|  |  |
| --- | --- |
| 3GPP TR 22.848 V0.3.0 (2023-11) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Interconnect of SNPN;  (Release 19) | |
|  | |
|  |  |
| 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 Specification 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. | |

|  |
| --- |
|  |
| ***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.  © 2023, 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 4

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Abbreviations 5

4 Overview 6

5 Use cases 6

5.1 Use case on Scalable SNPN Interconnect with dynamic connections 6

5.1.1 Description 6

5.1.2 Pre-conditions 7

5.1.3 Service Flows 7

5.1.4 Post-conditions 8

5.1.5 Existing features partly or fully covering the use case functionality 8

5.1.6 Potential New Requirements needed to support the use case 8

5.2 Use case on Interconnect between SNPNs 9

5.2.1 Description 9

5.2.2 Pre-conditions 11

5.2.3 Service Flows 11

5.2.4 Post-conditions 11

5.2.5 Existing features partly or fully covering the use case functionality 11

5.2.6 Potential New Requirements needed to support the use case 11

5.3 Use case on interconnection of standalone naval non-public networks 12

5.3.1 Description 12

5.3.2 Pre-conditions 13

5.3.3 Service Flows 13

5.3.4 Post-conditions 13

5.3.5 Existing features partly or fully covering the use case functionality 13

5.3.6 Potential New Requirements needed to support the use case 13

5.4 Use case on mobility in a group of interconnected standalone naval non-public networks 14

5.4.1 Description 14

5.4.2 Pre-conditions 15

5.4.3 Service Flows 15

5.4.4 Post-conditions 15

5.4.5 Existing features partly or fully covering the use case functionality 15

5.4.6 Potential New Requirements needed to support the use case 15

5.5 Use case on quality of service differentiation and resource prioritization in a group of interconnected standalone naval non-public networks 16

5.5.1 Description 16

5.5.2 Pre-conditions 16

5.5.3 Service Flows 16

5.5.4 Post-conditions 17

5.5.5 Existing features partly or fully covering the use case functionality 17

5.5.6 Potential New Requirements needed to support the use case 17

6 Consolidated requirements 18

6.1 General 18

6.2 Consolidated requirements for enabling of SNPN cellular hotspots 18

7 Conclusions and recommendations 18

Annex A (informative): Change history 19

# 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 describes use cases and aspects related to interconnect between SNPNs and interconnect of SNPN with identity providers that authenticate and authorize UE access to the SNPNs.

Potential service requirements are derived for these use cases and are consolidated in a dedicated chapter.

In addition, this document also includes a gap analysis between existing requirements for SNPN and the requirements that can be satisfied to enable interconnect between SNPNs and to enhance interconnect of SNPNs with identity providers that authenticate and authorize UE access to the SNPNs.

The report ends with recommendations regarding the continuation of the work.

NOTE: There is no requirement for a PLMN to enhance their interconnect with SNPNs or operate an identity provider.

# 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".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms 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].

**SNPN Credential Provider:** Entity within the 5G system that creates and manages identity information and provides authentication services for those identities for the purpose of accessing a SNPN

NOTE: The SNPN Credential Provider can also authorize access to a non-public network for a subscriber associated with an identity handled by this SNPN Credential Provider.

**Interconnect:** interaction between two SNPNs, or between a SNPN and a SNPN Credential Provider, allowing users subscribed to one SNPN (or to the SNPN Credential Provider) to use the other SNPN

**Standalone Non-Public Network:** an NPN that does not rely on network functions provided by a Public Land Mobile Network (PLMN)

## 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].

SNPN Standalone Non-Public Network

# 4 Overview

The present document captures a set of use cases and potential service requirements related to the following topics:

1. Interconnect of SNPN with SNPN Credential providers that authenticate and authorize UE access to the SNPNs.
2. Interconnect between SNPNs

# 5 Use cases

## 5.1 Use case on Scalable SNPN Interconnect with dynamic connections

### 5.1.1 Description

This use case relates only to SNPNs that provide services in a similar way as provided by WLAN hotspots.

Today's PLMNs have a centralized database of IP addresses of all operator nodes that connect to the inter-PLMN IP backbone network, including AAA Servers/Proxies. This information is used for firewall and Border Gateway configuration. Signalling connections between VPLMN and HPLMN are long-lived (Diameter and HTTP-based N32f) and support bidirectional (inbound and outbound) signalling.

In contrast, there is no administrative entity that manages the interconnect of SNPNs on one hand and SNPN Credential Providers on the other hand. In addition, the number of interconnected SNPNs and SNPN Credential Providers is expected to be considerably greater than the number of PLMNs today. Given the large number of SNPN Credential Providers with which a SNPN needs to interconnect, it is not feasible to maintain permanently established signalling connections between them. Instead, the signalling connection needs to be established dynamically. Ideally, a signalling connection between SNPN A and SNPN Credential Provider B should be established only when a subscriber of SNPN Credential Provider B attempts to connect to SNPN A, and should be released when the last subscriber of SNPN Credential Provider B disconnects from SNPN A.

The dynamic establishment of a signalling connection between the SNPN and the SNPN Credential Provider raises several new issues, as follows:

- **Outbound signalling issue**: The SNPN might not know the IP address of the SNPN Credential Provider’s signalling endpoints and vice versa. In some cases, the SNPN Credential Provider may be operated using a cloud provider using dynamic IP address assignment.

- **Inbound signalling issue**: The SNPN and/or the SNPN Credential Provider may reside behind a firewall or a Network Address Translation (NAT) device.

