Author
Edbom, Göran
Phone
+46 10 505 24 46
Mobile
+46 72 204 11 71
E-mail
goran.edbom@afry.com
Date
13/11/2023

Efficient Administration of Swedish E.212 MNCs and Related Demands

EXECUTIVE SUMMARY

The target of this study is an effective and simple management of Swedish E.212 MNC (Mobile Network Code) resources for public and private electronic communications networks. The study has been carried out on behalf of the Swedish Post and Telecom Authority (PTS). The study is based on comprehensive consultations with some significant market participants and European NRAs/NPAs.

At one hand the current drivers for future MNC demands are addressed. It is found that Standalone Non Public Networks (SNPNs) is the main consideration in this context. Neutral Host Networks (NHNs) is another area of high attention. However, it is found that NHNs will not drive any considerable MNC demands.

At the other hand a number of technical aspects are addressed as to achieve as effective MNC utilization as possible.

For SNPNs the main target is to limit the assignments of own unique MNCs. The main ambition is then to see to that shared/un-coordinated MNCs will be utilized as much as possible. The study concludes that the global Mobile Country Code (MCC) 999 is the most promising path in this perspective. MCC 999 implies that SNPN owner can pick any of the 1,000 MNCs at hand. Since nearby SNPNs should not apply the same MCC and MNC, MCC 999 allows for a simple handling to avoid "MNC interference". This contrasts with the allocated Swedish MNCs 65 & 66 which are only two. Further, MCC 999 is supported by Apple iOS today, whereas this is not the case for the Swedish ones. They may be supported future wise but all in all, MCC 999 is preferred as outlined above.

SNPNs will be applied for many purposes onwards. The industrial usage is extended to include personal devices as smart phones and tablets in addition to dedicated (I)IoT devices. This is exemplified by the fact that Apple is now officially entering the SNPN market with specific SNPN features as outlined in the study. Further, there are new SNPN concepts to be achieved in the upcoming years. The 3GPP SNPN roadmap is then analysed, addressing Network ID (5GC-NID), Credentials Holder, Onboarding and Localized Services.

A key achievement is to uniquely identify SNPNs despite that they have the same PLMN ID (MCC + MNC). By introducing a Network ID denoted as 5GC-NID, unique SNPN IDs can be accomplished by the combination of PLMN ID + 5GC-NID. There are 3 options on how to generate the 5GC-NID. By adopting the approach that SNPNs should apply IANA PENs for which the 5GC-NID is unique in itself, a very simple MNC administration will be achieved. The SNPN owners will then handle 5GC-NIDs completely by themselves.

Shared MNCs which implies that a specific MNC is divided into "sub-networks" has been in focus in recent years. The approach has been adopted by e.g. Germany, Norway, CBRS (US) and MulteFire Alliance (under global MCC 902) and has also been considered by PTS in the past. Shared MNCs then implies that there is a central body to administer the sharing of the MNC. Since un-coordinated MNC approach for MCC 999 combined with 5GC-NID scales very well (number of 5GC-NIDs is "endless") and no central administration is required, shared MNCs are ruled out.

It is expected that 5GC-NID will be general available in mobile systems and UEs in 2025. The 5GC-NID will only be applicable for 5G and not for 4G/LTE. There are some other 4G considerations addressed in the report yielding that it will take some years until 4G is phased out and SNPNs are uniquely identified by 5GC-NID. In the meantime, MNC interference shall be avoided. As outlined, MCC 999 is then very appealing.

There is a rising interest for SNPN roaming. However, 3GPP has not standardized any support for SNPN ID roaming. There are some "roaming substitutes" included in the 3GPP SNPN roadmap, pre-dominantly Credentials Holder which allow for 3rd party authentication using the home network credentials. Only authentication support is then accomplished and there are also some other considerations. Thus, it is proposed that PTS should address 3GPP, via ITU-T SG2 and CEPT WG Nan Liaison Statements, to define SNPN ID roaming support.

In any event, it will take time to achieve the roaming solutions above. Thus, some near term solutions will have to sought. A new role, already on the market, has been presented by Ericsson as direct input to the study. Major M(V)NOs with many roaming agreements in place, offer a solution for international roaming to the SNPNs. The SNPNs will then use a specific part of the M(V)NO IMSI range, as for shared MNC networks. These will not require any Swedish MNCs as the M(V)NOs will not use the Swedish MCC, However, there might be similar upcoming approaches for the Swedish market. The MNC demand will be very limited as this only requires one MNC per M(V)NO. This approach should be promoted as it limits the need for new MNCs.

There is then the ultimate question on how to increase the total number of MNCs. Sweden has as many other countries applied 2-digit MNCs. There has been a thinking for more than 10 years that it should be possible to introduce 3-digit MNCs as well. Thus, there would be a mix of a 2- and 3-digit MNCs. The obstacle is that 3GPP in the TS 23.003 specification states that a mix is not recommended. This has hindered many countries to take such a step. However, India and France have applied a mix without any reported problems. The study has analyzed the e2e 3GPP handling and concludes that 2- and 3-digit MNCs are clearly separated all the way.

Thus, a 2- and 3-digit mix shall be applicable. The condition is that the respective series shall not be overlapping. This was already stated by T-Mobile NL in 2012 and is still their opinion. As PTS has not assigned any MNCs for the 7x, 8x and 9x series, they are promoted to introduce 3-digit MNCs for these series. The number of MNCs will then increase ten times, from 30 to 300.

In the light of these conclusions, PTS are urged to push 3GPP, via ITU-T and CEPT WG NaN Liaison Statements, to remove the statements in their specifications that a mix is "not recommended".

There will be a significant evolution around NPNs and NHNs in the upcoming years, involving a number of new market players. In addition, there is a need to coordinate the SNPN MNCs and to communicate the adoption of 5GC-NID. PTS is then proposed to facilitate the establishment of a new Swedish NPN/NHN Forum.

Sammanfattning

Målet med denna studie är en effektiv och enkel hantering av svenska E.212 MNC (Mobile Network Code) resurser för allmänna och privata elektroniska kommunikationsnät. Studien har genomförts på uppdrag av Post- och telestyrelsen (PTS). Studien bygger på omfattande samråd med några betydande marknadsaktörer och europeiska nationella reglerings- och tillstånds-myndigheter.

Å ena sidan behandlas de nuvarande drivkrafterna för framtida behov av MNC:er. Det har visat sig att fristående privata/ icke-publika nät (SNPN) är den viktigaste drivkraften i detta sammanhang. Neutrala nät (NHN) är ett annat område med stor uppmärksamhet. Det har dock visat sig att NHN inte kommer att driva några betydande MNC behov.

Å andra sidan behandlas ett antal tekniska aspekter för att uppnå ett så effektivt MNC-utnyttjande som möjligt.

För SNPN är huvudmålet att begränsa tilldelningen av egna unika MNC. Den främsta ambitionen är då att se till att gemensamma/okoordinerade MNC används i så stor utsträckning som möjligt. Studiens slutsats är att den globala mobila landskoden MCC 999 är den mest lovande vägen i detta perspektiv. MCC 999 innebär att SNPN-ägaren kan välja vilken som helst av de 1 000 MNC:er som finns till hands. Eftersom närliggande SNPN:er inte bör tillämpa samma MCC och MNC, tillåter MCC 999 en enkel hantering för att undvika "MNC-störningar". Detta står i kontrast till de allokerade svenska MNC:erna 65 och 66 som bara är två. Dessutom stöds MCC 999 av Apple iOS idag, medan detta inte är fallet för de svenska MNC:erna. De kan komma att stödjas framtidsmässigt, men sammantaget är MCC 999 att föredra enligt beskrivningen ovan.

SNPN kommer att användas för många ändamål framöver. Den industriella användningen utvidgas till att omfatta personliga enheter som smarta telefoner och surfplattor utöver dedikerade (I)IoT-enheter. Detta exemplifieras av det faktum att Apple nu officiellt går in på SNPN-marknaden med specifika SNPN-funktioner som beskrivs i studien. Dessutom finns det nya SNPN-koncept som ska erbjudas under de kommande åren. 3GPP SNPN-färdplanen analyseras avseende nät-ID (5GC-NID), ”Credentials Holder”, ”Onboarding” och lokaliserade tjänster.

En viktig förutsättning är att unikt kunna identifiera SNPN:er trots att de har samma PLMN-ID (MCC + MNC). Genom att introducera ett nät-ID betecknat som 5GC-NID kan unikt SNPN-ID åstadkommas genom kombinationen av PLMN-ID + 5GC-NID. Det finns tre alternativ för hur man kan generera 5GC-NID. Genom att anta tillvägagångssättet att tillämpa IANA PEN för vilka 5GC-NID är unikt i sig, kommer en mycket enkel MNC-administration att uppnås. SNPN-ägarna kommer då att kunna hantera 5GC-NIDs helt själva.

Delade MNC, vilket innebär att en specifik MNC är uppdelad i "subnät", har varit i fokus de senaste åren. Metoden har antagits av bl.a. Tyskland, Norge, CBRS (USA) och MulteFire Alliance (under global MCC 902) och har även övervägts av PTS tidigare. Delade MNC innebär att det måste finns en central administration för tilldelningen av subnät. En okoordinerad MNC inriktning för MCC 999 i kombination med 5GC-NID skalar mycket bra (antalet 5GC-NID är "oändligt"). Ingen central administration krävs ej heller. Detta medför att det delade MNC avskrivs som alternativ.

Det förväntas att 5GC-NID kommer att vara allmänt tillgängligt i mobila system och enheter under år 2025. 5GC-NID kommer endast att vara tillämpligt för 5G och inte för 4G/LTE. Det finns några andra 4G-överväganden som tas upp i rapporten som innebär att det kommer att ta några år innan 4G fasas ut och SNPN kan identifieras unikt med 5GC-NID. Under tiden måste MNC-störningar undvikas. Som beskrivits är då MCC 999 mycket tilltalande.

Det finns ett ökande intresse för SNPN-roaming. 3GPP har dock inte standardiserat något stöd för SNPN ID-roaming. Det finns några "roaming-substitut" som ingår i 3GPP SNPN-färdplanen, främst Credentials Holder som möjliggör tredje parts autentisering med hjälp av hemmanätets autentiseringsuppgifter. Endast autentiseringsstöd åstadkoms då och det finns även några andra överväganden. Det föreslås därför att PTS adressera 3GPP via ITU-T SG2 och CEPT WG Nan ”Liaison Statements”, för att definiera stöd för SNPN ID-roaming.

I vilket fall som helst kommer det att ta tid att uppnå de roaming-lösningar som anges ovan. Därför måste man söka andra lösningar på kort sikt. En ny roll, som redan finns på marknaden, har presenterats av Ericsson som direkt input till studien. Stora M(V)NO:er med många roaming-avtal erbjuder SNPN:er internationell roaming. Ett SNPN använder då en specifik del av M(V)NO IMSI-serien, som för delade MNC-nät. Dessa kommer inte att kräva några svenska MNC eftersom de internationella M(V)NO:erna inte kommer att använda den svenska MCC:n. Liknande lösningar kan komma att erbjudas för den svenska marknaden. Efterfrågan på MNC kommer att vara mycket begränsad eftersom detta endast kräver en MNC per M(V)NO. Detta tillvägagångssätt bör främjas eftersom det begränsar behovet av nya MNC.

Sedan återstår den slutliga frågan om hur man ska öka det totala antalet MNC:er. Sverige har som många andra länder tillämpat 2-siffriga MNC. Det har funnits en tanke i mer än 10 år att det borde vara möjligt att införa 3-siffriga MNC:er också. Således skulle det finnas en blandning av 2- och 3-siffriga MNC:er. Hindret är att 3GPP i TS 23.003-specifikationen anger att en blandning inte rekommenderas. Detta har hindrat många länder från att ta ett sådant steg. Indien och Frankrike har dock tillämpat en blandning utan några rapporterade problem. Studien har analyserat 3GPP-hanteringen e2e och kommit fram till att 2- och 3-siffriga MNC är tydligt separerade hela vägen.

En blandning av 2- och 3-siffriga siffror kan därför tillämpas. Villkoret är att respektive serie inte överlappar varandra. Detta konstaterades redan 2012 av T-Mobile NL och är fortfarande deras åsikt. Eftersom PTS inte har tilldelat några MNC:er för 7x-, 8x- och 9x-serierna uppmanas de att införa 3-siffriga MNC för dessa serier. Antalet MNC kommer då att tiodubblas, från 30 till 300.

Mot bakgrund av dessa slutsatser uppmanas PTS att driva på 3GPP, via ITU-T och CEPT WG NaN ”Liaison Statements”, för att 3GPP ska ta bort de hindrande skrivningarna i sina specifikationer om att en blandning ”inte rekommenderas”.

Det kommer att ske en betydande utveckling kring NPN och NHN under de kommande åren, med ett antal nya marknadsaktörer. Dessutom finns det ett behov av att samordna SNPN MNC:er och att informera om tillämpningen av 5GC-NID. PTS föreslås då understödja bildandet av ett nytt svenskt NPN/NHN-forum.

ACKNOWLEDGEMENTS

There are many people who has been involved in this study as to provide valuable information to the study e.g. by responding to the questionnaires.
A great thank you to you all!

There are three persons who have been critical for the outcome of the study:

Mickael Lauritsen, Head of Radio at Allicon / Corporate Fiber, former at Nokia, is very experienced in mobile technology and particularly NPNs and Neutral Host Networks for the Swedish market. His engagement and eagerness to share his knowledge and experiences has been invaluable for this report.

Rainer Liebhart, has 30 years of experience in the telecommunication industry. He has been working at Nokia with mobile development and standardization for more than 15 years. He is (co-)author of around 100 patents in the telecommunication area, of several IEEE papers, and co-editor of the books LTE for Public Safety and 5G for the Connected World. Rainer´s insights into mobile technology and 3GPP standardization combined with his eagerness to contribute has been of outmost value in writing this report.

Erik Hedin, has been working for Ericsson in different roles for more than 15 years. He currently holds a position as "Head of Networks and Managed Services Pre-sales Northern and Central Europe. Erik coordinated the Ericsson contributions to this report which involved a lot of efforts to engage various Ericsson experts. A special thanks to these experts to taking their time to contribute.

Table of Contents

1 Background and Scope

1.1 Background

This study has been ordered by Post- och Telestyrelsen (PTS), the Swedish National Regulator Authority. PTS is the Numbering Plan Administrator (NPA) for e.g. E.212 MNCs and provided the following background in Swedish to the study (the English translation is done by AFRY).

E.212 MNCs (mobile network codes) are a very limited numbering resource and are primarily intended to be used as a public numbering resource for different operator types in public electronic communications networks. When the ITU-T recommendation was originally created, in the early days of mobile telephony, there was no need for public numbering resources for private networks – see more in CEPT ECC Report 212 [30]. Sweden's current plan for E.212 MNCs can be found in [1].

A recent global trend has been towards frequency assignments for private networks based on 4G and 5G systems. In autumn 2021, PTS chose to enable the allocation of frequencies for such private networks, called local licenses [3]. This affects the management of the E.212 public resource as in some cases it may be needed for private networks. Sweden, like the majority of the world's countries, has chosen to apply 2-digit MNCs under MCC 240, which limits the number of available MNCs to 100 per MCC. Such decisions to apply 2-digit MNCs, instead of 3-digit MNCs, were taken when only a few network-owning traditional mobile operators were expected to exist in each country.

In 2022, CEPT published a report, ECC Report 337 [31], on how countries should be able to manage the E.212 resource based on the development of private networks. At the global level, ITU-T in 2018 allocated a special mobile country code, MCC 999, intended for the use of private networks. In addition, PTS in 2013 allocated MNC 65 and 66 under the Swedish MCC 240 for un-coordinated use of closed/private networks. Both initiatives have been made to allow private networks to use an MNC, which is needed for the terminal's connection to the private network, thereby limiting the need for their own public MNC for a private network. However, it has become apparent that it is not always in line with the needs of the various new entrants.

The standardization organization 3GPP, have chosen to call the concept around private networks Non-Public Network (NPN), which was introduced in 3GPP Release 15. The industry organization GSMA has produced a White Paper [15], that gives its view on NPN, which GSMA calls the 5G industry campus network.

When it comes to operators that in some way provide public networks and public services, new types of actors have emerged, which are not classic mobile operators with their own radio access networks, such as MVNO, MVNE, SMS providers, etc. who also considered themselves in need of their own E.212 MNC. Annex 1 to the CEPT recommendation [32] gives some examples.

Since the majority of the world's countries assign MNCs in two-digit format and that 3GPP in its technical specification TS 23.003 does not recommend mixing 2- and 3-digit MNCs under one and the same MCC, PTS previously investigated the possibility of still trying to mix 2- and 3-digit MNCs below Sweden's MCC 240 for certain current applications. The study for PTS was conducted in 2014 by

Cybercom Group and did not lead to any direct change on PTS's part, except that MNC 70-99 was reserved for future needs. The idea with this was to possibly be able to make these 3-digit MNCs for certain applications – mainly for SMS providers and shared proxy use through so-called "HLR Proxy Providers".

PTS had included the idea of converting MNC 70-99 to 3-digit MNCs in its referral to market participants on 15 November 2021 [4]. In the referral, PTS asked, among other things, whether the referral bodies consider that it would pose any problems to mix 2- and 3-digit MNCs below MCC 240 for the different purposes, i.e. traditional allocation of 2-digit MNCs for operators/providers and 3-digit MNCs for private networks. From those who answered the question, there was some hesitation about mixing 2- and 3-digit MNCs in such a way.

In this referral, PTS also examined another alternative for economizing on MNC resources. That option involved allocating MNC 90 for shared use for private networks where the MSIN series is divided into two parts, one part pointing out the private network and the other part being used to identify end users within the private network.

However, PTS chose, based on the analysis of the consultation responses, not to proceed with any of the alternatives in the referral. The route currently applied by PTS is that described in PTS's guideline for applying for permission to use mobile network codes for private networks [2].

1.2 Scope

The translated heading of the call for tender from PTS is:
"Call-off request for study on efficient management and use, as well as an overall needs picture with appropriate solutions, of E.212 MNCs for current and future different applications for public and private electronic communications networks."

This wide scope was narrowed down, with a target that the conclusions could be organized as:

- How can the needs of own E.212 MNCs, primarily for private networks, be quantified. This is conditional to other alternatives linked to MNO MNC being available. The reasoning will be supported by describing the different general needs that exist for own E.212 MNCs and breaking them down.
- How can an effective assignment/use and management be made to meet these needs:
    - Is it technically possible that two-digit MNC spaces like 80-99 can be converted to three-digit codes. If that is not possible, clearly present what prevents this.
    - What other solutions are there for the efficient assignment of MNCs, and what management is required for these. Are there any implications for the current handling of MNCs 65-66.
      A new approach shall be proposed based on these conditions.

It shall be noted that insights gained during the study changed the scope somewhat as reflected in section 2.2.

2 Methodology and Report Structure

2.1 Methodology

It was concluded that information would be required from some different types of actors related to the MNC area. Hence, a critical part of the work was to conduct a number of dialogues with important actors in different roles. Identification of these took place in consultation with PTS, which was responsible for formulating introductory letters for each target group, see below. PTS had also the main responsibility for initiating contacts with other NRAs/NPAs.

