3GPP TR 22.830 V16.1.0 (2018-12)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Feasibility Study on Business Role Models for Network Slicing (Release 16)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

Slice, Role

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2018, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [5](#__RefHeading___Toc533173525)

1 Scope [6](#__RefHeading___Toc533173526)

2 References [6](#__RefHeading___Toc533173527)

3 Definitions, symbols and abbreviations [6](#__RefHeading___Toc533173528)

3.1 Definitions [6](#__RefHeading___Toc533173529)

3.2 Abbreviations [7](#__RefHeading___Toc533173530)

4 Overview [7](#__RefHeading___Toc533173531)

4.1 Business, stakeholder and management role models [7](#__RefHeading___Toc533173532)

4.2 Trust relationships [8](#__RefHeading___Toc533173533)

5 Role model scenarios [9](#__RefHeading___Toc533173534)

5.1 3rd party encryption [9](#__RefHeading___Toc533173535)

5.1.1 Description [9](#__RefHeading___Toc533173536)

5.1.2 Potential requirements [9](#__RefHeading___Toc533173537)

5.2 Private slice selection [9](#__RefHeading___Toc533173538)

5.2.1 Description [9](#__RefHeading___Toc533173539)

5.2.2 Potential requirements [10](#__RefHeading___Toc533173540)

5.3 Network slicing and roaming scenarios [10](#__RefHeading___Toc533173541)

5.3.1 Description [10](#__RefHeading___Toc533173542)

5.4 Enhanced network capability exposure for distribution network of smart grid [11](#__RefHeading___Toc533173543)

5.4.1 Description [11](#__RefHeading___Toc533173544)

5.4.2 Potential requirements [12](#__RefHeading___Toc533173545)

5.5 A/V production use cases with local standalone network deployment [12](#__RefHeading___Toc533173546)

5.5.1 Description [12](#__RefHeading___Toc533173547)

5.5.2 Potential requirements [14](#__RefHeading___Toc533173548)

5.6 A/V production use cases relying on PLMN infrastructure [14](#__RefHeading___Toc533173549)

5.6.1 Description [14](#__RefHeading___Toc533173550)

5.6.2 Potential requirements [16](#__RefHeading___Toc533173551)

5.7 Network slicing for Industry 4.0 verticals [16](#__RefHeading___Toc533173552)

5.7.1 Description [16](#__RefHeading___Toc533173553)

5.7.2 Potential requirements [17](#__RefHeading___Toc533173554)

5.8 End-to-end asset tracking [17](#__RefHeading___Toc533173555)

5.8.1 Description [17](#__RefHeading___Toc533173556)

5.8.2 Potential Requirements [19](#__RefHeading___Toc533173557)

5.9 Network slicing roles in (off-shore) wind farm [19](#__RefHeading___Toc533173558)

5.9.1 Description [19](#__RefHeading___Toc533173559)

5.9.2 Potential requirements [21](#__RefHeading___Toc533173560)

5.10 Private slice management [21](#__RefHeading___Toc533173561)

5.10.1 Description [21](#__RefHeading___Toc533173562)

5.10.2 Potential requirements [22](#__RefHeading___Toc533173563)

5.11 Management of network selection information in (off-shore) wind farm [22](#__RefHeading___Toc533173564)

5.11.1 Description [22](#__RefHeading___Toc533173565)

5.11.2 Potential requirements [22](#__RefHeading___Toc533173566)

6 Considerations [22](#__RefHeading___Toc533173567)

6.1 Considerations on security [22](#__RefHeading___Toc533173568)

6.2 Considerations on performance [23](#__RefHeading___Toc533173569)

7 Consolidated potential requirements [23](#__RefHeading___Toc533173570)

7.1 General [23](#__RefHeading___Toc533173571)

7.2 Service exposure [23](#__RefHeading___Toc533173572)

7.3 Network slice constraints [24](#__RefHeading___Toc533173573)

7.4 Cross-network slice coordination [24](#__RefHeading___Toc533173574)

7.5 Slice fault tolerance [24](#__RefHeading___Toc533173575)

8 Conclusion and recommendations [24](#__RefHeading___Toc533173576)

Annex A: Change history [25](#__RefHeading___Toc533173577)

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e., technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present document examines the business role models for network slicing in order to identify potential requirements that will enable a 3GPP system to adequately support those models, including:

Business role models for network slicing,

Trust relationships between MNOs and 3rd parties under various business role models,

Security relationships based on business role models,

Relationship of business role models with slice characteristics (e.g., slice scalability, slice flexibility), and

3GPP enhancements needed to support the business role models for slices.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.261: "Service requirements for the 5G system".

[3] 3GPP TR 22.804: "Study on Communication for Automation in Vertical Domains";

[4] ETSI TR 103 588v1.1.1: "Reconfigurable Radio Systems (RRS); Feasibility study on temporary spectrum access for local high-quality wireless networks".

[5] 5G NORMA Deliverable D3.3: "5G NORMA network architecture – Final report".

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**non-public network:** a network that is intended for non-public use

**private slice:** a dedicated network slice deployment for the sole use by a specific 3rd party.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5G 5th Generation

5GC 5G core network

A/V Audio/Visual

CD/DVD Compact Disc/Digital Versatile Disc

IoT Internet of Things

KPI Key Performance Indicator

LSA Licensed Shared Access

MIoT Massive Internet of Things

MNO Mobile Network Operator

OTT Over the Top

SCEF Service Capability Exposure Function

SPaaS Spectrum as a Service

URLLC Ultra Reliable Low-Latency Communications

V/NFs Virtual Network Functions

# 4 Overview

## 4.1 Business, stakeholder and management role models

5G supports new business role models relevant for 3GPP systems. In previous generations, business role models centered on two key types of relationships: those between Mobile Network Operators (MNOs) and their subscribers and those between MNOs (e.g., roaming, RAN sharing). To a limited extent, relationships between MNOs and 3rd party application providers have also been supported in the form of APIs (e.g., by the SCEF interface - see TS 23.682) allowing access to specific network capabilities, such as those used by 3rd party applications to access UE location information. 5G opens the door to new business role models for 3rd parties, allowing 3rd parties more control of system capabilities. This document considers these new business roles and how 3GPP can best support the trust relationships between MNOs and 3rd parties resulting from these new business role models.

In 5G three role models are envisaged for stakeholders.

1) The MNO owns and manages both the access and core network.

2) An MNO owns and manages the core network, the access network is shared among multiple operators (i.e., RAN sharing).

3) Only part of the network is owned and/or managed by the MNO, with other parts being owned and/or managed by a 3rd party.

The first two are essentially those found in previous generations of 3GPP systems, where MNOs are operating PLMNs. In 5G it is expected that a 3rd party can take on the role of an MNO, however in this case the 3rd party would operate its own network. From a 3GPP perspective, stakeholder role models 1 and 2 are the same whether an MNO or vertical 3rd party is involved. Basic support for the 3rd party stakeholder role model was provided in previous generations via APIs which allowed minimal access to or management of network capabilities. In contrast, the 5G enhancements will allow greater control and ownership by the 3rd party, which will require increased trust between the MNO and 3rd party. These new trust relationships become even more impactful when network slicing is considered, particularly where the 3rd party is authorized to control some aspects of network slices that are owned by the MNO.

