5G Mobile Network Sharing Security

—

v1.02

www.ngmn.org

WE MAKE BETTER CONNECTIONS

5G MOBILE NETWORK SHARING SECURITY

by NGMN Alliance

Version:	1.02
Date:	26.10.2022
Document Type:	Final Deliverable (approved)
Confidentiality Class:	P - Public
Authorised Recipients: (for CR documents only)	

Project:	Security Competence Team
Editor / Submitter:	**Stan Wong (Hong Kong Telecom)**
Contributors:	**Stan Wong (Hong Kong Telecom), Minpeng Qi (China Mobile), Xiaoting Huang (China Mobile), Sheeba Mary (Lenovo), Andreas Kunz (Lenovo), Ivy Guo (Apple)**
Approved by / Date:	**<NGMN Body/Date>**

NGMN Alliance e. V.
Großer Hasenpfad 30 • 60598 Frankfurt • Germany
Phone +49 69/9 07 49 98-0 • Email office@ngmn.org

Abstract

Mobile network infrastructure sharing is known as the sharing of physical or logical network resources. Mobile network sharing could occur on different levels and with various sharing options in the mobile network infrastructure. Usually, these various sharing options require a thorough consideration of levels of protection. However, these levels of protection and security measures might affect the decision of selecting the types of sharing options. Even though mobile network operators (MNOs) put a vast amount of defense effort to protect each of the sharing options, the vertical industry is facing a great challenge on selecting the suitable sharing option for their service and the adequate security for the particular mobile network infrastructure sharing option. Hence, this White Paper provides a reference for MNOs and vertical industries to identify the adequate security on each mobile network infrastructure sharing option.

Contents

1 INTRODUCTION

Mobile network infrastructure sharing has grown in demand for various services and business needs [1]. The increase in popularity of mobile network infrastructure as a service (MNIaaS) and the rise of flexibility of network infrastructure initiate a great opportunity to reduce the capital expenditures (CAPEX) and operational expenditures (OPEX). However, generally, infrastructure sharing always introduces an extra risk and vulnerability to the customers. Basically, it increases the probability of malware infection, exposes the attack surface to become wider, and extends the possibility of the loss or exposure of sensitive information. Without proper security measures in place, mobile network operators (MNOs) and vertical industries may possibly expose their sensitive data to the new security threats and ultimately would not benefit from the mobile network infrastructure sharing.

Therefore, a proper security measure guideline of mobile network infrastructure sharing could assist MNOs and vertical industries to capitalise the infrastructure sharing, and put defense mechanisms or methodologies in place. In fact, different types of sharing options might have different security measures. The deployment of security measures could affect the terms of commercial values and the decision of selecting the types of sharing options. Also, the security measures might require a thorough consideration of defense methods and can be divided into different level of protections. Even though MNOs put a vast amount of defense effort to protect the mobile network infrastructure, the vertical industry is facing a great challenge on selecting the suitable sharing option for their services and the adequate security for the particular mobile network infrastructure sharing option. Nevertheless, the runtime security issues and new security threats could affect the service availability. Hence, the shared infrastructure protection or defense can be differentiated from prior and post deployment protection approaches. In general, the prior deployment protection approaches are based on the standardisation specifications and the MNO's network infrastructure policies. Post deployment protection approaches would usually rely on the Security Operation Centre (SOC) Security Information and Event Management (SIEM) team.

This White Paper provides a reference for MNOs and vertical industries to identify the adequate security measures on each mobile network infrastructure sharing option. Figure 1 indicates eight different types of current deployable mobile network infrastructure sharing options. Each type of mobile network sharing option should have a specific protection requirement and

security importance. Moreover, MNOs and vertical industries (tenants) could also use this White Paper as guidance to protect their customers as well.

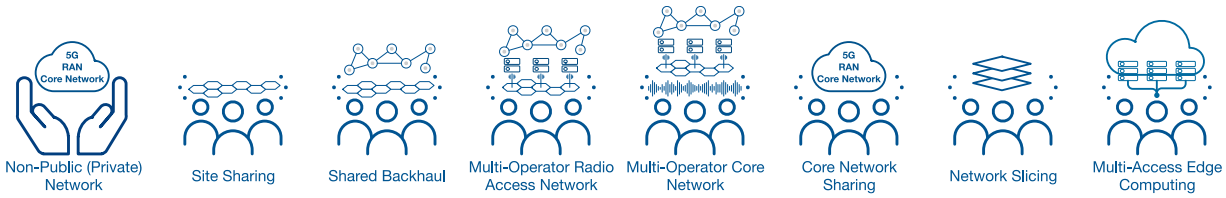

Figure 1: The Main Types of Mobile Network Sharing

1.1 Scope of the White Paper

This is a White Paper to define the mobile network sharing level of trust and to identify the suitable methodology to measure the level of network sharing security in the upcoming generation of networks. Particularly, this White Paper provides a security guideline for MNOs and vertical industries to secure their network sharing services.

2 MOBILE NETWORK SHARING DEPLOYMENT QUALITATIVE ANALYSIS

Traditionally, mobile network sharing can be seen as physical network element sharing and logical network partition. It is straight forward to identify the granularity of sharing resources and recognise the right network sharing option to the customers [2]. However, in the modern telecommunication system, mobile network sharing is more complex than the traditional one. It can involve spectrum sharing, physical network element sharing, computation resources sharing, storage sharing, logical network segment sharing, virtualised network function sharing and domain services sharing etc. These sharing options and mechanisms provide customers with flexibility and options to choose the suitable network sharing options for their services. But, with these flexibilities, different combinations of sharing and deployment methods often induce or introduce the security risks to the customer's services. Therefore, customers always wish to find out the level of security and seek the adequate defense on each of the mobile network sharing options. In this section, we establish a qualitative approach to analyse the mobile network sharing security, which does not only provide support to the customers' decision-making process, but also assist MNOs to identify the level of importance of defense from the customers' viewpoint. On one hand, this qualitative approach demystifies the complexity of mobile network sharing deployment options and security concerns from MNOs and their customers. On the other hand, it also assists MNOs and their customers in the thorough understanding of the service architecture planning of mobile network sharing.

In the following sections, we introduce eight main security concerns from the aspects of mobile network sharing providers and customers: deployment environment, data and traffic management, passive network component sharing, active network component sharing, network service purpose, level of assurance requirements, certification and local regulatory requirements, and subscriber management. These eight main security concerns could also narrow down the risks of mobile network sharing, simplify the deployment processes, speed up the sharing network architecture design process and identify the network security perimeter during the design stage. This approach carries out a qualitative analysis of obtaining and identifying the key parameter measurements. Figure 2 illustrates these eight main security concerns on a radar graph which provides a multivariate view on each of the aspects and can be used to distinguish the level of security in each of the network sharing options.

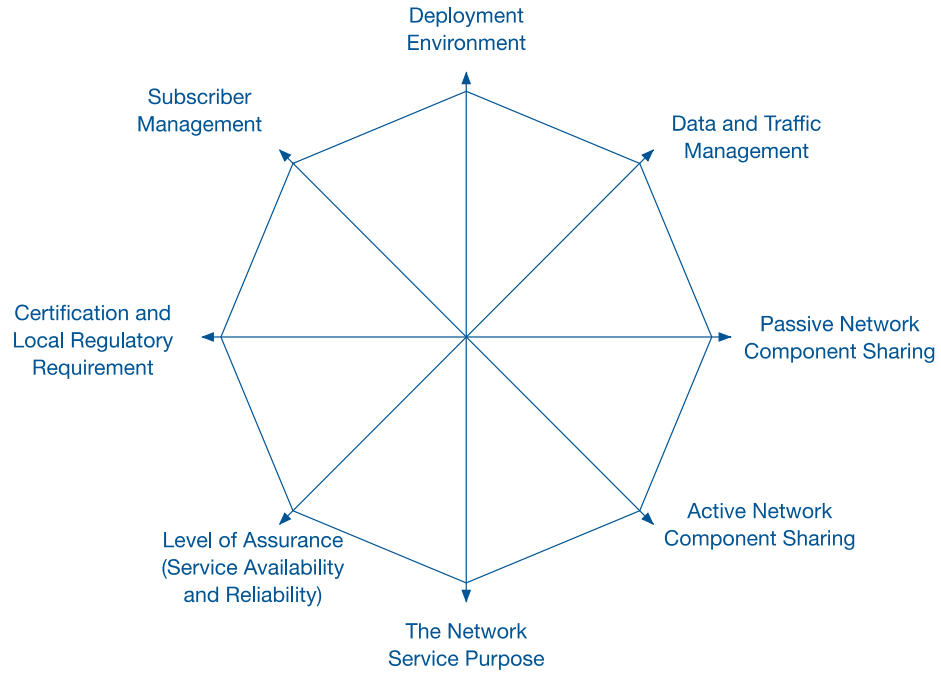

Figure 2: Mobile Network Sharing Trust Measurement Scheme

2.1 Deployment Environment

Deployment environment is the most important defense measure for deploying a mobile sharing network, which helps the MNO to identify the level of isolation and resources sharing in the network deployment architecture, to establish the network defense perimeters and to choose the appropriate defense mechanisms in each network perimeter. Moreover, this isolation level could be distinguished in three levels: a complete-isolated network environment, a semi-isolated network environment and a sharing network environment.

A complete-isolated network environment is the most secure method and is also called 'air-gap' isolation. It does not require to consider shared resources with the other networks in the network infrastructure. Therefore, the attack surface would be limited within an independent network environment. Usually, an insider attack would be mainly considered for a complete-isolated network. Also, this critical network infrastructure might operate on a privately-owned spectrum and might not have Internet access as well. For example, a government agency requires the most secured level of network sharing due to a number of national security reasons. Therefore, the network would be deployed as a complete-isolated network and might operate on a private spectrum, base stations, access network, core network and datacentres. Basically, it is an independent network, with a narrow attack surface and limited network

security perimeters to be identified, which is a highly defendable and most secured deployment environment compared to the other deployment environments.

A semi-isolated network environment is less secured than a complete-isolated network environment. It also has a slightly wider attack surface and number of network perimeters at the typical locations and resource sharing points. For example, a critical infrastructure vertical industry customer without a private spectrum would request the spectrum sharing. MNOs need to consider the spectrum capacity and the service availability. Then the MNO might also need an extra consideration on the physical security, and other vulnerabilities at the cell sites. Particularly, the consequence of man-in-the-middle attacks would cause service interruptions or services unavailability.

Lastly, a sharing network environment shares all resources with the other customers. It has the widest attack surface and a vast number of network perimeters to be protected, which is far more complex than the previous deployment environments. For example, a vertical industry customer requires a 5G network sharing for their plethoric services in which the cost effectiveness is the main deployment consideration while the other elements might not be the concern of the customer. Therefore, the MNO needs to put multiple levels of protections to such a network sharing environment to protect the overall network infrastructure.