The dialogues were set to address two main areas:

- Technical conditions and challenges
- Market demands for MNCs

A primary target group identified for the dialogues was **mobile systems providers**. These have global experience of the issues and have implemented technical solutions linked to the problems of the study. They also are also deeply involved in the 3GPP standardization. **Ericsson** and **Nokia** were selected to represent this group.

Dialogues were also to be conducted with a few European national regulatory authorities with experience in implementing regulations for the allocation and use of E.212 MNCs. The **NRAs/NPAs** of the following countries have been involved in this study:
Germany, France, UK, NL, Norway and Finland.

Swedish mobile operators and license holders for private networks, were identified as a third target group. It was further divided into Mobile Network Operators (MNOs) / Service Providers (SPs) and Neutral Host Providers. Some of the companies addressed did not engage. The companies participating were narrowed down to:

- **MNOs and SPs: Tele2, Telenor, Telia, VGR**[1]
- **Neutral Host Network Providers: Corporate Fiber, Proptivity**

Specific questionnaires were prepared for each of the four groups. As NPNs was identified as the primary interest area, the related 3GPP roadmap items as NID (supported in Rel 16.), Onboarding and Credentials Holder were targeted [2].
The main questions and related target groups are presented in Appendix 1.

The answers to these questions are discussed in the specific sections of this document.

It shall be noted that very limited information was obtained in terms of NPN market growth estimations, due to competition reasons.

In general, the MNO / SP contributions were very limited.

The NRA/NPA and NHN contributions were on the other hand more valuable.

As Ericsson and Nokia were resource constrained, substantial contributions were achieved by other means than written replies to the questionaries. Further, Ericsson and Nokia have been reviewing some critical parts of this document.

---

[1] VGR (Västra Götalands Regionen) is a private network (NPN) operator, obtained the same questions as the MNOs and SPs.
[2] The roadmap items are addressed and explained in chapter 5.

2.2 Report Structure

As outlined in the previous section, the study was to comprise two main areas:

- Technical conditions and challenges
- Market demands for MNCs

There are two main *technical evaluations* in this document:

- How a mix of 2- and 3-digit MNCs can be established. This is presented in chapter 8.
- How to proceed on allocation of MNCs for SNPNs, either un-coordinated or shared. This is presented in chapter 9.

In association, there are substantial roaming considerations, addressed in sections, 7.2, 9.2 and 9.6. Further, section 4.3 provides the technical background for roaming.

As there is currently no roaming support defined by 3GPP for SNPNs, some roaming “substitutes” related to the 3GPP SNPN roadmap, are presented in section 5.2. The section also presents some upcoming SNPN related concepts.

Another investigation area for the report is *future market demands for MNCs*.
The business drivers and additional needs are presented in chapter 7. As a significant growth is expected for Neutral Host Networks, these are described and evaluated in chapter 10. The total MNC needs are summarized in chapter 11.

An international outlook is provided in chapter 12, primarily to present the MNC orientation in some European countries, to compare with the Swedish situation.

The following sections / chapters are provided for readability of the report:

- Sections 1.1 and 1.2 provide the background and scope for this study.
- Chapter 3, presents the IMSI and MNC contexts and related international recommendations.
- Chapter 4, describes how the mobile networks handles the MNC related information as PLMN ID in different perspectives as network selection, network registration and roaming.
- Chapter 5, provides descriptions of the NPN alternatives and the 3GPP SNPN roadmap.
- Chapter 6, describes the radio license conditions for local SNPN licenses.

Chapter 13 summarizes the conclusions and chapter 14 outlines the recommendations.

3 IMSI and MNC Handling

This chapter presents:

- The IMSI concept.
- The associated international harmonisations and associated bodies
- MNC options

3.1 IMSI Structure

The International Mobile Subscriber Identity (IMSI) consists of maximum 15 digits and permits identification at three levels:

- Country level: Mobile Country Code (MCC), 3 digits.
- Network level: Mobile Network Code (MNC), 2 or 3 digits.
- User level: Mobile Subscription Identification Number (MSIN), max 10 digits.

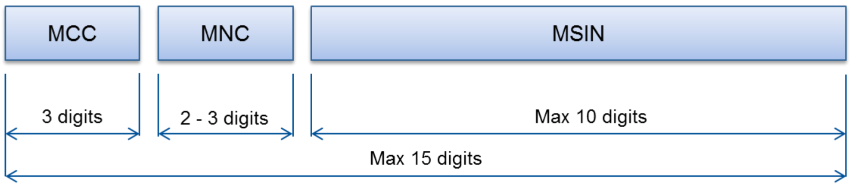

Figure 1 Structure and format of the IMSI [30]

MCCs are assigned by the Director of the Telecommunications Standardization Bureau (Director of TSB). Normally one "geographic" MCCs is assigned per country. MCC 240 has been assigned for Sweden.

MNCs in the "90X" MCC range are also assigned by the Director of TSB. "90X" MCCs are not tied to specific countries and are referred to as "Shared MCCs".

MNCs are 2 or 3 digits in length and, in accordance with ITU-T Rec. E.212 [30], and administered by the respective national numbering plan administrator (NPA), usually the National Regulatory Authority (NRA). MNCs under MCC 90x are the responsibility of the Director of TSB.

3.2 International and European Recommendations

ITU-T Rec. E.212 defines the structure of the IMSI, its components and usage as well as the responsibility and principles for the awarding of numbering resources. 3GPP further refines the concept in their specifications for 3GPP compliant systems. Specifically numbering, addressing and identification aspects are presented in TS 23.003 [41].

CEPT Electronic Communications Committee (ECC) is in the process to provide a new version of the ECC Recommendation on "Harmonised European Management and Assignment Principles for E.212 Mobile Network Codes (MNCs)" and has presented a draft version for comments [32][3]. The recommendations are based on the following considerations:

a. *the September 2016 revisions to ITU-T Recommendation E.212 "The international identification plan for public networks and subscriptions" introduce flexibility in the assignment of geographic MNCs to entities other than public networks offering public telecommunications services;*

[3] On public consultation until the 22nd of September 2023 – expected to be published in December 2023.

b. *that Amendment 1 (07/2018) of Recommendation E.212 (09/2016) introduces a new Appendix III on shared ITU-T E.212 mobile country code (MCC) 999 for internal use within a private network and that any MNC value under MCC 999 used in a network has significance only within that network. The MNCs under MCC 999 are not routable between networks. The MNCs under MCC 999 shall not be used for roaming;*
c. *the ECC Report 337 on "Public numbering resources for mobile non-public networks" (06/2022);*
d. *that, as a result of technology and service innovation, the value chain now contains different entities than those who operate their own networks with or without access to spectrum. Informational Annex 1 contains a non-exhaustive list of potential applicants for geographic MNCs;*
e. *that geographic MNCs and MNCs under shared MCC 90x series are required to enable interconnection with mobile networks for certain services;*
f. *that the majority of the existing geographic MNCs are not yet assigned which may represent an opportunity cost;*
g. *that broadening the circle of market entities which are eligible for an assignment of geographic MNCs may lead to a scarcity of the resource and may also lead to new demand for other numbering resources. This is particularly relevant when broadening the circle to entities not providing publicly available electronic communications networks and/or services;*
h. *that Over-the-Air (OTA) provisioning enables operator switching without the need to physically change SIM cards;*
i. *the shared use of geographic MNCs, via allocating different MSIN blocks*[4] *to multiple entities under a single assigned MNC, although technically feasible and a viable option in some cases, is seen as more demanding from operational and administrative point of view;*
j. *that harmonised management and assignment principles are required in order to maximise effective and efficient use of this resource in CEPT countries;*
k. *that MNCs under the shared MCC 90x series are assigned by the TSB of the ITU for global services;*
l. *that while Recommendation ITU-T E.212 allows the MNC to be either two or three digits in length, the migration from two to three digits under the same MCC seems to have a large operational impact and to be costly.*

The recommendations outlined are *"that CEPT administrations, when setting management and assignment principles for MNCs take account of the following high level principles:*

1. *geographic MNCs are to be managed and assigned to license the most effective and efficient use of a finite resource in order to defer, as long as is practicable, the need to request an additional MCC from the ITU TSB;*
2. *assignments of geographic MNCs are to be made according to procedures and criteria established by the national numbering plan administrator (NPA);*
3. *applicants for geographic MNCs should be required to:*
    - *provide substantiating documentation justifying their need for the resource which also describes the network, services and/or functions that the resource will be used for;*
    - *affirm that the network, services and/or functions comply with applicable standards (ITU-T, ETSI, 3GPP etc.);*

[4] Described in section 9.4.1 of this document

- *provide justification that other numbering solutions fail to meet requirements for specific services;*

4. *the shared use of MNCs should be considered as a viable option;*
5. *for mobile non-public networks:*
   - *Encourage the use of MCC 999 with 3-digit MNCs for Stand-alone non-public networks (SNPNs)[5] ;*
   - *In order to manage potential network attachment issues [6] , NPAs may consider encouraging industry stakeholders to lead on a national coordination regarding the use of MNCs under MCC 999;*
   - *Considering the allocation of one or more MNCs from the geographic MCC for shared use without direct assignment for SNPN;*
   - *Considering the assignment of a single MNC for the simultaneous use by multiple networks for shared usage;*
6. *for services to be provided in more than one country, excluding mobile roaming services, an applicant for a geographic MNC should, as an alternative, be encouraged to consider applying to the ITU TSB for the assignment of an MNC under a shared MCC in the 90x series to avoid the need for multiple assignments of MNCs under different geographic MCCs;*
7. *geographic MNCs may be allocated for testing purposes or assigned on a temporary basis for testing purposes[7] ;*
8. *where a CEPT administration requires a new MCC assignment from the ITU according to procedures in Annex C of Recommendation ITU-T E.212, this administration should consider using 3-digit MNCs under this new MCC, thus providing 1,000 rather than 100 MNCs*

As outlined by recommendation number 1, PTS (and other NRAs/NPAs) is responsible for an efficient and effective management of the geographic MNCs.

3.3 MNC Options

The shared MCC 90x series is not to be confused with shared geographic MNCs. The MCC 90x series is simply to be referred to as global MCCs.

A specific case of a global MCC is MCC 999 (outside of MCC 90x), as addressed in item 5 of the CEPT recommendations. MCC 999, is of vital interest and part of the recommendations specified in this document. MCC 999, is un-coordinated, i.e. any network owner can utilize this MCC with any MNC. Interestingly enough, either 2- or 3-digit MNCs can be selected, and one is encouraged to use either MNC 99 or 999 for testing purposes. This is the background for urging a national coordination by industry stakeholders, in item 5 of the draft recommendations.

Shared MNCs are on the other hand primarily within the geographic MCCs context. The implications of shared MNCs are thoroughly discussed in section 9.4 of this document.

The vast majority of countries, including Sweden have been using 2-digit MNCs. As to achieve an efficient management PTS is considering introducing 3-digit MNCs primarily for the 8xx and 9xx MNC series. However, there are number of considerations in terms of mixing 2- and 3-digit MNCs. These are penetrated in chapter 8 of this document.

---

[5] Which includes also SNPNs with shared RAN (see ECC Report 337 [31])

[6] Network attachment issues occur when an UE can try attach to different networks that use the same combination of MCC and MNC

[7] See also Amendment 2 (from 2020) of Recommendation ITU-T E.212 which introduce Annex G with assignments of MNCs by the Director of TSB of ITU under shared MCC 991 for conducting international non-commercial trials.

Please note that a mix is not considered in the CEPT recommendation. However, three digit MNCs are to be applied for new MCCs.

Traditionally the MNCs were only to be provided to public networks for which a unique MNC was provided. As presented in the CEPT recommendations, ITU-T SG2 updated the E.212 recommendations in 2016 as to also support other network types:

"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."

PTS was early to allocate MNCs 65-66 for private networks. As for MCC 999, these MNCs are also un-coordinated i.e. the network owners are free to select any of the MNCs without any coordination with PTS.

Unique MNCs can be provided to Non-Public Networks (NPNs), however strong motivations are required, as presented by the CEPT recommendations [32]. A specific consideration in this context is roaming, being addressed in this document.

4 Mobile Networks and IMSI Handling

This chapter presents how public mobile networks makes use of the IMSI. Further, the roaming aspects are discussed.

4.1 Network Selection Based on IMSI and PLMN ID

As presented in section 3.1, the IMSI consists of MCC + MNC + MSIN. The MCC + MNC combination is denoted as PLMN (Public Land Mobile Network) ID. Each subscriber will have a unique MSIN. The IMSI is stored on the SIM card[8] together with some authentication credentials.

The PLMNs broadcast the PLMN ID as system information. The User Equipment (UE) will read this information and match it towards information stored on the SIM card in different lists. Somewhat simplified, the initial network selection process in automatic mode works as follows:

- The UE will identify all surrounding PLMNs and divide them into two categories,
    - High quality ones which provide a signal strength above a specific threshold.
    - Low quality ones, for which it also keeps track of the signal strength received.
- The UE first checks the PLMNs with high quality signal strength. If the UE identifies its Home Network or an Equivalent Network it will try to connect (attach/register) to it, otherwise it will select the most preferred one (in random order).
- If there is no valid high quality PLMN available, the UE will evaluate the PLMNs in order of decreasing signal quality.

When a UE is connected to a network, it will stay on this network until the signal quality is not sufficient and initiate a new network selection. If the UE is not connected to its home PLMN it will regularly search for the home PLMN.

The UE has also information on what access technology (4G vs 5G etc) it shall prioritize for each PLMN. Further, there is other system information to be considered by the UE whether if it should try to register to the selected PLMN or not.

The FORBIDDEN PLMNs list defines PLMNs to which the UE does not automatically attempt to access.

The Equivalent HPLMN list defines a set of PLMNs which are treated as equivalent to the HPLMN in priority order. Thus, another PLMN can be given a higher priority than the home PLMN. If this list is present and populated it overrides the home PLMN selection.

The Operator Controlled PLMN Selector (with Access Technology) list defines the priority order of the preferred PLMNs.

There is also User Controlled PLMN Selector (with Access Technology) which will override the Operator Controlled one. However, this list is normally not populated.

In manual mode the user will be provided a list of the available PLMNs to select from.

[8] SIM card is used for simplicity and relates to UICC and SIM options, please see chapter 16 for clarifications.

4.2 Network Registration

When the UE has made a network selection, it will have to register to the selected network which works as follows.

The UE sends a Registration Request to the network. For 4G, only IMSI is the relevant identification information. In 5G, the UE provides the SUCI (Subscription Concealed Identifier). The SUPI (Subscription Permanent Identifier) is the vital part of the SUCI as to identify the Home PLMN (HPLMN) of the UE. The SUCI encrypts the user related parts of the SUPI, but the network related information is left open. This can be in two formats:

- IMSI, the traditional format
- NAI (Network Access Identifier), in string format, user@HNI where MNC is part of the HNI (Home Network Identifier).

With this information the Visiting PLMN (VPLMN) is able to identify to which network the UE belongs to. Further, the VPLMN will make a first validation if this is a valid request e.g. if a roaming agreement with the HPLMN of the UE exists.

The VPLMN uses the IMSI/SUCI information to resolve where to send the subsequent Authentication Request in the HPLMN. For 5G, the Routing Indicator can be included in the SUCI, which identifies a certain Unified Data Management (UDM) server (related to a specific IMSI subset).

Access to subscription data in HPLMN is only allowed if roaming agreements exist between the two networks. If the "serving network" (VPLMN) is successfully validated, there is exchange of encrypted authentication data between the involved entities in which the entities will be validated as well. If the UE authentication data matches with the corresponding data in the VPLMN, there will be a successful registration. Note that 5G traffic between the two networks is encrypted by using TLS between the Security Edge Protection Proxies (SEPP) of the two networks.

There are several different reasons for unsuccessful registration. The UE will receive a cause value to inform the UE about the reason for the failure [42]. Some of them will yield that the UE shall insert the PLMN ID of the network it tried to register to, into the FORBIDDEN PLMNs list. We denote cause values NOT yielding a FORBIDDEN PLMN list insertion as "soft" ones. The implications of this are discussed in section 9.5.2.

4.3 Roaming

From Wikipedia:

"Roaming refers to the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, by means of using a visited network.

The legal roaming business aspects negotiated between the roaming partners for billing of the services obtained are usually stipulated in so called roaming agreements. The GSM Association broadly outlines the content of such roaming agreements in standardized form for its members. For the legal aspects of authentication, authorization and billing of the visiting subscriber, the roaming agreements typically can comprise minimal safety standards, as e.g. location update procedures or financial security or warranty procedures"

Thus, there are at least two parties involved for roaming:

- The visited network (VPLMN) to which the UE will connect
- The home network (HPLMN) which is responsible for authenticating the user, as part of the registration explained in section 4.2.

There are two options for roaming, Local Breakout (LBO) or Home Routed, please see [35] for further elaboration. For local breakout the traffic is handled locally, whereas for home routed, the traffic is directed to the home network. It is possible to mix this between services e.g. to home route voice traffic whereas data is handled locally. The 5G architectures for the two concepts are outlined in *Figure 2* and *Figure 3*.

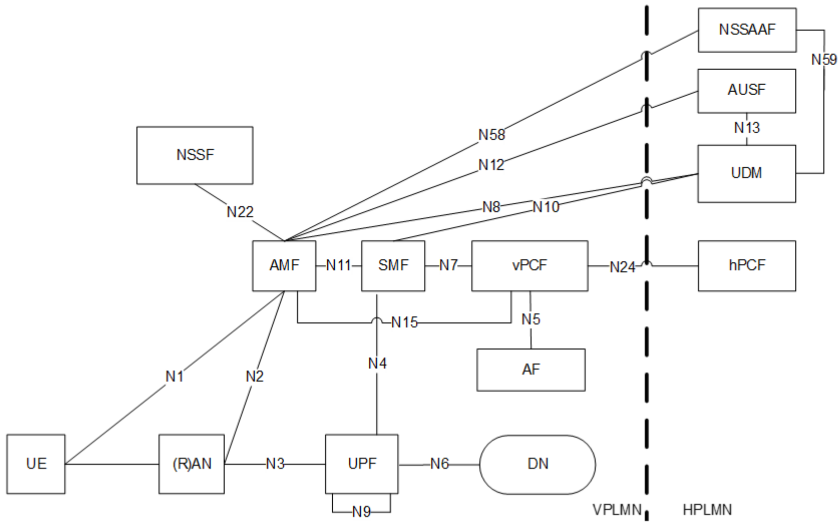

Figure 2. Roaming 5G System architecture - local breakout scenario [40]

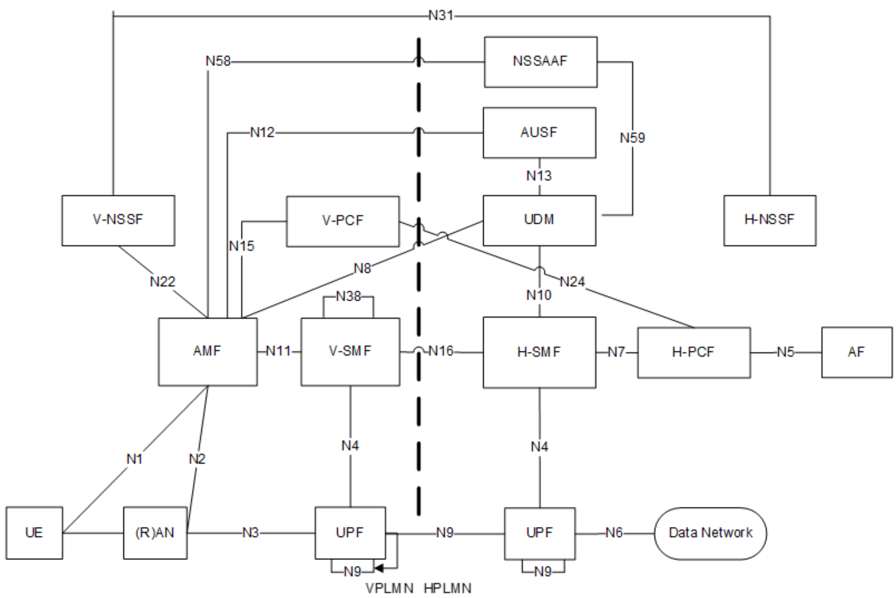

Figure 3. Roaming 5G System architecture - home routed scenario [40]

5G is based on Control and User Plane separation (CUPS). Of specific interest for this report, as addressed in section 4.2, is the registration signaling (Control Plane) which involves:

UE – N1 (NAS interface) – AMF – N8 / N12 – AUSF / UDM

In this document the Network Slicing considerations are not covered, which are related to the NSSF and NSSAF entities. Whereas the AMF handles the Access and Mobility Management Functions, the SMF handles the Session Management Functions with interface to related Policy Control Function (PCF). The data traffic passes in the user plane, which for LBO is:

UE – RAN – UPF (User Plane Function) – DN (Data Network)

It shall be noted that the connections between the networks will have to be secure and reliable. This is ensured by using SEPP and dedicated transport networks, part of "IP Packet exchange" (IPX). The IPX guidelines are presented in [39].

