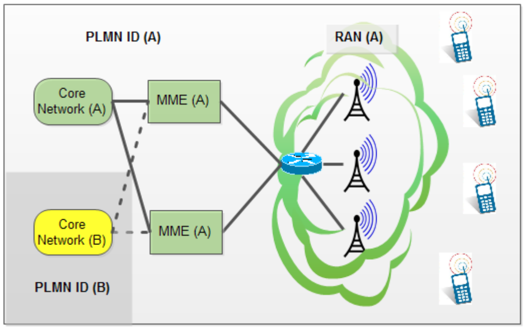


Figure 8: Gateway Core Network (GWCN).

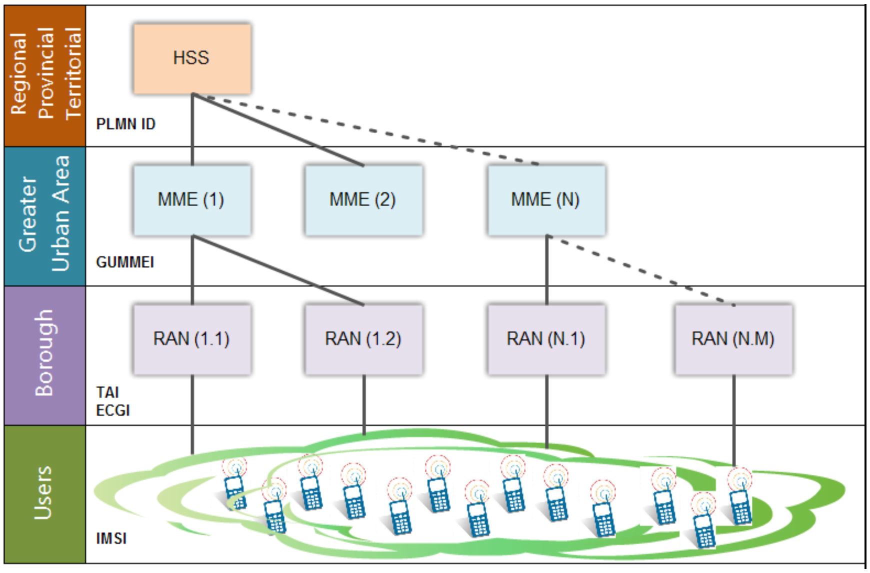


Figure 9: Possible logical construct of a regional network and hierarchy of network identifiers.

One PLMN ID for a nation-wide public safety network

Another approach to implement a nation-wide public safety network is with only one PLMN ID. With reference to Figure 9, the case of a single PLMN ID would mean that the HSS is hosted at the national level rather than having one HSS per region, province, or territory. Each region could have access to an HSS "portal" in order to manage the subscribers associated with that region. Federal users could also be managed through the same HSS portal under the control of an agency responsible for federal users. In case there are multiple independent federal agencies, each agency could access the HSS portal to manage the users under its authority. It is also possible to implement an HSS per region even under one PLMN ID. This would increase resiliency and reduce transport costs and latency at the expense of having multiple HSS.

With one PLMN ID, the notion of public safety users roaming between regions does not apply since roaming is only relevant between independent operators. All users are, therefore, considered to be in their home network. Roaming agreements would not be required between public safety jurisdictions. However, inter-jurisdictional agreements would be required in order to harmonize policies and the management of network IDs.

One PLMN ID can support 1 billion individual users (human, machine-to-machine, and sensors). Verizon Wireless and AT&T Wireless in the USA have one PLMN ID each for their nation-wide LTE networks covering 200 million and 100 million potential users, respectively. Based on 5% of the general population in 20 years' time, roughly 2 million public safety users could access the mobile broadband network. Another 8 million sensors and machine-to-machine devices could also access the network. Therefore, one PLMN ID would be more than sufficient to cover all potential subscribers on the Canadian public safety mobile broadband network for the long-term future.

Impact on Governance

Network identifiers impact the network architecture which has implications for the governance of the network. Technically, both approaches could support one national network architecture or an architecture composed of federated regional networks [7]. The main differences lie in the governance and delineation of responsibilities between regional level and national level authorities. This section examines some ways in which fundamental governance issues could be addressed by either approach.

