Canadian Electricity Association | Association canadienne de l'électricité

Sept 12th, 2019
Secretary General of the Commission
CRTC
Ottawa, Ontario
K1A 0N2

Subject: Response to July 5th questions for Consultation CRTC 2019-57

1. CEA is pleased to respond to the two questions posed by the CRTC:

At paragraph 58 of your submission, you refer to how mobile network codes (MNC's) are assigned in the Netherlands including changes that were made to allow shared MNCs.

a. Are you requesting that a similar scheme be adopted in Canada?

b. Are regulatory changes that would allow shared MNCs an absolute requirement for your proposed PVNO to operate? Explain with supporting rationale.

The Canadian Electricity Association

2. CEA is the National Voice of Electricity. CEA members generate, transmit, and distribute electrical energy to industrial, commercial, residential, and institutional customers across Canada. Members include integrated electric utilities, independent power producers, transmission and distribution companies, power marketers, manufacturers and suppliers of materials, technology, and services that keep the industry running smoothly. Canada's electrical grid is 82% non-GHG emitting and getting cleaner every year. CEA, and its members promote electricity as a key economic, environmental and social enabler that is essential to Canadian prosperity and the Clean Energy Future.

3. To that end Canadian electric utilities (CEUs) need telecommunications networks to: 1) maintain secure and dependable tele-protection systems, 2) monitor and control electric infrastructure, and 3) enable the safe and efficient dispatch of their field workforce for routine and recovery operations.

4. Utilities typically make use of both commercial services and private networks. This combination often provides the best overall cost, performance, resiliency, and coverage. CEA members operate infrastructure across Canada in the largest cities and, due to remote electrification mandates and distant generation assets, in the most remote populated regions. They require a range of telecommunications options that can meet the challenges imposed by this diverse geography.

275 Slater Street, Suite 1500
Ottawa, Ontario K1P 5H9
275, rue Slater, bureau 1500
Ottawa (Ontario) K1P 5H9
info@electricity.ca
www.electricity.ca
info@electricite.ca
www.electricite.ca
T 613.230.9263

Canadian Electricity Association | Association canadienne de l'électricité

Are you requesting that a similar scheme [to the Netherlands] be adopted in Canada?

5. The Netherlands provides an excellent example of telecom regulatory innovation with one of the most open and enabling regimes in the EU. In addition to conventional Mobile Network Operator (MNO) Mobile Network Codes (MNC), they have an MNC for defense (public safety), for railway, for shared public (90), shared commercial (91), and 3 MNCs for private local networks (95 to 97). The Dutch railway and electricity companies have taken advantage of these regulatory innovations. The options have allowed each to enter into different commercial agreements; Enexis using a shared MNC, and Alliander and Stedin through using a conventional MNC via 'Utility Connect'. In effect, these critical infrastructure operators (CIOs) can exercise choice in the market to better serve the people who depend on them, that is a vision CEA shares. Importantly the assignment of these MNCs follows international ITU recommendations[1]. Canada should follow the Netherlands example, with some alterations, and be a regulatory leader in North America.

6. CEA's Private Virtual Network Operator (PVNO) proposal, please see Appendix A for CEA's original submission to the CRTC on the topic of PVNO, is similar to the Netherlands in that it asks for the release of an MNC to the electrical utility sector. We are not asking for the release of both an MNC for public and private use nor should the Netherlands sharing scheme, which requires an HLR proxy, be mandated in Canada. CEA has a proposal later in this document on an MNC allocating scheme that is more MNC efficient and allows electrical utilities to choose how they wish to deploy a PVNO, all within the bounds of a single 2-digit MNC.

7. There are two very important differences between the Netherlands and Canada which is why CEA's allocation proposal is slightly different than the Dutch model.

    a) No equivalent industry body to the CEA in the Netherlands sought regulatory changes on behalf of multiple electrical utilities. CEA's consultant found that

        > *[T]he electricity grid operators in the Netherlands were each taking independent positions and were not organized as one entity to request e.g. numbering resources from the Netherlands Telecom Authorities.*

        Whereas Canada has the CEA which is the singular voice for the electrical utility industry at the federal level and has internal decision making and dispute resolution mechanisms to coordinate the efficient and fair use of a 2-digit MNC by multiple different utilities.

[1] Please see Annex B, item 2 of ITU-T E212 https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.212-201609-I!!PDF-E&type=items

b) The Dutch shared MNC system was not designed for the interconnection of private Radio Access Networks (RAN), CEA's consultant found that

> *[T]he shared MNC as in the Netherlands does not fulfill with the requirement of Canadian Electricity Utilities to exploit private RAN networks (but this was a regulatory decision, not a technical limitation)*

CEUs being able to access multiple RANs is a key feature of CEA's PVNO design and why it is economically efficient. Accessing multiple RANs allows CEUs to use multiple existing commercial cellular networks to achieve improved reliability.

8. It is also worth noting that the Netherlands land area is smaller than Nova Scotia[2] and it has almost 100% cell coverage[3]. CEA's recommendations address all these aforementioned differences.

9. To assist CEA in answering this first question posed by the commission we contracted Netherlands based Rabion Consultancy[4], a European leader in telecommunication system design with specific expertise in Machine to Machine (a.k.a M2M or IoT) systems. Rabion's work comprehensively looked at the Netherlands PVNO from the industry and regulatory perspective, see Appendix B for that work.

Are regulatory changes that would allow shared MNCs an absolute requirement for your proposed PVNO to operate? Explain with supporting rationale

10. Yes, an MNC, and the associated regulatory changes, please see Appendix A for CEA's original submission to the CRTC on this topic, is an absolute requirement for a CEU PVNO. Without an MNC the necessary improvements in reliability and security for CEUs to deliver the Smart Grid will not occur. Please see the next sections for the supporting rationale.

PVNO a New Class of MNC Holder

11. The regulatory change requested by CEA is not for MNC sharing per se but instead to allow a new class of MNC holder. This new MNC holder class, Critical Infrastructure Operators (CIO), uses an MNC to delivers significant public good through services enabled by telecommunications, not through direct telecommunication services to the public. As such this new MNC holder class is not mandated to broadcast its Public Land Mobile Network Identification (PLMNID), but still has other rights of an MNC holder including wholesale RAN access from existing MNOs in the same way

[2] https://www.worldatlas.com/webimage/countrys/europe/nl.htm
[3] https://mobile.lebara.com/nl/en/dekking
[4] https://rabion.com/

as Mobile Virtual Network Operators (MVNOs) do. CEA does propose a 'sharing' scheme below, but it is not technically a shared MNC as it allows for both sharing and sub-allocations.

12. Also, the commission already allows shared MNCs, Bell and Telus share 880[5] . So again, CEA does not see a need for regulatory changes to allow shared MNCs but instead the regulatory changes necessary to allow CIO PVNO; a private network of networks that has the other rights of an MVNO.

13. Rabion consultancy also found that:

> *Shared MNC 90 and 91 such as allocated in the Netherlands are not needed in Canada in case regular 3-digit MNC (or MNCs) would be made available to Canadian Electricity Utilities. Furthermore, a PVNO does not depend on shared MNC assignment such as 90 and 91 as in the Netherlands. A PVNO can be operated as well under a regular MNC (or MNCs).*

14. Because CEA is requesting a single 2-digit MNC for its members to use we are aware that a regulatory change by the Canadian Numbering Administration[6] (CNAC) could be required. It is our understanding that the CNAC holds the 10 places of a 2-digit MNC (XX0 to XX9) for the XX MNC holder to use sequentially out of normal practise, not a formal regulation.

Reliability

15. A 2-digit MNC to be used by electrical utilities is required because CEUs cannot satisfactorily improve the reliability of commercial cellular by subcontracting services from an existing MNC holder. The reason for this is that network switching on a PVNO (sometimes referred to as roaming) would put the subcontracted MNCs core network in-between the CEU and its field devices (the devices that control and monitor the electrical grid). Putting a non CEU core network in between a CEU and its field devices is exactly what PVNO is designed to avoid because the purpose of a PVNO is to not have to ask permission from an external network to move traffic. CEA highlighted this in our May 15th submission in paragraph 24[7]: The same, and further reasons, were determined by the commission in CRTC 2015-177[8] paragraph 161:

> *The Commission considers that allowing full MVNOs to acquire MNCs would provide MVNOs with a greater level of independence, because they would not have to rely on the host wireless*

[5] http://www.cnac.ca/other_codes/imsi/imsi_codes.htm
[6] http://cnac.ca/index.htm
[7] R]oaming agreements between MNOs do not satisfy CEU connection reliability needs. This is because if the CEU's primary MNO, for this example called Network A, is down for planned or unplanned maintenance the CEU cannot access its field devices even if it has roaming access to Network B. This is because the network keys are stored by Network A so there is no way to validate the connection of the CEU field device or route the data properly. PVNO solves this problem because the network keys are stored by the CEU and so are always accessible from either MNO RAN.
[8] https://crtc.gc.ca/eng/archive/2015/2015-177.htm

> *carriers' MNCs and subscriber identification module (SIM) cards. Having its own unique MNC enables a full MVNO to more easily switch its host wireless carrier, make arrangements with multiple wireless carriers, and negotiate its own wholesale roaming arrangements (e.g. with international wireless carriers). The Commission therefore considers that it is appropriate to amend the Guideline to allow for the assignment of MNCs to full MVNOs*

16. At the time of writing this response no MNO has offered a CEU the ability to interconnect with their competitors RAN. CEUs already have service agreements with multiple MNOs but no efficient way to leverage reliability through diversity and improve security with the current market offers. That is why a sub-contracted service is not the same as a CEU PVNO using its own MNC and why the current market is not able to deliver the needs of CEUs for the Smart Grid. Thus, a regulatory change is necessary so that telecommunications can better serve Canadians.

Roaming Vs. Switching

17. For an example of network switching vs. roaming imagine a bookstore as the RAN and an automobile as an MNC. You go to bookstore A and it doesn't have the book you want in stock (the RAN is down). An employee at the store says they can order the book for you from another location and deliver it using their vehicle (MNC), but it will take 3 days. A competing store B (RAN) has the book and is across the city, you could go there in an hour using your own car (MNC). If you order the book through the first store that is roaming. If you go to the competing store to buy the book yourself that is network switching. There are costs and benefits to either (the cost of owning a car in this analogy) and CEUs are of the firm opinion that network switching is a better option for them. Switching is vastly better because it offers greater reliability for the delivery of an essential service (electricity) by enabling CEUs to go to new RANs if the primary is down. That movement cannot be accomplished without an MNC independent of the RAN owner.

Security

18. The other major reason an MNC assigned to electrical utilities is necessary is that by owning an MNC CEUs can increase the security of their network; please see Appendix A section 3.4, as well as our May 15th submission paragraphs 29-32 for the explanation why. The short summary is that security is vastly improved if the cyberattack defender is also the MNC holder, because the defender can better identify malicious actors before harm is done.

19. Additionally, the ability of an MNC holder to customize their network configuration allows for both improved security and greater efficiency. The improvements are possible by optimizing the CEU network for fewer functions (in this case electric utility specific Smart Grid functions), as opposed to a general MNO network which cannot specialize in the same way as it needs to be good for numerous different customer types. The ability to control the network configuration also reduces security risks by ensuring that data and signalling do not exit Canada. Both benefits, increased security and network optimization, were also the case in the Netherlands, see section 0 of Appendix B.

CEA Proposal for MNC Sharing/Sub-Allocation

20. With consultation with experts CEA has determined that the best approach for a CEU MNC is the following.

- Assign a 2-digit MNC e.g. 50X to CEA
  - CEA will provide oversight for the 50X MNC
  - CEA will use its internal consensus reaching decision making procedures as well as its dispute resolution to ensure fairness

- The CNAC will hold 501 to 509 for the first 9 utilities put forward by CEA willing to operate their PVNO.
  - A PVNO requires core equipment as well as negotiating wholesale agreements with existing MNOs
  - 501 is assigned to the first utility, 502, the 2nd etc.

- 500 is reserved for CEA members who want to share network infrastructure
  - The 500 MNC is sub-allocated and will use a proxy service to handle traffic.
  - A condition of the proxy service is that all data and signalling must remain in Canada
  - CEA has recommended that Public Safety Canada through its Public Safety Broadband Network (PSBN) would be an ideal proxy service provider for critical infrastructure operators such as CEUs.

21. To help answer the question of how a 2-digit MNC would be best put to work to enable the Smart Grid CEA contracted Canada based Ambra Solutions. Ambra is an innovative world leader in private LTE for industry and its partner Ecotel is a Canadian MNC holder.