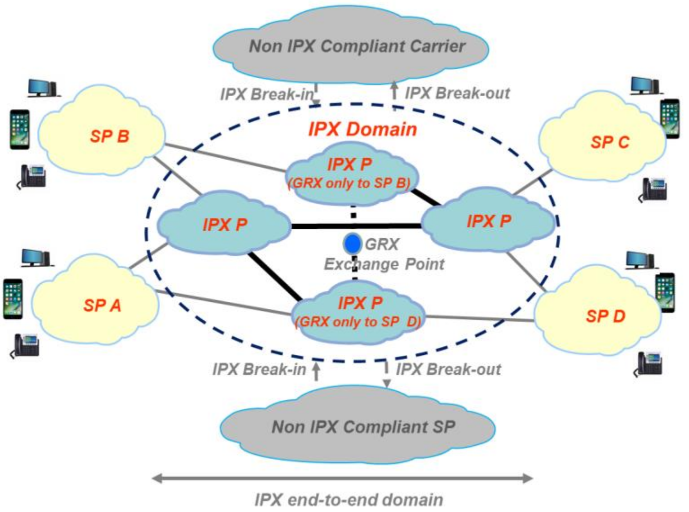

Figure 4. IPX Model [39]

Roaming provides a straightforward authentication handling, as the credentials[9] are stored in the HPLMN. Thus, there is only one set of traditional credentials to be handled. This is to be compared with the roaming "substitutions" presented in section 5.2.

Although, roaming is technically straight forward for public networks it is not established for SNPNs without an own MNC. With the introduction of Network ID, denoted as 5GC-NID, SNPNs will have a unique identity, please see section 9.2 for further details. In section 7.2, the full roaming implications are discussed.

Roaming agreements as addressed above, with associated implementation of charging and billing is a challenge on its own. Further, connections to IPX or direct inter-connections are required.

[9] Credentials are constituted by the UE identity (traditionally IMSI) and a shared secret key for encryption stored in the "SIM Card" and the home network.

5 Non Public Networks

This chapter presents:

- NPN variants and related MNC needs.
- The SNPN standardization within 3GPP related to overlay / underlay networks, UE onboarding, credentials holders and localized services.

5.1 NPN Variants

There are two basic NPN variants, Stand Alone (SNPN)[10] and Public Network Integrated (PNI-NPN). There are two SNPN options:

- *Isolated Stand Alone*, which implies that there is no PLMN involvement. SNPN frequencies will be used.
- *Shared RAN Stand Alone*, which implies that the RAN is shared between the PLMN(s) and the SNPN. There are no core network relations between the SNPN and the PLMN(s). Either the SNPN or the PN frequencies or both can be utilized.

The SNPNs will need an MNC, preferably not a unique one. They could then use either MNCs under MCC 999 or MNCs 65/66 under MCC 240. The 5G SNPNs, can future wise be identified by the SNPN ID, constituted by the combination of the PLMN ID and Network ID (5GC-NID), see section 9.2.

In the PNI-NPN case, the NPN is implemented as part of the PLMN. I.e. both core network and RAN is operated by the MNO using the MNO frequencies and PLMN ID. The NPN is typically implemented by means of Network Slicing. Access is controlled via Closed Access Group (CAG), to which the UE must belong to.

Since PNI-NPNs do not have any MNC considerations as the (existing) MNO MNCs are used, these are not for further considerations in this document.

5.2 3GPP SNPN Standardization

5.2.1 Roadmap

An excellent overview of the 3GPP SNPN roadmap up to R18 with related background is presented in [17] ("background document"). The roadmap is summarized in *Figure 5*.

[10] Whereas SNPN is a 5G term, in this document it is applied in a broader sense as to denote stand alone NPN also for 4G/LTE.

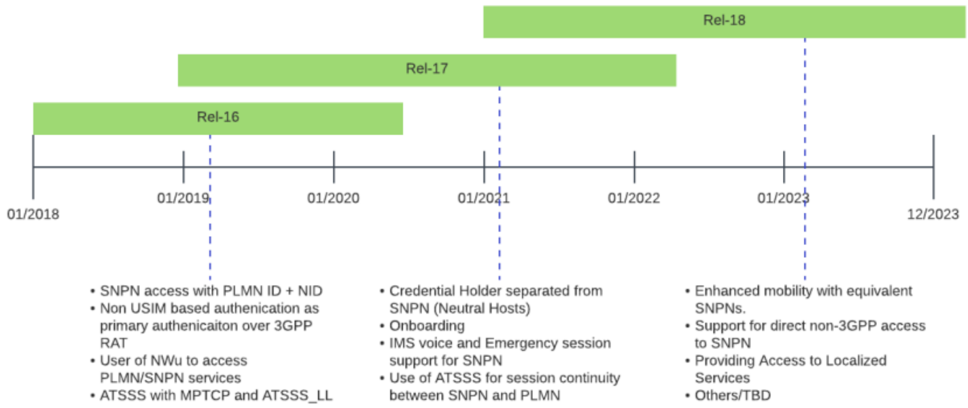

Figure 5. 3GPP SNPN Roadmap up to Release 18, [17][11]

The critical foundation is the 5GC-NID in R16, as described in detail in section 9.2 of this document. The document elaborates of different means as to authenticate to SNPNs. Some roaming "substitutes" are presented in the following sections.

5.2.2 Basic Architecture

The background document presents the following simplified architecture for user plane routing i.e. the control plane relations are omitted. The various aspects are presented in the following sections.

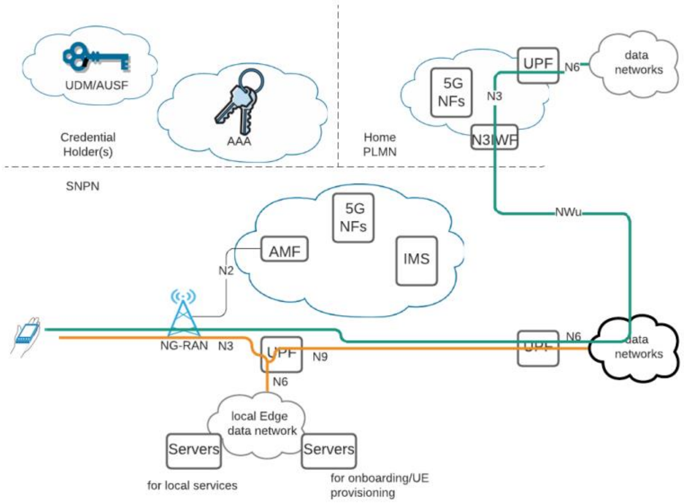

Figure 6. Simplified SNPN Architecture with User Plane Routing for Different Services, [17]

The Untrusted non-3GPP Access function N3IWF is a key component supporting secure IPSec tunnel access for different scenarios. Thus, the N3IWF is very similar to a VPN server from a client access perspective. A detailed overview of the 3GPP access alternatives is presented in [27]. The untrusted non-3GPP access reference architecture is presented in *Figure 7*. It should be noted that the N3IWF has the same internal interfaces as the (R)AN (N2 and N3).

[11] Some Access Traffic Steering, Switching, Splitting (ATSSS) limitations applies

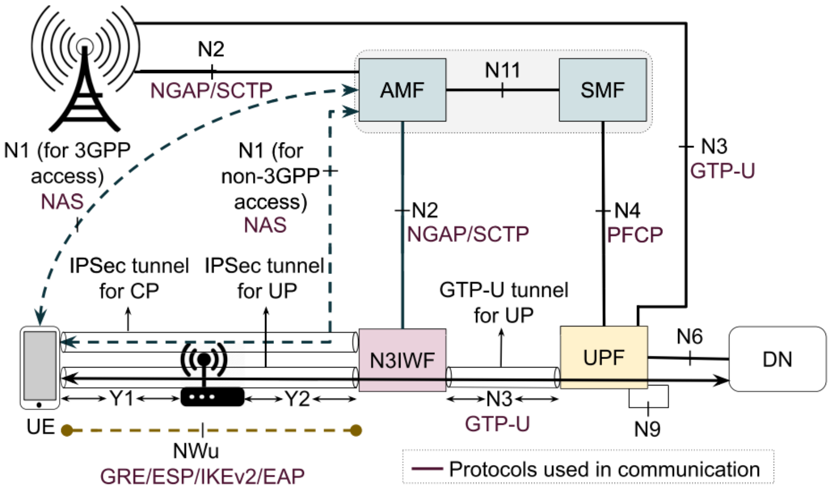

Figure 7. Architecture for 5G with untrusted non-3GPP access network [27]

5.2.3 Overlay and Underlay Networks

The background document presents:

"Interesting enough that even when 3GPP does not support roaming between SNPN and PLMN, the specification does allow a UE with dual credentials (e.g., similar to dual SIM dual standby (DSDS) or dual SIM dual active (DSDA)) to access both SNPN and PLMN services at the same time. This is particularly useful when a user wants to separate their usage between enterprise and personal domains or when the user is in a remote SNPN environments like caves or shielded factory where PLMN coverage is not available or accessible.

3GPP defines the following terms to cover this usage:

• *Overlay network: When UE is accessing SNPN service via NWu using user plane established in PLMN, SNPN is the overlay network. When UE is accessing PLMN services via NWu using user plane established in SNPN, PLMN is the overlay network.*

• *Underlay network: When UE is accessing SNPN service via NWu using user plane established in PLMN, PLMN is the underlay network. When UE is accessing PLMN services via NWu using user plane established in SNPN, SNPN is the underlay network."*

The document illustrates the case when the SNPN is used as an underlay network, as outlined in *Figure 8* below. The SNPN is in this case the serving network, and after successful authentication to the SNPN, the UE will be able to connect to the MNO HPLMN. The UE must either be supplied with SNPN specific credentials, or it can provide the MNO specific credentials stored on the UICC towards a Credentials Holder, see section 5.2.5. SNPN credentials could e.g., be retrieved via UE onboarding, see next section. Another challenge is that the MNO needs to grant access to its network and services (e.g. voice) via N3IWF to SNPN users. This requires SLA between SNPN and MNO. N3IWF is also not widely deployed today.

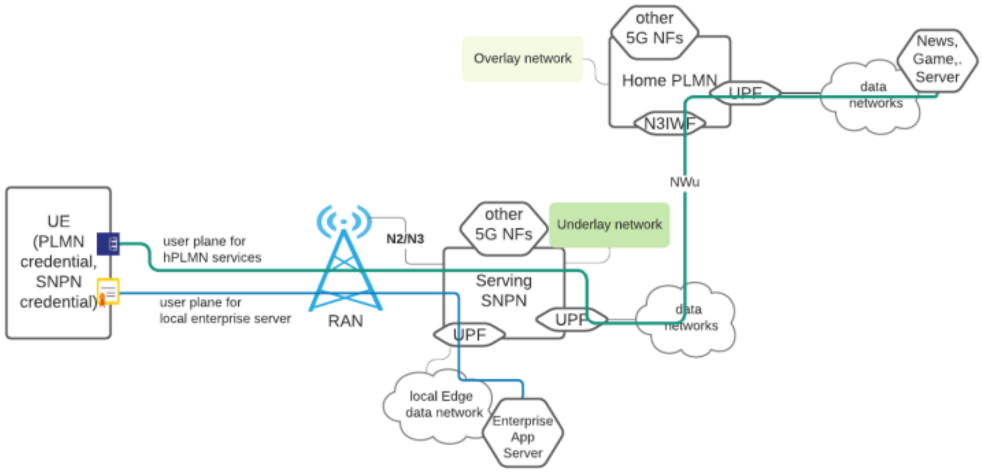

Figure 8. Access to HPLMN services via SNPN [17]

5.2.4 UE Onboarding

With UE onboarding, UEs will be able to authenticate with some default credentials towards an Onboarding SNPN which allows exclusive connectivity to a Provisioning Server (PS). The UE is then communicating with the Provisioning Server to obtain the (permanent) SNPN credentials. A particular use case is that (I)IoT equipment can be provided with the default credentials upon production and updated when connecting to the Onboarding SNPN. The SNPN will broadcast that it supports onboarding. The UE will indicate to the SNPN that it would like to connect for onboarding.

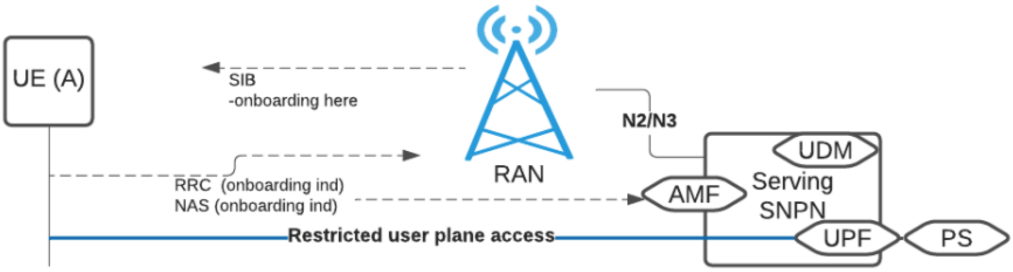

Figure 9. On-boarding Process for a non-initialized UE [17]

There is another onboarding option based on that "the UE can leverage existing credential and network connection" as stated in Annex N of [40]. Accordingly, the UE first establish a PDU (User Plane) session and then connects to the Provisioning Server. The PDU session can either related to a normal registration towards the SNPN or to a PLMN for which the UE has subscription,

5.2.5 Credentials Holder

From background document [17]:

"Credentials Holder (CH) is defined in 3GPP [40] as an entity which authenticates and authorizes access to an SNPN separate from the credentials holder. It means that the serving SNPN does not store the credentials that can be used to authenticate/authorize the UE. This is also commonly known as neutral host offering as it allows the SNPN to provide connectivity service to the users using credentials from 3rd party."

The Credentials Holders concept allows for Neutral Hosts deployments, i.e., the serving SNPN enables usage of its network resources for subscribers of the CH. It shall be noted that the serving SNPN will have to apply some kind of subscription information related to the CH, either per subscriber (means per SUPI) or per group of subscribers. *Figure 10* illustrates the CH concept.

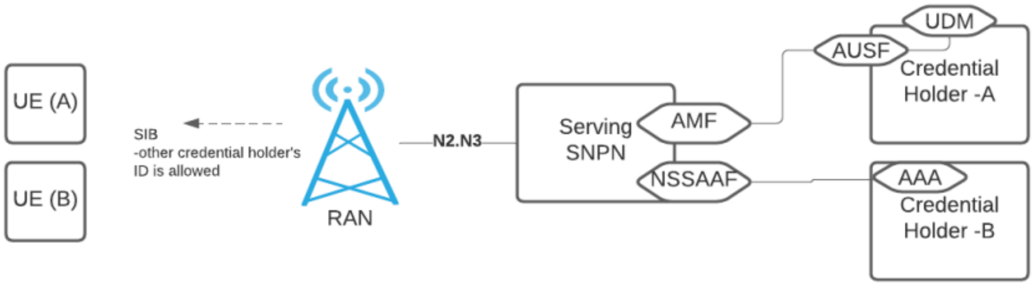

Figure 10. SNPN interacting with credentials holders [17]

Essentially the CH concept implies that the UE provides its home network credentials to the CH. The CH can be the home network (SNPN or PLMN) or a 3rd party with SLAs etc towards the home network.

Two different types of authentications are supported, see *Figure 10*.

- Credential information stored in UDM related to a SUPI and based on UICC usage (3GPP standard procedure).
- Credential information stored in AAA server (typically EAP server)

"When accessing a SNPN with credentials from 3rd party (credential holder), the UE must first check the system information block (SIB) broadcast message from the RAN to determine which 3rd party (credential holder) is supported by this SNPN. This could be in the form of a list of PLMN ID + NID or group ID (GIN) for network selection. GIN[12] represents a group of 3rd parties using a common Network ID to minimize the broadcast list in the SIB. If the UE has been configured with a credential from one of those 3rd parties that is shown in the SIB then the UE may proceed to register to the SNPN using the 3rd party credentials.

RAN may also broadcast an additional indication in the SIB to indicate that UE with any 3rd party (credentials holder) information can try to access this SNPN. This type of uncontrolled access[13] may be useful for general public usage (e.g., public access at the park, public library, etc.)"

The visitor capabilities outlined above using any 3rd party information may at a first glance seem promising as to support visitors as addressed in section 7.3. However, "connections" and SLAs must then be in place towards the home network as to achieve CH authentication.

[12] GIN is optional information representing a single or group of credentials holders the SNPN provides access to [40]
[13] The indication just tells the UE that the SNPN has contracts with some CHs without guaranteeing access to these CHs for the UE

5.2.6 Localized Services

The SNPN roadmap document [17], does not address the Localized Services support in R18. The basic approach is to support time limited access to specific events "hosted" by a SNPN (e.g. an arena event). Like any other SNPN it would need a SNPN ID.

- SNPN can use the onboarding feature to allow restricted access and download SNPN credentials to the UE. Restricted access is provided by using default credentials, but it is not specified how these default credentials are provided to the UE beforehand (can be via scanning a QR code).
- Other option is to use SLAs between local SNPN and CHs. The CHs can then be specific PLMNs (or SNPNs). As local SNPN can be provided in a stadium where actually everyone can access the event, SLAs with all PLMNs in a country are needed. There is then a need for a "Broker" role, interconnecting all the MNOs and SNPNs based on SLAs with all involved parties.

For SNPN selection the only addition is that selection based on time validity information and location assistance information can be used. Thus, UE is aware the local SNPN is only available in a certain area (arena) and during a certain time (during the event).

6 Radio Licenses

An SNPN must have a Radio Access Network (RAN) with an associated radio license. There are two main options in this perspective:

- SNPN radio license
- Public radio license(s) related to the involved MNO(s)

The first option is denoted as local license for which the estates to be covered need to be defined. The maximum output power is lower for local licenses than for public ones.