With the introduction of network slicing, the third stakeholder role model above warrants additional investigation to understand the trust relationships between MNOs and 3rd parties. There are four potential business relationship models impacting the trust relationships for stakeholder role model 3.

- Model 3a: MNO provides the virtual/physical infrastructure and V/NFs; a 3rd party uses the functionality provided by the MNO,

- Model 3b: MNO provides the virtual/physical infrastructure and V/NFs; a 3rd party manages some V/NFs via APIs exposed by the MNO,

- Model 3c: MNO provides virtual/physical infrastructure; a 3rd party provides some of the V/NFs,

- Model 3d: a 3rd party provides and manages some of the virtual/physical infrastructure and V/NFs.

Table 4.1-1 Business relationship models.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | Model 3a | Model 3b | Model 3c | Model 3d |
| Virtual/physical Infrastructure  (3GPP architecture) | Core | physical | MNO | MNO | MNO | MNO and 3rdparty |
| virtual | MNO | MNO | MNO | MNO and 3rdparty |
| RAN | physical | MNO | MNO | MNO | MNO and 3rdparty |
| virtual | MNO | MNO | MNO | MNO and 3rdparty |
| Virtual Network Functions (Applications/Servers) | Provider |  | MNO | MNO | MNO and 3rdparty | MNO and 3rdparty |
| Manager |  | MNO | MNO and 3rdparty | MNO and 3rdparty | MNO and 3rdparty |

Of these models, 3a and 3b have been addressed by the requirements in place in TS 22.261. Provision has been made to ensure appropriate APIs and management functions to support this extended 3rd party access and control of capabilities provided by the MNO, and to do so in a secure manner. Within these two models, the 3rd party has increasing control over the network capabilities that support its service. However, this control is limited to what is allowed by the MNO through the provided APIs.

Models 3c and 3d provide extended control for the 3rd party on the network capabilities supporting its service. However, these models still require ensuring appropriate levels of security are maintained for any communications.

In four potential business relationship models, three management role models can be considered for models 3c and 3d.

1. MNO manages all virtual/physical infrastructure and all V/NFs including 3rd party’s ones,
2. 3rd party manages its own virtual/physical infrastructure and/or its own V/NFs; MNO manages the others.
3. 3rd party manages virtual/physical infrastructure and/or V/NFs including its own virtual/physical infrastructure and/or V/NFs and some MNO’s virtual/physical infrastructure and/or V/NFs; MNO manages the others.

From the 3rd party perspective, the management role models 2 and 3 support the 3rd party management function and provide extended management for the MNO to coordinate with the 3rd party management. The 3rd party may use suitable APIs provided by the MNO to directly manage the V/NFs as well as the infrastructure resources so that it can properly handle when their business requirements are changed.

## 4.2 Trust relationships

The degree of trust between the MNO and 3rd party has an impact on the 3GPP system. In model 3a, the 3rd party must be able to trust the MNO to provide the necessary capabilities. In the other models, the MNO must also be able to ensure that the degree of control provided to the 3rd party does not allow the 3rd party to negatively impact the MNOs network. TS 22.261 addresses the trust relationships for models 3a and 3b. For models 3c and 3d to be supported, additional consideration is needed on the mechanisms to provide the isolation and interfaces that give the 3rd party the appropriate level of control while securing the PLMN.

Specifically for models 3c and 3d, where the 3rd party provides V/NFs or provides and manages some of the virtual/physical infrastructure and V/NFs, SLAs may be used to address some trust issues, such as what each party will provide and manage. However, the principles of trust and verification also come into play. The 3rd party must be able to verify, though the management interface, that all terms of the SLA are being met by the MNO. Similarly, the MNO must be able to verify that the 3rd party is managing resources appropriately so that there is no adverse impact to the rest of the network. Appropriate management interfaces are needed to support both the network operator and 3rd party.

The underlying trust relationships support such models and may lead to new 3GPP requirements, such as the abilities to provide slice based authentication and slice based encryption and integrity protection. The present document considers the trust relationships related to extended control by a 3rd party.

# 5 Role model scenarios

## 5.1 3rd party encryption

### 5.1.1 Description

A mobile network operator provides a slice for small business customers. This small business slice supports capabilities such as LAN emulation for the office environment, support for employee smartphones (e.g., voice, high speed data), and internet connectivity to support the business’ social media and advertising needs. The slice can be customized by individual small business customers to better meet their specific needs, using APIs provided by the operator.

In this scenario, a small business wants to ensure the privacy of its communications within the slice. The trust relationship between the network operator and the 3rd party requires that communications within the slice be private both in terms of other users of the network and the network operator. This trust relationship can be met by allowing the 3rd party to provide their own encryption algorithm for intra-slice communications, using a customization capability provided by the network operator.

This 3rd party encryption ensures the privacy of the business’ communications within the private slice, although certain metadata may still be visible to the MNO, providing the MNO with resource management data.

The new requirement for this model concerns the ability for the 3rd party to provide its own encryption algorithm for intra-slice communication. Such encryption could be done as an OTT capability, but this would have a negative impact on the overall efficiency of the slice communications. The additional layer of encryption/decryption at each UE and network element, on top of the normal 3GPP processing, increases resource usage, which reduces efficiency and impacts battery life. The time to perform the OTT encryption/decryption also adds to the latency delay for each communication.

Being able to use the 3rd party encryption in a 3GPP-supported manner allows the small business to ensure the privacy of its internal communications and to do so in a resource efficient manner. This requirement would be added to the network capability exposure clause of TS 22.261 [2].

### 5.1.2 Potential requirements

[PR 5.1.2-1] The 3GPP system shall provide suitable APIs to allow use of a trusted 3rd party provided encryption between any UE served by a private slice and a core network entity in that private slice.

## 5.2 Private slice selection

### 5.2.1 Description

A business wants to have a secure and isolated set of network capabilities that meets its communication needs, without having to purchase and maintain the network infrastructure. In this case, a mobile network operator can use network slicing as a means to provide a virtual private network, or private slice, for the enterprise.

The criteria for the private slice include the following:

- only UEs belonging to the 3rd party have access to the resources allocated to the slice – this prevents unauthorized UEs from consuming slice resources potentially resulting in an authorized UE not being able to access a needed resource

- some UEs belonging to the 3rd party may be authorized for use only on the slice (i.e., no access to other slices of the network) – a robot should only use resources belonging to the slice to ensure it receives the necessary service support (QoS etc.)

- some UEs belonging to the 3rd party may be authorized for use on the slice as well as on other slices of the network.

The MNO allocates the necessary resources that meet the agreed KPIs for the business to the private slice. The slice includes radio resources allocated for the sole use of the business as well as core network functionality. A business may arrange for more than 1 private slice to differentiate service offerings for different types of equipment, e.g., robotic manufacturing equipment that requires URLLC may be assigned to a specific slice while access to databases and office equipment may be assigned to a separate slice with different KPIs. Some equipment may need to have access to more than one of the private slices used by the business.

