Private network solutions in light of 5G

(Technical and regulatory aspects)

16 December 2021

Introduction

In today's fast-paced world, it is important to find time and cost-effective solutions in different areas of life that are flexible enough to adapt to technological developments. Such solutions can be provided by private networks based on mobile technology, which can be set up separated from the public network, and directly at customer premises, allowing, among other things, transmission speed, required response times or secure data management to be tailored to the individual needs of the customer. In recent years, the deployment of mobile private networks (non-public wireless networks, typically in geographically limited areas) has started, mostly based on LTE for now. However, with the advent of 5G technology, 5G private networks are expected to grow significantly with new use cases and needs emerging in this area.

5G can open up new opportunities for verticals discussed in this paper, such as industry, transport, education/research (universities) and healthcare. The ability to connect a large number of devices, low latency and increased data transmission capacities are seen as of paramount importance for verticals. In addition, an important feature of the new technology is its high customisability, such as the possibility of creating private networks (or non-public networks). With 5G, new developments have also emerged that allow private networks to be implemented using virtualisation techniques in addition to real physical deployment, such as network slicing. The new opportunities also increase and shape the needs of verticals and diversify the range of services offered by mobile network operators (hereinafter: operators or MNOs).

5G brings a new approach to all stakeholders (including state and market actors). This new approach also raises a number of new questions in terms of spectrum management and infrastructure use, such as whether the vertical representatives themselves need individual right to radio spectrum usage, in this case specifically to operate private networks, or whether it is sufficient for them to use a service. If those applying for private network capabilities wish to become radio spectrum users in their own right, the question is how they will have access to radio spectrum resources suitable for 5G. In the following chapters, we seek answers to these and similar questions by examining the available data from the perspectives of regulation, infrastructure and technology. The aim of this technical analysis is to identify the most typical cases, in particular those that require some form of regulatory legal action.

This professional overview by the National Media and Infocommunications Authority (NMHH) is for information purposes only, and based on the relevant constitutional principles and practice, the NMHH's opinion, issued without a regulatory procedure framework, cannot be considered a law, nor any other source of law or a public law instrument to regulate organisations, and it does not have any normative character, legal force or binding content.

1 Regulatory framework

1.1 Possible ways of accessing radio spectrum

There are several possible theoretical solutions to grant a private network (market players [whether legal entities or natural persons, hereinafter "private network applicants" or simply "private networks" for ease of reading] wishing to use a private network for any communication purpose or requiring private network capabilities) access to 5G capabilities. We have a broad range of options. From a regulatory point of view in the field of radio spectrum management, we have identified four substantially different use cases:

1. 5G capability (access to radio spectrum, network, possibly end user devices) is used as a **service** from a mobile network operator (MNO) with right of use for radio spectrum;
2. the possibility to utilize radio spectrum is acquired from an MNO under a **lease agreement** (secondary trading);

3. the right of use for radio spectrum are acquired from an MNO as a result of **a trade** (secondary trading);
4. the right (or entitlement) of use for radio spectrum is acquired from the authority exercising the property rights by means of a primary acquisition (e.g. as a result of competitive procedure or a light licensing procedure).

1 – *Options for private network applicants to gain access to radio spectrum*

	Rights of use for radio spectrum	**Radio spectrum user**	**Legal grounds**	**Comment on radio spectrum usage**
1. Service	MNO (as service provider)	MNO (as service provider)	Terms of service	
2. Lease (secondary trading)	MNO (as original right holder)	Private network (as the lessee)	Lease agreement	NMHH approval Simplified approval option
3. Acquisition of entitlement to radio spectrum usage by trade (secondary trading)	Private network (as "Buyer") (the original holder, the MNO is the "seller")	Private network (as "Buyer")	Trade agreement	NMHH approval Identical to item 4 except for method of acquisition
4. Right or entitlement to radio spectrum usage – as primary acquisition	Private network (as original right holder)	Private network (as original right holder)	Based on entitlement, right, law	NMHH individual licence There is currently no "dedicated[1]" radio spectrum for 5G private networks

Under the current legislation, a private network applicant can only access 5G capabilities through secondary trading or by using a service (cases 1, 2, 3 in Table 1).

Case 1 in Table 1 is the simplest, providing the resources needed for communication as an MNO service for private network applicants. In this case, the operator controls the radio resource.

In case 2 in Table 1, the private network applicant, as the lessee, acquires the right to collect the benefits of the radio spectrum under a lease agreement[2], thus gaining access to

[1] Dedicated radio spectrum can be defined as radio spectrum allocated and made available for a specific purpose, where radio spectrum usage for the specific purpose is possible either by law or based on an individual licence issued by the authority.
[2] Pursuant to Decree 7/2013 (IX.19) NMHH on the secondary trading of radio frequencies

the radio spectrum. In case 3, the rights (with the entitlement of use for radio spectrum also changes hands (in whole or in part).

Cases 3 and 4 in Table 1 are similar in the sense that the private network applicant in question acquires its own rights or entitlement to radio spectrum usage. From the moment of acquisition, it is also responsible for radio spectrum usage. One essential element here is that the applicant is responsible for the interference-free use of the radio spectrum.

Case 4 in Table 1 refers to radio spectrum which can be used without an individual licence under the law (license exempt) or which is licensed by the NMHH or subject to a competitive procedure. (In this case, the private network applicant does not need to use a service or acquire radio spectrum usage rights in secondary trading, but is responsible for the operation of its network and for ensuring that it is free from any interference.)

1.2 Approval for radio spectrum secondary trading agreement by the Regulatory Authority

Under current legislation, secondary trading is permitted in spectrum management, in addition to primary spectrum acquisition. The procedural rules are laid down in Decree 7/2013 (IX.19) NMHH on the secondary trading of radio frequencies, which requires the approval of the NMHH for the entry into force of lease or trade agreements.

In the specific cases listed in the amendment to Decree 7/2013 (IX.19) NMHH, to comply with the European Electronic Communications Code[3] (Decree 15/2020 (XII.15) NMHH), a simplified approval procedure will be possible. Like the light licensing procedure, this procedure will also be done electronically. The simplified procedure will be available from July 2022 if the lease agreement:

a) covers a territory of less than 500 km^2;
b) is for the provision of a non-publicly available electronic communications service; and
c) is for no more than 5 years.

1.3 Resource sharing categories

Even before the introduction of 5G, network operators were already making use of shared resources, primarily to increase efficiency, to comply with landscape protection considerations and, increasingly, to reduce costs. As a result, networks of mostly similar structures have been connected and interconnected at different levels (whether in the form of leases or other forms of cooperation). More and more frequently in recent times, we have seen not only the use of shared infrastructure or the sharing of equipment, but also the emergence of a more collaborative sharing of infrastructure from a radio perspective.

Figure 1[4] can help to understand how resources are shared:

[3] Complies with Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code,

[4] https://www.gsma.com/futurenetworks/wiki/infrastructure-sharing-an-overview/

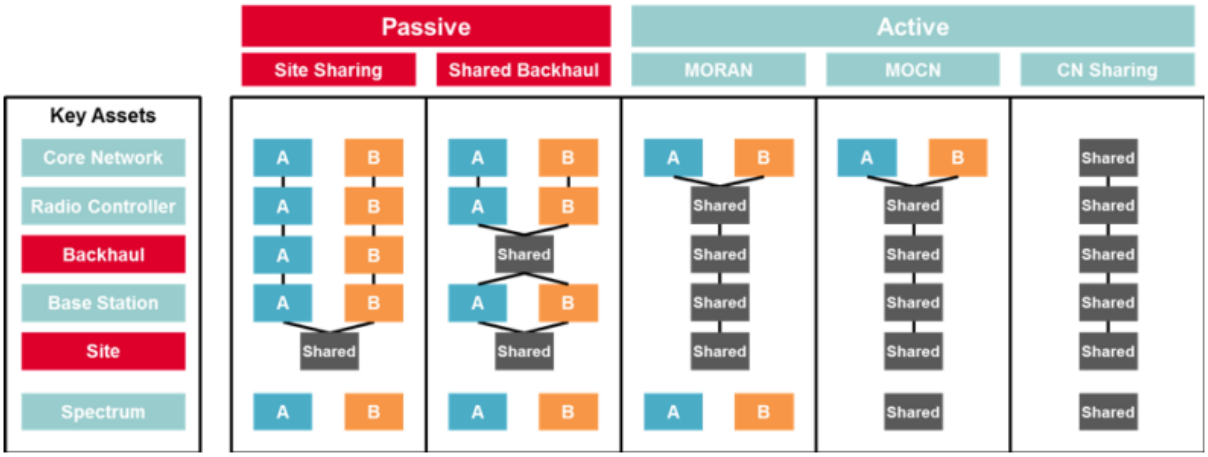


Figure 1 - Infrastructure sharing categories

The figure shows which elements of the network are affected in each resource sharing category, as follows:

- passive infrastructure sharing: as the name suggests, no active network elements are involved in the sharing (e.g. site sharing);
- MORAN (Multi Operator Radio Access Network): a category referring to the sharing of elements of a radio access network, where radio spectrum usage is not shared;
- MOCN (Multi Operator Core Network) +spectrum pooling (shared radio spectrum usage): in this case, there may be shared elements in the network up to the core network, including shared radio spectrum usage;
- CN Sharing (Core Network Sharing): the core network is also included in the shared network elements, this is the highest level of network sharing among the options listed.