2.2 Data and Traffic Management

Data and Traffic Management defense measure is to handle data under the network sharing. It helps MNOs to implement the data protection policies and assists customers for identifying the right data protection for their services when data is at-Rest, in-Motion, in-Use and in-Change. Moreover, those data protection policies and security methodologies could be independently applied to the shared network. The level of defense measure is an aggregation of these data protection methods.

Data-at-Rest protection aims to secure all the inactive data stored on any devices or network functions, and to prevent an individual with potentially malicious intentions to access the data. Typically, security methods would cover data confidentiality, data integrity and data availability.

Data-in-Motion (Data-in-Transit) protection aims to secure active data travelling from one device to another, or from a network function to another. Typically, security methods would

cover data confidentiality, data integrity and data reliability, e.g., transport layer security association and digital signature.

Data-in-Use is the data accessed by a device or network functions for temporary use and might only be needed for a finite duration in time. Data-in-use protection aims to secure data when accessed for temporary use. Typically, security methods would cover data confidentiality, data integrity and data availability. A multi-level of access control with data clearance should be formulated for accessing the data.

Data-in-change is the data that is being created, updated, deleted and modified at the end-points. Data-in-change protection aims to secure the original version of data under the sharing network. Typically, security methods would cover data confidentiality and access authorisation. For example, an identity access management could provide an authorisation or delegation to the data changing permissions.

2.3 Passive Network Component Sharing

Passive Network Component Sharing defense measure is to passively identify the type of network components, that MNOs or customers would share or not share with others. Passive network components as an essential part in a network, are involved in data transmissions, and are often referred to the key assets stack in the mobile network infrastructure. Therefore, identifying and protecting those key assets from the network infrastructure is a vital process to prevent various attacks. The level of defense measure would be based on where the shared or dedicated component locates in the 3GPP trust model. Moreover, the trust measurement would only require identifying the shared components, e.g., cables, network racks and optical fibres.

2.4 Active Network Component Sharing

Active Network Component Sharing defense measure is to actively identify the type of network components, that MNOs or customers would share or not share with others. Active network components are also an essential part in a network and usually require configuring to become active (network elements or network functions) in the network. Therefore, identifying and protecting these assets from the network infrastructure is also a vital process to prevent any particular type of attacks. The level of defense measure would be based on where the shared or dedicated component locates in the 3GPP trust model and service-based architecture.

Moreover, the trust measurement would only require identifying the shared components or network functions, e.g., switches, repeaters, hubs, bridges, routers, base stations.

2.5 Network Service Purpose

The Network Service Purpose defense measure is to protect the service availability and quality of service (QoS). This index could help MNOs and customers to identify the type of network service and apply security control to protect the service availability. Different types of networks would carry a specific QoS for their services to prevent the service interruption. Security control in a right place is critical. The level of defense measure can be defined as the criticality of the purpose of the network services. Obviously, mission critical communication network service requires a high level of service availability and QoS. On the other hand, non-mission critical communication network service would have a lower QoS comparing with the mission critical communication network service.

2.6 Level of Assurance

Telecommunication system assurance can be conveyed to a defense measure for protecting the level of network assurance by applying or compiling the assurance frameworks on testing the network products i.e., network elements and network functions. These assurance frameworks include 3GPP Security Assurance Methodology (SECAM) and Security Assurance Specifications (SCAS) [3], GSMA Network Equipment Security Assurance Scheme (NESAS) [4] and ISO/IEC TR 15443-1:2012 [5] information technology-security assurance framework etc. 3GPP SECAM and SCAS give the foundation of network sharing defense measure on various network elements and functions. GSMA NESAS provides a security assessment to network elements or network functions to ensure the level of confidence of the products. ISO/IEC TR 15443 provides IT level of guidance to achieve confidence of control in the operating network. Therefore, this defense measure can be used to obtain the confidence level of quality of assurance. The trust measurement could be based on the number of frameworks that an MNO applies to the network sharing services, and the number of security assurance and security control items achieved under each of the frameworks.

2.7 Certification and Local Regulatory Requirement

International certifications offer confidence of MNOs' competence to potential customers. Particularly, those certifications provide a level of compliance and assurance to the operational processes and control management scopes on managing, tackling, organising, and resolving

issues. Therefore, having a list of certifications would give customers a level of confidence according to the weight of certifications e.g., ISO/IEC 27001, 27701, 27018, 15433 and other certifications. Certifications often assist MNOs and customers to quantify the risk and reduce human errors for configuring and operating the shared network functions and the overall sharing network. Basically, certifications ensure the service availability and service reliability of the sharing network. The MNO or service provider might acquire various certifications to ensure the control processes and the confidence of service assurance in place in operation, provisioning and during the deployment. However, the usefulness of certifications can always be referred to the local community and regulatory practice. Moreover, having and following different certifications to comply with the requirements of managing and operating the sharing network, could assist a defense measure with confidence. However, not all certifications are suitable across the continents, with various local regulations and vertical industry needs. Therefore, local regulations might have an important role in such a measurement that aggregates certifications with local regulatory recommendations.

2.8 Subscriber Management

Subscriber Management is a defense measure for managing the subscriber privacy. Nowadays, all kinds of systems are required to fulfil and comply with data privacy frameworks such as the EU General Data Protection Regulation (GDPR) [6]. Basically, subscriber management would need to handle the subscription and billing data within the MNO's mobile network infrastructure or in the customer network infrastructure. Therefore, the appropriate data protection with data classification, anonymisation and pseudonymization should be applied at the subscription and billing repositories, the key management server and customer relationship management platform. In addition, sometimes collecting or accessing logs of network elements or functions in different network domains might be required for troubleshooting or other service adjustment purpose. Hence, the level of defense measure can be defined from the subscription management that takes place. All data is processed either within the MNO's mobile network infrastructure, or partially within the MNO's mobile infrastructure, or routed outside the MNO's mobile network infrastructure. Another aspect that Subscriber Management considers is the credential management that used to authenticate the subscriber. Basically, MNOs use the SIM-based authentication mechanisms which has been proved to be at high security level. Compared with the IT mechanisms like username/password and certificates which highly rely on the provisioning of the credentials, SIM-based subscriber management is not easy to replicate or be stolen.

3 5G NETWORK SHARING DEPLOYMENT OPTIONS

The 5G telecommunication system generates a vast number of opportunities to enable different types of new services, and enriches various network sharing approaches. These network sharing approaches aim to capitalise and utilise the MNO's mobile network infrastructure. Ultimately, MNOs would provide the network infrastructure on-demand and flexibly organise all recourses to increase the utilisation of the network infrastructure.

This chapter explores different types of network sharing approaches under the MNO's mobile network infrastructure.

3.1 Non-Public Network (NPN)

Non-Public Network (NPN) sometimes also called private network [7] operates with high quality of service (QoS) under an isolated network environment. Usually, NPN exclusively offers mobile network services for a specific or dedicated set of subscribers or network elements belonging to an organisation (e.g., any production plant, campus) to enable private usages. Furthermore, NPN can be deployed either as a standalone network or as part of a public network, i.e., Public Network integrated NPN (PNI-NPN), which typically would have the air-gap protection. Figure 3 illustrates a complete-isolated NPN network which might require an inter-MNO service, and then it would connect to another MNO's network via firewall and IPX network. It also does not connect to the Internet. Therefore, the network components, elements, and resource sharing in the context of NPNs differs with the type of NPN deployment.

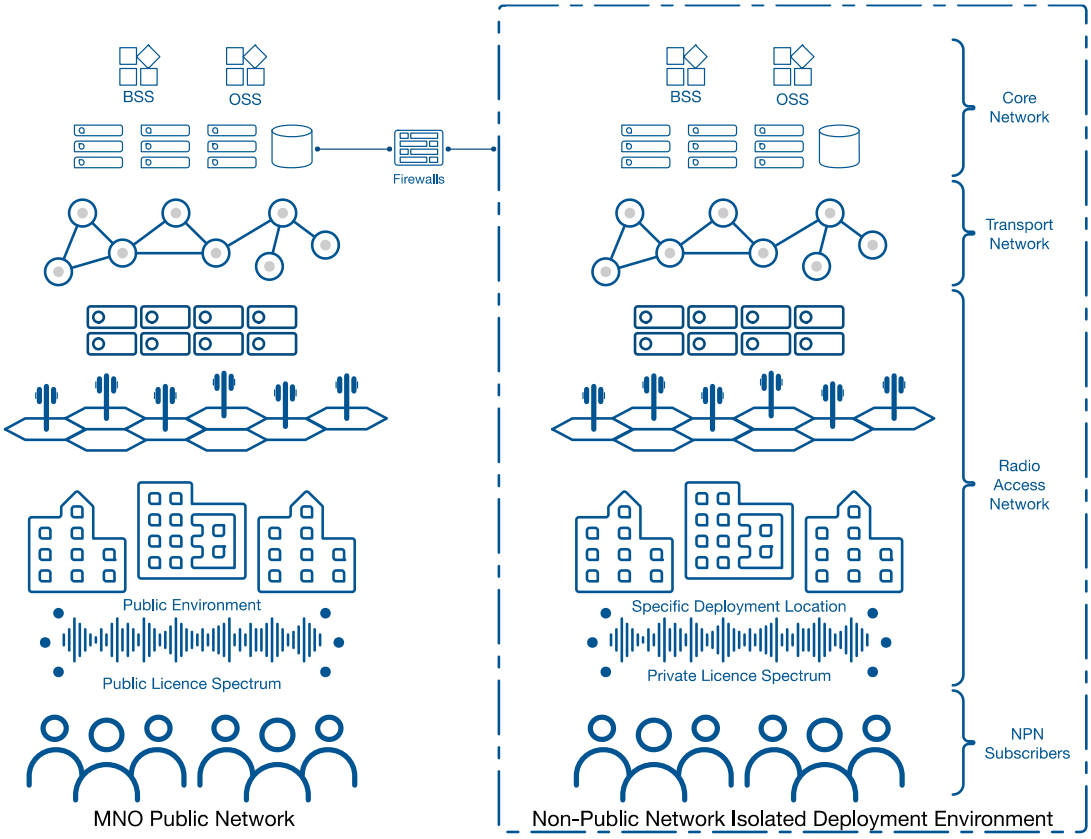

Figure 3: Non-Public Network in an Isolated Deployment Environment

There is a possibility that the NPN (vertical industry) and MNO would share the radio access network (RAN) or core network functions with other MNOs. The network components, elements, and resource sharing in PNI-NPN deployment can range widely such as the following [7]:

1) RAN sharing

   The NPN and Public Land Mobile Network (PLMN) share part of RAN, while other network functions remain segregated. The NPN traffic is handled within the logical perimeter of the defined organisational premises.

2) RAN and Control Plane sharing

   The NPN and PLMN share the RAN and network control operations which are always performed in the PLMN (i.e., implemented by means of network slicing to create logically independent networks within a shared physical infrastructure). The NPN traffic is handled within the logical perimeter of the defined organisational premises and the public network traffic alone is handled over the public network.