Inter-carrier roaming agreements

Roaming agreements allow public safety users to attach to commercial networks while they are outside the footprint of a public safety network. Roaming agreements would also allow commercial users to attach to public safety network(s), subject to negotiated rules and regulatory restrictions. In the case of multiple PLMN IDs for public safety, inter-jurisdictional roaming agreements would be required between all the public safety jurisdictions. Roaming between carriers is a complex process that requires the following minimum conditions:

a) There is a physical interconnection between the partners' networks such that user and signaling information can be passed from one network to the other.

b) Roaming agreements are in place as well as the mechanisms to implement the agreements.

c) The RAN technology deployed by each carrier is supported in the UE devices.

Figure 10 is an illustration of a UE from network-B roaming onto network-A and the two types of routing that pertain to its sessions. UE(B) can access the Internet locally from the hosting network (A), whereas specific information contained only in the home network (B) is accessed via secure tunnels through to the home-based databases. The latter session typically incurs greater latency.

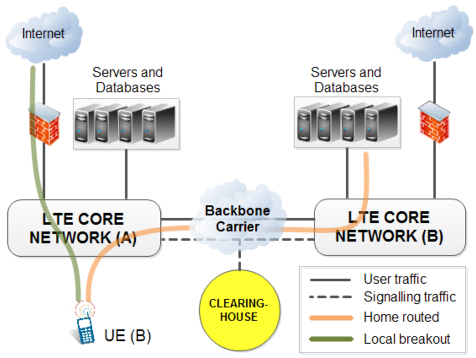
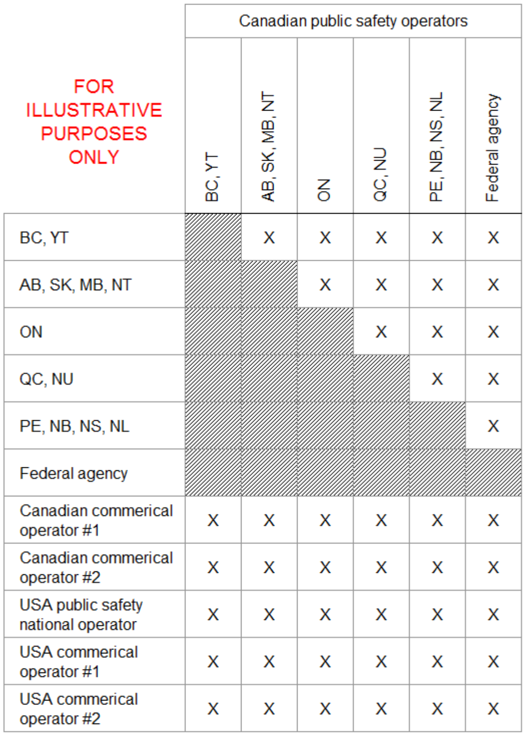


Figure 10: Home-routed access and local breakout access for a roaming UE.

With reference to Figure 10, one of the roles of the Clearinghouse is to help establish and manage the roaming agreements between the various parties. In the case that there is only one PLMN ID for the public safety network, then the public safety roaming agreements will likely be with Canadian commercial carriers, US commercial carriers, US public safety network operator(s), and possibly other international carriers. Alternatively, if each region in Canada were to have its own PLMN ID, then the number of agreements to be managed would be much higher. Table 2 shows an example of the number of roaming agreements that would be required between 6 independent Canadian regional public safety networks and 2 Canadian commercial operators, 2 US commercial operators, and 1 US public safety operator. In this example 45 agreements need to be established and maintained compared to only 5 agreements in the case of one national Canadian public safety operator.



FOR ILLUSTRATIVE PURPOSES ONLY	Canadian public safety operators					
	BC, YT	AB, SK, MB, NT	ON	QC, NU	PE, NB, NS, NL	Federal agency
BC, YT	▨	X	X	X	X	X
AB, SK, MB, NT	▨	▨	X	X	X	X
ON	▨	▨	▨	X	X	X
QC, NU	▨	▨	▨	▨	X	X
PE, NB, NS, NL	▨	▨	▨	▨	▨	X
Federal agency	▨	▨	▨	▨	▨	▨
Canadian commerical operator #1	X	X	X	X	X	X
Canadian commerical operator #2	X	X	X	X	X	X
USA public safety national operator	X	X	X	X	X	X
USA commerical operator #1	X	X	X	X	X	X
USA commerical operator #2	X	X	X	X	X	X

Table 2: Hypothetical illustration of the number of roaming agreements that would be required between multiple public safety operators and other partners.