The MVNO (Mobile Virtual Network Operator) and local/national roaming cases are not shown in the figure, but like CN Sharing, the elements listed in the figure can be considered shared, in which case the operator provides the service over the network it has been granted access to, with radio resource management being the responsibility of the network operator in all cases.

2 Providing the resources needed for 5G capability of private networks

The new opportunities and demands that 5G will bring mean that both operators and regulators will have to respond to the changed circumstances. This requires knowledge of real-world use cases, actors, as well as the feasible or planned business solutions that 5G can support. The aim is not to explore all the theoretical possibilities, but to research and, where necessary, support the most commonly used, typical solutions. In addition to the new possibilities, pre-5G solutions that were already in place before 5G should continue to be taken into account.

2.1 Resources

Basically, the radio spectrum needed for communication and infrastructure elements can be highlighted as essential resources for electronic communications. Operating private networks requires the right quantity (and quality) of these resources. The various options are summarised in Figure 2.

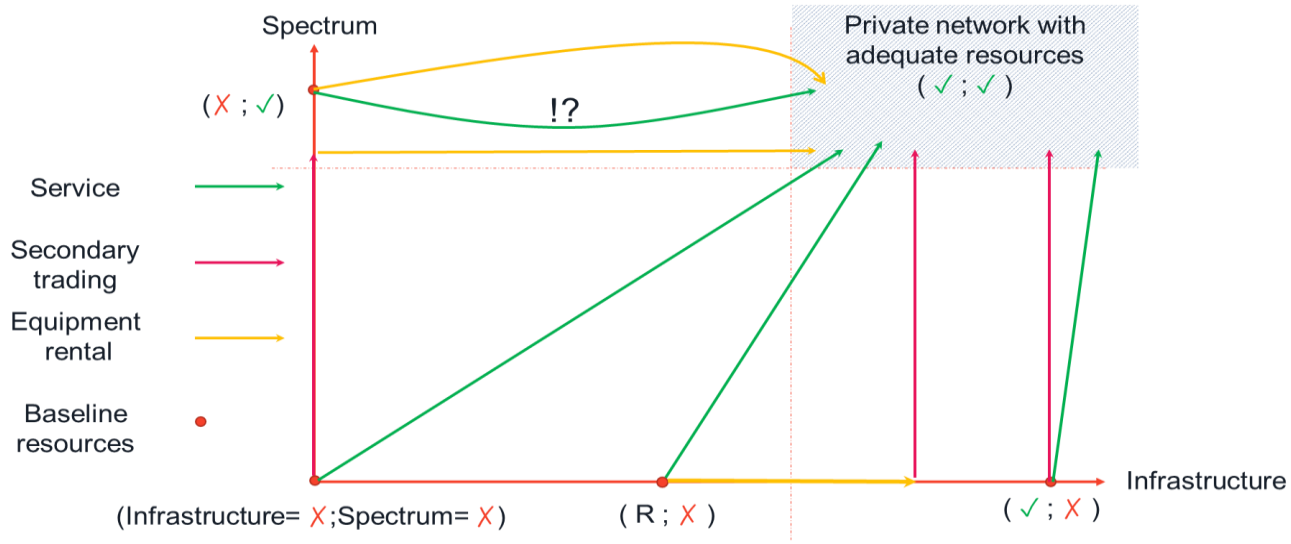


Figure 2 – Options for providing resources

In the case of infrastructure, this could include leasing the necessary equipment; deploying and operating it as a service; providing access to existing infrastructure (either through infrastructure sharing or virtualisation techniques for some of the functions and the capacity). The necessary radio spectrum can be provided through the options in Table 1.

2.2 Essential elements of the value chain

Partly to understand the possible roles, but equally to ensure consistent use of the terms, it is worth gathering together the actors relevant for private networks.

Private network

A private network is a mobile network that uses a broadband network, possibly including 5G capabilities, for some specific purpose (industrial, agricultural, scientific, logistical, health, transport, etc.) for wireless communication separated (partially, wholly or only virtually) from public networks.

The private networks in the focus of this document (especially with the 5G option available later) are characterised by a specific purpose and the corresponding deployment, as well as mostly by local and limited operational area(s).

Private networks can be set up in various ways depending on how separate they are from public networks. Thus we can distinguish between

- Independent private networks
- Hybrid private networks
- Virtual private networks

Independent private networks are completely independent from the public network, typically without any connection between them, and they operate in a completely autonomous way.

Hybrid private networks are created by combining private infrastructure with public infrastructure, typically using only parts of the public infrastructure.

Virtual private networks are created entirely using the resources of the public network, with private elements only to the extent required by the specific characteristics of the vertical.

Vertical

A group of actors focused on serving a defined set of end users or on achieving a specific, non-radiocommunication objective, but who need an electronic communications network to meet their internal communications needs. Private networks serving the same specific (or similar) purpose belong to the same vertical.

Verticals can be, for instance, healthcare, energy, transport, industry, education, logistics and public safety.

MNO

Mobile network operator[5], typically with its own infrastructure and right of use for radio spectrum.

As a market player, it typically provides electronic communications services for a fee to users, including those who require private network capabilities. Its services may include providing access to resources that are missing for 5G capabilities.

It can also provide access to 5G-ready spectrum to private network applicants through secondary trading.

Infrastructure provider

A market player that provides the infrastructure necessary for electronic communications networks – even for the provision of electronic communications services or private networks – to MNOs in the traditional sense, or even to private network operators.

A private network applicant can access the network directly, via an MNO or an infrastructure provider for certain infrastructure elements. MNOs can also be infrastructure providers.

Subcontractor

Potentially operating separately, these are civil law contractors involved in the deployment (from construction works to system integration) and operation of the private network. General contractors may use subcontractors if they do not have sufficient and appropriate resources.

Technology supplier

Actors providing the infrastructure elements and technology necessary for the operation of electronic communications networks.

[5] Section 188 (86) of the Electronic Communications Act.

Regulatory authority

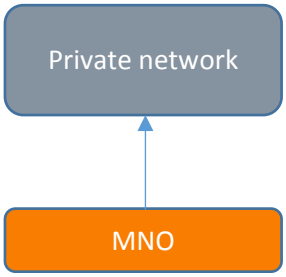
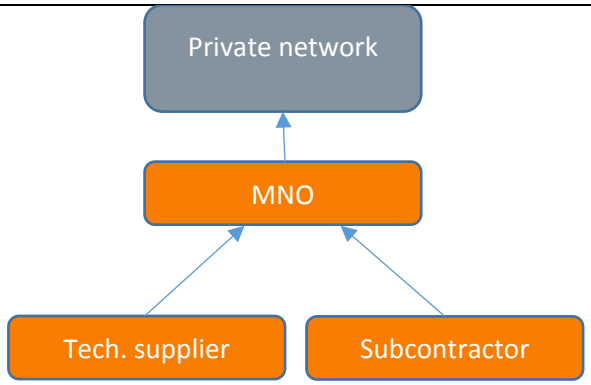
The NMHH is the regulatory authority of the electronic communications sector.

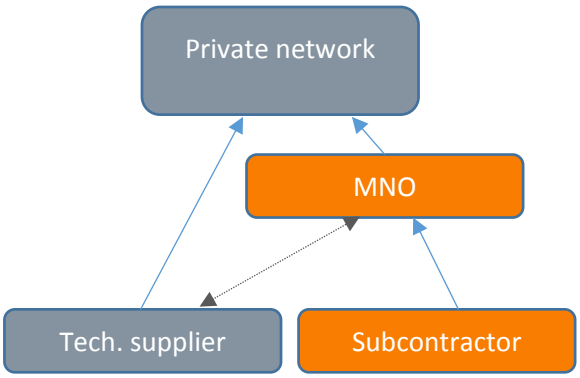
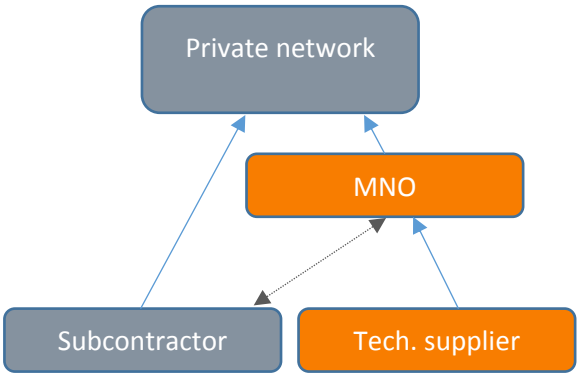
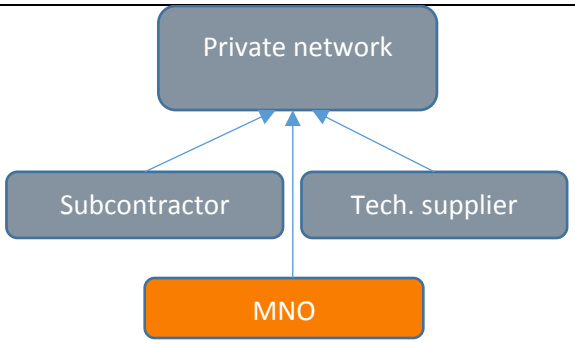
The NMHH is working to develop the most customer-friendly and broadest possible regulation to enable access to 5G capabilities, taking into account the needs of all stakeholders (in particular: mobile operators, infrastructure providers, users, verticals).

