CEPT ECC
Electronic Communications Committee

ECC Report 337

Public numbering resources for mobile non-public networks

approved 7 June 2022

0 EXECUTIVE SUMMARY

The development of Long Term Evolution (LTE) and 5G network technology continues apace and network rollout is likely to accelerate over the next few years. It is expected that this will result in a proliferation of non-public networks (NPNs) that might put distinct requirements on the use of public numbering resources.

A CEPT harmonised approach to the assignment and use of public E.164, E.212 and other relevant numbering resources for NPNs may be required. We have studied the emergence of NPNs in a mobile environment and looked at their need to use public numbering resource and found that, in general, NPNs are used to provide services to enterprises and they are not used for providing services to the general public, and proceeded to present various business models and network topologies that can more readily be termed as 'non-public networks', principally on the strength of two factors, namely (a) the limited, if any, interface with the 'general public' for the ECS being transmitted, and(b) the distinct or reduced requirements and usage of publicly assigned resources, in particular E.164, E.212 and E.118 numbering resources.

Some guidance to NPAs is provided on the management of public numbering resources for NPNs especially E.212 numbering resources.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Explanation
5GS	5G System
ACIA	Alliance for Connected Industries and Automation
ATIS	Alliance for Telecommunications Industry Solutions
CAG	Closed Access Group
CBRS	Citizens Broadband Radio Service
CEPT	European Conference of Postal and Telecommunications Administrations
CSG-ID	Closed Subscriber Group ID
ECC	Electronic Communications Committee
ECN	electronic communications network
EECC	European Electronic Communications Code
eMBB	enhanced Mobile Broadband
ETS	ETSI Telecommunication Standard
GMSC	Gateway MSC
GSM	Global System for Mobile communications
HLR	Home Location Register
ICCID	Integrated Circuit Card Identifier
ID	Identifier
IIN	Issuer Identifier Number
IIoT	Industrial Internet of Things
IMSI	International Mobile Subscription Identity
IOC	IMSI Oversight Council
IP	Internet Protocol
ISPC	International Signalling Point Codes
LTE	Long Term Evolution
NFV	Network Function Virtualisation
NHN	Neutral host network
NID	Network identifier
NNAI	Numbering, naming, addressing and identification
NPA	Numbering Plan Administrator
NPN	Non-public network
MCC	Mobile country code

Abbreviation	Explanation
MFA	MulteFire Alliance
MNC	Mobile Network Code
MNO	Mobile Network Operator
mMTC	massive Machine Type Communication
MOCN	Multi-Operator Core Network
MSRN	Mobile Station Roaming Number
MS	Mobile Station
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber ISDN Number
MVNO	Mobile Virtual Network Operator
OTT	Over-The-Top
PAN	Primary Account Number
PLMN	Public Land Mobile Networks
PNI-NPN	Public-Network Integrated Non-Public Network
PRN	Provide Roaming Number
RAN	Radio Access Network
ROIO	Regional and other international organizations
SANC	Signalling Area/Network Codes
SDN	Software Defined Networking
SIM	Subscriber Identification Module
SNPN	Stand-alone non-public network
TAC	Tracking Area Code
TMSI	Temporary Mobile Subscriber Identity
VLR	Visitor Location Register
VPN	Virtual Private Network
UE	User Equipment
UHD	Ultra-High-Definition
URLLC	Ultra-Reliable and Low-Latency Communication

1 INTRODUCTION

Long Term Evolution (LTE) and 5G network technology development continues apace and network rollout is likely to accelerate over the next few years. It is expected that this will result in a proliferation of non-public networks (NPNs), some of which would also need to interconnect/roam with public networks.

Various regulators around the globe are licensing spectrum for local access use, some of which is intended for non-public LTE and 5G networks for enterprises. It is likely that there will be a mix of network topologies and business models that could emerge from this, mainly:

- isolated and purely private networks;
- non-public networks with interconnection/roaming to public networks;
- wholesale/neutral-host networks;
- new managed service providers with spectrum in a number of locations (e.g. Smart Building Mobile Operators);
- Mobile Virtual Network Operators (MVNOs) or “slice” virtual networks linked to an existing Mobile Network Operator (MNO), perhaps with a separate core and local breakout run by the enterprise;
- Vertical players with wide-area/national networks (utilities, road and rail, public safety etc.).

From a numbering perspective, these developments raise some questions:

1 Is there a need for Numbering Plan Administrators (NPAs) to develop policies in relation to allowing NPNs to use numbers?

2 What numbering resources of ITU-T Recommendation E.164, E.212 and E.118 could be assigned for non-public networks?

3 What are their needs with respect to Mobile Network Codes (MNCs) within geographic Mobile Country Codes (MCCs) or can they use MCC 999 or MNCs under shared MCC 902 for Standards Development Organisations (SDOs) etc.?

A CEPT harmonised approach to the assignment and use of public E.164, E.212 and other relevant numbering resources for NPNs may be required. The purpose of this ECC Report is to examine the numbering requirements of NPNs and identify sustainable solutions to support market development while carefully managing scarce resources.

2 BACKGROUND

This section describes the different public numbering, naming, addressing and identification (NNAI) resources used in public mobile networks that might also be needed for NPNs.

2.1 NNAI RESOURCES FOR PUBLIC MOBILE ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES

The goal of any NNAI plan is to support electronic communications anywhere at any time in any medium and promote the interests of end-users through providing access to a wide range of electronic communications services and to other end-users.

There exists a variety of identifiers (IDs) in different types of NNAI plans and they can be structured in the following groupings depending of the primary usage of the plan:

- Plans for end-user services/applications;
- Plans for network functions/elements;
- Plans for administrative purpose;
- Plans for equipment/terminals/devices;

In Figure 1, the colour codings of the different IDs shows which organisations define, manage, allocate and assign IDs on the highest level. Light red means IDs under International Telecommunication Union (ITU) responsibility, light blue means ETSI, dark blue means ICANN/IANA/RIPE NCC, black means closed IDs (peer-to-peer) assigned by the entity providing these services (e.g. Over-The-Top (OTT) services), red means ISO, and grey means 3GPP/GSMA.

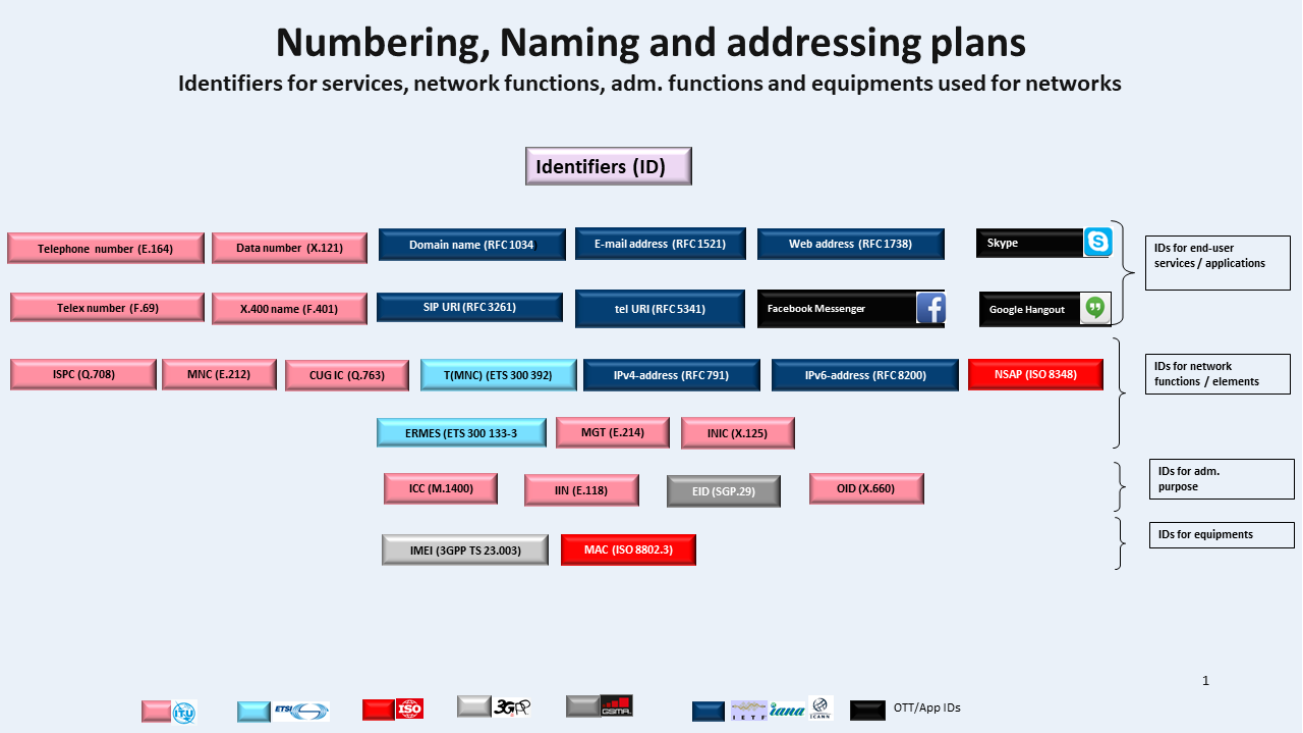


Figure 1: Overview of different identifiers used for public electronic communications networks and services

In general, NPAs' responsibility covers the management and assignments of resources (IDs) from plans under ITU and ETSI administration. For EU countries, this responsibility is stated in Recital 250[1] in the Directive 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code (EECC) [1].

Allocation and assignment can be made on different levels depending on kind of resource, also if the resource is built upon specific parts, e.g. concerning signalling point codes ITU, on a global level, assigns Signalling Area/Network Codes (SANC) to the Member State/NPA and then the NPA assigns International Signalling Point Codes (ISPCs) to the provider of electronic communications networks. This tier concept can be split on these levels; global level, regional level, national level and operator level.

