ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO report 2023 R10276

5G Non-Public Network Architectures

An overview of deployment options and implementation considerations for enterprises

Date	7 February 2023
Author(s)	Tim Bergman Floris Drijver Pascal Heijnen Toon Norp Yonatan Shiferaw
Copy no	
No. of copies	
Number of pages	37 (incl. appendices)
Number of appendices	
Sponsor	SMITZH
Project name	DO IoT - 5G inspection drone (SMITZH)
Project number	060.53172

In case this report was drafted on instructions, the rights and obligations of contracting parties are subject to either the General Terms and Conditions for commissions to TNO, or the relevant agreement concluded between the contracting parties. Submitting the report for inspection to parties who have a direct interest is permitted.

Management Summary

Titel :	5G Non-Public Network Architectures
Auteur(s):	Tim Bergman Floris Drijver Pascal Heijnen Toon Norp Yonatan Shiferaw
Datum :	7 februari 2023
Opdrachtnr. :	
Rapportnr. :	TNO 2023 R10276

This report was created as part of a SMITZH funded project, in which TNO partnered with TUDelft, MCS, Surf and ExRobotics. The report provides an overview of the options for 5G private architectures and compare their attributes and setups to facilitate executive decisions. This report combines information from multiple sources on 5G network implementations. Four 5G private deployment options are described, how they differ, and what to think about when setting up 5G for your enterprise.

5G is the fifth-generation wireless technology designed from the ground up for high performance. To exploit the full 5G capabilities you need compatible User Equipment, a 5G-Core Network, and a Radio Access Network. Due to its modular design and high standards of performance, it is suited and adaptable to many different requirements, and it is possible to create different deployment options for private use, namely:

1. **Standalone**: fully independent network and radio stations on enterprise premises.
2. **Radio-Shared**: independent network but sharing radio base stations with a service provider.
3. **Radio and Control Plane-Shared**: user data traffic stays on the enterprise network, but radio, subscriptions, and network-internal control functions are handled by a service provider.
4. **Slicing**: fully dependent on a public network, in which a *virtually* independent ‘network slice’ is reserved for secure, private use by the enterprise.

When compared to each other, the deployment options broadly differ in terms of its dependency on service providers, which *increase* moving down from option 1 to 4. Note that although a standalone deployment with its full 5G system setup is (technically) managed by the enterprise, they can still be service provider-built and maintained. The same is true for option 2 and 3.

When determining in what way 5G, and which deployment option and optional integrations are best suited for your enterprise, think about specific requirements and trade-offs with regards to: latency, data throughput, capacity, privacy, security, customizability, roaming capacity, the time-sensitivity of your operations, CapEx, and OpEx.

What also needs to be considered are the operational aspects of the desired deployment: setup and configuration of the network, the hiring or training of staff, subscriptions to the involved network(s) through (e-)SIMs, and any optional integration with services and/or capabilities like VOIP, IMS, Time-Sensitive Networking, device onboarding functionality, and firewalled connectivity to other public networking services (e.g., for providing regulatory services like NL-Alert, emergency calls and lawful intercept).

Contents

1 Terminology and Abbreviations Used in This Document

5G: *5th generation* wireless technology.

5GS: *5G System*. The full ‘stack’ of the 5G system. Consists of:

- **5G Access Network**. The part through which the user (wirelessly) communicates *with* the network, e.g., **NG-RAN**: *Next Generation Radio* Access Network (which is used for 5G). The interface technology that is used for 5G radio is known as **NR**: *New Radio*.
- **5GC**: *5G Core* Network. The part of the network that provides data routing from and to mobile subscribers, application services, and other networks.
- **UE**: *User Equipment*. Devices that use 5G to access network services.

Control Plane: the set of network functions and protocols in the *Core* and *Radio* network that controls the network and the flow of user information. User authentication, session management, data storage, subscription management and monitoring, e.g., happens here. Most of the network functions are part of the control plane.

User Plane: the set of network functions and protocols in the *Core* and *Radio* network through which user data packets are sent and routed.

Network Function: a modular specification of a specific function that the network is required in order to engage in network traffic and communication servicing, for example:

- **AMF**: *Access and Mobility Function*. The function which receives requests to connect to the network, then checks with authentication network functions if the user is allowed to communicate with the network and which then maintains a signaling connection with the UE for other 5G Core network functions.
- **UPF**: *User Plane Function*. The function which routes data to and from user devices.
- **AUSF**: *Authentication Server Function*. The function which governs authentication processes to determine whether UEs are who they say they are as part of authorizing access to the network (though the authorizing function happens elsewhere).
- **SMF**: *Session Management Function*. The part of the 5G Core network that sets up and manages communication sessions with UEs.
- **AF**: *Application Function*. A function in the 5G Core network that represents a certain application.
- **UDM**: *Unified Data Management*. A part of the 5G Core Network which handles subscriber data and profiles.
- **UDR**: *Unified Data Repository*. A part of the 5G Core Network which provides data storage for the 5G Core.
- **PCF**: *Policy Control Function*. A function which provides policies based on subscription information, that are then executed in other functions. For example, the PCF might issue modified resource allocation policies for the UPF for high importance subscribers, such as emergency services, over recreational services.

- **NRF**: *Network Repository Function*. The function which provides service discovery between individual network functions, i.e., which functions as a 'telephone book' so other network functions can advertise what they do, and where to find them within the network).
- **NEF**: *Network Exposure Function*. The function which provides a means to securely expose capabilities and events to be able to control and adapt the network.
- **NSSF:** *Network Slice Selection Function*. The function which selects the network slices serving the UE and decides through which AMF to access them.

gNB: *gNodeB*. The wireless base stations/radio equipment that sends and receives radio signals to and from the UEs.

Slice: a *virtually* independent network reserved for a client or purpose. Because 5G has virtualized network functions and is unbound with regards to the physical hardware, it is possible to create independent networks *not just* by setting up a new physical infrastructure, but also by creating multiple network functions of the same type, separating them, and reserving these for different clients or purposes. These independent virtual networks are called *slices*.

AAA: *Authentication, Authorization, Accounting*. A process for:

- **Authentication**: checking if the identity of a user is genuine.
- **Authorization**: checking if the user is allowed to use the network or service.
- **Accounting**: any appropriate logging is performed.

Onboarding: the process of providing credentials to a device that is visiting a new network, based on a credentialing server from an external network. For example: when a device visits a network on a branch location of an enterprise, credentials to that network may need to be added via another network first.

CAG: *Closed Access Group*. A group of subscribers who are allowed to access one or more CAG cells associated with them. Used in PNI-NPNs (deployment options 2-4) to restrict access to only enterprise-authorized UEs when in an enterprise's CAG cells.

Cell: the coverage area of a network base station.

Roaming: the process of still having or guaranteeing connectivity to an operator's network via networks that do not belong to the operator when a device goes outside of its network's coverage.

SIM: the *Subscriber Identity Module* of a device, i.e., a module that securely stores the subscriber identity of a device used to authenticate it as a subscriber on a mobile network.

e-SIM: *embedded-Sim, a* programmable SIM that is permanently embedded in a device. Because it is hardwired onto a device, the SIM can *only* be used by that device, but unlike regular SIMs, e-SIMs can be programmed with the credentials or subscriptions to networks such that the physical SIM card does not have to be removed or added every time a device must work on a new network.

Cloud: cloud services or cloud computing are those (computing) services that are accessed via the internet and may not be bound to any physical location or computer.

Server: any computer or program that provides a service to clients. For example: AAA-servers are servers dedicated to providing Authentication, Authorization and Accounting services for an enterprise. Mostly refers to the physical computer, though these may also be running in the cloud.

S-NPN: *Standalone Non-Public Network*. A private network that is built on and maintained by the enterprise. Corresponds to deployment option 1 in this document's overview.

