BEREC
Body of European Regulators for Electronic Communications

BoR (25) 33

BEREC Report on the evolution of private 5G networks and interrelation with public networks in Europe

13 March 2025

Contents

Executive Summary **2**

1 Introduction **4**

2 Private networks **6**

2.1 Definitions 8
2.2 Architectures of private networks/interrelations with public networks 9
2.2.1 Standalone private network (isolated deployment) 9
2.2.2 Private network in conjunction with public networks 10
2.2.3 Private network hosted by the public network 11
2.2.4 Architecture options and spectrum 11
2.3 Status of private network spectrum regulation 13

3 Numbering considerations **16**

3.1 E.164 numbers 16
3.2 Mobile Country Codes and Mobile Network Codes (MCC-MNC) 16
3.2.1 Issuer Identifier Numbers (IINs) 18
3.2.2 eUICC Identifier (EID) 18
3.2.3 Other kinds of 3GPP numbering resources 19
3.3 BEREC's summarizing insights on numbering 19

4 Drivers and case studies **21**

4.1 Various drivers for the implementation of private networks 21
4.1.1 Drivers as described during the consultations 22
4.1.2 BEREC's observations and considerations on drivers 22
4.2 Case studies 22
4.2.1 NRA views 22
4.2.2 Use cases as described during the consultation 23
4.2.3 BEREC's observations and considerations on use cases 26
4.3 BEREC's summarising insights on drivers and use cases 26

5 Identified challenges to 5G private network deployment and other observations **27**

6 BEREC's position and next steps **30**

Annex A Summary of NRA questionnaire results **31**

Annex B Questions at consultation stage **36**

Questions – Numbering as set out at chapter 3 of BoR (24) 150 36
Additional questions – Set out at chapter 4 of BoR (24) 150 36

Executive Summary

This report sets out BEREC's preliminary views on the current status, and needs, and regulatory issues concerning the implementation of private 5G networks in Europe, from the perspective of national regulatory authorities ("NRAs"). BEREC's views are predominantly based on an internal survey[1] to NRAs, which highlights that few dedicated frameworks for private networks have been implemented to date, and those that have, are designed to meet specific needs in countries. As a result of its preliminary analysis, BEREC considers that the case for further harmonisation of frameworks for private networks is inconclusive at this stage. BEREC is also aware that EU Member States are taking different approaches regarding numbering and spectrum issues and that it is the intent of the European Commission (through the Radio Spectrum Committee) to harmonise dedicated radio frequency ranges for private networks. BEREC has sought views from interested parties which may help to provide new perspectives for consideration by NRAs.

The report is divided into five chapters:

- **Chapter 1** sets out some background information, identifies the reasons for issuing this report and sets the frame for the public consultation
- **Chapter 2** briefly presents various definitions of private mobile networks, the technical architecture of networks, the status of private network spectrum regulation in countries, in particular by briefly introducing the relevant spectrum ranges being used in countries to support private mobile networks
- **Chapter 3** sets out the first consulted issue on numbering resources, where some relevant information from NRAs and from the consultation responses point to the challenge of ensuring unique resources for private networks are in place.
- **Chapter 4** sets out the second consulted issue on "drivers and use cases". The chapter briefly summarises main drivers for private networks and typical case studies that were described in consultation responses
- **Chapter 5** provides an overview table which summarises the identified challenges to 5G private network deployment and other observations, as these were derived from the consultation responses

[1] To draft this report, BEREC set out an internal questionnaire to consider NRA views on the following relevant topics, amongst others:

- Type of services offered / business model & value chain / innovative or defining aspects
- Use of standard and non-standard network elements
- Relation with MNOs and/or MVNOs and/or other private networks, including possible approaches such as active or passive infrastructure sharing, public/private interplay through network slicing, or solutions for providing (indoor or campus) access to public voice and SMS services
- Potential need of public numbering resources for private networks and the impact of that for public networks (roaming, (e)SIM-cards etc.), and potential use of the global Mobile Country Code (MCC) 999 from ITU to fulfil some private networks' need of E.212 MNCs
- Potential issues concerning QoS, security, and sustainability mobility, and roaming (including possible interoperability and standards issues) regulatory issues, examining what existing regulations assist deployment of private networks and if there are gaps / needs for new regulations and what these might be.

- **Chapter 6** summarizes BEREC's position and next steps, and
- **Annex A** sets out the results of a questionnaire issued to BEREC Members regarding the private networks.
- **Annex B** provides the original list of consultation questions that were part of the consultation report. The consultation reactions have been used to update the report.

BEREC's consultation on this report ran from 8 October until 29 November and stakeholders were encouraged to answer the questions on numbering, drivers and use cases raised in chapters 3 and 4 and provide comments on any aspect of the report.

BEREC Document BoR (25) 32 assesses and summarizes the contributions received.

1 Introduction

Newer generations of mobile technologies offer more flexibility towards applying technologies for specific user groups and use cases e.g. for private networks (called non-public networks (NPN) by 3GPP). Services delivered over public and private 5G networks may not only complement each other but also compete with each other, and with services that can be offered using a fixed network with a wireless local access network (Wi-Fi). Private 5G network use may therefore have different or overlapping user groups and service requirements as compared to public networks, for instance with regards to quality of service (QoS), mobility, security, numbering, emergency communication and roaming.

In the broader context, trends such as satellite communication, small cells, infrastructure and spectrum sharing, and neutral hosting may play a role in private networks. In addition, as public and private 5G networks have different concepts, there are different ways of facilitating them including by licensing where necessary. In relation to licensing, there may be competitive awards, such as auction or tender for the use of spectrum for wide area public networks, and /or first-come-first-served awards which may be more suited to smaller isolated areas for private networks.

Concerning numbering resources for private 5G networks there may be challenges since most numbering resources (e.g. E.212 Mobile Network Codes, E.164 numbers and E.118 Issuer Identifier Numbers) administered by NRAs are for public electronic communication services and networks, and not intended for private network use according to the E-series of ITU-T Recommendations. In this regard, other competent bodies such as the CEPT are interested in private network deployments in Europe and published ECC Report 337[2] “Public numbering resources for mobile non-public networks” following a public consultation process.

In addition, CEPT has in July 2024 consulted on a number of relevant spectrum considerations in bands used by private networks in Europe, in order to facilitate private 5G networks operation in the frequency range 3800-4200 MHz (whole band or parts of it) as a long-term solution.

Examining the implementation of public and private networks that share the same radiofrequency spectrum helps regulators ensure maximum use of frequency resources while still maintaining interference free operation for different network types. In addition, ensuring a proper functioning market with sufficient capacity (including spectrum resources) for niche services which need specialised and/or localised use rather than a one size fits all solution, such as certain mission critical and business critical use cases, also supports opportunities for innovation.

A business owner who wishes to implement a connected private network into a business that is distributed across different geographical locations nationally or internationally may have certain challenges in connecting or combining such physically separated and geographically distributed networks. In addition, it may face the challenge of potential interference aspects concerning the usage of E.212 MNCs between nearby private networks. Reporting on

[2] https://docdb.cept.org/download/4025

spectrum usage can help to minimise compatibility issues, but the burden of reporting for entities that are unlikely to have regulatory affairs teams needs to be considered too. Finally, the role of neutral host networks (in private settings) or providing a form of roaming to (public) voice- and SMS-services to users of the private networks, for instance in campus, offshore, mining or indoor environments, is not widespread or widely reported on by NRAs, which raises the issue whether there are barriers to this function.

This report sets out information from the NRAs' perspective using a questionnaire to NRAs, as well as with the relevant views from stakeholders that contributed to the consultation. As a result, BEREC considers that the report provides an informative overview for NRAs of the following:

- the extent of the use of private 5G networks and interrelation with public networks in Europe,
- potential relevant numbering aspects for private networks, and what kind of public numbering resources private networks might need and probably apply for,
- the drivers for, and requirements of, private networks,
- the evolution of private networks aimed at meeting new user demands for specific user groups, and
- relevant private 5G network case studies and interrelations between private and public 5G networks.

A summary of some of the main results of the NRA questionnaire is set out at Annex A.

2 Private networks

Private networks and in particular private mobile or wireless networks, are networks owned and operated by private entities and organisations such as enterprises, industries, and governments and in most cases primarily intended for specific use by these entities and organisations.[3] As a result, private mobile networks are typically deployed to serve a private entity's premises, such as a campus or a factory by providing connectivity within a specific geographic area ('plot-related'). Various technologies can be associated with private mobile or wireless networks: 3GPP-based generations of mobile technologies, Wi-Fi, Satellite, and proprietary technologies: TETRA, P25, WiMAX, Sigfox, LoRaWAN. This also means that there are various ways private mobile or wireless networks may be deployed in the field.

In addition, this means that there are numerous relevant actors in the private network ecosystem. In particular, NRAs observed the role that MNOs play where MNOs and/or MVNOs may act as full-service providers of private 5G networks or provide parts of the relevant services. In addition, NRAs reported that traditional mobile network equipment suppliers are active in the ecosystem.[4] Finally, NRAs also set out that other players include the hyperscalers[5], which also provide cloud services, as well as other vendors/integrators and consultants.[6] Also the user organisations of private mobile networks are relevant actors.