In Public Land Mobile Networks (PLMNs[2]) most of the basic ITU/ETSI/3GPP resources are used together with other kind of Internet based IDs. In general, each resource in electronic communications networks and/or services are specified in recommendations/technical specifications from SDOs, e.g. Issuer Identifier Numbers (IINs) are described in ITU-T Recommendation E.118.

For mobile networks, since the introduction of Global System for Mobile communications (GSM), first ETSI[3], then 3GPP have collected all NNAI resources used in PLMNs in a specific technical specification, 3GPP TS 23.003[4] [2]. The origin of the resource is normally from another 3GPP specification and then it is summarised in TS 23.003.

There are many different kinds of resources in TS 23.003 and the amount has grown[5] since 2G networks up to 5G networks. IDs that are covered by TS 23.003 include both public IDs, private IDs and IDs that are assigned to (Mobile Stations (MSs)/(User Equipment) UEs). Many of the IDs are used temporary in the networks and are allocated and assigned by the operators and some other IDs are allocated and assigned on either global, regional and national level by an administrator. Some of the resources are comprised of parts coming from other public resources, e.g. of E.212 MCCs and MNCs.

The numbering resources assigned by NPAs for providing mobile services are mainly those pertaining to the following ITU-T Recommendations E.164, E.212, and E.118:

- E.164 numbering resources are mainly used as Mobile Subscriber ISDN Number (MSISDN) and also as Mobile Station Roaming Number (MSRN);
- E.212 numbering resources are mainly used for the registration of the Subscriber Identification Module (SIM) in the PLMN and for the identification of the subscription using International Mobile Subscription Identity (IMSI) and Temporary Mobile Subscriber Identity (TMSI);
- E.118 numbering resources are the primary account number and are used only in management systems as Integrated Circuit Card Identifier (ICCID), that is the serial number of the SIM and in case of embedded SIM (eSIM), the ICCID is the identifier of the profile;
- Q.708 numbering resources are used to identify the ISPC used by the Signalling System No. 7. An ISPC is defined as a signalling point code with a unique 14-bit format used at the international level for signalling message routing and identification of signalling points involved.

[1] All elements of national numbering plans should be managed by national regulatory authorities, including point codes used in network addressing. Similar was stated in Recital 20 in the framework directive (2002/21/EC).

[2] Digital cellular telecommunications system and the 3GPP system.

[3] Technical specification GSM 03.03, also numbered by ETSI as ETS 300 523.

[4] Numbering, addressing and identification, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729.

[5] The first version of the specification for GSM was around 15 pages and for the latest 5G version for Release 17 has grown up to around 146 pages.

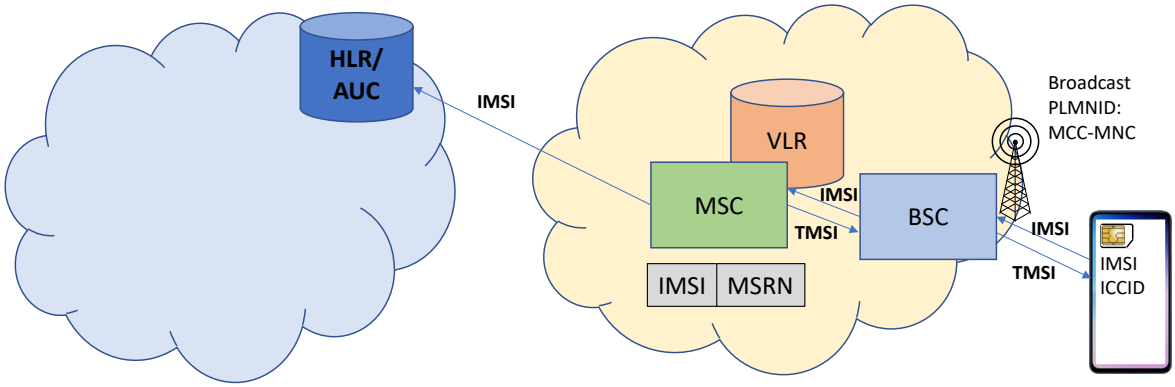


Figure 2: Mobile network architecture and main numbers used in mobile terminal registration

Figure 2 shows the main elements (their names could change with the different technology, i.e. 2G, 3G, 4G and 5G) and the main numbers involved in the registration of the mobile terminal when this is switched on. IMSI, stored in the SIM, and the mobile terminal position (i.e. Mobile Switching Centre/Visitor Location Register (MSC/VLR) address) are sent to the Home Location Register (HLR), where they are associated with the mobile telephone number (MSISDN). For security reason, a TMSI is generated by the VLR and communicated to the mobile terminal in order to be used in subsequent communications, so limiting the number of times the IMSI is sent over the radio interface. The ICCID is not communicated by the mobile terminal to the network and therefore the ICCID is not used in the signalling system but only in management systems.

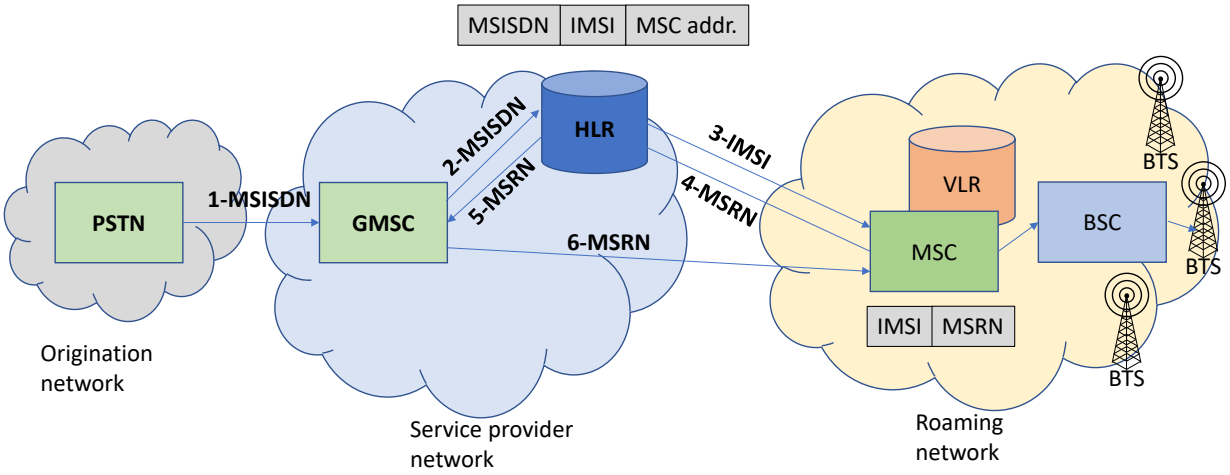


Figure 3: Mobile network architecture and main numbers used in incoming calls

Figure 3 shows the main steps involved in order to reach the registered mobile station when a call is originated in a fixed network. First of all, on the basis of the called MSISDN, the home network handling the MSISDN is reached (1). In the implementation, other elements, not shown in the picture, may be involved considering number portability. Upon reaching such network, before proceeding with the call set-up, a Send Routing Information (SRI) query is issued by the Gateway MSC (GMSC) to the HLR using the MSISDN (2). The HLR then sends a Provide Roaming Number (PRN) request including the IMSI to the MSC/VLR identified by the stored MSC/VLR address (3) and the HLR then receives the MSRN to be used in the response (4). Such number is communicated to the GMSC (5) in order to proceed with the call setup towards the destination mobile terminal (6).

2.2 WHAT IS A NON-PUBLIC NETWORK?

As noted in Section 1, new business models and network topologies are emerging, which to some extent, are different from public mobile electronic communications networks, with implications on the continued suitability of current policy and regulatory approaches towards these new models, in particular on the need for and

assignment of public NNAI resources. To distinguish the models within the scope of this Report from the public electronic communications networks, this Report analyses "non-public networks" (NPN), introduced from Release 16 by 3GPP TS 22.261 [3]. From a technical point of view, NPNs are defined in 3GPP TS 22.261 as *networks that are intended for non-public use*. Moreover, it is described that *non-public networks are intended for the sole use of a private entity such as an enterprise, and may be deployed in a variety of configurations, utilising both virtual and physical elements. Specifically, they may be deployed as completely standalone networks, they may be hosted by a PLMN, or they may be offered as a slice of a PLMN*.

On the other hand, from a legal and regulatory point of view, it must be noted that there is no specific definition for "non-public networks"[6] in the European Electronic Communications Code (EECC). Given this situation, and the above 3GPP definition, the term "non-public network" could be understood as referring to a variety of networks that do **not** fit within the defined term of "public electronic communications network" as per Article 2(8) of the EECC, namely:

- 'public electronic communications network' means an electronic communications network **used wholly or mainly** for the provision of publicly available electronic communications services which support the transfer of information between network termination points.

By implication, this could mean that **non-public** electronic communications network (ECN) are **not** wholly or mainly used for the provision of publicly available electronic communications services. However, a **non-public** electronic communications network may be realised using part or sharing components/part of the network elements of a public electronic communications network.

This Report is therefore not intended to identify, from a legal and regulatory perspective, whether a specific network is to be considered as a public or a non-public (ECN). Indeed, it is up to CEPT administrations to determine it, not least in the context of regulating providers and ensuring adherence with national regulations (e.g. notification for general authorisation and other obligations). In general, however, NPNs are used to provide services to enterprises and they are not used for providing services to the general public.

In the next sections, the Report presents various business models and networks that can more readily be termed as 'non-public networks', principally on the strength of two factors, namely:

a) the limited, if any, interface with the 'general public' for the ECS being transmitted,

b) the distinct or reduced requirements and usage of publicly assigned resources, in particular E.164, E.212 and E.118 numbering resources.