It is evident that having more independent operators imposes a greater burden to administer the agreements which entails greater cost.

Inter-carrier billing settlement

One of the functions of the Clearinghouse is to track the charges incurred by roaming users, reconcile the balance of how much is owed to which operator, and issue the bills or pass along the payments. The allocation of charges is typically done at the level of the PLMN ID. But a finer level of granularity can be achieved down to a range of IMSI numbers. In the case of a single nation-wide public safety network, any responder that roams onto a commercial network will incur a charge that can be billed to the jurisdiction of that roaming responder.

Commercial partnerships

There can be several different types of commercial partners, such as funding partners, service delivery partners, and roaming partners. Funding partners would finance the implementation and/or operation of the networks. Service delivery partners could be commercial carriers. Roaming partners would be other commercial and public safety operators. A partner can fulfill one or more of these roles. Whether the public safety network is composed of multiple PLMN IDs or a single PLMN ID any regional jurisdiction could enter into partnership agreements independently of other jurisdictions. However, in the case of a single PLMN ID the roaming partnerships would likely be managed at the national level, but could also be managed at the regional level through a Clearinghouse using IMSI ranges.

Interoperability assurance

Interoperability is a fundamental requirement for the 700 MHz broadband public safety network, underpinned by all 5 lanes of the Interoperability Continuum [6] [‡]. Whether there is one national network operator or multiple regional operators, achieving and maintaining interoperability across multiple jurisdictions presents numerous challenges. Some of the technical challenges can be met by ensuring that all jurisdictions adhere to common technology and configuration standards. For example, a national entity could be the

[‡] The 5 lanes of the Interoperability Continuum are: Governance; Standard Operating Procedures; Technology; Training and Exercises; Usage

licensee of the public safety spectrum and sub-license the spectrum to those jurisdictions that demonstrate continued compliance to a minimum set of national interoperability standards. The national licensee would then be the internationally recognized public mobile network operator and grantee of the PLMN ID, but would be an "operator" in a titular sense only.

In anticipation of disagreements between jurisdictions that could impact interoperability, a mechanism would be required to resolve them, as well as resolving matters that fall in between regional jurisdictional responsibilities. For example, when the networks of two adjoining jurisdictions grow into each other geographically how will the issue of potential interference at the boundary between the two regions be mitigated and how will the cost be shared? A national licensee can facilitate the establishment of guidelines and dispute-resolution processes which could be co-owned by all jurisdictions.

Network Administration

An area that needs attention is the long-term continual management of network identifiers, IP addressing scheme, updating of Domain Name System (DNS) servers and Access Point Network IDs as networks grow. In the case of a single national PLMN ID, the identifiers would be managed at the national level. For multiple PLMN IDs, each regional operator would manage its identifiers, thus repeating this function among all the regions.

In addition to managing identifiers and addressing schemes, an operator would need to manage the network in the broader sense (performance, access controls, maintenance, etc.). It would be possible for any regional jurisdiction to have this ability either under one national PLMN ID or under its own PLMN ID.

Network resiliency

One of the ways to increase the resilience of the public safety network is to provide redundancy for the critical elements of the network, whose failure would result in catastrophic loss of service. Redundancy could be provided by fail-over to a neighboring network rather than duplicating the network elements which would remain in an idle stand-by mode for the vast majority of the time. For example, if a region had only one MME in its network and it failed, it is conceivable that a neighboring jurisdiction's MME could act as a back-up for the failed MME. This approach could be implemented more easily if both jurisdictions use the same PLMN ID than if each jurisdiction uses different PLMN IDs. This assumes the same vendor is used by both jurisdictions and that the network elements are maintained at the same revision levels. Cooperating jurisdictions could enter into agreements for mutual fail-over.

If two public safety regional network operators share the core and radio infrastructure with two different commercial operators, the ability to rely on neighboring network elements for fail-over may be more difficult since it is unlikely that a commercial network operator would interface its MME with another commercial operator. In this case each public safety network operator would need to rely on its partner to have a sufficiently robust back-up strategy to meet the reliability requirements of the public safety operator. If the resiliency requirements for public safety are more stringent than what the commercial operator would normally do for its commercial services, then the cost to increase robustness would likely be borne by the requesting entity.