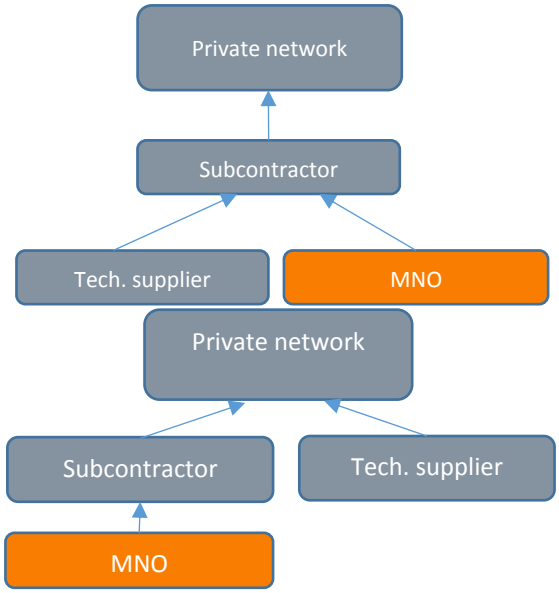
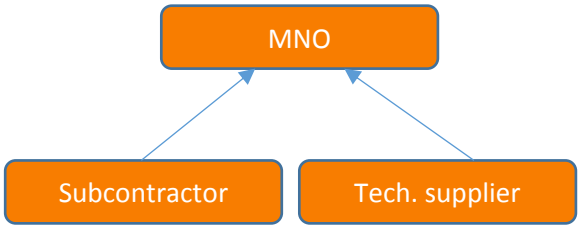
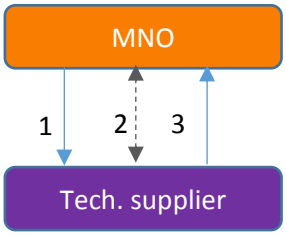
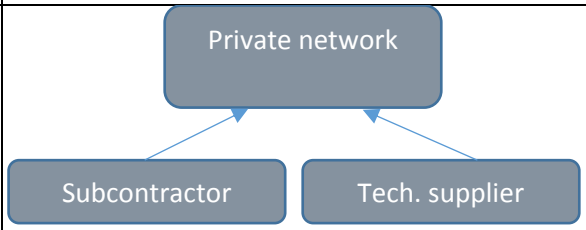
2.3 Relationships between identified actors

Table 1 shows the 4 basic options for accessing 5G capabilities (on-demand, access to spectrum through secondary trading (trade and lease) and as a primary spectrum holder) (with the two intermediate options already legally regulated, alongside the extremes of the range of options). Applying these possibilities to the relationships between actors relevant for private networks will bring us closer to real-world cases of 5G capabilities being used. In Table 2, these identified cases are assigned to the cases in Table 1, with a schematic representation of the relationship model and a simplified description.

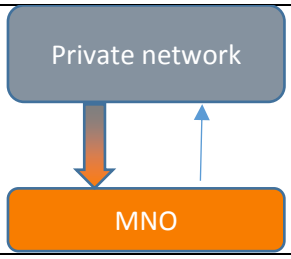
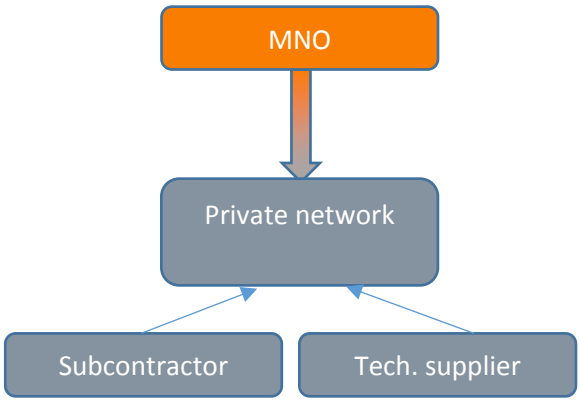
Table 2 – Models for access to 5G capabilities (spectrum, infrastructure, service)

Category	Model	Description
1. Service		Full 5G service from the MNO for the (even complete) provision of private network 5G capabilities (e.g. off-the-shelf, with customisation options) Characteristics: • the private network applicant has minimum private network resources at its disposal; and • uses the MNO's network and/or equipment up to the last element (even the terminals may be provided by the MNO as a provider); or • uses the MNO's network for communication between terminals and the internal network (intranet); and • uses the MNO's public network.
1. Service		MNO custom deploys and operates (through subcontractors and suppliers) the necessary system as a service. **Characteristics:** • uses MNO network and MNO radio spectrum (even separated); and • MNO radio spectrum management with possibility of deploying local core network functions.

1. Service		The private network is <u>partly</u> deployed and operated by the MNO (e.g. MNO does not need to know the technical details of the specific equipment). Characteristics: • management of radio spectrum usage is the responsibility of the MNO, with MNO radio spectrum usage (even separated for the private network); and • RAN partly under the supervision of the MNO and the private network applicant
1. Service		For the private network applicant, the MNO provides a service to access 5G capabilities using the MNO network and (even separated) MNO radio spectrum. Characteristics: • the radiocommunications system is installed and maintained (at least in part) by the subcontractor of the private network applicant (e.g. because the MNO cannot be present at the installation site); and • the management of radio spectrum usage is the responsibility of the MNO.
1. Service	 or	MNO provides access to the radio spectrum as a service for a deployed private network and also performs core network functions (at least radio resource control). If a private network applicant uses 5G capabilities as a service, the involvement of the MNO would be required to this minimum extent, as in the case of a service, the MNO with entitlement to radio spectrum usage is responsible for controlling radio resources related to radio spectrum.

1. Service		As in the previous case, the radio spectrum must be provided to a private network that has been deployed, but in these two (sub)cases it is subcontracted, with the MNO's spectrum being used by the private network through the subcontractor. Characteristics: • radio resource management is the responsibility of the subcontractor; and • a secondary trading agreement is required for the subcontractor's radio spectrum usage
4. Radio spectrum usage in own right[6] or 3. Trade or 2. Lease		This could include the deployment/testing of the MNO's own mobile network or 5G private network roll-outs. The subcontractor (optional) deploys the system using the technology procured. Characteristics: • own (MNO) radio spectrum management
2. Lease		The technology supplier uses the MNO's network and/or frequencies 1. applying for radio spectrum (e.g. for research, development) from the MNO 2. under complex cooperation agreements 3. or even as part of a contract for work, e.g. to develop technology. Leasing the right to radio spectrum usage could also be a solution. In addition, the possibility of using experimental licences could be explored.
4. Own radio spectrum		The private network applicant acquires radio spectrum as an original holder, completely independently of the MNO.
2. Lease and 1. Service		A private network applicant leases the radio spectrum it originally acquired as a holder to the service provider so that the

[6] hereinafter referred to as own radio spectrum

		service provider can use this spectrum to provide a service to the private network applicant to meet its communication needs.
3. Trade or 2. Lease		Through secondary trading in the form of a lease or trade, a private network applicant obtains radio spectrum usage for a spectrum that can also be used for 5G. It acquires the right to collect the benefits of the radio spectrum (under a lease agreement) or the rights (with entitlement) of use for radio spectrum (as a result of a trade) from the original radio spectrum holder.

3 Access to spectrum for private network applicants – from service to own radio spectrum usage

The ability to implement private networks depends to a large extent on the resources available to the private network for autonomous communication and the extent to which private network applicants need to rely on the services of an MNO to implement communications. This chapter presents examples of typical private network implementations from a radio spectrum usage perspective.

One of the new 5G technology solutions to guarantee network resources for a given purpose is the use of “network slicing”. The cases of private network implementation using the “network slicing technique” are described in Chapter 4.

3.1 Private network with own network and radio spectrum

A private network may have access to radio spectrum usage rights (either as an original holder or through secondary trading) and may have its own deployed[7] system, but there may still be other actors in the life of the private network. Most importantly, private network applicants may have access to the radio spectrum through a secondary trading agreement, but other market players, including MNOs, may also participate in the deployment of the private network, but the operation of the radio system is legally in the interest of the private network. An important link to other actors could be that in certain cases active and passive infrastructure sharing methods may also be employed.

[7] Ownership is not the determining factor, it can be leased.