The questionnaire that was issued to NRAs to inform this report, focused on the evolution of 3GPP-based private mobile networks. This suite of private mobile networks is interesting to BEREC for many reasons:

- Global mobile Suppliers Association (the GSA) reports that demand for 4G LTE and 5G technology based private mobile networks is growing[7];
- 3GPP-based private mobile networks are one of the use cases frequently associated with 5G Stand Alone (5G SA) networks because of network slicing functionalities. As a result, some private mobile networks can be an indicator of 5G SA deployments;
- Edge computing resources (MEC / mobile edge computing[8]) can be used by private networks[9] and BEREC observes that both 5G SA and MEC are the subject of the political targets for the EU regarding the development of 5G for smart communities[10],

[3] In contrast, public mobile networks offer services to the general public--
[4] Ericsson and Nokia
[5] Amazon Web Services, Microsoft Azure and Google Cloud
[6] Oracle, Teradata, Cellnex, Boldyn Networks, Vaiscom, Digita, Mavenir, Athonet, Nae and Radtonics
[7] https://gsacom.com/paper/private-mobile-networks-summary-february-2024/
[8] https://www.etsi.org/technologies/multi-access-edge-computing
[9] For example, Telefonica has partnered with Microsoft on Azure Private Edge Zone to integrate their 5G private industrial connectivity and edge computing capabilities on customer premises https://www.telefonica.com/en/communication-room/press-room/telefonica-tech-partners-with-microsoft-to-provide-the-industrial-sector-with-private-5g-connectivity-and-on-premises-edge-computing/ and also with Google Cloud's Mobile Edge Computing platform for the joint development of a 5G solutions portfolio https://www.telefonica.com/en/communication-room/press-room/google-cloud-and-telefonica-partner-to-accelerate-digital-transformation-for-spanish-businesses/
[10] https://digital-strategy.ec.europa.eu/en/activities/5g-smart-communities
The CEF2 Digital programme will grant funds for 5G technology in smart communities to modernise socio-economic drivers in many sectors, notably in healthcare, education, public administration and transport, making them more efficient and resilient

cloud and edge computing, including objectives in terms of investment and take up as set out in the EU Digital Decade Policy Programme 2030[11]. Cloudification of networks[12] and specifically the RAN (and Open RAN[13]) may propel and ease the deployment of private networks[14];

- Technical implementation and radio spectrum used by private mobile networks can depend on the mode of deployment. For example, as regards 4G LTE and 5G technologies, private mobile networks can be deployed in the following variants:
    - **Standalone Private Network[15]**, i.e. operated by a non-public network (NPN) actor and not relying on network functions provided by an MNOs Public Land Mobile Network (PLMN)[16]; or
    - **Public network integrated Private Network**[16,17], i.e. a non-public network deployed with the support of an MNOs PLMN
- The traditional vertically integrated mobile value chain is expanding, and there are new market players at different levels in the value chain (market players inventing new business models and/or implementing new solutions) which may give rise to barriers to deployment in some cases.

In addition to the above, the GSA sets out that [3GPP-based] private mobile networks are often part of a broader digital transformation programme for entities, which gives some insight into the drivers of these networks, but there may also be other drivers which could influence supply/demand:

- *"Organizations of all types are combining connected systems with big data and analytics to transform operations, increase automation and efficiency or deliver new services. Wireless networking with LTE or 5G enables these transformations to take place even in the most dynamic, remote or highly secure environments, while offering the scale benefits of a technology that has already been deployed worldwide.*" And
- *"The arrival of LTE-Advanced systems delivered a step change in network capacity, throughput and deterministic latency. 5G networks will bring increased densities of users and devices, even greater capacity and further improvements to latency that enable use of mobile technology for time-critical applications"*

[11] DECISION (EU) 2022/2481 of 14 December 2022 establishing the Digital Decade Policy Programme 2030.
[12] See also the BEREC Study carried out by Stratix/Plum on "Study on the trends and cloudification, virtualization, and softwarization in telecommunications" which examined the impact virtualization on private networks (see Appendix D of the study): https://www.berec.europa.eu/en/document-categories/berec/reports/external-study-on-the-trends-and-cloudification-virtualization-and-softwarization-in-telecommunications.
[13] BEREC Document BoR (22) 138 Summary Report on Open RAN workshop.
[14] BEREC Document BoR (24) 136 BEREC Report on Cloud Services and Edge Computing, which spotlights this aspect.
[15] Of course 'standalone' in this definition means a 'separate/distinct' private network, not to be confused with standalone 5G / 5G SA network which is a 'non-hybrid' 4G5G network consisting of a 5G core.
[16] Terminology set out in ETSI 3GPP TS 28.557 V18.2.0 (2023-12). A Non-Public Network (NPN) is a 5GS deployed for non-public use, see TS 23.501
[17] https://www.drei.at/de/business/grossunternehmen/loesungen/private-network/private-independent-network.html

In short, how market demand can be met for broadband private networks may be of interest in terms of efficient use of spectrum, and other market shaping aspects associated with spectrum assignment including interoperability / interworking and roaming issues.

2.1 Definitions

Considering the terminology used by international organizations, BEREC notices parallel and interchangeable use of terms private networks, private mobile networks and non-public networks, which can lead to misunderstandings if care is not used to describe the context at hand. Below sets out some relevant definitions observed by BEREC:

3GPP[18] adopts the definition of a Non-Public Network (NPN) as a 5G System (5GS) deployed for non-public use: "*In contrast to public networks that offer mobile network services to the general public, non-public networks are intended for the sole use of a private entity such as a college or an enterprise. Non-public networks may be deployed on the entity's defined premises such as a campus or a factory to provide coverage within a specific geographic area*".

According to the European 5G Observatory[19]: "*Private networks are best defined as those networks that are not typically utilised by consumers (for mobile voice and data services) but use network elements and resources to provide dedicated secure services to private enterprises such as factories, plants, large campuses, ports and airports*".

The 5G PPP Technology Board[20] follows the 3GPP terminology and refers to 5G technology on private networks as Non-Public Networks (NPNs): "*An NPN is a 5G System (5GS) deployed for the sole use of a given customer (e.g., vertical customer, government, industry…) and is designed to support services for non-public use, including infrastructure services, communication services and other digital services*".

GSA[21] sets that a private mobile network – also called a Non-Public Network (NPN) provides mobile services for a dedicated and clearly defined set of users or 'things' that are usually part of a single organisation.

NRA views

Out of the 27 NRAs that answered the questionnaire and have full or partial responsibility of spectrum management, only 7 NRAs provided a definition for private mobile networks from their regulatory framework and more specifically[22], they:

- either use a definition that was adopted before the arrival of 4G-5G broadband technologies and thus refers to all private networks (also TETRA, P25, Digital Mobile Radio, GSM-R and Wi-Fi) (e.g. EL, IT, LV)

[18] https://www.3gpp.org/ftp/tsg_sa/WG5_TM/TSGS5_153/SA_103/28557-i30.docx
[19] https://5gobservatory.eu/5g-private-networks/
[20] https://5g-ppp.eu/wp-content/uploads/2022/11/WhitePaperNPN_MasterCopy_V1.pdf
[21] https://gsacom.com/non-public-networks-private-mobile-networks/
[22] DK, EL, HR, IT, LV, NL, SI

- or introduced definitions for specific use for broadband networks (e.g. HR, DK[23]) or in the frame of a tender procedure (e.g. SI) or a license issuing procedure, coupling the network to a specific organisation and plot or location (e.g. NL, DK)

In some cases, although a specific definition has not been adopted, several conditions have been set in the license that is granted so that a private mobile network is properly delineated from other network types (e.g. CH).

2.2 Architectures of private networks/interrelations with public networks

There are many configurations / architectures of private mobile networks from the isolated standalone private networks to public network integrated private networks in the form of a network slice. 5G Alliance for Connected Industries and Automation (5G-ACIA) has identified the four major scenarios of private networks.[24]

2.2.1 Standalone private network (isolated deployment)

The first scenario is standalone private network, where all network functions are located inside the defined premises of the organization and the private network is separate from the public network.

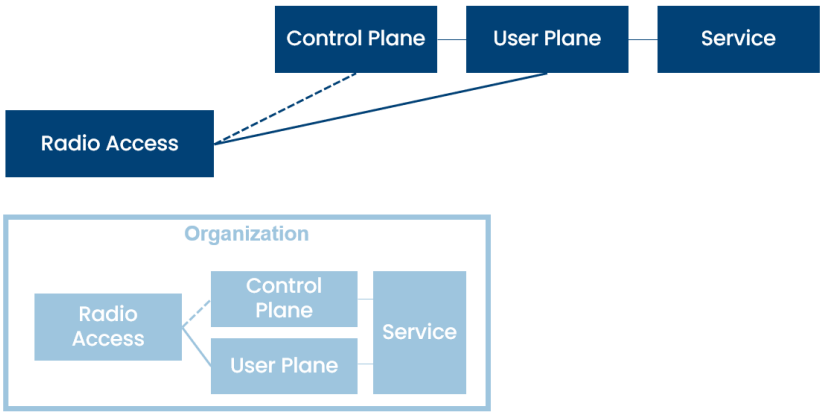

Figure 1: Standalone private network (isolated deployment)

2.2.2 Private network in conjunction with public networks

Shared radio access network

[23] Specifically with respect to the 3400-3410 MHz and 24,25-24,65 GHz frequency bands.
[24] WP_5G ACIA Private Networking_KURZFASSUNG_July 2019_22.07.19.indd (5g-acia.org)

The second scenario is public network integrated private network with shared Radio Access Network (RAN)[25], where part of the RAN is shared among the owner and the mobile operator. All other network functions are segregated as in the case of standalone private network. Note that with this scenario, the private network data resides within the defined premises of the organization.

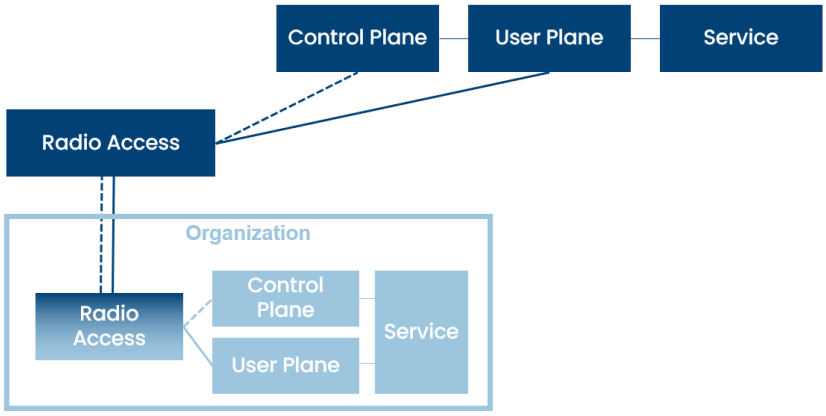

Figure 2: Shared only the radio access network

Shared radio access network and control plane

The third scenario is the deployment with shared RAN and control plane, where not only the RAN is shared but also the network control tasks are performed by the public network. Note that the NPN data still resides within the defined premises of the organization. This scenario can be implemented by the means of Access Point Name (APN) or network slicing, where a network slice can be dedicated to the owner of the private network.