Despite best efforts and precautions to avoid loss of service, network-wide outages do occur. If each region were to have its own PLMN ID the extent of the service disruption would likely be limited to the affected jurisdiction's network and would not impact other jurisdictions, with the possible exception of MVNO operators sharing the same infrastructure. Since even a locally contained outage is unacceptable it is desirable for first responders to have alternative ways to access critical information. In the case of Verizon Wireless' events of LTE service outages [§], their users were still able to access data services through Verizon's 3G network. Their UE devices are multi-mode and can access both 3G and LTE networks with preference given to LTE.

Interaction with Canadian regulatory agencies

The decision to assign one PLMN ID or multiple PLMN IDs to the Canadian public safety community will likely be made by an authority outside of the public safety community. If each region is granted a license to operate a mobile broadband network, then one PLMN ID would probably be assigned to each regional operator. The regulatory authority would have the responsibility to ensure that each regional network operator adheres to the regulatory framework associated with operating a wireless

[§] Verizon Wireless LTE nation-wide service disruptions reported Apr.26, Dec.7, Dec.21, 2011.

broadband communications network. However, one of the fundamental drivers for the nation-wide public safety broadband network is communications interoperability of public safety users across agencies, jurisdictions, and across Canada. In 2010 a similar situation arose in the USA. The Federal Communications Commission (FCC) imposed a number of conditions regarding interoperability on the 21 public safety waiver recipients. It also mandated the Emergency Response Interoperability Center (ERIC) to verify that the waiver recipients complied with those conditions [10]. It is reasonable to assume that in the case of independent regional public safety network operators, each Canadian regional operator would probably be required to demonstrate that it complies to some minimum conditions concerning interoperability and that this may also need to be done when upgrading the networks to ensure they remain interoperable with each other.

On the other hand, if one PLMN ID is assigned for all public safety networks in Canada, as the FCC requested be done [9] for the 21 waiver recipients, the Canadian regulatory agency could rely on the national public safety licensee to self-regulate the sub-licensing of broadband spectrum to regional jurisdictions. Furthermore, the national public safety licensee would need to demonstrate that it can ensure compliance by each jurisdictional level to the regulatory framework that may be imposed, which may include partnering or sharing to some degree with commercial operators. In this model, the regulatory authority would essentially delegate some of its compliance enforcement functions to the national public safety licensee, providing the latter can carry out that duty.

Summary

This section summarizes the advantageous governance aspects of having one PLMN ID for the nation-wide public safety mobile broadband network, as well as the advantages for governance of having one PLMN ID per regional public safety network.

<u>Advantages of having one PLMN ID for the nation-wide network</u>:

- *Managing roaming agreements* would be simpler and less costly to administer at the national level, especially with US-based carriers. The task could be facilitated through the services of a Clearinghouse provider at the national level.
- *Assuring interoperability* over the operational life the network requires dedicated and verifiable adherence to nationally accepted guidelines. A national broadband spectrum licensee could self-regulate compliance at regional levels.
- *Federal users* from independent agencies are more easily accommodated by adding HSS portals rather than requesting additional PLMN IDs.

<u>Advantages of having multiple PLMN IDs</u>:

- *Allocating bi-lateral billing credits and debits* to the responsible jurisdiction would be simpler, but can be done by IMSI ranges under one national PLMN ID.
- *Isolating network outages* to the affected region could be more easily achieved than by exposing the national network to the risk of a nation-wide outage.

<u>Governance aspects which are unaffected by the choice of one versus multiple PLMN IDs</u>:

- *Contracting authority and autonomy* for entering into agreements with commercial partners is retained at the regional and national jurisdictional levels.
- *Controlling access to the network* is within the purview of each jurisdiction, including federal agencies.
- *Monitoring and administering* the network can be done by each jurisdiction such as subscriptions and user priorities.

Conclusion

An internationally supported convention for network Identifiers has been established that pertains to LTE networks. The Canadian public safety mobile broadband network operator(s) will apply the network identifiers according to the construct that will satisfy whatever regulations accompany an anticipated pronouncement on the allocation of 700MHz spectrum for public safety. The assignment of network identifiers to the various elements of the broadband network must be done with care and attention to (i) avoid duplication, (ii) respect regional autonomy, (iii) have an efficient and resilient network, and (iv) allow for growth over time. If identifiers need to be changed at a future point in time, this could lead to network-wide outages, thus further reinforcing the need to plan the assignment of identifiers carefully at the outset.