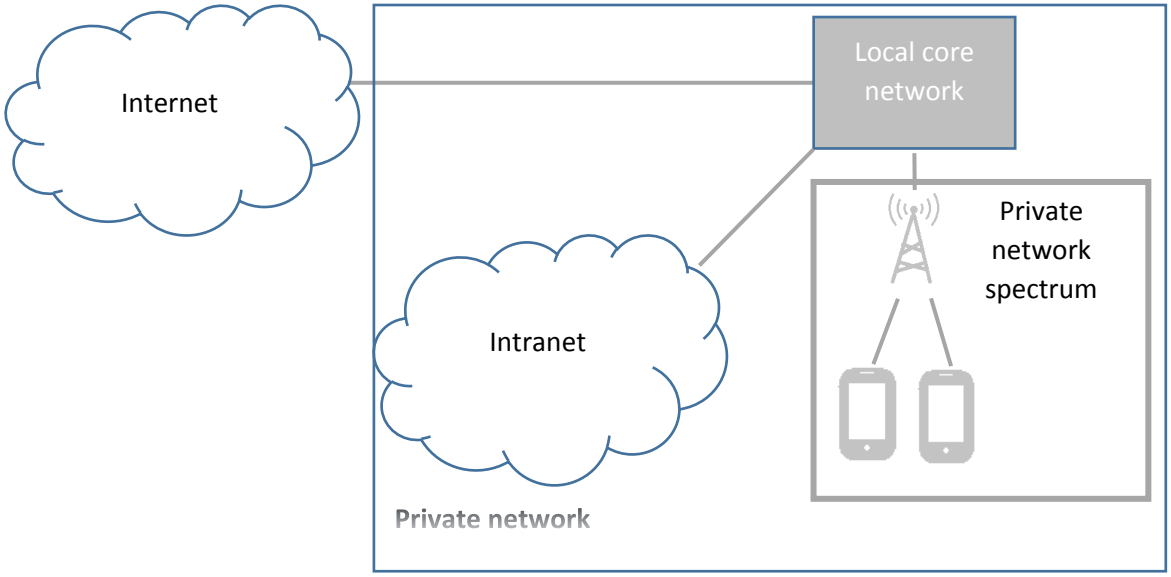


Figure 3 – Phisically isolated private network

Shared resource:	This can happen in some cases, i.e. secondary trading (at most a deployment service, but the right of use belongs to the private network user, who is the one holding the radio licence). For networks based on such a model, MOCN + "spectrum pooling" could also be considered with the operators.
Equipment rental:	It is possible that some infrastructure elements are leased to the private network.
Radio spectrum access:	Own radio spectrum usage right
Authority approval required:	If the radio spectrum was acquired through secondary trading, then yes
Simplified approval option:	Possible, depending on whether the relevant conditions are met
Possible examples, real implementation cases	e.g. for international car manufacturers, to develop production based on a uniform model

Table 3 – parameters of a independent private network

The first example presented in section 4.2 of Chapter 4 (an independent, physically isolated 5G private network with own or leased radio spectrum) is otherwise similar in structure to the case shown in this section.

3.2 Service model – MNO provides mobile services

The private network is given access to the MNO's network and uses it to communicate between its radio devices and its own internal network.

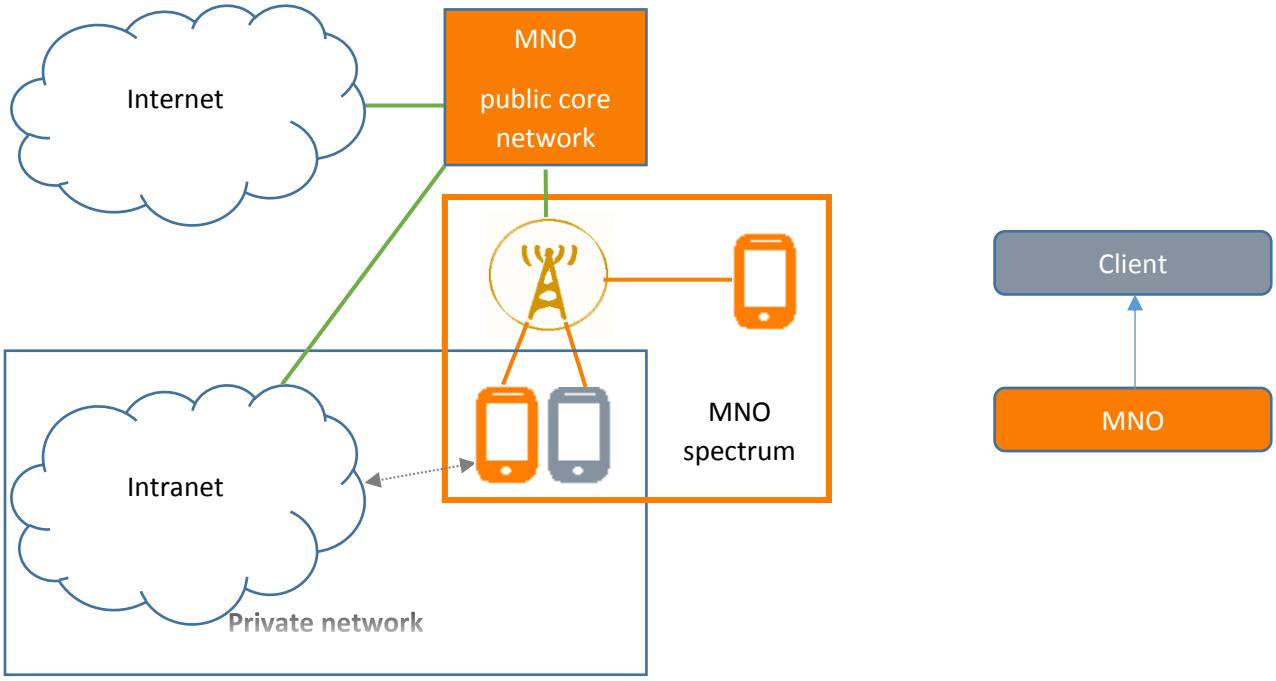


Figure 4 – Private network through a service

This can mean fully public radio spectrum usage (as any other average end user, i.e. subscriber, of the MNO) or using a radio spectrum that is technically separated to guarantee the service to the private network. In this case, the private network practically uses a service.

As long as there are no other deployed private network elements than the terminals, there is no clear private network use.

Shared resource:	Service (network and radio spectrum)
Equipment rental:	No (use of an electronic communications service), the use of end user equipment is also possible in a service configuration.
Radio spectrum access:	No
Authority approval required:	No
Simplified approval option:	-
Possible examples, real implementation cases	On the production line, an MNO SIM card is inserted into the standard SIM slot of the robotic arm and communication is via the public MNO network.

Table 4 – Private network as a service -– parameters

3.3 MNO provides local core network functions and separated radio spectrum

In the case of equipment leasing or the provision of core network functions and radio spectrum, it is also possible to separate spectrum for the private network if network elements providing autonomous core network functions are provided to private networks by the MNO on an equipment lease basis (Figure 5).

Depending on the service model, radio spectrum can be provided separately to the private network while the MNO retains the management of radio spectrum. The difference will lie in the amount of frequencies that can be used in a given area, as the separated radio spectrum will only be available to the private network in the operational area of the private network.

In this case, the operator also provides equipment implementing core network functions for private network purposes. In addition, the radio access network and its control is within the

MNO's competence. In the figure below, the management of the (separated) radio spectrum of the private network is independent of the MNO's public network.

In this case, it is important to highlight one of the edge cases of making radio spectrum available as a service. Where there is a private network deployed but no usable spectrum is available, radio spectrum can be made available as a service from the MNO to operate the private network.

For it to be treated as a service, the radio resource management tasks (in MHz, W terms) must still be performed by the MNO, while the private network operator performs the higher level management of the system resources (in Mbit/s, priorities, possibly in QoS terms, etc.).

This is also likely to raise the need to deploy infrastructure elements (radio resource control, control plane, core network functions) in the otherwise deployed private network. However, it is not clear which elements need to be deployed or integrated into the private network to implement this task (where the boundary is between the competence of the MNO and that of the private network).