- **End-to-end signalling issue**: The SNPN and/or the SNPN Credential Provider need to have assurance that they are indeed establishing a signalling connection with each other and that the signalling connection is secure.

The issues related to dynamic establishment of a signalling connection between the SNPN and the SNPN Credential Provider are illustrated in Figure 5.1.1-1.



**Figure 5.1.1-1: Issues with dynamic establishment of signalling connection between SNPN and SNPN Credential Provider**

### 5.1.2 Pre-conditions

1) NetAbove is an Internet service provider that operates SNPNs and serves as a SNPN Credential Provider. As part of the subscription contract, NetAbove allows its subscribers to connect to SNPNs owned by a variety of companies (e.g., hospitality and convention centres, airports, government institutions, schools, restaurants, coffee shops, etc.).

2) NetAbove serves as a SNPN Credential Provider that can authenticate and authorize its subscriber when the subscriber attempts to connect to a SNPN.

3) NetAbove does not have a direct agreement with any of these SNPNs and instead relies on a third party that assists the interconnect of entities affiliated with this third party for the purpose of subscriber authentication and authorization.

4) Kaffa Koffee has launched a chain of coffee shops across the country. Each coffee shop is equipped with a small SNPN allowing customers to access Kaffa Koffee’s private entertainment system, in addition to providing Internet access.

5) Kaffa Koffee’s customers get free access to the entertainment system on the condition that they can assert an identity that can be authenticated by a supported SNPN Credential Provider.

6) A wide variety of companies can take the role of SNPN Credential Providers (e.g., mobile operators, other SNPNs). Kaffa Koffee does not have a direct agreement with any of these SNPN Credential Providers and instead relies on a third party that assists the interconnect of entities affiliated with this third party for the purpose of subscriber authentication and authorization.

7) BananaFed is a third party that assists the interconnect of entities affiliated with this third party for the purpose of subscriber authentication and authorization.

8) NetAbove and Kaffa Koffee both are affiliated with BananaFed.

### 5.1.3 Service Flows

1) Roy is a subscriber of NetAbove.

2) Roy is visiting a Kaffa Koffee shop and wants to access Kaffa Koffee’s famous entertainment system using his 5G-capable laptop.

3) Using the connection manager on his laptop, Roy selects his NetAbove subscription credentials for connection to Kaffa Koffee’s SNPN.

4) Kaffa Koffee’s SNPN has no direct signalling connection with NetAbove. In order to authenticate the request coming from Roy’s laptop, Kaffa Koffee’s SNPN turns to BananaFed, a third party, for assistance. Both NetAbove and Kaffa Koffee are affiliated with BananaFed.

5) NetAbove’s SNPN Credential Provider server resides in NetAbove’s administrative IP domain and is located behind a firewall.

6) With BananaFed’s assistance, the Kaffa Koffee’s SNPN is able to forward the outbound authentication request to a SNPN Credential Provider server that is owned by NetAbove, even though Kaffa Koffee’s SNPN has no prior knowledge of the IP address of any NetAbove’s SNPN Credential Provider servers.

7) With BananaFed’s assistance, the NetAbove’s SNPN Credential Provider server is able to receive the inbound authentication request originated by Kaffa Koffee’s SNPN even though it is located behind a firewall.

8) With BananaFed’s assistance, the Kaffa Koffee’s SNPN and NetAbove’s SNPN Credential Provider server get assurance that they are establishing a secure connection with the intended remote party.

9) Kaffa Koffee’s SNPN succeeds in authenticating Roy with the SNPN Credential Provider server at NetAbove.

10) NetAbove’s SNPN Credential Provider server desires to be informed when Roy disconnects from Kaffa Koffee’s SNPN. With BananaFed’s assistance, NetAbove’s SNPN Credential Provider server is able to forward the outbound subscription request to the SNPN operated by Kaffa Koffee, even though Kaffa Koffee’s SNPN is located behind a NAT device.

### 5.1.4 Post-conditions

1) Once Roy’s laptop is connected to the Kaffa Koffee’s SNPN network, Roy can enjoy access to Kaffa Koffee’s entertainment system and access to the Internet.

2) After some time, Roy disconnects gracefully from Kaffa Koffee’s SNPN and the disconnection event is signalled to NetAbove’s SNPN Credential Provider server.

### 5.1.5 Existing features partly or fully covering the use case functionality

None. The existing interface for interconnect between SNPN and SNPN Credential Provider (aka Credentials Holder) relies on permanent signalling connection between the SNPN and the SNPN Credential Provider.

### 5.1.6 Potential New Requirements needed to support the use case

[PR 5.1.6-001] Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for a SNPN to be able to interconnect with a large number of SNPN Credential Providers with which the SNPN might not have preconfigured information detailing the IP addresses used by these SNPN Credential Providers to interconnect with the SNPN.

[PR 5.1.6-002] Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for a SNPN Credential Provider to be able to interconnect with a large number of Standalone Non-Public Networks (SNPNs) with which the SNPN Credential Provider might not have preconfigured information detailing the IP addresses used by these SNPNs to interconnect with the SNPN Credential Provider.

[PR 5.1.6-003] Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for a SNPN to be able to determine how to connect to a SNPN Credential Provider capable of verifying the identity presented by a user attempting to connect to that SNPN.

[PR 5.1.6-004] Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for a SNPN to be able to securely interconnect with a SNPN Credential Provider in deployments where the required security information is not preconfigured.