The role of a Canadian regulatory agency, and the manner in which public safety jurisdictions would interact with it, will be strongly affected by whether only one PLMN ID will be assigned or multiple PLMN IDs. Having one PLMN ID assumes that a national public safety network licensee will be established to ensure that any regional jurisdiction, desirous to implement a public safety broadband network in its province or territory, will meet federal regulations and requirements for interoperability. This includes federal public safety operators that are likely to operate as MVNOs or operate logical networks. They could be treated as regional jurisdictions, where their regions span multiple provinces or territories.

Governance and choice of network architecture are closely linked to whether Canada's public safety broadband network will be established under one PLMN ID or under multiple PLMN IDs. Each approach has advantages with respect to the governance of the public safety mobile broadband network, ie, setting policies, achieving agreements with commercial and other partners, and administering the network. Based on the factors examined in this TAN, having one PLMN ID for the nation-wide network appears to be the better choice. While each regional jurisdiction could retain its autonomy to manage its users and direct its investments in the network, a national level entity would be required to hold the PLMN ID and provide necessary support to the regions to coordinate and provide guidance on the implementation of their networks.

References

1. "The international identification plan for mobile terminals and mobile users", International Telecommunications Union (ITU) Recommendation E.212, Oct.16, 2008.
   http://www.itu.int/rec/T-REC-E.212-200805-I

2. "Digital cellular telecommunications systems (Phase 2+); UMTS; **Numbering, Addressing, and Identification**", 3GPP TS 23.003 v8.14.0, Release 8, October 2011.
   http://www.etsi.org/deliver/etsi_ts/123000_123099/123003/08.14.00_60/ts_123003v081400p.pdf

3. "Mobile Network Codes (MNC) for the international identification plan for public networks and subscriptions (According to Recommendation ITU-T E.212)", ITU TSB, updated periodically.
   http://www.itu.int/pub/T-SP-E.212B-2011

4. Harri Holma and Antti Toskala, "LTE for UMTS – OFDMA and SC-FDMA Based Radio Access", 2009, John Wiley & Sons.

5. "3GPP; Technical Specifications Group Services and System Aspects; **Network Sharing**; Architecture and functional description (Release 8)" 3GPP TS 23.251 v8.3.0, March 2011.
   http://www.etsi.org/deliver/etsi_ts/123200_123299/123251/08.03.00_60/ts_123251v080300p.pdf

6. "Communications Interoperability Strategy for Canada", Government of Canada, January 2011.
   http://www.publicsafety.gc.ca/prg/em/_fl/cisc-eng.pdf

7. C.Lucente, "700TAG - Technical Advisory Note #4: A comparison of communications Network Architectures for a Public Safety Mobile Broadband Network", Centre for Security Science, Government of Canada, Oct. 7, 2011.

8. Public Safety Communications Research, "Public Safety 700 MHz Demonstration Network: Network Identifier Guidelines", Version 1.0, January 2012.
   http://www.pscr.gov/projects/broadband/700mhz_demo_net/testing/PSCR_Network_Identifiers_Demonstration_Network_Guidelines.pdf

9. FCC Order, "guidance to 700 MHz public safety broadband waiver recipients on their implementation of a public land mobile network identifier and related network identification numbering scheme to support the interoperability of the network deployments", PS Docket No. 06-229, January 9, 2012.
   http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0109/DA-12-25A1.pdf

10. FCC Order **"**FCC Grants Conditional Approval of 21 Petitions by Cities, Counties and States to Build Interoperable Broadband Networks for America's First Responders". May 2010.

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-79A1.pdf

NOTE: *DRDC Centre for Security Science warrants that this advisory note was prepared in a professional manner conforming to generally accepted practices for scientific research and analysis. This advisory note provides technical advice and therefore is not a statement of endorsement of Defence Research Development Canada, Department of National Defence, or the Government of Canada*

Author: *Claudio Lucente*, P.Eng

Scientific Authorities:

Jack Pagotto, Head/ESEC S&T [Emergency Mgmt Systems & Interoperability, Surveillance/Intel, E-security, Critical Infrastructure Protection]

Claude Belisle, Vice-President, Satellite Communications and Radio Propagation Research Branch, Communications Research Centre.

Joe Fournier, Research Program Manager, Communications Research Centre.

Eric Lafond, Senior Research Engineer, Communications Research Centre.

Approval for Release: *Dr. A. Vallerand*