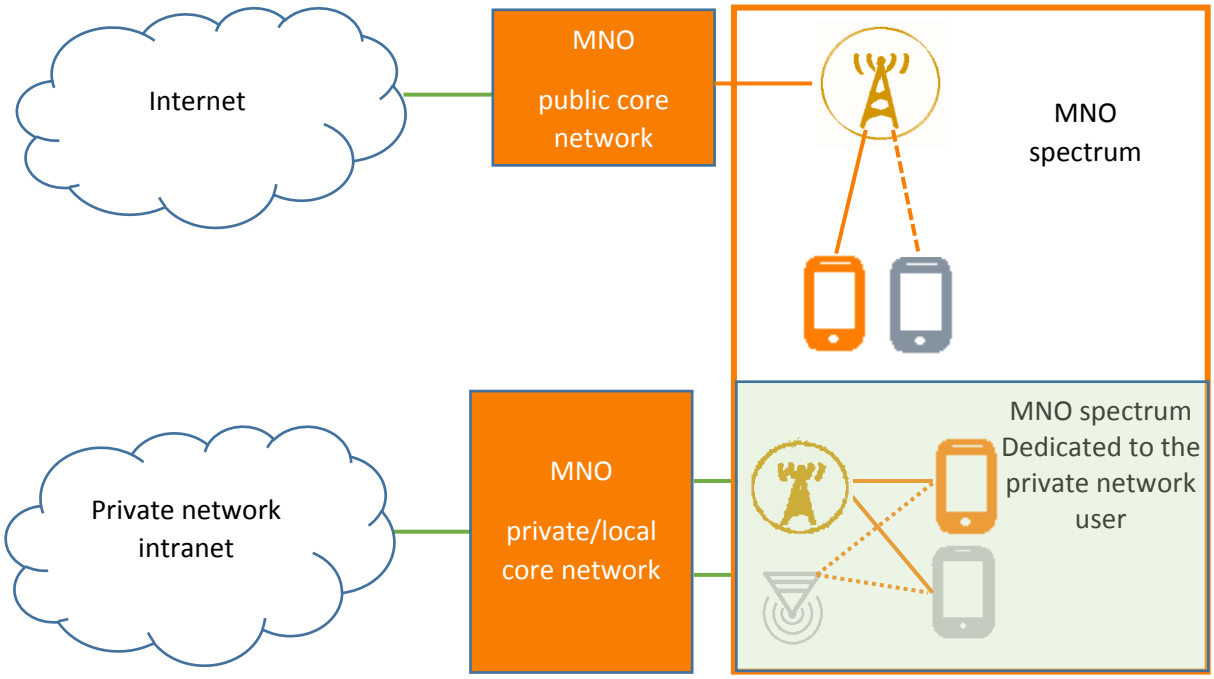


Figure 5 – Private network under lease and service/asset rental

This also raises the question as to whether it is a realistic use case that, in addition to leased core network functions, private networks can have both private and MNO radio access network elements, and whether private network terminals can also connect to the MNO public network (presumably a completely separate network, so this is why it is not clear). If this is a real case, it is worth further exploring the room for manoeuvre provided by the regulatory framework, as based on general electronic communications rules this case raises additional questions beyond spectrum management rules, such as whether it is possible to provide access to a separated spectrum under a service model. However, this question is only worth pursuing if the answer to the first question is "yes".

Shared resource:	Equipment rental + service (service includes rental of network equipment and radio spectrum usage)
Equipment rental:	Partly (core network elements, and possibly end user devices, local base stations)

Radio spectrum access:	No
Authority approval required:	No
Simplified approval option:	-
Possible examples, real implementation cases	Implementing complete private on-premises network communication wholly independent of public mobile networks with the advantages and disadvantages of a dedicated spectrum (fixed amount of spectrum).

Table 5 – Private network under lease and service/asset rental – parameters

3.4 MNO provides local core network functions and (not separated) radio spectrum access

In contrast to the previous case, if there is no separated spectrum, spectrum management tasks must be performed in coordination with the locally available public MNO mobile network (as there is no fixed and clear boundary between the spectrum separated for private use and the one publicly available). This also means that there can be no autonomy for the private network. If the system is not fully autonomous, it is also possible to connect core networks for voice/data transmission. The thick green link in the figure indicates the difference compared to the previous case.

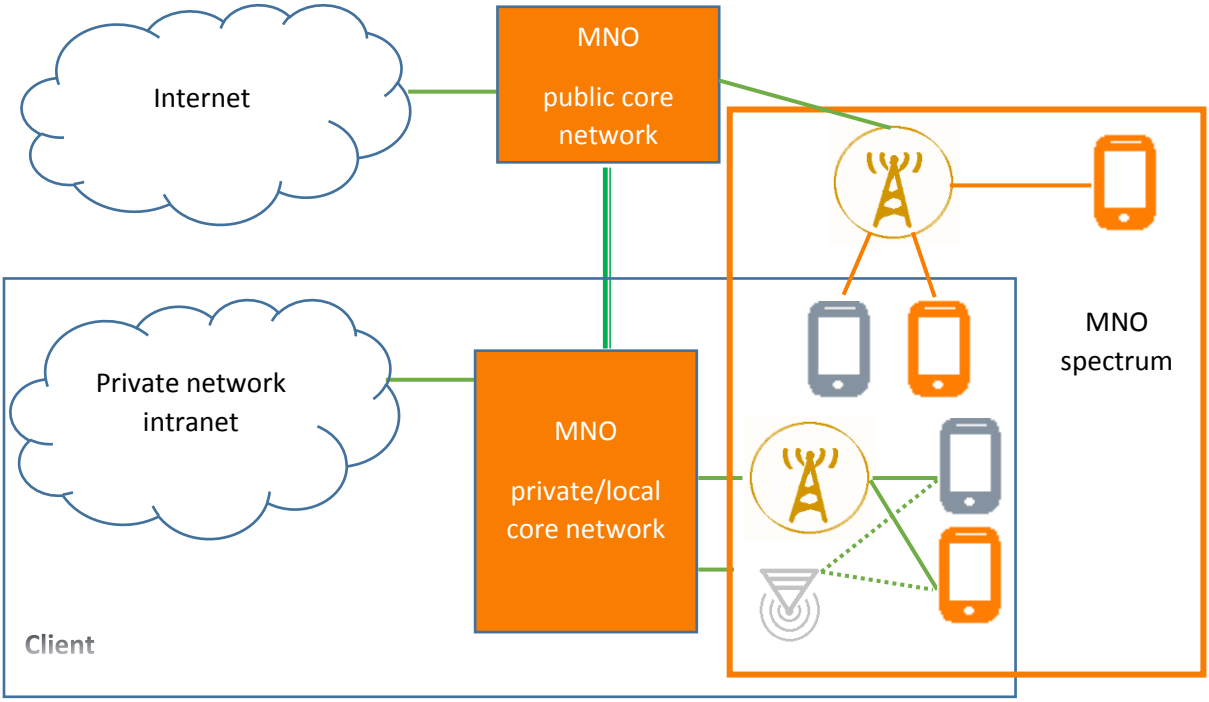


Table 6 – Private network under lease and service/asset rental

Shared resource:	Equipment rental + service (service includes rental of network equipment and radio spectrum access)
Equipment rental:	Partly (core network elements, and possibly end user devices, local base stations)
Radio spectrum access:	No
Authority approval required:	No
Simplified approval option:	-
Possible examples, real implementation cases	Implementing communications for a complete on-premises private network The amount of radio spectrum available at any given time may vary (both +/- directions) due to radio spectrum usage on public mobile networks Depending on the tightness of the connection to the public network, even low-latency data connections to other sites in the private network are available, which is useful in the event of remote surgery, for example.

Table 7 – Private network under lease and service/asset rental – parameters

3.5 Active infrastructure sharing - (e.g. MOCN without spectrum pooling)

When a private network has the means to implement core network functions but no radio spectrum is available (and even no RAN), it can use the MNO's radio access network and the radio spectrum it shares with it.

This is not the radio spectrum separated for the private network and managed by the MNO, but the radio spectrum made available to and shared with the private network and managed by the private network user under its own authority.

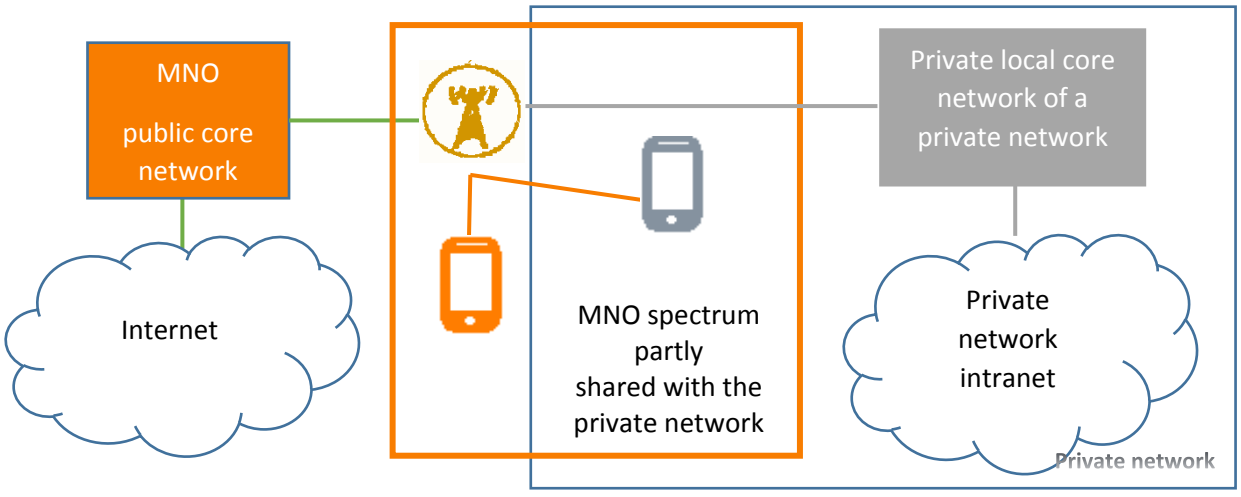


Figure 6 – Private network with active infrastructure sharing

Shared resource:	Network + radio spectrum
Equipment rental:	Full RAN is an option
Radio spectrum access:	Leasing The private network uses the MNO's radio spectrum
Authority approval required:	Yes
Simplified approval option:	If the conditions are met
Possible examples, real implementation cases	-

Table 9 – Private network with active infrastructure sharing – parameters

4 Technical solutions after the 5G roll-out

4.1 5G private networks with network slicing

At present, networks with 5G capabilities are still operating in the so-called 5G non-standalone (5G NSA) configuration, which means that LTE networks are complemented by 5G NR (New Radio) systems, thus accelerating the roll-out of 5G services. The full range of 5G capabilities will be complete with the advent of 5G standalone (5G SA) systems, with some networks already switched to this mode, and private network deployment will then have another opportunity to use network slicing.