PNI-NPN: *Public Network Integrated Non-Public Network*. Network architectures that are (partially) dependent on public networks. Corresponds to deployment options 2-4 in this document's overview.

PLMN: *Public Land Mobile Network*. A cellular mobile network that is publicly accessible (as opposed to private networks).

TSN: *Time Sensitive Networking*. A network protocol layer that synchronizes processes across the network, which is crucial for time-sensitive operations.

CapEx: *Capital Expenditure*, i.e., the cost of setting up the system. Includes for example buying and setting up the base station, cloud infrastructure, software needed, etc.

OpEx: *Operational Expenditure*, i.e., the running costs of running the system. Includes for example licensing costs of the spectrum bands, usage fees of public network service providers, hiring IT staff, etc.

IoT: *Internet of Things*. Networked devices ranging from self-driving cars to sensor networks.

B2B2X: *Business-to-Business-to-X*: business model in which services are provided between businesses, as well as to any number of end users.

2 Introduction

This report is created as part of a SMITZH-project. “5G in de maak-industrie” Partners in this project are ExRobotics, TU Delft, TNO, MCS and SURF. The latter four partners also work together in the Do IoT Fieldlab on creating 5G knowledge and managing test- and demonstration- facilities for various sectors, including the manufacturing industry.

In the manufacturing industry there are production processes where the application of (new) communication technology is particularly complex due to extreme circumstances. Extreme circumstances include very high temperatures (e.g. printing or welding metal), or toxic environments (e.g. thermo coatings, very humid or dusty environments). Before companies can work with 5G applications in such environments, two questions must be answered: which technical solutions can withstand such extreme conditions, and can these solutions be certified in the current safety standards so that they can actually be used.

ExRobotics is the global market leader in autonomous inspection robots for such extreme environments in industry that require ATEX certification, especially for environments with explosive vapors, high temperatures, moisture or dust, and aims to strengthen this position in the manufacturing industry. The project will demonstrate and validate to what extent both questions can be met to this end.

The project also set out to create a report on different types of 5G private network architectures for different situations at industrial production sites. Specifically describing options of private network architectures that can work internationally. This allows companies to improve their feasibility study and business case in advance, also for export.

The robots are able to navigate independently, have sensors on board for a wide variety of on-site measurements including abnormal temperatures, and can also read meters as a human would using Computer Vision technology. They offer remote experts the opportunity to monitor a hazardous environment. Such robots are used to make the production process safer, more efficient and fully continuous.

ExRobotics supplies around 60 robots per year, currently mainly to the petrochemical industry, and it wants to increase its footprint in the manufacturing industry. To this end, the product (platform) should offer a number of additional options, whereby the (cyber security of) communication between robot, data processing environment ('cloud') and control room over 4G is no longer sufficient. If, in these strictly certified environments, 5G can be implemented, it is expected that many of these additional possibilities can be realized.

Since ExRobotics already has a working robot platform EXR-2, we will demonstrate the new modular 5G housing on that platform. The platform is now mainly used in the petrochemical industry, but the product requirements for extreme environments in the manufacturing industry are largely the same as those for the petrochemical industry.

3 What Is 5G and What Can It Offer Enterprises?

5G is the fifth generation of cellular wireless technology. The first four cellular wireless technologies were designed with a focus on voice calls (1G), sending short text messages in addition (2G), mobile and wireless internet connectivity (3G), and greater mobile connectivity for more and varied types of internet traffic simultaneously (4G). 5G has been designed from the ground for flexibility and big data handling requirements. This is because 5G needs to support applications and use cases that are projected to become important in the future. The three key service types 5G is designed for are:

- **Ultra-Reliable Low-Latency Communication**: that is, communication in which the time between sending and receiving messages is extremely low, and which is very unlikely to be compromised or lost in transit. This kind of communication is important for *mission critical applications* such as *critical infrastructure, factory automation, robotics, or self-driving cars*.
- **Massive Machine-Type Communication**: that is, a communication type which can handle large amounts of devices communicating with it continually. This kind of communication is important for *Internet of Things applications such as sensor networks, self-driving cars, and monitoring and control services*.
- **Enhanced Mobile Broad Band**: that is, being able to quickly send and receive large amounts of data simultaneously. This kind of communication is important for *mobile user experience-focused applications such as streaming and virtual reality, and real-time monitoring services*.

To accomplish this, the 5G system is designed in various parts, namely *Radio* (which includes antenna design and operation, and electromagnetic spectrum considerations) and *Core* (which includes the various functions the network should be able to accomplish such as user authentication, billing subscriptions, and sending data to and from end-users, as well as how these distinct functions ‘talk’ to each other, and how networks and its parts connect). An important part of the Core design is that these functions are *virtualized*, i.e., they are not hard coded into hardware, but can be run on most generic processing devices, such as (cloud) servers.

Because its parts are disentangled from each other and many parts are virtualized, there are a lot more options to choose from in setting up 5G private networks when compared to 4G. In 4G, the options are setting up a private network yourself, or having an integrator or MNO set up the network. For 5G, sharing parts of the network and even virtual network slices become possible. These will be covered in the rest of this document.

In summary:

- 5G is the fifth-generation wireless technology designed from scratch for high performance.
- The benefits to using 5G are its greater capacity in handling simultaneous users and data, its speed, and its reliability for critical applications and quality of experience.
- Due to its modular design, virtualized network functions, and high standards of performance, 5G is suited and adaptable to many different industries, requirements and use cases.

- Compared to 4G, 5G is more flexible and has more options for setting up private networks.

4 The Basic 5G Architecture

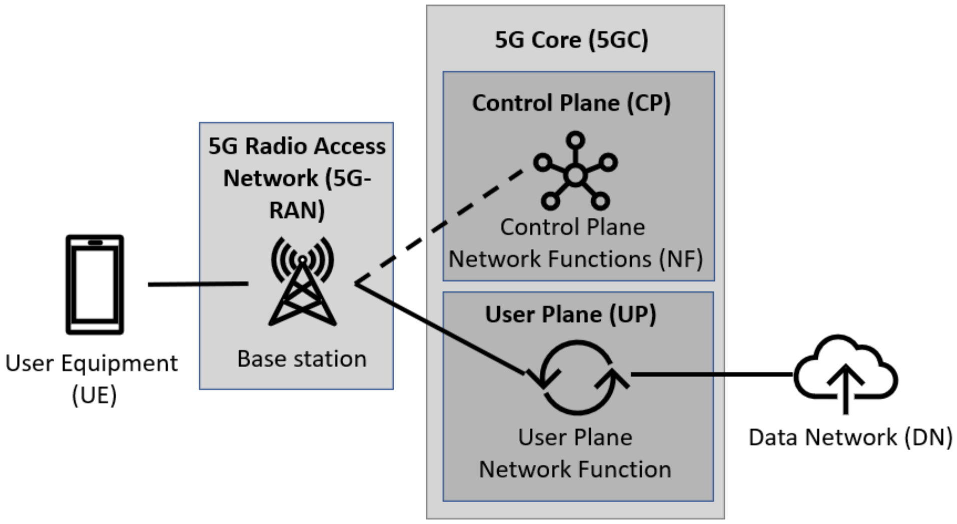
5G Core (5GC)
Control Plane (CP)
Control Plane Network Functions (NF)
User Plane (UP)
User Plane Network Function
5G Radio Access Network (5G-RAN)
Base station
User Equipment (UE)
Data Network (DN)

Figure 1: The basic 5G architecture

The basic architecture of a 5G network consists of 3 sections: UE, Core and Radio.

UE: you will need *User Equipment able to connect* to the network, i.e., equipment that has a *5G capability* and a *SIM with a subscription to the network*.