Other Important Considerations for why an MNC is required

PSBN is not a complete solution for CEUs

22. CEUs need their own MNC, and not a sub-division of public safety's PSBN MNC because PVNO is the more flexible solution. PVNO gives each CEU the ability to choose the network that it needs to serve its customers best and to customize their network design for system efficiency and security. PSBN has the potential to be an excellent tool for CEU telecommunications and should work very well with PVNO to allow the interconnection of various public and private networks. PVNO can by thought of as a toolbox that holds and organizes different tools. PSBN is a good tool but it is not a toolbox.

Wholesale Access is Necessary

23. The benefits of CEUs being able to use their own MNC will by negated if they do not also receive the ability to gain wholesale access to existing RANs as MVNOs can. Because CEUs have diverse geographic needs that span remote, rural, and urban spaces as well as RAN diversity needs to ensure reliability they need the ability to negotiate wholesale RAN access agreements between themselves

and multiple available MNOs. The same was stated by the commission in CRTC 2015-177[9] paragraph 109:

> *"[T]he Commission determines that wholesale network access to the GSM-based mobile wireless networks of Bell Mobility, RCP, and TCC is essential for their competitors to provide broad or national network coverage to their retail customers. As such, the Commission determines that GSM-based wholesale roaming and MVNO access provided by Bell Mobility, RCP, and TCC are essential."*

24. If wholesale access is necessary for competitors to incumbent MNOs CEA does not see a policy issue in allowing wholesale access for non-competitive purposes. As identified in our May 15th submission paragraph 27[10], to develop the Smart Grid CEUs want to buy substantially more wireless services from existing MNOs but can only make those investments when reliability, security, and public/private interconnection (coverage) issues are solved via PVNO.

25. Wholesale access via a PVNO is an economically efficient solution to these challenges for two primary reasons 1) it does not require CEUs to build new single use wireless networks where existing wireless networks already are. 2) It allows all CEUs to choose what technology they can use in areas where existing cellular networks are not available or adequate. Both these points were highlighted in our May 15th submission paragraphs 42-47.

26. Rules for who qualifies for wholesale access to existing RANs are laid out in the Essentiality Test and CEA is confident that our PVNO request (see Appendix A for CEA's original submission) passes that test. Key points of which are below

Essentiality Test

27. A CEU MNC to support a PVNO passes the essentiality test for the input, duplicability, and policy concerns outlined in CRTC 2015-326[11]. CEUs are not mobile market competitors for a retail market so that portion of the essentiality test is not applicable in the traditional sense but PVNO would still play an important role.

    - Input: The ability to access multiple RANs of existing MNOs is essential for PVNO to receive the necessary improvements in reliability and security to allow the Smart Grid.

[9] https://crtc.gc.ca/eng/archive/2015/2015-177.htm

[10] To make the Smart Grid a reality CEUs want to purchase, at negotiated rates, significantly more wireless services in the years ahead but will only do so if there are large improvements in commercial cellular service reliability (where it is recognized that reliability is both system resiliency and operational redundancy/diversity) and security.

[11] https://crtc.gc.ca/eng/archive/2015/2015-326.htm

- Duplicability: The PVNO is economically efficient because it allows CEUs to use existing wireless infrastructure without having to build new Field Area Networks (FAN). The expense of new FANs would be unjustly put to CEU customers if a less expensive and just as good (if not better) solution is achievable, i.e. PVNO.

- Competition: Because PVNO is a mobile network enabler, through stable contracts, it will improve competition in the wireless market by supporting new entrants. This was highlighted in our May 15th submission paragraphs 54 and 55.

- Policy Concerns: As highlighted throughout our May 15th submission an electrical utility PVNO will have significant public good, improve network interconnection and innovate.

Note on other submissions - Other proposed solutions are complimentary

28. CEA, along with most all other parties to this consultation agree that innovation in Canada's wireless market will be good for Canada. That innovation can be technical, 5G being the forefront example, as well as regulatory. The PVNO request put forward by CEA and the Rail Association of Canada (RAC), as well as Halton Police Departments prioritized MVNO, and Cogeco's HMNO are all examples of regulatory innovation that looks to tackle the challenge that customer needs, be they individual citizens, public safety organizations, or critical infrastructure operators, are not being met by the current wireless market.

29. CEA does not view the regulatory proposals put forward by other stakeholders as competitive because each is designed to serve different needs. Cogeco is a commercial entity that has offered a solution to Canada's underdeveloped MVNO market to better serve the public's need for increased competition in the mobile market. The Halton Police Department's system is designed for first responders and is specialized for that. For example, the Halton model is to commercial cellular services as an ambulance is to a regular passenger van. An ambulance is a van, but it is highly modified for a specific use. The PVNO model is an economically efficient solution for critical infrastructure operators (CIOs) who need to interconnect public and private networks across large geographies, as well as increase the reliability and security of public networks to allow those systems to meet the needs of CIOs without burdening existing MNOs or CIO customers.

30. CEA asks the commission to not view these different solutions as competitive but as distinct voices looking to solve their customers needs. There is no one size fits all solution for all of Canada's wireless market especially as the market continues to diversify with the evolution of telecommunications technology. Telecommunication innovations, both technological and regulatory, are economic enablers. And the commission can enable competitive MVNO markets, increased public safety, and the Smart Grid through regulatory innovation.

Conclusion

31. CEA thanks the commission for the opportunity through this consultation to consider the view of its members on both why and how PVNO related regulatory changes will serve Canadians.

Sol Lancashire, Manager Telecom Engineering, BC Hydro

Chair, CEA Operating Technology & Telecommunications Committee

Francis Bradley

President and CEO, CEA

Justin Crewson

Director Transmission and Distribution Policy, CEA

Canadian Electricity Association | Association canadienne de l'électricité

Special Acknowledgements

Special thanks to members of CEA's Operating Technology & Telecommunications Committee (OTTC) for their invaluable efforts in developing this submission. The OTTC includes representatives from the following CEA member companies.

275 Slater Street, Suite 1500
Ottawa, Ontario K1P 5H9

275, rue Slater, bureau 1500
Ottawa (Ontario) K1P 5H9

info@electricity.ca
www.electricity.ca

info@electricite.ca
www.electricite.ca

T 613.230.9263

Canadian Electricity Association | Association canadienne de l'électricité

Appendix A – Oct 2018 Submission by the CEA to the CRTC

BEFORE THE CANADIAN RADIO-TELEVISION

AND TELECOMMUNICATIONS COMMISSION

IN THE MATTER OF

AN APPLICATION BY CANADIAN ELECTRICITY ASSOCIATION

(APPLICANT)

PURSUANT TO PART I OF THE *CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION RULES OF PRACTICE AND PROCEDURE* AND SECTIONS 24, 25(1), 32, 35(1), 46.1, 46.2, 47, AND 55 OF THE *TELECOMMUNICATIONS ACT*

TO GRANT CANADIAN ELECTRICITY ASSOCIATION A SHARED MOBILE NETWORK CODE AND OTHER ASSOCIATED RELIEF

29 OCTOBER 2018

Canadian Electricity Association | Association canadienne de l'électricité

TABLE OF CONTENTS

Executive Summary ..... **Error! Bookmark not defined.**

1.0 Introduction and request for relief ..... **Error! Bookmark not defined.**

2.0 The electrical grid is critical infrastructure and is undergoing significant changes that require the increased and flexible use of mobile wireless networks by CEUs .... **Error! Bookmark not defined.**

2.1 The electrical grid constitutes critical infrastructure ..... **Error! Bookmark not defined.**

2.2 The electrical grid is evolving rapidly to meet societal needs and take advantage of new technological developments ..... **Error! Bookmark not defined.**

2.3 Efficient and effective wireless data communications constitute an increasingly important element of the electrical grid ..... **Error! Bookmark not defined.**

2.4 The smart grid requires extensive connectivity services that are best provided by using Canadian mobile wireless networks ..... **Error! Bookmark not defined.**

3.0 The relief sought by CEA will greatly improve the management of the electrical grid ..... **Error! Bookmark not defined.**

3.1 SIM card lock-in is hampering the development of Smart Grid in Canada ..... **Error! Bookmark not defined.**

3.2 SIM card lock-in undermines redundancy in the smart grid **Error! Bookmark not defined.**

3.3 CEUs need to be able to deploy and interconnect their private networks with the networks of MNOs ..... **Error! Bookmark not defined.**

3.4 CEUs must be able to secure the smart grid and protect the privacy of confidential information ..... **Error! Bookmark not defined.**

4.0 A shared two-digit MNC for CEUs will overcome the obstacles that CEUs are experiencing and that impede the development of smart grid in Canada ..... **Error! Bookmark not defined.**

5.0 Regulatory change is needed for CEA to acquire an MNC and be granted PVNO status . **Error! Bookmark not defined.**

6.0 Other jurisdictions are granting or considering granting MNCs to electrical utilities ..... **Error! Bookmark not defined.**

7.0 The relief requested by CEA advances the policy objectives and is consistent with the Policy Direction ..... **Error! Bookmark not defined.**

8.0 Conclusion ..... **Error! Bookmark not defined.**

Canadian Electricity Association | Association canadienne de l'électricité

Canadian Electricity Association | Association canadienne de l'électricité

Executive Summary

ES-1. As Canadian Electrical Utilities ("CEUs") increasingly rely on wireless communications for a myriad of services essential to the continued reliable function of Canadian electrical transmission and distribution grids, it is essential for the CEUs to be able to access public wireless communications networks in the most reliable and cost-effective manner possible.

ES-2. CEA is submitting this application ("Application") pursuant to Part 1 of the *Canadian Radio-Television and Telecommunications Commission Rules of Practice and Procedure* and sections 24, 25(1), 32, 35(1), 46.1, 46.2, 47, and 55 of the *Telecommunications Act*[12] ("the *Act*").

ES-3. CEA is requesting the following relief from the Commission:

a. An order from the Commission directing that the CRTC Interconnection Steering Committee (CISC) Canadian Steering Committee on Numbering ("CSCN") revise the Canadian International Mobile Subscriber Identity Guideline ("IMSI Guideline") such that CEA may be granted a two-digit Mobile Network Code ("MNC") to be shared amongst its CEU members;

b. The recognition by the Commission of a new type of Mobile Virtual Network Operator ("MVNO") namely a Private Mobile Virtual Network Operator ("PVNO"), which, while similar in most respects to a Full MVNO, would not offer telecommunications services to the general public, coupled with recognition that CEUs meet this definition.

ES-4. Canada's electrical grid has been identified by the federal government as constituting critical infrastructure. Electricity is necessary for the proper function of many other critical services, including, but not limited to, Health, Food, Finance, Water, Information and Communication Technology, Safety, Manufacturing, Government and Transportation. The failure of the electricity supply could result in loss of life, adverse economic effects, and a loss of public confidence in the integrity of Canada's electrical grid.

---

[12] SC 1993, c 38 ["*Telecommunications Act*"].

ES-5. Canada's electrical grid is also undergoing constant evolution to meet societal needs and take advantage of new technological developments. For example, electricity is increasingly being generated, stored, and distributed closer to end customers, partly as a result of the accelerating adoption of renewable energy sources and new storage technologies. The electrical grid is also becoming increasingly digitized as CEUs and customers rely upon so-called "smart devices" to control, where, when, and how electricity is being used.

ES-6. In order to ensure the "always on" reliability required of Canada's electrical grid in the twenty-first century, CEUs are increasingly leveraging wireless communications in their operations. Some of the key ways in which wireless communications are being used include:

a. Real-time information sharing between field crews (typically for intra-utility, but also for inter-utility mutual aid including cross-border operations during emergencies);
b. Remote monitoring and control of crucial components of the distribution and transmission grids (including smart meters, fault detectors and substation management);
c. Remote monitoring of sensors in key elements of power generation (including seismic, slide, slope, flood, and other sensors);
d. Tracking of workers and assets for planning as well as optimization of incident response efforts;
e. Backup for fixed wireless microwave and wireline fibre optic telecommunications systems also used as described in items a through d.

ES-7. This new digitized electrical grid that leverages wireless communications is also known as the "smart grid". The smart grid allows CEUs to deliver energy more reliably, by deploying a smarter, more distributed grid. It also provides the tools for CEUs to create innovative new business models, such as enabling customers to optimize their use of electricity, as well as achieving operational and cost efficiencies, all while meeting demand securely and reliably.