A mechanism is needed to ensure that the business’ traffic is confined to the slices allocated to the business. This avoids potential churn to the remaining network resources as well as constrains resource usage metrics for slice management and charging purposes. For similar reasons, a mechanism is also needed to prevent non-authorized UEs from attaching to a slice. If the business uses more than one slice (e.g., URLLC/non-URLLC) then a mechanism is needed to ensure that UEs only access the slice(s) within the business that they are authorized for (e.g., printer cannot access a URLLC slice). At the same time, some UEs need to be able to access both slices and slices open to other users (e.g., employee phones). Techniques similar to CSG could be used to optimize the access attempts to certain slices. An optional secondary authentication may also be used to ensure that only authorized UEs access the functionality of the private slice.

The trust relationships in this scenario include the following aspects.

- The business trusts the MNO to provide the agreed resources and functionality needed by the business.

- The MNO is responsible for ensuring isolation of the slice communications from the rest of the network, including only allowing authorized UEs to access a slice and constraining authorized UEs to the authorized slice.

- The business may provide a secondary authentication to ensure only authorized UEs access the private slice.

### 5.2.2 Potential requirements

[PR 5.2.2-5] The 3GPP system shall support a mechanism to prevent a UE from accessing a cell it is not authorized to select.

[PR 5.2.2-6] The 3GPP system shall support a mechanism for a 3rd party to authenticate a UE for access to a private slice.

## 5.3 Network slicing and roaming scenarios

### 5.3.1 Description

A customer may require certain network slice capabilities that work across a very large area. For example, a company that provides transportation services may have vehicles that cross borders between operators and between nations. These vehicles may use certain slices in their HPLMN that they also need to access in VPLMNs. The 5G system should support the use of specific network slices in the HPLMN as well as VPLMNs that mobile devices may roam to. There are at least 3 methods to do this:

a) Define standardized slices so that a roaming device can obtain service from the same slice that it uses in home network. This approach is somewhat inflexible, as it requires 3GPP specification. Customers would also need to design their applications to work in the standardized slices.

b) Define slices with comparable characteristics that will be supported by a group of agreeable operators. As long as the customer is served by those operators, the required slice will be available. This could be done without a 3GPP specification.

c) Define signalling that allows the HPLMN specific slices to be “ported” to a serving PLMN. Essentially the home network could provide a slice’s blueprint to the VPLMN. The VPLMN would then create a slice that meets the requirements or respond that it cannot support the specific requirements.

## 5.4 Enhanced network capability exposure for distribution network of smart grid

### 5.4.1 Description

A mobile network operator provides a slice for a power grid company. This slice supports power grid specific services such as MIoT service for grid sensors in the company's Distribution Network. These sensors, deployed at each home, could record the usage of power, and send the recorded data back to the company via the mobile network. The manager of power grid company could customized the slice to meet their specific needs, by using APIs provided by the mobile network operator.



Figure 5.4.1-1: Overview of the role model scenario between MNO and power grid company

As depicted in Figure 5.4.1-1, the private slice provides MIoT services for power grid company’s sensors across multiple areas. In the control centre, a management tool, which is called Unified device management platform, could manage these sensors distributed in different areas via the APIs provided by the mobile network operator. The Unified device management platform could further cooperate with other specific tools or platforms for smart grid applications, e.g., electricity meters, charging pile, distributed generation, distribute automation.

In this scenario, a power grid company wants to manage their numerous devices more effective via the APIs provided by the mobile network operator. For example, the company wants to know the current status (e.g., location, connection status and etc.) of their devices in a specific area to get the whole view for this area. The numbers of the devices could be in a range from digits to tens of thousands. Some devices perform normally, but some devices may be abnormal, i.e., there is no feedback from the UE at company’s application layer. Once there are one or more abnormal devices, the company would like to get further information from the operator that whether the problem comes from the network communication to a UE or from the UE itself. If a failure device is identified, a repair team will be sent to fix it.

Being able to provide more information via APIs allows the power grid company to get the whole picture for their deployed devices and to identify and repair the abnormal device in a more efficient way. These requirements would be added to the network capability exposure clause of TS 22.261 [2].

### 5.4.2 Potential requirements

[PR 5.4.2-1] The 3GPP network shall provide suitable APIs to allow a trusted 3rd party to monitor the status (e.g., locations, lifecycle, registration status) of its own UEs served by a private slice in a specific area that covered by this slice.

NOTE: The number of UEs could be in the range from single digit to tens of thousands.

[PR 5.4.2-2] The 3GPP network shall provide suitable APIs to allow a trusted 3rd party to get the network status information of a private slice dedicated for the 3rd party, e.g., the network communication status between the slice and a specific UE.

## 5.5 A/V production use cases with local standalone network deployment

### 5.5.1 Description

Consider the case of an audio/video production company that may require covering and producing professional live A/V content of an event (e.g., sports, culture, entertainment, politics, news gathering, etc.) in a location where no 5G system infrastructure is available. We distinguish two deployment scenarios:

1) No MNO’s 5G system is available, i.e., neither 5G core network (5GC) nor 5G radio access network (NG-RAN) infrastructure is available

2) Only MNO’s 5GC is available

In the first deployment scenario, since neither 5GC nor NG-RAN infrastructure is available at the desired location, none of the three stakeholder models described in clause 4.1 are feasible. In fact, this deployment scenario would require a vertical 3rd party to deploy on demand the full network infrastructure necessary to set up a standalone non-public network at the desired location. In this contribution, we consider the case that the vertical 3rd party is an A/V production business and that it has the ability to deploy its own standalone non-public network to satisfy its communication requirements. Thus, the 5G local standalone network may follow a non-public network deployment and includes both core and access components.

However, for successful wireless communication not only network infrastructure but also access to radio spectrum is needed. The requirement for guaranteed QoS levels as described in [3] precludes the operation of the considered standalone non-public networks in licensed-exempt spectrum, mostly related to coexistence problems and targets instead access to exclusive licensed spectrum. Since no MNO is involved at the desired location, the vertical 3rd party deploying such a standalone non-public network needs to find an alternative way to access spectrum. One alternative way could be provided by the framework of evolved Licensed Shared Access [4], which extends the scope of the LSA licensees to include vertical 3rd parties as independent local communication service providers.

The first deployment scenario does not put any requirements on the 3GGP system. It is provided to illustrate the specific case where 3rd party network operators may need to deploy on demand standalone non-public networks – comprising both core and access components - at locations where no other 5G system infrastructure is available.

For the second deployment scenario, role model 2) in clause 4.1 can be leveraged. It is stated in that clause that from a 3GPP perspective, role model 2) does not change whether an MNO or a vertical 3rd party is involved, if the vertical 3rd party would operate its own network. Following this thinking, a suitable business relationship model for deployment scenario 2) is one in which a 3rd party deploys and manages at the required location anon-public network.

In addition, deployment scenario 2) aims to introduce new considerations regarding spectrum access for non-public networks. Deployment scenario 2) assumes that the involved MNO may be able to provide spectrum access and/or interference management services to non-public networks deployed by a 3rd party. Therefore, the non-public networks and the MNO Operations System need to be connected through appropriate standardized interfaces. This scenario is illustrated in Figure 5.5.1-1 and Figure 5.5.1-2.