5GC: you will need access to a running *5G-Core*. The Core network is made up of Network Functions, which each fulfil a role in the network's operation. These can be separated into the Control Plane (for network-internal tasks like authentication) and User Plane (for transmitting user data). There are various implementations of 5G-Core, some of which are open source. This core will need to be hosted on a *server*, usually running on a physical machine or a virtual machine on a cloud server.

RAN: access to an operational *5G-Access Network such as a radio base station*, and *usage plans to the electromagnetic spectrum bands* which it will *use (and, if applicable, paid-for usage licenses)*.

As these components may be expensive or difficult to build, buy/rent, secure and support, it may not be feasible or even necessary for every enterprise to set up their own complete 5G system, nor do they have to only use public networks. Because the 5G System has been designed in a modular and virtualized/software-based way, there are also other deployment options to allow for various levels of private deployment vs. public integration.

In summary:

- The 5G System consists of a (Radio) Access Network, the Core Network and User Equipment.
- The Core network is made up of Network Functions, which each fulfil a role in the network's operation. These can be separated into the Control Plane

(for network-internal tasks like authentication) and User Plane (for transmitting user data).

- The RAN is made up of radio base stations, and the Core is often deployed on virtual machines running on (cloud) servers.
- To use 5G you need compatible User Equipment with subscriptions to the network, a Core network hosted on a (cloud) server, and a Radio Access Network and spectrum usage plans.
- Because of the modularity and virtualized nature of 5G, there are various deployment options, some of which do not require a full network installation.

5 Four Possible Non-Public Network Architectures for Enterprises

This chapter will give an overview of the four non-public network architectures (also known as *deployment options*), how they differ, what their pros and cons are, and what aspects are the responsibility of (and therefore to be discussed with) a service provider vs. kept in-enterprise.

The four non-public 5G network architectures that are explored are:

1. **Standalone**: fully independent private network managed by the enterprise.
2. **Shared RAN**: independent Core but sharing the Radio network with a service provider.
3. **Shared RAN and CP**: independent User Plane so enterprise data traffic stays within the enterprise but sharing the Radio network and Control functions with a service provider.
4. **Slicing**: fully dependent on a public network, in which both Core and RAN are shared, and a *virtually* independent ‘network slice’ is set up for secure, private use by the enterprise.

For a visual diagram of these architectures, see the figure below.

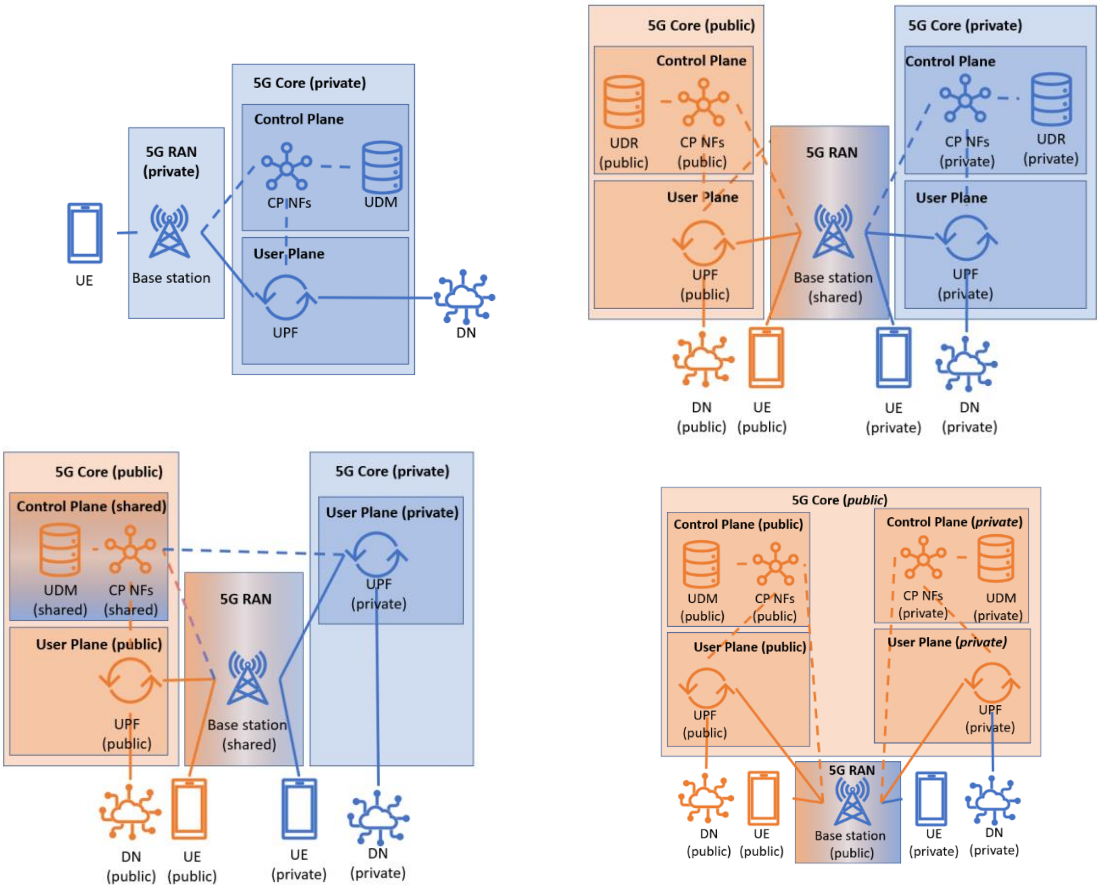

Figure 2: The four non-public network options, from Top-Left (TL) to Bottom-Right (BR): 1. Standalone (TL), 2. Shared Radio Access Network (TR), 3. Shared Radio Access Network and Control Plane (BL), 4. Network Slice (BR)

5.1 1. Standalone

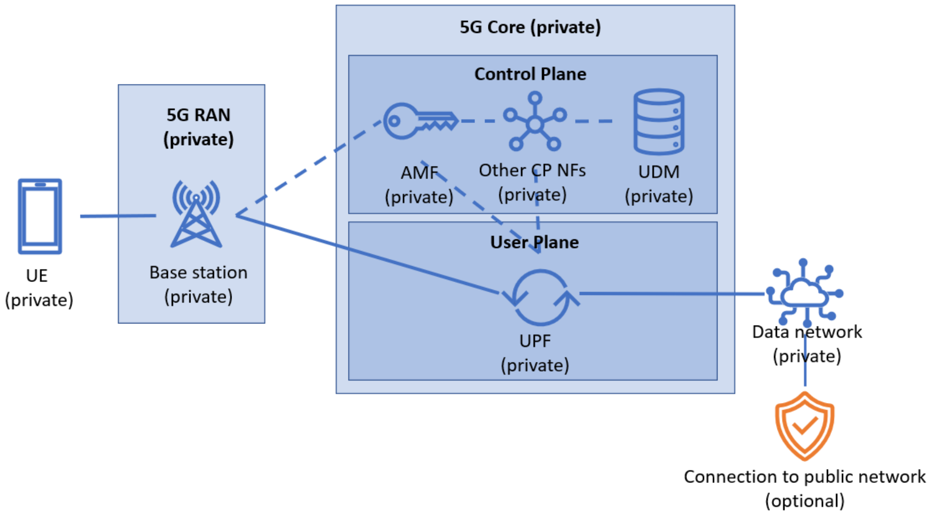

Figure 3: Standalone Non-Public Network

The Standalone Non-Public Network deployment option has all elements of the system located and set up for use within the enterprise. When a UE connects to the network via an enterprise base station, all authentication, session management and user data transfer is done through the enterprise's private network. All subscription and operational data are managed and kept within the enterprise network. As the network is independent, it has its own Network ID, manages its own subscriptions, and UEs require a SIM with a subscription to the network.