Local radio licenses can be obtained for 3.5 and 26 GHz bands. In terms of the 3.5 GHz band the following assignments have been made.

- 3400-3500 MHz, Hi3G
- 3500-3620 MHz, Telia
- 3620-3720 MHz, Net4Mobility
- 3720-3800 MHz, Local Licenses

There is a total of 80 MHz allocated for the local licenses, which can be requested in blocks of 10 MHz.

Not only is the output power more limited for the local radio licenses, there is also a required synchronization relative the public radio license holders. The latter will have profiles for providing more downlink capacity due to streaming services etc. However, IoT requires the reverse split, as the sensors are sending uplink data. Thus, the actual capacity for local licenses will be substantially lower than the ideal one without synchronization considerations.

The SNPN owners could find it attractive to aim for shared RAN, using the MNO radio license. In this case, the SNPN will have an MNC without any associated local radio license.

7 Business Drivers and Additional Needs for SNPNs

This chapter presents critical demands and considerations for SNPNs related to MNC allocations:

- Why to select a SNPN vs PNI-NPN.
- The implications of roaming in the light of that roaming for SNPNs without an own MNC is not supported by 3GPP.
- How visitor access could be supported, in general and for some specific use cases.
- Distributed SNPN considerations.
- Device availability for MNC options.

7.1 Autonomy

As addressed, only SNPNs would need separate MNCs, whereas PNI-NPNs take use of the MNO MNCs. The major reason to head for an SNPN vs PNI-NPN, is to ensure a full autonomy. Thus, the SNPN shall not rely on any external components as in the PNI-NPN case. The SNPNs will be a vital part in the productions systems etc. with IIoT as an important driver. Reliability and security must be ensured to 100%.

From the other end, mobile radio access networks are much more complex than WLANs. A shared Radio Access Network (RAN) could then be a good compromise, on the condition that the RAN will be autonomous.

As described in section 11.1, the market uptake for SNPNs in Sweden has been slow. This is probably related to the high complexity and MNO positioning. Thus, SMEs have so far primarily selected PNI-NPNs. As the market will evolve, there should be other parties like system integrators who will act between the system providers and the companies.

7.2 Roaming

The starting point for roaming is that commercial roaming agreements must be established between the involved parties. Roaming agreements can be on bilateral bases between two networks or between a network and a roaming hub (broker). This may be a bigger obstacle than the technical ones.

The need for roaming related to SNPNs is an open question. From one end, an argument is that private (non-public) networks are to be private and standalone by nature, thus roaming shall not be needed. The lack of roaming support for SNPNs (with 5GC-NID) in 3GPP specifications, could to a large extent be tracked to this argument.

However, there are clear indications on that there is an increasing interest for roaming for SNPNs. Should those then need a separate MNC?

The lack of roaming support for SNPNs (without own MNC) in 3GPP is to be addressed, since there is a rising need for roaming and the basic argumentation for not supporting it is unclear. Further, our understanding is that there should only be limited work to fulfill an end2end support for SNPN ID roaming in 3GPP.

PTS, potentially with support from other NRAs/NPAs, should then urge 3GPP to complete the SNPN parts, as to include roaming support. Liaison statements from CEPT WG NaN and ITU-T SG2 should be the preferred way. Thereby an un-coordinated

MNC approach could be adopted without the need for own MNCs. Please see section 9.6 for further details.

There are upcoming 3GPP SNPN features as credentials holder, onboarding and underlay/overlay networks in the 3GPP specifications as presented in section 5.2. They could then be understood as roaming substitutions. However, they introduce limitations and other complexities and should not replace the need for native roaming support. Since these options will not be at hand in the near future, other short term alternatives must be sought.

It should be noted that VPN solutions are other ways to connect to the home network remotely. However, the VPN will not be tightly coupled to the SNPN.

A new role, already on the market, has been presented by Ericsson in direct dialogue. Major M(V)NOs with many roaming agreements in place, offer a solution for international roaming to the SNPNs. Thus, the SNPN users will be able to roam home to the SNPN on an international basis. The SNPNs will utilize a specific part of the M(V)NO IMSI range, as for shared MNC networks. The same MNC as the M(V)NO one, will be used in the SNPN.

This is similar to the HLR Proxy Provider approach presented in 2013/2014 adopted by NL, see section 4.4 in [30]. The current M(V)NO international roaming offer will not require any Swedish MNCs as the M(V)NOs will not use a Swedish MCC. However, there might be similar upcoming approaches for the Swedish market. The MNC demand will be very limited as this only requires one MNC per M(V)NO. This approach should be promoted as it limits the need for new MNCs.

7.3 Visitor Support

In the previous section, the roaming need is related to SNPN UEs, accessing the SNPN while outside the coverage of the SNPN. I.e. utilization of a connectivity service from another network, either another SNPN or a PLMN. From the other end, there is a need (in some cases) to provide access to the SNPN for visitors. Some examples:

- Within a mine, only the local RAN will provide coverage. The visitors should be able to connect to their public MNO. One option is shared RAN jointly with the MNO. However, this might not be the desirable way, yielding that only the SNPN will be maintaining the local RAN. One future option is that the visiting UEs will use their home credentials via CH ("connected" to home network) or credentials in the underlay SNPN, via onboarding. A simpler approach would be roaming, however not supported for SNPNs without an own MNC.
- Within a hospital, there is a need to provide indoor coverage for the MNOs as to provide service coverage for the patients (and visiting workers). Traditionally, this has been accomplished by DAS solutions[14]. However, as 5G networks are introduced in the hospitals, DAS solutions should no longer be applicable as not supporting required positioning resolutions. Direct options are shared RAN or Femto cell deployments. However, this might not be applicable, leading to a roaming approach as for the mining example.
- There should be a (future) need for shopping malls, airports etc to provide local services coupled to positioning. However, this survey has not revealed

[14] A Distributed Antenna System (DAS), as the name implies, distributes the outdoor radio signals into the buildings by means of antenna systems.

any examples of such solutions. In any event, the solution options should be the same as for the mining and hospital cases.

7.4 Distributed SNPNs

Distributed SNPNs implies that roaming solutions must be sought as to achieve continuous connectivity. This yields that a dedicated MNC is needed for the SNPN. An example of a distributed SNPN with a dedicated MNC is the VGR (Västra Götalands Regionen) SNPN with MNC 60.

As a continuous network access is sought, there are different solutions available to provide dual connectivity to the SNPN and PLMN. The new Apple iOS capabilities will also ease the implementation e.g. supporting geo-fencing with SNPN priority, please see next section.

7.5 Device Availability

As the use cases for SNPNs evolve from IIoT applications with dedicated equipment to personal applications as voice, there is also a need to support smart phones and tablets in the NPNs.

There has been limited equipment support for SNPNs from leading equipment manufacturers related to traditional certification processes for the MNO networks. This is now to change as Apple recently communicated that they will support some specific private networks for both LTE and 5G (SA and NSA) starting from iOS 17 [61].

In summary:

- The following networks are supported
  - MCC 999 with any MNC
  - Germany: 262-98
  - Sweden: 240-41 and 49
  - US: 315-010 (CBRS)
- Prioritizing Cellular over WiFi, to see to that the UE prioritizes the SNPN
- Geofencing, enabling the UE to select the SNPN when coming into reach. There can be two profiles etc, in the UE as to handle the SNPN and a PLMN in parallel.
- eSIM handling
- Voice is not supported for SNPNs (only PLMNs)

It is currently unclear if 240-65/66 will be supported, however we assume that this will be the case. MCC 999 is supported worldwide as of today and has been the default option for SNPN systems for some time. It offers about 1,000 MNCs in contrast to the two ones for Swedish MNCs 65 & 66. Thus, it will be easier to handle the “MNC interference” problem with MCC 999, see section 13.1.2. This should yield a clear interest for adopting MCC 999 for SNPNs.

It shall be noted that Apple has changed the support for Swedish MNCs. In the first release Apple stated support for MNC 60, being the VGR SNPN MNC. This was then withdrawn in favor of MNCs 41 and 49, being PNI-NPNs for Telenor and Telia. Since VGR is the forerunner for Swedish healthcare in terms of SNPNs, it is surprising that they have been removed. Thus, we expect that they should obtain their Apple device support soon.

As voice is a critical application for SNPNs like the VGR one, it is expected that voice will be supported for SNPNs as well. The understanding is that some other device manufactures offer such support today.

All in all, it is believed that other device manufacturers will follow the Apple approach to support specific MNCs, with a foundation for MCC 999, combined with specific SNPN features. The SNPN service capabilities should not be limited to data services but also to include e.g. voice services.

8 Two and Three Digit MNC mix

This chapter presents how a mix of 2- and 3-digit MNCs can be supported and related considerations.

- The background section describes how ITU-T and 3GPP has addressed this area. A major consideration is that 3GPP states that a mixture of two and three digit MNC codes within a single MCC area is not recommended.
- Conclusions from earlier studies are presented, indicating that a mix shall be possible.
- Implementations and related experiences are presented also indicating that a mix is possible.
- A technical analysis of the 3GPP specifications also indicates that a mix shall be possible.
- The findings are accordingly that a mix shall be possible.

8.1 Background

The ITU-T Rec. E.212 allows for either 2- or 3-digit MNCs and it is the NRA/NPA in the respective country that decides on the specific MNC allocations and assignments, see chapter 3. The vast majority of countries, have started with two-digit MNC allocation plans. However, new needs have yielded that 100 MNCs will probably not be enough on a per country basis. The introduction of NPNs is the major driver for implementing three-digit MNCs due to the expected large number of private networks.

Thus, there is a need to adopt three-digit MNCs. As ITU TSB will not assign a new MCC until the existing one(s) are utilized to the large extent (80%), a mix of two- and three-digit MNCs will have to be sought.

However, the approach of 3GPP is that a mix should is not recommended as further elaborated below. This goes back to studies in 2012 when 3GPP launched a Liaison Statement [9] answering ITU-T TSB Circular 285 [67], indicating a number of problems associated with a 2/3-digit mix. In parallel the GSM Association for Europe also concluded that a mix shall be avoided [11].

The 3GPP numbering specification [41] define that:

"A mixture of two- and three-digit MNC codes within a single MCC area is not recommended and is outside of this specification"

Section 2.2 of the specification, IMSI composition, also states that

"The length of the MNC (two or three digits) depends on the value of the MCC"

This is not in line with how the 3GPP systems are designed as described below. This is probably related to "historic" releases prior to 1998 when the SIM card did not have the information on the MNC length

Further, the 3GPP NAS specification [42], is even more restrictive as it refers to "not permitted" as shown in *Figure 11*.

Annex A (normative):
HPLMN Matching Criteria

With the introduction of PCS1900 with the regulatory mandate to allocate 3-digit MNC codes, additional functionality is required to identify the HPLMN.

Assumptions

An MNC code shall consist of 2 or 3 decimal digits. In NA PCS1900, all SIMs shall store 3 digit MNCs.

Any network using a 2 digit MNC code shall broadcast the hexadecimal code "F" in place of the 3rd digit.

For PCS1900 for North America, regulations mandate that a 3-digit MNC shall be used; however during a transition period, a 2 digit MNC may be broadcast by the Network and, in this case, the 3rd digit of the SIM is stored as 0 (this is the 0 suffix rule).

With the exception of North America during the transition period:

a) Within a single country (or area identified by a MCC) all networks shall broadcast a 2 digit MNC code, or all networks shall broadcast a 3 digit MNC code. A mixture of broadcast 2 and 3 digit MNC codes is not permitted within a single country (or area identified by a MCC).

b) A network which broadcasts a 2 digit MNC code, will issue SIMs with a 2 digit MNC code in the IMSI on the SIM. A network which broadcasts a 3 digit MNC code, will issue SIMs with a 3 digit MNC code in the IMSI on the SIM.

Figure 11. 3GPP HPLMN matching criteria [42]

These 3GPP statements have to a large extent blocked introductions of three-digit MNCs.

However, there are a number of proven implementations of two- and three-digit MNC mixes under the same geographic MCC.

It will be shown that there is no longer a technical ground for not implementing a mix as supported by the successful implementations.

8.2 Earlier Studies

In 2012 the ITU-T TSB Circular 285 survey [67] was conducted with a majority of the respondents being against introducing a mix. The NL report from 2013 produced by Dialogic [10], presents the following summary of the conclusions from the ITU study.

With regard to the mixed usage of 2- and 3-digit MNCs within one MCC, the feedback is negative:

> Regarding Question (e), "Are you aware of any issues that might arise if 3-digit MNCs are assigned in the future under your existing MCCs?", the majority of the responses indicated that:
>
> a. An existing MCC under which 2-digit MNCs were assigned should not be converted into an MCC under which 3-digit MNCs would be assigned.
>
> b. All MNC assignments under a particular MCC should have the same length, that is, all should be either two digits or three digits.

Box 13: Source: ITU, "Summary of Replies to TSB Circular 285: Possibility of parallel usage of 2 and 3 digit E.212 Mobile Network Codes (MNCs) under one geographic Mobile Country Code (MCC)".

Also here there is little support for the mixed usage of 2- and 3-digit MNCs. In the specific answers by ITU member countries, the visions however diverge strongly: some indicate significant and hardly foreseeable consequences for networks, mobile networks and billing/provisioning systems, yet others indicate they foresee little or no problems.

The Dutch contribution is fairly explicit and indicates that T-Mobile expects that 3-digit MNCs can be introduced relatively effortlessly, as long as there is no overlap in the MNCs (thus the 2-digit MNC cannot overlap with the first two digits of a 3-digit MNC).

The summary document mentions three countries that already make use of 2-digit and 3-digit MNCs within one MCC: Argentina, Nicaragua and Honduras. No particular problems were reported for these countries. While we were able to find specific number allocation information for Argentina (see the table below), we were not able to locate similar information for the two other countries.

Figure 12. Conclusions of ITU-T TSB Circular 285 study 2012 as presented by Dialogic [10]

One should then note the reference that T-Mobile (NL) indicated a smooth introduction of a 2/3-digit mix as long as there would be no overlap. The report further highlights:

> Another reference case identified is India. Reportedly there have been over 100 3-digit MNCs allocated in the MCC 405, mixed with 2-digit MNCs (see Appendix C). However, overlap between the two first digits has been avoided: the first two digits of the assigned 3-digit MNCs never overlap with an assigned 2-digit MNC. While we must assume that the Indian situation is working without significant problems, we have not been able to find additional evidence on this. Contact with the CEO of an Indian GSM network equipment vendor indicate no known problems with 3-digit MNCs in India while using it at a very large scale and with many different mobile phones.

In 2013 and 2014 there were some additional studies conducted in NL [12] and Sweden [13] related to three-digit MNC (and shared MNCs). The common conclusions were that it should be possible to introduce 3-digit MNCs. However, the 3GPP statements remained a blocker for implementing these.

In 2021 PTS sent out a referral, see also section 1.1, and the participating mobile system provider (Ericsson) in principle agreed that it should be possible to introduce 3-digit MNCs [68]:

"Although mix of 2- and 3-digit MNC are implemented in some countries and in principle this option should work, it is unclear if all vendors (Network as well as UE) support mixing as 3GPP recommends against it".

The approach by the MNOs was mixed. One major MNO was against a mix with reference to the 3GPP considerations. No information on why it should not be possible was presented. Another major MNO stated that it should not be any technical problem to mix 2- and 3-digit MNCs. In the parallel Nkom study in Norway[15], the same MNO promoted an introduction of 3-digit MNCs.

8.3 Implementations and Experiences

At the time of the 2013 [10], [12] and 2014 [13] studies, there were one critical reference case for mixing 2- and 3-digit MNCs, India as presented in the previous section. As of today, we have not obtained any information that any specific problems have occurred. Further roaming with India has been working for a long time.

In 2018, France introduced 3-digit MNCs for NPNs (5xx series) and Broadband Internet Access (7xx series) respectively. According to Arcep no problems have been encountered thereafter. The French usage of MNCs can be retrieved from the Arcep website [62].

For the NPN 5xx series, Arcep also applies an internal two-digit code (after the MNC in the list above) to define in what French department[16] the NPN resides. The MNCs within a specific department will then be spread among the MNCs in the allocated series. Thus, 100 MNCs are supported within a department. Further, a specific MNC may be reused in another department. Thus, these MNCs can be seen as shared MNCs with no distinctive individual ID in the 3GPP context.

The fact that either 2- or 3-digit MNCs can be used for MCC 999, is another indication that a mix shall be possible.

Finland has allocated the 8xx series for 3-digit MNCs but this has not been taken into use. No technical analysis has been reported.

8.4 3GPP Specifications

The broadcasted PLMN ID has for a long time been set to consist of 3-digit MCC and 3-digit MNC. In case that the assigned MNC consists of two digits, an ´F´ (hexadecimal 1111) shall be inserted at the end [42].

The User Equipment (UE) will check the broadcasted PLMN ID vs information stored in the SIM card [45]:

- The IMSI is stored in a 64-bit (8 bytes) field, there 4 bits are allocated for parity etc. There are 60 bits left for the IMSI. Thus, up to 15 hexadecimal digits are supported. The field can be of variable length, length of IMSI is defined separately and IMSI of less than 15 digits shall be encoded so that unused digits ("nibbles") shall be set to ´F´.
- The Administrative data includes the field, "length of MNC in the IMSI". The UE will then be able conclude if the IMSI consist of 2- or 3-digit MNC. This field was added in 1998 and serves as an important milestone for supporting 2/3-digit MNC mix. Only equipment manufactured before 1999 should then have associated limitations, and these should be outdated by now.

---

[15] Documentation obtained from Nkom
[16] "Départements" are the second-tier administrative subdivisions of France, below the regions. Departmental numbers are widely used in France to designate locations. They form the first two figures of any French postcode. Source: https://about-france.com/french-departments.htm

- For Equivalent HPLMNs, Preferred PLMNs, Forbidden PLMNs etc lists, the MCC and MNC is presented in 3 bytes = 3+3 digits. For 2 digit MNCs a trailing 'F' shall be applied.

Thus, the UE will have all data at hand to conduct a network selection in networks with 2/3-digit MNC mix. The criteria for matching HPLMN, retrieved from Annex A of the 3GPP NAS specification [42], are outlined in *Figure 13* below.

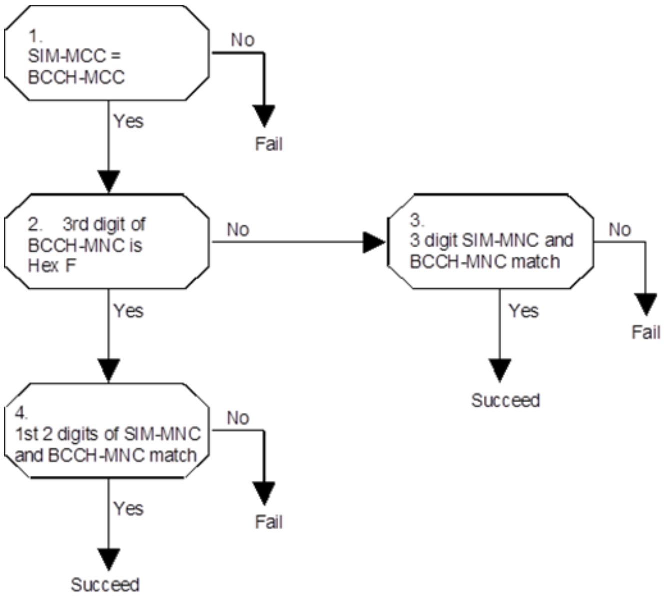

Figure 13. 3GPP HPLMN matching sequence [42]

Matching data for the other lists is not defined in detail but will have to follow the same type of principles:

1. Read the broadcasted MCC and MNC (as part of identifying the PLMN)
2. Match this information towards the data in the lists on the SIM card. The format will then be the same with ´F´ used as the third digit for 2-digit MNCs.