3) Public network hosted NPN

Both NPN traffic and public network traffic are external to the defined organisational premises but handled as if they were parts of completely different networks (i.e., implemented by means of network slicing or access point name (APN)).

3.2 Multi-Operator Radio Access Network (MORAN)

Multi-Operator Radio Access Network (MORAN) is a network sharing configuration which allows MNOs to share a RAN, while having their proprietary core networks. MNOs would use their own dedicated radio frequencies on the same RAN [14]. Basically, MORAN allows MNOs to control cell-level parameters and share the radio controller, backhaul, base station and cell site but not the spectrum. Ultimately, MNOs have independent cell coverages to serve their own subscribers. Figure 4 illustrates two MNOs share RAN and provide mobile services to subscribers using their own spectrums.

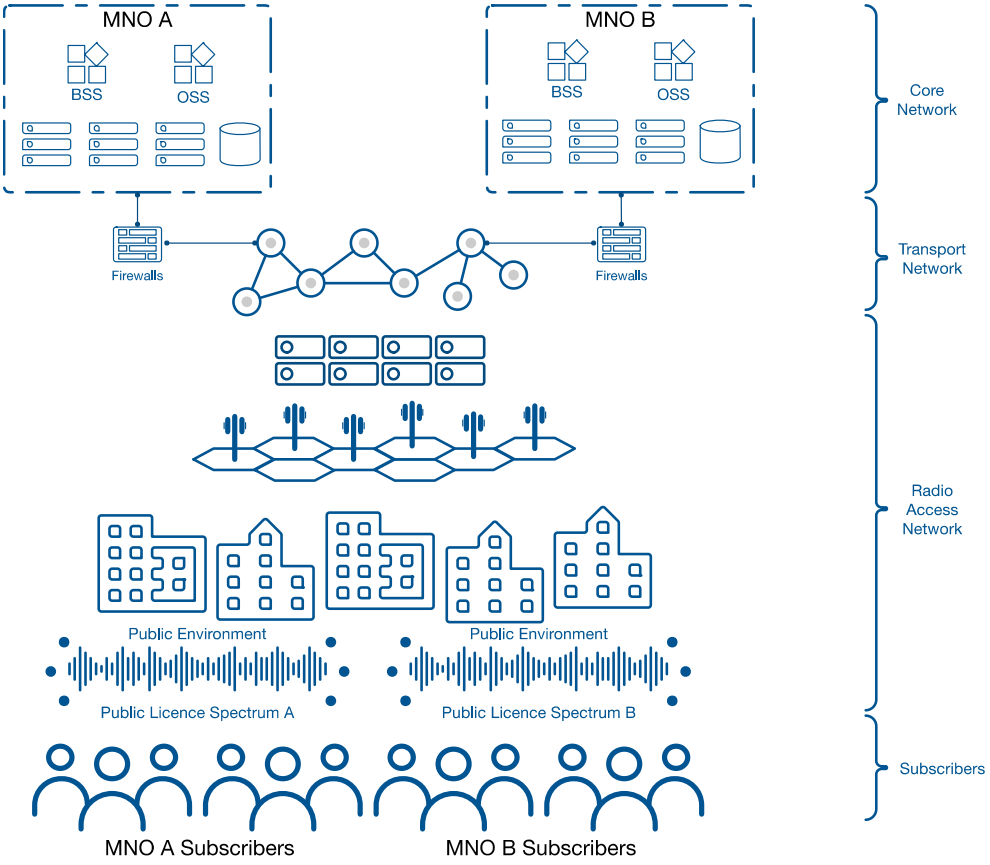

Figure 4: MORAN Illustration

3.3 Multi-Operator Core Network (MOCN)

Multi-Operator Core Network (MOCN) is a network sharing configuration which allows MNOs to share a RAN over the same radio frequencies, while having their proprietary core networks [15]. Basically, MOCN allows MNOs to share the radio controller, backhaul, base station, cell site and spectrum. Ultimately, MNOs would be under the same cell coverage. Figure 5 illustrates two MNOs share RAN and provide mobile services to subscribers using the same spectrum.

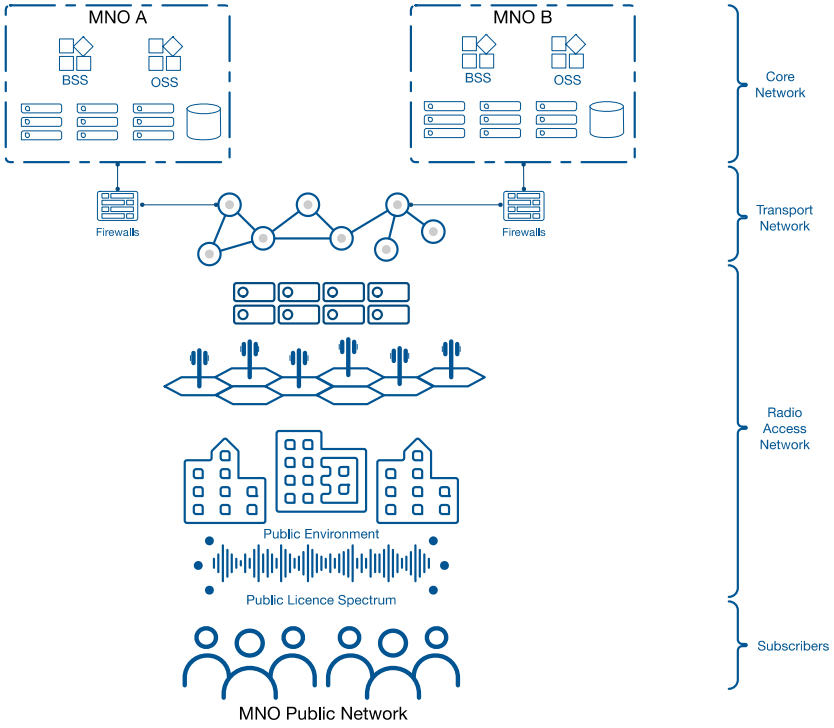

Figure 5: MOCN Illustration

3.4 Site Sharing

Site Sharing is an approach to share site facilities such as the power supply units, air-conditioning or masts within the site location. Within the site facilities, often, MNOs would have their own equipment and connect to their network infrastructure (Backhaul). However, MNOs might also share support and maintenance service providers on those sharing sites to reduce to the cost of operation. This form of sharing is often seen in urban areas due to the lack of available sites or complex planning restrictions. Figure 6 illustrates two MNOs share a site and provide mobile services to subscribers using their own spectrum.

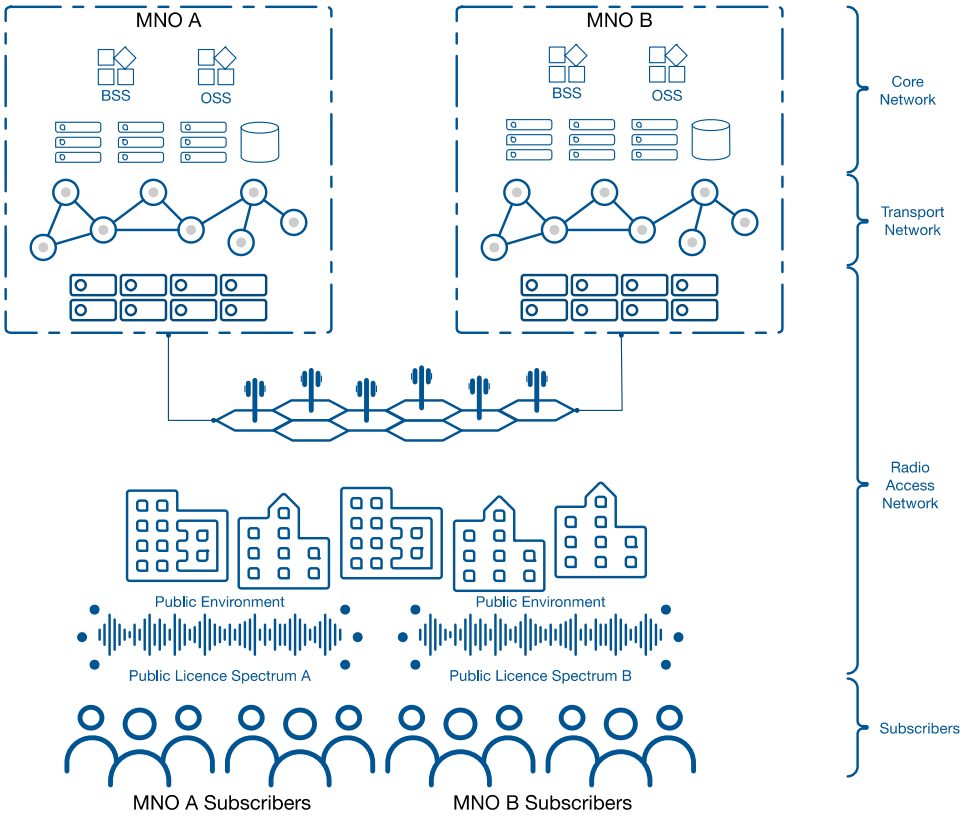

Figure 6: Multi-operator Site Sharing Illustration

3.5 Backhaul Sharing

Backhaul Sharing usually refers to the sharing of the transport network which is located in between core network and RAN. Backhaul network is an essential component of a mobile network infrastructure. Sharing backhaul would require the transport network has the capability to forward the control plane traffic to the appropriate core network and forward the data plane traffic to the appropriate network function or Internet gateway. Therefore, MNOs applying this form of infrastructure sharing might require having a network aggregation anchor points arrangement and a network capacity overloading preparation due to traffics on-demand. Figure 7 illustrates two MNOs share a backhaul network infrastructure and provide mobile services to subscribers using their cell sites, base stations and spectrum.