[25] For now, we do not distinguish between the different forms of RAN sharing but please see here for more information BEREC Common position on infrastructure sharing (europa.eu) page 13.

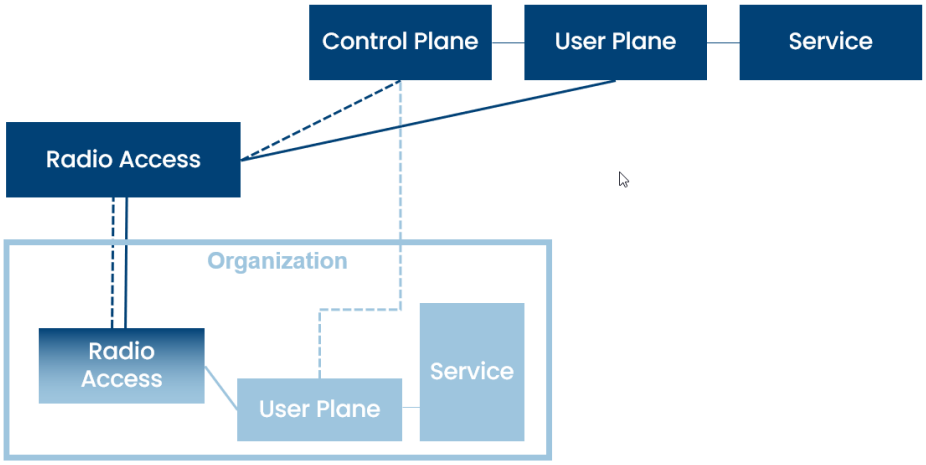

Figure 3: Shared both the radio access network and the control plane

2.2.3 Private network hosted by the public network

The fourth scenario is where the private network is hosted by the public network. This means that the private network is deployed in the public network and the public network from end-to-end is used for private network. This scenario can also be implemented by the means of APN or network slicing, where network slice in this case would be end-to-end.

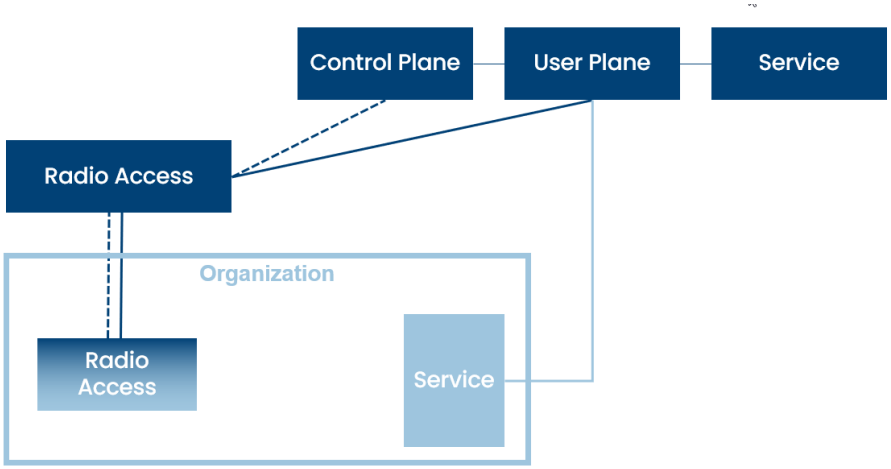

Figure 4: Private network hosted by the public network

2.2.4 Architecture options and spectrum

The architectures described above are independent of the frequency ranges that are used to implement an architecture. However, because of national differences, regulation and history, some NRAs tend to also consider the primary holder of the rights of use to the spectrum to classify networks as ‘isolated’ or ‘integrated’, while others put more stress on the way networks are deployed regardless of the origin of the spectrum. As a result, some NRA answers with

regards to the classification of private networks were interpreted flexibly by BEREC at this point.

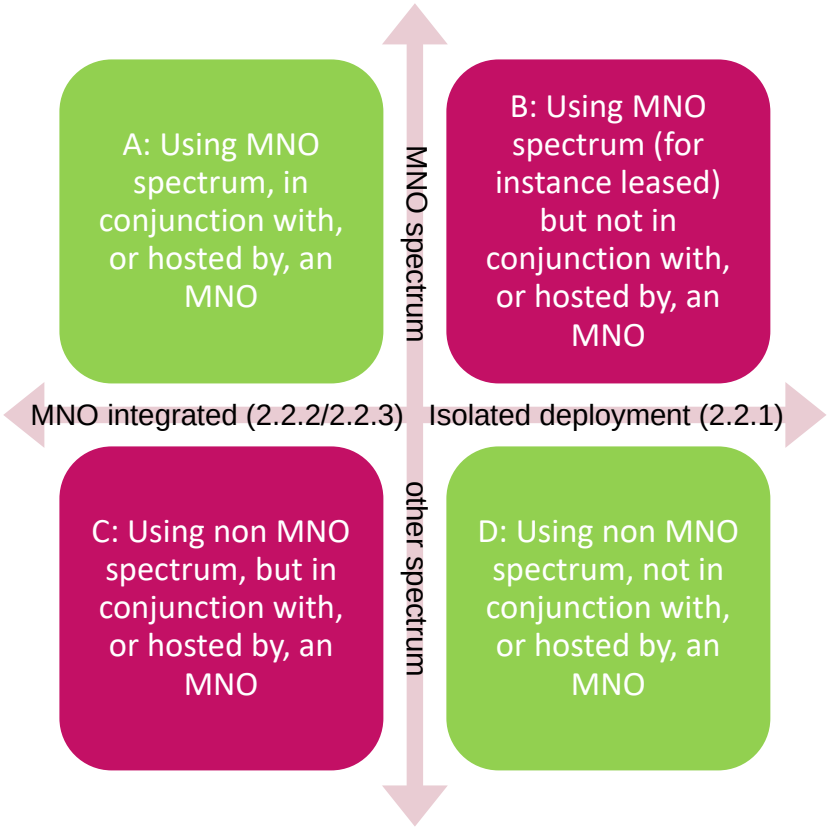

Figure 5: Architecture and spectrum options matrix – source BEREC

BEREC is curious whether all the variants (A, B, C, D) described in the figure above exist in practice and whether or not there would be merit in harmonizing an approach to classification. Many of the stakeholders that gave input to the public consultation ensured that all above variants are used in practice but acknowledged that the most common variants are public network integrated non-public and standalone non-public (variants A and D).

- Variants A and D (see descriptions above) are very well understood by NRAs, even if there were few examples,
- Variant B (using MNO spectrum, but using a network architecture not in conjunction with, or hosted by, an MNO) may be used in some European countries, but in many cases these networks do not need to be specifically registered by an NRA or because they would fall under spectrum leasing frameworks, were not directly considered by NRAs when responding to this particular questionnaire.
- Variant C (using non-MNO spectrum, but using a network architecture in conjunction with, or hosted by, an MNO) may be restricted in many European countries (for example on competition grounds and level of spectrum resources controlled by

MNOs). Where allowed, these networks may sometimes be registered as separate networks, in other cases be considered part of MNO networks.

2.3 Status of private network spectrum regulation

As mentioned above, there are several implementations of private networks which differ on whether they use components of public networks and what parts of them they use.[26] Private mobile networks also differ by spectrum band used. The RSPG's extensive work from October 2023 on private 5G in its Opinion on "5G developments and possible implications for 6G spectrum needs and guidance on the rollout of future wireless broadband networks" [27] is an essential source for inclusion in this report. It discusses the need for planning and use of spectrum, infrastructure development, regulatory harmonisation, research and innovation.

Spectrum is an essential input when implementing a private mobile network. Spectrum may be used on a licence exempt basis (where appropriate), on a licensed basis (where spectrum is assigned locally for the purpose of a private network), or on a leased basis between operators (where specific spectrum rights are leased from an existing operator with exclusive frequency usage rights). Such a lease might be based on a voluntary agreement or based on conditions attached to the rights of use that make such lease mandatory.

According to the results of the questionnaire, half of the countries have allocated dedicated spectrum bands or frequency ranges for use by private operators. When comparing the different frequency bands used to implement private networks in Europe, it is clear that the private network users seek access primarily to resources in the 3400-3800 MHz frequency range (the 26 GHz band is also available, but not widely used).

Such high-level information was provided because of the respective licensing activities of the NRA (e.g. whether an individual licence was granted, an experimental licence, or via public operator spectrum with relevant consent etc). Only one country has a reporting obligation on private networks in public mobile bands (EL), EL is therefore able to report that there are 7 private networks of which 2 are under development at the time of writing, all integrated within the public networks.

The lack of EU spectrum harmonisation has in some cases contributed to national options for private mobile networks. For instance, a possible reason for the current more frequent (according to the provided data from the NRA) use of 3400-3800 MHz for private 5G networks among the reporting countries could be the fact that 3800-4200 MHz has not yet been harmonized.

3400-4200 MHz

[26] However, all private networks are restricted to a specific user group/end user organisation and thus not open to the public. A private network enables a connection between a limited group of users, thus the wider public cannot use the private network.