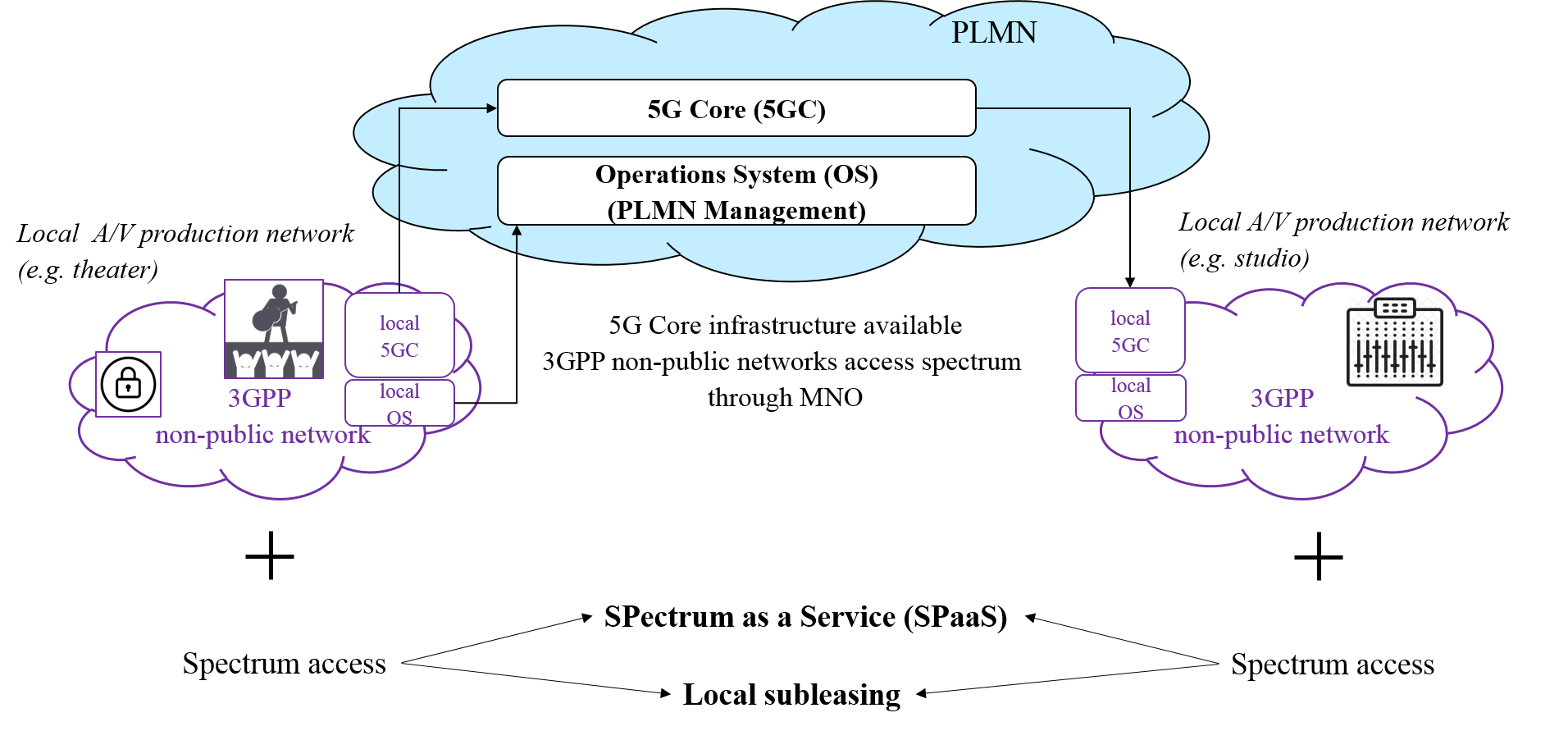


Figure 5.5.1-1: Two local A/V production networks deployed as 3GPP non-public networks and remotely connected over the 5G Core infrastructure of a PLMN

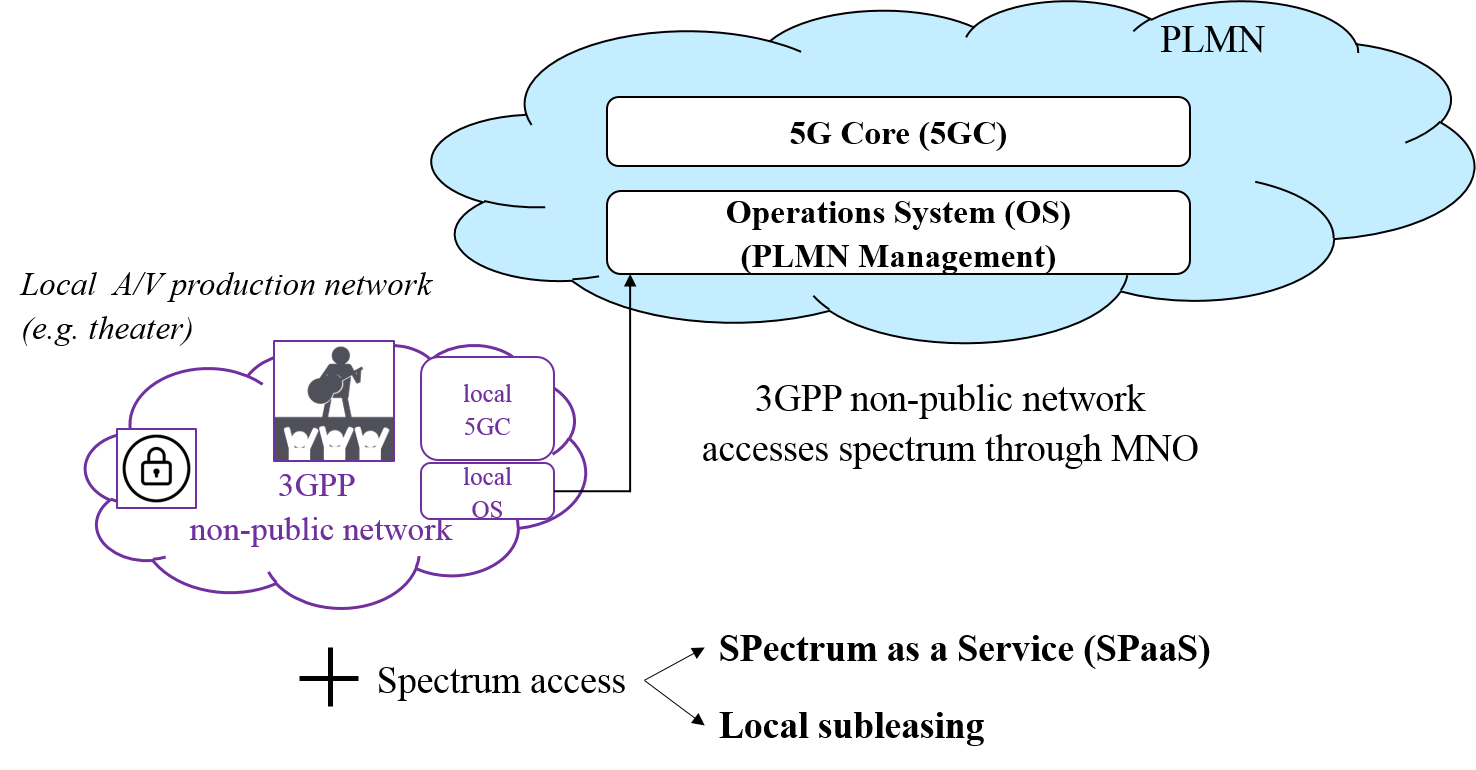


Figure 5.5.1-2: Local A/V network deployed as a 3GPP non-public network connected to the Operations System of a PLMN

As depicted in Table 5.5.1-1, deployment scenario 2 distinguishes two cases:

- Spectrum as a Service (SPaaS): MNO is willing to provide both spectrum access and automatic interference management services to a non-public network deployed by a vertical 3rd party and connected to the MNO’s Operations System through appropriate standardized interfaces.