[PR 5.1.6-005] Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for a SNPN to enable a SNPN Credential Provider to securely notify events (e.g., a user’s subscription ending) to the Standalone Non-Public Network (SNPN).

## 5.2 Use case on Interconnect between SNPNs

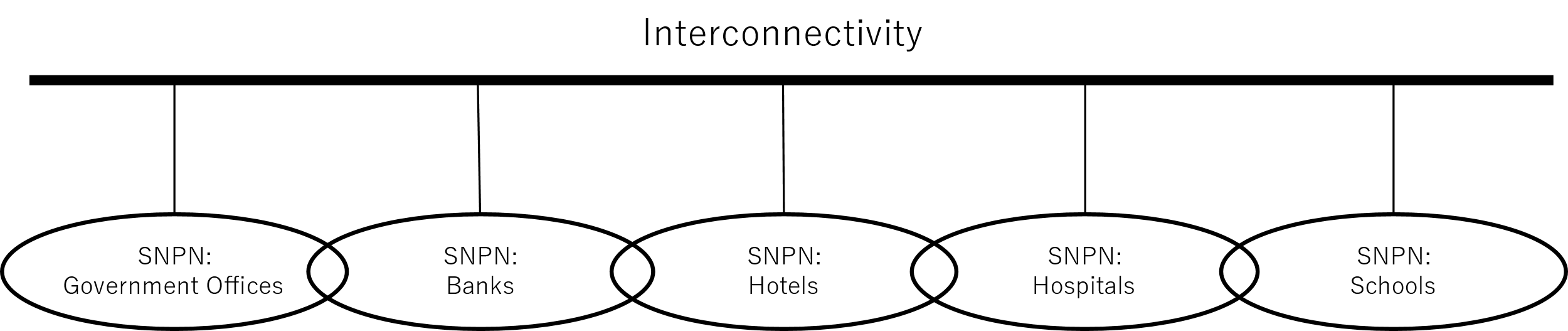
### 5.2.1 Description

SNPNs are expected to be deployed in government offices, banks, hotels, hospitals, schools, etc. in an administrative area. Each SNPN exposes its localized services.

Interconnect between different SNPN, subject to appropriate agreements, can make access to localized services seamless. Namely, when SNPNs, deployed by different administrations, are interconnected with each other and their services exposed, local services of one SNPN can be accessed via the other SNPNs. For example, a medical service, instantiated on a SNPN deployed in a central hospital, can be exposed to distributed family clinics. Also, an identity created in a family clinic can be utilized at the central hospital.

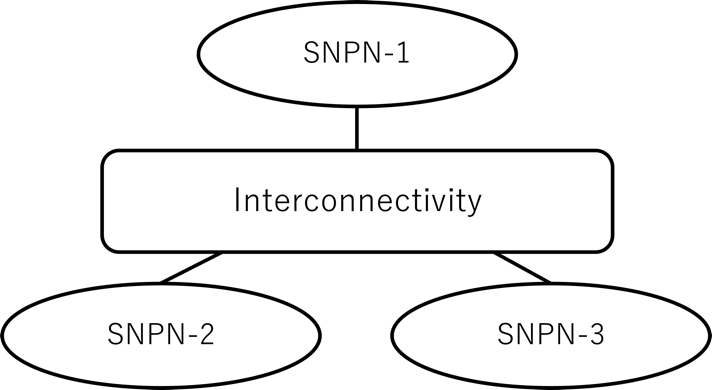
A benefit of the interconnect between SNPN can also be seen when a disaster happens, where PLMN-based service become unavailable due to congestion caused by the disaster in the area. On the other hand, as SNPNs are basically isolated from the PLMNs, the SNPNs are not impacted by the congestion in the PLMNs. This is, for example, good for city governments because the city government can keep their public services over the interconnected SNPNs.

In the context of interconnected SNPNs, identity providers authenticate individual users in SNPNs and authorize them to consume services on the SNPNs.



**Figure 5.2.1-1: Interconnect between SNPNs**

Assume that multiple SNPNs, for example, SNPN-1, SNPN-2 and SNPN-3, are deployed at different places. In Figure 5.2.1-2, SNPN-1 is the central SNPN and SNPN-2 and SNPN-3 are branches. It is also expected that there is a backbone/transport network to provide interconnectivity among SNPN-1, SNPN-2 and SNPN-3. The backbone network could be a public network (e.g. The internet) or a private/ managed network (e.g. enterprise network owning the SNPNs).

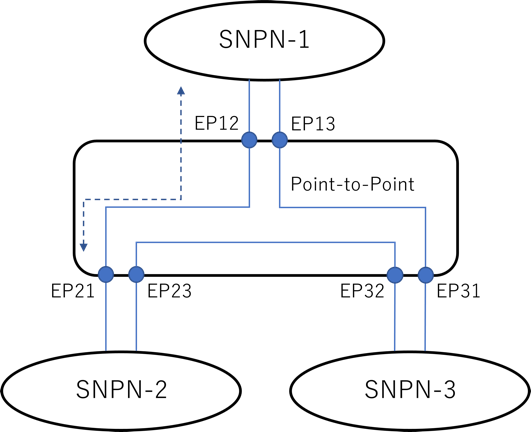


**Figure 5.2.1-2: Overview of interconnect**

Following interconnectivity can be considered but the list is not exhaustive.