Upon network registration the UE will have to provide the Subscription Concealed Identifier (SUCI) in 5G, or IMSI (pre-5G) to the selected network. The Subscription Permanent Identifier (SUPI) is the vital part of the SUCI as to identify the HPLMN. The HPLMN is the receiver of the SUCI information to be used for authentication and authorization. For 5G the SUPI can be in two formats:

- IMSI, the traditional format
- NAI (Network Access Identifier), string format user@HNI where MNC is part of the HNI (Home Network Identifier).

If IMSI is provided (either in 5G-SUPI or separately), the MNC is provided as three digits with a trailing ´F´ for 2-digit MNCs, see "Mobile Identity" in [43], [44], [47].

If the SUPI is provided in NAI format (SNPNs only), the MNC is also represented by three digits. As these are alphanumeric characters, there is a leading ´0´ for 2-digit MNCs.

The Home Network Identifier for a SNPN with 5GC-NID, see section 9.2, will look like:

5gc.nid<NID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The subsequent roaming communication with associated session and charging handling should be working as the initial SUCI communication is accomplished (from an MNC perspective). The fact that roaming with operators using a 2/3-digit mix is working, is further evidence that a mix is handled by existing equipment and systems.

8.5 Use Cases

If we consider UEs not working as they should in terms of separating 2- and 3-digit MNCs, the problem could be limited by ensuring that the 2- and 3-digit series do not overlap. Thus, 2-digit MNCs cannot be in the range of the 3-digit ones, e.g. if MNC 75 is used, the whole 7xx series is blocked. This has been the thinking for a long time, e.g. T-Mobile (NL) highlighted that this would be working in 2012, please see section 8.2. They have also confirmed that this is still their opinion. Our understanding is that the 3GPP considerations were related to a general case not considering non-overlapping 2- and 3-digit series. This is reflected in the following statement in the 3GPP reply [9] to the ITU-T TSB Circular 285 [67] in 2012:

"The mixing of 2-digit and 3-digit MNCs in a single MCC would therefore have a major impact on the existing 3GPP specifications and existing implementations, based on fixed length of MCC+MNC, will identify the wrong PLMN <u>if there is an overlap of 2-digit and 3-digit MNC allocation plans</u> in a given MCC."

Considering specific use cases, see also section 4.2 for a technical background:

- A legacy UE belonging to a PLMN with 2-digit MNC will not have a problem to identify and access its home network. Further, as there is no overlap with the 3-digit MNC network the UE will not be blocked to access it´s home network. I.e. the situation will not occur that the UE will incorrectly relate the 3-digit MNC network to be the HPLMN resulting in a cause value to block the UE for attempting to connect to the HPLMN.
- If an UE belonging to 2-digit MNC network would need to roam to its HPLMN from a 3-digit network this should technically work as long as the network will resolve the 2-digit MNC provided in the IMSI, which is to be expected. The main problem is if the UE will first unsuccessfully try to roam to another network with an MNC in the same 3-digit series as the desired network, the corresponding 2-digit PLMN ID will be inserted into the FORBIDDEN PLMNs list.
- Since the 3-digit MNCs will be allocated to new networks, they will have to comply with 2/3 mix handling. Any problems will have to be handled by the 3-digit network owners.

As there is a complete generic support for a mix, no specific limitations have been identified related to applications and actors. Thus, 3-digit series would not have to be limited to NPNs. I.e. they could also be used for new MNOs etc.

8.6 Findings

The intended direction by PTS to allocate the 8xx and/or 9xx MNC series for 3-digit MNC seems to be a solid direction. The 3GPP systems are designed to separate between 2- and 3-digit MNCs end2end. By further ensuring non-overlapping MNC series, this has been claimed to work for a long time.

Further, PTS is encouraged to urge 3GPP to update the specifications as to remove that a 2/3-digit mix is not recommended. The ways to do it are discussed in chapter 14.

9 Un-coordinated vs Shared MNCs

There are two major MNC options for SNPNs, not accounting for own MNCs:

- Un-coordinated, implying that specific MNCs can be selected by the SNPN owners free of choice. I.e. the same MNC can be used without any coordination from NPAs as PTS.
- Shared MNCs, implying that specific MNCs are split into sub-networks based on the MSIN part. The sub-network allocation and assignment must then be coordinated by some instance.

These concepts and associated considerations are penetrated. The upcoming network identifier for 5G SNPNs, 5GC-NID, will play a central role. The usage and implications of 5GC-NID introduction are elaborated.

It is found that the un-coordinated MCC 999, is the most relevant choice onwards. However, there is a related coordination need as to avoid MNC interference between nearby MNCs.

9.1 Basic Considerations

As of today, Swedish SNPN owners can either select global MCC 999 with any MNC or they can select MCC 240 (Sweden) and one of allocated MNCs 65 or 66. We denote these as un-coordinated MNCs as the network owners will be responsible themselves in terms of selecting the MNC to be applied. PTS does not keep track of the MNCs being used.

Shared MNCs described further in this chapter, has been introduced in recent years for a number of applications. These, on the other hand, require a central administration. The main question is the level of the administration to apply as further elaborated below.

One critical development, affecting both options, is the introduction of a Network ID (5GC-NID) in 5G as presented below.

9.2 5G SNPN Network Identification

For 5G only, the 40-bit Network ID (5GC-NID) was introduced in 3GPP R16. 5GC-NID combined with the MNC constitute the SNPN ID uniquely identifying an SNPN. It shall be noted that 5GC-NID establishes a clear separation between all SNPNs. Thus, each SNPN should be able to use the complete MSIN space.

There are three options for assigning the 5GC-NID.

- *Assignment Mode 0 – IANA Private Enterprise Number (PEN).* In this mode, a PEN as assigned by the Internet Assigned Numbers Authority (IANA), is used as the NID to ensure global uniqueness. The IANA assigned PEN is 32-bits, with the remaining 8-bits as NID Code used to distinguish up to 256 networks.
  - The list of PENs can be found at [63].
  - PENs can be obtained using the form at [64].
- *Assignment Mode 1 – Self-Assigned*. Not recommended as global uniqueness cannot be guaranteed.
- *Assignment Mode 2 – Globally Unique with PLMN-ID*. The NID and the PLMN ID combination must be globally unique. I.e. the administrator of the related MNC(s) will have to define separate NIDs within each MNC context.

Assignment Mode 2 (AM=2), has been adopted by e.g. CBRS (US MCC), MFA (global MCC 902) and the German NRA (BNetzA), see section 9.4 and chapter 12. This allows for a simple administration as the NIDs only need to be unique within the MNC.

Assignment Mode 0 (AM=0), on the other hand ensures global uniqueness in itself. The SNPN owners could/should then apply for the PEN themselves. This is applicable for un-coordinated MNCs as described below.

It is the administrator of the MNC who sets the conditions for what AM to apply for an MNC. AM=2 can only be applied for central administration cases as to avoid that the same 5GC-NID will be used. With AM=0, there is a complete freedom whether the administrator of the MNC or the SNPN owners shall apply for the PEN.

Thus, 5GC-NID is the mechanism to identify 5G SNPNs. However, 5GC-NID is not supported in UEs and mobile systems yet. This is surprising as the R16 specifications were frozen in late 2020 and traditionally it takes some 18 months to implement a release. The delay is most likely related to the fact that there is limited support for SNPNs from the large number of MNOs, being major customers of mobile systems and components. The indications are that 5GC-NID support will be generally provided in 2025.

The SNPN ID (PLMN + NID) [40], will be broadcasted as to identify the private network. Further, the SIM card will store SNPN ID tuples as to select or block specific networks. The NAI format for HNI e.g. for SUPI/SUCI also includes the 5GC-NID:

5gc.nid<NID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org

However, the roaming interfaces have not been updated to support NID, despite that there should be limited work as to achieve it, see section 7.2. Since major enterprises now indicate an increasing interest in roaming, the final step to have a complete support for SNPNs should be accomplished soon.

9.3 Un-coordinated MNCs

Since Apple will now support MCC 999, see section 7.5, this should drive a large adoption of MCC 999. Apple might support the Swedish MNCs 65 and 66 future wise. In any event MCC 999 is more attractive as offering substantially more MNCs.

MCC 999 has been default option for SNPNs lately. Hence, one should expect that this would be the primary target also for other equipment manufacturers than Apple.

The 5GC-NIDs, can be introduced for un-coordinated MNCs by the SNPN owners themselves. Further, the whole MSIN space can be reused between SNPNs, which is not the case for shared MNCs, see section 9.4. Thus, we foresee that un-coordinated MNCs will be the main track vs. shared MNCs onwards.

However, roaming is currently not supported as further elaborated in section 9.6. This could be handled by 3-digit MNCs and other approaches outlined in section 5.2.

Without the 5GC-NID support, MCC 999 will in any event not be able to support roaming as highlighted in [32]:
"The MNCs under MCC 999 are not routable between networks. The MNCs under MCC 999 shall not be used for roaming"

9.4 Shared MNCs

9.4.1 Sub-network Handling

The concept of shared MNCs has been on the table since the NPN discussions started. The approach is simply to divide the MSIN part into two sub-fields:

- IMSI Block Number (IBN) which will identify the "sub-network"
- User Identification Number (UIN), which will identify a specific user within the specific sub-network

One basic question is how to divide the MSIN into IBN and UIN. Two-digit MNCs yields a larger space than 3-digit MNCs, as 10 digits are available for the MSIN. A 4 digit IBN yields a support for 10k sub-networks with up to 1M users.

Some examples of well-known adoptions of shared MNCs are CBRS and MFA. The German and Norwegian NRAs have also assigned shared MNCs. In 2021, PTS had a working assumption for introduction of shared MNCs, but this was not implemented. The IBN/UIN splits for these applications are outlined in Table 1.

Table 1. IBN/UIN applications

Application	Number of digits MSIN/IBN/UIN	Number of sub-networks	Number of users
CBRS	9/4/5	10k	100k
MFA	10/6/4	1M	10k
Germany	10/6/4	1M	10k
Norway	10/5/5	100k	100k
Sweden (assumption)	10/4/6	10k	1M

The number of networks supported within one MNC is then at least 10k, which is by far exceeding the number of networks supported by 3-digit MNCs. However, the latter approach will support roaming which is currently not the case for shared MNCs.

9.4.2 Managed IDs for Shared MNC Networks

Since the shared MNCs are not unique, there must be other information to identify each sub-network within an MNC. Thus, some kind of "Network ID" (NID) is needed.

For 5G, the 5GC-NID will be available as presented in section 9.2. The 5GC-NID will then see to that the sub-networks will be uniquely identified to support network selection. As highlighted in some other sections of this document, some parts are missing in the 3GPP specifications as to achieve a complete end2end handling of roaming. The lack of roaming support is then a main consideration.

For LTE there is no generic "NID" defined by 3GPP, and some other parameters will have to be used. The common approach from CBRS and MFA is to use the Closed Subscriber Group ID (CSG-ID) as to serve as "NID". For CBRS this is denoted as CBRS-NID. The CSG-ID/CBRS-NID is then broadcasted as System Information.

The UEs (SIM cards) will have to be configured with the allowed CSGs to be related to the home PLMN ID, in CBRS denoted as (Shared) Home Network Identifier

(HNI/SHNI). The UEs should NOT try to connect to other CSGs than the one(s) allowed in the UE.

However, CSG checking may not be enabled for all UEs due to power constraints. From [49] page 8:

"Few LTE UEs support the CSG-ID mechanism, due to power consumption impacts of supporting CSG-IDs, and lack of demand from the Mobile Network Operators (MNOs). As such, an LTE UE configured to use the CBRS Shared HNI will attempt to connect to any network using the CBRS Shared HNI, regardless of the CBRS-NID broadcast by the network. This will result in OnGo[17] networks using the CBRS Shared HNI having unrecognized devices attempt to connect."

Since a general support of CSG-ID cannot be established, there are some other coordinated LTE IDs within a shared network with a common HNI.

• *Tracking Area Identifiers (TAIs).* The LTE systems need to know where the UEs reside, as to be able to contact (page) them when new incoming calls/connections are to be established. The systems keep track of the Tracking Area in which the UE currently resides. The Tracking Area ID (TAI) needs to be locally unique, with no neighboring systems using the same value. The TAI is composed of the HNI (PLMN ID) plus a 16-bit Tracking Area Code (TAC). As the HNI is shared, the TAC part will have to be unique (between nearby networks with the same HNI).

• *E-UTRAN Cell Global Identifier (ECGI).* Every LTE base station (eNodeB) shall be uniquely identified by an ECGI that is composed of PLMN-ID (HNI) and Cell ID. Thus, unique Cell IDs will have to be established.

• *MME ID (GUMMEI).* Every Mobility Management Entity (MME) in an LTE system requires a Globally Unique MME Id (GUMMEI). Because it contains the Shared HNI as a prefix, the 24-bit MMEI values must be coordinated within the Shared HNI.

Table 2. *CBRS 4G/LTE identifiers [49]*

Identifier	Assigned by...			Identifies	Quantity
	IMSI Admin	OnGoA	OnGo Operator		
IMSI	MCC+MNC (SHNI) + IBN	—	UIN	Subscription	10,000 IBN x 100,000 UIN per SHNI
CBRS-NID (LTE & NR[2])	—	CBRS-NID (Conditional[3])	—	Network	2^{27} per SHNI[4]
GUMMEI (LTE Only)	SHNI	MMEGI	MMEC	MME	2^{16} MMEGI x 2^{8} MMEC per SHNI
ECGI (LTE Only)	SHNI	eNB ID	Cell Identity	Cell or sector (eNodeB)	2^{20} eNB ID x 2^{8} Cell Identity per SHNI
TAI/TAC (LTE Only)	SHNI	Optional (see §5.7.2)	IBN-derived TAC (see §5.7.1)	Tracking area	65,534 per region of overlap

[17] The CBRS Alliance uses the OnGo name as its consumer-facing brand.

For 5G networks, that don’t support the R16 5GC-NIDs, the corresponding set of identifiers would have to be coordinated (by the same body that handles the 4G ones):

- *5G Tracking Area Identity (TAI) with Tracking Area Code (TAC).*
- *NR Cell Global Identity (NR CGI).*
- *AMF-ID (GUAMI).*

Whereas the CSG-ID consists of 27 bits, the 5GC-NID consists of 4 (mode=2) + 40 (value) bits. CBRS proposes for operators deploying both LTE and 5G NR networks, that the CBRS-NID may use the rightmost 27 bits of the 5GC-NID.

9.5 Basic UE Behavior

9.5.1 ”Do not knock on other networks”

The starting point is that UEs shall not try to register in other SNPNs, unless they are listed as “preferable networks”. The 5GC-NID supports a traditional network selection, i.e. the networks are selected in the same manner as for public networks. The difference is that the networks are selected on the SNPN ID (PLMN ID + 5GC-NID), and that the UE shall be in *SNPN access mode*. How the UE shall enter SNPN access mode is however outside the scope of the 3GPP specifications.

Thus, 5GC-NID UEs shall only try to access their home SNPN. Their SIM cards will constrain their SNPN registration attempts to the home SNPN. It should be noted, that UEs could be equipped to also support access to a public network.

UEs not capable of handling the 5GC-NID will handle the network selection in the same way as they handle it for public networks. I.e. these UEs will only consider the traditional PLMN ID information.

As discussed in the previous section, there is no standardized “NID” for 4G/LTE. Organizations like CBRS and MFA[18] have adopted the Closed Subscriber Group ID (CSG-ID) as to serve as a NID. If all UEs belonging to different networks with a shared MNC have CSG-ID enabled and restricting SIM card information, these will only try to connect to their home SNPN.

However, it is noted in the CBRS specifications that CSG handling in the UEs are battery consuming. Thus, non SNPN 4G/LTE UEs would to a large extent have CSG disabled. Public network UEs could then be blocked to access the 4G/LTE SNPNs in the same way as for national roaming.

Alternatively, the number of tries will be limited depending on the returned cause value as outlined in the next section.

9.5.2 “Continue to knock on other networks”

In the event, that SNPN UEs are “incorrectly” knocking on the door to other SNPNs, with the same MNC (shared or un-coordinated), these shall NOT be blocked to try to knock on the door to the home SNPN (and other SNPNs with the same MNC as to find the home SNPN).

The way to accomplish this is to generate “soft” cause values e.g. #15 (see section 4.2), as described in the CBRS specifications [48], see *Figure 14* below. This is applicable for 4G/LTE SNPNs, and nearby networks with the same MNC must NOT use the same TAC.

The drawback with the soft cause values, is that non SNPN UEs could also continue to knock on the doors to other SNPNs. However, this would only occur in roaming situations and well known SNPN MNCs could be part of the FORBIDDEN PLMNs list.

---

[18] CBRS and MFA are presented in chapter 12.

5.5.3.1 REJECTING ACCESS ATTEMPTS BY A UE WITH IMSI NOT BELONGING TO NETWORK USING CBRS-I

The EMM cause used for ATTACH REJECT, TRACKING AREA UPDATE REJECT and SERVICE REJECT by a CBRS network's EPC identified by CBRS-I and connected to a hybrid CSG RAN [17] shall be Cause #15 defined in 3GPP TS 24.301 [5], when the associated UE uses an IMSI that does not belong to the network. Exceptions to this requirement include but are not limited to:

- security attacks by the UE,
- the UE is determined to be stolen using ME identity check procedure (see section 5.3.10.5 of 3GPP TS 23.401 [14]),
- repeated unsuccessful access attempts by the UE,
- the UE causes excessive signaling.

Note : Use of other EMM cause values (e.g., Cause #3, Cause #8) can cause the UE to suspend access to all networks broadcasting CBRS-I, including networks where the UE's USIM based subscription is accepted (see section 5.5.1.2.5 of 3GPP TS 24.301 [5]).

Note : When using the EMM Cause #15, TACs of nearby networks should be coordinated to ensure that nearby networks do not use same TAC. When two nearby networks use the same TAC, a UE belonging to one of the networks on receiving a reject from other network with above cause code will temporarily not attempt access to its home network.

A CBRS-Profile I UE can be enhanced so that it does not connect to a hybrid cell [17] to register with an EPC identified by CBRS-I if the cell broadcasts a CBRS-NID that is not in the UE's CSG list. However, this requires that the lists are well maintained. If the lists are not well maintained, the enhancement can result in the UE not connecting to its home network.

Figure 14. CBRS cause value handling [48]

9.6 Roaming

There has been input from various sources indicating that there is an increasing demand for roaming for NPNs. Further, a major Nordic MNO actively stressed the roaming needs (and pushed for 3-digit MNCs) in the Nkom referral 2021 [6].

Currently, roaming is not supported for SNPNs without own MNC. As stressed in other sections in this chapter, the only way forward in terms of roaming is 5GC-NID. Although not supported today there should be limited work needed to technically achieve a roaming support for 5GC-NID SNPN.