[27] RSPG Opinion on 5G developments and possible implications for 6G spectrum needs and guidance on the rollout of future wireless broadband networks - Document RSPG23-040 (October 2023)

Table 1 provides an overview of the information provided by NRAs for private mobile networks in the 3400-4200 MHz frequency range. The information is illustrative and not intended to be exhaustive because most NRAs have limited engagement with private network actors. NRAs that provided information generally did not elaborate on specific criterion at this stage, so the table highlights both where BEREC made an enquiry and where an NRA may have made a remark. In particular, seven NRAs indicated a total number of private networks using this particular band in their country. [28]

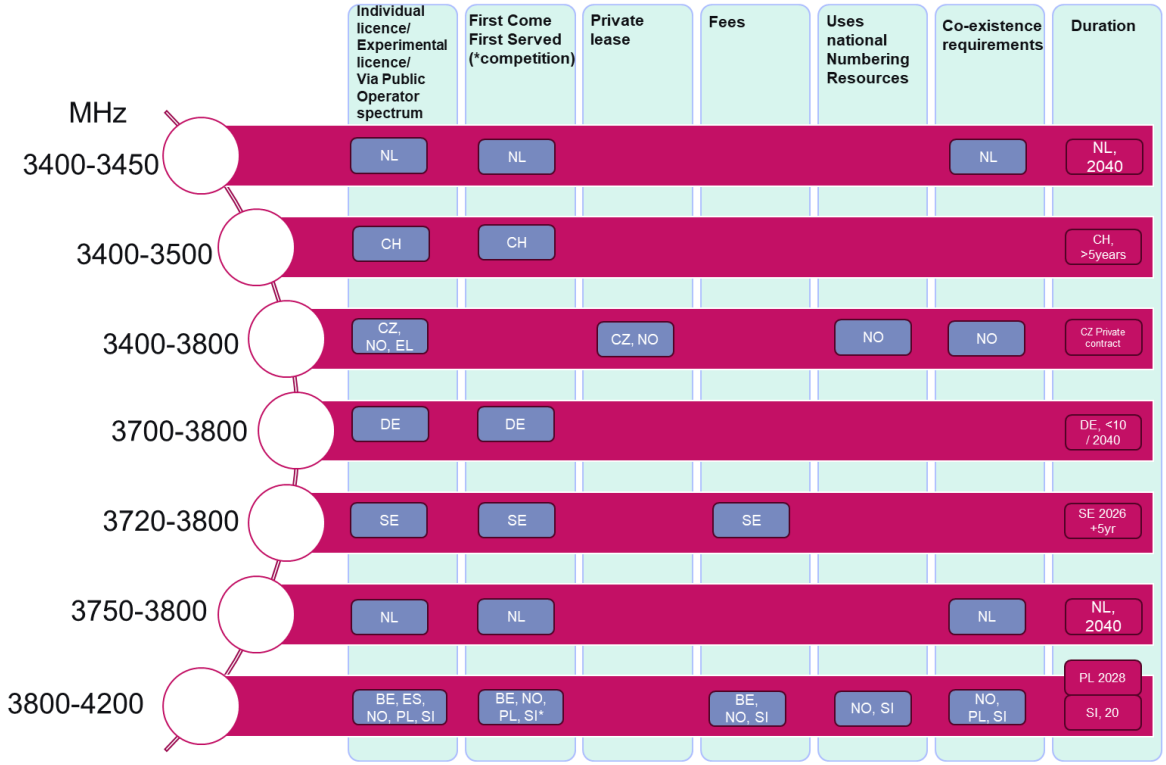

Table 1.0 Overview of information on 3400-4200 MHz – illustrative purposes only.

As stated above, the frequency range 3400-4200 MHz is the most common range for private 5G networks in Europe. Germany reports about 400 networks in that spectrum range, Sweden (PTS has granted 90 permits in 3700MHz and 4 permits in 26GHz[29]), Spain 43 in the 3800-4200 MHz (temporary experimental authorisations and only 10 remain in force at time of writing) and Norway about 30 networks. Slovenia reported one network is operating on temporary basis in 3800-3900 MHz. Slovenia plans to open the whole 3800-4200 MHz for local networks in 2025. The NRAs from other countries report single-digit numbers or none at all. Spectrum usage rights are either based on individual licence requiring a specific application or leased from mobile network operators. In the former case, it is almost always on a first-come first-served principle. Slovenia granted access in public procurement 20 MHz in the band 3400-3420 MHz on a local basis to one MNO and 4 local users (industries and local communities). Reported individual licences were granted on a local basis, so there is

[28] BE, CZ, DE, ES, NO, PL and SE
[29] The numbers for SE only reflect number of granted local permits (and may include inactive networks)

usually sufficient spectrum available. In the latter case, private networks lease spectrum from an MNO which has purchased the usage rights. All the relevant NRAs from countries set out at Table 1 reported the use of particular licence conditions, such as payment of fees or rules on existence with other networks. Licences are granted for periods between 5 and up to 20 years, with most licences being available up until 2040 thus enabling long-term investment (Germany). In terms of the number of networks, Germany is leading with around 400 known private networks. NRAs did not report having legal intercept requirements in licences issued for private networks.

Other frequency ranges

For mmWave spectrum, five countries (DE, EE, ES, LV, SE) report private networks with specific spectrum licences and only three report numbers of networks (DE, ES and SE[30]). BEREC concludes that private networks based on mmWave are therefore less popular compared to midband 3400-4200MHz. SI reported on a plan for introducing private networks with specific spectrum licences in part of mmWave.

Another band mentioned by two NRAs is the 2300-2400 MHz band. ES grants individual licences for up to 20 MHz on a first-come first-served basis and mentions private networks in several sectors. SI granted in a public procurement access to 30 MHz in that band on a local basis to one MNO and factory, harbour and a local community.

In HR, the 2600 MHz TDD band is being used for a private 5G network in the seaport of Rijeka. FR also reports use of 2600 MHz for private mobile networks.

Three countries (NL, SE and SI) report other private mobile networks in some bands, but with only up to 5 MHz in FDD mode.

Four countries (BE, EL, ES[31] and SI) report private networks in public mobile bands, integrated into public networks and based on MNO spectrum (700MHz, 800MHz, 900MHz, 1800MHz etc).

For SI, in frequency bands 800 MHz, 900 MHz, 1500 MHz, 1800 MHz, 2100 MHz, 2600 MHz private networks can be provided only by MNOs.

For DK, without prejudice to MNO licence obligations, MNO's may use their licenced spectrum in 700 MHz - 26 GHz both for standalone private networks and for public integrated private networks if they wish to do so. This is entirely up the MNO's commercial considerations.

[30] DE reports 19, ES reports 1 and SE reports 4 in mmWave

[31] ES reports public network integrated private networks deployed using MNOs spectrum, mainly in 3400-3800 bands, but sometimes with additional use of lower bands (such as 700 MHz) for better indoor coverage.

3 Numbering considerations

The introduction below is based on NRA answers to the questionnaire as set out in BoR (24) 150 and complemented with a selection of relevant observations from the stakeholder consultation (see also Annex A and BEREC Document BoR (25) XX/YY published alongside this report).

Private mobile networks can be deployed in a standalone or a public network integrated model (see section 2.2), which may have implications on numbering resources availability and assignments.

End users in a private network need to be uniquely identified to that specific private network. One option is for private mobile networks to rely on numbering resources (e.g. IMSIs[32]) based on a shared Mobile Country Code (MCC) (e.g. MCC=999) that has been allocated by ITU TSB in 2018. Another option is to specifically allocate MNC numbers within the national E.212 numbering plan. In the case of shared MCC999, neighbouring private networks that might rely on the same MCC might end up in a situation where a number might not work anymore as a unique identifier. In that case, co-ordination between neighbouring private networks is required.

3.1 E.164 numbers

Standalone private networks providers can use any sequence of numbers to identify the user devices attached to the private network. Generally, NRAs only assign E.164 numbering blocks to service providers intending to offer a publicly available (number-based) ECS. If private networks are interconnected with public networks for voice or SMS services, they are likely to need public E.164 numbering resources in order to be able to call public network subscribers and to receive calls from public networks. Among the NRAs that responded to BEREC's questionnaire, only 2 (AT and CZ) received at least one request for E.164 numbers for standalone private network.

Operators of public network integrated private networks usually use the numbers assigned to the MNO in which the private network is integrated. Among the respondents, only one NRA received at least one request for E.164 numbers for a public network integrated private network (CZ).

3.2 Mobile Country Codes and Mobile Network Codes (MCC-MNC)

Standalone private network actors have four options regarding MCC-MNC:

- Unique MNCs under the geographic MCC: 3 NRAs (BE, ES, FR) decided to assign 2-digit or 3-digit MNC codes to private mobile networks with their own spectrum. This

[32] The International Mobile Subscriber Identity (IMSI) is a unique number intended to identify subscribers attached to a specific mobile network. It is composed by adjoining the Mobile Country Code (MCC), Mobile Network Code (MNC) and the Mobile Subscription Identification Number (MSIN).

type of MNCs is particularly suitable for private networks that need to be connected to public networks and that need extended coverage throughout the national territory, with high requirements regarding safety and reliability.

- Specific MNCs allocated under the geographic MCC for shared use by private mobile networks: this type of MNC is available in 7 (BE, CZ, DE, IT, FI, HU, SE) countries among the respondents[33]. NRAs point out that interoperability between private and public networks cannot function with this type of MNC (for shared use).

- MCC 999, dedicated to private networks for shared use in ITU-T Recommendation E.212: this type of MCC/MNC is recommended at first by 16 NRAs (AT, CH, CY, CZ, DE, DK, ES, FI, FR, HR, IT, MT, NL, NO, PT, SE and SI) and proposed as one of two solutions with no preference by 3 NRAs (BE, DE, HU). This option is particularly suitable for private networks with localized coverage since MNC under the MCC 999 cannot be used outside of the network for which they apply (interoperability is not available).

- MNCs under shared MCCs 901 and 902, which are assigned by the ITU-T to entities who meet the eligibility criteria according to Annex A and Annex H in ITU-T Recommendation E.212. Such entities typically operate international networks with connecting physical nodes in two or more countries, and where the networks are intended for commercial implementation in at least two countries, or in geographical areas in two different countries.

Operators of public network integrated private actors can use the MNC assigned to the MNO in which the private network is integrated or make a request for a new MNC under the geographic MCC to the NRA. Among the respondents, 6 NRAs received at least one request for a specific MNC for public network integrated private networks provided by MNOs.