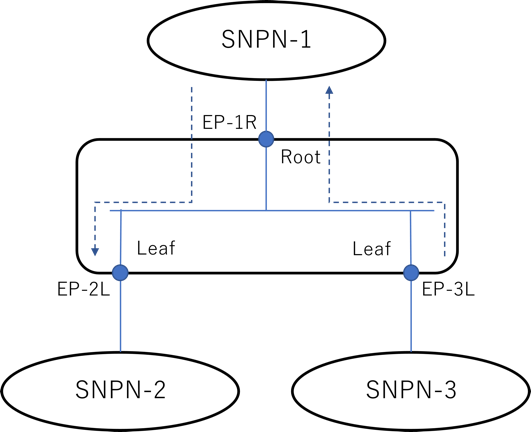
1. Point-to-point interconnectivity that connects a point with another point.
2. Hub & Spoke interconnectivity that connects a root point with other leaf points.
3. Gateway interconnectivity that connects multiple points with other multiple points with a full mesh topology

In a case where a pair of point-to-point interconnectivity in Figure 5.2.1-3 is deployed between SNPN-1 and SNPN-2 and between SNPN-2 and SNPN-3, the interconnectivity has 6 interconnectivity endpoints. Each of SNPN-1, SNPN-2 and SNPN-3 uses 2 interconnectivity endpoints to reach to other SNPNs. As for a traffic destined from a SNPN to another SNPN, each SNPN should manage which route is reached to another a SNPN (e.g. EP12 hosting SNPN-1 supports a point-to-point connectivity to EP21 hosting SNPN-2).



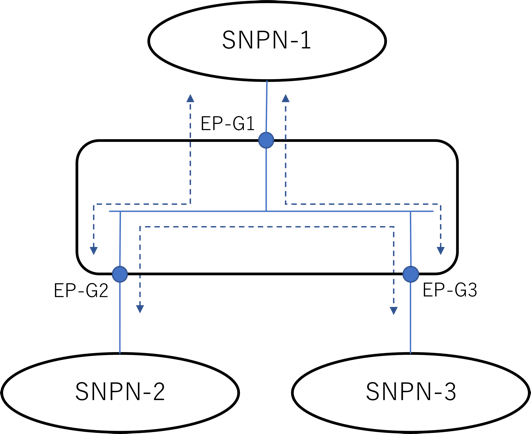
**Figure 5.2.1-3: point-to-point connectivity**

In a case where hub & spoke interconnectivity in Figure 5.2.1-4 is deployed among SNPN-1, SNPN-2 and SNPN-3, internal traffic among interconnectivity endpoints transferred via the root endpoint. For example, a central hospital provides SNPN-1, whereas family clinics #2 and #3 are consumers of SNPN-2 and SNPN-3, respectively. As assumed that SNPN-1 is the central SNPN, SNPN-1 can also provide identity services. For example, the internal traffic from EP-3L hosting SNPN-3 is transferred to SNPN-1 via EP-1R and then SNPN-1 routes the traffic from EP-1R to EP-2L hosting SNPN-2. It should be noted that an identity provider service could also be located in the external data network connecting to SNPN-1.



**Figure 5.2.1-4: Hub & spoke connectivity**

In a case where gateway interconnectivity in Figure 5.2.1-5 is deployed among SNPN-1, SNPN-2 and SNPN-3, internal traffic among interconnectivity endpoints transferred between each interconnectivity endpoint. Each SNPN can communicate with each other via the gateway interconnect service. For example, services such as an identity provider service could directly be interfaced with the interconnectivity. In this case, the identity provider service can seamlessly be consumed via any SNPNs and an identity assigned with a user can be authenticated and authorized in any SNPN.



**Figure 5.2.1-5: Gateway connectivity**

An interconnectivity (e.g. point-to-point, hub & spoke, gateway, etc.) is, for example, designed by a producer of the interconnect. The interconnect describes a collection of interconnectivity endpoints and how to access to the interconnectivity endpoints from SNPN-1, SNPN-2 and SNPN-3.

In general, the interconnect information is provided by a producer to consumers. For example, there is a case where the backbone network operator is a producer of the interconnect and SNPN-1, SNPN-2 and SNPN-3 are consumers. In another case, SNPN-1 is a producer of the interconnect and SNPN-2 and SNPN-3 are consumers. The interconnect information may be exchanged between the producer and consumers.

### 5.2.2 Pre-conditions

It is assumed that a hub & spoke model is deployed in a central hospital and family clinics for this service flow. SNPN-1 is the root, deployed in central hospital and SNPN-2 and SNPN-3 are leaves, deployed in family clinics #2 and #3, respectively. SNPN-1, SNPN-2 and SNPN-3 are connected to the backbone network and they are at least IP reachable with each other. As such, this use case discusses a case of managed interconnect between different SNPNs.

### 5.2.3 Service Flows

1. An interconnect for a hub & spoke model is designed by a producer of SNPN-1, deployed in the central hospital. The interconnect describes a collection of interconnectivity endpoints for the root and branches and how to access to the interconnectivity endpoints from SNPN-1, SNPN-2 and SNPN-3.
2. The interconnect provided by SNPN-1 to SNPNs deployed in the family clinics, i.e. SNPN-2 and SNPN-3.
3. The management system of SNPN-1 selects an endpoint within 5GS of SNPN-1 to an interconnectivity endpoint (root) and then prepares an access link to the interconnectivity endpoint.
4. The management system of SNPN-2 selects an endpoint within 5GS of SNPN-2 to an interconnectivity endpoint (leaf) and then prepares an access link to the interconnectivity endpoint.
5. The management system of SNPN-3 selects an endpoint within 5GS of SNPN-3 to an interconnectivity endpoint (leaf) and then prepares an access link to the interconnectivity endpoint.