In-enterprise setup: in the standalone option, the enterprise sets up a *full* 5G System (radio base stations, 5G Core instance running on a server, with a full Control Plane to handle network-internal functions, User Plane Function to handle user data traffic, and Unified Data Management for storing subscription data. If public network or internet connectivity is wanted, a firewalled connection to the public network is also needed.

Pros: due to its isolation from public networks, operational and subscription data is secure and private on the enterprise premises, and Quality of Service can be guaranteed independent of public networks, and no monthly subscription charges for public network usage is required. Due to the proximity of all network components, Ultra-Reliable Low Latency can be guaranteed.

Cons: since the whole network must be managed in-house, requiring dedicated software, hardware, spectrum licenses (if the network needs access to licensed spectrum bands, else it can use the unlicensed, publicly shared spectrum bands), specialized staff, and any other 3rd party support, the CapEx is significantly higher than in the other options. Furthermore, when roaming is needed any (multi-SIM) user equipment will need a subscription to the public network provider in addition to the subscription to the private network.

The network *may* be built and provided by a Service Provider (SP) such as a systems integrator or an operator, then the network may have access to the SP-licensed spectrum and could be maintained by the SP through Service Level Agreements. The CapEx may still be high, but may be subsidized (e.g., by certain governments), and the OpEx will consist of monthly SP-fees.

Attributes, and if the architecture *performs* better (High) or worse (Medium, Low) on them *compared to the others*:

- **Connectivity**: **Medium**. Depends on the network's (optional) connection to the public network: if a connection to the public network is setup, connectivity is higher, else it is lower as devices can only connect to the enterprise network.
- **Service continuity**: **Low**. See above. Note that even if a UE has a subscription to a PLMN, leaving the service area of the enterprise network will imply a dropped session.
- **Low latency**: **High**. Due to traffic isolation and physical proximity, the network is highly performant in achieving low latencies.
- **Throughput**: **High**. See above, except that high throughput can be achieved.
- **Availability**: **High**. See above, except that high availability can be achieved.

- **Monitoring**: High / Medium. Monitoring quality depends on the degree of access that the NPN operator has within the network.
- **Privacy**: High. Due to physical separation and enterprise-managed data storage and traffic, this can be highly protected.
- **Security**: High. See above. Do note that this is only in terms of security by physical separation of the network. Any further security measures become the responsibility of the enterprise. It is therefore also highly dependent on how well the enterprise implements it. This requires attention and expertise.
- **Customizability**: High. As the enterprise sets up its own network, customizability is high. Note that when you have a connection to a PLMN, it will have to be (at least partially) adapted to the requirements of the public network, in which case customizability is (slightly) lowered.

Costs, i.e., how the architecture compares with the others in terms of expenses:

- **CapEx**: **High** / **Medium**. Depending on whether the private 5G architecture is subsidized (which some governments grant), the CapEx is relatively high as the entire network will have to be privately set up, and spectrum licenses will have to be bought.
- **OpEx**: **High** / **Medium**. Depending on in-house vs. SP-management and maintenance costs, OpEx may be high.

In summary:

- A standalone deployment has a full 5G system setup and is managed by the enterprise, although they can be service provider-built and maintained. CapEx is comparatively high.
- Due to physical proximity and isolation of traffic to the enterprise network, comparatively, latency is low, and throughput, availability, privacy, and security are high.
- Depending on whether an additional optional connection and subscriptions to a public network is set up, connectivity and customizability can be either high or medium. For better connectivity UEs will need at least two independent subscriptions in the device.

5.2 2. Shared Radio Access Network

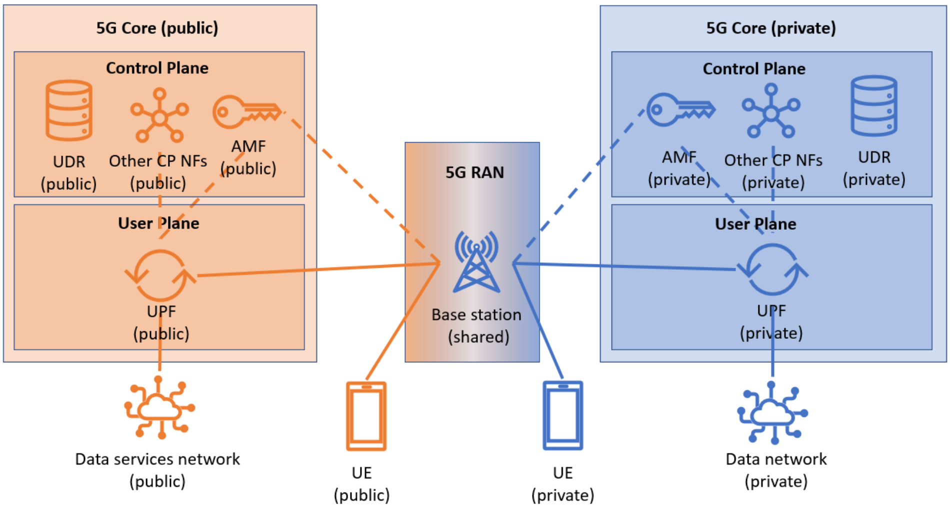

Figure 4: Shared Radio Access Network

The Shared Radio Access Network deployment option has all elements of the system located and set up for use within the enterprise but shares a radio base station with an operator. When a UE connects to the network via radio base stations shared with a service provider, all authentication, session management and user data transfer is still done through the enterprise's private core network. All subscription and operational data are managed and kept within the enterprise network. As the core network is still independent (the deployment only sharing radio access), it has its own Network ID, manages its own subscriptions, and UEs require a SIM with a subscription to the network.

In-enterprise setup: the enterprise will need a 5G-Core with Control Plane and User Plane, a UDM for subscription storage, and the optional firewalled connection to the public network.

Operator-shared: the radio base station located at the enterprise, as well as the frequency bands the operator has access to, will be shared between the operator and the enterprise.

Pros: both subscription and operations data are stored and routed only through the enterprise-private network. Due to the proximity of all components, and a dependence on *only* the SP’s radio access network, low latency and quality of service can be (relatively) independently guaranteed. As the radio system is shared, the enterprise *may* have access to, or may even lease some of the operator-licensed spectrum (though this is dependent on the regulatory conditions in the country in which the network is setup). Otherwise it can use the unlicensed shared spectrum or enterprise-licensed spectrum. The operator maintains the running of the radio network based on service level agreements.

Cons: as the radio base stations also support public UEs, security and (potentially) quality of service metrics may be impacted. For CapEx, there is still the software, hardware and potential licensing needed to operate the Core Network and UDM on a (cloud) server. OpEx consist of monthly fees or charges for usage rights of the RAN, as well as any IT staff or 3rd parties for enterprise-specific operation of the network and troubleshooting.

Attributes, and if the architecture *performs* better (High) or worse (Medium, Low) on them *compared to the others*:

- **Connectivity**: **Medium**. Depends on the network's (optional) connection to the public network: if a connected to the public network is setup, connectivity is higher, else it is lower as devices can only connect to the enterprise network.
- **Service continuity**: **Low**. See above. Note that even if a UE has a subscription to a PLMN, leaving the service area of the enterprise network will imply a dropped call.
- **Low latency**: **High** / **Medium**. As this option depends on shared RAN, latency will be dependent on whether resource isolation/allocation in the RAN allows for QoS requirements and agreements.
- **Throughput**: **High** / **Medium**. See above.
- **Availability**: **High** / **Medium**. See above.
- **Monitoring**: **High** / **Medium**. Monitoring quality depends on the degree of access that the NPN operator has within the network.
- **Privacy**: **High**. Due to physical separation and enterprise-managed data storage, and with the traffic being logically separated in the RAN, this can be highly protected.
- **Security**: **High**. See above.
- **Customizability**: **High** / **Medium**. As this option depends on the public network setup, and any requirements and adaptations of the private network elements in connecting to the public network shared elements, customizability can be said to be (somewhat) lowered.