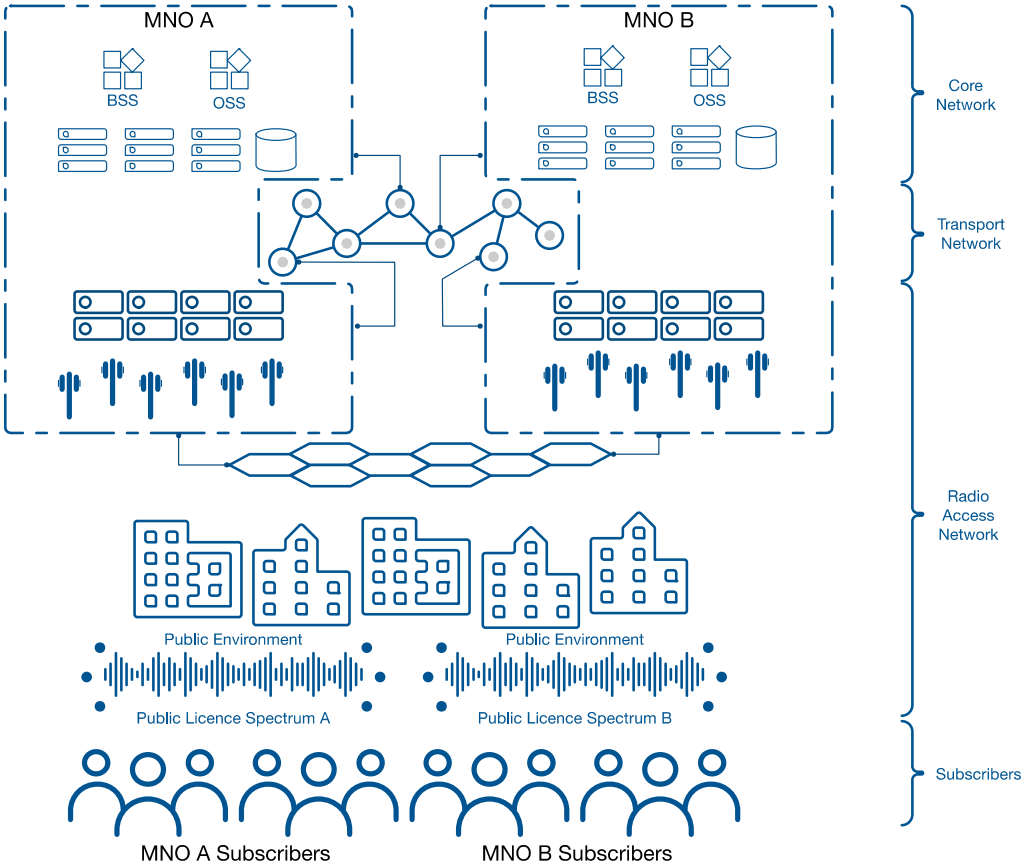

Figure 7: Multi-operator Backhaul Sharing Illustration

3.6 Core Network Sharing

Core Network Sharing often refers to the sharing of the transmission ring and core network functional entities. In this sharing form, MNOs share the core network functions for authentication, authorisation, accounting and other basic services. Particularly, the billing processes and subscription policy functionalities would be shared in between MNOs within the service-level-agreement (SLA). Moreover, MNOs essentially share the RAN and the spectrum illustrated in Figure 8.

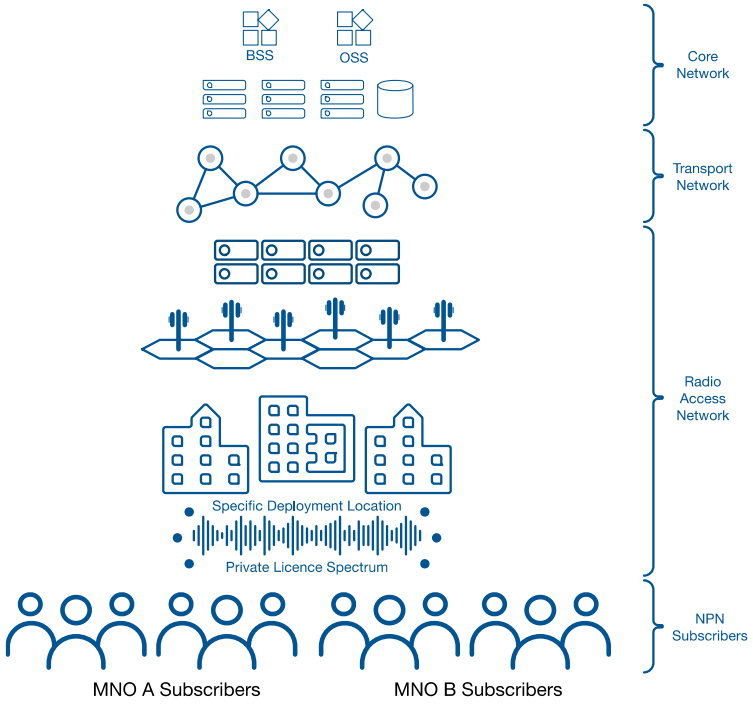

Figure 8: Multi-operator Core Network Sharing Illustration

3.7 Network Slicing

Network slicing is a logical network representation, composed with a specific mobile network infrastructure configuration, which is enabled by virtualisation, containerisation, software-defined network (SDN), virtual network function (VNF) service chain, network function virtualisation (NFV) and flexible transport network technologies [8]. Furthermore, basically, network slices share the physical network infrastructure. Each of the network slices would have its logical network resources over a shared physical infrastructure to offer tailor-made mobile network infrastructure services and is corresponding to a particular type of application. There are 8 types of network slices that have been proposed by GSMA [9]. These 8 types of network slices could be formulated or configurated by network slice generic templates [10]. MNOs could allocate a powerful bare metal server to all tenants, and all network slice VNFs could be collocated in the same bare metal. Also, function collocation logic or clustering VNFs could further organise the sharing of resources to tenants, when the customer SLA is being established or formulated. Figure 9 illustrates a logical representation of multiple network slices within an MNO's mobile network infrastructure.

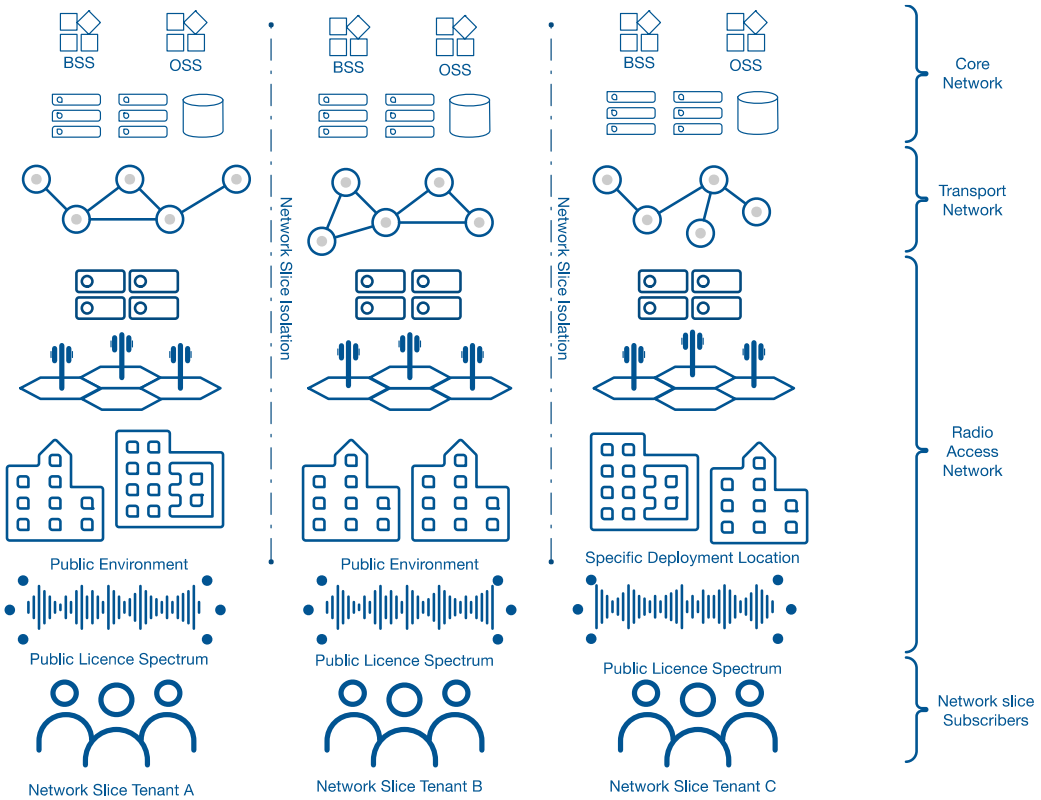

Figure 9: Multi-network Slice Illustration

3.8 Multi-access Edge Computing (MEC)

Multi-access Edge Computing (MEC) is a service demand-oriented methodology with an effective deployment close to the user, which aims to provide services with ultra-low latency and high bandwidth capabilities at the edge of the mobile network infrastructure. MEC has many different deployment scenarios that might target a specific location or target to a specific group of subscribers across the mobile network. These services share the physical network infrastructure. More specifically, these services usually share the transport network connection to the UPF and RAN. ETSI has proposed 4 MEC basic scenarios to be integrated with 3GPP 5G architecture [12], [14], [17]. On the other hand, 3GPP has also defined 3 server-side and 2 UE-side enabler functions to be integrated with MEC [13]. Those enabler functions on the server side are Edge Application Server (EAS), Edge Configuration Server (ECS) and Edge Enabler Server (EES), and on the UE side are the Application Client (AC) and the Edge Enabler Client (EEC). These network functions would be based on 3GPP service-based architecture using virtualisation or containerisation technologies as a foundation of deployment technology. Therefore, MNOs can fully utilise the resources and take advantage of the continuous integration (CI) and continuous delivery (CD) with DevOps methodology to enable an effective and efficient service deployment. Figure 10 illustrates multiple MEC services within an MNO's mobile network infrastructure.

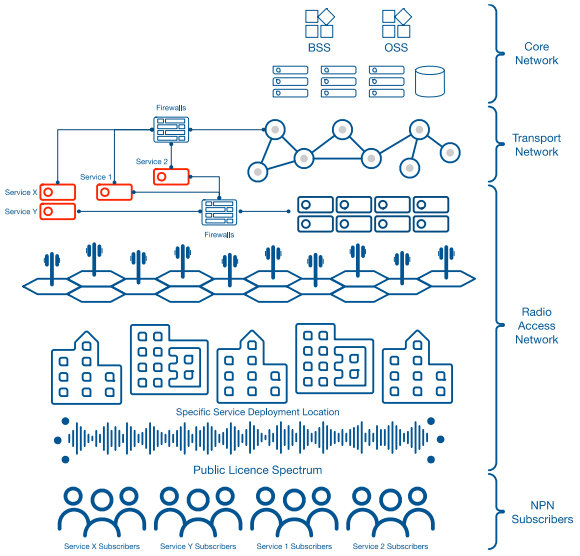

Figure 10: Multi-services MEC Platform Sharing Illustration

4 CHARACTERISTICS OF NETWORK SHARING SECURITY

Mobile network infrastructure sharing is one of the most important methods to maximise the utilisation of the mobile network in various levels. Once the network sharing option has been chosen by the MNO, based on the MNO technical competence or business needs, the network defense perimeters would be established by the design of the network infrastructure sharing approach. Each type of network sharing option would have different network attack surfaces, defense perimeters, defense mechanisms, and attack vectors.