ES-8. With emerging technologies and applications, the smart grid requires more and more devices integrated to the home. Without being exhaustive, according to CEA, a smart grid includes

ES-9. components such as smart meters, Intelligent Electronic Devices, plus two-way communications and power flow functionalities to:

- Quickly detect outages, so as to minimize the impact on the rest of system;
- Allow power to be distributed more efficiently and reliably (including peak load shaving);
- Integrate highly variable renewable energy sources, like wind and solar;
- Manage electricity generation flow from centralized power generating stations out to consumers, or from consumers and businesses back into the grid; and
- Facilitate the integration of electric vehicles.

ES-10. Smart grid technology is the necessary future of electricity generation, distribution, and transmission in Canada. Absent the deployment of smart technology, it will be very difficult for CEUs: (a) to ensure the 'always on' availability of electricity throughout the country that is so vital to the twenty-first century economy; and (b) integrate the renewable and user-generated energy sources necessary for Canada to meet its emissions reduction targets.

ES-11. Smart grid technology is also consumer friendly in that it better allows customers to control their electricity costs.

ES-12. There is a significant public safety element to the smart grid as disruptions in the electricity supply can put lives at risk. For example, the 2003 blackout in eastern Canada and the United States led to the deaths of at least 11 people. A subsequent review determined that smart technology would have largely prevented that blackout. A reliable electrical supply is also becoming increasingly important for protecting the sick and elderly who rely upon medical devices powered by electricity. Finally, smart grid technology enhances public safety by allowing the easier detection and thus deterrence of the increasingly common, but very dangerous, practice of electricity theft.

ES-13. Smart grid technology also enhances the safety of utility workers by allowing CEUs to better detect instances of 'islanding', where portions of the grid can remain electrified from local generators during blackouts despite appearing to not be electrified.

ES-14. A truly smart grid also greatly benefits the economy by reducing the frequency and duration of power outages that can result in billions of dollars of losses each year.

ES-15. For Canada's current electrical grid to evolve into a smart grid, CEUs need to be able to communicate effectively with the millions of smart devices that will be deployed into the smart grid. CEA conservatively estimates that within the next 10 to 15 years, CEUs will deploy more than 25 million wireless data devices and over 50,000 voice devices to support the management of the electric supply.

ES-16. Realistically, given the vastness of Canada's electrical grid and the already significant overlap of the grid with the mobile wireless networks of Canada's Mobile Network Operators ("MNOs"), CEUs need to use these wireless networks in order to be able to communicate with the smart devices that they are deploying throughout the electrical grid. Given the immense costs of deploying mobile wireless networks, it simply is not feasible for even the largest CEUs to deploy their own ubiquitous mobile wireless networks. Indeed, many smart devices being used by CEUs today are built to contain SIM cards and are already connected to the mobile wireless networks of MNOs.

ES-17. Unfortunately, while leveraging mobile wireless networks is the best path forward for facilitating the development of the smart grid in Canada, CEUs are experiencing a number of problems under the current regulatory environment that are hampering the deployment of the smart grid in Canada.

ES-18. A significant problem is the phenomenon of SIM card lock-in. As noted above, a smart grid consists of tens of millions of smart devices deployed throughout Canada's electrical grid. Many of these smart devices rely upon SIM cards and mobile wireless connectivity to ensure two-way communications with the CEU and the smart device. However, these SIM cards are only programmed to connect to the mobile wireless network of the MNO that provided the SIM cards that is to say, they are locked into that network.

ES-19. This can be extremely problematic for CEUs. It effectively prevents CEUs from switching mobile wireless providers as switching would require truck rolls to each smart device, which could number in the hundreds of thousands or millions for large CEUs, to manually swap out SIM cards. The cost of these truck rolls is a serious competitive constraint that makes it prohibitively costly for CEUs to switch to a different MNO, even if a different MNO can provide better terms and conditions for providing mobile wireless connectivity to that CEU's smart devices.

ES-20. The high cost of switching and the resulting inability of CEUs to negotiate the best deals possible for providing mobile wireless connectivity for smart devices drives up the cost of deploying smart devices and slows down the development of the smart grid in Canada.

ES-21. SIM card lock-in also limits redundancy in the smart grid. Currently, smart devices subject to SIM card lock-in will not automatically switch communications to the mobile wireless network of an alternative MNO if the primary MNO's network ceases to function for any reason. When these outages in mobile wireless networks occur, CEUs are unable to communicate with their smart devices and effectively lose all visibility into the grid, thus preventing the proper functioning of the smart grid and immediately transforming a smart grid into a legacy grid.

ES-22. Aside from the competitive and redundancy issues associated with SIM card lock-in, CEUs have issues with extending mobile wireless network coverage in rural, and remote areas not served by MNOs in which the CEUs may have electrical infrastructure.

ES-23. In places where MNOs do not offer cellular coverage, CEUs could deploy their own private wireless networks. However, numbering resources are required to do so using 3GPP technology and CEUs must be able to interconnect with the existing networks of MNOs in order to ensure that CEUs can communicate with these smart devices located in rural and remote areas. The relief requested by CEA in this Application will enable this interconnection to occur.

ES-24. Furthermore, there are significant privacy and security concerns inherent in the development of the smart grid as each smart device is potentially a gateway for a cyber-attack by a malicious actor. Currently, CEUs do not have any control over key aspects of the security of their smart devices, including control of the SIM card credentials and subscription database, which are controlled by the MNOs providing mobile wireless connectivity to the smart device. This is unacceptable to CEUs and the relief requested in this Application will allow CEUs to apply utility-grade security standards to these potential vulnerabilities.

ES-25. In order to solve the problems noted above that are hindering the timely development of Canada's smart grid, CEA is proposing that CEUs be permitted to share a unique two-digit MNC that will be administered by the CEA. With a unique two-digit MNC, CEUs will be able to provision their own SIM cards, implement the appropriate systems/networks under their own control, and negotiate corresponding parallel commercial agreements with MNOs.

ES-26. Having their own MNC will allow CEUs to let smart devices select the proper mobile network automatically and switch to another network when quality of service is inadequate or in case of major network failures. Crucially, if CEUs have their own MNC, this switching functionality will be able to be done remotely and will not require truck rolls to each and every one of the tens of millions of smart devices being deployed throughout Canada's electrical grid.

ES-27. Thus, at a stroke, the problem of SIM card lock-in will be solved, thereby addressing the competitive and redundancy shortcomings described above.

ES-28. Access to a unique two-digit MNC will also allow CEUs to interconnect their private wireless networks in rural and remote areas with the mobile wireless networks of MNOs, thus ensuring that CEUs have a path to communicate with these particular smart devices.

ES-29. With a unique two-digit MNC CEUs will be in a position to have their own core networks, which will be under their own control, thereby addressing the security concerns described above.

ES-30. In order for CEUs to be granted a shared two-digit MNC, regulatory change is required as the current ISMI Guideline, which governs the allocation of MNCs in Canada, does not envision the CEA being able to apply for a shared two-digit MNC for CEUs for the purpose of facilitating the deployment of the smart grid in Canada.

ES-31. CEA is thus proposing the following amendments to the IMSI Guideline, which would allow it to apply for a two-digit MNC to be shared amongst its CEU members:

a. Subsection 7.1 amended to add a new paragraph (d) that reads: "An Electric Utility related association, some of whose members operate as PVNOs, may also be an applicant for a two-digit MNC to be shared amongst its members who operate as PVNOs."

b. Subsection 7.3(a) amended to read: "The ability of a terminal to access telecommunication services from mobile wireless networks, regardless of whether the terminal itself is in motion or not, and the capability of the network to identify and locate that terminal."

c. Section 15.0, the Glossary, amended to add a new definition of PVNO as follows: "Private Virtual Network Operator (PVNO): is a full MVNO that only provides telecommunication services to itself and not to consumers, operates core network hardware (e.g., switches, routers) separate from all WSPs and has a service profile management system (e.g. Home Location Register [HLR], Home Authentication, Authorization, and Accounting [AAA], or Home Subscriber System [HSS]) for devices owned and/or operated by the PVNO that can access WSP networks in Canada."

ES-32. CEA is proposing that the Commission recognize a new category of wireless service provider, namely PVNOs. A PVNO would be the same, technically, as a full MVNO. However, it would not provide mobile wireless services to consumers, but only to itself (namely for private enterprise needs and internal telecommunication purposes). As such, there should be no requirements for PVNOs to

adhere to any of the consumer-centric obligations imposed on MVNOs or wireless carriers such as wireless number portability. CEUs would be recognized as PVNOs.

ES-33. CEA notes that its proposal is not radical or unprecedented. The solution proposed by the CEA to facilitate the deployment of millions of SIM-card enabled smart devices throughout Canada's electrical grid has actually been implemented by the national telecommunications regulator in The Netherlands. Furthermore, both Belgium and Germany are also considering following the Dutch model and assigning MNCs to electrical utilities.

ES-34. The relief requested by CEA advances a number of policy objectives contained in section 7 of the *Act*, by buttressing the Canadian economy, enhancing competition, stimulating innovation, and protecting the privacy and security of customers of CEUs. The relief requested by the CEA is also consistent with the Policy Direction as by addressing the problem of SIM card lock-in, which effectively prevents competition in the provision of mobile wireless services to smart devices, it enhances reliance on market forces. The requested relief is efficient and proportionate as it only requires minor changes to the IMSI Guideline and the recognition of PVNOs. The requested relief is competitively neutral.

1.0 Introduction and request for relief

1. Founded in 1891, the Canadian Electricity Association ("CEA") is the national forum and voice of the evolving electricity business in Canada. CEA contributes to the regional, national, and international success of its members. CEA is governed by a Board of Directors comprised of senior executives from its Corporate Utility Members. CEA's mission is to be the national voice for safe, secure, and sustainable electricity for all Canadians.

2. CEA members generate, transmit, and distribute electrical energy to industrial, commercial, residential, and institutional customers across Canada. Members include integrated electric utilities, independent power producers, transmission and distribution companies, power marketers, manufacturers and the suppliers of materials, technology, and services that keep the industry running smoothly. CEA's strategic goal, on behalf of its membership, is to provide a comprehensive roadmap to address the industry's most pressing issues, including: infrastructure renewal, environmental protection, innovation and technology, Indigenous and North American partnerships, and regulation and security. CEA strives to deliver a coherent and convincing industry viewpoint to decisionmakers on critical policy and regulatory issues. CEA members involved in the generation,

transmission, and distribution of electrical energy are collectively referred to as Canadian Electrical Utilities or "CEUs" in this Application.

3. CEA submits this application ("Application") pursuant to Part 1 of the *Canadian Radio-Television and Telecommunications Commission Rules of Practice and Procedure* ("Rules") and sections 24, 25(1), 32, 35(1), 46.1, 46.2, 47, and 55 of the *Act*.

4. As set out more fully below, CEA is requesting the following relief from the Commission:

a. An order from the Commission directing that the CRTC Interconnection Steering Committee (CISC) Canadian Steering Committee on Numbering ("CSCN") revise the Canadian International Mobile Subscriber Identity Guideline ("IMSI Guideline") such that CEA may be granted a two-digit Mobile Network Code ("MNC") to be shared amongst its CEU members;

b. The recognition by the Commission of a new type of Mobile Virtual Network Operator ("MVNO") namely a Private Mobile Virtual Network Operator ("PVNO"), which, while similar in most respects to a Full MVNO, would not offer telecommunications services to the general public, coupled with recognition that CEUs meet this definition.

2.0 The electrical grid is critical infrastructure and is undergoing significant changes that require the increased and flexible use of mobile wireless networks by CEUs

2.1 The electrical grid constitutes critical infrastructure

5. The electric grid is a key element of the Canada's critical infrastructure. Public Safety Canada[13] defines "critical infrastructure" as "the processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders."

6. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.

7. Critical infrastructure is supported by a wide range of stakeholders and entities and it is not straightforward to paint a complete picture of all processes and services, but electricity underpins the proper

[13] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx.

functioning of many of the other critical services, notably Health, Food, Finance, Water, Information and Communication Technology, Safety, Manufacturing, Government and Transportation.

2.2 The electrical grid is evolving rapidly to meet societal needs and take advantage of new technological developments

8. The electrical grid is also under constant evolution. It is becoming increasingly decentralized with energy generated, stored and distributed closer to end customers. This is in part driven by the acceleration of renewable (e.g., wind, solar) and storage technologies. At the same time, the grid is becoming increasingly digitized. The digitization of the electrical grid allows electricity system operators and customers to control where, when, and how electricity is being used. This is critical to allow for efficient capacity planning and capital allocation.

9. Finally, the electrification of Canada is accelerating. Transportation (rail, automotive, aerospace) are gradually becoming integrated into the electrical grid. These use cases further emphasize the need for a reliable electrical grid.