2.3 ENABLERS FOR THE ADOPTION OF NON-PUBLIC NETWORKS

The implementation of NPN may be based on a physical separation or utilising different techniques allowing the creation of logical separation of the single NPN with respect to the other networks.

This section explores the main enablers for NPNs.

2.3.1 5G Capabilities

The main novelty with the introduction of 5G is the expansion of mobile networks to different vertical businesses besides the traditional mobile broadband market. 5G is expected to create an ecosystem for technical and business innovation involving several different vertical markets including utilities, smart cities, healthcare, public sector, public transportation, agriculture and manufacturing. It will serve a larger portfolio of applications with requirements such as high reliability, ultra-low latency, high bandwidth and mobility. This is possible since 5G would provide far more enhanced capabilities than previous mobile generations which were primarily

[6] The term "non-public networks" (NPN) is used in this report while the term "private networks" has been used in other CEPT deliverables, e.g. ECC Report 265 (clause 9.3 - Migration from PSTN/ISDN to IP-based networks and regulatory aspects) and ECC report 301 (clause 2 - Provision of Caller Location Information from Private/Corporate Networks).NPN, as used in this Report, has a wider scope than "private networks" as used in these other CEPT reports.

designed as general purpose communication networks with limited service differentiation capabilities across use cases.

The three major service categories expected to be supported by the 5G include enhanced Mobile Broadband (eMBB) services, Ultra-Reliable and Low-Latency Communication (URLLC) services, and massive Machine Type Communication (mMTC) services as illustrated in Figure 4.

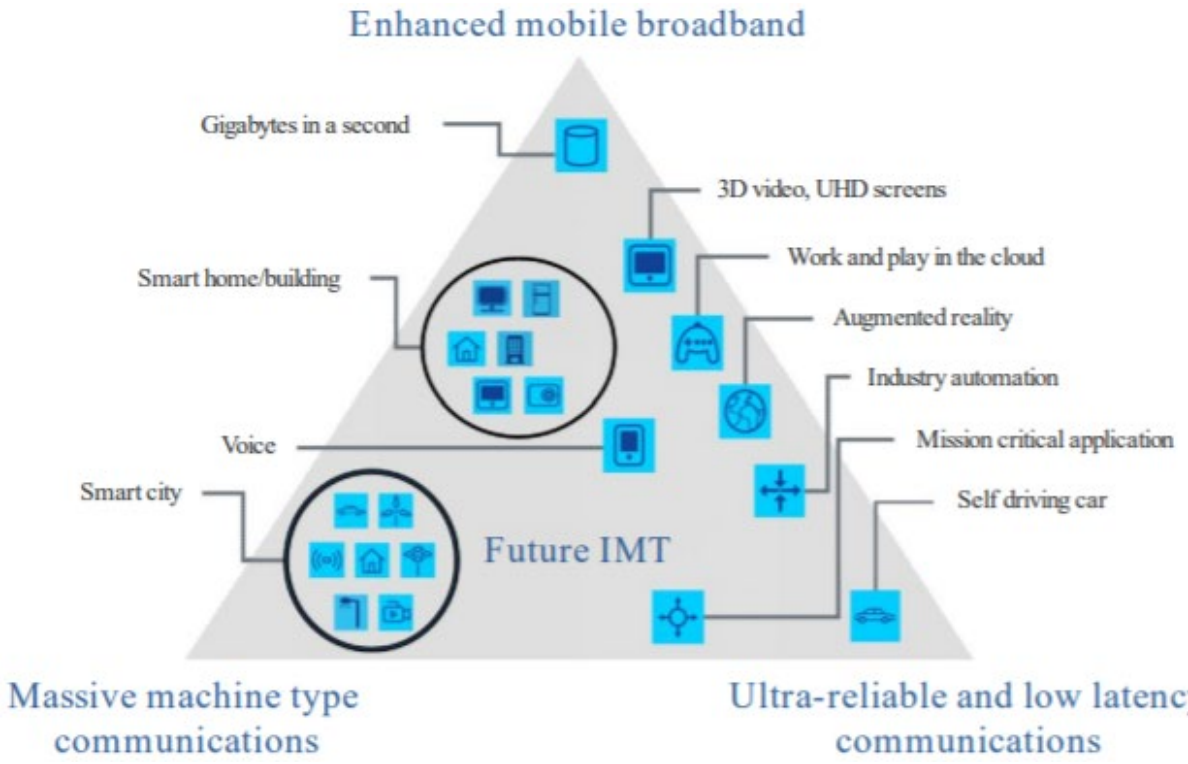


Figure 4: Usage scenarios for IMT for 2020 and beyond (Source: Recommendation ITU-R M.2083-0)

eMBB services allow end-users to experience high-speed and high-quality multimedia services (e.g. virtual reality, augmented reality, 4k or 8k ultra-high-definition (UHD) videos and even hologram services) at any time and place. In this respect, these services mainly address human-centric use cases for access to multi-media content, services and data. The eMBB usage scenario will come with new application areas and requirements in addition to existing mobile broadband applications for improved performance and an increasingly seamless user experience. This usage scenario covers a range of use cases which have different requirements. These include:

- The hotspot case for areas with high user density where very high traffic capacity is needed, the requirement for mobility is low and user data throughput is higher than that of wide area coverage, and
- The wide area coverage case where seamless coverage and medium to high mobility are required together with much higher user throughput rates than existing rates. However, in this case, the data throughput requirement may be lower when compared to the hotspot case.

URLLC services enable delay-sensitive and mission-critical services that require very low end-to-end delay. The URLLC usage scenario has stringent requirements for capabilities including throughput, latency and availability. Examples of URLLC use cases include tactile Internet, real-time traffic control, self-driving vehicles, wireless control of industrial manufacturing or production processes, distribution automation in a smart grid and remote medical surgery.

mMTC services (i.e. IoT/M2M services) enable services involving massive numbers of MTC devices which are typically characterised by a very large number of connected devices typically transmitting a relatively low volume of non-delay-sensitive data. An important requirement in mMTC use cases is for devices to be low cost and with very long battery life.

5G capabilities would enable several innovative usage scenarios. In particular, there are a number of envisaged scenarios (e.g. for industry automation, enterprise-controlled network, utilities, public safety, smart buildings, self-driving vehicles, medical equipment, mining and supply-chain management such as at airports and ports, etc.) which may be considered as best-served by non-public networks, depending also on the circumstances of each use case including specific requirements such as low latency and/or high reliability, high availability, high bandwidth, security, enterprise-specific integration and economic considerations.

2.3.2 Network Slicing

The ubiquitous digitalisation in all realms of private and professional life as well as the exponential growth of network and storage capacities have paved the way for the emergence of new use cases in the field of telecommunications technologies – self-driving cars, smart factories, smart cities, smart grids, multimedia applications etc.

The 5G telecommunications standard has a key role in this development allowing higher data transfer rates due to the increased bandwidth. Users, devices and applications in those new fields often have different performance and service requirements for the telecommunications networks. In order to meet the various challenges of different service level needs, great flexibility is required. For example, M2M applications have other demands in regard of latency, data transfer rates, coverage/reach, availability, reliability, maximum device density etc.

Network slicing is considered as a key technology to achieve the necessary flexibility. Using techniques as Software Defined Networking (SDN), Network Function Virtualisation (NFV) and Cloud Computing makes it possible to create separate logical networks within a common physical network such that each network slice provides certain specific capabilities and characteristics to address different mobile services market scenarios. These independent logical networks or "slices“ can be modified accordingly to the individual requirements of the particular user, application or device. Adjusting and thus making the common telecommunications network more flexible through network slicing enables it to serve better the highly individual needs of the customers.

2.3.3 Virtual private networks

The term Virtual Private Network (VPN) has been used for many years in electronic communications terminology and is now broadly used to describe a number of different network scenarios. The basic principle of a VPN is that the network is for the sole use of a private individual or organisation but is realised using inputs from public networks. Applications running across a VPN therefore benefit from the functionality, security, and management of a private network.

VPN technology was developed to provide access to corporate applications and resources to remote or mobile users, and to offices distributed over a wide geographic area. In a circuit-switched world, different parts of the private network could be connected using dedicated fixed or wireless links provided by a public network for a fee. As technology evolved, public inputs to private networks became available using Internet Protocol (IP) technology. A VPN can therefore be created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunnelling protocols over IP networks.

2.3.4 Neutral host network

According to Alliance for Telecommunications Industry Solutions (ATIS) [5], a neutral host network (NHN) combines two concepts - the concept of "hosting" and the concept of "neutrality". The hosting concept refers to an entity that provides a certain set of resources that are made available to clients (i.e. MNOs) in order to allow the hosted clients to provide continuous services. The "neutrality" concept refers to the host acting as a shared platform to multiple hosted clients. Neutrality in this context does not imply strict equality between hosted clients, as the resources offered to each hosted client are subject to commercial agreement between the neutral host and the hosted client, and policy-based management may be applied.

From a user’s point of view, the system behaviour and services using the resources of a neutral host should be available without user intervention and these should be seamless and identical to those provided by their hosted clients’ dedicated resources. Because neutral hosting provides service equivalence to the user, it can be a viable alternative to conventional dedicated infrastructure.

NHNs have many possible use-cases, and several business and technical architecture models. The main common theme is wholesale enablement of 4G/5G, in areas with poor coverage, reflecting difficult economics or tricky accessibility. A secondary motivation is a desire by venue/property owners for more control of wireless usage - and ideally monetisation.

The key uses for NHN deployment are:

- Rural / remote areas;
- Metropolitan centres needing 4G/5G densification with small cells;
- In-building, especially for large sites such as offices, stadiums and hotels;
- Road and railtrack coverage (and potentially in-vehicle);
- Industrial sites and large transport hubs;
- Temporary sites and events (e.g. festivals, major construction projects);
- Some classes of residential and SME commercial venue.