### 5.2.4 Post-conditions

The interconnect between SNPN-1, SNPN-2 and SNPN-3 is realised using the selected topology model and 5GS endpoints, and then the SNPNs can exchange data.

### 5.2.5 Existing features partly or fully covering the use case functionality

Further existing features that partly or fully cover the use case functionality are FFS.

### 5.2.6 Potential New Requirements needed to support the use case

[PR 5.2.6-001] Subject to SNPNs operators’ agreement, the 5G system shall be able to support mechanisms to enable interconnect between standalone non-public networks.

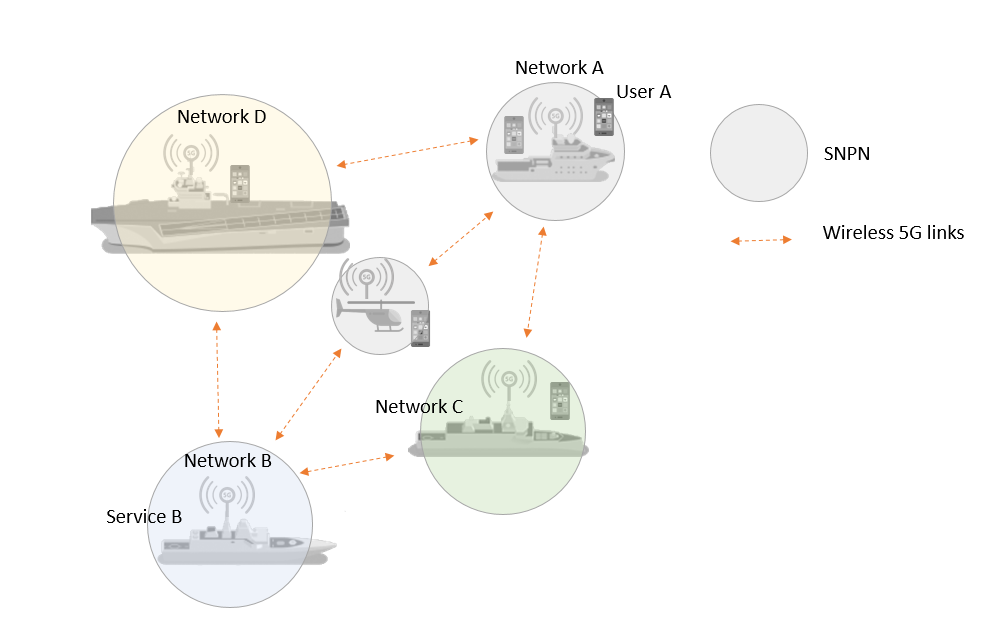
[PR 5.2.6-002] Subject to SNPNs operators’ agreement, the 5G system shall be able to support mechanisms for a selection of 5GS endpoints for SNPNs’ interconnect.

## 5.3 Use case on interconnection of standalone naval non-public networks

### 5.3.1 Description

This use case deals with self-organizing, broadband, low latency, connectivity solutions between ships in a fleet. It can apply to different sectors including military, coast guard fleet, or fleet of fishing vessels… in short to any situation where intra-fleet communication and coordination is needed.

In this use case, 5G systems are deployed on each ship within a fleet, where each system is a fully autonomous communication network enabling inter-ship and intra-ship communication. All vessels in the fleet eventually form a group of 5G standalone non-public networks connected altogether in an inherently variable topology. An example of such an interconnected group of standalone non-public networks is depicted on the Figure 5.3.1-1 below:



**Figure 5.3.1-1: Example of interconnected group of standalone non-public networks**

All standalone non-public networks are interconnected together through wireless links, preferably 5G links operating in the same frequency band as the 5G radio links connecting the terminals and the SNPNs (access network). In addition, as the group of interconnected SNPNs can be deployed in operation theatres, or in difficult sea conditions, it is important that its capacity be preserved even in the event of the loss of one or more vessels.

Each SNPN in the fleet can both be connected to the other ships through wireless links and offers connectivity in the immediate proximity of the ship where it is deployed. A user on a ship can consume any of the services hosted by the other vessels composing the fleet.

This system will finally have the following characteristics:

* Average size of targeted fleets: 5 or 6 ships
* Self-organized group of SNPNs with interconnection links established dynamically and according to the position of the ships in relation to each other’s and the quality of the radio links
* Dynamic routing according to the quality of access and interconnection links
* Full-duplex communication between ships
* Mobility of terminals from one ship (one SNPN) to another (another SNPN) without loss of communication
* Differentiated quality of service management
* Very high resilience, the connectivity between the set of SNPNs must remain operational during ship engagements, regardless of sea conditions and number of remaining vessels.
* Performances:
  + 40 km range in line of sight for the interconnection links
  + 1-10 Mbit/s in 5MHz bandwidth
  + Latency << 100ms

### 5.3.2 Pre-conditions

User A terminal is loaded with a USIM that is registered to SNPN A.

SNPN A has local coverage on-board ship A and SNPN B has coverage on-board ship B.

Service B is offered by an application B instantiated on ship B. Application B has 5G connectivity through SNPN B.

User A has needed credentials to access service B.