- Local subleasing: MNO is willing to provide spectrum access service but no automatic interference management service to a non-public network deployed by a 3rd party and connected to the MNO’s Operations System through appropriate standardized interfaces. This case follows the concept of local sub-leasing described in [4].

Thus, the difference between the two models is whether the automatic interference management service is also offered by the MNO’s Operations System to the local A/V production network or not.

Table 5.5.1-1: Role model scenarios for stand-alone non-public network operation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Roles** | | **Business relationship models** | | |
| **Scenario 1**  **eLSA (note 1) Local Licensing** | **Scenario 2** | |
| **Spectrum as a Service (SPaaS)** | **Local Subleasing** |
| **Spectrum** | Owner | Incumbent(note 2) | MNO | MNO |
| Manager | eLC (note 3) | MNO | eLC (note 7) |
| **Infrastructure** | CORE | 3rd Party (note 4) | 3rd Party (note 4) and MNO | 3rd Party (note 4) |
| RAN | 3rd Party | 3rd Party | 3rd Party |
| **V/NFs** | CORE | 3rd Party (note 4) | 3rd Party (note 4) and MNO | 3rd Party (note 4) |
| RAN | 3rd Party | 3rd Party | 3rd Party |
| **Management** | CORE | 3rd Party (note 4) | 3rd Party (note 4) and MNO | 3rd Party (note 4) |
| RAN | 3rd Party | 3rd Party | 3rd Party |
| **Network User** (note 5) | Service | A/V Production business (note 5) | A/V Production business (note 5) | A/V Production business (note 5) |
| Service user | Consumers (note 6) | Consumers (note 6) | Consumers (note 6) |
| NOTE 1: evolved Licensed Shared Access (LSA)  NOTE 2: Incumbent may include MNOs  NOTE 3: evolved LSA controller  NOTE 4: As part of local RAN (embedded)  NOTE 5: Depending on the selected model, the A/V production business decides for which roles it would like to act as the 3rd Party.  NOTE 6: Consumer of the A/V application service can be e.g., the live audience of an event or the off-line audience listening/watching CDs/DVDs or downloading the post-produced content from a media center, etc.  NOTE 7: evolved LSA controller [4] as part of the MNO’s 5G system | | | | |

## 5.5.2 Potential requirements

[PR 5.5.2-1] The 3GPP system shall allow a 3rd party to connect non-public networks to an MNO’s Operations System through standardized interfaces.

[PR 5.5.2-2] The 3GPP system shall support MNOs to offer spectrum access and/or automatic configuration services (for instance, interference management) to non-public networks deployed by 3rd parties and connected to an MNO’s Operations System through standardized interfaces.

## 5.6 A/V production use cases relying on PLMN infrastructure

### 5.6.1 Description

Consider the case of an audio/video (A/V) production company producing professional live A/V content of an event (e.g., sports, culture, entertainment, politics, news gathering, etc.) in a location where 5G infrastructure is available.

We distinguish two deployment scenarios:

1) Fixed 5G installations, e.g., in a state theatre, stadium, convention centre, exhibition hall, etc.

2) Nomadic 5G installations, e.g., typical during a band tour or entertainment show hosting at several different cities

In both scenarios, it is assumed that 5G core network infrastructure is available at the desired locations. In the first scenario, the 5G access network infrastructure (5G-AN) is fixed installed at the desired location. In the second scenario, the 5G-AN infrastructure is installed on demand for the duration of the event in the desired locations. Any of the business relationship models 3b, 3c and 3d introduced in clause 4 of this TR are considered feasible in both scenarios, fixed or nomadic.

Table 5.6.1-1 illustrates each of the possible business relationships from the perspective of the A/V production business in charge of the event. The A/V production business should have the possibility to choose between any of the three business relationship models presented in Table 5.6.1-1. Depending on the selected model, the A/V production business should have again the possibility to decide for which roles it would like to act as the 3rd party.

Further note that in a typical vertical use case, the network users are not, as in typical MNO business, the subscribers of the MNO, but subscribers of the service application of the vertical use case, in this clause the A/V production business. In turn, the users of the A/V production business are the consumers, e.g., the live audience of an event or the off-line audience listening/watching CDs/DVDs or downloading the post-produced content from a media center, etc.

For all business relationship the A/V production network should be a 3GPP network that is not for public use and may interact with a PLMN. The A/V production network may be deployed as a network slice provided by an MNO or a vertical 3rd party.

For all business relationship models in Table 5.6.1-1 following aspects apply:

- In the case that the A/V production network is deployed as a network slice:

- The A/V production business trusts the MNO and any other 3rd party involved in its A/V production network slice to provide the agreed resources and functionality as described in [3].

- The privacy of communication within the A/V production network slice shall be ensured by the MNO and or any 3rd party involved.

- Either the MNO or the 3rd party providing the slice is responsible for ensuring isolation of the slice communications from the rest of its network. This includes only allowing authorized UEs to access the A/V production network slice and constraining authorized UEs to the authorized slice.

- Mutual sharing of assets (e.g., infrastructure, V/NFs) may be allowed between the 3rd party and the MNO.

In addition, for business relationship 3d the following features are required:

- The A/V production network contains both core and access components

- The 3GPP system shall support connection (plug-in) of 3rd party network infrastructure (i.e., physical/virtual network entities at RAN/core level) to a private slice.

Table 5.6.1-1: Feasible business relationship models for fixed & nomadic A/V production network scenarios

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Roles** | | **Business relationship models** | | |
| **Model 3b**  **A/V production network slice with limited control** | **Model 3c**  **A/V production network slice with extended control** | **Model 3d**  **A/V production network slice** |
| **Spectrum** | Owner | MNO | MNO | MNO |
| Manager | MNO | MNO | MNO |
| **Infrastructure (Physical)** | CORE | MNO | MNO | 3rd Party and MNO  (note 5) |
| AN | MNO | MNO | 3rd Party and MNO  (note 5) |
| **Virtual NFs**  **Provision** | CORE | MNO | 3rd Party and/or MNO | 3rd Party and MNO  (note 5) |
| AN | MNO | 3rd Party and/or MNO | 3rd Party and MNO  (note 5) |
| **Virtual NFs**  **Management** | CORE | 3rd Party (note 1) and/or MNO | 3rd Party and/or MNO | 3rd Party and MNO  (note 5) |
| AN | 3rd Party (note 1) and/or MNO | 3rd Party and/or MNO | 3rd Party and MNO  (note 5) |
| **Network User (note 2)** | Service | A/V Production business (note 3) | A/V Production business (note 3) | A/V Production business(note 3) |
| Service User | Consumers (note 4) | Consumers (note 4) | Consumers (note 4) |
| NOTE 1: V/NFs are managed via APIs exposed by the MNO.  NOTE 2: The network user is the A/V application service.  NOTE 3: Depending on the selected model, the A/V production business decides for which roles it would like to act as the 3rd Party.  NOTE 4: Consumer of the A/V application service can be e.g., the live audience of an event or the off-line audience listening/watching CDs/DVDs or downloading the post-produced content from a media center, etc.  NOTE 5: In this model, both a 3rd party and MNO provide and manage some of the virtual/physical infrastructure and V/NFs. | | | | |

## 5.6.2 Potential requirements

[PR 5.6.2-1] The 3GPP system shall provide suitable APIs to allow use of additional encryption mechanisms, provided by a trusted vertical 3rd party between any UE served by a private slice and a core network entity in that private slice.