10. Ubiquitous communication is essential to securing that reliability.

2.3 Efficient and effective wireless data communications constitute an increasingly important element of the electrical grid

11. There are five (5) key drivers for the use of wireless communications in electrical operations:

    a. Real-time information sharing between field crews (typically for intra-utility, but also for inter-utility mutual aid including cross-border operations during emergencies);
    b. Remote monitoring and control of crucial components of the distribution and transmission grids (including smart meters, fault detectors and substation management);
    c. Remote monitoring of sensors in key elements of power generation (including seismic, slide, slope, flood, and other sensors);
    d. Tracking of workers and assets for planning as well as optimization of incident response efforts;
    e. Backup for fixed wireless microwave and wireline fibre optic telecommunications systems also used as described in items a through d.

12. Historically the electrical grid had few dependencies on public wireless communication networks. Most of its connectivity was, out of necessity, provided through separate dedicated purpose-built fixed and mobile wireless networks.[14] .

13. However, it is becoming increasingly less cost-efficient to build out dedicated wireless networks. Spectrum is a scarce resource, the build out of a physical network infrastructure is cost-intensive, and the operational cost is high. Furthermore, cellular technology has become more capable and general public network capabilities have improved to the point that it makes economic sense to explore the enterprise-wide adoption of commercial network technology for utility operations. Thanks to the standardization of LTE and 5G through the 3GPP[15] organization, cellular technology has the critical mass required to attract innovation, making it cost-efficient and ensuring that a broad device ecosystem is available. Specifically, innovation targeted for emerging public safety networks is well suited to electricity operational needs.

14. CEU field crews increasingly rely on public networks for backup communications and high-speed data transfer. Access to public networks is important for inter-utility assistance (including international support) and mutual aid assistance.

2.4 The smart grid requires extensive connectivity services that are best provided by using Canadian mobile wireless networks

15. In addition to all of the factors driving the need for connectivity that have been discussed, the most important such driver, particularly of wireless connectivity, is the evolution of electrical grids into the smart grid.

16. CEUs have deployed their electric system infrastructure over many decades. As Canadians increasingly rely on electricity for their quality of life and economic prosperity, CEUs are investing in new digital protection, automation, monitoring, and control technologies. Many of these new technologies require telecommunications to be deployed deeper and deeper into Canada's electrical grids. This new more connected grid is referred to as the "smart grid."

[14] These alternatives include Private Microwave, WiMAX, and SCADA Radio for grid operations; P25, TETRA for Land Mobile Radio (LMR) or Mesh networks for Smart Metering have been the dominant technologies.

[15] 3rd Generation Partnership Project. See http://www.3gpp.org/.

17. The smart grid allows CEUs to deliver energy more reliably, and implement a smarter, more distributed grid. It also provides the tools for CEUs to deliver the best customer experience, as well as achieve operational and cost efficiencies, all while meeting demand securely, and reliably.

18. With emerging technologies and applications, the smart grid requires more and more devices integrated to the home. Without being exhaustive, according to CEA, a smart grid includes components such as smart meters, Intelligent Electronic Devices,[16] plus two-way communications and power flow functionalities to:

- Quickly detect outages, so as to minimize the impact on the rest of system;
- Allow power to be distributed more efficiently and reliably (including peak load shaving);
- Integrate highly variable renewable energy sources, like wind and solar;
- Manage electricity generation flow from centralized power generating stations out to consumers, or from consumers and businesses back into the grid; and
- Facilitate the integration of electric vehicles.[17]

19. CEA has attached a background paper ("CEA Smart Grid Paper") further explaining the components of the smart grid and its benefits as Appendix A to this Application.[18]

20. Smart grid technology is the necessary future of electricity generation, distribution, and transmission in Canada. Absent the deployment of smart technology, it will be very difficult for CEUs: (a) to ensure the 'always on' availability of electricity throughout the country that is so vital to the twenty-first century economy; and (b) to integrate the renewable and user-generated energy sources necessary for Canada to meet its emissions reduction targets.

21. Smart grid technology is consumer-friendly technology that, in an age of increasing costs for electricity stemming from a variety of factors, will be particularly beneficial to low and middle-income consumers by enhancing their ability to control their usage of electricity and thus the amount they are ultimately charged. For example, consumers will be able to monitor their electricity usage via an application on their smartphones and reduce their consumption during peak hours. Smart grid technology also reduces the costs of delivering power, by allowing utilities to monitor usage remotely as opposed to sending workers out to customer premises to physically check meters.

---

[16] An Intelligent Electronic Device is a term used in the electric power industry to describe microprocessor-based controllers of power system equipment, such as circuit breakers, transformers and capacitor banks.

[17] Canadian Electricity Association, "The Smart Grid: A Pragmatic Approach", 2010. ["CEA Smart Grid Paper"].

[18] *Ibid*.

22. There is also a significant public safety element to the smart grid. As explained in the CEA Smart Grid Paper, when the power grid goes down, lives are at risk. The infamous 2003 blackout in eastern Canada and the United States caused the loss of at least eleven lives.[19] A review of the root causes of the blackout determined that the entire incident was caused by tree branches in Ohio brushing against power lines and the failure of an alarm to go off subsequently at the local utility.[20] Had smart technology been deployed throughout the grid in 2003, the voltage disruptions caused by the tree branches brushing up against the power lines would have been detected well in advance, thereby enabling the relevant utilities to dispatch workers to remove the branches before the disruptions cascaded throughout eight US states and Ontario.[21] Even if the power lines had been knocked down, smart grid technology would have allowed utilities throughout Canada and the United States to identify the source of the problem correctly, isolate the affected area to prevent the adverse consequences from cascading throughout the grid, and reroute power through other networks in order to minimize the size of the blackout.[22]

23. The smart grid has an important role to play in protecting the sick and elderly, who often use medical devices that require electrical power to operate correctly and are therefore vulnerable to disruptions in the electrical power supply.

24. Smart grid technology also enhances the safety of utility workers. During blackouts, a frequent risk to worker safety is the possibility of "islanding" where portions of the grid remain electrified by power from local generators.[23] Presently, these islands of electricity can be incredibly difficult to detect and pose a constant risk to utility workers seeking to restore power to areas that otherwise appear to be completely devoid of electricity.[24] However, with smart grid technology deployed throughout the grid, utilities will be able to monitor instances of islanding in real-time actively, advise workers to take extra precautions, and shut down generators in the affected areas remotely until workers have fully restored service.[25]

---

19 *Id.* at pg 10.
20 *Ibid*.
21 *Ibid*.
22 *Ibid*.
23 *Id.* at pgs 6, 8, 10.
24 *Id.* at pg 8.
25 *Ibid.*

25. By allowing the monitoring of power-flow, smart grid technology also enhances public safety by deterring the very dangerous, but unfortunately increasingly common, practice of electricity theft. For example, BC Hydro has had to deal with over 1,500 instances of electricity theft over three years, all associated with illegal marijuana growing operations.[26]

26. Finally, smart grid technology, by reducing the frequency and duration of outages, will dramatically benefit the economy. A 2004 study found that power interruptions cost the economy of the United States $80 billion per year and other estimates indicate that the loss was as high as $150 billion per year.[27] While the amounts in Canada would be lower due to the smaller size of Canada's economy, the negative impact is still no doubt measured in the billions of dollars per year.

27. Overall, it is vital for economic, public safety, and environmental reasons that CEUs can deploy smart grid technology throughout their grids and have access to the resources necessary to do so in the most cost-effective and reliable way possible.

28. One of the most important aspects of the evolution of the smart grid is the need for CEUs to be able to communicate with the very numerous individual devices that comprise it. CEA expects that within the next 10 to 15 years, more than 25 million wireless data devices and over 50,000 voice devices will be deployed to support the management of the electric supply by CEUs. Considering the current pace of technological evolution and rapid adoption of the Internet of Things ("IoT"), these estimates could be conservative.

29. Clearly, the availability of ubiquitous, reliable and secure wireless communications technology is essential to the development and operation of the smart grid.

30. Since there is a high degree of overlap of coverage between the aggregate footprints of the mobile wireless networks of Canada's Mobile Network Operators ("MNOs")[28] and CEU electrical grids, it is efficient for CEUs to have their wireless data communications needs met by the MNOs. While it is possible to connect smart devices in the grid via fibre in some cases, realistically, the only way to cover the vastness of Canada's electrical grid, particularly in more rural and remote areas, is to leverage existing mobile wireless networks.

---

[26] *Id.* at pg 12.

[27] *Id.* at pg 5.

[28] Those are the entities listed as Wireless Carriers on the Commission's List of Telecommunications Service Providers. See https://applications.crtc.gc.ca/telecom/eng/registration-list?_ga=2.114163207.1818544366.1539969706-670211790.1509399832.

Thus, many smart devices being used by CEUs today are built to contain subscriber identification module ("SIM") cards and are connected to existing mobile wireless networks of the MNOs.

3.0 The relief sought by CEA will greatly improve the management of the electrical grid

31. Leveraging commercial mobile networks can bring significant benefits to CEUs. The Commission has estimated that between 2012 and 2016 Canadian telecom providers have spent $8.7B in wireless plant and equipment and $8.9B on spectrum (AWS-3, 700MHz, and 2,500MHz).[29]

32. Clearly, CEUs do not have the capabilities to invest similar amounts of capital in mobile communication network deployments, nor is the diversion of such resources consistent with their core mandate. From an economic and societal perspective, it makes sense to maximize the use of existing assets as opposed to driving additional network deployments (unless that is necessary for specific coverage, security, reliability or capacity requirements).

33. While existing mobile wireless networks constitute a promising method of telecommunications for CEUs to develop the Canadian smart grid, unfortunately CEUs have been experiencing a number of problems under the current mobile wireless regulatory environment that are hindering the deployment of the smart grid in Canada. These problems are discussed below, where we also demonstrate how the relief sought by CEA will solve them.

3.1 SIM card lock-in is hampering the development of Smart Grid in Canada

34. MNOs are fostering vendor lock-in. They do this through a practice known as "SIM card lock-in". The practice ensures that SIM cards placed in devices will only connect to the mobile wireless network of the MNO that provided the SIM cards. CEUs are subjected to this practice when they obtain SIM cards from MNOs for deployment in smart grid devices.

35. This situation can be extremely problematic if the entity deploying the smart devices later decides that it wishes to switch MNOs. In such a case, the deployer of the smart devices has to physically attend, at every smart device, in order to manually remove each SIM card programmed by the previous MNO, so that it can be replaced with the SIM card programmed to connect to the network of the new MNO. The 'truck rolls' necessary

[29] https://crtc.gc.ca/eng/publications/reports/policymonitoring/2017/cmr5.htm.

for completing this task entail significant cost, which increases exponentially in the case of a comprehensive changeover. Further, there is also a risk of interruption of electricity during these activities.

36. CEUs operate millions of smart devices, including in many rural and remote areas. The cost of sending utility workers to swap out the SIM cards on smart devices in rural and remote areas, for example, could be thousands of dollars per swap. Even in dense urban areas, the sheer number of smart meters and other smart devices involved would make the cost of switching providers prohibitive for any CEU.

37. The problem of SIM card lock-in is a serious competitive constraint which makes it prohibitively costly for CEUs to consider switching MNOs for their smart devices, even if another can provide the CEU with more favourable financial or other terms than the CEU's current provider.

38. The high cost of switching SIM cards and MNOs is a variable that CEUs must factor into their business cases when deploying smart devices. Consequently, it slows down the deployment of smart devices in Canada and is an impediment to potential new innovative services that will improve control of the electric grid. If a CEU had the ability to switch MNOs so as to obtain service from the MNO that provides the best financial and other terms, including the best quality of service, as other businesses and consumers can do, the costs of deploying and operating smart devices in Canada's power grid would be lowered and the pace of innovation and deployment could be correspondingly increased.

39. This problem is not unique to the smart devices of CEUs and has been identified by the Organization for Economic Co-operation and Development as a serious challenge to overcome to enable the widespread deployment of IoT devices (which include IoT smart devices that form part of the smart grid).[30]

40. It is imperative for CEUs to have access to a more competitive market for the provision of mobile wireless services. The relief sought in this Application would reduce the cost of switching service providers significantly, thereby giving CEUs more negotiating power when dealing with MNOs . The net result would be increased innovation and reduced costs. One of the incidental, yet very significant outcomes, will be lower electricity rates, which will, among other things, improve the international competitiveness of the Canadian manufacturing sector.

-

[30] Organization for Economic Co-operation and Development, *OECD Digital Economy Outlook 2015*, http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm, at pg 252.