Costs, i.e., how the architecture compares with the others in terms of expenses:

- **CapEx**: **Medium** / **Low**. CapEx will be lower than in the standalone option, but we will still need own cloud and core instance. Depending on the deployment used, this may range to be lower or higher.
- **OpEx**: **Medium** / **Low**. Depending on in-house vs. operator-management and maintenance costs, OpEx may range to be lower or higher.

In summary:

- A RAN-shared deployment has most of the 5G system built managed by the enterprise, but the RAN radio system is shared with a public service provider.
- Due to physical proximity and the isolation of traffic to the enterprise network, latency, throughput, availability, privacy, and security are comparatively high, though these become more reliant on the service provider's RAN.
- Depending on whether an additional optional connection and subscriptions to a public network is set up, connectivity and customizability can be either high or medium. For better connectivity UEs will need at least two independent subscriptions in the device.

5.3 3. Shared Radio Access Network and Control Plane

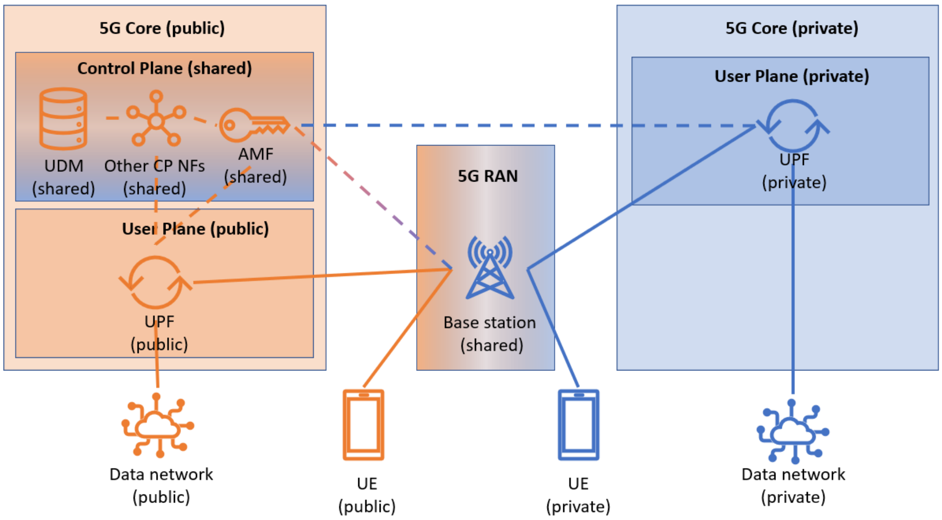

Figure 5: Shared Radio Access Network and Control Plane

The Shared Radio Access Network and Control Plane deployment (also known as **Local Breakout / LBO**) **option** shares the radio and network-internal control functions with the service provider but keeps user data routing within the enterprise premises. When a UE connects to the network via radio base stations shared with a service provider, all authentication, session management and other control functions are done through the service provider's network. When the user data session is setup, however, user data traffic goes through the at the enterprise-hosted user plane function. Subscription data is managed and kept with the service provider, but operational data is kept and routed within the enterprise network. This deployment option can be realized through network slicing (creating a logically separate virtual network instance reserved for the network's traffic), or via the 3GPP Access Point Name feature, which allows traffic to be routed to the network in question. As this deployment option is hosted by the operator, subscriptions are managed by the public network, and UEs require a SIM with a subscription to the public network.

In-enterprise setup: the enterprise will still need a 5G-Core with User Plane Function, and an optional firewalled connection to the public network.

Operator-shared: the radio base station at the premises, and the 5G-Core deployment including Control Plane and User Data Management in operator's edge cloud are shared between the operator and enterprise.

Pros: due to the proximity of user data server, ULLC and QoS can still be guaranteed independent of the public network. Due to sharing radio resources with an operator, access to the operator-licensed spectrum is *possible* (though this is dependent on the regulatory conditions in the country in which the network is setup, else it uses the unlicensed shared spectrum). CAGs can be used to reserve radio resources for the enterprise. CapEx is significantly lower, as only a server running a User Plane is needed. The operator maintains the running of network through

SLAs. Operational data is still stored locally and securely. Roaming is possible as you have a subscription to the operator.

Cons: as the Control Plane is serviced by the operator, signaling is dependent on operator network, and a subscription to the service provider is needed, and the subscription info of enterprise private UEs are stored in operator's servers. OpEx consists of monthly subscription or charges, and any IT staff or 3rd parties for enterprise-specific operation of the network and troubleshooting.

Attributes, and if the architecture *performs* better (High) or worse (Medium, Low) on them *compared to the others*:

- **Connectivity**: **High**. Due to the fact this deployment option requires a connection and subscription to the public network, high connectivity can be guaranteed.
- **Service continuity**: **High**. See above.
- **Low latency**: **High** / **Medium**. As this option depends on shared RAN and CP, latency will be dependent on whether resource isolation/allocation in the RAN allows for QoS requirements and agreements.
- **Throughput**: **High** / **Medium**. See above. Note that CAGs can be used to reserve radio resources for the enterprise.
- **Availability**: **High** / **Medium**. See above.
- **Monitoring**: **High** / **Medium**. Monitoring quality depends on the degree of access that the NPN operator has within the network.
- **Privacy**: **Medium.** Due to a logical separation in the RAN and CP, privacy can still be guaranteed, but not as high as the standalone, physically isolated case could.
- **Security**: **High** / **Medium**. See above, and additionally, this would also depend on the quality of the security measures of the public network and any further agreements made.
- **Customizability**: **High** / **Medium**. As this option depends on the public network setup, and any requirements and adaptations of the private network elements in connecting to the public network shared elements, customizability can be said to be (somewhat) lowered. Network slicing gives relatively more control over the requirements and setup of the network, however, which would make the customizability relatively high.

Costs, i.e. how the architecture compares with the others in terms of expenses:

- **CapEx**: **Medium** / **Low**. CapEx will be lower than in the standalone option, but we will still need own cloud and core instance. Depending on the deployment used, this may range to be lower or higher.
- **OpEx**: **Medium** / **Low**. Depending on in-house vs. operator-management and maintenance costs, OpEx may range to be lower or higher.

In summary:

- A RAN- and CP-shared deployment has most of the 5G system shared and managed by the service provider, with only the User Plane located in-enterprise.

- Due to physical proximity and the isolation of traffic to the enterprise network, latency, throughput, availability, privacy, and security are comparatively high, though these become more reliant on the service provider’s RAN and CP.
- Due to a required connection and subscriptions to public network, connectivity is comparatively high, customizability low, and roaming is easier to implement.