[PR 5.6.2-2] The 3GPP system shall support a mechanism to prevent a UE from accessing a private slice it is not authorized to access.

[PR 5.6.2-3] The 3GPP system shall support a mechanism for a 3rd party to authenticate a UE for access to a private slice which is allocated to this 3rd party.

[PR 5.6.2-4] The 3GPP system shall provide suitable APIs to allow a 3rd party infrastructure (i.e., physical/virtual network entities at RAN/core level) to be part of a private slice.

## 5.7 Network slicing for Industry 4.0 verticals

### 5.7.1 Description

Based on an example described in [5], an Industry 4.0 factory owns and operates a non-public network for its communication needs and sole use. This network consists of multiple slices that allow specific needs to be met with different infrastructure. For example,

- slice A is able to meet specific KPIs for time critical functions for robotic manufacturing controls,

- slice B provides non-time critical IoT communications for various sensors and package tracking devices within the factory, and

- slice C is used for the employee communications services on their smartphones.

Each of these slices has separate core functions and radio resources available to avoid any competition for resources between the three types of devices. Due to the highly critical functions addressed by the robotic control slice A, UEs served by that slice have no interaction with a PLMN, even though both networks provide coverage in the same geographic area.

The factory owner contracts with a local MNO for two additional private slices.

- slice D that can interact with factory slice C for employee communications. This allows employees to access the factory communication service via the private slice when they are out of range of the factory radio resources. In this case, the private slice is based on the trust relationship model 3c where the 3rd party provides and manages some of the virtual/physical infrastructure and V/NFs, namely, access to the factory communication service. Only UEs of factory employees have access to MNO private slice D.

- slice E that provides IoT radio coverage for the sensors and tracking devices which occasionally move outside the building and outside the range of the radio resources of slice B. This MNO slice is restricted to a coverage area within a perimeter of the factory to avoid conflict with non-factory devices. This slice is also based on trust model 3c, with the factory providing the IoT supporting services. Devices using this slice are not authorized for use on the PLMN outside of slice E.

The slices in this scenario illustrate the trust needs between the Industry 4.0 vertical, or factory, and the MNO. In the case of slice A, a strict separation is enforced, such that no interaction between that slice and the PLMN is possible. In the case of slices C and D for employee communications, the MNO must provide appropriate security measures and APIs to ensure the factory system cannot negatively impact the rest of the network outside of slice D and ensure that only UEs belonging to the factory are able to access slice D. The factory owner must provide appropriate security measures to protect any proprietary information carried over slice D.

The IoT slices B and E require similar protective actions on behalf of both the MNO and factory, with a clear distinction that the IoT devices accessing MNO provided slice E also be constrained against accessing any other part of the PLMN.

To ease such security concern, reduce the factory owner's burden on network operation, and realize a smoother network operation, an alternative to deploy slices A to E is for an MNO to act as an integrator that provides a certain level of network operation that covers slices A to C as well, while keeping the factory owner's ownership to them and supporting the factory owner's capability to manage those slices via APIs.

### 5.7.2 Potential requirements

[PR 5.7.2-1] Subject to an agreement between the operators/service providers, operator policies and the regional or national regulatory requirements, the 5G system shall support intersystem mobility between a network slice in a non-public network and a PLMN.

[PR 5.7.2-2] A 5G system shall support a mechanism to limit slice radio coverage to a specific geographic area.

[PR 5.7.2-3] A 5G system shall support a mechanism to associate a UE with one or more slices such that the UE is not authorized to receive service from any other network or slice.

[PR 5.7.2-4] A 5G system shall be able to bar UEs from trying to access a network slice they are not authorized to receive service from.

[PR 5.7.2-5] Subject to an agreement between a PLMN and a 3rd party, a 5G system shall be able to allow the PLMN to authenticate and authorize UEs for the usage of the 3rd party's own 3GPP network and to operate it in combination with their private slice(s) in the PLMN.

[PR 5.7.2-6] A 5G system shall be able to allow a PLMN to provide suitable APIs to enable the 3rd party to manage its own 3GPP network and its private slice(s) in the PLMN in a combined manner.

## 5.8 End-to-end asset tracking

### 5.8.1 Description

Current and emerging production processes require continuous tracking of workpieces and goods. Complex goods are often produced and assembled at different sites. 5G networks can enable continuous asset tracking of workpieces (end-to-end asset tracking). Some parts of the end-to-end asset tracking may be deployed through private slices. Figure 5.8.1-1 illustrates such a scenario.



Figure 5.8.1-1: Example of end-to-end asset tracking by use of 5G networks and private slices

A workpiece is tracked in factory A. A wireless 5G UE is used for tracking. This UE is connected to the private slice of factory A. The private slice is provided as a dedicated network slice for use by factory A. The private slice is provided by an MNO, and it is part of a PLMN (PLMN 1).

The workpiece is transported from factory A to factory B. As soon as the 5G UE of the workpiece loses connectivity to the private slice of factory A, it connects to the 5G PLMN 2 in order to continue to provide asset-tracking information (e.g., its location) to the asset tracking application in factory A.

When the 5G UE of the workpiece gets into the connectivity range of factory B, it disconnects from the PLMN and connects to the network slice for asset tracking in the non-public network of factory B. The 5G network of factory B deploys one or more network slices.

Other examples for the deployment of end-to-end asset tracking by use of 5G networks and network slices are shown in Figure 5.8.1-2 and Figure 5.8.1-3.



Figure 5.8.1-2: Example of end-to-end asset tracking by use of geographically constrained private slice



Figure 5.8.1-3: Example of end-to-end asset tracking by use of private slice throughout the PLMN

Position of the workpiece with the asset tracking UE is monitored in a uniform way, independent of the 5G network or network slice the UE is connected to.

The time-stamps of the asset-tracking information use the same time base throughout all visited 5G networks/slices.

Corresponding credentials for the different 5G networks will be used for authorisation and authentication.

Since the information sent back to the factory can be quite sensitive, encryption of the information is required. Commonly, UEs used for asset tracking are energy constrained, which is why OTT security often is not an option and network encryption usually is relied on. The operators of the factories need an assurance that network security is switched on (and what kind). This assurance can be provided through suitable monitoring mechanisms.

### 5.8.2 Potential Requirements

[PR 5.8.2-1] The 3GPP system shall enable communication service continuity between network slices of non-public networks and 5G PLMNs if a 5G UE moves from a non-public network to a 5G PLMN or vice versa.