3.2 SIM card lock-in undermines redundancy in the smart grid

41. Another issue associated with SIM card lock-in is its deleterious impacts on public safety and the economy by limiting redundancy in the smart grid. SIM card lock-in makes it very expensive and overly complex to create communications redundancy in the smart grid. In the absence of the ability to program SIM cards such that a CEU could switch communications to smart devices to a secondary MNO, when there is a technical problem with the service provided by the primary CEU, the CEU would have to integrate additional communications mechanisms to achieve high availability and seamless switching between communication paths, and that could certainly push additional complexity in to the smart grid devices.

42. As described above, minimizing the frequency and duration of outages is vital to Canada's public safety and the country's economy. Smart devices in the power grid help minimize the duration and frequency of outages by: (a) allowing CEUs to detect problems in the grid before they transform into a full-blown outage; and (b) enabling CEUs to pinpoint the sources of the problems in the grid precisely when outages do occur, thus allowing for resources to be focused on those problem areas instead of time being wasted while first trying to determine the cause of the problem. Obviously, for these benefits of the smart grid to be realized, the smart devices in the grid need to be able to provide data to CEUs via telecommunications.

43. A frequent issue encountered by CEUs is the inability to communicate with smart devices deployed throughout the grid due to either planned or unplanned outages in the networks of the MNOs contracted to provide connectivity to the smart devices. CEA understands that unplanned outages can occur in the networks of MNOs for a variety of reasons. However, in CEA's experience, it is rare for all the mobile wireless networks in a given area to experience an outage at the same time. Usually at least one mobile wireless network will still be offering service, even if others are down. Accordingly, if smart devices could have access to two or more networks, network availability would clearly be increased.

44. Unfortunately, due to SIM card lock-in, smart devices deployed throughout the grid will not automatically connect to the mobile wireless networks that are still functioning in a given area and use a still functioning network as a new home network. CEA notes that there is no technical justification for this state of affairs; it is merely the business decisions of the MNOs that result in this lack of redundancy existing in the smart grid.

45. This is a serious reliability issue that compromises public safety and has negative economic impacts by hindering the ability of CEUs to monitor and respond to issues in the grid. CEUs face losing visibility into the

power grid if they are solely reliant on a single MNO that experiences an unexpected outage and there is no ability for the CEU's smart devices to switch seamlessly onto still functioning mobile wireless networks.

46. Electric utilities are deemed to be critical infrastructure providers by Public Safety Canada and are subject to the National Strategy for Critical Infrastructure, the purpose of which is to strengthen the resiliency of critical infrastructure in Canada in the face of current and emerging hazards.[31] Accordingly, the current lack of redundancy in CEU's smart devices is highly problematic.

47. In summary, SIM card lock-in, by tying a CEU's smart devices to the network of only one MNO which may experience planned or unplanned service outages, is undermining redundancy by creating single points of failure in the smart grids of CEUs. It is imperative that CEUs smart devices have the ability to automatically connect to still functioning mobile wireless networks in the event that the primary home network of a smart device experiences an outage. The relief sought by CEA in this Application would enable this to occur.

3.3 CEUs need to be able to deploy and interconnect their private networks with the networks of MNOs

48. Aside from the competitive and redundancy issues associated with SIM card lock-in, CEUs have issues with extending mobile wireless network coverage in rural and remote areas not served by MNOs in which the CEUs may have electrical infrastructure.

49. CEA does not necessarily expect MNOs to expand their networks so the entire Canadian electrical grid is served by commercial mobile wireless networks. In many cases, CEUs already deploy their own telecommunications networks. In places where MNOs do not offer cellular coverage, CEUs could deploy their own private wireless networks. However, numbering resources (IMSI / MNC) are required to do so using 3GPP technology.

Where coverage is not available from MNOs, a CEU should be able to deploy its private network and interconnect with the existing networks of MNOs in the areas in which they do offer service to the public. The relief sought by CEA in this Application would enable this to occur.

---

[31] Public Safety Canada, *National Strategy for Critical Infrastructure*, 2009, at pg 2.

3.4 CEUs must be able to secure the smart grid and protect the privacy of confidential information

50. The deployment of the smart grid inherently involves significant security and privacy risks. Each smart device constitutes a potential vulnerability that could be hacked by malicious actors to gain access to confidential information or used as a gateway to attack the rest of the smart grid. These privacy and security concerns are mounting significantly as millions of smart devices are being deployed throughout Canada's power grid.

51. Some security issues are related to the control of the SIM card credentials, also known as security keys, and subscription databases owned and controlled by the serving MNO core networks. CEUs have no control over these aspects and rely completely on the serving MNO to which the SIM card is associated.

52. Without control of the SIM card and Packet Data Network Gateway, CEUs are not able to protect their control systems from network layer attacks. For example, without the SIM card security keys, CEUs have no way of knowing whether a device connected to their networks actually belongs to the CEU or is a device that is operated by a malicious actor. With control of these security keys, CEUs will be able to prevent devices operated by malicious actors from connecting to their networks, thereby ensuring the security of the smart grid. Consequently, CEUs need their own isolated core networks to have control over device and subscription related security aspects while also ensuring the required redundancy and reliability discussed above by being connected to more than one MNO's Radio Access Network ("RAN").

53. CEA has attached as Appendix B to this Application a diagram demonstrating how if they are permitted to operate as PVNOs with their own shared two-digit MNC, CEUs will be able to deploy their own core networks with the key security elements described above, safely under their own control and subject to utility-grade security standards.

54. Accordingly, the relief sought by CEA in this Application, namely allowing CEUs to access a unique two-digit MNC administered by the CEA and permitting CEUs to operate as PVNOs, will address the security concerns by allowing CEUs to develop their own core networks.

4.0 A shared two-digit MNC for CEUs will overcome the obstacles that CEUs are experiencing and that impede the development of smart grid in Canada

55. CEA wishes to emphasize that Canada's MNOs are valued business partners who obviously have a vital role to play in the deployment and development of Canada's smart grid. However, current technical and

56. regulatory limitations have hampered CEU's ability to fully leverage the capabilities of Canada's MNOs and have frustrated the timely development of Canada's smart grid. Fortunately, as explained below, there is a simple solution to the problems identified in Part 4.0 above that would help resolve both technical and policy matters: allowing CEUs to share a two-digit MNC.

57. As noted above, to facilitate the necessary deployment of the smart grid in Canada, CEA is requesting that the Commission issue an order directing that the CSCN revise the IMSI Guideline such that CEA may be granted a unique two-digit MNC to be shared amongst its CEU members. CEA would be responsible for providing access to this two-digit MNC to its CEU members.

58. The Commission explained the purpose of an MNC in Telecom Decision 2015-496[32] ("TD 2015-496") as follows:

> An MNC is a unique identification number that identifies a specific wireless service provider's (WSP) network in a given country. The MNC permits a WSP to establish direct roaming agreements with both domestic and international providers because its network can be uniquely identified.[33]

59. If CEA is allocated a two-digit MNC, CEUs will be in a position to share this MNC with its CEU members which, in turn, will be able to deploy their own SIM cards in smart devices, as well as implement the appropriate systems/networks under their own control and negotiate the necessary corresponding commercial agreements with MNOs.

60. Having their own MNC, and commercially negotiated service agreements with multiple MNOs in the same area, will allow CEUs to let smart devices select the proper mobile network automatically and switch to another network when quality of service is inadequate or in case of major network failures. It is this ability of an MNC to allow the devices to be directly managed by the CEUs, which CEA believes will solve many the problems identified in Part 3.0 of this Application.

---

[32] Telecom Decision CRTC 2015-496, *CISC Canadian Steering Committee on Numbering – Revised Canadian International Mobile Subscriber Identity Guideline*, 6 November 2015 ["TD 2015-496"].

[33] *Id.* at para 2.

61. With their own MNC, CEUs will be able to overcome the obstacles caused by SIM card lock-in. A unique two-digit MNC, shared amongst CEUs, will allow CEUs to install their own SIM cards in their smart devices, as opposed to SIM cards programmed by the contracted MNO.

62. By having their own SIM cards, CEUs will be in a position to negotiate more competitive pricing for smart devices as mobile wireless service providers will know that CEUs will have the capability of moving to another provider instead of being locked-in due by prohibitive costs arising from the need to physically switch SIM cards on multitudes of deployed smart devices.

63. SIM cards belonging to CEUs with a shared MNC belonging to CEA will also make it possible to address the redundancy issue described in Part 3.0. Currently, if the home network of a smart device experiences an outage, that device does not automatically switch to another mobile wireless network that may still be functioning. This is a serious problem. It means that CEUs lose the enhanced automation and control of their grids provided by cellular enabled smart devices during the outage of the home network.

64. However, with a unique two-digit MNC belonging to CEA, individual CEUs will be able to enter into agreements with MNOs such that if one mobile wireless network in a given area fails, the smart device will switch to alternative mobile wireless networks that are still functioning. Without a unique two-digit MNC, CEUs are unable to enter into these agreements directly and must rely on inter carrier agreements, which effectively precludes their smart devices from being switched to alternative home networks in the event of an outage in the primary home network of the smart device.

65. With an MNC it will also be easier for CEUs to interconnect their private cellular networks with MNOs' networks, in areas where MNOs do not offer coverage so that a CEU can deploy smart devices within its own network. This will ensure that those devices can communicate with the rest of the smart grid, which is served by other MNOs. In this way, the geographic scope of the smart grid will not be unduly constrained.

66. As explained in previous sections, there are security issues related to the control of the SIM card credentials and subscription databases, which are currently owned and controlled by the serving MNO's core network. CEUs currently have no control over these aspects and rely completely on the serving MNO to which the SIM card is associated. With an MNC belonging to CEA, a CEU would be able to have an isolated core

network under its own control, connected to more than one RAN, and have control over security aspects while ensuring redundancy and reliability.

67. Overall, if CEA acquires its own unique two-digit MNC, which it will share amongst its CEU members, it will be able to overcome the obstacles noted in Part 3.0 of this Application, which are hindering the deployment and development of the smart grid in Canada. However, as explained further below, CEA will only be able to obtain an MNC through regulatory change.

5.0 Regulatory change is needed for CEA to acquire an MNC and be granted PVNO status

68. The allocation of MNCs in Canada is governed by the ISMI Guideline.[34] Currently, the ISMI Guideline is drafted in a restrictive fashion such that, although they have a bona fide need for an MNC, CEUs are unable to currently receive an MNC from the ISMI Administrator.

69. The following subsections of the IMSI Guideline prevent CEA from applying for an MNC on behalf of its CEU members:

> 7.1 The MNC applicant must be one of the following:
>
> a) an entity who is licensed by Industry Canada for the spectrum utilized by a wireless network and be registered as a telecommunications carrier with the CRTC to operate in the area in which it intends to provide a mobility service, and who provides evidence of certification to the IMSI Administrator.
>
> b) A public safety related association that has a need to roam onto/from telecommunications carriers' networks in Canada may also be an applicant for an MNC. See Appendix 2.
>
> c) an entity registered with the CRTC as a Full MVNO.
>
> [….]
>
> 7.3 The applicant must certify that the MNC will be used for mobile applications. That is, the applicant must certify that the service provided will have the following characteristics:
>
> a) Terminal Mobility – The ability of a terminal to access telecommunication services from different locations and while in motion, and the capability of the network to identify and locate that terminal.

[34] TD 2015-496 at para 2.

b) Personal Mobility – the ability of a user to access telecommunications services at a terminal on the basis of a personal identifier, and the capability of the network to provide those services according to the user's profile. Personal mobility involves the network capability to locate the terminal associated with the user for the purpose of routing.

[….]

Appendix 2

1. The IMSI Administrator will assign a single, common Mobile Network Code (MNC) for use by all Industry Canada authorized 700 MHz public safety broadband network operators.

2. In addition to the allocation of the single public safety MNC, the IMSI Administrator is authorized to set aside additional MNCs for use by public safety if justified to the IMSI Administrator, CRTC staff and Industry Canada staff.

70. Unfortunately, CEA does not fit neatly into any of the categories required to obtain an MNC under the ISMI Guideline. CEA does not qualify under subsection 7.1(a) as neither it, nor all its members, are telecommunications carriers for mobility services. CEA also does not qualify under subsection 7.1(c) as neither it, nor its members, are Full MVNOs.

71. CEA closely examined the possibility of applying under subsection 7.1(b) as a public safety related association. Certainly, one of the roles of CEA is advancing public safety and, as detailed above, CEUs play a vital role in public safety through their efforts to maintain the integrity of Canada's supply of electricity. In addition, CEA is participating in consultations related to the 700 MHz public safety broadband network ("PSBN") and expects CEUs to be included as users and/or operators of that network.