3 VARIANTS OF NON-PUBLIC NETWORKS IN MOBILE ENVIRONMENT

This section explores four 'variants' of NPNs, as described in the 5G Alliance for Connected Industries and Automation (5G-ACIA) white paper entitled "5G Non-public networks for Industrial scenarios" [6].

The four variants can be grouped, according to 3GPP terminology, under three categories, with the first solely containing the 'Stand-alone Non-Public Network (SNPN)' (Section 4.1), the second containing the SNPN with shared Radio Access Network (RAN) (Section 4.2) and the third containing two variants of 'Public-Network Integrated-Non-Public Networks – (PNI-NPN)' (Section 4.3). A number of implementation options for these variants are also considered[7]. Similar NPN variants could also exist for LTE, albeit these would not be based on 5GS.

3.1 VARIANT 1 – STAND-ALONE NON-PUBLIC NETWORK

In the first scenario (Figure 5) the SNPN is separated from the public one. In this scenario, the SNPN has its own dedicated base station(s) and core network functions. There could be different implementation approaches to realise SNPNs, some of which are explored in Section 6.

An optional connection to the public network services via the firewall, as shown in Figure 5, could be employed to enable access to public network services while the NPN service customer is within SNPN coverage. If desired, the fixed optional connection can be leveraged to access services offered inside the SNPN via the public network.

5G-ACIA [6] illustrated that alternatively, devices inside the SNPN could subscribe directly to the public network to access its services (devices with multiple subscriptions – e.g. multiple SIMs (MUSIM)) without going through the NPN firewall, which may represent security issues.

If the SNPN area is also covered by the public network RAN, a device with two SIMs, one related to the SNPN and the other one related to the public network, could operate with both mobile networks.

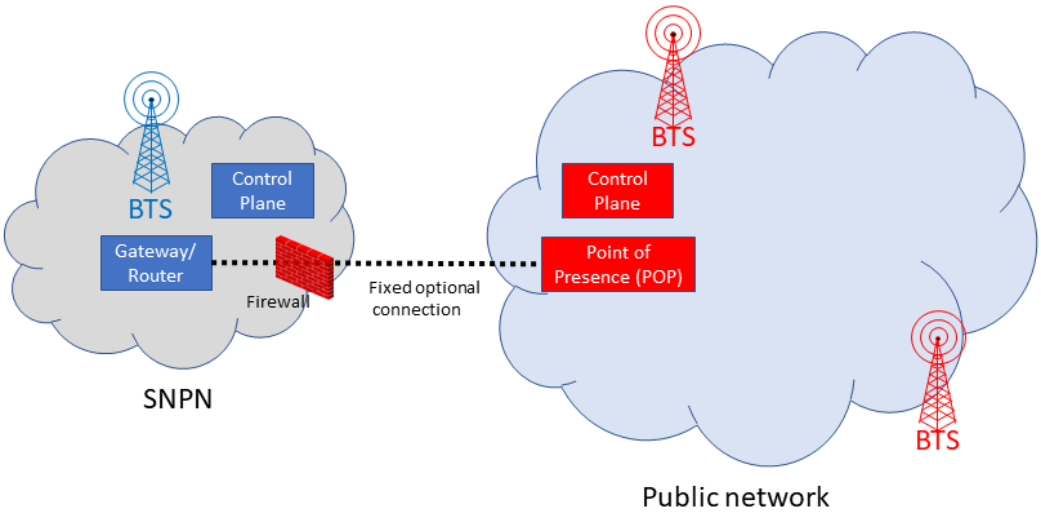


Figure 5: Deployment as isolated network (adapted from: 5G-ACIA)

[7] The implementation options are described to illustrate possible technical solutions but do not imply that they are possible from a legal/regulatory point of view, also due to national specificities.

3.2 VARIANT 2 – STAND-ALONE NON-PUBLIC NETWORK WITH SHARED RADIO ACCESS NETWORK

In the scenario below (Figure 6), the non-public network and the public network share part of the RAN, including one or more base stations, while other network functions remain segregated. RAN sharing functionality is specified in 3GPP TS 23.251 "Network sharing; Architecture and functional description" [7].

Under this variant, network control and user plane tasks for activity by devices with an NPN subscription (i.e. devices of NPN service customers) are directed from the (shared RAN) base station towards the non-public network, whereas if the same device can also attach to the public network (only if it is dual subscription), then this portion of traffic would be directed to and controlled by the public network.

In this case, the alternatives for the PLMN ID of the non-public network would be identical to those for Variant 1.

For the Variant 2, it is also possible to have an optional connection between the non-public network and the public network, typically established through a firewall for security reasons, and the same considerations as described for Variant 1 would apply.

As in the previous scenario, using a device with a MUSIM enables the communication through both networks.

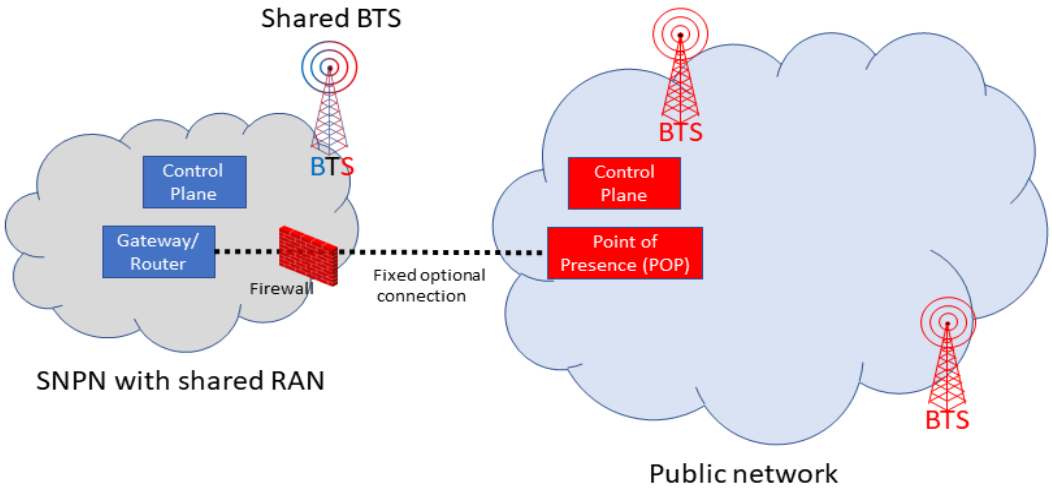


Figure 6: Deployment with shared RAN (adapted from: 5G-ACIA)

3.3 VARIANTS 3 AND 4 – PUBLIC NETWORK INTEGRATED NON-PUBLIC NETWORKS (PNI-NPN)

The 5G ACIA white paper [6] lists two distinct scenarios, which depend on sharing core network functionality between the NPN and public network.

In the scenario of Variant 3 illustrated in Figure 7, the main difference with respect to the scenario of Figure 6 is that the control plane (i.e. signalling part) is also shared with the public network, whereas user plane (i.e. bearer part) tasks for NPN service customers are handled within the NPN. Variant 3 would allow NPN devices to connect directly to the public network and its services, including roaming. Furthermore, there may also be an optional connection from the non-public network services to public network services, as shown in Figure 7, to connect NPN devices to non-public network services via the public network when the device is outside NPN coverage, but within public network coverage. If public network services are accessed directly via the public network, the optional connection is not needed for this purpose.

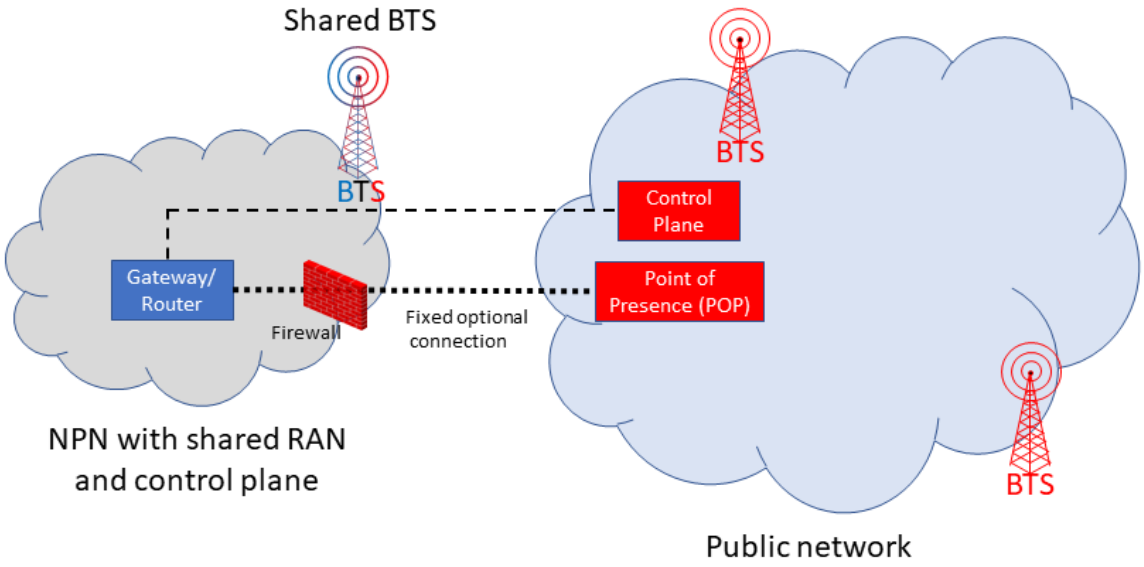


Figure 7: Deployment with shared RAN and control plan (adapted from: 5G-ACIA)

In the scenario for Variant 4 illustrated in Figure 8, the non-public network is realised in the public network. Since all control and user plane traffic is routed via the public network in this scenario, access to public network services and the ability to roam can be implemented easily in accordance with the agreement between the NPN owner on the one hand and the public network operator on the other. The optional connection between the NPN and the public network via the firewall is not needed in this scenario.