### 5.3.3 Service Flows

1. User A on-board ship A and attached to the on-board SNPN A establishes a PDU session to access service B.
2. In the process of establishing the PDU session, the 5G system identifies that communication with service B shall be routed from SNPN A to SNPN B through SNPN D to fulfil the quality of service required by service B. The 5G system configures all resources on this path according to service B quality of service requirements.
3. Later on, ships have moved relatively from each other’s, based on metrics collected on the wireless interconnection links, the 5G system now identifies that the communication with service B shall be routed through SNPN C. The call is handed over to the new path without the user A even noticing it.
4. Later on, unfortunately, SNPN C is no more available (or goes out of reach) and is replaced by a helicopter embedding an ad hoc SNPN. As part of a discovery process, the new SNPN in the helicopter identifies and authenticates itself to those SNPNs in range. The new route now comprising the SNPN on board the helicopter is evaluated against quality of service requirements and eventually selected by the 5G system for user A PDU session.
5. Meanwhile, while the helicopter is being launched, the 5G system realizes that the communication path using SNPN C is no more available and, as a result, User A communication to service B is reconfigured to the initial communication path through SNPN D. The communication is experiencing quality issues until the communication path is switched over to the one involving the SNPN on board the helicopter.
6. The communication with service B is terminated by user A and all resources used for the communication between SNPN A and SNPN B are released.

### 5.3.4 Post-conditions

User A is attached to SNPN A.

### 5.3.5 Existing features partly or fully covering the use case functionality

None

### 5.3.6 Potential New Requirements needed to support the use case

[PR 5.3.6-001] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to support interconnect of standalone non-public networks through links established on a temporary basis forming a group of interconnected Standalone Non-Public Networks with a variable topology.

[PR 5.3.6-002] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to support routing of user data through interconnected Standalone Non-Public Networks.

[PR 5.3.6-003] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to support discovery, addition and authentication, or detachment of Standalone Non-Public Networks in a group of interconnected Standalone Non-Public Networks.

[PR 5.3.6-004] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to support per UE communication, the establishment, reconfiguration and release of user data transmission path between two Standalone Non-Public Networks in a group of interconnected Standalone Non-Public Networks.

[PR 5.3.6-005] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to support a user subscribed to one Standalone Non-Public Network to consume a service offered by another Standalone Non-Public Network in a group of interconnected Standalone Non-Public Networks.

[PR 5.3.6-006] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to support a mechanism to exploit interconnection links metrics (e.g. jitter, latency, packet loss, capacity) as a criterion to select a suitable route between two distant Standalone Non-Public Networks in a group of interconnected Standalone Non-Public Networks.

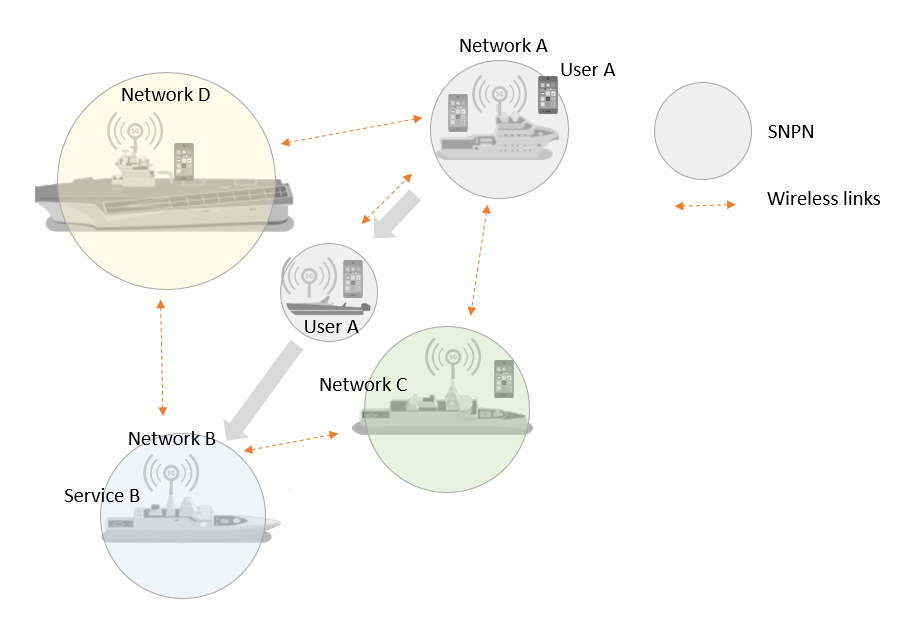
## 5.4 Use case on mobility in a group of interconnected standalone naval non-public networks

### 5.4.1 Description

This use case deals with self-organizing, broadband, low latency, connectivity solution between ships in a fleet. It is an extension of the use case 5.3 on interconnection of standalone naval non-public networks.

This network architecture, unusual in the world of public cellular networks, will however have to support all the mobility functions supported by terrestrial networks. In particular, a terminal will have to be able to move freely from one vessel to another, either in standby or while being actively involved in a communication. This movement should not be perceptible to the user.

The situation described in this use case is depicted on the Figure 5.4.1-1 below:



**Figure 5.4.1-1: Example of mobility in a group of interconnected standalone naval non-public networks**

### 5.4.2 Pre-conditions

User A terminal is loaded with a USIM that is registered to SNPN A.

SNPA A has local coverage on-board ship A and SNPN B has coverage on-board ship B.

Service B is offered by an application B hosted on ship B. Application B has 5G connectivity through SNPN B.

User A has needed credentials to access service B.