The standardisation of network slicing is not yet complete and is expected to be fully implemented with the finalisation of Release 17, but Release 16 already includes the standardised basis for this efficient resource management principle. So this may well be one way of building private networks in the future, especially in countries where some level of operator involvement is essential in the creation of private networks.

As mentioned earlier, there are three typical types of private network: independent private networks, hybrid private networks and virtual private networks. Network slicing is a technique used in some hybrid solutions and in all virtual solutions, which allows for an optimal allocation of resources and provides for the necessary quality conditions. It is therefore advisable to consider how this technique can be used by the public operator to offer private network solutions. To understand how 5G private networks can be created using network slicing, we need to understand the system elements within the 5G network and the standard interfaces between them. This is because they play a fundamental role in the various levels of system deployment.

The designations and notations used in connection with network slicing are discussed in the following sections. The figures presented here are intended as references to illustrate network slicing, but for completeness they also show independent private networks using the uniform terminology, where the 5G private network, completely separated from the public network, is shown using radio spectrum acquired as the original holder or through a lease/trade.

4.1.1 Terms and definitions used

The left side of the figures shows the private network, deployed either by the enterprise itself or by the operator or a commissioned general contractor. This is irrelevant from a systems engineering point of view.

The abbreviations shown in the figure stand for:

5GC-CP	5G Core - Control Plane, i.e. the control plane of the 5G core network. This element is present in both public and private networks, as it is a basic element of the 5G network.
UPF	User Plane Function, i.e. the data plane function of the 5G network. This element is also present in both the public and the private networks and should be present in the public network in the core part and in the cloud of the edge network.
UDM	Unified Data Management, i.e. the 5G network's subscriber database on the public network and its user database on the private network.
MEC	Multi-access Edge Computing, formerly known as Mobile Edge Computing, is a smart system at the edge of the 5G network, which is designed to bring intelligent functions closer to the terminal equipment for faster response times, without the need for a central 5G network system.
gNB/5G-gNB	Next Generation Node B, gNB for short, is the name of the base station for 5G networks, sometimes used with the prefix "5G", but most of the time not, because the base station for 4G networks is abbreviated as eNB, for 3G networks as NodeB, and for 2G networks as BTS.

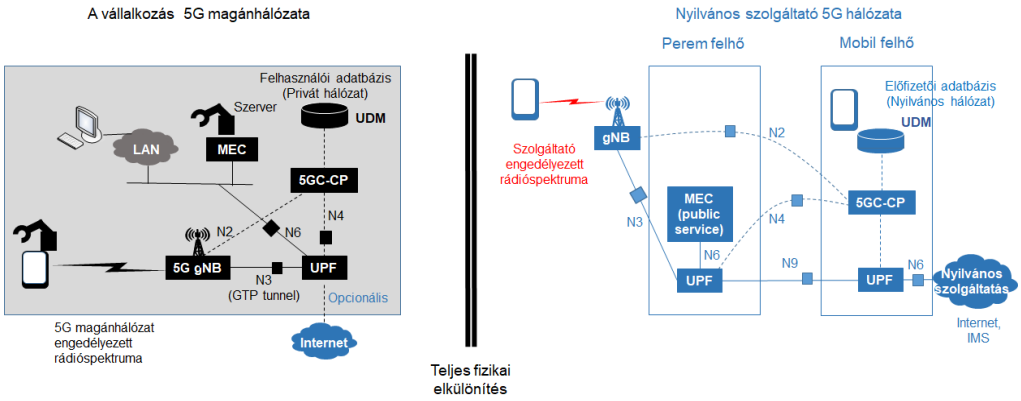
The reference points defined between the individual elements are marked in the figures according to 5G standards, where the dashed line indicates control and the solid line indicates data flow.

N2	Reference point for 5GC-CP control signals to gNBs.
N3	Reference point for data traffic between UPF and gNB
N4	Reference point for control signals between 5GC-CP and UPF
N6	Reference point between UPF and data networks
N9	Reference point between UPFs

4.2 Independent, physically isolated 5G private network

In these cases, the private network infrastructure is a given. The left side of the figures shows the private network, deployed either by the enterprise itself or by the operator or a commissioned general contractor. This is irrelevant from a systems engineering point of view.

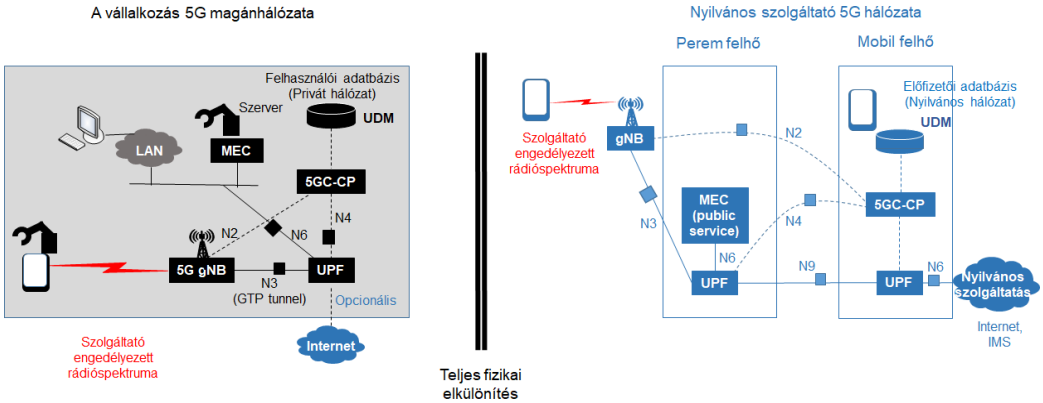
a) With own radio spectrum



Physically isolated 5G private network with the enterprise's own radio spectrum

A vállalkozás 5G magánhálózata	5G private network of the enterprise
Felhasználói adatbázis (privát hálózat)	User database (private network)
Opcionális	Optional
5G magánhálózat engedélyezett rádióspektruma	Licensed radio spectrum of the 5G private network
Nyilvános szolgáltató 5G hálózata	5G network of a public operator
Perem felhő	Edge cloud
Mobil felhő	Mobile cloud
Előfizetői adatbázis (nyilvános hálózat)	Subscriber database (public network)
Nyilvános szolgáltatás	Public service
Szolgáltató engedélyezett rádióspektruma	Operator's licensed radio spectrum
Teljes fizikai elkülönítés	Full physical isolation
Szerver	Server

b) With radio spectrum acquired from an operator



Physically isolated 5G private network with radio spectrum licensed to the operator

The only difference between these two cases is that in the latter case the terminal equipment is not supplied on the radio spectrum acquired by the enterprise, but on the radio spectrum licensed to the operator, within the premises of the enterprise.

In both cases there is full physical isolation between the public 5G network and the private 5G network, so all the reasons for the enterprise to deploy a fully independent network are met. A separated UDM does not allow the operator to access the internal information of the enterprise (e.g. number and configuration of connecting devices, robots, tablets, etc.), the fully separated data plane (UPF) separates the enterprise's data traffic from the public 5G network traffic, so sensitive data remains entirely within the closed system of the enterprise. The only point where some security measures are needed, even with full isolation, is the operation of the system. If the enterprise handles this itself (which is rare), even this is not an issue.

The specific needs of the enterprise, if any, can be taken into account when designing and deploying the 5G private network. Next to a production line or in a complex, automated assembly plant, ultra-reliable low latency communication (URLLC) type operation can be of paramount importance. This can be achieved by deploying a MEC system deployed at the appropriate points in the private network, which can perform special tasks without the need to send information up to the 5GC-CP central system for decision and intervention. This allows for extremely fast interventions within the deployed private network. In many cases, the MEC server is the unit of the enterprise that needs the highest level of protection because it contains most of the know-how (and more recently, artificial intelligence), which can give the enterprise a competitive edge over its rivals.

The deployment of 5G private networks, therefore, offers the advantage of a completely reassuring solution for data security and network security, the most efficient possible solution for URLLC and, of course, the advantage that production lines and servicing robots do not need to be equipped with a static optical network, which means that production remains flexible and can be reconfigured in a short time. Another advantage is that the network works reliably even if there is a failure in the public 5G network.

One serious disadvantage, of course, is the high deployment cost, which is further increased by the additional costs of selection and preparation. Another disadvantage is the need for an operational solution, because it either has to be outsourced, which can be very costly, or it requires in-house staff, which also has an above-average wage cost impact.

In these cases, the entire 5G private network is deployed with all its elements within the enterprise premises or building. This can be managed by the enterprise itself, the operator or a third party.