Basically, mobile network infrastructure mainly requires protecting the subscriber privacy, the mobile network infrastructure service availability and the communication pipelines across the network infrastructure. A usual defense approach is to put a firewall at those identified network defense perimeters, to separate the Internet and the internal network or in between datacentres. However, mobile network sharing defense would be more complex than just applying a firewall to resolve all kinds of attacks. Furthermore, various attacks might depend on the type of services on the sharing network infrastructure and the level of QoS of the services. For example, the same type of mobile network infrastructure sharing might have roaming services, or might only serve the local subscribers. Some types of mobile network infrastructure sharing might use bare metal servers only or public cloud service infrastructure. Therefore, the same type of mobile network infrastructure sharing might have a variety of deployment approaches that could consequently have widened or narrowed the attack surfaces.

Hence, firstly, to assess the safety of sharing network infrastructure during the design of the architecture, we have to ensure to put the network security perimeters in place. Then, we need to identify the physical and logical sharing network components and the necessary defense principles of the sharing network architecture such as zero trust, defense in depth, zero knowledge, micro-segmentation, secure access service edge, network onion (zone) defense, which could be applied to the design of the mobile network sharing services defense according to the service characteristics.

In this White Paper, we provide a qualitative model (see Chapter 2) to measure the level of security in a usual or general deployment.

5 NETWORK SHARING LEVEL OF TRUST

This chapter applies the developed qualitative analysis model in Chapter 2 to all types of mobile network infrastructure sharing options identified in Chapter 3. Each type of mobile network infrastructure sharing would have an indication of level of trust in an area of the diagram. The larger indicated area means the type of mobile network infrastructure sharing has a better security protection.

5.1 NPN

As introduced in Section 3.1, NPN includes both SNPN and PNI-NPN, but we only analyse the level of trust for PNI-NPN as it shares network resources with PLMN, while SNPN does not. Thus SNPN is not in the scope of this document.

PNI-NPN is deployed under a semi-isolated environment and aims to share network components with MNO's PLMN. Figure 11 illustrates the level of trust of PNI-NPN.

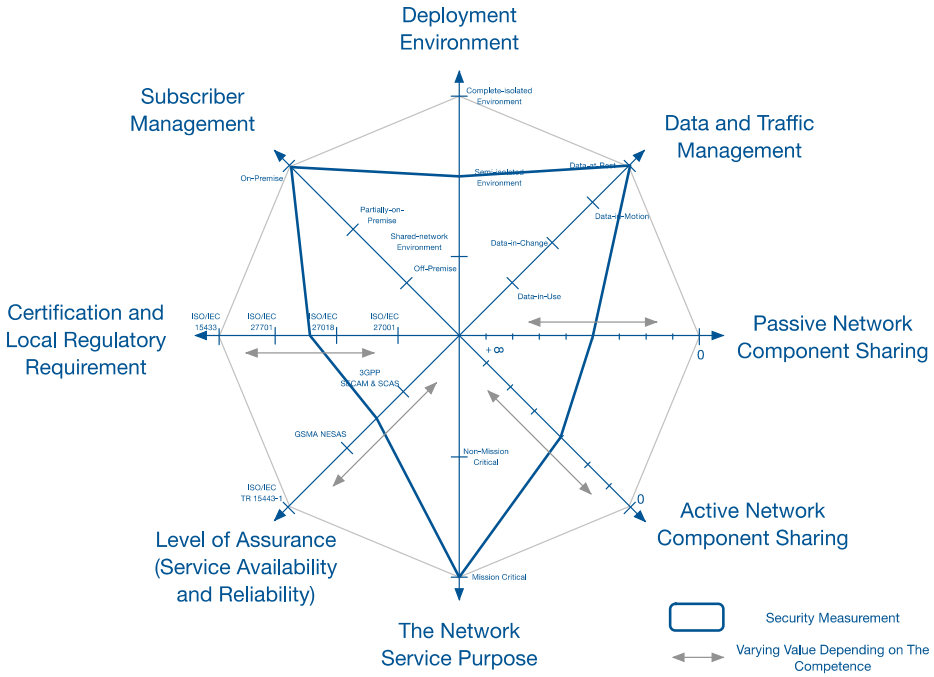

Figure 11: Level of Trust for PNI-NPN

- **Deployment Environment:** PNI-NPN shares resources with PLMN in terms of RAN only, RAN and control plane and the public network, etc., which poses vulnerabilities at the sharing points. For example, when the PNI-NPN shares RAN with the PLMN, the attacking

risks occurring at the air interface could cause threats to the PNI-NPN. Particularly, the consequence of man-in-the-middle attacks would cause service interruptions or affect service availability.

- **Data and Traffic Management:** Since PNI-NPN shares parts of network functions with the PLMN, the data-at-rest should be protected by both the PLMN and the NPN tenants, via protecting the infrastructure which stores the data, e.g., physical security, virtualised machine or container security. The data-in-motion could also be protected by the current security mechanisms specified in 3GPP, e.g., the confidentiality and integrity of the data transmitted in the air interface could be protected. The data-in-use and data-in-change are under access control with differentiated authorities to the NPN tenants and PLMN operators.
- **Passive Network Component Sharing:** The level of defense measure would be based on where the shared or dedicated components locate in the 3GPP trust model. Furthermore, the trust measurement would only require identifying the shared components, e.g., cables, network racks and optical fibres. Figure 11 indicates the trust measurement with mid value, however, in practice, the measurement would be based on the preliminary design of the NPN architecture.
- **Active Network Component Sharing:** Similar to its passive network component sharing, PNI-NPN has nothing shared with other networks. Thus, its security level is very high. Also, Figure 11 indicates the trust measurement with mid value, however, in practice, the measurement would be based on the preliminary design of the NPN architecture.
- **Network Service Purpose:** The specific security requirements and the service needs depend on which services the PNI-NPN provides. Usually, the mission critical services require higher security than the non-mission critical services.
- **Level of Assurance:** PLMN applies both 3GPP SECAM and SCAS, and GSMA NESAS mostly. Thus, only the sharing parts of PNI-NPN with PLMN assure its security. The security level from this perspective is dependent on how many parts or network functions are shared with the PLMN.
- **Certification and Local Regulatory Requirement:** The trust measurement of level of assurance is dependent on the number of network entities or functions tested on the supply chain. PLMN always has more certificates than the NPN operator, as a result of meeting security and regulatory requirements.
- **Subscriber Management:** The subscription management for PNI-NPN is partially done within the MNO's mobile infrastructure. The security relies on the data management security provided by both the PLMN and the NPN.

5.2 MORAN

MORAN deployment aims to share the network infrastructure with the use of its own spectrum (see Section 3.2). Therefore, even though other operator's air interfaces have service interruption or disturbance in the same base station, it would not affect the MORAN services due to the spectrum isolations. Also, physical protection of base stations is one of the most important perimeters, and due diligence should be applied to the physical protection of those base stations. Furthermore, the data and traffic management protection from the fronthaul to backhaul should be in place. Figure 12 illustrates the MORAN level of trust with general or basic deployment.

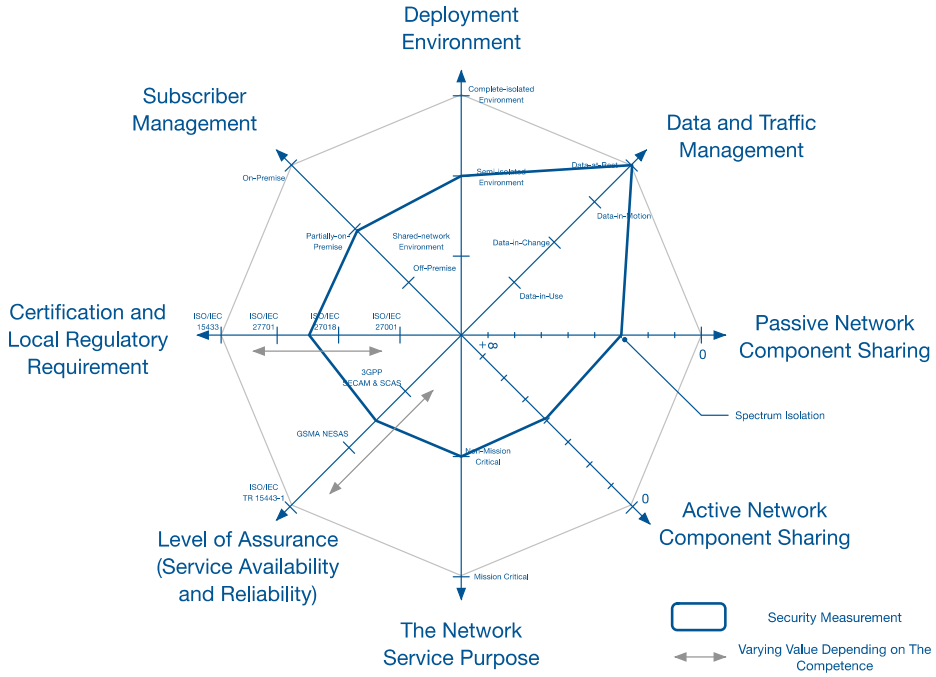

Figure 12: Level of Trust for MORAN

- **Deployment Environment:** A typical deployment of MORAN is under a semi-isolated environment. Basically, it shares the resources from the fronthaul to backhaul. The core network would be managed by the MNO itself.
- **Data and Traffic Management:** All the traffic would be routed back to the destination MNO's core network. Therefore, the traffic route should be fully protected by applying the data-at-rest, -in-use, -in-change and -in-motion, and traffic management policy.
- **Passive Network Component Sharing:** All RAN passive network components would be shared in between MNOs. Only the spectrum is not shared.

- **Active Network Component Sharing:** All RAN active network components would be shared in between MNOs. However, base stations require to be configured to support MNO's spectrum.
- **Network Service Purpose:** MORAN usually has an SLA in between two MNOs. This is often specified as non-mission critical communication.
- **Level of Assurance:** PLMN applies both 3GPP SECAM and SCAS as a baseline. GSMA NESAS assurance would depend on the vendor needs. The security level from this perspective is dependent on the number of network entities or functions tested under those schemes or certifications.
- **Certification and Local Regulatory Requirement:** Typically, local regulator might have different requirements for the local market competitions and regulations. Figure 12 indicates the trust measurement with an ISO 27001 that is a well-known common certification from ISO.
- **Subscriber Management:** Since MORAN would use a shared-RAN infrastructure, subscriber and billing information would be routed back to the destination MNO's core network. Therefore, part of subscriber data would be processed within the RAN. The subscriber management should also fulfil the worldwide or regional adopted basic subscriber privacy protection such as GDPR. There are other user privacy protection policies available in the market, which would be chosen by the local regulations and applied to the shared infrastructure.

5.3 MOCN

MOCN deployment aims to have a shared network infrastructure including the air interface (see Section 3.3). Therefore, when an MNO gets service interruption or disturbance on the air interface by a man-in-the-middle attack, it would affect other MNO's services due to shared spectrum on the same air interface. Also, every level of protection from the fronthaul to the backhaul requires due diligent to govern the shared network infrastructure. Furthermore, the data and traffic management protection from the fronthaul to backhaul should be in place. Figure 13 illustrates the MOCN level of trust with general or basic deployment.