### 5.4.3 Service Flows

1. User A on-board ship A and attached to the on-board SNPN A establishes a PDU session to access service B.
2. User A takes a speed boat, equipped with necessary communication equipment to deploy locally SNPN around the speed boat and to enable connectivity with any vessels in the fleet through wireless links. Once it is deployed, the on-board SNPN selects the SNPNs in range, identifies and authenticates itself to those SNPNs. The SNPN on board the speed boat is then added in the group of interconnected SNPNs through wireless links.
3. As the speed boat moves away from ship A, radio measurements made by user A terminal trigger the 5G system to handover the ongoing communication from SNPN A to the SNPN on-board the speed boat.
4. At this point, user A terminal, although under radio coverage of the SNPN in the speed boat, keeps consuming service B through a communication path made of speed boat SNPN + SNPN A + SNPN D + SNPN B.
5. Somewhere along the path from ship A to ship B, as radio conditions on the 5G link to ship A worsen and as the speedboat approaches ship D, the SNPN on-board the speed boat selects SNPN D as a new anchoring point to the group of interconnected standalone non-public networks. Based on the new resulting topology, the 5G system then seamlessly reconfigures the communication path from user A’s UE to service B so that it can still continue to fulfil QoS required by service B. The communication path is now made of speed boat SNPN + SNPN D + SNPN B.
6. Later on, as the speedboat approaches ship B, the on-board SNPN directly connects to SNPN B in the same anchoring point selection and communication path switching process as previously described to reduce communication latency.
7. From the point in time user A gets on board the speedboat and gets to ship B, his communication with service B is maintained. There is no noticeable alteration of the communication along the path from ship A to ship B.
8. When user A arrives at his destination on ship B, his communication is seamlessly handed over from the SNPN on-board the speedboat to one of the cells on SNPN B. Once connected to SNPN B, he can still access to service B and other local services according to authorizations he’s entrusted with.

### 5.4.4 Post-conditions

User A is attached to SNPN B and still in communication with service B.

### 5.4.5 Existing features partly or fully covering the use case functionality

None

### 5.4.6 Potential New Requirements needed to support the use case

[PR 5.4.6-001] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to support discovery, addition and authentication, or detachment of Standalone Non-Public Networks in a group of interconnected Standalone Non-Public Networks without interrupting ongoing communications.

[PR 5.4.6-002] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to support service continuity of UE communications between interconnected Standalone Non-Public Networks with overlapping radio coverage.

[PR 5.4.6-003] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall enable packet loss to be minimized during mobility of a UE between interconnected Standalone Non-Public Networks with overlapping radio coverage for some or all connections associated with this UE.

[PR 5.4.6-004] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall minimize communication service interruption time during mobility of a UE between interconnected Standalone Non-Public Networks with overlapping radio coverage for some or all connections associated with this UE.

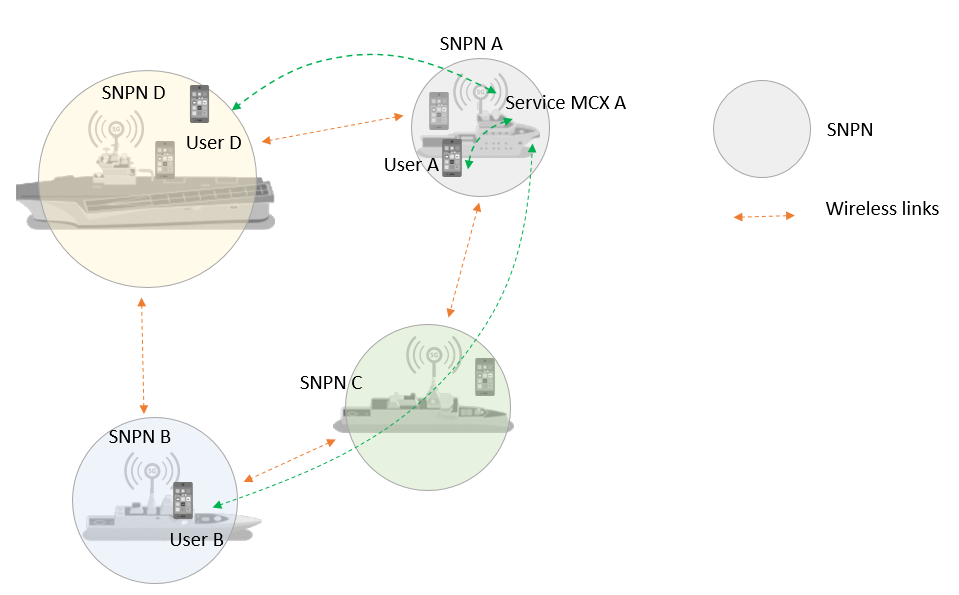
## 5.5 Use case on quality of service differentiation and resource prioritization in a group of interconnected standalone naval non-public networks

### 5.5.1 Description

This use case deals with self-organizing, broadband, low latency, connectivity solution between ships in a fleet. It is an extension of the use case 5.3 on interconnection of standalone naval non-public networks.

In this use case, several users located on different ships are involved in a real time mission critical communication while the interconnection links between the Standalone Non-Public Networks inside the group of interconnected Standalone Non-Public Networks experiences heavy load.

The situation described in this use case is depicted on the Figure 5.5.1-1 below:



**Figure 5.5.1-1: Example of critical communication in a group of interconnected standalone naval non-public networks**

### 5.5.2 Pre-conditions

All User Equipment are loaded with a USIM and are registered to their local SNPN.