There are also other approaches as Credentials Holder and underlay/overlay networks supported in R17- to accomplish substitutions to roaming. However, they introduce other implications. Please see section 5.2 for further details.

9.7 5G vs 4G Considerations

As described, 5GC-NID is the only way forward to accomplish complete NID support for shared and un-coordinated MNC SNPNs. However, 5GC-NID support is not available in the market yet. No clear target date has been presented due to competition aspects. The indications are that 5GC-NID should be available in 2025.

Since 5G is generally presented and perceived as superior to 4G, 5G should be the obvious choice for SNPNs. However, there are some current 5G constraints, that promotes a co-existence of 4G and 5G for SNPNs for some years ahead. The following features are still lacking for 5G.

- Stand alone capabilities
- Voice i.e. VoNR
- UE functionality as e.g. only supporting 4G

Installed NPNs could have some 4G limitations not to be overcome by migration efforts. They will then not fully benefit from the NID handling. As new SNPNs will have a complete 5GC-NID handling at some point, those UEs will not try to access the other SNPNs (in SNPN access mode).

New NPNs with 4G components, to be considered for new shared MNC handling, should on the other hand be expected to be able to be migrated to 5G-SA in some years.

There are also cost considerations that would promote adoption of 4G only equipment. Thus, one could expect that 4G will be applicable for some years ahead.

9.8 5GC-NID Migration Considerations

The migration to 5GC-NID handling is the foundation for the SNPN management onwards. System wise the migration should be straight forward. The UE migration on the other hand could have some implications.

First the UE will have to be upgraded as to support 5GC-NID handling. Then, the SIM cards will have to be updated with the associated information as to select the SNPN applying the SNPN ID. This should be accomplished with Over The Air (OTA) updates.

However, provisioning of (e)UICCs ("SIM cards") is not a trivial thing, one needs to be certified by GSMA before allowed to do so. Most of the enterprises, especially SMEs are not certified and will require a partner support. ETSI is currently working on how to make this process easier.

Another method is the Steering of Roaming (SoR) mechanism which allows providing a controlled list (Steering Information List) containing preferred and forbidden PLMNs/SNPN(s) to the UE via a secured NAS container from UDM during or after registration. SoR was introduced to update UEs in an e2e encrypted manner, which means that a VPLMN cannot read or change the content of the container. This is not straight forward, as both UE and network must support it.

9.9 Findings

It is evident that the mid- and long-term path for SNPNs spells 5G. Within some years, 5G will at least have the same support for applications (incl. voice) and UEs as for 4G as well as SA support. Further, a native NID handling is only supported by 5G, expected to be available in 2025. The 5GC-NID also allows for a full MSIN overlap.

The recent Apple support for existing un-coordinated MNCs, primarily global MCC 999 with any MNC, should generate a substantial interest for such solutions. This is further strengthened by the fact the SNPN owners will be able to introduce 5GC-NID when applicable. The SNPN owners will be able to administer the 5GC-NIDs themselves, by registering their unique 5GC-NID via IANA and apply it subsequently.

Since the full MSIN space can be reused between SNPNs with 5GC-NID, there should NOT be any demand for shared MNCs.

However, 4G (in combination with 5G) will be applicable for some years ahead. The network owners should be motivated to migrate away from 4G, as long as there are no considerable cost impacts. It is difficult to estimate when SNPNs should be expected to fully support 5GC-NID. From the other end, future SNPNs for Localized Services etc will need the 5GC-NID.

The question is what role PTS should take when continuing to support an un-coordinated MNC approach. Until a pure 5GC-NID handling will be established, the primary target is to see to that nearby SNPNs will not adopt the same MNC. It shall be noted that MCC 999 offers about 1,000 MNCs, to be compared with two Swedish MNCs, 65 and 66. Most likely, the interest for the Swedish MNCs will diminish for new installations.

Some kind of MNC coordination is then needed as addressed by CEPT:

> *"In order to manage potential network attachment issues, NPAs may consider encouraging industry stakeholders to lead on a national coordination regarding the use of MNCs under MCC 999"*

However, we see that this should be handled within a new NPN/NHM forum to be established. Please see chapter 14 for further details.

10 Neutral Hosts Networks

Neutral Host Networks (NHNs) has gained a lot of attention internationally. The impact on MNC needs is of thus of major interest. This chapter presents the NHN concept, implementation options and impacts on the MNC needs.

10.1 NHNs and Shared RAN options

Analysys Mason (AM) summaries the need for indoor coverage in [19] as:

"With continuing adoption of 5G services, customers are increasingly demanding in their expectations for the speed and availability of connections in all locations, not least in indoor environments. Building owners also consider that unified, predictable, and futureproof in-building digital infrastructure is a key value proposition to their tenants, as well as an enabler for their own digital transformation. It is clear that these expectations will not be met by existing networks and require instead a new dedicated 5G indoor solution. Neither distributed antenna systems (DAS), nor outside-in coverage from macro sites, nor Wi-Fi 6G can deliver that seamless, reliable, gigabit experience."

Thus, the building owners have an incitement to take control of the digital infrastructure of their buildings with state-of-the-art 5G small cell technology.
AM refers to the building owners industry group REDI and states:
"In short, Swedish building owners see 5G as a vital and integral part of the future building infrastructure, just like water and electricity."

AM refer to the REDI conclusions as follows, please also see the REDI report [20].

- *Predictable coverage, capacity and speed of the service in the whole building.*
- *High-performance 4G and 5G - indoor user experience should be as good as outdoor with the high-speed 5G subscriptions that now are offered in most markets.*
- *One network and one party to manage the network. Building owners would like to avoid having 3-4 networks from different service providers as this would drive up costs, affect the look and feel of the buildings, and increase management overheads for building owners.*
- *All or most of the MNOs should have the ability to connect to the network and provide service.*

Thus, the building owners are willing to take the cost for the infrastructure and provide it to the MNOs as open networks referred to as Neutral Host Networks (NHNs).

Small Cell Forum (SCF) defines Neutral Host in [22] as:

"A provider of venues and value added equipment and services to help mobile operators extend and enhance the delivery of mobile services to their subscribers, indoor and outdoor. Neutrality means the offer is made on a fair and equal-opportunity basis to all tenant MNOs."

The SCF report presents the evolution from legacy RAN sharing models to the modern small cell ones:

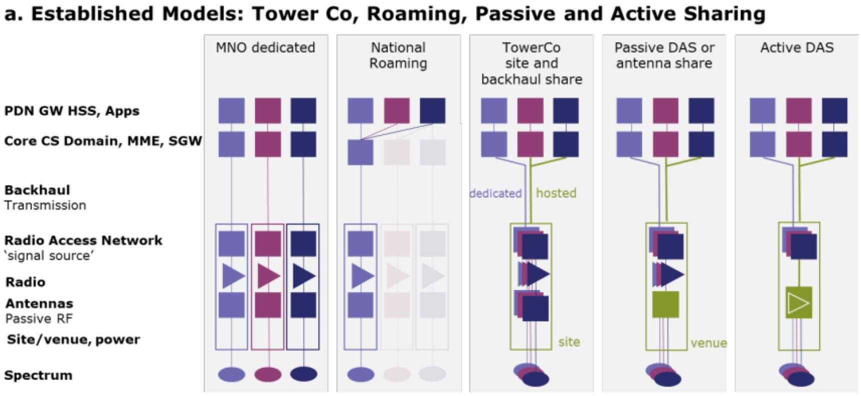

Figure 15. Legacy shared RAN options [22]

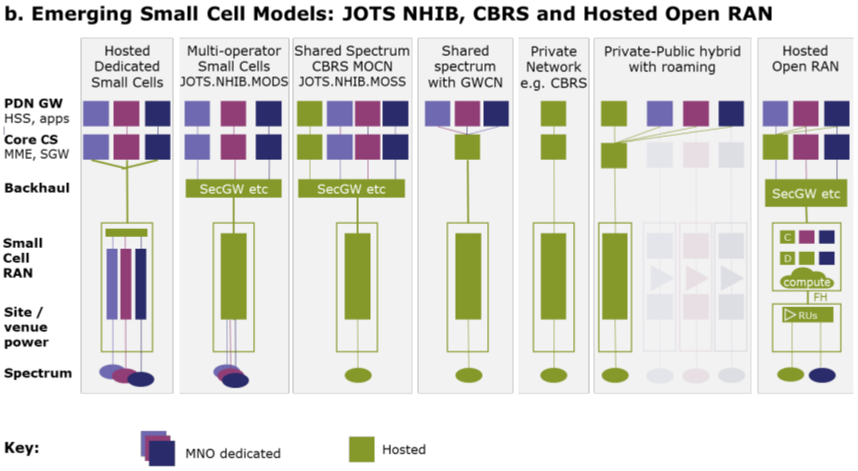

Figure 16. Small cell shared RAN options [22]

As 5G small cell technology e.g. offers precise location information, one would expect that DAS solutions would be ruled out by the MNOs by now. However, it seems that is not the case as IKEA will be provided with a DAS solution for indoor coverage as communicated on 4 April this year [65].

According to a NHN provider, Sweden is lagging behind Norway in terms of NHN adoption. This can be tracked to both technology choices and openness for NHN solutions. Hopefully, the transition period to establish trust for NHNs will be short as there are substantial cost savings to be made for the MNOs as well as state-of-the-art solutions can be provided to the end customers. The NHN announcement from 3 is some indication of a rising MNO interest [66]. Please see the AM report [19] for further details on the overall NHN approach.

As shown in *Figure 16* above, there are some different options on how to share the RAN. The alternatives as such, are outside the scope of this document. From an MNC perspective the key part is, to what extent the NHN will also provide local services. This yields that NHN will need an own MNC. These implications are not addressed by the SCF report when addressing shared RAN options (from a pure NH perspective). However, the report relates to the CBRS specifications [48] (4G/LTE technology) including local services as shown in *Figure 17*. Please also note the local networks outlined in section 5.2.

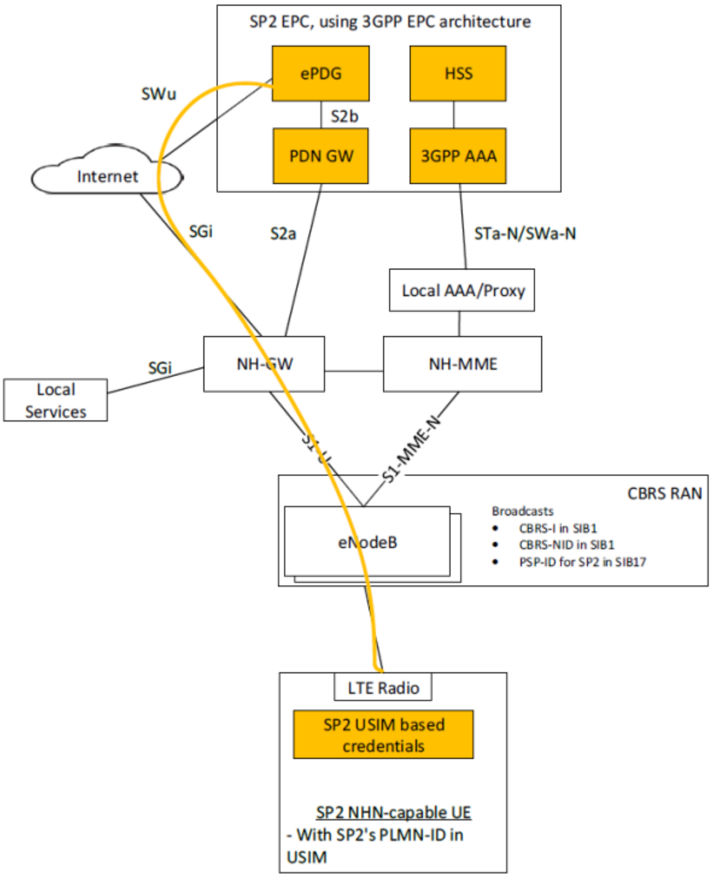

Figure 17. CBRS 4G network core diagram [48]

In this survey, input on to what extent local services would be offered via the NH was requested. No input was obtained as to indicate a market evolution in this perspective. This may seem surprising at a first glance, as precise location services should be of great interest in many cases. Directions on where to find a specific place in shopping malls, airports, hospitals etc. should be of large interest. A particular example would be IKEA (as presented above) providing directions to their customers, using any MNO, based on the current location in the shops.

These services could however reside in the cloud and be reachable via the MNOs.
In addition, there seems to be a tradition that the Swedish MNOs cooperate on big installations as to achieve shared RANs. Hence, so far there has been no room for NHs. As the estate owners, now has a desire to take control of the digital infrastructure etc, a change is expected to take place.

The local networks will need MNCs. Since there should not be any roaming implications, no dedicated MNCs should be needed.

As addressed in other sections, the provisioning of credentials to the local networks is an outstanding item.

10.2 Dual Connectivity

The ATIS NHN document [25][19], highlights how multiple UPFs can support NHN implementations. Dual connectivity can then be established for single UE.

"Multiple UPFs (User Plane Functions) can serve the same UE. For example, UEs concurrently accessing two (e.g., local and central) data networks using multiple PDU Sessions is illustrated in Figure 18. This figure shows the architecture for multiple PDU Sessions where two SMFs are selected for the two different PDU Sessions. However, a single SMF may also have the capability to control both a local and a central UPF within a PDU Session. <u>This use of multiple UPFs can be advantageous for some Neutral Host architectures since both the Neutral Host as well as the hosted client network are now able to terminate traffic from a single UE simultaneously</u>."

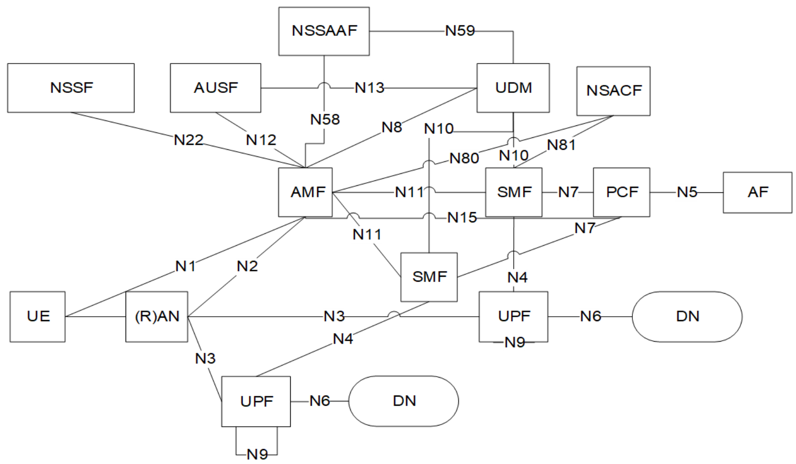

Figure 18. 3GPP non-roaming 5GC reference architecture, multiple UPFs, dual SMFs [40]

"In addition, the 5GC architecture also supports concurrent access to two (e.g., local and central) data within a single PDU Session through the use of two UPFs in series. This architecture is shown in the Figure 19. <u>As in the previous case, this architecture may also be of interest in 5G Neutral Host deployments where both the Neutral Host as well as the hosted client network.[20]"</u>

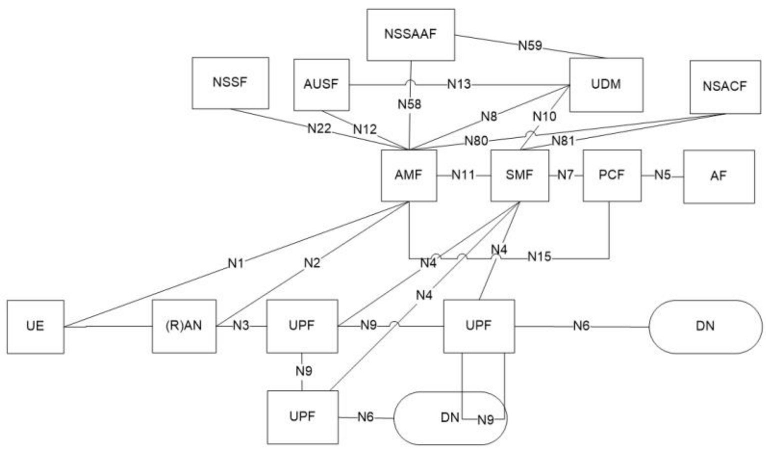

Figure 19. Non-roaming 5GC reference architecture, multiple UPFs, UPFs in series [40]

[19] Figure 18 and Figure 19 are obtained from the R18 specifications whereas [26] presents older versions.
[20] The sentence seems to be truncated in the original document. It should end with: are now able to terminate traffic from a single UE simultaneously (as for the previous example).

11 Total Need of MNCs

11.1 SNPNs

As discussed, the major driver for MNCs is SNPNs. There is then a total need for NPNs to start with, to be further divided into the PNI-NPNs and SNPNs shares.

In this study, inputs on the expected market growth figures for NPNs were requested. However, very limited input was received due to competition aspects. The single input received, indicates a CAGR of 25-40% for NPNs. Further, the SNPN part has been estimated to some 20%.

In the discussions with the system providers, it has been stated that the uptake of SNPNs has been considerably lower than expected. This is e.g. related to the complexity of 4G/5G systems vs WiFi and limited sales channels to the SME market. Thus, PNI-NPNs provided by the MNOs have dominated so far.

As of November 2023, there are 87 local radio licenses in Sweden. A rough estimation yields that there is maximum some 50 SNPNs for business operations. A CAGR of 40% would then yield some 270 SNPNs in five years' time. Of those, there will be existing SNPNs not applicable for the future MNCs covered in this document.

On the other hand, if the SNPN part will grow a higher number will be estimated. With a 20% share, the total number of NPNs (SNPNs and PNI-NPNs) would today be around 250. A 40% CAGR would yield some 1.350 NPNs in five years' time. If the SNPN part would be 30%, this would result in some 400 SNPNs in total.

In any event, these are only loose estimates.

11.2 Others

None of the respondents indicated that they have recognized other (substantial) needs for MNCs other than SNPNs.

12 International Outlook

12.1 Europe

12.1.1 Germany

In February 2022 Bundesnetzagentur (BNetzA) introduced the new shared MNC 262-98 for Campus Networks / NPNs. The MNC is divided into 1M sub-networks (6 digits) each supporting 10k subscribers (4 digits).

BNetzA administers the full set of 4G and 5G IDs in the same way as for CBRS and MFA. Please see section 9.4.2 for details.

BNetzA analyzed the advantages and disadvantages of introducing 3-digit MNCs in 2015. However, a conclusive assessment of the risks and uncertainties connected to the introduction of 3-digit MNCs was not possible at this time according to BNetzA, referring to Communication Nr. 982/2015 of 26.08.2015; Official Gazette Nr. 16/2015, p. 2337, 2370 f.

The German Federal Ministry for Economic Affairs has published "Guidelines for 5G Campus Networks – Orientation for Small and Medium-Sized Businesses" [21]. This should stimulate 5G NPN implementations.

12.1.2 France

In 2018, Arcep introduced the 3-digit 5xx series for NPNs. No problems have been identified in relation to the mix of 2- and 3-digit MNCs.

The MNC assignments can be retrieved from [62].

For the NPN 5xx series, Arcep applies an internal two-digit code (after the MNC in the list above) to define in the French department where the NPN resides. The MNCs within a specific department will then be spread among the MNCs in the allocated series. Thus, 100 MNCs are supported within a department. Further, a specific MNC may be reused in another department. Thus, these MNCs can be seen as shared MNCs with no distinctive individual ID in the 3GPP context.