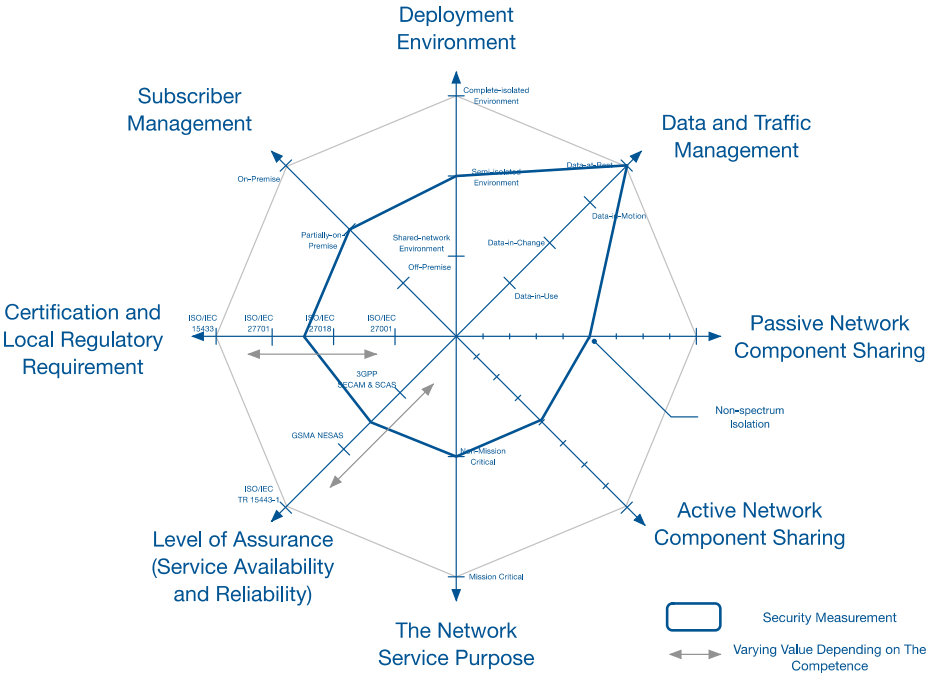

Figure 13: Level of Trust for MOCN

- **Deployment Environment:** A typical deployment of MOCN is under a semi-isolated environment. Basically, it shares the resources from the fronthaul to backhaul including spectrum. The core network would be managed by the MNO itself.
- **Data and Traffic Management:** All the traffic would be routed back to the destination MNO's core network. Therefore, the traffic route should be fully protected by applying the data-at-rest, -in-use, -in-change and -in-motion, and traffic management policy.
- **Passive Network Component Sharing:** All RAN passive network components would be shared in between MNOs.

- **Active Network Component Sharing:** All RAN active network components would be shared in between MNOs. However, it requires to track the capacity and availability of the resources at the cell level.
- **Network Service Purpose:** MOCN usually has an SLA in between MNO and tenants. This is often specified as non-mission critical communication.
- **Level of Assurance:** PLMN applies both 3GPP SECAM and SCAS as a baseline. GSMA NESAS assurance would depend on the vendor needs. The security level from this perspective is dependent on the number of network entities or functions tested under those schemes or certifications.
- **Certification and Local Regulatory Requirement:** Local regulator might have different requirements for the local market competitions and regulations. Figure 13 indicates the trust measurement with an ISO/IEC 27001 that is a well-known common certification for information security management. The trust measurement would be based on the number of certificates the MNO has.
- **Subscriber Management:** Since MOCN would use a shared-RAN infrastructure, subscriber and billing information would be routed back to the destination MNO's core network. Therefore, part of subscriber data would be processed within the RAN. The subscriber management should also fulfil the world-wide or regional adopted basic subscriber privacy protection such as GDPR. There are other user privacy protection policies available in the market, which would be chosen by the local regulations and applied to the shared infrastructure.

5.4 Site Sharing

Site Sharing deployment aims to share the cell site facilities (See Section 3.4). Site Sharing is often seen in urban and remote area. Physical security [16] of the site facilities to deny unauthorised access would be the main policy and protection. Figure 14 illustrates the site sharing level of trust with general or basic deployment.

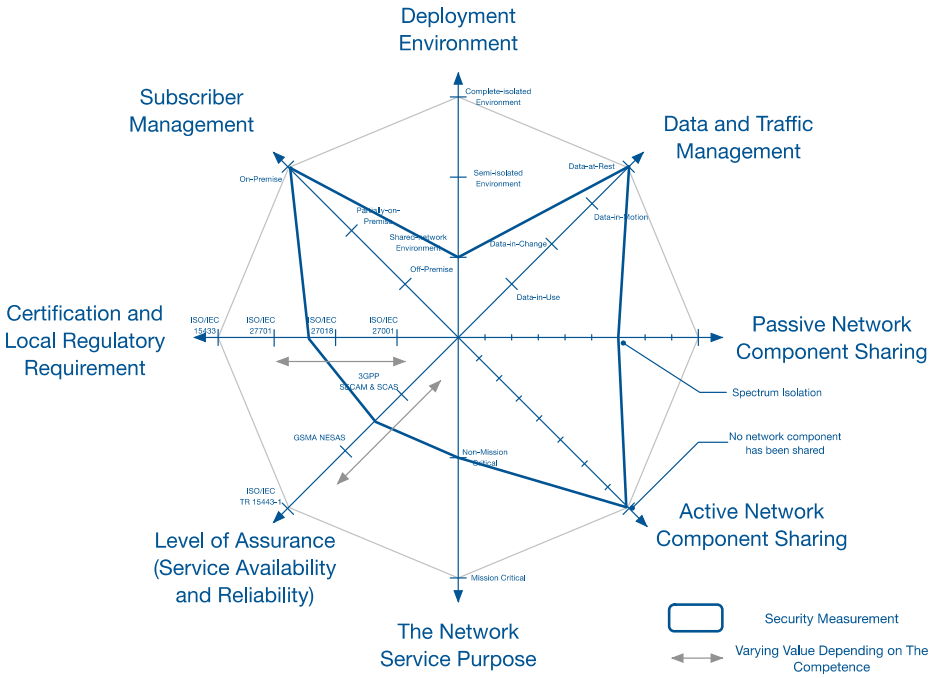

Figure 14: Level of Trust for Site Sharing

- **Deployment Environment:** Site Sharing is under a semi-isolated network environment. This poses vulnerabilities on the site sharing facilities. For example, an unauthorised access of network element might occur, and human errors on inappropriate access during the maintenance might cause service interruptions or affect the service availability.
- **Data and Traffic Management:** Site sharing has great potential risks on the site facilities. Therefore, data-in-motion protection should be enabled under the current security mechanisms specified in 3GPP. Also, data-at-rest, data-in-use and data-in-change should be applied to protect the overall network infrastructure. Access control has differentiated authorities to the NPN tenant and PLMN operator.
- **Passive Network Component Sharing:** The level of defense measure would be based on where the shared or dedicated components locate in the 3GPP trust model. Furthermore, the trust measurement would only require identifying the shared components, e.g., cables,

network racks and optical fibres. Figure 14 indicates the trust measurement with mid value. However, in practice, the measurement would be based on the preliminary design of the NPN architecture.

- **Active Network Component Sharing:** There is no active network component shared in site sharing. Thus, its security level is very high.
- **Network Service Purpose:** Typically, site sharing applies for PLMN services which are usually non-mission critical.
- **Level of Assurance:** PLMN applies both 3GPP SECAM and SCAS. GSMA NESAS would depend on the MNO or vendor requirements. The security assurance level would depend on the number of network functions that obtain those certificates.
- **Certification and Local Regulatory Requirement:** The measurement of level of assurance is dependent on the number of network entities or functions tested on the supply chain. PLMN always has more certificates than the NPN operator to meet the security and regulatory requirements.
- **Subscriber Management:** This is another typical case. The subscription management would be done within the MNO's mobile infrastructure. The level of security relies on the data management security provided within the MNO.

5.5 Backhaul Sharing

Backhaul Sharing deployment aims to share the backhaul transport infrastructure (see Section 3.5). MNOs might share the backhaul transport network with the others. Therefore, when the backhaul transport gets service interruption or disturbance, it would not affect the PLMN services immediately. But it would not able to register any subscriber or it might require to reroute the subscriber registration traffic to other secured routes. Also, backhaul transport provider should have certain protection on the network service resilience, reliability and availability. Furthermore, the data and traffic management protection at backhaul transport should be in place according to 3GPP. Figure 15 illustrates the backhaul level of trust with general or basic deployment.

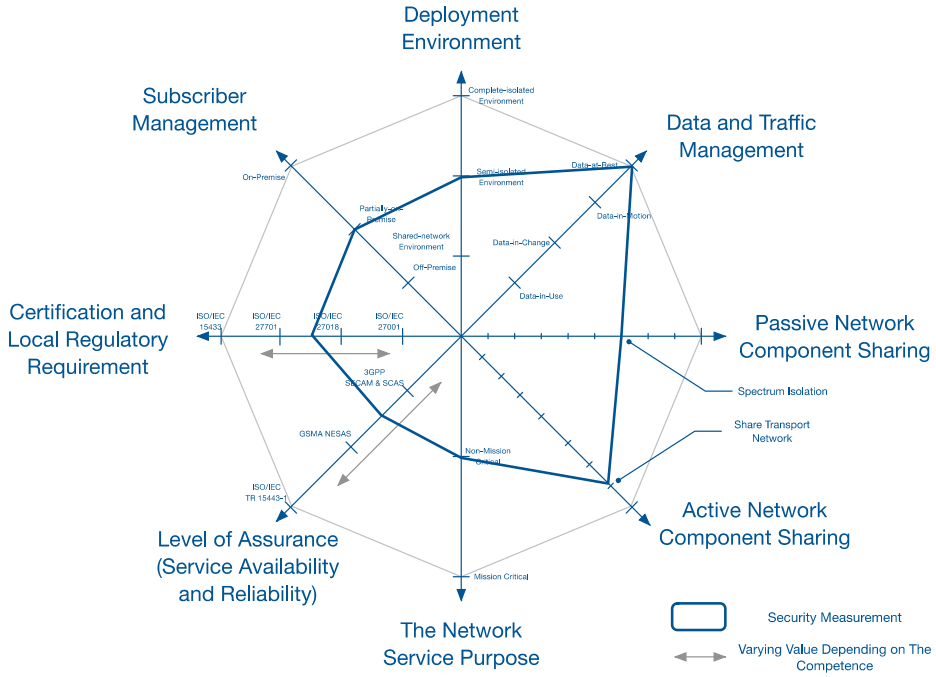

Figure 15: Level of Trust for Backhaul Sharing

- **Deployment Environment:** Backhaul sharing is under a semi-isolated network environment. Basically, it shares the transport network with other MNOs. But the RAN and core network are still managed by the MNO.
- **Data and Traffic Management:** All the traffic would be routed back to the destination MNO's core network. Therefore, the traffic route should be fully protected under the 3GPP security mechanism specification when data are in motion, and traffic management policy. Data-in-use and Data-in-change should also be applied to the core network and RAN.