72. However, as the PSBN is not yet established, it is not certain that CEU will achieve the desired level of network access and control on a permanent basis.

73. In any event, even if CEA was considered by the Commission to be able to apply for an MNC under subsection 7.1(b) of the ISMI Guideline, CEA's application would still be stymied by the restrictive requirements of subsection 7.3 of the ISMI Guideline, which require that a MNC be used for "mobile applications." Subsection 7.3(a) of the ISMI Guideline specifically requires that an applicant for an MNC use it for "terminal mobility", namely the ability of a terminal "to access telecommunication services from different locations and while in motion." This is a problematic and restrictive definition for CEA as the smart devices that make up Canada's smart grid are mostly fixed in place, although they rely upon mobile wireless networks and technology for connectivity.

74. Thus, CEA would propose the following amendments to the ISMI Guidelines in order to facilitate the granting of an MNC to CEA and all the benefits that will flow from such a grant:

a. Subsection 7.1 amended to add a new paragraph (d) that reads: "An Electric Utility related association, some of whose members operate as PVNOs, may also be an applicant for a two-digit MNC to be shared amongst its members who operate as PVNOs."

b. Subsection 7.3(a) amended to read: "The ability of a terminal to access telecommunication services from mobile wireless networks, regardless of whether the terminal itself is in motion or not, and the capability of the network to identify and locate that terminal."

c. Section 15.0, the Glossary, amended to add a new definition of PVNO as follows: "Private Virtual Network Operator (PVNO): is a full MVNO that only provides telecommunication services to itself and not to consumers, operates core network hardware (e.g., switches, routers) separate from all WSPs and has a service profile management system (e.g. Home Location Register [HLR], Home Authentication, Authorization, and Accounting [AAA], or Home Subscriber System [HSS]) for devices owned and/or operated by the PVNO that can access WSP networks in Canada."

75. As noted above, CEA is proposing that the Commission recognize a new category of wireless service provider, namely PVNOs. A PVNO would be the same, technically, as a full MVNO. However, it would not provide mobile wireless services to consumers, but only to itself (namely for private enterprise needs and internal telecommunication purposes). As such, there should be no requirements for PVNOs to adhere to any of the consumer-centric obligations imposed on MVNOs or wireless carriers such as wireless number portability. CEUs would be recognized as PVNOs.

76. CEA notes that while it would be the entity applying for a unique two-digit MNC, this MNC would then be shared among its CEU members who operate as PVNOs.

77. CEA is open to working with the Canadian Steering Committee on Numbering (CSCN) to further modify the proposed modification to the ISMI Guideline set out above, as well as any other consequential amendments required to the ISMI Guideline, so long as it enables CEA to obtain the necessary two-digit MNC so that its CEU members can share the MNC and operate as PVNOs so that CEUs can use smart devices more efficiently.

78. Regulatory action on the part of the Commission is required for CEA to obtain a shared two-digit MNC for its CEU members that will allow them to operate as PVNOs and access and operate reliable cellular

communications systems to support the build out of a cost-effective communications infrastructure for smart grid applications in Canada.

6.0 Other jurisdictions are granting or considering granting MNCs to electrical utilities

79. CEA is aware of at least one other national telecommunications regulator that has granted the relief that CEA is now seeking in this Application. The national telecommunications regulator of The Netherlands created a shared MNC to be used by public utilities and recognized a new category of mobile wireless service provider, namely PVNOs.[35]

80. The Dutch electrical and gas utility Enexis has taken advantage of the opportunity to have its own MNC, independent of the control of the telecommunications companies, to facilitate its roll-out of smart devices throughout its grid.[36] Further, Enexis indicated that the PVNO solution, in which it has access to a shared MNC, allows it to avoid the issue of SIM card lock-in.[37]

81. Other European jurisdictions, namely Belgium and Germany are also considering following the Dutch model and assigning MNC's to electrical utilities.[38] In fact, Europe's Electronic Communications Committee, which is responsible for coordinating spectrum and numbering policy across Europe, issued a report in 2014 which specifically contemplated the possibility of national regulators providing MNC's directly to utilities:

> According to Recommendation ECC/REC/(11)03 on "Numbering and Addressing for Machine-To-Machine (M2M) Communications", M2M is a communication technology where information can be transferred in an automated way with little or no human interaction between devices and applications.
>
> Machine-To-Machine (M2M) communications offer promising opportunities for new and existing market players and the M2M supply chain may vary depending on the nature of the service, the size of the M2M customer (i.e. number of M2M devices) and whether services are provided on a national or global basis. For illustrative purposes we use three examples where E.212 resources are required and where the MNC assignment may be made directly to the end customer, to a specialist intermediary or using the existing MNC
> and IMSI resources of the underlying mobile network operator.
>
> [….]

---

[35] Enexis, "Enexis Private MVNO Solution" Presented 5 November 2015 at European Utility Week, https://www.engerati.com/sites/default/files/eventpres/151105%20Enexis%20Private%20MVNO%20solution%20PUBLISH_0.PDF, at pg 18 ["Enexis Presentation"].

[36] Enexis Presentation, at pg 24.

[37] Enexis Presentation, at pg 24.

[38] Organization for Economic Co-operation and Development, *OECD Digital Economy Outlook 2015*, http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm, at pg 253.

A utility company may deploy millions of smart meters at customer premises over a wide geographic area. If the utility company wishes to move to a new MNO on better commercial terms or for improved network coverage it would need to swap out the SIM card in each of its millions of meters.

Visiting each meter would be cost prohibitive and logistically impracticable. Therefore, a network "lock-in" effect is introduced which could have a distortive effect on competition in the market. If the utility company has its own MNC and unique IMSI range then the barrier to switching could be reduced as changes to network systems could be made to facilitate the change rather than through the physical replacement of SIM cards.

Communications for smart metering is essential to facilitate customer billing but it is also an integral component in the development of smart grids. In the future, communications with smart meters will become more critical and utility companies will demand uninterrupted communications by having network redundancy arrangements in place through national roaming agreements. By having its own MNC and unique IMSI range, the utility company could enter into national roaming agreements with all the available network operators to ensure uninterrupted communications. The social and economic benefits of smart metering and smart grids should be considered in assessing the need for MNCs for this purpose.[39]

82. Domestically Canadian Researchers and Manufacturers have been promoting the PVNO operating model for electricity management. In 2014, IREQ and Ericsson published an article in IEEE Canadian Review describing the benefits of the PVNO operating model for Canadian Electric Utilities.[40]

83. Based on all of these developments, it is clear that CEA's requested relief is not radical, nor unprecedented. Utilities have successfully been granted their own MNC in The Netherlands and other European regulators are also examining the possibility of providing utilities with MNCs to facilitate the "social and economic benefits" of the smart grid.

7.0 The relief requested by CEA advances the policy objectives and is consistent with the Policy Direction

84. The relief requested by CEA advances the policy objectives in section 7 of the Telecommunications Act and is consistent with the Policy Direction.[41]

85. CEA's requested relief will advance the following policy objectives:

---

[39] European Conference of Postal and Telecommunications Administrations, Electronic Communications Committee, *ECC Report 212*, 9 April 2014, at pgs 18-19.

[40] Basile, et al. "*LTE for Smart Grid Communication The Canadian Outlook", IEEE Canadian Review, 2014*, at pgs 26-29. See http://canrev.ieee.ca/cr72/ICR72_SmarterGrid-LTE.

[41] *Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives*, SOR/2006-355 ["Policy Direction"].

a. The policy objective in subsection 7(a) will be advanced as the smart grid will provide more reliable and more affordable electricity for all Canadians than is currently available from the present power grid, thus advancing the economic and social fabric of Canada and its regions.

b. The policy objective in subsection 7(b) will be advanced as significant amounts of Canada's telecommunications infrastructure and devices rely upon electricity generated and delivered by CEUs. By improving the reliability and affordability of electricity in Canada, the smart grid will also enhance the quality of telecommunications services in Canada by ensuring that telecommunications devices and infrastructure are always able to function.

c. The policy objectives in subsection 7(c) and 7(f) will be advanced by addressing the problem of SIM card lock-in. SIM card lock-in severely limits the ability of CEUs to switch between mobile wireless carriers and is therefore a bar to effective competition. In effect, a single carrier can lock in a utility customer for years even if another carrier offers better rates or service due to the high cost of switching associated with locked-in SIM cards. If a carrier has an effective monopoly on the smart grid business provided by a CEU once it wins the initial contract, then, by definition, neither competition nor market forces are present.

d. The policy objective in subsection 7(g) will be advanced by the relief requested by CEA by placing Canada at the forefront of innovation when it comes to smart devices. The requested relief will also give Canada a vital competitive edge in the race to deploy smart grids.

e. The policy objective in subsection 7(i) will be advanced by addressing security issues and privacy of customers as CEUs would be in a position to have isolated core networks under their own control, with their own subscriber databases and management tools, thereby giving the CEUs control over all the security aspects of the service.

86. The relief requested by CEA is also consistent with the Policy Direction. By addressing the problem of SIM card lock-in, the relief will enhance competition as well as increase reliance on market forces.[42] Obviously, if a mobile wireless service provider has an effective monopoly on the provision of service to a CEU's smart devices, there can be no competition or reliance on market forces.

87. The relief is also efficient and proportionate and only requires minor changes by the Commission to definitions in the ISMI Guideline to enable CEUs to obtain their own MNCs,[43] and the creation of a PVNO category.

[42] Policy Direction at ss 1(a)(i)-(ii).
[43] Policy Direction at s 1(a)(ii).

88. The relief sought is also competitively neutral and does not favour any particular technology, carriers, or "resellers".[44]

89. Overall, CEA's requested relief advances the policy objectives in section 7 of the *Telecommunications Act* and is consistent with the Policy Direction.

8.0 Conclusion

90. Canada's power grid, while still enviable by many international standards, needs upgrading to meet the energy needs of the country in the twenty first century. The Canadian economy demands 'always on' reliable and affordable electricity. Governments are requiring CEUs to reduce their carbon emissions and deliver energy more efficiently. Individual consumers want more control over how they consume electricity and, in some cases, to sell electricity that they generate, for example, via solar panels, back to CEUs.

91. To meet these demands, CEUs need to invest in transforming their individual grids, which collectively make up the network of networks that is Canada's national electrical grid, into a smart grid. This transformation requires the deployment of millions of smart devices connected to mobile wireless networks throughout the grid to remotely monitor and modify the flow of electricity throughout the grid as necessary.

92. Unfortunately, the issue of SIM card lock-in stemming from CEUs' inability to operate their own MNC is slowing the development of Canada's smart grid by imposing significant costs and hindering the establishment of redundancy throughout the smart grid. CEUs also have significant security concerns stemming from their inability to control the security certificates associated with SIM cards that they currently receive from the MNO with whom they contract provide connectivity to their smart devices.

93. However, these obstacles will be overcome, and the deployment of the smart grid in Canada facilitated, by the Commission enabling CEA to obtain a unique two-digit MNC to share amongst its CEU members, which is the principal relief requested by CEA in this Application. In order to achieve this result, CEUs will also need to be granted PVNO status.

---

[44] Policy Direction at s 1(b)(iv).

94. With their own MNC, CEUs will be able to avoid the problems associated with SIM card lock-in, interconnect their private networks with those of other MNOs, ensure that security protocols meet utility standards, and ensure the best network reliability possible.

95. The relief sought by CEA is not only technically feasible, but it has already been implemented in The Netherlands and is being examined by national telecommunications regulators in other European jurisdictions.

96. Consequently, CEA urges the Commission to grant its request for relief in this Application and allow it to have access to a unique two-digit MNC to be shared amongst its CEU members.

97. By enabling CEA to have its own MNC, the Commission will be clearing the way for CEUs to continue deploying smart devices throughout Canada's power grid in order to transform it into a true, twenty-first century, smart grid, with all the associated benefits for reliability, affordability, the environment, and public safety that the smart grid entails.