[PR 5.8.2-2] The 5G system shall support a mechanism to enable uniform monitoring of the position of the asset-tracking UE independent of the network (slice) it is connected to.

[PR 5.8.2-3] The 5G system shall support a mechanism to provide time stamps with a common time base at the monitoring API, across the different network slices and 5G networks.

[PR 5.8.2-4] The 5G system shall be able to expose the information of the enabled security mechanisms of a UE to an authorised user for logging and auditing purposes.

## 5.9 Network slicing roles in (off-shore) wind farm

### 5.9.1 Description

Several roles for network slicing can be inferred from use cases for wind power plant networks, especially for off-shore or remote wind farms. The use case “Customised access of stakeholders to wind power plant network” in [3] details pertinent usage scenarios.

The wind power plant communication network is realised by a 5G system, i.e., a 5G core network and base stations at each wind turbine. The base stations enable wireless communication in their vicinity, e.g., to UEs in helicopters. The wind turbine networks and the local control centre are part of the wind power plant communication network. Moreover, the local control centre connects to a remote service centre, e.g., through the core of a PLMN. The network structure is illustrated in Figure 5.9.1-1.



Figure 5.9.1-1: Example of a communication network for a wind power plant

The wind power plant communication network is deployed as a non-public network. This network consists of at least one slice. The operator of the network can be a PLMN MNO or, for instance, the wind farm operator or grid operator. The operator of the wind power plant communication network has full control over the operation of the network, including the definition, instantiation, configuration, and operation of any network slices. The operator also manages the subscriber data base for this non-public network.

The remote service communication between the local control centre in the wind power plant communication network and the remote service centre uses one or more PLMNs. If more than one PLMN is involved, the private slices in the different PLMNs are connected by suitable mechanisms and APIs.

The main objective of the wind power plant communication is to provide customised access for different stakeholders to the applications in a wind power plant. The setup of the communication services with different service requirements is dynamic.

The applications are very diverse. They range from monitoring of sensor data (e.g., collection of sensor data at local control centre) over audio and video surveillance (local at wind turbine and between wind turbine and local control centre) to control applications for controlling the wind turbine operation (locally, from local control centre, and from remote service centre). Most of these applications require dependable communication, control applications require URLLC.

Network slicing enables the assurance of demanding QoS requirements such as low latency, high dependability, and high communication service availability. Network slicing ensures that the not so demanding communication services do not disturb the communication services with high, demanding requirements such as URLLC. Communication services with similar characteristics might be clustered in network slices. However, the operator of the wind power plant communication network might assign select communication services to separate network slices in order to enforce strict isolation between them (one communication service per network slice).

An important use of network slices is the separation of the different users (3rd parties) of the wind power plant communication network. Besides the operator of the wind power plant communication network, there are several external stakeholders that require temporary or continuous access to the network, e.g., grid regulation signalling and grid pricing, external maintenance and helicopter companies. Often, this access is restricted to certain parts of the wind power plant communication network, e.g., a select subset of the UEs attached to this network. The UEs are assigned to corresponding network slices in order to enforce the separation of the different users.

The network slices will be monitored via suitable APIs such as network slice status, slice KPIs, UEs connected to the network slice, etc.

The so-called wind turbine network requires special network slicing roles. It is part of the wind power plant communication network and it contains all network devices of a single wind turbine (see Figure 5.9.1-1). Each wind turbine has a local wind turbine controller for autonomous operation of the wind turbine (in case the connectivity to the local control centre is lost). Furthermore, certain activities on a wind turbine such as maintenance work require network slices restricted to (a subset of) devices of the wind turbine.

External stakeholders have to get access to certain UEs of the wind power plant communication network. Network slices will be set up in order to separate the external stakeholders from the other communication services of the wind power plant communication network (for instance, from the control application of the wind farm). Furthermore, the access to the network slice has to be restricted to the necessary UEs.

The setup of network slices has to be dynamic and automatic (for instance, if on-site maintenance personnel connects to the wind turbine network wirelessly for performing test procedures).

Several network slices of the wind power plant communication network may extend through a PLMN to the remote service centre (network slices for sensor information, monitoring information, data analytics information).

### 5.9.2 Potential requirements

[PR 5.9.2-1] For autonomous operation in case connectivity inside the network slice is lost, the 3GPP system shall be able to continue operation in unaffected parts of the network slice.

[PR 5.9.2-2] The 3GPP system shall be able to setup and operate network slices constrained to a subarea of the 5G network, that can autonomously operate even if connectivity to the other parts of the 5G network is lost.

[PR 5.9.2-3] The 3GPP system shall provide suitable APIs for additional 3rd party authorisation and authentication for controlling the access to network slices.

[PR 5.9.2-4] The 3GPP system shall be able to bar UEs from trying to access a network slice they are not authorized to receive service from.

[PR 5.9.2-5] The 3GPP system shall be able to provide network slices through multiple 5G networks so that select communication services of the non-public network can be extended through a PLMN. The 3GPP system shall provide suitable APIs for this.

## 5.10 Private slice management

### 5.10.1 Description

A business wants to have a diversity of network functionality and capabilities that meets its business requirements. In this case, a mobile network operator can provide a private slice by means of provisioning it that meet the agreed KPIs. Furthermore MNO can agilely provide a customized network slice for their customers (e.g., enterprise), as a service, which is called NSaaS as shown in TS 28.530. This service allows the customer to use and optionally manage the private slice. There are two trust relationships between MNOs and 3rd parties based on the management role models.

The criteria for the private slice management include the following:

- The network function/slicing management function(s) of MNO can create and manage a private slice. The network function/slicing management function(s) of 3rd party provides to the MNO information required to create private slice.

- The network function/slicing management function(s) of 3rd party can create and manage some component of a private slice. It provides to the network function/slicing management function(s) of MNO information related to created private slice.

Usually, network slices are provided with different compositions to the businesses which may involve different management responsibilities and network slice provisioning procedures for MNO and the 3rd party. MNO need clearly understand what businesses want from a network and can set adequate SLA according to the business requirements. As every business has its own priorities (some value bandwidth more than response times and vice versa), if directly providing private slice management, the 3rd party can get exactly the amount of performance and features it requires.

The trust relationships in this scenario include the following aspects.

- The 3rd party trusts the MNO to provide the agreed private slice management needed by the business.

- The 3rd party may directly manage the private slice via suitable APIs provided by MNO.

### 5.10.2 Potential requirements

[PR 5.10.2-1] The 3GPP system shall provide suitable APIs to allow the 3rd party to create and manage a private slice, subject to an agreement between the 3rd party and the MNO.

## 5.11 Management of network selection information in (off-shore) wind farm

### 5.11.1 Description

This role model scenario belongs to the same usage scenario as clause 5.9, i.e. an (off-shore) wind farm.

The 5G network that supports maintenance and operation activities within a wind farm is deployed as a non-public network. This non-public network is hosted by a PLMN (henceforth referred to as PLMN1). The UEs—including their network selection information—are managed by the wind farm operator. Service continuity of select communication services—for instance transmission of video streaming from a maintenance helicopter to the maintenance ships in the wind farm area—is provide even if the helicopter temporarily leaves the coverage area of the non-public network.