12.1.3 UK

Ofcom has not allocated any MNCs specifically for NPNs yet. Investigations are ongoing. So far Ofcom has been referring to MCC 999, which is line with the conclusions of this document.

UK is also in favorable position as two MCCs, 234 and 235, have been assigned to UK.

12.1.4 Netherlands

The NL MNC administration is somewhat special as it is divided between the Ministry of Economic Affairs (MinEZ) and Authority for Consumers and Markets (ACM). The former is responsible for the regulation and policies (NRA) whereas ACM handles the assignments (NPA).

NL was very active in the MNC area around 2013/2014 with a number of investigations (and CEPT WG NaN / ITU-T SG2 contributions).

NL early targeted implementation of 3-digit MNCs and allocated some series for those. One company (Shyam) was assigned a 3-digit MNC, but that was later withdrawn because of concerns regarding the feasibility of mixing 2- and 3-digit MNC's. Currently there are no assigned 3-digit MNCs.

However, in the NL input to this study, it is stated that:
"The conclusion is that no handset problems are to be expected if two- and three-digit MNCs are mixed under the same MCC."

NL early adopted shared MNCs applying the HLR Proxy Provider approach. MNC 90 and MNC 91 were allocated for this purpose. MNC 90 has been handled by ACM whereas MNC 91 was assigned to an energy grid operator. However, the HLR Proxy Provider approach has not been applied for any of these MNCs.

MNCs 95, 96 and 97 are assigned to NPNs for which an un-coordinated handling is applied. I.e., the NPN owners are free to select any of these MNCs.

12.1.5 Norway

As of 1 January 2023, Nkom has allocated six MNCs 70-75 for NPN purposes. The main direction is that a shared MNC approach is applied for MNCs 71-74. The MNCs are divided into 100k sub-networks (5 digits) each supporting 100k subscribers (5 digits).

12.1.6 Finland

The Traficom input e.g. stated:
"NPN model has not realised practically any demand for MNCs in Finland. MCC 999 has been taken in use for testing purposes instead of using MNCs under Finland's MCC 244."

Thus, Finland should be in a good position since conclusions of this report indicate that MCC 999, should be a good choice.

Finland has allocated the 8xx series for 3-digit MNCs but this has not been taken into use.

12.1.7 Sweden

In 2013 PTS allocated the 65 and 66 MNCs for private networks, as well as 67 and 68 for test purposes.

In 2014 PTS ordered a study around 3-digit MNCs and shared MNCs. The study promoted 3-digit MNC implementation, however conditioned on the 3GPP constraints. MNC series 7x-9x were reserved for future use.

In 2021 PTS conducted a market investigation on realization aspects for 3-digit MNCs and shared MNCs. As the responses were mixed and the ID management involved this did not lead to any decisions other than to order this study.

12.2 CBRS – United States

Citizens Broadband Radio Service (CBRS) is a 150 MHz wide broadcast band of the 3.5 GHz band (3550 MHz to 3700 MHz) in the United States. On January 27, 2020, the FCC authorized full use of the CBRS band for wireless service provider commercialization without the restrictions to prevent interference with military use of the spectrum. CBRS are based on 4G/LTE and 5G technologies without the need to acquire spectrum licenses.

There is a substantial ID management as a shared MNC approach is adopted as presented in section 9.4.2 of this document. Various roles as NHN and Service providers, with associated implementations are described in the specifications [48].

12.3 MulteFire Alliance - Global

The CEPT document [31] summarizes MulteFire as follows.

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

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

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."

MFA has adopted the same shared MNC approach with ID management as CBRS, please section 9.4.2 of this document.

13 Conclusions

This study has addressed two main areas related to efficient MNC administration:

- Technical conditions and challenges
- Market demands for MNCs

The outcome of the technical analysis is presented in section 13.1. The result of the market demands analysis is presented in section 13.2. The recommended actions for PTS in conjunction to the conclusions are outlined in chapter 14.

13.1 Technical Analysis

The overall question to be answered is how the MNCs can be as efficiently administered as possible. Three major technical areas have been addressed in this perspective:

- To what extent is it possible to introduce 3-digit MNCs for the 8x and 9x MNC series under MNC 240.
- How shall un-coordinated vs shared MNCs be handled.
- Roaming considerations for SNPNs, addressing new SNPN features related to “roaming substitutions” as well as specific roaming considerations.

13.1.1 2- and 3-digit MNC Mix

The implications on introducing 3-digit MNCs are analyzed in Chapter 8. It is concluded that, notwithstanding the 3GPP statement that a mix of 2- and 3-digit MNCs is not recommended, there should not be any technical issues associated to this matter if the 3GPP specifications are followed.

This is supported by the fact that 2-digit and 3-digit mixes have been working in countries like India and France for some time. Further, roaming with India (both directions) has been working for a long time.

The fact that either 2- or 3-digit MNCs can be used for MCC 999, is another indication that a mix shall be possible.

The issue is that 3GPP specifications state that a mix is not recommended. This is to be considered as outdated and yielding an inefficient usage of MNCs.

To be noted is that 3GPP in 2012 as a response [9] on TSB Circular 285 [67] to ITU-T, related the problem to overlapping MNCs, see section 8.5. In the NL response to ITU-T in 2012, T-Mobile also presented that there should not be any problems for non-overlapping MNCs. In a dialogue with AFRY, T-Mobile NL has declared that they still have this view.

Thus, non-overlapping MNC series should in any event be a safe bet. The 3-digit MNCs could be multi-purpose, i.e. they will not have to be limited to any specific applications as e.g. NPNs. Thus, PTS is free to decide on the actual assignments.

13.1.2 Un-coordinated vs Shared MNCs

The analysis of un-coordinated vs shared MNCs is carried out in chapter 9. It is evident that 5GC-NID is the way forward as to separate between SNPNs. Since the 5GC-NID together with the PLMN ID uniquely identifies the SNPNs the whole MSIN range can be used. The 5GC-NID is 40 bits long yielding that the number of supported SNPNs is “endless”.

This indicates that there should not be any future need for shared MNCs. Un-coordinated MNCs with an attention to MNCs within MCC 999, will on the other hand be of major interest. A main reason is that Apple from iOS 17 fully supports 4G/LTE and 5G (SA and NSA) for MCC 999. Other device manufacturers are expected to follow.

However, there are some obstacles to overcome as to introduce the 5GC-NID:

- 5GC-NID is introduced in 3GPP R16, and has not been implemented yet. The indications are that 5GC-NID will be supported in systems and UEs in 2025.
- In the near term, there is some need for 4G/LTE (combined with 5G) for SNPNs as there are some current feature limitations in 5G. Further, there are cost implications to be considered.

The main technical requirement is that nearby SNPNs shall not interfere with each other. Nearby SNPNs shall accordingly be configured with different PLMN IDs, i.e. different MNCs if the same MCC is used. It shall be noted that MCC 999 offers about 1,000 MNCs, to be compared with two Swedish MNCs, 65 and 66. Most likely, the interest for the Swedish MNCs should diminish.

Soft cause codes, described in section 9.5.2, should be supported by the SNPNs, as to limit the effects of using the same MNCs. When 5GC-NID is implemented, SNPN UEs will not try to register to other SNPNs unless specified to do so.

13.1.3 Key Future SNPN Features

Section 5.2 outlines some critical future SNPN features. The 5GC-NID is then the foundation as to achieve unique SNPN IDs.

The Credentials Holder (CH) concept is key as to achieve guest access by means of applying the home network credentials for 3rd party authentication. The CH can either be the home network itself (PLMN or SNPN), or a 3rd party "connected" to the home network. There should then be a need for a Broker role to interconnect the MNOs and SNPNs especially for Localized Services.

Localized Services will be related to a new type of SNPN, supporting time constrained access with localization support, typically for arena events.

The onboarding feature provide means to provide credentials (and subscription for the "visited" SNPN) to the UE. One application for onboarding is Localized Services and similar guest access. Further, onboarding provides the means to connect new IIoT devices to the SNPN.

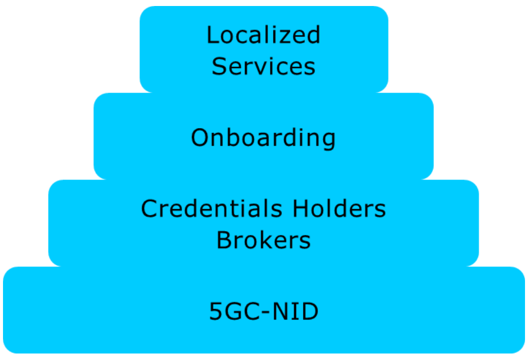

Figure 20. Future SNPN feature dependencies.

13.1.4 Roaming Considerations

As presented, there is no support for SNPN ID roaming in the 3GPP specifications. From the other end, there is an increasing interest from the enterprises for roaming e.g. as the SNPN applications are broadened. Hence, there is a risk that own MNCs will be requested instead of un-coordinated ones.

There are upcoming 3GPP SNPN features as credentials holder, onboarding and localized services in the 3GPP specifications as summarized in the previous section. They could be perceived as roaming substitutions. However, they introduce other complexities and should not replace the need for native roaming support.

As the roaming substitutes and SNPN ID roaming will take time to establish, some near term alternatives must be sought.

A new role, already on the market, has been presented by Ericsson in direct dialogue. Major M(V)NOs with many roaming agreements in place, offer a solution for international roaming to the SNPNs. The SNPNs will then use a specific part of the M(V)NO IMSI range, as for shared MNC networks. These will not require any Swedish MNCs as the M(V)NOs will not use the Swedish MCC, However, there might be similar upcoming approaches for the Swedish market. The MNC demand is limited as this only requires one MNC per M(V)NO. This approach should be promoted as it limits the need for new MNCs.

13.2 Swedish MNC demands

In the survey no one pinpointed other applications than SNPNs to drive the MNC needs.

In terms of SNPN volumes, the starting point is that the current number of SNPNs are very limited when studying the radio licenses. In total, 87 ones have been assigned by PTS per Nov. 2023. Out of these a maximum of 50 commercial ones has been estimated. For a number of reasons, PNI-NPNs have dominated so far, some input relates to an 80% market share. Applying a 40% CAGR, with different constraints yields that total number of SNPNs in 5 years' time would be 250-400.

This indicates that the 200 MNCs in the 8xx-9xx MNC series would not be sufficient. Thus, an un-coordinated MNC approach should be established for the general cases. The open question is then to what extent separate MNCs must be provided as discussed in section 7.2.

Neutral Hosts are receiving a lot of attention (however very limited from the Swedish MNOs). A "pure" NHN will not need any MNC on its own as it just transfers the PLMN IDs of the participating MNO(s). In the survey, the case that the NHNs would also provide local services thereby requiring an own MNC was brought to the table. However, no such needs were presented.

14 Recommendations

14.1 Effective MNC Management

To achieve an effective MNC management the following actions are recommended.

- Three-digit non-overlapping MNCs shall be assigned as far as possible.
- Continue with the un-coordinated MNC approach, without adding any new MNCs
  - Global MCC 999 to be the main path, allows for simple means as to avoid MNC interference. To be promoted by PTS.
  - MNCs 65 and 66 to be maintained but will most likely not be used to a great extent.
  - Make market aware of that MNCs shall be spread out. System/solution providers will play a vital role.
  - Communicate the importance of 5GC-NIDs and how those shall be self-assigned.
- Limit assignments of own MNCs for SNPNs to those who have roaming needs
  - Direct MNC applicants to market players offering SNPN roaming (using M(V)NO IMSI ranges)
  - Promote establishment of new (local) offerings of SNPN roaming.
  - Push for technical SNPN ID roaming support in 3GPP specifications.
  - Follow the future evolution of the CH concept and how it can function as a roaming substitute.
  - Potentially, promote the CH Broker role and stimulate/promote MNO participation.

14.2 Recommended PTS Actions

14.2.1 Introduction of 3-digit MNCs

As outlined in section 13.1.1, a mix of 2- and 3-digit MNCs for non-overlapping series, is supported by 3GPP implementations.

PTS should, as soon as possible, reallocate the 8x and 9x series into 8xx and 9xx series as desired. The 3-digit MNCs should be treated as multi-purpose i.e. PTS is free to decide on the applications for these MNCs.

An issue is that 3GPP specifications state that a mix is not recommended. This is to be considered as outdated and yielding an inefficient usage of MNCs. We recommend PTS to address 3GPP, as to make a revision in this context. Primarily 3GPP should be addressed via Liaison Statements from ITU-T and CEPT WG Nan. In parallel PTS could seek active support from mobile system providers and Swedish MNOs.

14.2.2 Roaming Considerations

According to section 13.1.3, there should be limited work required to complete the 3GPP specifications to support SNPN ID roaming, PTS is urged to contact 3GPP as to stress the need for roaming support. 3GPP should then be addressed in the same way as described in the previous section. Thus, mixed 2- and 3-digit MNC support and SNPN ID roaming could be addressed together.

The M(V)NO approach to offer roaming services for SNPNs by applying shared own MNCs, as outlined in section 7.2, should be promoted by PTS. Thereby, roaming can be supported with very limited needs for new MNCs.

14.2.3 Establishment of Swedish NPN/NHN Forum

There is a need to establish a NPN/NHN Forum. The major reason for establishing this forum is that NPNs and NHNs will play a vital role for future MNC considerations and that the market involves small players who do not have a forum.

PTS could have a central role as to facilitate the establishment of the forum. However, other arrangements could be possible if there would be any market players being interested to take the role.

The Forum should handle:

- National coordination of MNCs under MCC 999, as recommended by CEPT. The industry stakeholders would thus be taking part in the forum. It shall be noted that very limited efforts would be required there are many MNCs to select from.
- Establishment of SNPN guidelines related to MNCs and 5GC-NIDs.
- Coordination of activities related to 3GPP.
- Knowledge sharing in terms of timing for future SNPN features. Common testing could also be addressed.
- Follow and stimulate roaming services and CH establishment.
- Stimulate NHN adoptions (using 5G Small Cell Technology).

14.2.4 Summary of Recommended Actions to PTS

Table 3. Recommended PTS actions.

Action	Background
Reallocate 2-digit 8x and 9x series into 3-digit 8xx and 9xx series.	Technical possible and extends the range of MNCs
Contact 3GPP, via ITU-T and CEPT WG NaN, to remove the obstacles for introducing 2- and 3-digit mix of MNCs (for non-overlapping series).	These limitations are found to be outdated and blocking activities for extending the national MNC ranges.
Contact 3GPP, via ITU and CEPT, as to stress the need for roaming support for SNPNs.	Roaming for SNPNs is not currently supported by 3GPP. Clear demand for roaming and only limited work should be needed by 3GPP as to establish support.
Promote M(V)NO roaming services for SNPNs.	Very limited MNC needs to support SNPN ID roaming.
Facilitate establishment of Swedish NPN/NHN Forum.	NPNs and NHNs will be critical for future MNC considerations. Necessary coordination and information sharing will be achieved via the forum.

15 References

[1] PTS, “Plan of Mobile Network Codes (MNC) according to ITU-T Recommendation E.212”. Current version of 2023-08-22. Available: https://pts.se/globalassets/startpage/dokument/bransch/telefoni/nummer-och-adressering/tekniska-planer/plan-mnc-rev-2023-08-22.pdf

[2] PTS, ”VÄGLEDNING: Ansökan om tillstånd för att använda mobila nätkoder (MNC) för privata nät”, June 2022. Available: https://www.pts.se/globalassets/startpage/dokument/bransch/telefoni/nummer-och-adressering/vagledningar/vagledning---mnc-for-privata-nat---svensk---2022-06-03.pdf

[3] PTS, ”Information om och anvisningar till ansökan om tillstånd att använda radiosändare i 3720–3800 MHz och 24250–25100 MHz banden, så kallade lokala tillstånd”, not dated. Available: https://www.pts.se/sv/bransch/radio/radiotillstand/lokala-tillstand-i-37-ghz--och-26-ghz-banden/

[4] PTS 21-14852, ”Remiss avseende PTS inriktning för hantering av ansökningar om mobila nätkoder (MNC) för privata nät”, November 2021. Available: https://pts.se/sv/dokument/remisser/telefoni--internet/2021/remiss-avseende-pts-inriktning-for-hantering-av-ansokningar-om-mobila-natkoder-mnc-for-privata-nat/

[5] RCR Wireless news, “Private network spectrum strategy, Part 2: Sweden´s PTS”. Available: https://www.rcrwireless.com/20221122/spectrum/private-network-spectrum-strategy-part-2-swedens-pts

[6] Nkom, “Forslag om å allokere mobile nettverkskoder til private nett og til testformål”, June 2021. Obtained from Nkom.

[7] BNetzA, “Mitteilung Nr. 31/2022, Bundesnetzagentur Amtsblatt 04/2022 vom 23.02.2022, Internationale Kennungen für Mobile Teilnehmer (IMSIs); Anhörung zur Änderung des Nummernplans im Hinblick auf Campusnetze und die Verwendung und Verwaltung bislang nicht regulierter Netzkennungen; Zusammenfassung und Bewertung der Stellungnahmen”, February 2022. Available: https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Nummerierung/Campusnetze/IMSI_Anhoerung.pdf?__blob=publicationFile&v=1

[8] BNetzA, “Verfügung Nr. 15/2022, Bundesnetzagentur Amtsblatt 04/2022 vom 23.02.2022 (mit Begründung) Nummernplan Campusnetze”. Available: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/Allgemeinverfuegungen/Vfg15_2022.pdf?__blob=publicationFile&v=2

[9] 3GPP TSG SA, “Reply LS on Assignment of 3 digit MNC”, June 2012. Obtained from PTS.

[10] Dialogic 2013.034 – 1254, “Feasibility study to assign 3-digit MNC codes to mobile network operators in the Netherlands”, October 2013. Obtained from PTS

[11] GSMA, “Comments on Draft ECC Report 212 on Evolution in the use of E.212 Mobile Network Codes”, January 2014. Obtained from PTS.

[12] Rabión Consultancy B.V., “Onderzoek Effecten Gebruik Driecijferige Mobiele Netwerk Codes In Lokaal Private Netwerken” (Research Effects Of Use Three-Digit Mobile Network Codes In Local Private Networks), February 2014. (Translated to English in Microsoft Word)

[13] Jan Yngvar Olsen, Cybercom SIN-035-14006-1, “Report on mixed use of 2 and 3 digit MNC codes under Sweden´s MCC 240”, May 2014. Obtained from PTS.

[14] Decree of the Minister of Economic Affairs [Minister van Economische Zaken] of 3 March 2014, no. ETM/TM/14024019, containing amendments to the Numbering Plan for international mobile subscription identities (IMSIs) relating to the use of IMSIs by private networks (NL). Obtained from Ministry.