The assignment process for MCC/MNC for private networks takes mostly two forms among NRAs:

- Direct attribution to spectrum license holders: 5 NRAs (CZ, DE, ES, HU, PT) indicated using this assignment process for MNC under the geographic MCC.

- No direct attribution, i.e. MNC allocated to private network under geographic MCC and/or MNCs under global MCC 999 are allowed to be used on a free-for-all (uncoordinated) basis: among the respondents, this is the case in 3 countries (NL, FR, and SE) for allocated MNCs under geographic MCCs, and in 8 countries (CH, CZ, DE, DK[34], ES, FI, FR and SE) for MNCs under global MCC 999.

However, this assignment process of MNCs for shared use by private networks raises some concerns since there are no guarantees that the MCC/MNC is not already used in the concerned area and could therefore result in interferences. In this case, the devices may attempt to connect to another private network using the same PLMN ID[35] (MCC+MNC). Most

[33] In one country (FR), another range of MNC under the geographic MCC is available for test-only private networks.
[34] DK encourages use of global MCC999
[35] See clause 12.1 in 3GPP TS 23.003

NRAs indicate that it is the responsibility of the parties involved to coordinate and avoid interferences. 4 NRAs (BE, DK, NL, PT) leave the coordination process to the parties involved, 5 other NRAs (AT, CZ, DE, MT, NL) have implemented or will implement measures to encourage coordination such as:

- for MNCs under geographic MCC: 3 NRAs (CZ, DE and NL) have included in spectrum licenses an obligation to find an agreement and coordinate to prevent incompatibility, when the MNC is allocated to a license holder;
- for MNCs under MCC 999: 2 NRAs (AT and DE) advise providers of private networks to inform them of the MNCs they use and the area they cover so that the NRAs can inform (informally or through a public directory) the willing-to-be private networks in the same area of MNCs used in their area to avoid the use of the same MNC for different private mobile networks. One NRA (MT) intends to adopt such an approach should it receive requests for numbering resources from providers of private mobile networks which may be satisfied through MNCs under global MCC 999.

Concerning the Operating System (OS) of terminals used in a private network there might be some limitations of what combinations of MCC/MNC can be used for the private network. Other restrictions on access to services or functionalities by OS providers are also set out in the BEREC Report on the entry of large content and application providers into the markets for electronic communications networks and services.[36] As regards limitations in the context of private networks, these might differ between OS providers and maybe between different terminal vendors for a specific OS.[37]

3.2.1 Issuer Identifier Numbers (IINs)

Geographic IINs are allocated by ITU to Member States and then NRAs assign IINs to actors. Registrations forms[38] are submitted by the country approving organization, most frequently NRAs, for completion before it is sent to ITU for registration. Among the respondents, 2 NRAs (DE and SE) received requests for IINs for standalone private networks.

3.2.2 eUICC Identifier (EID)

EIDs are assigned directly by the GSMA.[39] One NRA (DE) indicated that a public network integrated private network in its country has applied for an EID.

[36] BEREC Document BoR(24) 139 Report on the entry of large content and application providers into the markets for electronic communications networks and services.
[37] Apple have public information (https://support.apple.com/en-mt/guide/deployment/depac6747317/web) on which MCC/MNC combinations for private 5G and LTE networks are supported by its OS.
[38] https://www.itu.int/en/ITU-T/inr/forms/Pages/iin.aspx.
[39] eUICC Identity Scheme - Device Services (gsma.com).

3.2.3 Other kinds of 3GPP numbering resources

One NRA (DE) assigned other numbering resources for the use in combination with a shared MNC under the country MCC such as Closed Subscriber Group-IDs (CSG IDs)[40], Tracking Area Identities (TAIs)[41], E-UTRAN Cell Global Identification (ECGI)[42], Globally Unique Mobility Management Entity Identifier (GUMMEI)[43] and Network Identifiers (NIDs)[44].

Another NRA (SE) is investigating the option of also using NIDs for private network.

3.3 BEREC's summarizing insights on numbering

BEREC notes that using self-assigned MNCs under the shared MCC 999, provided by ITU-T for private networks, is the preferred option for most stakeholders to avoid wasting numbering resources. In fact, one stakeholder suggests using 3-digit MNCs, as they allow for 1,000 MNCs instead of just 100 under MCC 999.

Public MNOs can use their existing MNCs for private networks, as long as private users are isolated from the public network. However, BEREC points out that a unique MNC would be needed for private network use cases requiring roaming onto the public network, which could provide a competitive advantage to MNOs.

From the contributions received, BEREC also highlights the need for handset/device support for certain MCC-MNC combinations, which may not always be implemented.

A major concern raised by stakeholders is the risk of network collisions in nearby private networks using uncoordinated shared PLMN IDs, such as with MCC 999. While there are few practical examples due to limited 5G private network deployment, the risk of collisions is more likely in high-demand scenarios and this is an issue that NRAs should already be aware of[45]. Several solutions proposed by stakeholders to address collisions include coordination mechanisms, lower-power transmissions, and the use of more network identifiers.

In summary, BEREC believes further examination by NRAs on a case-by-case basis may be needed. In particular, the role of coordination between networks may require awareness of relevant points of contact between providers. Although some NRAs are implementing measures to encourage coordination mechanisms by the parties, this issue still seems challenging. Further, the potential for combinations of identifiers to serve as a solution remains unclear, as insufficient details were provided to suitably assess the matter. In particular, the assignment of NIDs in 5G networks is currently not coordinated by a competent authority, and some stakeholders question ecosystem support in both handsets and network equipment.

[40] 3GPP TS 23.003 – clause 4.9
[41] 3GPP TS 23.003 – clause 19.4.2.3
[42] 3GPP TS 23.003 – clause 19.6
[43] 3GPP TS 23.003 – clause 2.8.1
[44] 3GPP TS 23.003 – clause 12.7
[45] This concern has also been addressed in ECC Recommendation 17(02) amended 28 November 2023 *"Harmonised European Management and Assignment Principles for E.212 Mobile Network Codes (MNCs)".*

BEREC's goal at this point is to raise awareness of these issues for NRAs, and as more 5G private networks are deployed, sharing best practices will help address these challenges.

4 Drivers and case studies

The paragraphs below are based on NRA answers to the questionnaire as set out in BoR (24) 150 and complemented with a selection of relevant observations from the stakeholder consultation (see also BEREC Document BoR (25) 32).

Paragraph 4.1 summarises the various drivers for the implementation of private networks. Paragraph 4.2 summarises several relevant case studies mentioned in the consultation responses. Paragraph 4.3 describes BEREC's view on the drivers and use cases.

4.1 Various drivers for the implementation of private networks

Some NRAs briefly mentioned sectors / examples of private networks in their responses, such as logistics and warehousing as well as manufacturing. For logistics and warehousing, NRAs reported that ports, airports and railways logistics increasingly rely on private networks. For manufacturing, private networks were mentioned in the automotive and chemical industries. Educational institutions were mentioned by three NRAs, electricity and energy and public authorities (including defense) by a further two NRAs. Other examples mentioned included the extraction of raw materials/mining, agriculture, forestry, and retail and healthcare.

NRAs provided limited views on drivers for the implementation of private networks, but some views can be described by BEREC as follows:

- While private mobile network implementation is more widespread in certain sectors than others, most industries seem to have examples of private network connectivity solutions.
- The existing availability of public 5G networks (or Wi-Fi solutions) may not suit certain business requirements (e.g. control ownership or certain QoS requirements) so users turn to other solutions for more control over latency, capacity or other requirements that cannot be met in other ways. In some cases vendor lock-in may be a reason, including the need to be in full control of technology upgrades etc. The principal reasons for developing a private 5G solution seem to be many and varied. First and foremost, there are all the improved service parameters that a 5G service has to offer but managed on a private / tailored basis: high performance, network flexibility, high reliability, high service availability, low latency, high data rates and network sovereignty. These, in turn, create guaranteed and controlled Quality of Service (QoS), a fast and reliable network with short reaction times and a high level of privacy of information. In a private setting, this can result in stricter supervision of the network and tailored cybersecurity with a better targeted coverage for an industry user who can pick and choose where to put the signal, both indoor and outdoor.
- Such high-level network service parameters may suit specific industrial processes. Up until now, these needs might have been solved by private Wi-Fi networks or other networks. Private 5G connectivity solutions could facilitate the digitalization

of businesses and allow the implementation of use cases with specific connectivity needs depending on the type of industry.

- Security and privacy of business information and data is considered a high need of many industries, as well as a tight integration with the operational systems and optimization of automation.
- Another important factor is the network sovereignty or independence of a private network, which allows for the industry to determine themselves when software adaptations or maintenance cycles need to be carried out. With this, other advantages emerge such as strong cybersecurity and the protection of confidential data, as well as the ability to supervise the network, all decided by the industry themselves.

4.1.1 Drivers as described during the consultations

In the main, the information received during the consultation on drivers for 5G private networks was consistent with the NRA views. BEREC thanks respondents for the information which it considers is helpful to know. Interestingly, BEREC received few indications of network slices being used to provide private mobile network functionality.

4.1.2 BEREC's observations and considerations on drivers

BEREC considers that depending on the needs, the cost of the solution, and the level of technical knowledge inside the company using a private network, the deployment of the private network can be led by the company via a standalone solution with owned spectrum, led by, or outsourced to, specialist providers including MVNOs, with spectrum owned by them or their customers for private 5G Networks or led by the MNO with different configuration possibilities (see section 2.2.4). BEREC understands that the deployment of a private 5G solution may also satisfy other financial returns, such as enhancing efficiencies in terms of site management, remote monitoring, and addressing bespoke risk management requirements. In short, BEREC considers that drivers combine to provide additional long-term return on investment including increased efficiency, higher productivity and reduced energy consumption.

4.2 Case studies

BEREC sought information on case studies as a way to understand if any potential regulatory barriers need to be overcome in establishing the particular 5G private networks.