- **Passive Network Component Sharing:** All backhaul transport fibre optics, switches and other passive network components would be shared in between MNOs.
- **Active Network Component Sharing:** All backhaul transport switches, firewall and other configurable active network components would be shared in between MNOs.
- **Network Service Purpose:** Backhaul sharing usually has an SLA in between MNO and backhaul transport network provider. This is specified as a non-mission critical communication.
- **Level of Assurance:** PLMN and backhaul transport provider apply both 3GPP SECAM and SCAS as a baseline. GSMA NESAS assurance would depend on the vendor needs. The security level from this perspective is dependent on the number of network entities or functions tested under those schemes or certifications.
- **Certification and Local Regulatory Requirement:** Local regulator might have different requirements for the local market competitions and regulations. Figure 15 indicates the trust measurement with an ISO/IEC 27001 that is a well-known common certification for information security management. The trust measurement would be based on the number of certificates the MNO and backhaul transport provider own.
- **Subscriber Management:** Since MNOs share the backhaul transport and their subscribers, the billing information would be routed back to the destination MNO's core network via third party transport. Therefore, part of subscriber data would be processed within the RAN, and then forwarded to the core network via third party transport. The subscriber management should also fulfil the world-wide or regional adopted basic subscriber privacy protection such as GDPR. There are other user privacy protection policies available in the market, which would be chosen by the local regulations and applied to the shared infrastructure.

5.6 Core Network Sharing

Core Network Sharing deployment aims to share the core network (see Section 3.6). Therefore, all subscriber information would be under the infrastructure shared with other MNO or tenants. The protection of the core network would highly rely on the security control and policies. The core network should not get service interruption or disturbance, but require network service resilience, reliability and ensure the service availability. Generally, an overall mobile service should be highly protected of the service availability when designing the shared network infrastructure and all network perimeters should be thoroughly considered. Figure 16 illustrates the core network sharing level of trust with general or basic deployment.

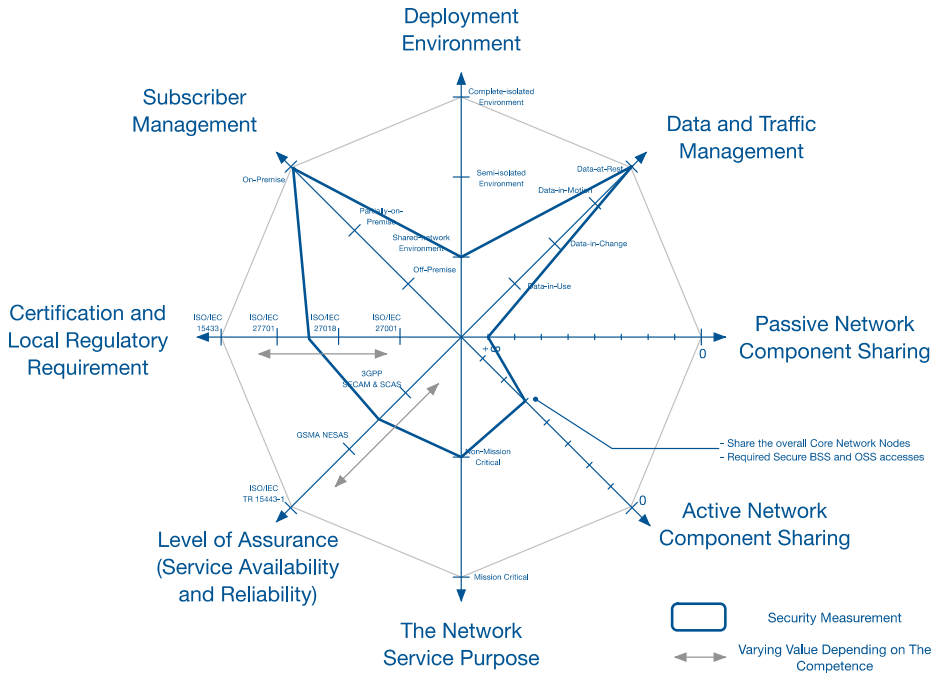

Figure 16: Level of Trust for Core Network Sharing

- **Deployment Environment:** Core network sharing is under a shared-network environment. Basically, it shares the physical infrastructure among the others. The core network sharing would be fully managed by the MNO.
- **Data and Traffic Management:** All traffic should be fully protected to avoid impersonation, tampering and eavesdropping etc. Core network sharing should be fully complied with the 3GPP security mechanism specification when data are in motion, and the traffic management policy. Data-in-use and Data-in-change should also be applied when data are being accessed.

- **Passive Network Component Sharing:** All core network sharing passive network components would be shared in between MNO and tenants.
- **Active Network Component Sharing:** All core network sharing active network components would be shared in between MNO and tenants.
- **Network Service Purpose:** Core network sharing is usually applied as a non-mission critical communications service. The service reliability and availability would be based on the MNO network infrastructure.
- **Level of Assurance:** PLMN should apply both 3GPP SECAM and SCAS as a baseline. GSMA NESAS assurance would depend on the vendor's needs. The security level from this perspective is dependent on the number of network entities or functions tested under those schemes or certifications.
- **Certification and Local Regulatory Requirement:** Local regulator might have different requirements for the local market competitions and regulations. Figure 16 indicates the trust measurement with an ISO/IEC 27001 that is a well-known common certification for information security management. The measurement would be based on the number of certificates the MNO and backhaul transport provider own.
- **Subscriber Management:** MNOs would enforce the security protection to the overall network infrastructure. A number of subscriber management policies could be embedded into the design of core network sharing infrastructure and all subscribers should be remained on-premise. Therefore, subscriber data processing for customer service and billing would be within the MNO's network infrastructure. Also, the subscriber management should fulfil the world-wide or regional adopted basic subscriber privacy protection such as GDPR. There are other user privacy protection policies available in the market, which would be chosen by the local requirements and applied to the shared infrastructure. However, sometimes, tenants would like to manage their own subscribers. Therefore, the subscriber management would become partially-on-premise and must fulfil the GDPR and 3GPP specified security mechanism protections.

5.7 Network Slicing

Network slicing is a revolutionary concept of enabling mobile network on demand. The deployment of network slicing aims to share the physical infrastructure using virtualisation and containerisation technologies (see Section 3.7). Basically, network slicing allows connectivity and data processing tailored to the customer's specific requirements. The customisable network capabilities can range from data speed, quality of service, latency, reliability, security, to services. There is a possibility of wrongly put isolation points in the network slice, which might lead to service interruption or disturbance. Also, network slice may comprise dedicated and/or shared resources [5]. The network dedicated functions might locate within a bare metal machine and be shared among other network slices. Therefore, network slice security might require an extra-level of protection on virtualisation and containerisation technologies and handling the subscriber and their credentials. Figure 17 illustrates the network slice level of trust with general or basic deployment.

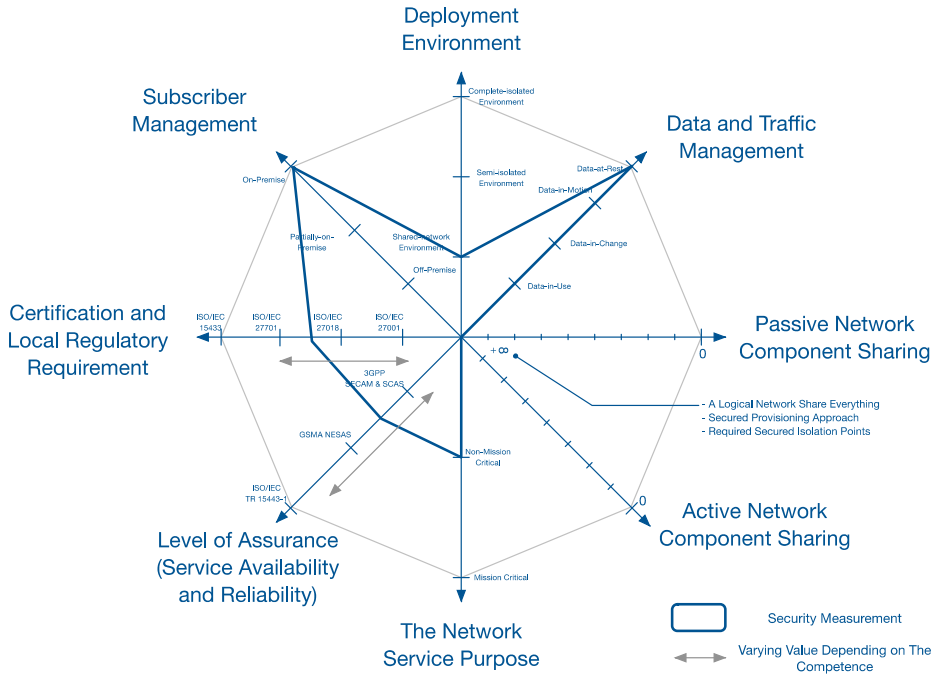

Figure 17: Level of Trust for Network Slice

- **Deployment Environment:** Network slicing is under a shared-network environment. Basically, it shares the physical infrastructure among others. The network slice might be managed by the MNO. But there is a high possibility that tenants would like to manage it on their own.
- **Data and Traffic Management:** All traffic should be fully protected to avoid impersonation, tampering and eavesdropping etc. Network slice should be fully complied with 3GPP security mechanism specification when data are in motion, and traffic management policy. Data-in-use and Data-in-change should also be applied to the network slice provisioning platform.
- **Passive Network Component Sharing:** All network slice's passive network components would be shared in between tenants.
- **Active Network Component Sharing:** All network slice's active network components would be shared in between tenants.
- **Network Service Purpose:** Ideally, network slice could be used as a mission critical communication service. However, the mission critical communication service requires a certain level of service reliability and availability in operation. Therefore, network slice would typically be used as a non-mission critical communication service.
- **Level of Assurance:** PLMN should apply both 3GPP SECAM and SCAS as a baseline. GSMA NESAS assurance would depend on the vendor needs. The security level from this perspective is dependent on the number of network entities or functions tested under those schemes or certifications.
- **Certification and Local Regulatory Requirement:** Local regulator might have different requirements on network slices for the local market competitions and regulations. Figure 17 indicates the trust measurement with an ISO/IEC 27001 that is a well-known common certification for information security management. The trust measurement would be based on the number of certificates the MNO owns.
- **Subscriber Management:** MNOs might provide subscriber and billing management via a network slice provisioning platform which can enforce the security protection to the overall network slices. A number of subscriber management policies could be embedded into the design of the network slice. Therefore, subscriber data processing for customer service and billing would be within the MNO's network infrastructure. Also, the subscriber management should fulfil the world-wide or regional adopted basic subscriber privacy protection such as GDPR. There are other user privacy protection policies available in the market that would be chosen by the local regulations and applied to the shared infrastructure.