Canadian Electricity Association | Association canadienne de l'électricité

Appendix B – Rabion Consultancy opinion on Netherlands PVNO

Rabion was asked to answer the following

1) How is the dedicated Netherlands MNC used, being shared and implemented?
2) What problems, if any, have been encountered with the Netherlands PVNO system using a dedicated MNC?
3) Does the Netherlands model from 2014 support the 2019 main objectives for Canadian Electric Utilities (CEUs): why, or why not?
    a) CEUs want to improve commercial cellular service reliability through MNO diversity, improve security (with our HSS)
    b) CEUs want to be able to fully exploit 3GPP/LTE technology for their own private networks in private licensed bands (ex: 1,8 GHz) and seamlessly interconnect with commercial networks.
    c) CEUs want to share an MNC allocated exclusively to their industry with a minimum of overhead (avoid IPX and HSS Proxy).

rabiónconsultancy

MNC ASSIGNMENT AND IMPLEMENTATION FOR UTILITY M2M MOBILE COMMUNICATION SERVICES

Rabión Consultancy BV
Koningsweg 1-B, 7255 KR Hengelo (gld) - the Netherlands
Tel. +31 (0) 650287899 - office@rabion.com – www.rabion.com

2 September 2019 (final version)

MNC ASSIGNMENT AND IMPLEMENTATION FOR UTILITY M2M MOBILE COMMUNICATION SERVICES

0. Introduction

The objectives of the Canadian Electricity sector to request Mobile Network Code (MNC) numbering resources for robust, secure, reliable and cost effective M2M communication for smart electricity grids are (1) Control of relevant portion of the core network (2) Diversity of host MNOs for availability and continuity (3) Price and contract negotiation power (4) Avoid 'lock-in' to network and switching cost for SIM cards (5) Opportunity to build private network (RAN) solutions (6) Full Control over security and authentication of SIM cards and Mobile traffic (own HLR/HSS). This memo describes the approach in the Netherlands for allocation and assignment of MNC for the utility sectors and in particular for shared MNC application, and how this would apply and compare to the request of the Canadian Electricity Association (CEA) as in Canada.
In recent times the security of access to vital elements in Mobile Networks has become subject of concern internationally. By allowing parties such as Utilities to use their own MNC, IMSI ranges and SIM cards, these parties will not be dependent on the (general purpose) security levels that the Mobile Network Operator (MNO) and their suppliers have set. By having their own MNC resources, parties such as an electricity utility are able to independently select their own suppliers (e.g. for vital network elements such as HLR/HSS), and set their own security policy and SIM card security implementation, as well as a multiple partner national roaming policy.

1. How is the dedicated Netherlands MNC used, being shared and implemented?

The country the Netherlands has been assigned the Mobile Country Code (MCC) 204, in accordance with ITU-T E.212 recommendation [7]. According its IMSI numbering plan [1], the MNC in Netherlands has a length of 2 digits, or 2-3 digits. In practice, all MNC have a length of 2 digits. A Decree [2] enforced in Netherlands in March 2014 enabled the allocation of MNC 90 and MNC 91 under the MCC 204 (shared MNCs for M2M applications). The MNC 90 and MNC 91 are allocated to identify a particular non-public electronic communication network (for cases where the MNC is not to be transmitted via radio signals and the MNC is exclusively used for the selection of a subscriber of that network for mobile communication services). The MNCs 90 and 91 can be assigned to one or more parties, and this way are available for MNC sharing scenarios. It should be noted that the Decree does not mandate that the MNC 90 or 91 must be shared. The rationale for introduction of this MNC type was to avoid that M2M applications would potentially experience large costs for SIM card replacement ('swapping') in case of a change of mobile network operator. In addition, increased commercial and public sector interest, and security and continuity of M2M services were reasons for the introduction of these MNCs.

For the deployment of shared MNCs a distinction is made between parties that have a general interest (MNC 90) and parties that fulfill a task that has been assigned based on a lawful obligation (MNC 91). Please note that currently MNC 91 is assigned only to the Electricity grid company Enexis. MNC 90 currently is not assigned. Apparently, the main reason for the low number of assignments is that no other relevant request for assignment of the shared MNCs have been received by the Numbering Plan Administrator in the Netherlands.

The Decree allows that potentially the same IMSI number starting with 204 90 or 204 91 may be assigned to multiple requesters. In cases where co-operation is required, these multiple requesters must agree on conditions for the shared use of these resources. For MNC 91 in particular this obligation is the responsibility of the first applicant (i.e. Enexis) that takes care of the governance of the shared MNC on behalf of other potential participants. Under the shared MNC multiple (MSIN) subranges of IMSIs can be defined for multiple parties that each independently can manage the deployment of such subrange (including security, roaming agreements, continuity etc.). There will be a network-related dependency however between the parties that requires deployment of certain central network elements and functions, as any external entity based on the MCC MNC will not identify these parties separately.

Private local network operators that are based on 3GPP standards also have a demand for IMSI numbers. In addition to shared MNC 90 and 91, the Decree reserves MNC 95 up to 97 (but at the same time excludes these from the numbering plan for regular MNC allocation) for network internal use for particular non-public electronic communication networks for mobile communication. The demand for these MNCs is the result of the regulation in the Netherlands for unlicensed spectrum as in the 1800 MHz range (1780-1785 MHz and 1875-1880 MHz, also known as the 'DECT guard band') that enables the deployment of Private local GSM and LTE networks. Multiple private GSM and LTE network applications will make use of these MNCs for radio identification and SIM/IMSI deployment. There is a potentially the risk of overlap of radio coverage, and IMSI assignment. This is subject for self-governance by the industry sector of private local network. Access to this spectrum is of interest to industrial and other type users because it is within the operating range of standard equipment for the 1800 MHz mobile band.

For the governance and operation of the shared MNC 91 by multiple applicants, Enexis has set up a so-called 'HLR-proxy' solution. Participants that use the same shared MNC, should together agree on the implementation, governance and distribution of responsibilities and costs for such facility. For the participating parties that share the MNC 91, all IMSIs should start with 204 91 and then a 3 number sub-range ('sub-MNC') of the MSIN that identifies to which participant in the MNC sharing this particular IMSI belongs. It should be noted that the sub-MNC is not internationally defined or standardized. As an example, the sub-range '000' is assigned to Enexis, '001' is for a next participant etc. It should be noted that the National Numbering Plan administrator assigns these sub-MNCs, although these are not notified in the Numbering plan register.

The HLR-proxy acts as the (virtual) home network gateway, and the central network element to further differentiate between the networks of each of the sub-MNC holders. From the (external) mobile network operator perspective, the HLR-proxy behaves as a regular HLR/HSS but re-directs all signalling from external networks to the desired actual HLR/HSS from the participating holder of the sub-MNC. The participating sub-MNC holder this way is flexible to (1) deploy its own SIM cards and subscriptions independent of a host Mobile Network (no 'lock-in') and of other sub-MNC holders (2) potentially has multiple national roaming agreements with host MNO networks in order to increase availability and continuity of mobile network services (3) define its own security parameters and settings independent from host MNO network(s) and of other sub-MNC holders.

It should be noted that the proxy HLR and shared MNC solution allows that participants have flexibility to decide how to implement the HLR/HSS, that is the central element in their independent network solutions:
(1) In addition to proxy-HLR, each participant can operate its own HLR/HSS
(2) Participants can decide to share an HLR/HSS. In this way an explicit 'proxy-HLR' is not required as the shared HLR/HSS functions as such.

Also, hybrid solutions are possible where multiple, but not all, participants share an HLR/HSS. Additional network elements required for a Private Virtual Network Operator (PVNO, see Annex A, Item II) tare GGSN/PGW, IPX network, DNS, SMSC (optional), and DEA/DRA. Also, for these additional network elements there is the option of sharing. It should be noted that additional Numbering resources may be required to operate PVNO, depending on service applications and type of signalling system such as MSISDNs, Signaling Point Codes, and Global Titles

It should be noted that in 2014 when the Decree was enforced, in the Netherlands there were already assignments of MNCs for non-public service. One MNC was assigned to the Ministry of Defense, for a private GSM network, and one MNC was assigned to the national Public Railway infrastructure company (ProRail) for deployment of a GSM-Rail network. The shared MNC solution would prevent having to make additional cases for similar requests (Utilities, Police, Transport companies, Automotive Industry etc.) that were expected. In the Netherlands Numbering Plan for IMSI as referred to in the Telecommunication law (article 4.1) GSM-R and Ministry of Defense are explicitly defined as a 'destination' for an MNC, in [1a] and [1b] respectively.

2. What problems, if any, have been encountered with the Netherlands PVNO system using a dedicated MNC?

Although a PVNO solution has been prepared in the Netherlands by making use of a shared MNC 91 for the purpose of M2M applications, the actual usage of the solution has not met expectations. It was expected that the substantial growth in M2M connections would trigger the use of independent IMSIs in several segments (including the Electricity Utility sector). Eventually only Enexis has rolled out the initial PVNO solution for the shared MNC, but no other Utilities have followed. Also, other segments have not applied to the shared MNCs. Enexis does not necessarily use the IMSI in the shared MNC range as they provide dual IMSI SIM cards that in addition have an IMSI in the range of one of the leading MNOs. In this respect the PVNO still provides the opportunity to avoid lock-in by this MNO, but as a passive facility that is not actively operated for the electricity market in the Netherlands. At the same time two large grid electricity network providers have decided to deploy a mobile network (CDMA450 EVDO) making use of a regular MNC. It should be noted that the electricity grid operators in the Netherlands were each taking independent positions, and were not organized as one entity to request e.g. numbering resources from the Netherlands Telecom Authorities.

In addition to the development to deploy Private MVNO for Utilities for electricity by Enexis, another mobile communication network is operated by a company named Utility Connect, that is a subsidiary of Alliander and Stedin that both are independent electricity grid operators in Netherlands. The network they operate for connectivity to Smart meters etc. is a CDMA450 (EVDO) network. Utility Connect has a PAMR license for the (unshared) use of the radio spectrum. Utility Connect has been assigned a regular MNC (MNC 66) that they use to operate this CDMA450 (EVDO) network. Reasons for operating their own network is to have maximum control over the network, and over safety/security and reliability and availability, and the autonomous nature of the network. As the 450 MHz spectrum range came available, this provided good opportunity and alternative for the PVNO solution. The advantage for them in operating a 450 MHz network is the relatively effective propagation of radio signals and deep indoor coverage this results in. It should be noted that Utility Connect as a registered provider of (public) electronic communication services, and assignee for a regular MNC, has the obligation to provide public communication services. The network however, although potentially could be used by other parties that need M2M services for critical infrastructure, is primarily used for smart meter connectivity for the Stedin

and Alliander' networks (and by Westland, another electricity grid utility). The case this way is subject to discussion as to whether the network is providing a public electronic communication service.

The lack of MNC assignment for the shared MNC resources apparently is not caused by eSIM deployment, as only very recently in Netherlands eSIM applications have been announced by T-Mobile (MNO) and by Voiceworks (MVNE/MVNO), although there may already have been proprietary solutions, or dedicated customer implementations. It should be noted that eSIM application may decrease the risk of 'lock-in', but it does not resolve the need to control relevant portion of the core network, the need to have diversity of host MNOs, the opportunity to build private network (RAN) solutions, and the need to have full control over security and authentication of SIM cards.

3. Does the Netherlands model from 2014 support the 2019 main objectives for Canadian Electric Utilities (CEUs): why, or why not?

Looking back the lesson of all this for the Netherlands is that, in 2014, for the purpose of allowing the Electricity Utility sector to independently and autonomously have mobile network connectivity in a secure and reliable manner, the Netherlands Telecom authorities as well could have assigned a regular MNC in the same way as for the Railway infra company or the Ministry of Defense. The recommendation for the Canadian case is to assign a single regular MNC (or MNCs) to the electricity sector as a whole, and to avoid the concept of shared MNC, and to leave it to the industry sector if and how occasionally they would want to make use of IMSI sub-ranges under this MNC for various electricity companies (more or less similar to MNOs that make IMSI subranges available to 'light MVNO' service providers). It should be noted that ITU-T E.212 facilitates such assignments other than for public telecommunication services as long as in accordance with procedure and criteria by the national numbering plan administrator (see Annex A, item I).

MVNOs, in the Canadian IMSI Assignment Guidelines are defined to be service providers who use a wireless carrier's facilities '*to provide mobile wireless services to consumers*'. A private virtual network service (PVNO) would not fall into this category. However, if a commercial data-only full MVNO makes use of its own MNC, and would provide M2M or IoT services to e.g. companies that apply the SIM cards in machines and equipment (whether surveillance cameras, remote monitoring systems, containers, vehicles etc.) also that is hardly a 'mobile wireless service to consumers'. If MNOs are allowed to offer such data services, why would MVNOs (or PVNOs) be restricted? This should not be argument to block allocation of MNCs e.g. to an electricity utility company, but should lead consider amendment of the IMSI Assignment Guidelines. In addition, it should be noted that ITU-T E.212 does not provide such restrictions, on the contrary (see Annex A, item I).