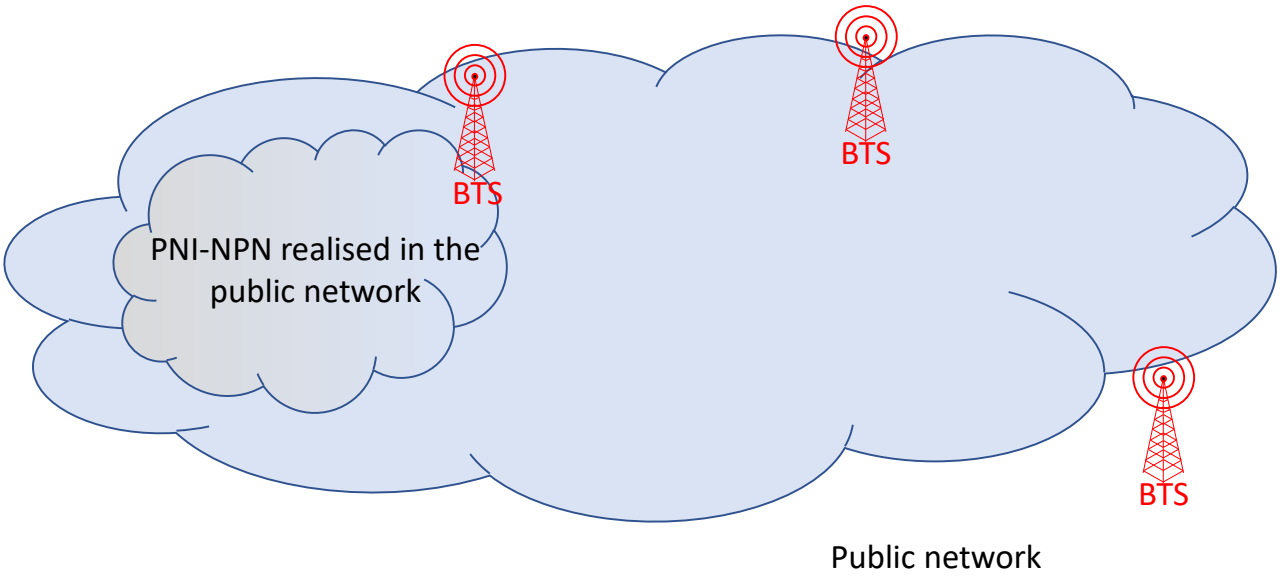


Figure 8: Deployment in public network (adapted from: 5G-ACIA)

4 3GPP STANDARDS CONCERNING THE USE OF THE PUBLIC NUMBERING RESOURCES FOR NON-PUBLIC NETWORKS

NPN architecture aspects were first introduced as from Release 16 of 3GPP, thus contextualising the term NPN within 5GS. Indeed, 3GPP (TS 23.501 [8]) states that "*a Non-Public Network (NPN) is a 5G System (5GS) deployed for non-public use*". For 3GPP TS 22.261 [3], NPN are intended for the sole use of a private entity such as an enterprise, and may be deployed in a variety of configurations.

An NPN is either:

- a SNPN, not relying on network functions provided by a PLMN, or
- a PNI-NPN, relying on network functions provided by a PLMN

The following description is based on the 3GPP specification (TS 23.501 [8]).

As already reported in Section 3, the variants can be grouped under the two categories: SNPN and PNI-NPN. SNPN contains two variants SNPN without sharing RAN (Section 3.1) and the SNPN with shared RAN (Section 3.2). PNI-NPN contains two variants (Section 3.3). A number of implementation options for these variants are also possible.

The solution 5G Multi-Operator Core Network (5G MOCN) supports the following sharing scenarios involving NPN, where Next Generation RAN (NG-RAN) can be shared by any combination of PLMNs, PNI-NPNs with Closed Access Group (CAG), and SNPNs (each identified by PLMN ID and Network identifier (NID)).

In a cell different configuration of NPN variants and PLMN can coexist.

SNPN 5GS deployments are based on a non-roaming architecture.

PNI-NPNs are NPNs made available via PLMNs e.g. by means of dedicated Data Network Names (DNNs)[8], or by one (or more) Network Slice instances allocated for the NPN. From a technical perspective, in order to access PNI-NPN, UE should avail of a subscription that can access the PLMN.

As network slicing does not enable the possibility to prevent UEs from trying to access the network in areas where the UE is not allowed to use the Network Slice allocated for the NPN, Closed Access Groups may optionally be used to apply access control.

The Broadcast System Information broadcasts a set of PLMN IDs and/or PLMN IDs and NIDs and one or more additional set of parameters per PLMN e.g. cell-ID, Tracking Areas, CAG Identifiers.

4.1 SNPN IDENTIFIER

A SNPN is identified by a combination of PLMN-Identifier (see 3GPP TS 23.003 "Numbering, addressing and identification", clause 12.1 [2]) and Network Identifier (NID) (see 3GPP TS 23.003 "Numbering, addressing and identification", clause 12.7 [2]).

The PLMN ID used for SNPNs is not required to be unique. 3GPP states that PLMN IDs reserved for use by private networks can be used for non-public networks, e.g. based on mobile country code (MCC) 999 defined by ITU-T Recommendation E.212 Amendment 1 [9]. Alternatively, a PLMN operator can use its own PLMN IDs for SNPN(s) along with NID(s), but registration in a PLMN and mobility between a PLMN and an SNPN are not supported using an SNPN subscription given that the SNPNs are not relying on network functions provided by the PLMN.

The NID shall consist of an assignment mode and an NID value as shown in Figure 9.

[8] A DNN is equivalent to an APN

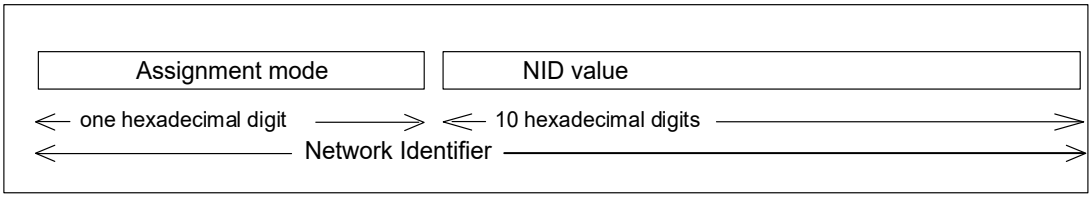


Figure 9: Network Identifier (NID) (Source: 3GPP TS 23.003 [2])

The NID can be assigned using the following assignment models:

- Self-assignment: NIDs are chosen individually by SNPNs at deployment time; this assignment model is encoded by setting the assignment mode to value 1;
- Coordinated assignment: NIDs are assigned using one of the following two options:
  - option 1: the NID assigned such that it is globally unique independent of the PLMN ID used. Option 1 of this assignment model is encoded by setting the assignment mode to value 0.
  - option 2: the NID assigned such that the combination of the NID and the PLMN ID is globally unique. Option 2 of this assignment model is encoded by setting the assignment mode to value 2.

Other Assignment mode values are reserved.

4.2 PNI-NPN IDENTIFIER

A Closed Access Group (CAG) identifies a group of subscribers who are permitted to access one or more CAG cells associated to the CAG. CAG is used for the PNI-NPNs to prevent UE(s), which are not allowed to access the NPN via the associated cell(s), from automatically selecting and accessing the associated CAG cell(s).

In a PNI-NP with CAG:

- A CAG is identified by a CAG Identifier which is unique within the scope of a PLMN ID;
- A CAG cell broadcasts one or multiple CAG Identifiers per PLMN;
- A CAG cell may in addition broadcast a human-readable network name per CAG Identifier.

The CAG-Identifier shall be a fixed length 32 bit value.

5 PRESENT IMPLEMENTATIONS

In this section, various technical solutions that allow the identification and/or the sharing of different networks are reported. The physical or logical separation of the networks could be used for facilitating the offering of NPNs.

5.1 CITIZENS BROADBAND RADIO SERVICE

The creation of a new publicly available transmission band in the 3.5 GHz frequency band was identified as a possibility by the US National Telecommunications and Information Administration (NTIA) for shared federal and non-federal use. This band was identified as the Citizens Broadband Radio Service (CBRS)[9] in a Notice of Proposed Rulemaking released by the FCC in December 2012 [10], which the FCC found would promote two major advances that enable more efficient use of radio spectrum: small cells and spectrum sharing.

The IMSI Oversight Council (IOC), a committee of the Alliance for Telecommunications Industry Solutions (ATIS), manages the IMSI resource in the United States and oversees the performance of the IMSI. With such broad and low-cost access to the shared licensed spectrum, concerns were raised that the demand for PLMN IDs from a significant number of smaller CBRS Spectrum users would place undue pressure on available resources. Therefore, ATIS derived a scheme [11] for allocating blocks of IMSIs for the CBRS Spectrum users in order to conserve the available E.212 resource. These guidelines address allocation of an Home Network Identifier (HNI) and IMSIs for systems that utilise IOC-approved Radio Technologies using the shared CBRS Spectrum.

5.1.1 Overview of CBRS Numbering Scheme

The MCC and MNC together provide the HNI or PLMN ID. In the CBRS scheme, the HNI identifies CBRS HNI in the CBRS range. The first four digits of the MSIN is called the IMSI Block Number (IBN) and the remaining five digits of the MSIN is the User Identification Number (UIN). The Shared HNI together with the operator-specific IBN then forms a globally unique identifier.

This CBRS scheme allows for 10000 Blocks of 100000 IMSIs to be allocated, thus making efficient use of this scarce numbering resource. All IBN assignments are available at the IMSI-A website; https://imsiadmin.com/cbrs-assignments. Figure 10 below provides an overview of the scheme.