4.2.1 NRA views

Most NRAs provided only high-level views in their survey responses on private network case studies in their countries or on the applicable radio spectrum regulation approach where private networks have or have not been deployed to date (AT, CH, DK, IE, LV, LT, LU, ME, MT, NL, PT, UA), with some setting out that lists of case studies are reported on by the 5G

Observatory (5G Private networks – 5G Observatory) and other publications (such as the Swedish Broadband Forum report on use cases[46]). The reason for this is that most NRAs do not require a specific license for the use of spectrum for the private network (see section 2.3).

In general, reasons for the lack of information on private networks in countries include that 1) it is too early to provide such information because pilots and trials are ongoing, 2) there are no (regulatory) obligations for private networks to provide information to NRAs, 3) there are no private networks in operation, or 4) the data of licence holders for private networks (where applicable) are treated as trade and business secrets (DE).

Where NRAs did set out information on case studies, BEREC observes a variety of use cases such as;

- to digitise and automate operations of underground mining (FI, SE)
- seaport terminal and energy-efficient cargo handling (ES, FI and NL)
- a neutral host indoor mobile connectivity network solutions provider (SE)[47]
- ultra-low latency smart manufacturing (SE)
- secure logistics (NO)
- specific business activities at submarine network landing sites (FR), and
- smart factories and robotics solutions (CZ), to name but a few.

One NRA publishes information on its website via a portal dedicated to the ongoing trials of professional mobile networks in 4G/5G technologies (FR). In particular, the NRA's online portal gives access to (i) an interactive map of the ongoing trials in 26 GHz, 2.6 GHz TDD and 3.8-4.0 GHz bands; (ii) an OpenData including description on the trials that are both ongoing and that are finished, in the same bands (https://exp5g.arcep.fr/).

4.2.2 Use cases as described during the consultation

In its public consultation, BEREC invited contributors to provide any additional information they may have about use cases.[48] BEREC thanks the respondents for their views and encourages readers to consult all the case studies by reviewing stakeholders' full contributions, which are published alongside this report on the BEREC website.

[46] Reports available here https://bredbandsforum.se/media/1400/Private5GnetworksinSweden2023.pdf
[47] However, no application for an MNC for this type of use case
[48] The call to invite stakeholder views on case studies and drives was because based on the results of the NRA survey, the ability of BEREC to extract information on specific drivers for private networks was limited. For example, it was not clear if the driver was because of technical features of 3GPP based private networks or a cost efficiency reason arising from implementing a private network into business operations, or a combination of these two reasons and others. In almost all cases from NRAs, there seemed to be multiple drivers and no one killer application. In short, the requirements of private networks seem to be varied. In addition, NRAs provided little information about neutral hosting and interworking with 5G PLMNs.

In line with BoR (24) 150, and from the selection of case studies received, BEREC has carefully considered the descriptions of two use cases[49], which also include details about targeted drivers for deployment of their 5G private networks.

a) Case Study 1: Professional production of audiovisual content

Use case description provided by the stakeholder[50]

Audiovisual productions underpin all media services including broadcasting. Thereby a range of use cases is covered: news gathering, live productions such as music festivals with recording or sports events, but also documentaries, drama, etc. AV productions can be complex with a multitude of signals including video and audio signals, telemetry, communication, tally etc., which have to be transmitted together synchronously and error-free, often only with minimal latency. Especially for live productions, very high quality (Quality of Service, QoS) is extremely important, since live events cannot be repeated, and quality cannot be increased at a later stage. Tests and trials confirmed that the 5G technology, under the right conditions, can provide high-performance connectivity with high data rates and low latency that meet the technical and operational requirements in several production use cases, such as remote production, live events, breaking news, and studio production. 5G also offers new possibilities for media production and seems to be well suited for cloud- and IP-based productions.

Identified drivers for the use of 5G SNPNs in professional content production:

- Operational flexibility

Wireless productions can dramatically reduce the effort of a production. Setup time is shorter; changes are easier as there are no cables to install. This also means no safety measures to consider due to the risk of accidents caused by cables. As wireless equipment is mobile it allows the crew to react more spontaneously to developments at live events and get closer to people. Remote productions are also possible.

Wireless production equipment such as cameras, microphones, in-ear monitors, telemetry and communications equipment, also known as Programme Making and Special Events (PMSE) applications[8], is widespread and has been in use for a long time. With conventional PMSE each of these devices needs its own radio link in its own frequency and dedicated infrastructure. This means a high coordination effort, long planning and high costs, especially for larger and complex productions.

- Technological developments

Production technologies are generally moving to IP supported workflows and this also requires wireless production technology to be updated to support these workflows. In IP-based production, different signals are treated as individual IP streams. A 5G network allows different signals to be carried within the same bi-directional radio connection as illustrated below:

The demands of different use cases require different network characteristics. At the same time, 5G specifications provide for various network configurations. Best efforts 4G and 5G mobile networks are widely used for bonded cellular solutions. For some use cases, a professional service in a public telecom network with guaranteed QoS may be appropriate if the 5G network provides a wide coverage area and network capabilities that are adequate to meet the production requirements. Technically, QoS in public 5G networks may not suit requirements. Another technical consideration is that public mobile networks are designed to

[49] Stakeholders from the European Broadcasting Union and Volvo Autonomous Solutions provided use cases
[50] Please consult the stakeholder responses for the definitive version of their views

support higher downlink than uplink traffic whereas audiovisual productions typically require much higher uplink than downlink capacity.

Therefore, if a large uplink capacity and guaranteed QoS are required, a dedicated, standalone non-public 5G network (SNPN) may be used, primarily to provide local connectivity. This option is particularly interesting for some media production use cases as the network can be configured to meet specific production requirements and is not shared with general public. It is important that 5G NPNs can be deployed permanently (e.g. in the production facilities or on campus) or temporarily (e.g. for the duration of an event). They may be deployed either by the production team itself or by a third party, e.g. provided by venue owners or specialised companies.

- Productivity and cost efficiency

There are expectations that the use of 5G in content production will enable better utilisation of the crews and equipment leading to higher productivity. 5G also enables efficient use of network resources dynamically. The economies of scale achieved within the global 5G ecosystem are expected to result in lower costs of equipment and networks.

- Security

Most productions, especially when the content is of high commercial or cultural value require the content to be protected which may be easier to achieve in a 5G SNPN than in a public network.

b) Case Study 2: Private Networks in Mining & Quarry applications

Use case description provided by the stakeholder

Connectivity is a crucial enabler for digitalization, electrification and especially automation of the mining and quarry business. A dimensioning use case is deployment of autonomous vehicles on a site, such as trucks hauling material from point A to B. In this context, private networks are used to provide secure and reliable connectivity between a central control tower and the autonomous vehicles.

Non-Public Networks (NPN) in the form of local standalone 5G networks are a good match for this kind of open pit implementations. This is due to the fact that a larger area typically can be covered with a significantly less amount of network infrastructure compared to traditional Wi-Fi networks running on license-exempt spectrum. Further, access points in Wi-Fi networks in Europe are not allowed to use the same amount of output power as base stations in private 5G networks, which is the main reason for the less amount of network infrastructure equipment required for private 5G networks. High throughput Wi-Fi is also operated almost 1.5 GHz higher up in carrier frequency further reducing the effective communication range. Many of the mines and quarries are also located in areas with limited access to public networks and poor availability of fiber networks, meaning that a local standalone often is the most suitable solution.

The main drivers for deployment of private mobile networks in autonomous applications in the mining and quarry context were described as follow.

- Many sites are located in areas with no or very poor access to public networks, meaning that it is often not cost efficient to expand the public network to these locations. It is also by definition so that extracting of material from the ground creates an open [mining] pit where coverage of public mobile networks is problematic unless new antennas are installed anyway.
- Autonomous systems typically require a stable and predictable network since a glitch in communication or a spike in latency can cause costly stops of vehicles and transport

operations. Achieving the required level of stability and predictability may be problematic in public mobile networks, but is often fulfilled by local private network where the QoS parameters like latency, traffic prioritization and network load can be controlled and monitored, with alsothe possibility to control service windows and upgrades.

- MNO offerings may not suit private 5G network requirements due to cost implications for services only requiring low numbers of SIM-cards.
- The flexibility to tune the network for high uplink applications is crucial for most industrial use cases. The data is typically generated by machines and sensors onboard the connected devices and needs to be sent to central servers and data centers for processing, instead of the typical consumer use cases where the data is distributed from servers and data centers to the connected devices (e.g., phones, tablets, TVs etc.). In public networks, the downlink capacity is far more important than the uplink capacity, and it is the other way around for industrial use cases such as the operation of autonomous machines and trucks in mines and quarries.

4.2.3 BEREC's observations and considerations on use cases

The information on use cases elaborates on the potential of private 5G networks and is interesting for BEREC to receive. At this moment the information does not lead to any particular conclusions on regulatory barriers to deployment of private 5G networks. The result of the consultation revealed a set of interesting challenges some of which are summarized in a dedicated chapter (chapter 5) and which BEREC highlights so that NRAs can consider in more detail as part of their own studies on private 5G mobile networks.

BEREC will continue to engage with stakeholders on private 5G networks to ensure that it can provide support to NRAs on relevant developments (challenges and deployments) in the markets of its Members and Participants without Voting Rights.

4.3 BEREC's summarising insights on drivers and use cases

The private 5G network use cases are varied and address specific connectivity problems and complement existing connectivity solutions. One key insight is that the deployment of private 5G networks is at different stages in different countries. The interest in private 5G networks is growing and regulators are putting in place frameworks to deal with new demands. If it seems like a nascent market now, it does seem to be gaining momentum. The absence of particular use cases based on network slices offered by mobile operators could be an indication of the limited maturity of stand-alone 5G networks with dedicated 5G cores, something that may have implications in reaching EC's connectivity targets which is a matter outside of the scope of this project.

5 Identified challenges to 5G private network deployment and other observations

While BEREC's enquiry into drivers and use cases did not uncover detailed regulatory barriers, a plethora of interesting ideas and concepts were raised (see topics 1-9 in table 2.0 below). Some of these topics complement the information already presented. Other topics may have been unknown to NRAs during the internal questionnaire stage, and therefore BEREC summarises a selection of observations to raise awareness aout such topics amongst NRAs.