5.4 4. Network Slice

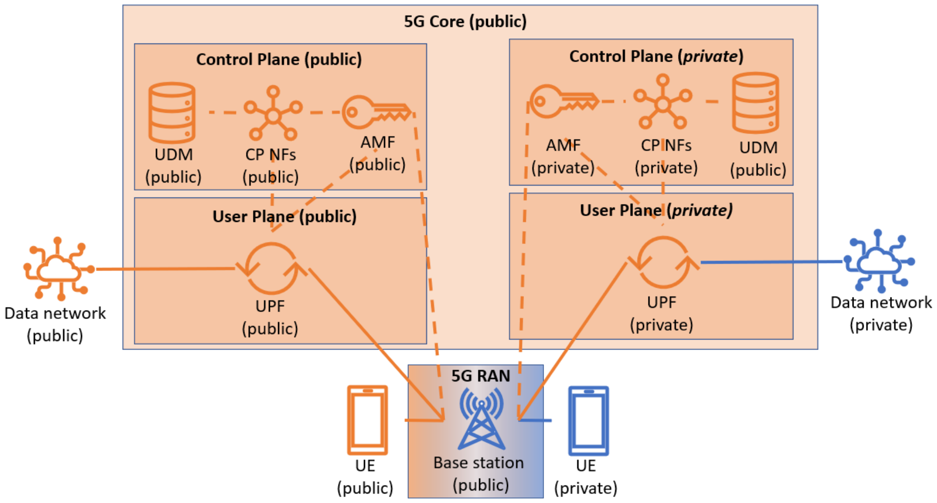

Figure 6: Network Slice

The Network Slice deployment option has all elements of the system deployed in a public network (*virtually* isolated from other public traffic). When a UE connects to the network via a (shared) radio base station, all authentication, session management, and control functions, as well as all user data transfer is done through the public network infrastructure (though, again, *virtually* isolated from other public traffic). All subscription data is managed and kept within the enterprise network. Operational data can be kept and managed within the enterprise, though any of its data traffic will be routed through the (virtually isolated) public network. As the public network manages the subscriptions, UEs require a SIM with a subscription to the public network, and the network slice is identified via its public network ID, and the S-NSSAI (Single-Network Slice Selection Assistance Information), consisting of the SST (Slice/Service Type) and an optional SD (Slice Differentiator).

Operator-shared: in the slicing option, the *full* 5G system has been implemented *by the service provider* (i.e., radio base stations, 5G Core instance running on the operator's cloud, with a full Control Plane and User Plane, and Unified Data Management for storing subscription data). Within this network a virtual ‘network-slice’ has been isolated for use by the private enterprise.

Pros: as the infrastructure is already built and maintained, and spectrum licenses already bought by the service provider, the CapEx costs are the least compared to other cases, and services are instead guaranteed through Service Level Agreements and OpEx fees. Due to the virtual network slice, there is still a *logical* separation with public network traffic, so data traffic is still (relatively) secure. Because devices require a subscription to the operator-network, roaming is easier to implement.

Cons: depending on the use-case, a subscription to the public network may not be wanted. Both operational data traffic and control signaling of enterprise-private user devices are routed off premises and subscription data is stored in operator’s servers, which may be undesirable from a security or privacy standpoint. Because the Slicing option is more of a service, OpEx consists of monthly subscription or usage fees to the service provider.

Attributes, and if the architecture *performs* better (High) or worse (Medium, Low) on them *compared to the others*:

- **Connectivity**: High. Due to its reliance on a connection and subscription with a public network, connectivity is high, and roaming is possible.
- **Service continuity**: High. Due to its reliance on a connection and subscription with a public network, connectivity is high, and roaming is possible.
- **Low latency**: High / Medium / Low. Whether low latency can be achieved depends on the distance signals and data needs to travel: the closer an edge computation node is, the lower the latency will be; similarly, if traffic must travel to a far-away cloud computation node, latency will be higher. It also depends on whether the resource isolation/allocation within the network (which may fluctuate depending on the load on the operator) allows for the QoS requirements and agreements.
- **Throughput**: High / Medium / Low. Depending on whether the resource isolation/allocation within the network (which may fluctuate depending on the load on the operator) allows for the QoS requirements and agreements. The greater the operator is impacted in its functioning (for whatever reason, e.g., DDOS, defects), the greater the slice may be impacted, and thus the lower the throughput may become. Note that CAGs can be used to reserve radio resources for the enterprise.
- **Availability**: High / Medium / Low. See above.
- **Monitoring**: High / Medium. Monitoring quality depends on the degree of access that the NPN operator has within the network.
- **Privacy**: Medium. Due to only a logical separation in the RAN and CP, data privacy is not as high as in the other options. In the slicing option, the subscriber information will be stored and managed by the operator. User data traffic is also routed via the operator's network, which may bring privacy and security concerns: the operator has access to user data, and may be forced to support lawful intercept.
- **Security**: High / Medium / Low. See above, and additionally, this now fully depends on the quality of the security measures of the public network and any further agreements made.
- **Customizability**: High. As this option is completely hosted on public network elements, the customizability is limited to the options and agreements that are offered by the operator. Due to a network slice being a purely logical construct, it does give a large amount of control over the requirements and setup of the network, making the customizability high.

Costs, i.e. how the architecture compares with the others in terms of expenses:

- **CapEx**: Low. As SP already has all the infrastructure, CapEx is the lowest of all the deployments. If anything, new radio base stations may need to be placed, which may be subsidized.
- **OpEx**: Medium / Low. Depending on in-house vs. operator management and maintenance costs, OpEx may range to be lower or higher.

In summary:

- A sliced deployment has all the 5G system built and managed by the operator, in which a *virtually* independent ‘slice’ is reserved for private and secure use by the enterprise.
- Latency, throughput, availability, privacy, and security can vary depending on agreements with and the capacities of the operator's network.
- Due to a required connection and subscriptions to the public network, connectivity is comparatively high, customizability low, and roaming is easier to implement.
- Compared with all the other options, CapEx is the lowest.

6 Comparing and Evaluating Network Attributes of the Architectures

This chapter will give a summarized, brief comparison of the four non-public network architectures, and how they differ in terms of which aspects are the responsibility of (and thus to be discussed with) the network service provider, and which aspects are to be maintained by the enterprise (or any 3rd parties it may hire to do so), as well as key network attributes which may be important for the running of the services of the enterprise. For more details, see the dedicated chapters for each network architecture above.

6.1 Who is Responsible for What Part of the Network

	1. Standalone	2. Shared RAN	3. Shared RAN and CP	4. Network Slice
Radio Access Network	**Enterprise is responsible**	**Shared with Operator**	**Shared with Operator**	**Shared with Operator**
5G Core: Control Plane Functions	**Enterprise is responsible**	**Enterprise is responsible**	**Shared with Operator**	**Via Operator -slice**
User/Subscription database	**On enterprise's own servers**	**On enterprise's own servers**	**In Operator's Servers**	**In Operator's Servers**
Operational data	**On enterprise's own servers**	**On enterprise's own servers**	**On enterprise's own servers**	**Via Operator-slice**
5G Core: User Plane Functions	**Enterprise is responsible**	**Enterprise is responsible**	**Enterprise is responsible**	**Via Operator-slice**
(Cloud) Server	**Enterprise is responsible**	**Enterprise is responsible**	**Both enterprise and Operator are responsible**	**Operator is responsible**
Staff	**Enterprise is responsible**	**Both enterprise and Operator are responsible**	**Both enterprise and Operator are responsible**	**Both enterprise and Operator are responsible**

In summary:

- When compared to each other, the deployment options differ in terms of:
  - Dependency on service providers, which increase from option 1 to 4.
  - Responsibility for the operation of the system, which decrease from 1 to 4.
  - Necessity of a subscription to the operator, which is not necessary for 1 and 2 (unless public connectivity or roaming is wanted) but *is* necessary for options 3 and 4.

6.2 Network Attributes of the Architectures

For each of the architectures we assessed the strengths for each network attribute. Note that this also considers in part the costs of achieving this (e.g., service continuity in option 1, the standalone architecture, can become High, but that would be more expensive than for a service provider with multiple customers as in option 3 or 4, hence the assessment of medium/low).