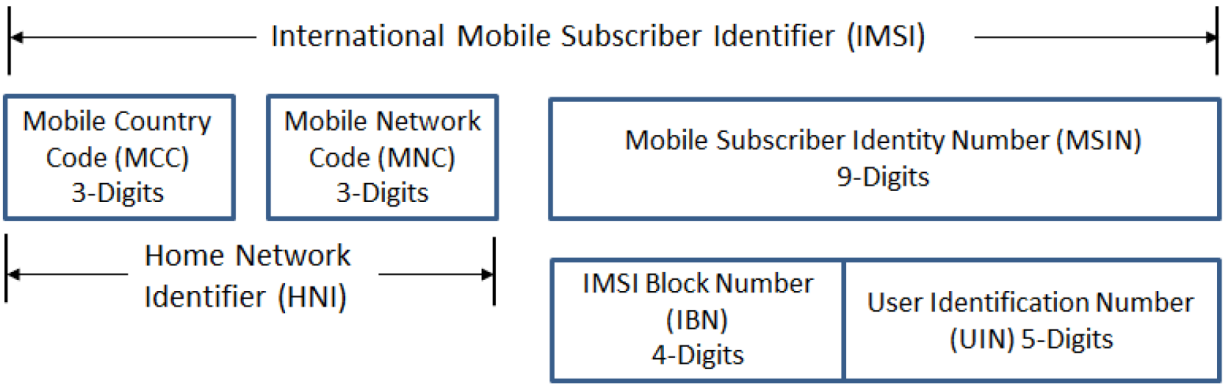


Figure 10: Overview of CBRS Numbering Scheme

The scheme [11] specifies assignment principles and criteria for the assignment of IBNs.

[9] https://ongoalliance.org/news/cbrs-alliance-rebrands-to-ongo-alliance-to-support-global-shared-spectrum-initiatives/

As applicants for IBNs may not qualify under the existing IMSI assignment guidelines, the scheme was established to allow the assignment of Shared HNI resources. Guidelines and procedures as set forth in the scheme remain in effect until there is either industry consensus or regulatory policy direction to change them.

The administration of the scheme is funded through application fees and an annual maintenance fee.

The CBRS Alliance coordinates the equipment and activities of manufacturers, operators and other participants in the CBRS and has developed technical specifications and guidelines specifically oriented to operations in the CBRS frequency range that are not addressed by 3GPP or other organisations.

In order to be able to uniquely identify the different service providers sharing an HNI, a new identifier referred to as CBRS Network ID (CBRS-NID) is introduced in "CBRS Alliance Identifier Guidelines for Shared HNI" [12]. This identifier is based on the LTE Closed Subscriber Group ID (CSG-ID) and consists of 27 bits. The CBRS-NID is broadcasted in the CSG-ID field to uniquely identify the shared HNI Network since the shared HNI that is also broadcasted is not sufficient to uniquely identify the network. An operator is provided with flexibility to decide whether to use one CBRS-NID for each CBRS network site, or to use one CBRS-NID across multiple sites. However, the CBRS Alliance points out that it would be beneficial for operators to use a separate CBRS-NID if ownership of a site (e.g. campus, mall, office building) can be transferred independently from other sites.

The first shared HNI consisting of a MCC 315 and a three-digits MNC 010 has been assigned by the US IMSI Administrator for shared use for all CBRS spectrum users implementing networks that require IMSI (e.g. LTE or 5G-NR). Additional shared HNIs may be assigned in the future [13].

The CBRS Alliance maintains a register of CBRS-NID codes[10] in order ensure that a code is only assigned to a single operator, thus achieving global uniqueness among operators using the CBRS Alliance CBRS-NID codes.

Furthermore, in order for CBRS LTE systems to be able to coordinate between themselves, two new identifiers are introduced - Tracking Area Code (TAC) and Tracking Area Identity (TAI). The TAC identifies the tracking area within a particular network and the PLMN ID and TAC combined makes up the globally unique TAI. The TAC has a range of 0 to 65536 which allows for many different logical networks to be identified that are sharing the PLMN ID. The TAIs/TACs are broadcasted over the air, as per the 3GPP specifications (36.331) [14] . The TAC is assigned by the operator, not the CBRS Alliance, and should be locally unique (i.e. not used by any other nearby network) [13]. In this respect, the CBRS Alliance recommends a method that takes into consideration the IBN to enable an operator to define six TAC codes that would produce TAI codes that would not conflict with any other network using the same method.

5.2 MULTEFIRE

MulteFire is a technology that enables private wireless networks by operating cellular-based technology standalone in unlicensed spectrum [15].

MulteFire 1.0 and 1.1 is an LTE-based technology that operates standalone in unlicensed spectrum, with a roadmap to solutions based on 5G New Radio (NR). By removing the requirement for licensed spectrum, MulteFire allows entities to deploy and operate their own private network, targeting areas such as Industrial Internet of Things (IIoT) or enterprises. MulteFire can also be configured as a neutral host network, e.g. for an enterprise or venues, to serve users from multiple operators.

The LTE-based MulteFire Release 1.0 specification was completed in January 2017 by the MulteFire Alliance. MulteFire Release 1.0 builds on 3GPP standards and is targeted for operation in the global 5 GHz unlicensed spectrum band. It implements Listen-Before-Talk (LBT) to efficiently coexist with other spectrum users in the same band, such as Wi-Fi or Licensed Assisted Access (LAA). MulteFire 1.0 enables the full range of LTE services including voice, high-speed mobile broadband (data), user mobility and security.

[10] Online ordering system in place: https://ongoalliance.org/ongo-identifiers/

The Release 1.1 specification, completed in December 2018, brings new optimizations especially for IoT, such as support for Narrowband - IoT (NB-IoT) and enhanced Machine-Type Communication (eMTC) in unlicensed spectrum

As with mobile networks, MulteFire enables full mobility as a user walks around a building and enables seamless handover between small cells as required. MulteFire will also interwork with public mobile networks to provide service continuity when users leave the area where MulteFire service is available.

Amendment 3 (December 2020) of Recommendation E.212 introduced Annex H on Criteria and procedures for the assignment and reclamation of shared ITU-T E.212 mobile country codes (MCC) for regional and other international organizations (ROIO)/standards development organization (SDO)-specified networks and their respective mobile network codes (MNCs)

MulteFire Alliance (MFA) applied for a shared E.212 resource on 18 November 2020. TSB assigned the E.212 MNC 01 under MCC 902 to MFA as for ROIO/SDO-specified networks shared code.

The request is accompanied with the following information on the use:

- the service intended to be provided with the MCC-MNC is Internet access: it is “functionally similar” to a WiFi Internet access with a few possible benefits (bandwidth, robustness etc.);
- no voice/telephony service would be provided on such access;
- the justification of the application for a global MCC-MNC is that it avoids the IMSI issuer and manufacturers to apply for an MNC in every/any country.

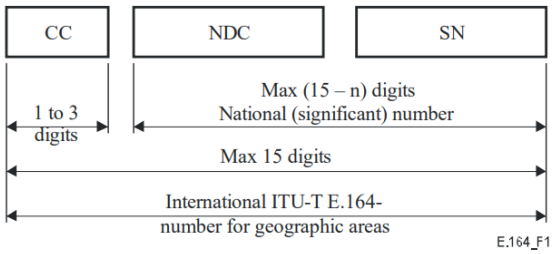
In the request, it is also specified that one typical resource delegation model may be as follows:

- a global MCC-MNC would be assigned to MFA;
- any vendor implementing an MFA specification would use the MCC-MNC for its equipment;
- An entity (e.g. a football stadium owner) buys such equipment for their premises in country X and may issue licenses to Internet access providers or resellers who would be issuing IMSIs under that MCC-MNC to provide such services in that area;
- That service provider may have a contract with the owner of the equipment (not the vendor), and none with the assignee of the MCC-MNC.

6 DRIVERS AND ASPECTS OF THE NEED TO USE PUBLIC NUMBERING RESOURCES FOR NON-PUBLIC NETWORKS

6.1 PUBLIC E.164 RESOURCES FOR USE IN NPN

Recommendation ITU-T E.164 [16] (The international public telecommunication numbering plan) defines the structure of E.164-numbers as follows:



CC Country Code for geographic area
NDC National Destination Code
SN Subscriber Number
n Number of digits in the country code

NOTE – National and international prefixes are not part of the international ITU-T E.164-number for geographic areas.

Figure 11: International ITU-T E.164-number structure for geographic areas

The number consists of:

- Country Code (CC) of the country in which the UE is registered, followed by:
- National (significant) number, which consists of:
  - National Destination Code (NDC);
  - Subscriber Number (SN).

Generally, NRAs only assign E.164 numbering blocks to service providers intending to offer a publicly available (number-based) ECS. Given that NPNs do not necessarily offer a publicly available ECS, some NRAs may consider such NPNs ineligible for an assignment of E.164 numbers. Nevertheless, the continued application of such policies may need to be reviewed as business models around NPNs evolve.

The Mobile Station Roaming Number (MSRN) is used to route calls to a mobile terminal. On request, MSRN is temporarily associated to a mobile terminal by the VLR where the terminal is registered. The MSRN is used to route calls to the UE, in case of roaming. MSRNs are not used for subscriber dialling.

MSRNs have the same structure as international E.164 numbers in the area in which the terminal is in roaming, i.e.:

- the country code of the visited country;
- the national destination code of the visited PLMN or numbering area;
- a subscriber number with the appropriate structure for that numbering area.

In case of PNI-NPN, NPAs should consider the assignment of E.164 numbering resources to be used for deriving MSRN to support roaming.

Whether NPNs require E.164 numbering resources depends, for example, on how UEs are addressed within the NPNs. For example, TETRA networks use an internal numbering and addressing scheme and do not require E.164 numbering resources for internal communications. Some 5G-UEs have capabilities to use PLMN radio technology while using a proprietary addressing scheme (i.e. no E.164 numbers needed) for internal communications.