The selection of topics were identified by BEREC following its careful analysis of the respondents answers to the questions set out in BoR (24) 150 (see also annex B for a list of the questions asked) and also after an additional round of engagement with invited experts to a BEREC working group meeting on 27 January 2025 (note non-confidential meeting material is published alongside this report)[51].

Topic/challenge	BEREC's observations
1. Drivers	- Mostly addressed at chapter 4 above i.e no single killer application for 5G private networks - Application Program Interfaces (API) developments may offer new opportunities and capabilities for 5G private networks
2. Administrative and regulatory obstacles for solutions	- No dedicated frequency bands for private networks (e.g. NRA examples include 2.3 and 2.6 GHz and more bands) - Large variety of options between the different Member States (MSs) with regard to technical or administrative requirements resulting in complexity across MSs, for instance with regard to the licensing procedure, lack of coordination on spectrum availability and price variations - Other challenges depending on the specific characteristics of stakeholders, like the timely licensing for private networks that will cover urgent circumstances, or the differentiation of the license with regard to its duration. - Contradiction between need for temporary licences & location nomadic licences (e.g. media production for outdoor events) and longer-term licences (e.g. at ports) - Neutral hosting not widely reported

[51] BEREC would like to thank the individual expert exchanges it held over the course of this project including in particular Port of Barcelona, Port of Valencia and HubOne ADP, Paris

Topic/challenge	BEREC's observations
	- Local variations in licensing probably cannot be avoided and some flexibility may assist to identify what works best, but BEREC can share best practices
3. **Technical obstacles for solutions**	- Network dimensioning differs between networks with different schemes of uplink and downlink UL/DL; this may require inter-network coordination - Availability of an advanced device ecosystem: several stakeholders complain about the lack of devices enabled with important features for private network use cases, 5G enabled devices are currently not always plug and play on networks, resulting in additional time and resources spent on testing devices. So improved availability of approved 5G devices enabled for private networks are needed. - Network collision avoidance (i.e. enabling networks identify devices in high network demand scenarios) is a technical matter. Mix of solutions to network collision avoidance (enhanced coordination between parties, power considerations, mix of identifiers). Roles and responsibilities unclear – no competent authority may be coordinating NIDs - Network resiliency needs to be considered by the parties if hosted on a public network - Some stakeholders cited a lack of access to necessary technical experts (more specialized than managing an IT network). While private network customers may share common needs, they will likely require tailored configurations and skilled integrators to implement the end-to-end solution.
4. **Roaming, connectivity, 112 and legal intercept**	- Few practical experiences of roaming, 112, and legal intercept - Public network integrated non-public networks are likely to more easily address these issues - Law enforcement authorities may not be aware of private network presence; monitoring and interception not obvious in that scenario - Desire for these features on a large scale yet unclear (clearer in some examples e.g. ports), dual SIM raises costs, but better to have one coverage than none so private network paying to extend mobile coverage
5. **Interconnection of private and public networks**	- Few practical experiences of interworking - Integrated non-public networks are likely to more easily address interworking - Interconnection will mainly be triggered by a need to go outside the private network area / plot - Unclear how prevalent inter-working will be (neutral hosting not widely reported)
6. **Classifications**	- Consultation confirms BEREC's views that all variants exist, Stakeholders acknowledge the most common variants as public network integrated non-public and standalone non-public (variants A and D)

Topic/challenge	BEREC's observations
7. Spectrum harmonization and frequency allocation issues	- BEREC does not hold spectrum competence, but spectrum issues are indirectly relevant for BEREC in relation to ongoing work by RSPG and CEPT (and the EC) on relevant aspects reflected by it herein[52] - Timely access to spectrum is important, so is enabling testing and prescribing technical conditions (especially in areas of high concentration) - Some stakeholders support a gradual approach to harmonisation - Some stakeholders support dedicated spectrum for private networks
8. **Transnational networks**	- There are use cases where transnational private networks might apply - Few practical examples from respondents to the consultation but BEREC is aware from other interactions with stakeholders (e.g. at workshops on satellite about capabilities for such networks)
9. Cloudification	- Potential impact may depend on users balancing the benefits and drawbacks from their own perspective - BEREC also reported on 5G private networks in BEREC Report on cloud and Edge Computing Services BoR (24)136 here

[52] Although BEREC is not the competent authority regarding spectrum access or licensing conditions, spectrum issues can potentially have indirect consequences for markets and end user rights, and are part of the discussions surrounding private networks. Therefore BEREC included some spectrum related questions in its consultation questions, and reflects on the answers, to raise awareness for NRAs.

6 BEREC's position and next steps

There are many configurations and architectures of private mobile networks from the isolated standalone private networks to public network integrated private networks in the form of a private slice of a public 5G network. The implementation of the latter is at an early stage in Europe because it requires rollout out of networks with an advanced 5G core, a practice that is at different stages in Europe.

The frequency range 3400-4200 MHz is the most common band for private 5G networks in Europe. The drivers of 5G private networks are varied and include deploying specifically the technical features of 3GPP based private networks in private settings such as a low latency or a very high availability. There may also be considerations with regard to optimizing security or privacy of business information, as well as reasons related to cost efficiency, the need to implement very specific solutions and avoiding vendor lock-in. The reasons mentioned by stakeholders vary per case and may be very diverse.

In BEREC's view, it is very likely that a significant part of private network deployments is not known to NRAs because of the different classifications and registrations used by different NRAs, and private 5G networks is a nascent domain but with growing demand. For coordination and interaction between private 5G network users, the points of contact of private network solutions may need to be shared via NRAs so that users can coordinate networks, particularly in high deployment scenarios (coordination on collision avoidance, and to ensure efficient use of resources UL/DL scheme matching).

In MNO deployments of private networks, MNOs may manage some of these issues internally, and thus the benefit of registrations of such private 5G networks may not be as obvious as it could be for those entities deploying standalone private 5G networks.

BEREC is of the view that the case for further harmonisation of the framework for private networks is inconclusive at this stage because deployments are not widespread and the identified challenges and observations set out in this report come from few practical examples. BEREC also considers that some flexibility at local levels may help NRAs adapt practices to suit local needs, observing that BEREC intends to support NRAs share practices so that there can be timely exchanges where different approaches regarding numbering and spectrum issues may be considered by authorities. However it is useful for NRAs and other stakeholders to be aware of the different classifications and registration procedures currently used within Europe. BEREC observes that the intent of the European Commission (through the Radio Spectrum Committee) to harmonise dedicated radio frequency ranges in midband radio spectrum for private networks will likely address some of the challenges for 5G private network stakeholders.

BEREC encourages interested stakeholders to provide inputs to the BEREC Work Programme 2026 consultation due to be launched for stakeholder input in spring 2025 if they believe BEREC should continue working on this subject.

Annex A: Summary of NRA questionnaire results

Introduction

As part of preparing this report, BEREC issued a short questionnaire from 25 March until 29 April 2024 to its Members and Participants without Voting Rights so that it could consider the current status of private networks in Europe and potential regulatory challenges. Thirty-one responses were received, and a summary of the results of this questionnaire are presented hereunder with relevant detail set out in the main report.

Is your NRA responsible (or partially responsible) for spectrum management in your country?

YES *	28																									
	AT	BE	BG	CH	CZ	DE	DK	EE	EL	FI	FR	HR	HU	IE	IT	LT	LU	LV	ME	MK	MT	NO	PL	PT	RS	SE	SI	UA
NO	3																											
	CY	ES	NL																									

* Include partial responsibility in FR, IT, LU and LV.

For the vast majority, the NRA is (partially) responsible for spectrum management in the respective countries. When there is a partial responsibility, it is often shared with a dedicated national institution, agency or ministry. In case the NRA is not responsible for spectrum management, there exists a separate dedicated department elsewhere in the governmental structure.

Is there a (regulatory, administrative, legislative, …) framework for private mobile networks in your country?

YES *	23																				
	AT	BE	CH	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LU	LV	ME	MT	NL	NO	SE	SI
NO	8																						
	BG	CY	LT	MK	PL	PT	RS	UA															

* Includes indicated future plans by IE, LU, ME and MT.

For the vast majority, there is a dedicated framework for (some) private mobile networks in the respective countries. For countries where this is not the case, they are planning to implement a dedicated framework in the near future with or without a clear schedule at this stage or there is no plan at this moment mainly due to a lack of interest for private networks from the industry.

Do MNOs have an obligation to report to the competent authority (e.g. NRA or relevant OCA) contracts they have signed for the provision of private mobile networks?

YES	5																									
	DK*	EL	FR	ME	NO																					
NO	26																									
	AT	BE	BG	CY	CH	CZ	DE	EE	ES	FI	HR	HU	IE	IT	LT	LU	LV	MK	MT	NL	PL	PT	RS	SE	SI	UA

* For DK there is only a reporting obligation with regard to contracts signed by the MNO the TT-Network (Norlys (formerly Telia) and Telenor's RAN joint venture) under its leasing obligation in relation to 3740-3800 MHz with parties interested in establishing local, private wireless networks using this particular spectrum.

For the vast majority, MNOs do not have an obligation to report contracts for private mobile networks to the competent authority as MNOs decide how to use their licensed spectrum. For countries with a reporting obligation, the main reasons are for statistical purposes and to understand the emerging demand for such private services.

Does the competent authority for spectrum management allocate dedicated spectrum bands (or parts of bands) which can be used by private mobile networks?