5.8 MEC

MEC has a number of edge enabler functions under the 3GPP specification and these edge enabler functions could share the same UPF, transport network and RAN. A typical MEC deployment aims to provide URLLC, fast control interactive applications and service agility (see Section 3.8). Figure 18 gives an example of MNO A and B that share a MEC platform with a 3rd party provider. The UEs of both subscribers can consume services from the shared MEC platform of the 3rd party service provider.

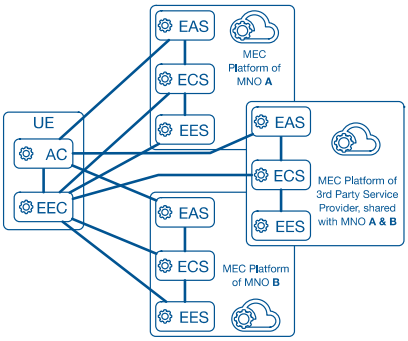

Figure 18: 3GPP MEC Enabler Functions Example

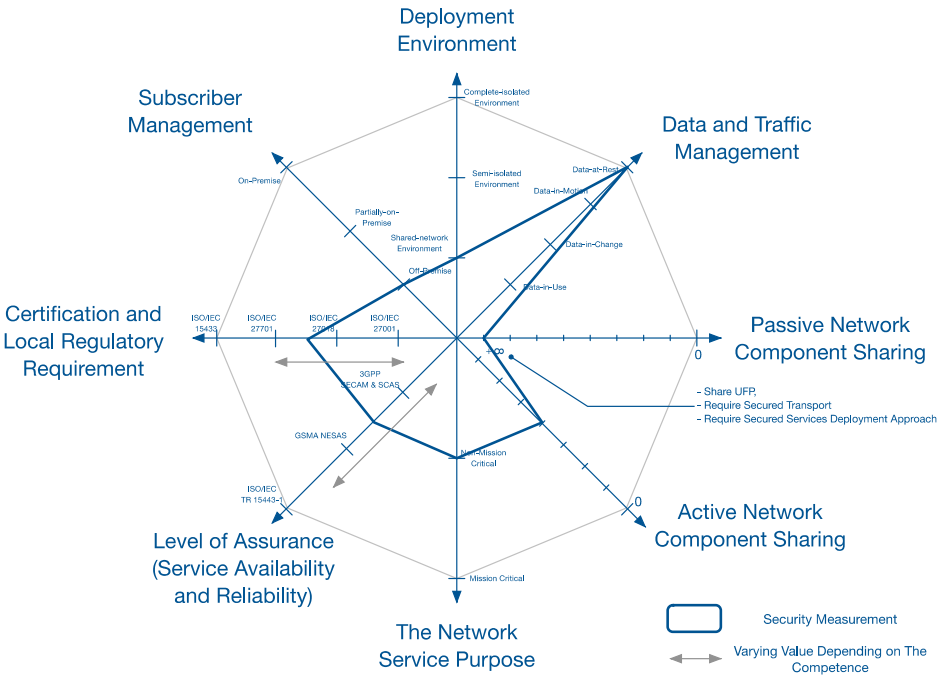

Figure 19: Level of Trust for MEC

Moreover, MEC usually allocates in a shared-network environment, and relies on the cloud security protections and regulations. The nature of cloud computing has been labelled as high service reliability and availability. Service interruption might occur due to the attacks of resources overflow or zero-day exploits. Furthermore, the data and traffic management protection should be thoroughly applied on the identity and access management. Figure 19 illustrates the MEC level of trust with general or basic deployment.

- **Deployment Environment:** MEC is under a shared-network environment. Basically, it shares the physical infrastructure among others. The MEC might be managed by the MNO. But there is a high possibility that tenants would like to link their own service to/from the public cloud.
- **Data and Traffic Management:** All traffic must be fully protected to avoid impersonation, tampering and eavesdropping etc. MEC should be fully complied with 3GPP and ETSI security mechanism specifications when data are in motion, and traffic management policy for inbound and outbound traffic via MEC. Data-in-use and Data-in-change restriction should also be applied to the MEC microservice provisioning platform.
- **Passive Network Component Sharing:** All MEC enabler's passive network components might be shared in between tenants.
- **Active Network Component Sharing:** All MEC enabler servers, physical and virtualised switches, and other active network components might be shared in between tenants.
- **Network Service Purpose:** Typically, MEC is a service enabler which would be classified as a non-mission critical communication service.
- **Level of Assurance:** PLMN might apply both 3GPP SECAM and SCAS as a baseline. GSMA NESAS assurance would depend on the vendor needs. The security level from this perspective is dependent on the number of network entities or functions tested under those schemes or certifications.
- **Certification and Local Regulatory Requirement:** Typically, local regulator might have different requirements for the local market competitions and regulations. Figure 19 indicates the trust measurement with an ISO/IEC 27001 that is a well-known common certification for information security management. The trust measurement would be based on the number of certificates the MNO and MEC provider own.
- **Subscriber Management:** MNOs might have a MEC platform for their customers. The MEC provisioning platform should provide a list of subscriber and tenant information protections and enforce the overall MEC platform and network infrastructure protections. Service resources and billing information should be managed on premise within MEC platform which enforces the all over security. However, the MEC enabler functions are still

under a shared environment. Therefore, the subscriber management must fulfil the world-wide or regional adopted basic subscriber privacy protection such as GDPR. There are other user privacy protection policies available in the market that would be chosen by the local regulations and applied to the shared infrastructure.

6 NETWORK SHARING DEPLOYMENT SECURITY OPERATION AWARENESS

Under the modern network traffic on-demand runtime, network expansion, network services elasticity, network resources auto-optimisation during operation, we should be aware of the self-expansion and contraction of network infrastructure that might potentially abuse the network resources, e.g., DNS IP addresses, ports, bandwidth, compute resources, network resources or storage resources. Practically, self-expand and -contract network resources, and zero-day attacks on services might cause unexpected issues on the shared network infrastructure. Therefore, we have to increase the shared network infrastructure visibility that should be clearly indicated by the shared network infrastructure behaviour from threat intelligence, and appropriately use SIEM on network behavioural anomaly detection. While the network has become more and more intelligent, those intelligence might violate the international or local privacy rules. Therefore, the design of shared mobile infrastructure should fundamentally comply with those international or local privacy rules.

7 CONCLUSION

Mobile network infrastructure sharing is one of the most important methods to maximise the utilisation of the mobile network in various levels. Also, the overall goal of developing mobile network infrastructure sharing aims to reduce the CAPEX and OPEX, and to capitalise the information technology applied on mobile network infrastructure. Particularly, when sharing the infrastructure, whichever option applied, we shall enforce the right security mechanisms to protect the network perimeters, and other perimeters in the network.

In this White Paper, we review different types of mobile network sharing infrastructure options and formulate a qualitative analysis approach to assist MNOs and tenant in determining the importance of shared infrastructure security. Those trust measurements could provide us with a high-level understanding of each mobile network sharing infrastructure option's importance and awareness on deployment. Even though, from the trust measurement figures, mobile network sharing infrastructure deployment environment appears to be the most important element. When the actual deployment takes place, we must take into account that the other elements would be equally important.

In practice, MNOs might require fulfilling the local regulations and market to adopt various certificates for providing a level of confidence to their customers. Obviously, obtaining such assurance would increase the level of confidence on managing the network with a regular routine on each security control and process. Furthermore, data and traffic management protections are essential to another level of complexity in deploying the shared network. The protection on-premise and off-premise would require different security mechanisms and security control. Ultimately, any data breach would cause MNOs' reputation damage or affect customer privacy. Therefore, data protection should be thoroughly integrated with the mobile network sharing infrastructure, especially in those systems across different domains e.g., Operations Support System (OSS) and Business Support System (BSS). Therefore, sharing a network architecture design with embedded security would help to identify the overall security concerns.

LIST OF ABBREVIATIONS

5G	Fifth Generation
APN	Access Point Name
BSS	Business Support System
CAPEX	Capital Expenditures
MNO	Mobile Network Operator
MNIaaS	Mobile Network Infrastructure as a Service
MORAN	Multi-Operator Radio Access Network
MOCN	Multi-Operator Core Network
MEC	Multi-access Edge Computing
NPN	Non-Public Network
NESAS	Network Equipment Security Assurance Scheme
OPEX	Operating Expenses
OSS	Operations Support System
PLMN	Public Land Mobile Network
PNI-NPN	Public Network integrated NPN
QoS	Quality of Service
RAN	Radio Access Network
SCAS	Security Assurance Specification
SECAM	Security Assurance Methodology
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SNPN	Standalone Non-Public Network
SOC	Security Operation Center

REFERENCES

[1] Djamal-Eddine Meddour, Tinku Rasheed and Yvon Gourhant, “On the Role of Infrastructure sharing for Mobile Network Operators in Emerging Markets”, Computer Networks, Vol. 55, Issue 7, 16 May 2011, Pages 1576-1591

[2] GSMA, “Mobile Infrastructure Sharing”

[3] 3GPP TS 33.117, Release 17, “Catalogue of general security assurance requirements”

[4] GSMA, “The Network Equipment Security Assurance Scheme (NESAS)”

[5] ISO/IEC TR 15443-1:2012, “Information technology – Security techniques – Security assurance framework – Part 1: Introduction and concepts”

[6] Stavroula Rizou , Eugenia Alexandropoulou-Egyptiadou, and Konstantinos E. Psannis, “GDPR Interference With Next Generation 5G and IoT Networks”, IEEE Access, Volume 8, 2020.

[7] 5G-ACIA, "5G Non-Public Networks for Industrial Scenarios“, July 2019

[8] GSMA, “An Introduction to Network Slicing”, Jan 2020

[9] GSMA, White Paper, “Network Slicing Use Case Requirements”, April 2018

[10] GSMA, NG.116, “Generic Network Slice Template”, Version 6.0, 25 November 2021

[11] Stan Wong, Bin Han, Hans D. Schotten, “5G Network Slice Isolation”, MDPI Network, Volume 2, Issue 1, 2022

[12] ETSI White Paper No.28, “MEC in 5G networks”, ISBN No. 979-10-92620-22-1, June 2018

[13] 3GPP TS 23.558 Rel 17, “Architecture for enabling Edge Applications”, March 2022

[14] ETSI White Paper No. 46, “MEC security: Status of standards support and future evolutions”, 1st edition – May 2021, ISBN No. 979109262040

[15] 3GPP TS 23.251 v15.1.0, Network sharing; Architecture and functional description

[16] 3GPP TS 22.104 v16.0.0, Service requirements for cyber-physical control applications in vertical domains, Stage 1

[17] 3GPP TS 23.501 v15.4.0, System architecture for the 5G System, Stage 2