If NPNs are interconnected with public networks for voice or SMS services, they are likely to need public E.164 numbering resources in order to be able to call public network subscribers and to receive calls from public networks.

The demand for E.164 resources is expected to be from mobile and/or machine-to-machine number ranges. While it is difficult to estimate the likely increase in demand that could arise from NPNs, it is not expected to be significant. However, NPAs should monitor and be alert to any 'demand shocks' and this context could be taken into account by NPAs to determine whether or not (and how) national E.164 numbering resources are to be assigned to NPNs.

6.2 PUBLIC E.212 RESOURCES FOR USE IN NPN

ITU-T Recommendation E.212 [17] defines the structure of the International Mobile Subscription Identity (IMSI), which is primarily used by Mobile Network Operators (MNOs) to identify individual subscriptions on mobile networks. Every SIM card in every mobile device in the world is programmed with a unique IMSI number of 15 digits in length. The first 3 digits identify the subscriber's home country. This is called the Mobile Country Code (MCC). The next 2 or 3 digits identify the subscriber's home network. This is called the Mobile Network Code (MNC) and is configured in most countries with only 2 digits. The remaining 9 or 10 digits make up the Mobile Subscription Identification Number (MSIN) which is used to identify individual subscribers.

The MCC and MNC together make up the Home Network Identifier (HNI) also referred to as the Public Land Mobile Network Identifier (PLMN ID). The PLMN ID is broadcast by the network's base stations so that eligible devices can pick up the signal and attach to the network.

The IMSI structure and format is illustrated in Figure 12:

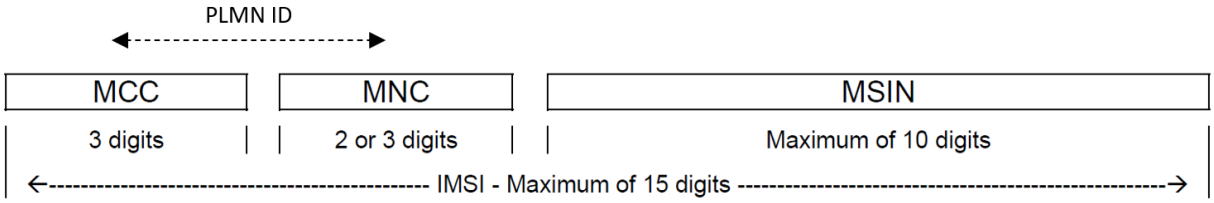


Figure 12: The IMSI structure and format

The IMSI is an integral identifier used in mobile networks. The E.212 concept was developed at a time when MNOs were the only stakeholders in the mobile value chain with a justifiable need for MNC resources to facilitate authentication, roaming, billing and routing. However, the use of E.212 resources has evolved over time. ECC Report 212 [18] provides a comprehensive overview on the evolution in the use of E.212 Mobile Networks Codes.

In NPN, terminals with dual-SIM UEs (MUSIM) may also be used. In these cases, there will be at least two IMSIs - one for the NPN and one for the public network. The public network IMSI/SIM will use the public network operator's E.212 numbering resources, while the NPN IMSI/SIM may use either MNC under MCC 999 or a national MCC + MNC. In the case of NPNs Variant 1 or 2 (see clause 3.1 and 3.2), when the MCC used is not 999, it could either be a shared MNC under geographic MCC or the MCC + MNC of an existing MNO. For NPNs Variant 3 or 4 (see clause 3.3), the MCC + MNC would be the same as that used for the public network. Given the variety of options available to NPNs in terms of MCC+MNC that can be availed of, NPAs should evaluate to what extent, and how, to allow the use of national MNCs under their respective national MCC. In the case of SNPN, MCC 999 could also be used.

Table 1 displays the E.212 numbering resources that are technically possible for the different types of NPN.

Table 1: E.212 numbering resources that are technically possible for the different types of NPN

Variant	Type of NPN	E.212 numbering resources
1	SNPN	global MCC (e.g. 999, 901, 902) or geographic MCC[11]
2	SNPN with shared RAN	global MCC (e.g. 999, 901, 902) or geographic MCC[12]
3	PNI-NPN with shared RAN and shared control plane	geographic MCC or global MCC (excl. 999)
4	PNI-NPN realised in the public network	geographic MCC or global MCC (excl. 999)

6.2.1 Assignment of E.212 resources

The ITU assigns MCCs to countries (usually one MCC per country only), and the relevant national authorities subsequently assign MNCs to entities who meet the eligibility criteria. The ITU also assigns MNCs with 2 digits directly from a shared MCC (e.g. MCC 901 or 902) to entities who meet the eligibility criteria according to Annex A and Annex H in ITU-T Recommendation E.212.

In most countries in the world, the IMSI is implemented with a 2-digit rather than a 3-digit MNC configuration. This means that in most of the countries, only 100 MNCs (00-99) are available for assignment under each MCC. The MCC pool capacity is also limited with only 1000 MCCs (000-999) available for assignment by the ITU to countries or for designation as shared codes (e.g. MCCs 901 and 902). As MCCs and MNCs are a scarce resource, regulations or number assignment rules in most CEPT countries restrict the assignment of MNCs to MNOs only or MNOs and Mobile Virtual Network Operators (MVNOs) who meet certain specified criteria.

Should the assignment of national E.212 public resources be allowed for implementing NPNs, this will place further pressure on an already limited resource. Therefore, innovative ways of using and sharing E.212 resources could be considered to avoid exhaustion in the short to medium term.

ITU-T Recommendation E.212 Appendix III, as described in Amendment 1, introduces a "Shared ITU-T E.212 mobile country code (MCC) 999 for internal use within a private network". MCC 999 is allocated by the Recommendation for internal use within a private network. MNCs under this MCC are not subject to assignment and therefore may not be globally unique. Consequently, for using a MNC value under this MCC, no application to ITU is required. The Recommendation foresees that any MNC value under MCC 999 used in a network should have significance only within that network. Characteristics of this MCC/MNCs is that it is not routable between networks, and they shall not be used for roaming. MNCs under this MCC may be 2- or 3-digits long.

One of the issues in using the MCC 999 is that if two adjacent SNPNs use the same MNC values interferences are likely to occur, since terminals of one network may try to unsuccessfully connect to the adjacent SNPNs and as a consequence not be able to connect to their home network. The use of 3-digit MNC instead of 2-digit MNC may reduce the issue of conflicts/interferences since a greater number of alternative values is available. Another possible solution in order to prevent, or at least make such malfunctioning less likely, is for some level of industry coordination regarding the use of MNCs under MCC 999 to avoid local interference. However, since the use of MCC 999 is not dependent on an assignment by the ITU or NPAs, facilitating such coordination is unlikely to be within the competence of NPAs.

An alternative to the use of MCC 999 is that the NPA makes available one or more shared MNCs for SNPNs. Similar to MCC 999, MNCs would be used without assignment. The difference would be that the MNC would be from the geographic MCC of the country of use. However, the risk of local interference would remain unless some element of coordination was introduced.

[11] Assignment of geographic resources is within the discreation of NPAs

A further possibility to manage demand for MNCs could be that more networks, and in particular more NPNs, share the same MCC-MNC and are distinguished by using different parts of the MSIN. There are a variety of ways to achieve this, including facilitation by the NPA, or assignment to a lead provider or a third party who would then facilitate use by different NPNs. For instance, a geographic MCC-MNC could be assigned for a specific type of industry use (e.g. utilities) and sub-assignments made by the assignee for different NPN use within that industry using the MSIN to distinguish between NPNs.

In case of a significant increase of requests for E.212 numbering resources, NPAs should also consider applying to the ITU for an additional geographic MCC. In such case, the NPA should evaluate the possibility of using the new MCC to provide 3-digit MNCs, thereby achieving a greater capacity for assignment to different networks. Currently, in Europe only MCCs with 2-digit MNCs are used and the ITU-T Recommendation states that the number of digits dedicated to a MNC under a geographical MCC could be 2 or 3-digit. From 3GPP point of view, it is not recommended to have MNCs with different digit lengths under the same MCC[12]. However, having a new MCC would allow for the assignment of 3-digit MNCs. In the case where a new MCC is needed, a coordinated approach in CEPT countries should be considered.

6.3 PUBLIC E.118 RESOURCES FOR USE IN NPN

ITU-T Recommendation E.118 [19] concerns "The international telecommunication charge card" and defines Primary Account Numbers (PANs) in accordance with ISO/IEC 7812-1 [20], that is the ISO/IEC standards for payment cards (i.e. credit cards, debit cards, …).

ETSI Telecommunication Standard (ETS) 300 608 [21] specifies the use of PAN in the SIM cards, calling such numbering resources Integrated Circuit(s) Card Identification (ICCID). ICCID is also known as the serial number of the SIM card.

By the definition of the ITU-T recommendation, E.118 numbering resources are those resources that identify the SIM cards as charge cards. PAN/ICCID is stored inside the SIM card and stamped on it.

The maximum length of the PAN/ICCID is 19 digits and is composed of the following subparts (see Figure 13):

- Issuer Identification Number – variable number of digits (maximum 7) and it is composed by:
  - Major Industry Identifier (MII) “89”, assigned for telecommunication purposes in accordance with ISO/IEC 7812-1 [20];
  - Country Code – variable from 1 to 3 digits in accordance with ITU-T Recommendation E.164[16];
  - Issuer Identifier Number (IIN) – variable number of digits, but fixed number of digits within a country or world zone where appropriate;
- Individual account identification number – variable number of digits, but fixed number for each particular issuer identification number;
- Parity check digit computed according to the Luhn formula (see ISO/IEC 7812-1, Annex B [20]).

[12] See section 2.2 3GPP TS 23.003 [2].