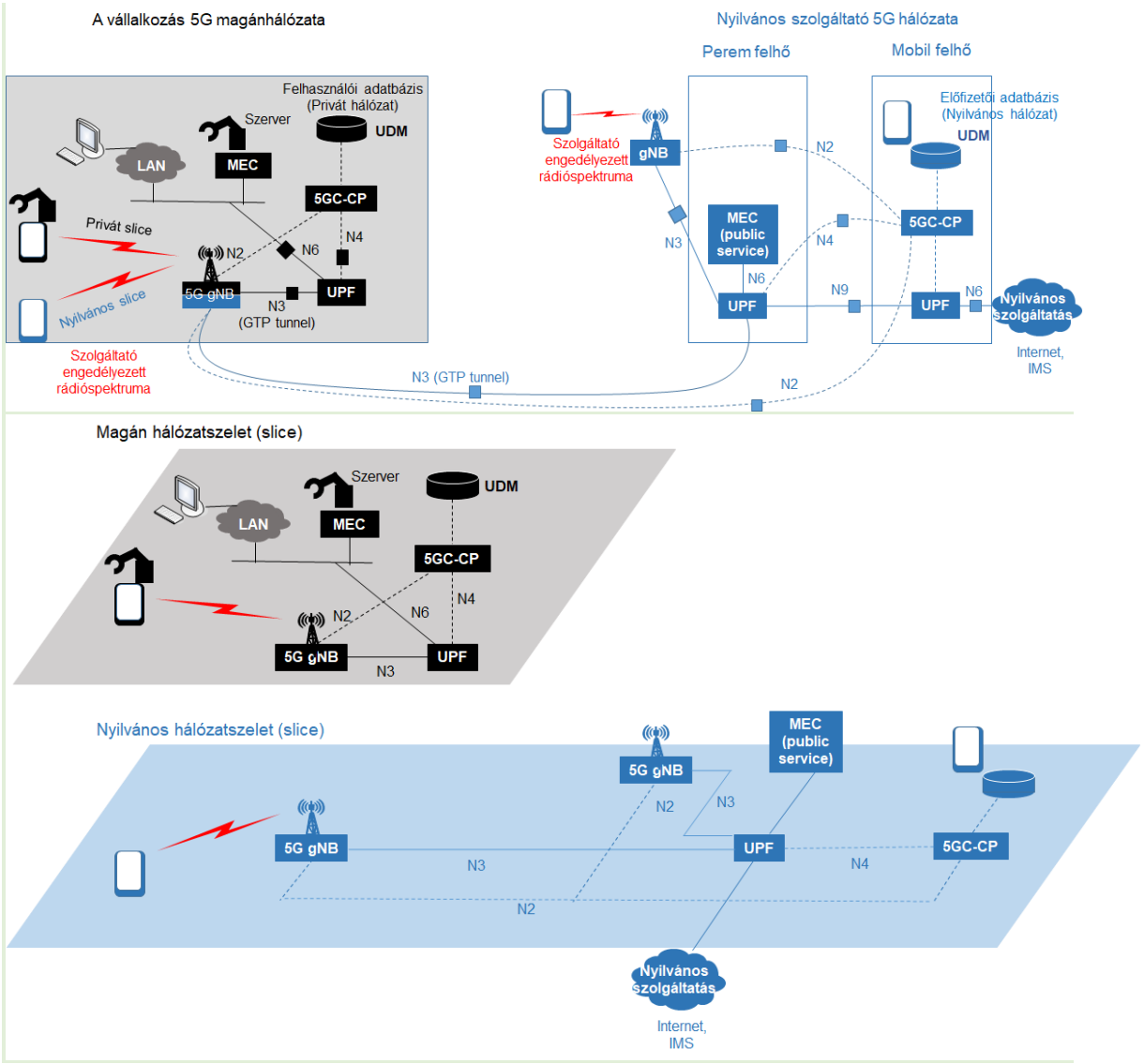
4.3 Hybrid private networks with network slicing

4.3.1 Sharing RAN network between private network and public network

In this solution, a network still physically separate is deployed for the enterprise, but both a 5G private network service and a public service are operated in the deployment area. To resolve this, the RAN network of the private network will be shared between the private network and the public network. In the figure, the shared gNB base station(s) are indicated by the mixed black (private) and blue (public) colouring. In this case, both applications are served by the licensed spectrum of the operator, but the 5G private network service is served from the private network, while the public 5G service is served from the public network. For this reason, a separate network slice is created by the public operator and the gNB is controlled from the control plane of the public network via the N2 reference point. The public network data traffic between the data plane of the public network and the base station uses an N3 reference point connection, but it is useful to include a GTP tunnel (GPRS Tunnelling Protocol) in the connection. Although GTP was originally invented for GPRS, which complemented the GSM system via packet switching, it has been extended to 3G and 4G systems, and more recently to 5G networks for some traffic passing through the N4 and N9 reference points, as well as for traffic passing through the N3 reference point between the gNB and UPF.

In the case of RAN network sharing, the public network provides a network slice to serve the shared RAN, and the private network also serves the entire enterprise and the shared RAN network in a single network slice (in most cases, this is the same as the entire 5G private network system).

The solution and the corresponding network slices are shown in the figures below.

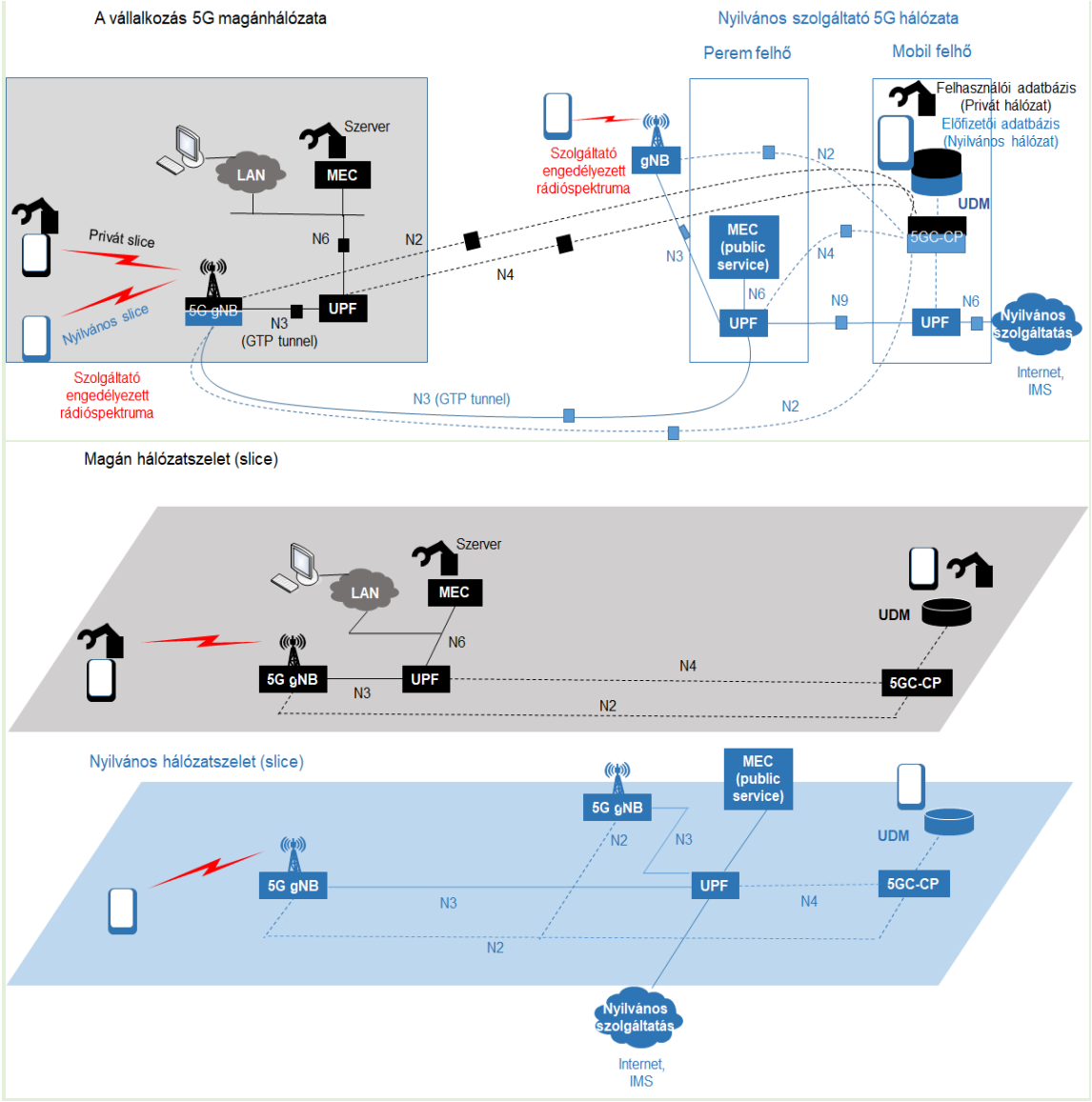


Sharing the RAN network within the private network

Magán hálózatszelet (slice)	*Private network slice*
Szerver	*Server*
Nyilvános hálózatszelet (slice)	*Public network slice*
Privát slice	*Private slice*
Nyilvános slice	*Public slice*

The solution differs from a fully physically isolated solution in that the 5G supply of the enterprise private network manages both closed applications and public connections on the same RAN. There is now an actual connection to the public network, but as private and public network traffic is still completely separated outside the RAN network, there is no real risk of any information about the enterprise falling into the wrong hands.