[15] GSMA: "5G industry campus network deployment guideline", v2.0 October 2021. Available: https://www.gsma.com/newsroom/resources/ng-123-5g-industry-campus-network-deployment-guideline-v2-0

[16] 5G-ACIA: "5G Non-Public Networks for Industrial Scenarios", March 2019. Available: https://5g-acia.org/whitepapers/5g-non-public-networks-for-industrial-scenarios/

[17] SCTE CableLabs and NCTA, “New Service Paradigm With 5G Private Network”, October 2021. Available: https://www.nctatechnicalpapers.com/Paper/2021/2021-new-service-paradigm-with-5g-private-network/download

[18] 5G PPP Technology Board, “Non-Public-Networks – State of the art and way forward”, v1.0 November 2022. Available: https://5g-ppp.eu/wp-content/uploads/2022/11/WhitePaperNPN_MasterCopy_V1.pdf

[19] Lei Shi & Jacob Renning, Analysys Mason, ”Rethink the Approach to 5G Indoor Coverage”, February 2023. Available: https://www.analysysmason.com/contentassets/750c9111e4ea4f07b2f653a3820711bb/analysys-mason---rethink-the-approach-to-5g-indoor-coverage.pdf

[20] REDI, ”5G Inomhus Fastighetsägares Perspektiv”, 2022. Available: https://assets.website-files.com/634f40460714a5e23af01779/640f46f836bcf33c4199baaa_Epicenter_Rapport_5G_RGB_Print_Final-1.pdf

[21] German Federal Ministry for Economic Affairs and Energy, “Guidelines for 5G Campus Networks – Orientation for Small and Medium – Sized Businesses”, April 2020. Available: https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/guidelines-for-5g-campus-networks-orientation-for-small-and-medium-sized-businesses.html

[22] SCF, Document 244.10.01, “Neutral Host Requirements, Part One: Architectures”, July 2021. Available: https://www.scf.io/en/documents/244_Neutral_Host_Requirements_Pt_1_Architectures.php

[23] SCF, Document 245.10.01, “Neutral Host Requirements, Part Two: Hosted RAN high-level design”, June 2022. Available: https://www.scf.io/en/documents/245_Neutral_Host_Requirements_Pt_2_Hosted_RAN_high-level_design.php

[24] SCF, Document 191.08.02, “Multi-operator and neutral host small cells -Drivers, architectures, planning and regulation”, December 2016. Available: https://www.scf.io/en/documents/191_-_Multi-operator_and_neutral_host_small_cells.php

[25] ATIS-I-0000073: "Neutral Host Solutions for 5G Multi-Operator Deployments in Managed Spaces", July 2019. Available: https://access.atis.org/apps/group_public/download.php/48403/ATIS-I-0000073.pdf

[26] R. Bajracharya , R. Shrestha , H. Jung & H. Shin, IEEE Access, "Neutral Host Technology: The Future of Mobile Network Operators", September 2022. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9895249

[27] M. T. Lemes, A. M. Alberti, C. B. Both, A. C. De Oliveira Junior, K. V. Cardoso, IEEE Access, "A Tutorial on Trusted and Untrusted Non-3GPP Accesses in 5G Systems – First Steps Toward a Unified Communications Infrastructure", October 2022. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9940294

[28] J. Prados-Garzon, P. Ameigeiras, J. Ordonez-Lucena, P. Muñoz, O. Adamuz-Hinojosa and D. Camps-Mur, IEEE Access, "5G Non-Public Networks: Standardization, Architectures and Challenges", November 2021. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9611236

[29] 5G Americas White Paper, "5G Technologies in Private Networks", 2020. Available: https://www.5gamericas.org/5g-technologies-in-private-networks/

[30] ECC Report 212, "Evolution in the Use of E.212 Mobile Network Codes, Approved April 2014". Available: https://docdb.cept.org/download/1152

[31] ECC Report 337, "Public Numbering resources for mobile non-public networks", June 2022. Available: https://docdb.cept.org/download/4025

[32] ECC Recommendation 17(02), "Harmonised European Management and Assignment Principles for Geographic E.212 Mobile Network Codes (MNCs)", Soon to be updated on CEPT web site.

[33] ITU-T Recommendation E.212: "The international identification plan for public networks and subscriptions", September 2016. Available: https://handle.itu.int/11.1002/1000/12831-en?locatt=format:pdf&auth

[34] ITU-T Recommendation E.212 Amendment 1: "New Appendix on shared E.212 Mobile Country Code (MCC) 999 for internal use within a private network", July 2018. Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.212-201807-I!Amd1!PDF-E&type=items

[35] GSMA NG.113, "5GS Roaming Guidelines", Version 6.0, May 2022. Available: https://www.gsma.com/newsroom/wp-content/uploads/NG.113-v6.0.pdf

[36] GSMA NG.132, "Report 5G Mobile Roaming Revisited (5GMRR) Phase 1", Version 2.0, 06 July 2022. Available: https://www.gsma.com/newsroom/wp-content/uploads/NG.132-v2.0-1.pdf

[37] GSMA IR.88, "EPS Roaming Guidelines", V26.0, May 2023. Available: https://www.gsma.com/newsroom/wp-content/uploads//IR.88-v26.0.pdf

[38] GSMA IR.61, "Wi-Fi Roaming Guidelines", v13.0, October 2021. Available: https://www.gsma.com/newsroom/wp-content/uploads//IR.61-v14.0.docx

[39] GSMA IR.34, "Guidelines for IPX Provider networks (Previously Inter Service Provider IP Backbone Guidelines)", Version 17.0, May 2021. Available: https://www.gsma.com/newsroom/wp-content/uploads//IR.34-v17.0.pdf

[40] 3GPP TS 23.501, "System architecture for the 5G System (5GS), Stage 2 (Release 18)", V18.0.0 (2022-12). Available: https://portal.3gpp.org/Specifications.aspx

[41] 3GPP TS 23.003, "Numbering, addressing and identification (Release 18)", V18.0.0 (2022-12). Available: https://portal.3gpp.org/Specifications.aspx

[42] 3GPP TS 23.122, "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (Release 18)", V18.1.0 2022-12. Available: https://portal.3gpp.org/Specifications.aspx

[43] 3GPP TS 24.501, "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3; (Release 18)", V18.1.0 (2022-12). Available: https://portal.3gpp.org/Specifications.aspx

[44] 3GPP TS 24.301, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 18)", V18.1.0 (2022-12). Available: https://portal.3gpp.org/Specifications.aspx

[45] 3GPP TS 31.102, "Characteristics of the Universal Subscriber Identity Module (USIM) application (Release 18)", V18.0.0 (2023-03). Available: https://portal.3gpp.org/Specifications.aspx

[46] 3GPP TS 38.304, "User Equipment (UE) procedures in Idle mode and RRC Inactive state (Release 17)", V17.3.0 (2022-12). Available: https://portal.3gpp.org/Specifications.aspx

[47] 3GPP TS 24.008, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 18), V18.3.0 (2023-06). Available: https://portal.3gpp.org/Specifications.aspx

[48] OnGo Alliance, OnGo-TS-1002, "CBRS Network Services Stage 2 and 3 Specification", V4.0.0, March 2021. Available: https://ongoalliance.org/wp-content/uploads/2021/06/OnGo-TS-1002-V4.0.0_Published-March-16-2021.pdf

[49] OnGo Alliance, OnGo-TR-0100, "OnGo Alliance Identifier Guidelines for Shared HNI", V1.2.2, December 2021. Available: https://ongoalliance.org/wp-content/uploads/2019/01/ONGO-TR-0100-V1.2.2-.pdf

[50] OnGo Alliance, OnGo-TR-0101, "OnGo Alliance Identifier Administration Guidelines for Shared HNI", V1.2.0, December 2021. Available: https://ongoalliance.org/wp-content/uploads/2019/01/ONGO-TR-0101-V1.2.0-.pdf

[51] OnGo Alliance, OnGo-TS-1003, "Extended Subscriber Authentication Technical Specifications", V3.0.0, February 2020. Available: https://ongoalliance.org/wp-content/uploads/2020/02/CBRSA-TS-1003-V3.0.0_Approved-for-publication.pdf

[52] MulteFire Alliance (MFA), "The MFA Shared PLMN-ID – The Ideal Solution for Your Private Network Deployment". Available: https://www.mfa-tech.org/white-papers/

[53] MulteFire Alliance (MFA), "MulteFire Release 1.1 Enhancements", 2019. Available: https://www.mfa-tech.org/white-papers/

[54] MulteFire Alliance (MFA), MFA TS MF.202, "Architecture for Neutral Host Network Access Network Access Mode Stage 2 (Release 1.1"), V1.1.3, February 2019. Available: https://www.mfa-tech.org/technology/specifications/

[55] MulteFire Alliance (MFA), MFA TS MF.201, Architecture for PLMN Access Mode Stage 2 (Release 1.1), February 2019. Available: https://www.mfa-tech.org/technology/specifications/

[56] GSA Member Report, "Private Mobile Networks", May 2023. Available. https://gsacom.com/paper/private-mobile-networks-may-2023-member-report/

[57] R. Keller, T. Cagnenius, A. Ryde, D. Castellanos, Ericsson Technology Review, “Migration from EPS to 5GS”, January 2020. Available: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/migration-from-eps-to-5gs

[58] Ericsson Mobility Report, “5G Voice Network Evolution – A guide to enabling voice services to 5G smartphones”, not dated. Available: https://www.ericsson.com/en/core-network/guide/forms/guide-5g-voice

[59] Ericsson White Paper, GFMC-284 23-3163 Uen Rev D, “Voice and communication services in 4G and 5G networks”, July 2022. Available: https://www.ericsson.com/en/reports-and-papers/white-papers/voice-and-communication-services-in-4g-and-5g-networks

[60] Nokia White Paper, “Voice over 5G: the enterprise opportunity for Communications Service Providers – How 5G for enterprises will change the game for CSPs”, 2020. Available: https://pf.content.nokia.com/t0080q-vo5g-benefits-and-features/nokia-voice-over-5g-the-enterprise-opportunity-for-csps-whitepaper?lb-mode=overlay

[61] Apple, Device support for private 5G and LTE networks. Available: https://support.apple.com/en-om/guide/deployment/depac6747317/web

[62] Arcep, French MNC allocations. Available: https://www.data.gouv.fr/fr/datasets/r/5606408f-5248-4316-9c79-1c3213d63eb8

[63] IANA, PEN Allocations. Available: https://www.iana.org/assignments/enterprise-numbers

[64] IANA, PEN Application Form. Available: https://pen.iana.org/pen/PenApplication.page

[65] Telekom idag, “Telenor delivers 5G Networks to IKEA”. Available: https://telekomidag.se/satsningen-telenor-levererar-5g-nat-till-ikeas-varuhus/

[66] NHN Announcement from Swedish MNO 3. Available: https://tre.mynewsdesk.com/pressreleases/tre-foerst-med-ny-ericsson-loesning-foer-snabbare-inomhus-5g-3261514.pdf

[67] ITU TSB Circular 285, “Possibility of parallel usage of 2 and 3 digit E.212 Mobile Network Codes (MNCs) under one geographic Mobile Country Code (MCC)”. Available: https://www.itu.int/md/T09-TSB-CIR-0285/en

[68] Ericsson, “Ericsson response on PTS consultation - handling of applications for mobile network codes (MNC) for private networks (Ref: 21-14852)”. Available: https://pts.se/globalassets/startpage/dokument/icke-legala-dokument/remisser/2021/mnc-privata-nat/ericsson-211203-sweden---pts-mnc-english---final.pdf

16 Glossary

Term	Description
3GPP	Third Generation Partnership Project Standardization body for mobile systems as e.g. 4G/LTE and 5G
4G/LTE	4^{th} generation mobile system also denoted as Long Term Evolution
5G	5^{th} generation mobile system
5GC	5G Core Network
5GC-NID	5G (Core) Network Identifier for SNPNs
AAA	Authentication, Authorization and Accounting
AM	Assignment Mode for 5GC-NID
AMF	Access and Mobility Function (5G)
ATIS	Alliance for Telecom Industry Solutions
AUSF	Authentication Server Function (5G)
BCCH	Broadcast Control Channel
CAG	Closed Access Group
CAGR	Cumulative Annual Growth Rate
CBRS	Citizens Broadcast Radio Service (US) Administrated by OnGoAlliance
CBRS-I	CBRS Identifier
CBRS-NID	CBRS Network Identifier
CEPT – ECC	European Conference of Postal and Telecommunications Administrations – Electronic Communications Committee
CH	Credentials Host
CN	Core Network
CSG-ID	Closed Subscriber Group ID
CUPS	Control and User Plane Separation
DAS	Distributed Antenna System
DN	Data Network
ECGI	E-UTRAN Cell Global Identifier
EPC	Evolved Packet Core (4G)
EPS	Evolved Packet System
eSIM*	embedded Subscriber Identity Module
eUICC*	embedded Universal Integrated Circuit Card
PLMN	Public Land Mobile Network
FQDN	Fully Qualified Domain Name
GIN	Group ID for Network selection, associated to CH handling

GTP	GPRS Tunneling Protocol
GSMA	GSM Association
GUAMI	Globally Unique AMF Identifier (5G)
GUMMEI	Globally Unique Mobility Management Entity (MME) Identity (4G)
GW	Gateway
HLR	Home Location Register (pre 4G term)
HNI	Home Network Identifier
HPLMN	Home PLMN
HR	Home Routed
HSS	Home Subscriber System (4G)
IBN	IMSI Block Number
IMEI	International Mobile Equipment Identity The ID of the mobile equipment (device)
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPX	IP Packet exchange
iSIM*	Integrated SIM
ISP	Internet Service Provider
ITU	International Telecommunications Union
LADN	Local Area Data Network
LBO	Local Break Out
LTE	Long Term Evolution
MCC	Mobile Country Code, part of IMSI
MFA	MulteFire Alliance
MME	Mobility Management Entity
MNC	Mobile Network Code, part of IMSI
MNO	Mobile Network Operator
MOCN	Multi Operator Core Network
MODS	Multi Operator Dedicated Spectrum
MVNO	Mobile Virtual Network Operator
MORAN	Multi Operator RAN
MOSS	Multi Operator Shared Spectrum
MSIN	Mobile Subscription Identification Number
N3IWF	Non-3GPP Interworking Function
NAI	Network Access Identifier
NAS	Non Access Stratum, handles the communication between UE and core network
NH	Neutral Host

NH-GW	Neutral Host Gateway (OnGo / CBRS term)
NHN	Neutral Host Network
NID	Network Identifier
NPA	Numbering Plan Administrator
NPN	Non Public Network
NRA	National Regulatory Authority
NR CGI	New Radio Cell Global Identity
NSA	Non Stand Alone (5G) , relies on 4G/LTE
OnGo Alliance	Former CBRS Alliance, responsible for the CBRS specifications
OS	Operating System
PDN	Packet Data Network
PLMN	Public Land Mobile Network
PLMN ID	Combination of MCC and MNC
PTS	Post och Telestyrelsen
(R)AN	(Radio) Access Network
RAT	Radio Access Technology, 3GPP terminology to separate between mobile system generations as 4G and 5G.
REDI	Real Estate Digitalization Initiative (SE)
ROIO	Regional and Other International Oganizations.
SA	Stand Alone (5G), no dependencies to 4G/LTE
SBA	Service Based Architecture
SCF	Small Cell Forum
SCTP	Stream Control Transmission Protocol
SDO	Standards Development Organizations
SEAF	Security Anchor Functionality
SEPP	Security Edge Protection Proxy
SIB	System Information Block
SIM*	Subscriber Identity Module Embedded …
SLA	Service Level Agreement
SME	Small and Medium sized Enterprises
SMF	Session Management Function (5G)
SNPN	Stand-alone Non Public Network
SNPN ID	Combination of PLMN ID and 5GC-NID
SUCI	Subscription Concealed Identifier, encrypts (conceals) part of the SUPI
SUPI	Subscription Permanent Identifier

TA	Tracking Area
TAC	Tracking Area Code
TAI	Tracking Area Identity
TMSI	Temporary Mobile Subscription Identifier
TNAN	Trusted Non-3GPP Access Network
TNAP	Trusted Non-3GPP Access Point
TSB	Telecommunications Standardization Bureau
UDM	Unified Data Management
UE	User Equipment
UICC*	Universal Integrated Circuit Card
UIN	User Identification Number
UPF	User Plane Function (5G)
USIM*	Universal Subscriber Identity Module
VoNR	Voice over New Radio
VPLMN	Visited PLMN

* The UICC is the smart card computer used in mobile terminals which e.g. runs the SIM application. USIM is the SIM application term used since 3rd generation (3G) mobile systems (UMTS). The UICC also stores various data types as contact lists, manages mobile data usage, and allow data roaming across different mobile networks.

The SIM card is the traditional physical card carrying the UICC. With embedded SIM (eSIM) the UICC is carried as a separate chip and integrated in the hardware of the device. Integrated SIM (iSIM) comes with a smaller form factor and is part of system on a chip (SoC) also including radio and CPU.

The eUICC, is a technology standard that enables over-the-air provisioning of mobile network operator profiles (up to 24 profiles) to a UE. It can work with both eSIMs and SIM cards with eUICC.

iUICC is hosted by the iSIM and comes with the same properties as eUICC.

Appendix 1 – Summary of Survey Questions

Question areas	Target Groups			
	System Providers	NPAs / NRAs	MNOs / SPs	NHN Providers
To what extent have you evaluated a mix of 2-and 3-digit MNCs? What are your conclusions in terms of feasibility and time of introduction?		X		
Which countries do you know of that have mixed 2- and 3-digit MNCs?	X	X		
What international experiences of mixing 2- and 3-digit MNCs have been identified?	X	X		
What specific technical limitations could be identified as to prohibit a mix of 2- and 3-digit MNCs?	X			
What is the background to 3GPP not recommending a 2- and 3-digit mix?	X			
Could there be any drivers for implementing 4G/LTE instead of 5G for new SNPN systems?	X		X	X
When is R16 to be expected with NID support??	X		X	
Do you agree that only NID and IBN will have to be administrated when NID is in place?	X			
Should there be any specific considerations for UEs not supporting R16?	X			
In the event that R16 will not be available soon, what would the implications on ID handling etc for 5G NPNs? How could NRA/NPA administration of MNCs be limited in this case?	X			
What is your thinking about implementing shared MNCs? If implementing what would be the split between number of blocks and users? How do you intend to handle the NID part in terms of assignment mode?		X		
Are there any other ways to technically manage shared MNCs (than CBRS etc)?	X			

What should be expected in terms of soft error codes for UEs belonging to other SNPNs with the same shared MNC?	X			
In terms of Credentials Holders: • Elaborate on the role • Demand for MNCs • Relation to HLR Proxy Provider role	X		X	
In terms of Onboarding: • When will it be available? • Other considerations?	X		X	
What roaming aspects shall be considered for NPNs/SNPNs today and future-wise?	X		X	X
How are NHNs implemented, and how do these relate to the need for MNCs?	X		X	X
How do you see that courtesy access will come into in relation to the 3GPP specifications?	X		X	
What evolution do you see in terms of local services related to NHNs and NPNs?	X		X	X
What are the expected future volumes för NPNs in Sweden, and how are they distributed between SNPNs and NPI-NPNs?	X		X	
What are the main drivers for customers to select PNI-NPNs instead of SNPNs? What are your estimations on the demand for new separate MNCs to support PNI-NPNs?			X	
To what extent have you estimated the NPN MNC demand?		X		
What needs to you see for MNCs related to MCC 901?			X	
What other demands could be identified as to drive the need for MNC?	X	X	X	
What kind of evolution do you see around Neutral Hosts and Credentials Holders in relation to MNC demands?		X		
What kind of (new) roles do you see will be developing in the next few years and what is the expected impact on demand for MNCs?	X		X	

How is SNPN access mode expected to work?	X			
How is Neutral Host access mode (CBRS, MFA) expected to work?	X			
Are there any other MNC aspects you want to highlight?	X	X	X	