Strong Points	**1. Standalone**	**2. Shared RAN**	**3. Shared RAN and CP**	**4. Network Slice**
Connectivity	**Medium**	**Medium**	**High**	**High**
Service continuity	**Low**	**Low**	**High**	**High**
Low latency	**High**	**High** / **Medium**	**High** / **Medium**	**High** / **Medium** / **Low**
Throughput	**High**	**High** / **Medium**	**High** / **Medium**	**High** / **Medium** / **Low**
Availability	**High**	**High** / **Medium**	**High** / **Medium**	**High** / **Medium** / **Low**
Monitoring	**High** / **Medium**	**High** / **Medium**	**High** / **Medium**	**High** / **Medium**
Privacy	**High**	**High**	**Medium**	**Medium**
Security	**High**	**High**	**High** / **Medium**	**High** / **Medium** / **Low**
Customizability	**High**	**High** / **Medium**	**High** / **Medium**	**High**
Cost	**1. Standalone**	**2. Shared RAN**	**3. Shared RAN and CP**	**4. Network Slice**
CapEx	**High** / **Medium**	**Medium** / **Low**	**Medium** / **Low**	**Low**
OpEx	**High** / **Medium**	**Medium** / **Low**	**Medium** / **Low**	**Medium** / **Low**

In summary:

- When compared to each other, the deployment options differ in terms of:
  - **Latency, throughput, capacity, and guaranteeing Quality of Service** (QoS), which get increasingly dependent/*potentially* affected from 1 to 4. **Customizability, privacy, and security**, which all decrease from 1 to 4.

- **Subscription and roaming**, where you do not necessarily need a subscription to the public network in options 1-2 (unless you want roaming) but do need one for 3-4.
- **Capital Expenses** (CapEx), which decrease from 1 to 4, and **Operational Expenses** (OpEx), which increase from 1 to 4 (though possibly not proportionally).

7 Additional Considerations When Choosing an Architecture

There are other considerations and integrations that an enterprise might want to investigate depending on their use case or requirements.

Time-Sensitive Networking: TSN is a network layer to synchronize time-sensitive processes. 5G-TSN is the layer specifically designed for use within 5G networks. Use cases for TSN are for example manufacturing to coordinate manufacturing communication but could also be used in other key processes like self-driving cars, video streaming, medical and chemical processes, and security.

Roaming: roaming guarantees service outside of enterprise premises. When using private networks, supplying a roaming solution requires public network subscriptions and agreements. These are included in options 3-4 by virtue of their integration of the control plane in the public network but are optional in 1-2. If roaming is wanted in these deployment options, these will have to be integrated in addition.

Onboarding: when a device new to a network needs to be authenticated and authorized via another network or AAA-server. See the next chapter for a dedicated discussion on onboarding.

CAGs: *Closed Access Groups* can be defined to restrict the usage of your premises' radio cells to only authorized devices. As standalone public networks have a private radio base station, CAGs will only have to be defined and used if wanted in deployment options 2-4, as the radio cells there are also accessible to the public due to them belonging to public service providers. These will have to be defined (and paid for) through SLAs with the operators.

Firewalled public internetwork connectivity: to connect to external and public networks, a firewalled connection is necessary, which are not by default included in 5G private networks. Because deployment option 4 is fully integrated with a public network, internet connectivity is implicit in this deployment option. In options 1-3, this connectivity is optional, and will have to be explicitly arranged to guarantee access to the internet or other public network services.

In summary:

- There are additional considerations and integrations that an enterprise might investigate:
    - **Time-Sensitive Networking Layer**: to synchronize time-sensitive processes.
    - **Roaming**: to guarantee service outside of enterprise premises needs public network subscriptions and agreements, which are included in options 3-4, but optional in 1-2.
    - **CAGs**: *Closed Access Groups* can allow the private network to restrict usage of the network's (public) radio cells to *only* authorized devices in deployment options 2-4.

  - **Firewalled public network connectivity**: to connect to external public networks, a firewalled connection is necessary, which is included in option 4, but optional in 1-3.

8 Providing connectivity between (Standalone) Non-Public Networks

There are three ways to provide connectivity to UEs and an SNPN via other networks, for example when the UE or network is not by default configured for the UE's AAA, or when the UE needs access to services in that SNPN via another network.

AAA by a Credentials Holder (CH): AAA by a Credentials Holder simply outsources the AAA process to an external Credentials Holder. This can be done in two ways. One option is to directly contact the AUSF and NSSAAF on another network and ‘forward’ the results of those to the SNPN. Another is to authenticate and authorize the UE via a CH's AAA Server. These options can be pre-configured in the UDM in the SNPN, based on the setup and SLA between Credentials Holder and the SNPN.

Onboarding: onboarding is the process where a device new to a network has the credentials *loaded* through another network. Like in AAA by CH, this can also be done in two ways, namely via an external network’s AUSF, or an external AAA-server. This is configured (and initiated) by the UE.

Note how these last two options are different: AAA by Credentials Holder is a process where the network *outsources* the authentication and authorization to another network. Onboarding is a process where the UE asks another network to load a new SNPN's credentials onto the UE, so the UE can now be directly authenticated and authorized on the new SNPN (which happens only once per onboarded network in onboarding). This can be done through another standalone network (for example the factory or enterprise headquarters location where a product is assembled or shipped from, where the product UE will be setup for deployment in another network), or via temporary roaming on a public network (where the UE will temporarily ‘roam’ in order to access the credentials to the non-public network it will operate in).

Access to an SNPN via a PLMN (and vice versa): if a UE has a subscription/credentials to both networks, it can get access to operator services *via* an SNPN, or access t o SNPN services *via* a PLMN using IPsec tunnels. This is initiated by the UE via the SNPN or PLMN's User Plane.

In summary:

- There are three ways to provide connectivity *between* SNPNs and other networks, namely:
    - **AAA by Credentials Holder**: outsources the AAA process to an external network.
    - **Onboarding**: loads the credentials for a new SNPN onto a UE via another network.
    - **IPsec Tunneling**: to get access to a SNPN via a PLMN, or to a PLMN via a SNPN.

9 Enterprise Types and Requirements

In the above comparisons, several key attributes, considerations, trade-offs, and additional integrations have been discussed. These are aspects which can determine which deployment option fits an enterprise best. In this chapter, these aspects are briefly listed, as well as which aspects are broadly more or less important for distinct types of enterprises.

Requirements for distinct types of enterprises can be broadly defined into 4 types (Private Campus Networks | Arthur D. Little (adlittle.com)):

Industrial network: in this enterprise network type, machines are the primary user of the network, through IoT devices, and B2B2X solution devices. Indoor and on-premises outdoor coverage is required, for the purpose of monitoring and control functionality and secure, reliable connectivity. As such, high throughput, low latency, high security, and high availability are the key requirements for this campus type. Additionally, capacity and time-sensitivity may be additional considerations. Examples of this type of campus are automated factories, warehouses or refineries, in which various kinds of production line machines, sensors, automated vehicles and drones are communicating with each other or a central processor for coordination.

Office network: in this enterprise network type, employees are the primary users of the network, through IoT devices and phones or computers. Indoor coverage is required, for the purpose of providing information and entertainment, monitoring and control functionality, and secure connectivity. As such, throughput and availability are the key requirements for this campus type. Additionally, public connectivity, and public subscriptions may be required outside of the premises as well, and connectivity for visitors. An example of this campus type is an office, in which employees and visitors (perhaps through different slices) are communicating with each other and are browsing the internet.

Visitor network: in this enterprise network type, visitors are the primary users of the network, through wearables and phones or computers, as well as monitoring IoT devices on the venue itself. Indoor and (possibly) outdoor on-premises coverage is required, for the purpose of providing information and entertainment, and monitoring and control functionality. For this reason, throughput, latency, and availability are the key requirements. Examples of this network type are a shopping mall, or a sports stadium which would want to provide connectivity during events with large amounts of visitors.

Mobile or distributed network: in this enterprise network type, mobile or distributed UEs, for example IoT devices, vehicles, and phones or computers, are the primary users of the network. On-premises outdoor and off-premises coverage is required, for the purpose of monitoring and controlling functionality and secure connectivity. For this reason, security and availability are key requirements for this campus type. Examples of this campus type are railways, automated vehicles and transport and logistics providers. It is likely that this campus type would require the use of public 5G architectures, possibly through a private slice, as it requires a very broad coverage.