One of the concerns behind this scenario is that the users of non-public networks hosted by PLMNs do not want to update the network selection information in their UEs in cases the host PLMN or the associated roaming PLMN is changed. Such an update is unwanted since it could lead to interruptions in productivity, the need for new certification, high administration efforts, etc. A single state-of-the-art wind turbine may host up to 3000 sensors that provide input to the turbine controller, and some of them are in places that are difficult to reach.

In order to simplify this role model scenario in the example provided below, it is assumed that service continuity outside the perimeters of the non-public network is initially provided by PLMN1.

At some point, the wind farm makes an operational change in their network and the non-public network is no longer hosted by PLMN1. One option for the wind farm is to have the non-public network hosted by another PLMN. Another option is for the wind farm to realise the non-public network with 3GPP hardware owned and operated by the wind farm operator. In neither case, a change to the network selection information stored in the non-public-network UEs is necessary

### 5.11.2 Potential requirements

[PR 5.11.2-1] The 5G system shall support a change of host of a non-public network from one PLMN to another PLMN without changing the network selection information stored in the UEs of the non-public network.

# 6 Considerations

## 6.1 Considerations on security

The 5G system shall provide suitable APIs to allow use of a trusted 3rd party provided encryption between an authorized UE served by a private slice and a network entity within that private slice.

Subject to an agreement between an MNO and a 3rd party, a 5G system shall support a mechanism for the PLMN to authenticate and authorize UEs for access to both the 3rd party's own non-public network and private slice(s) of the PLMN associated with the 3rd party.

The 5G system shall provide suitable APIs for additional authorisation and authentication provided by a trusted 3rd party for controlling the access to private slices.

## 6.2 Considerations on performance

Network slicing as an enabling capability is foundational for a variety of roles dependent on business models. The notion of a collection of functions and resources that constitute a given network slice is a building-block for virtualization.

Since service categories have diverse quality of service profiles and configurability options for a network slice, it would be useful to adapt the realization of a network slice to meet the established key performance targets. Such configuration choices would enable performance improvements, such as latency reduction, minimization of faults, and overall robustness.

From an end-to-end perspective, impact of any performance degradation in a virtualized core network and/or access network will need to be minimized to meet the agreed KPIs (Key Performance Indicators) [2].

Network slice performance studies are important for an assessment of the system-level KPIs (e.g., availability, reliability, latency, mobility, retainability, user experience, coverage, and capacity). Consistency in network slice performance is vital for supporting the service demands associated with different market scenarios and service-level agreements, based on business models and stakeholder requirements.

The performance aspects of network slicing are to be studied in terms of optimization and configurable arrangements.

# 7 Consolidated potential requirements

## 7.1 General

The 5G system shall support MNOs to offer spectrum access and/or automatic configuration services (for instance, interference management) to non-public networks deployed by 3rd parties and connected to an MNO’s Operations System through standardized interfaces.

The 5G system shall provide a mechanism to enable an MNO to operate a non-public network and private slice(s) of the PLMN associated with the 3rd party in a combined manner.

The 5G system shall support a mechanism to enable monitoring of the position of a UE independent of the network or network slice it is connected to.

The 5G system shall support a change of host of a non-public network from one PLMN to another PLMN without changing the network selection information stored in the UEs of the non-public network.

## 7.2 Service exposure

The 5G network shall provide suitable APIs to allow a trusted 3rd party to monitor the status (e.g., locations, lifecycle, registration status) of its own UEs when served by its private slice.

NOTE: The number of UEs could be in the range from single digit to tens of thousands.

The 5G network shall provide suitable APIs to allow a trusted 3rd party to get the network status information of a private slice dedicated for the 3rd party, e.g., the network communication status between the slice and a specific UE.

The 5G system shall support APIs to allow the non-public network to be managed by the MNO’s Operations System.

The 5G system shall provide suitable APIs to allow 3rd party infrastructure (i.e., physical/virtual network entities at RAN/core level) to be used in a private slice.

A 5G system shall provide suitable APIs to enable a 3rd party to manage its own non-public network and its private slice(s) in the PLMN in a combined manner.

The 3GPP system shall provide suitable APIs to allow the 3rd party to create and manage a private slice, subject to an agreement between the 3rd party and the MNO.

## 7.3 Network slice constraints

The 5G system shall support a mechanism to prevent a UE from trying to access a radio resource dedicated to a specific private slice.

The 5G system shall support a mechanism to limit slice radio coverage to a specific geographic area.

The 5G system shall support a mechanism to limit a UE to only receiving service from an authorized slice.

## 7.4 Cross-network slice coordination

The 5G system shall support a mechanism to provide time stamps with a common time base at the monitoring API, for services that cross multiple network slices and 5G networks.

The 5G system shall provide suitable APIs to coordinate network slices in multiple 5G networks so that the selected communication services of a non-public network can be extended through a PLMN (e.g., the service is supported by a slice in the non-public network and a slice in the PLMN).

## 7.5 Slice fault tolerance

The 5G system shall support full functionality in a private slice even when connectivity to the PLMN is not available.

# 8 Conclusion and recommendations

The study has analysed a number of use cases supporting use of private slices provided by an MNO on behalf of a 3rd party. The use cases highlight various business role models and trust relationships that will need to be supported by a 3GPP system in order to support private slices and identify potential requirements to provide that support. The resulting potential requirements and considerations on security and performance have been consolidated in clauses 6 and 7 of the TR,

The content of clauses 6 and 7 should be considered as the basis of normative Rel-16 requirements to support private slices.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2017-11 | SA1#80 | S1-174285 |  |  |  | Agreements in SA1#80: S1-174110, S1-174112, S1-174361, S1-174536, S1-174537, S1-174375, S1-174538  And rapporteur’s clean up. | 0.1.0 |
| 2018-02 | SA1#81 | S1-180253 |  |  |  | Agreements in SA1#81: S1-180055, S1-180382. S1-180383, S1-180573, S1-180575, S1-180622, S1-180623  And rapporteur’s clean up. | 0.2.0 |
| 2018-05 | SA1#82 | S1-181293 |  |  |  | Agreements in SA1#82: S1-181502, S1-181503, S1-181507, S1-181553, S1-181554, S1-181555, S1-181557, S1-181558, S1-181725  And rapporteur’s clean up. | 0.3.0 |
| 2018-05 | SA#80 | SP-180338 |  |  |  | MCC Clean-Up for presentation for information to SA | 1.0.0 |
| 2018-08 | SA1#83 | S1-181xxx |  |  |  | Agreements in SA1#83: S1-182143. S1-182457, S1-182458, S1-182708, S1-182709, S1-182710, S1-182713, S1-182714, S1-182761, S1-182762  And rapporteur’s clean up. | 1.1.0 |
| 2018-09 | SA#81 | SP-180779 |  |  |  | Raised to v.2.0.0 for presentation for approval to SA | 2.0.0 |
| 2018-09 | SA#81 | SP-180779 |  |  |  | Raised to v.16.0.0 following SA's approval | 16.0.0 |
| 2018-12 | SP-82 | SP-181017 | 0001 |  | F | Completion of consolidation potential requirements | 16.1.0 |
| 2018-12 | SP-82 | SP-181017 | 0002 | 2 | F | Replacing tenant with 3rd party | 16.1.0 |