A MCX service is available onboard ship A (called MCX A in the following section)

All users involved in the use case have needed credentials to access MCX A service.

### 5.5.3 Service Flows

1. User A requests a real time video streaming involving a MCX server located onboard ship A to users B and D respectively located on ship B and D.
2. If the requested quality of service can be reached, users A, B, D on-board ships A, B, D, and attached to the on-board SNPNs A, B, D, can establish a PDU session to access the video streaming service provided by the MCX server on ship A.
3. While establishing the user B’s PDU session, the 5G system identifies that communication shall be routed from SNPN A to SNPN B through SNPN C to fulfil the quality of service required by the MCX service A. The 5G system configures all resources on this path according to MCX service A’s quality of service requirements.
4. While establishing the user D’s PDU session, the 5G system identifies that communication can be directly routed from SNPN A to SNPN D. The 5G system configures all resources on this path according to MCX service A’s quality of service requirements.
5. At this point in time, users A, B, D consume the real time video service hosted by the MCX server A and the 5G system constantly monitors the achieved end to end quality of service with regards to the application known requirements.
6. The delivered end to end quality of service changes (due to e.g. path loss increase on the interconnection links), thus triggering a notification from the 5G system to the MCX application which decides to lower the video resolution to match the end to end connection capacity and maintain an acceptable experience for the users.
7. Meanwhile, lower priority communications are setup inside the fleet and start to heavily load all the interconnection links.
8. The 5G system ensure that the critical video streaming communication between users A, B, D has higher priority related to the other ongoing data exchanges which results in user A, B, D continuing experiencing a good quality MCX service A.

### 5.5.4 Post-conditions

Users A, B, D are attached to SNPN A, B, D and still in communication with MCX service A.

### 5.5.5 Existing features partly or fully covering the use case functionality

None

### 5.5.6 Potential New Requirements needed to support the use case

[PR 5.5.6-001] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to support prioritization of resources for a service offered by a Standalone Non-Public Network that is consumed by users attached to other interconnected Standalone Non-Public Networks.

[PR 5.5.6-002] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall enable a SNPN to monitor the currently delivered end to end QoS for a service hosted by this SNPN and consumed by one or several users attached to other Standalone Non-Public Networks inside a group of interconnected Standalone Non-Public Networks.

[PR 5.5.6-003] Based on SNPN configuration and subject to SNPN operator’s policy, the 5G system shall be able to provide event notification upon detecting that the requested end to end QoS level cannot be met for a service hosted by this SNPN and consumed by one or several users attached to other Standalone Non-Public Networks inside a group of interconnected Standalone Non-Public Networks.

# 6 Consolidated requirements

## 6.1 General

Editor's note: Placeholder for general service requirements.

## 6.2 Consolidated requirements for enabling of SNPN cellular hotspots

The potential requirements for enabling of SNPN cellular hotspots correspond to the use case in clause 5.1 (Scalable SNPN Interconnect with dynamic connections) and are listed in Table 6.2-1.

The requirements for SNPN cellular hotspots are intended to enable support of connectivity hotspots based on 3GPP 5GS technology that provide services in a similar way as provided by WLAN hotspots. Charging requirements are considered out of scope for this functionality.

Table 6.2-1 – Consolidated requirements for enabling of SNPN cellular hotspots

| CPR # | Consolidated Potential Requirement | Original PR # | Comment |
| --- | --- | --- | --- |
| CPR 6.2-1 | Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for an SNPN to be able to interconnect with a large number of SNPN Credential Providers with which the SNPN might not have preconfigured information detailing the IP addresses used by these SNPN Credential Providers to interconnect with the SNPN. | [PR 5.1.6-001] | Scalability |
| CPR 6.2-2 | Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for an SNPN Credential Provider to be able to interconnect with a large number of Standalone Non-Public Networks (SNPNs) with which the SNPN Credential Provider might not have preconfigured information detailing the IP addresses used by these SNPNs to interconnect with the SNPN Credential Provider. | [PR 5.1.6-002] | Scalability |
| CPR 6.2-3 | Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for an SNPN to be able to determine how to connect to an SNPN Credential Provider capable of verifying the identity presented by a user attempting to connect to that SNPN. | [PR 5.1.6-003] |  |
| CPR 6.2-4 | Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for an SNPN to be able to securely interconnect with an SNPN Credential Provider in deployments where the required security information is not preconfigured. | [PR 5.1.6-004] | Security |
| CPR 6.2-5 | Based on the Standalone Non-Public Network (SNPN) configuration, the 5G system shall support a mechanism for an SNPN to enable an SNPN Credential Provider to securely notify events (e.g., a user’s subscription ending) to the Standalone Non-Public Network (SNPN). | [PR 5.1.6-005] | Security |

# 7 Conclusions and recommendations

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2023-05 | SA1#102 | S1-231156 |  |  |  | TR skeleton | 0.0.0 |
| 2023-05 | SA1#102 | S1-231343 |  |  |  | Inclusion of agreed pCRs: S1-231157, S1-231500, S1-231775, S1-231637, S1-231628, S1-231636 | 0.1.0 |
| 2023-08 | SA1#103 | S1-232598 |  |  |  | Inclusion of agreed pCRs: S1-232461, S1-232639, S1-232466, S1-232467, S1-232459 | 0.2.0 |
| 2023-08 | SA1#104 | S1-233263 |  |  |  | Inclusion of agreed pCRs: S1-233480 | 0.3.0 |