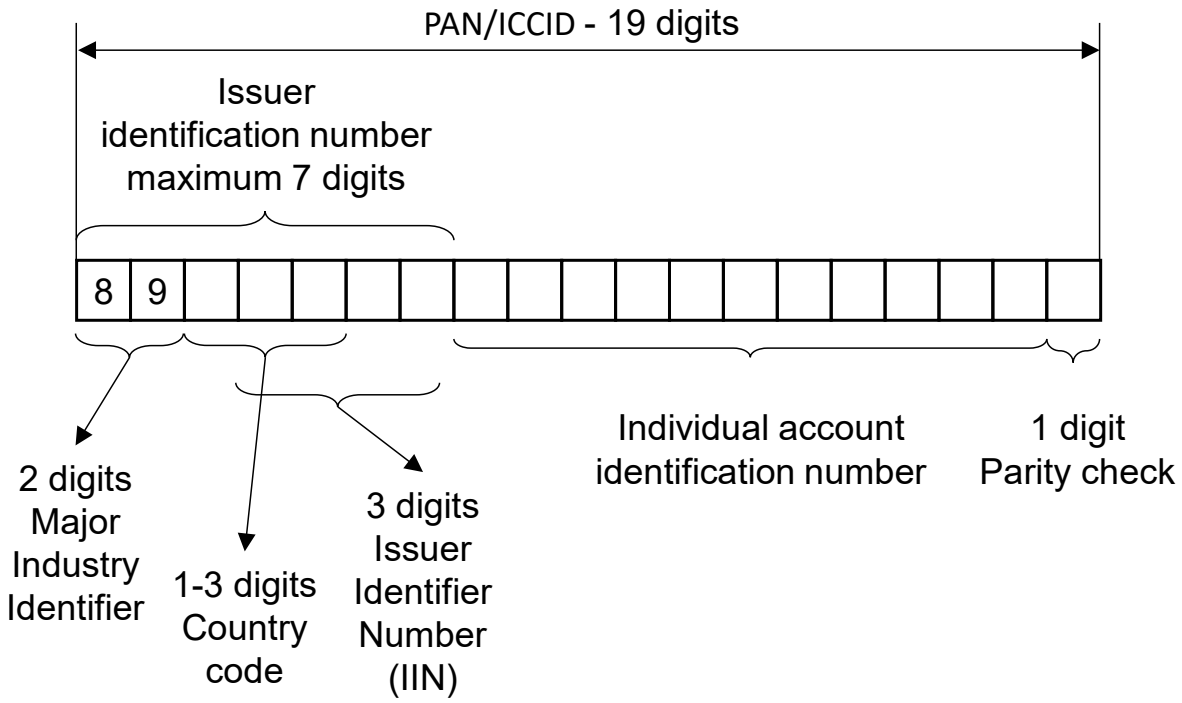


Figure 13: PAN/ICCID numbering structure

For the embedded SIM (eSIM), GSMA [23] foresees that ICCID (i.e. E.118 numbering resources) is used as identifier of the single profile stored in the eSIM, since an eSIM may contain more than one profile even if only one can be active at a time.

This implies that also in case of SNPNs (where serial number may not be necessary for charging), E.118 numbering resources may be used to distinguish the possible different profiles present in an eSIM.

It is noted that use of E.118 resources for NPNs may lead to scarcity issues. In CEPT countries, the number of digits for IINs is always equal to two and consequently the maximum number of assignees is 100.

While ITU-T Recommendation E.212 Amendment 1 Appendix III introduces a "Shared ITU-T E.212 mobile country code (MCC) 999 for internal use within a private network" [9], no similar numbers have been defined in ITU-T Recommendation E.118 numbering resources. A technical possible alternative could be that ITU introduces an E.164 Country Code that has the meaning of "private" or "non-public" network.

Moreover, while in ITU-T Recommendation E.212 globally usable resources have been defined and assignment criteria adopted by TSB are included in Annex A of the ITU-T Recommendation E.212, no similar numbers have been defined in ITU-T Recommendation E.118 numbering resources[13].

[13] ITU-T Recommendation E.118 is currently under revision notwithstanding that some E.118 numering resources were already assigned with some present global E.164 country code.

7 CONCLUSIONS

We have studied the emergence of NPNs in a mobile environment and looked at their need to use public numbering resources. The Report found that, in general, NPNs are used to provide services to enterprises and they are not used for providing services to the general public, and proceeded to present various business models and network topologies that can more readily be termed as 'non-public networks', principally on the strength of two factors, namely (a) the limited, if any, interface with the 'general public' for the ECS being transmitted, and (b) the distinct or reduced requirements and usage of publicly assigned resources, in particular E.164, E.212 and E.118 numbering resources.

We have identified the following important elements in relation to NPNs:

- A NPN may be realised using part, or sharing components/part of the network elements of a public electronic communications network;
- NPNs need to be identifiable to ensure that the right user equipment connects;
- NPNs may need to be able to interconnect/roam with public networks.

Given these elements, it is concluded that there are justified cases where NPAs could allow the use of national public numbering resources in NPNs. The following is provided to NPAs to serve as potential guidance on the management of public numbering resources for NPNs:

7.1 E.164 NUMBERING RESOURCE

It was found that some NRAs may consider NPNs ineligible for an assignment of E.164 numbers, since NPNs do not necessarily offer a publicly available ECS, however, the continued application of such policies may need to be reviewed as business models around NPNs evolve. NPNs are likely to need public E.164 numbering resources if interconnected with public networks for voice or SMS services. Moreover, in case of PNI-NPN, NPAs should consider the assignment of E.164 numbering resources to be used for deriving MSRN to support roaming.

Although the demand for E.164 numbering resources is expected to be from mobile and/or machine-to-machine number ranges, the growth and increased interest in NPNs from various entities may require that NPAs review their national numbering regulations and policies, including in relation to any specific rules or definitions that might prohibit and/or discourage NPN use.

7.2 E.212 NUMBERING RESOURCE

The use of E.212 numbering resources is crucial for mobile NPNs, and NPAs should determine what would be permitted use by NPNs, for both SNPN and for PNI-NPN.

NPAs should be alert to the level of demand for MNCs under their respective MCC that could arise from NPNs and consider the following measures to increase efficient use and/or increase supply:

- Encourage the use of MCC 999, where appropriate (e.g. for SNPN). In order to manage potential interference issues, the use of MCC 999 with 3-digit MNCs should be considered. Also, some level of coordination may be required and NPAs may consider encouraging industry stakeholders to lead on this initiative;
- Allocate one or more MNCs from the geographic MCC for shared use without direct assignment for SNPN and/or mobile private networks;
- Assign MNCs for use by multiple networks, and in particular multiple NPNs. There would need to be a method for having more SNPNs with the same MCC+MNC, such as allowing the use of parts of the MSIN to distinguish between different SNPNs. There are a variety of ways to achieve this, including facilitation by the NPA, or assignment to a lead provider or a third party who would then facilitate use by different NPNs;
- Evaluate the need to seek the allocation of an additional geographical MCC from the ITU. The new MCC could be used with 3-digit MNCs, thus providing 1000 rather than 100 MNCs.

7.3 E.118 NUMBERING RESOURCE

The use of E.118 numbering resources is similarly applicable for mobile NPNs, regardless of whether traditional SIM cards or eSIMs are used in the UE. Thus, the use of E.118 resources by NPNs could be permitted by NPAs, who should determine applicable parameters. In this regard, NPAs should be alert to the level of demand for E.118 numbering resources that could result from their use for NPNs and the scarcity issues that could develop as a result. Moreover, it is unclear what E.164 country code should be associated to E.118 numbering resources when E.212 MCC 999 is used in NPNs. This aspect needs to be addressed by ITU-T SG2.

ANNEX 1: LIST OF REFERENCES

[1] Directive 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code (EECC)

[2] 3GPP TS 23.003: "Numbering, addressing and identification"

[3] 3GPP TS 22.261: "Service requirements for the 5G system"

[4] Recommendation ITU-R M.2083-0 (09/2015): "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond", September 2015

[5] ATIS-I-0000073: "Neutral Host Solutions for 5G Multi-Operator Deployments in Managed Spaces", July 2019

[6] 5G-ACIA: "5G Non-Public Networks for Industrial Scenarios", March 2019

[7] 3GPP TS 23.251: "Network sharing; Architecture and functional description"

[8] 3GPP TS 23.501: "System architecture for the 5G System (5GS)"

[9] Recommendation ITU-T E.212 Amendment 1: “New Appendix on shared E.212 Mobile Country Code (MCC) 999 for internal use within a private network”, July 2018

[10] Federal Communications Commission - FCC 12-148: "Amendment of the Commission’s Rules with Regard to Commercial Operations in the 3550-3650 MHz Band”, December 2012

[11] ATIS: “International Mobile Subscriber Identity (IMSI) - Assignment and Management Guidelines for Shared HNI for CBRS”, May 2018

[12] CBRS Alliance Identifier Guidelines for Shared HNI, November 2018

[13] CBRS Alliance Identifier Administration Guidelines for Shared HNI (CBRS-TR-0101), January 2019

[14] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification"

[15] MulteFire - "MulteFire Release 1.1 Technical Overview White Paper", December 2018

[16] Recommendation ITU-T E.164: “The international public telecommunication numbering plan”, November 2010

[17] Recommendation ITU-T E.212: “The international identification plan for public networks and subscriptions”, September 2016

[18] ECC Report 212: "Evolution in the use of E.212 Mobile Network Codes", approved April 2014

[19] Recommendation ITU-T E.118: “The international telecommunication charge card”, May 2006

[20] ISO/IEC 7812-1:2017: “Identification cards – Identification of issuers – Part 1: Numbering system”

[21] ETS 300 608: “Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface” (GSM 11.11 version 4.18.3), August 1997

[22] SGP.01: “Embedded SIM Remote Provisioning Architecture”, February 2019

[23] GSMA: "5G industry campus network deployment guideline", November 2020