Some (non-exhaustive) general key requirements and considerations for enterprise 5G, then, are:

Latency: guaranteeing low delay between sending and receiving messages. Potentially important for industrial and entertainment purposes.

Throughput: guaranteeing that a large amount of data can be sent or received. Potentially important for industrial and entertainment purposes.

Capacity: guaranteeing that many users can use the networks. Important for entertainment purposes, and crucial for industrial and business purposes, especially guaranteeing sufficient capacity in all conditions (e.g. when a traffic jam occurs nearby an enterprise, this may result in increased traffic within a public network. When using an NPI-NPN option, this may result in a lowered capacity that the enterprise can use. It is therefore important to set up private networks to guarantee this capacity so that business or industrial processes do not suffer (e.g. by SLA, slicing, CAGs or SNPN).

Privacy and Security: guaranteeing that network data is maintained such that it cannot be read or altered by those that are not authorized to do so. This may require considerations of how isolated the deployment must be and whether to use CAGs, whether to store subscription data in-enterprise vs. with the operator, and whether to let traffic on vs. off-premises through public network connectivity.

Connectivity: when additional connectivity is required (for example VOIP/IMS, or public network or internet connectivity), these will have to be integrated additionally. It is important to note that when public network services are needed, a subscription to the public network is also needed.

Availability: guaranteeing that network service is quickly and easily available for use by client devices. Potentially important for industrial, business, and venue purposes. This may require onboarding and AAA-by-CH considerations, where devices that enter the enterprise premises are automatically authenticated and authorized.

Coverage: to have adequate availability on the enterprise premises, site surveys may need to be done to determine signal quality, interference and dead zones. The enterprise may need *indoor* base stations in addition to outside base stations (or operator-managed base stations). To have availability *off*-premises (roaming), UEs need to have a subscription to an operator's public network. Both private and public network connectivity require network subscriptions/credentials via SIMs/e-SIMs.

CapEx/OpEx: in determining which deployment option to choose, budgetary considerations may also play a role. Some deployment options are more expensive than others to set up, whereas others may cost more in monthly operational fees. Analyses of the costs and trade-offs between the two could provide insight into which is more suited to the enterprise. When dealing with public networks, Service Level Agreements (SLAs) and Quality of Service (QoS) agreements should be made and agreed upon.

Time-sensitivity: when operational processes are time-sensitive, a Time Sensitive Networking layer can be additionally integrated on top of the 5G system. This is an additional feature that will have to be planned for, set up and maintained.

In summary:

1. There are broadly 4 campus types for 5G with different requirements:
    - Industrial: throughput, latency, security, availability; indoor, on-premises coverage.
    - Office: throughput, security; indoor coverage.
    - Venue: throughput, latency, availability; indoor, off-premises coverage.
    - Distributed/non-stationary: security, availability; on- and off-premises coverage.
2. When considering setting up 5G, determine specific requirements and trade-offs regarding:
    - Latency, throughput, capacity (on vs. off-premises data traffic, edge computing).
    - Privacy, security, customizability, CapEx, OpEx (SNPN vs. PNI-NPN, CAGs).
    - Coverage: site surveys (to determine signal strength, propagation, and interference).
    - How to handle private/public credentials and subscriptions (SIMs/e-SIMs).
    - Determine if traffic stays on-premises or needs public network access? (VOIP/IMS/IP).
    - Determine if/how to onboard devices (AAA through other networks).
    - Determine if time-sensitive network synchronization is needed (TSN integration).
    - Subscriptions, SLAs and QoS agreements when dealing with operator-networks.

10 Overall Take-Aways

5G is the fifth-generation wireless technology designed from the ground up for high performance. The benefits to using 5G are its greater capacity in handling simultaneous users and data, speed, and reliability for critical applications and quality of experience.

To use 5G you need compatible User Equipment (UE) with a subscription to the network, a 5G-Core Network hosted on a (cloud) server, and a Radio Access Network (RAN) and spectrum usage plans. The Core network is made up of Network Functions, which can be separated into the Control Plane (CP, for network-internal tasks) and User Plane (UP, for transmitting user data). The RAN is made up of gNodeB radio stations (gNb), and a Core is often deployed on Virtual Machines on (cloud) servers.

Due to its modular design, virtualized network functions, and high standards of performance, 5G is suited and adaptable to many different industries, requirements and use cases, and makes it possible to create deployment options which do not require a full network installation. These 4 options are:

1. **Standalone**: fully independent private network managed by the enterprise. These may be built and maintained by third parties, but the usage will be private to the enterprise.
2. **RAN-Shared**: independent Core but sharing the Radio network with a service provider.
3. **RAN and CP-shared**: independent User Plane so enterprise data traffic stays private within the enterprise but sharing the Radio network and Control Plane with a service provider.
4. **Slicing**: fully dependent on a public network, in which both Core and RAN are shared, and a *virtually* independent ‘slice’ is defined for private and secure use by the enterprise.

When compared to each other, the deployment options differ in terms of:

- Dependency on operators, which increase from option 1 to 4.
- Latency, throughput, capacity, and independence in guaranteeing Quality of Service (QoS). Where these get increasingly dependent and impacted by operator’s services from 1 to 4.
- Capital Expenses (CapEx) and Operational Expenses (OpEx). Where the CapEx decreases from 1 to 4, the OpEx increases, though not necessarily proportionally or in-line.
- Customizability, privacy, and security by physical isolation. Where all decrease from 1 to 4.
- Subscription and roaming. Where you do not necessarily need a subscription to the public network in the 1-2 options (unless you want roaming capability), you do need one for 3-4.

Additional integrations that 5G networks can work with are:

- **Time Sensitive Networking**: a network layer to synchronize time-sensitive processes.

- **Firewalled public connectivity**: firewalled connections to public networks and the internet.
- **CAGs**: a method to restrict access to radio cells to only authorized devices in options 2-4.
- **Roaming and Onboarding**: to guarantee service outside and between private network sites.

Campus types that 5G can be used for are: Industrial, Office, Venue and Non-Stationary/Distributed. These have different typical requirements in their operation and can be used to determine what requirements and trade-offs are to be considered for your enterprise use case. Specifically, think about the requirements and trade-offs with regards to latency, throughput, capacity, privacy, security, customizability, CapEx, and OpEx. Site surveys for coverage may need to be done. Private/public credentials and subscriptions through SIMs/e-SIMs must be handled as well as SLAs and QoS agreements when dealing with operator-networks. Additional integrations may need to be determined and taken care of, such as public (internet) connectivity, onboarding and roaming capability, and a time-sensitive network synchronization layer.

11 Sources for further reading

5G Non-Public Networks for Industrial Scenarios (5G-ACIA)
Private Networks & 5G NonPublic Networks (NPNs) (3G4GUK)
First Report on 5G Network Architecture Options and Assessments (5GSMART)
Second Report on 5G Network Architecture Options and Assessments (5GSMART)
5G industry campus network deployment guideline V. 1.0 (GSMA)
Architecture Integration of 5G Networks and Time-Sensitive Networking with Edge Computing for Smart Manufacturing (Electronics, 2021)
5G Non-Public Networks: Standardization, Architectures and Challenges (IEEE, 2021)
3GPP Specification 23.501: System architecture for the 5G System (5GS)
3GPP Specification 23.502: Procedures for the 5G System (5GS)
Private Campus Networks (Arthur D. Little)
Non Public Networks | Private Mobile Networks - GSA (gsacom.com)
InDesign-5G-Technologies-for-Private-Networks-WP.pdf (5gamericas.org)

12 Signature

Amsterdam, 7 febr. 2023

TNO

ValidSigned by Annemieke Kips
on 2023-02-16 10:10:49

Tim Bergman

A.J.R.(Annemieke) Kips
Head of department

W.A.L. (Tim) Bergman
Author