3a. CEUs want to improve commercial cellular service reliability through MNO diversity, improve security (with our HSS)

The Netherlands model of shared MNC facilitates the main objective that Canadian Electric Utilities have to improve (commercially available) cellular service reliability through diversity and to improve security. It should be noted however that nor a shared MNC, nor a regular MNC as a matter of course will lead to multiple host MNO network operation. For MVNOs in the telecom market it is common to guarantee exclusivity in exchange for maximum traffic volumes and lowest wholesale rates. So, a multiple host MNO network operation may be achieved but it comes with a price to pay to the MNOs. In addition, MNO tend to charge high one-off fees in order to further encourage exclusivity in the relations with MVNOs. In this respect to achieve MNO Diversity would require that MNOs have the obligation to offer communication services in case they are relevant for facilities that are vital for the public interest. It should be noted that the

large MNOs in the Netherlands, at the request of the Telecom Authorities, have implemented a solution to allow their respective subscribers on their network (as a 'regional roaming') in case one of the MNOs has a major network outage. This is however not for regular operation but only in case of network major outage. As a conclusion the introduction of shared MNCs as such has not led to multiple host MNO operation for the Utility sector.

- **3b. CEUs want to be able to fully exploit 3GPP/LTE technology for their own private networks in private licensed bands (ex: 1,8 GHz) and seamlessly interconnect with commercial networks**

The Netherlands model facilitates the ability to be able to fully exploit 3GPP/LTE technology for private networks (in private licensed bands) and to seamlessly interconnect with commercial networks. This is mainly as Netherlands Telecom authorities have been able to assign regular MNCs for the Railway infrastructure (GSM-R), the PAMR CDMA450 EVDO network for M2M, for the Ministry of Defense as well as a set of MNCs outside the scope of the IMSI Numbering plan (MNC 95-97) for private LTE and Private GSM networks. The shared MNC 90 and 91 however are explicitly for cases where the MNC is not to be transmitted via radio signals. In this respect the shared MNC as in the Netherlands does not fulfill with the requirement of Canadian Electricity Utilities to exploit private RAN networks (but this was a regulatory decision, not a technical limitation), but other MNC allocation clearly allows for that.

Shared MNC 90 and 91 such as allocated in the Netherlands are not needed in Canada in case regular 3-digit MNC (or MNCs) would be made available to Canadian Electricity Utilities. Furthermore, a PVNO does not depend on shared MNC assignment such as 90 and 91 as in the Netherlands. A PVNO can be operated as well under a regular MNC (or MNCs).

- **3c. CEUs want to share an MNC allocated exclusively to their industry with a minimum of overhead (avoid IPX and HSS Proxy)**

Although Canada uses MNC of 3 digits, in practice not the full 3-digit space is used. The background of this is found in 3GPP document TS 23.122 [4] that describes that (for North-America) a third digit of the MNC on the SIM cards is always stored as '0' (during a 'transition period'). It should be noted that initially in GSM as developed in Europe in the 1990s, MNCs were 2 digits only. The IMSI Assignment Guideline for Canada describes [8] that MNCs are assigned in the format XX0, and that XX1 to XX9 shall not be assigned to other applications. The reason is that in certain international roaming (2-digit MNC) partner networks, a 3-digit MNC potentially would not be supported. This problem did exist in the past, although at a later stage, relevant amendments in 3GPP document have been made, see [5] and [6], to avoid problems if 2- and 3-digit length MNC would be mixed. A related problem may still exist – but very exceptionally – for old mobile terminals that are according specifications for GSM older than Release 1998. For a PVNO such as a Canadian electricity utility such problems in other networks and terminals are not relevant (i) there are no (unknown) terminals (let alone pre-Release 1998 terminals) that would need to roam on the Canadian Utility PVNO network (ii) the Canadian Utility PVNO terminals do not internationally roam in networks that potentially may not support 3-digit MNCs (if international roaming would exist anyway, it is with networks in the neighboring USA).

In case that exhaustion of MNC resources may be a consideration for the Canadian Telecom authorities not to allocate a XX0 resource, the above determines that the authorities could consider assignment of a true 3-digit MNC (XXY) and optionally reserve the remaining 9 combinations under the XX for similar independent assignments for different industry or public sectors. Such XXY combination will not limit Canadian Utilities in their objectives, and it will not negatively impact the Canadian MNOs (These MNOs have no difficulty to distinguish between 2-digit and 3-digit as otherwise they could not service e.g. European MNOs that all

have 2-digit MNCs). Under the XXY the Canadian Utilities can define their own IMSI sub-ranging scheme without involvement of the Telecom authorities (assuming there are no conflicting rules in the IMSI Assignment policy or Telecom law). The assumption for this case however is that the Utilities need to cooperate to govern, operate under the same MNC, and share some mobile communication network facilities.

Alternatively, each Electricity Utility company may have its own true 3-digit MNC. This has the advantage that it is not mandatory for Utilities (although likely feasible) to cooperate and share mobile communication network facilities such as an HLR-proxy or an HLR/HSS. Following the Netherlands experience – where electricity utility companies were taking independent positions – this option is preferred as it provides optimal independency and flexibility, and independent decision-making for investment in mobile communication network solutions. Given the current IMSI Assignment Guideline it seems logical to assign MNC to Canadian Utilities under the same XXY range for that matter and assign XX0, XX1 etc. to the individual applicants, where even one XXY combination could be reserved for MNC (future) sharing by multiple applicants.
The latter case best reflects the situation in the Netherlands that has shared MNCs for multiple applicants, as well as MNC for dedicated parties such as the operators of the CDMA450 network, the railway infrastructure, and the Ministry of Defense. In Netherlands however, these MNCs are not a sequential MNC range, but random in the IMSI numbering plan.

By providing one or several true 3-digit MNCs in Canada to Canadian Electricity Utilities a shared MNC such as enforced in Netherlands are of low purpose. Other than in a 2-digit case, 3-digit MNC assignments have a very low effect impact on MNC resource capacity/depletion. It also is an advantage that a true 3-digit MNC solution is fully compliant with the ITU-T E.212 recommendation and does not require regulatory directives for central governance or central facilities, such as is the case in the Netherlands. As a conclusion for Canada a shared MNC solution as in the Netherlands is feasible for Canada and technically will function, but it seems to solve a problem that Canada does not have. By allowing 10 MNCs in an XXY combination, there is kind of 'sharing' however when compared to the current practice of assigning only XX0, but it should not be called 'sharing' as the MNCs are to be considered as regular MNCs in accordance with ITU-T E.212. Obviously the IMSI Assignment guideline will have to be amended for this matter and allow assignment of true 3-digit MNCs for particular parties such as Canadian Electricity Utilities (that generally have no interest in International roaming).

4. Conclusion and summary of major findings

This memo describes the approach in the Netherlands for allocation and assignment of MNC for the utility sectors and in particular for shared MNC application, and how this would apply and compare to the request of the Canadian Electricity Association (CEA) as in Canada.

In Netherlands, the MNC 90 and MNC 91 are allocated to identify a particular non-public electronic communication network (where the MNC is not to be transmitted via radio signals) and can be assigned to one or more parties, and this way are available for MNC sharing scenarios for M2M applications. In addition, MNC 95 up to 97 are reserved for the deployment of Private local GSM and LTE networks (in 'DECT guard band'). In the Netherlands there were already assignments of MNCs for non-public service. One MNC was assigned to the Ministry of Defense, for a private GSM network, and one MNC was assigned to the national Public Railway infrastructure company (ProRail) for deployment of a GSM-Rail network. Although a PVNO solution has been prepared in the Netherlands, and share networks solution is implemented, the actual usage of the shared MNC solution has not met expectations. At the same time two large grid electricity network providers have decided to deploy a mobile network (CDMA450 EVDO) making use of a regular MNC.

The Netherlands model facilitates the main objective that Canadian Electric Utilities have to improve (commercially available) cellular service reliability through diversity and to improve security. The Netherlands model facilitates the ability to be able to fully exploit 3GPP/LTE technology for private networks and to seamlessly interconnect with commercial networks.

The recommendation for the Canadian case is to assign a single regular MNC (or MNCs) to the electricity sector as a whole, and to avoid the concept of shared MNC. The authorities could consider assignment of a true 3-digit MNC (XXY) and optionally reserve the remaining 9 combinations under the XX for similar independent assignments for different industry or public sectors. Alternatively, each Electricity Utility company may have its own true 3-digit MNC. This has the advantage that it is not mandatory for Utilities (although likely feasible) to cooperate and share mobile communication network facilities such as an HLR-proxy or an HLR/HSS. This option provides optimal independency and flexibility, and independent decision-making for investment in mobile communication network solutions.

The ITU-T E.212 identification plan was originally developed for use of IMSI in Public Land Mobile Networks, and did not facilitate the use of IMSI and the assignment of MNC for private network application or private usage. It should be noted that the current version of the ITU-T E.212 recommendation facilitates national assignment policies for MNCs for non-public application

REFERENCES

[1] https://wetten.overheid.nl/BWBR0010199/2014-03-13

[1a] https://wetten.overheid.nl/BWBR0010199/2014-03-13, Artikel 1, sub d, punt 3

[1b] https://wetten.overheid.nl/BWBR0010199/2014-03-13, Artikel 1, sub d, punt 5

[2] Decree 'Nummerplan voor identiteitsnummers ten behoeve van internationale mobiliteit ('IMSI-nummers)'

[3] Artikel 4.2b of the Telecommunicatiewet

[4] Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode; 3GPP Technical Specification (TS) 23.122; v12.2.0; September 2013

[5] Numbering, addressing and identification; 3GPP TS 23.003; v12.0.0; September 2013

[6] Characteristics of the Universal Subscriber Identity Module (USIM) application; 3GPP TS 31.102 V12.1.0; September 2013

[7] The International Identification Plan for Public Networks and Subscriptions; ITU-T E.212 (09/2016), version 6.0

[8] Canadian International Mobile Subscription Identity (IMSI) Assignment Guideline, Version 5.0, Approved by Telecom Decision CRTC 2015-496, Dated: 6 November 2015

Annex A Back up items

I. ITU-T E.212- the purpose of the IMSI (MNC)

The ITU-T E.212 identification plan was originally developed for use of IMSI in Public Land Mobile Networks (PLMNs), and did not facilitate the use of IMSI and the assignment of MNC for private network application or private usage.
In the current version of the recommendation [7] still the assignment of MNCs is addressing the public use of IMSIs for identification. The recommendation however has been modified (Annex B, Item 6) and defines that '*MNCs are to be assigned to applicants and used by assignees for public networks offering public telecommunication services. In addition MNCs may be assigned to other applicants (e.g. for GSM-R networks) and these assignments are to be made according to procedure and criteria established by the national numbering plan administrator*'.
This way the ITU-T E.212 recommendation facilitates assignment policies for MNCs for non-public application (for Utilities, GSM-R, private local networks or else) in compliance with the ITU-T E.212 recommendation. It should be noted that at the time of the enforcement of the Decree [2] in the Netherlands that introduced shared MNC 90 and MNC 91, as well as MNC 95-97 for private local networks, was prior to the above modification of the ITU-T E.212, and in this respect was causing discussion of compliancy to the recommendation.

Furthermore, Annex B, item (2) in the recommendation is of relevance for the Canadian Utilities request for an MNC: '*The applicant must demonstrate a need for the resource and must further demonstrate that other reasonable technical and operational alternatives (e.g., use of already assigned MNCs, use of national allocated or assigned shared MNCs, use of embedded SIM) are not appropriate. The applicant must attach substantiating documentation justifying this fact*'.

II. The concept of PVNO

A mobile virtual network operator (MVNO) is a provider of public electronic communication services, but that that does not own a radio network infrastructure MVNOs enter into wholesale agreements (national roaming agreement) with a mobile network operator for access to network service. An MVNO (in case a 'full MVNO') provides own SIM cards and IMSI ranges (based on MNC assigned to the MVNO), operates its own core network architecture including HLR/HSS, and its own interconnection and international roaming agreements. In addition, 'light' MNVOs (or Service Providers) exist that make use of SIM card, IMSI ranges, core network architecture of the host Mobile network Operator for the MNVO, and interconnection and international roaming agreements.
A private virtual network operator (PVNO) is like an MNVO but for closed group of users.

III. DECT Guard band

Private local mobile networks in te Netherlands can make use of the DECT guard band. Since 2008 the band contained two small paired spectrum ranges 1782,5-1785 MHz and 1877,5-1880 MHz (2*2,5 MHz) that in the National Frequency Plan had been made free of license. Since February 2013 the spectrum ranges were extended to 1780-1785 MHz and 1875-1880 MHz. The DECT guard band lies within the spectrum range of regular GSM mobile terminal that support the 1800 MHz band (1710-1785 MHz and 1815-1880 MHz).