YES	18	AT BE CH CZ DE DK EE ES FI FR HR LV MK NL NO SE SI UA
NO	13	BG CY EL HU IE IT LT LU ME MT PL PT RS

An overview is listed for dedicated (parts of) spectrum bands used for standalone and public network integrated private networks (please also see section 2.2.4 above which elaborates on the potential differing NRA perspectives as regards architecture options and spectrum):

Used frequency bands for stand-alone private networks.		
400 MHz	0	-
700 MHz	0	-
800 MHz	0	-
900 MHz	0	-
1500 MHz	0	-
1800 MHz	2	NL SE
2100 MHz	0	-
2300 MHz	2	ES FI
2600 MHz	2	FR HR
3500 MHz	8	CH CZ DE DK MK NL NO SE
4000 MHz	3	BE FR PL
26GHz	8	CZ DE DK ES FI FR LV SE
28 GHz, 29 GHz	0	-

Used frequency bands for public integrated private networks.		
400 MHz	0	-
700 MHz	3	BE ES SI
800 MHz	4	BE EL ES SI
900 MHz	3	BE ES SI
1500 MHz	2	BE SI
1800 MHz	4	BE EL ES SI
2100 MHz	3	BE ES SI
2300 MHz	2	FI SI
2600 MHz	5	BE EL ES FR SI
3500 MHz	6	BE DK EL ES MK SI
4000 MHz	1	FR
26GHz	6	DK EE ES FI FR SI
28 GHz, 29 GHz	0	-

Are you aware of requests for private mobile networks, either to an NRA or OCA or an MNO, that were not successfully granted or where requirements could only be partly met?

The reported cases of unsuccessful granted requests for private mobile networks are very limited. Only one country reports an unsuccessful request due to incompatibility with the legislative framework in place.

What other challenges are you aware of?

The answers also reported several challenges with regard to private mobile networks such as:

- The demand for nationwide frequency availability for nomadic networks for applications in the fire department, police and news transmission sectors cannot yet be met;
- Lack of low/mid band spectrum for private local networks;
- Understanding of the regulatory framework by non-operator actors and their ability of seizing the importance of efficient spectrum use;
- In relation to the potential use of 3.8-4.2 GHz band for private mobile networks, there are known compatibility and coexistence issues with incumbent and adjacent users;
- Synchronization between private mobile networks and public mobile networks: the layout of the numbering plan no longer fits the needs of the market;
- Lack of equipment supporting the entire 3.8-4.2 GHz band;
- Geographical limitations and the inherent consequence, namely interference and coordination between authorized users;
- Seamless access when moving from a private network to any public network;
- Lack of interest by the industry for specific band or for private networks in general.

Have private mobile networks requested any numbering resources?

An overview is listed of numbering resources used for standalone and public integrated private networks:

In case of stand-alone networks, have private mobile networks requested any numbering resources?												
ITU-T E.164 numbers	2											
	AT	CZ										
ITU-T E.212 MNCs	12											
	BE	CZ	DE	DK	ES	FI	FR	HU	IT	NL	NO	SE
ITU-T E.118 IINs	2											
	DE	SE										
GSMA EIDs	0											
	-											

In case public network integrated private networks, have private mobile networks requested any numbering resources? *Member states are included when answered YES and/or received requests or inquiries about numbering resource.									
ITU-T E.164 numbers	3								
	AT	BE	CZ						
ITU-T E.212 MNCs	9								
	BE	CZ	DE	DK	ES	HU	PT	SE	SI
ITU-T E.118 IINs	1								
	BE								
GSMA EIDs	2								
	BE	DE							

Other kinds of 3GPP numbering resources:

- Closed Subscriber Group-IDs (CSG-IDs), Tracking Area Identities (TAIs), E-UTRAN Cell Global Identification (ECGI), Globally Unique Mobility Management Entity Identifier (GUMMEI) and Network Identifiers (NIDs).

- One NRA let a consultant firm do a study and one of the recommendations was to use 5GC-NID for private networks – the NRA is further investigating this option now.

Assignment process for MCC-MNC, among the respondents:

- No attribution: 6 NRAs
- No direct attribution, i.e. MNC dedicated to private network under country MCC and/or 999-MNC are allowed to be used on a free-for-all (uncoordinated) basis
    - 2XX-MNC: 3 NRAs
    - 999-MNC: 5 NRAs
- Direct attribution to spectrum license holders
    - 2XX-MNC: 6 NRAs

What issues do you consider to be relevant in connection with requests for any of the above numbers?

The most important reported issues are listed below.

For interoperability with public networks (MNC) under the country MCC:

- Roaming/interconnection with public networks is not allowed.
- It is not appropriate to use the MNCs allocated for shared use by closed/private networks in cases when roaming with public networks are needed.
- In case interoperability is needed with public networks for roaming, the solution of shared MNCs cannot function. For such a situation the numbering regulation foresees the possibility to apply for a unique 2-digit MNC.
- No interoperability problems reported but as understood, it is not appropriate to use the MNCs allocated for shared use by closed/private networks in cases when roaming with public networks are needed.
- Interoperability between private and public networks is not available. However, some industries, for example car manufacturers, expressed the wish that their cars (already equipped with public SIM profiles) may roam in their private networks for in-factory software provisioning.
- Possible interoperability scenarios with 3-digit codes are under study but, at the moment they are not allowed.

For interoperability with MNCs under MCC 999:

- Possible interoperability scenarios with 3-digit codes are under study but, at the moment they are not allowed

For issues with the OS:

- Initially there were indications especially concerning iOS devices.
- These MNCs were initially not open in Apples iOS but are open now.
- From an interview with an operator interested in allocation of second MNC (beside existing one) the problem with the global MCC 999 is if there are multiple private networks in close proximity, the devices may attempt to connect to another network with the same PLMN ID. Secondly, the operator considered more potential in private

networks from which the users will be able to use public network when needed and such transition requires public identification.

- The need of numbering resources must be justified to ensure the correct management and that the usage conditions attached to the use of the numbering resources are fulfilled. One of the key aspects when analyzing the request for public numbering resources is to ensure that the private network has interconnection with the public network (i.e., it allows communications to and from numbers from the national or international numbering plans and allows roaming).

Please describe measures to address interference aspects between private mobile networks close to each other if they are assigned / use the global MCC 999, or some other national allocated E.212 MNC allocated for shared use?

The most common measure is one of coordination to avoid or minimize mutual interference where the license conditions state that operators have an obligation to prevent incompatibility and to find out a mutual agreement in the event of interference with another experimental network. Second, some countries have plans to attempt to collect information from operators of private mobile networks regarding the associated MNCs used behind shared MCC 999 as well as the area covered and to provide information on request to other operators of such networks.

In any of the examples you have identified, does the private mobile network include neutral host connectivity services?

There is one case reported where a public company is building a private 5G network and a public 5G network as a host for public MNOs in the private 2300 MHz band and public 700 MHz and 3500 MHz bands. The contract provides for this infrastructure to be made available to telecommunications operators to provide their services to areas where deployment would not be economically viable at present.

Another case of private mobile networks that includes neutral host connectivity services offers indoor coverage solutions from both public and private mobile networks. They establish a neutral solution that provides the opportunity for all public mobile operators to connect and also allows the connection of private 5G networks.

Annex B: Questions at consultation stage

Questions – Numbering as set out at chapter 3 of BoR (24) 150

1. Did you request any numbering resources for private mobile networks, and if so, please specify:
   - Standalone networks

     i. ITU-T E.164 numbers?
     ii. ITU-T E.212 MNCs?
     iii. ITU-T E.118 IINs?
     iv. GSMA EIDs?

   a) Are you using for private networks the global MCC 999 allocated by ITU TSB for shared use by private mobile networks?

   b) Are you using for private mobile networks specific MNCs allocated under the geographic MCC used in your country for shared use by private mobile networks? Have you noticed any problems that these allocated MNCs are not open in mobile phone operating systems (iOS and/or Android)? Have you noticed any problem in terms of interoperability with public networks (for cases in which private networks could need to interconnect/roam with public networks)?

   d) Are you using private mobile networks with any other kind of 3GPP numbering resources (e.g. NID etc.)?

2. Please describe measures to address interference aspects between private mobile networks close to each other if you are using the global MCC 999, or some other national E.212 MNC for shared use.

Additional questions – Set out at chapter 4 of BoR (24) 150

1. What are the main reasons that drive the implementation and deployment of private mobile networks in your view (e.g. guaranteed QoS parameters, security, lack of awareness of MNO offerings, MNO offerings not fitting requirements, fears of vendor lock-in, other)?

If you are the owner/prospective owner of a private mobile network or if you have deployed (or tried to deploy) a private network, please also answer the following questions 2 to 4.

2. What type of private mobile network solution did you select and why (e.g. standalone, public network integrated, implemented by an integrator)?
   a. If you have deployed a 3GPP-based broadband private mobile network, what are the main reasons to select this technology vis a vis other wireless technologies (such as Wi-Fi)?
   b. If you have already deployed a private network based on wireless or proprietary technologies, would you foresee a migration in the future towards

a 3GPP-based broadband private mobile network? What would be the driver for this migration?

3. What are the main administrative/regulatory obstacles you encountered to deploy the solution?

4. What are the main technical obstacles you encountered (network planning and deployment, integration with IT or operational technology used by the company, lack of specialized skills/expertise…)?

5. Are there roaming, connectivity issues to 112 emergency communications services, or legal intercept issues that you know of, please specify?

   The above question may be relevant if the private mobile network includes neutral host connectivity services, such as to extend connectivity to public mobile networks for guests (e.g. voice, SMS and/or other)

   OR

   if the private mobile network offers (connectivity to) public mobile network services to own users (i.e. not guests)

6. Please provide your views on the role of interconnection with one or more public networks (interconnection, purpose of interconnection)?

7. Please provide any views on the variants (A, B, C, D) described in figure 5. What variants exist or could exist in practice? What could be the merits in harmonizing an approach to classification?

8. Please provide views on spectrum harmonisation for private mobile networks in the EU?

9. Do you see a demand from actors for transnational private networks, using a combination of private networks in multiple Member States and are there issues to be addressed in that regard (for instance with regard to roaming or coordination along specific corridors)?

10. For frequency ranges that are assigned to users of private mobile networks, what are your thoughts on how NRAs may facilitate future demand (see also question 4), particularly in areas with a high concentration/density of potential needs/demand to deploy such networks (such as ports, industrial areas, etc.)?

11. How would you describe the (actual or potential) impact of networks' cloudification on the interest in the deployment of private mobile networks?