4.3.2 Sharing RAN network and control plane between private network and public network



5G private network using shared RAN and control plane

The next level of sharing is when only the data plane and the edge intelligence and RAN are deployed in the private network, but the entire control is provided from the public network, operating the 5G private network as a network slice of the public network. The RAN network can still be shared for private network closed and public network use, if the enterprise requires that. However, a significant change here is that the entire database, the UDM, is also divided into private and public database elements as the control plane is also shared. The gNB in the enterprise RAN network and the 5GC-CP and UDM in the public network are therefore logically separated in terms of the operation of the two systems. In the private network, the data plane (UPF) and the edge intelligence (MEC), which carries the specialities of the enterprise, continue to appear as physically separated entities. However, the entire system is powered by network slices on the public network, as shown in Figure 4.

The traffic on the 5G private network slice continues to be served over the on-premises data plane (UPF) of the enterprise, while its public traffic will reach the public network core via the public network's edge intelligence. It is also advisable to use GTP tunnelling here for public traffic. In this system design, since the traffic between the private network data plane and the RAN network is also operated by a network slice of the public 5G network, it is also appropriate

to secure the traffic flowing through the N3 reference point of the private network by using GTP tunnelling.

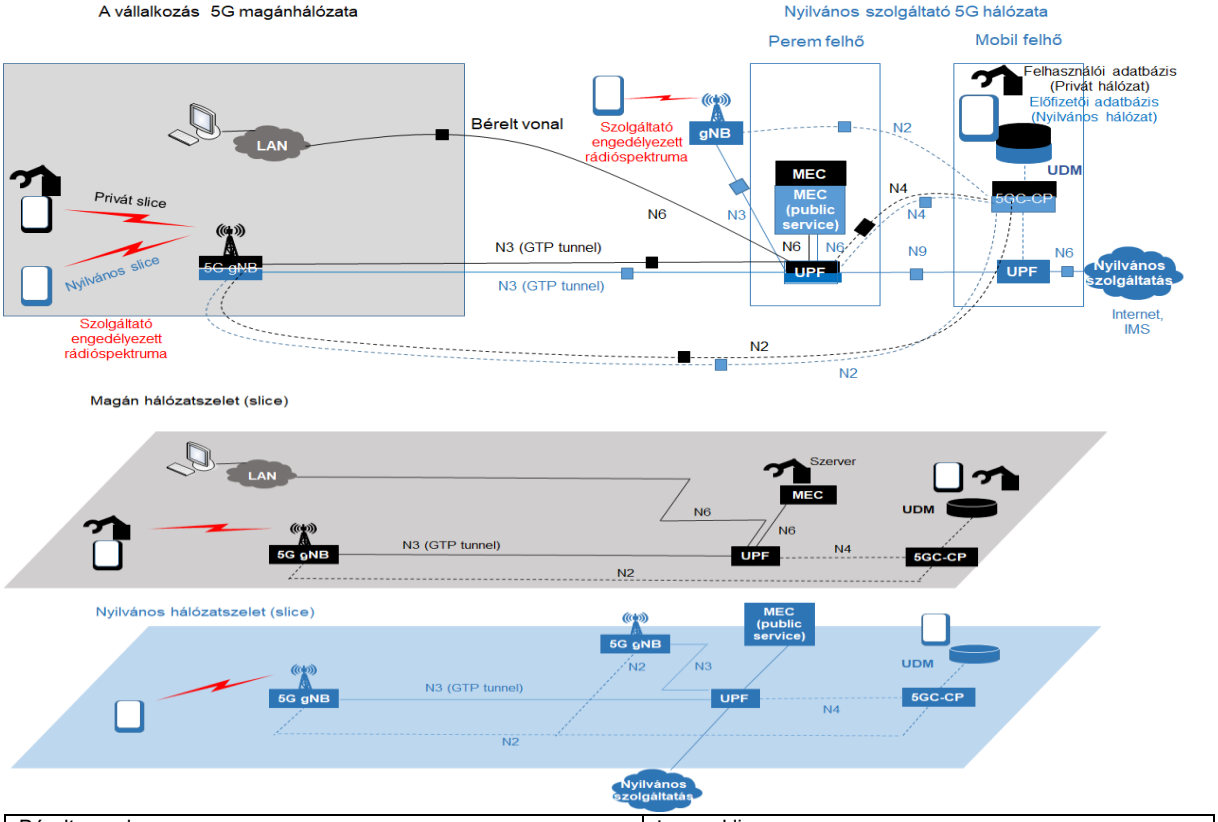
With this solution the investment costs of a separated part of the 5G private network can be kept relatively low, while the URLLC services required by the enterprise are available in high quality due to the locally deployed UPF and MEC, and this constellation also addresses critical data protection issues.

4.4 Virtual private network with network slicing: Sharing RAN network and core network between private network and public network (end-to-end control)

On the investment side, the least investment-heavy solution is when only the RAN network is deployed at the premises of the enterprise, and the RAN network as well as the entire core network are under the control of the public network's network slices, and the enterprise's data plane and edge intelligence are part of the public network, preferably controlled by the edge intelligence of the public network.

One of the characteristics of the solution is that, since only the gNB elements are deployed on enterprise premises, there is no on-site communication between the 5G private devices and the LAN network of the premises, unlike in the previous solutions. This means that the information has to reach the edge intelligence of the public network and then back to the LAN network and vice versa. This is achieved by a leased line connection linking the public edge cloud's shared data plane (UPF) and the enterprise's LAN network via the N6 reference point.

Consequently, 5G equipment serving enterprise 5G applications are controlled from the remote public edge intelligence, which can cause latency issues if the public network edge intelligence is not close enough to the premises. The system diagram of the solution and the private and public network slices are shown in the figure below.



Bérelt vonal	Leased line
Nyilvános slice	Public slice
Privat slice	Private slice
Magán hálózatszelet	Private network slice

Nyilvános hálózatszelet	Public network slice

Private network by creating an end-to-end controlled network slice

Obviously, this solution raises the question of data security, as all data traffic moves outside the enterprise premises. While MEC and UPF were still implemented within the private network in the previous solution, here all mobile traffic is transferred over the public network, and security protection can be ensured by GTP tunnelling, which forwards both private and public traffic of the RAN network on the premises over the N3 reference point.

In terms of investment costs, this is by far the cheapest solution for the enterprise, as only the deployment of the RAN network requires investment, alongside the potential added cost of the leased line for the LAN network. At the same time, network latency can be difficult to manage, data security issues can only be resolved on a trust basis and the enterprise is completely at the mercy of the availability parameters of the public operator.

Appendix 1
Abbreviations

MNO	Mobile Network Operator
RAN	Radio Access Network
MORAN	Multi Operator RAN
MOCN	Multi Operator Core Network
MCC	Mobile Country Code
MNC	Mobile Network Code
5GC-CP	5G Core - Control Plane
UPF	User Plane Function
UDM	Unified Data Management
MEC	Multi-Access Edge Computing
gNB / 5G-gNB	Next Generation Node B

Appendix 2
Definitions

Private network	A private network is a network that uses a broadband network, possibly including 5G capabilities, for some specific purpose (industrial, agricultural, scientific, logistical, health, transport, etc.) for wireless communication separated (partially, wholly or only virtually) from public networks.
Vertical	Generally it means “the sum of vertically related economic units”, whereas in 5G terms vertical refers to entities engaged in a similar range of activities within a sector (vertical industry). In this document, the term “vertical” primarily means a group of actors focused on serving a defined set of end-users or on achieving a specific, non-communication objective, but who need an electronic communications network to meet their internal communications needs. Verticals can be, for instance, healthcare, energy, transport, industry, education, logistics and public safety, etc.
Mobile Network Operator (MNO)	In this document, the electronic communications service provider operating a mobile telephony network with rights (with entitlements) of use for radio spectrum usage.
5G Core - Control Plane	The control plane of the 5G core network. This element is present in both public and private networks, as it is a basic element of the 5G network.
User Plane Function	The data plane function of the 5G network. This element is also present in both the public and the private networks and should be present in the public network in the core part and in the cloud of the edge network.
Unified Data Management	The 5G network’s subscriber database on the public network and its user database on the private network.
Multi-Access Edge Computing, formerly known as Mobile Edge Computing	A smart system at the edge of the 5G network, which is designed to bring intelligent functions closer to the terminal equipment for faster response times, without the need for a central 5G network system.
Next Generation Node B	gNB for short, is the name of the base station for 5G networks, sometimes used with the prefix “5G”, but most of the time not, because the base station for 4G networks is

	abbreviated as eNB, for 3G networks as NodeB, and for 2G networks as BTS.
N2	Reference point for 5GC-CP control signals to gNBs.
N3	Reference point for data traffic between UPF and gNB
N4	Reference point for control signals between 5GC-CP and UPF
N6	Reference point between UPF and data networks
N9	Reference point between UPFs.

5