|  |  |
| --- | --- |
| 3GPP TR 23.700-08 V0.2.0 (2022-04) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on enhanced support of Non-Public Networks;  Phase 2;  (Release 18) | |
|  | |
|  |  |
|  | |
| 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.  © 2022, 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 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Void 9

3.3 Abbreviations 9

4 Architectural Assumptions and Requirements 9

5 Key Issues 10

5.1 Key Issue #1: Enabling support for idle and connected mode mobility between SNPNs without new network selection 10

5.1.1 Description 10

5.2 Key Issue #2: Support of Non-3GPP access for SNPN 10

5.2.1 Description 10

5.3 Key Issue #3: Enabling NPN as hosting network for providing access to localized services 10

5.3.1 Description 10

5.4 Key Issue #4: Enabling UE to discover, select and access NPN as hosting network and receive localized services 11

5.4.1 Description 11

5.5 Key Issue #5: Enabling access to localized services via a specific hosting network 12

5.5.1 Description 12

5.6 Key Issue #6: Support for returning to home network 13

5.6.1 Description 13

6 Solutions 14

6.0 Mapping Solutions to Key Issues 14

6.1 Solution #1: Enable efficient mobility via equivalent SNPNs 14

6.1.1 Introduction 14

6.1.2 Functional Description 14

6.1.3 Procedures 15

6.1.4 Impacts on services, entities, and interfaces 17

6.2 Solution #2: Access to SNPN services via Untrusted non-3GPP access network 17

6.2.1 Introduction 17

6.2.2 Functional Description 18

6.2.3 Procedures 18

6.2.4 Impacts on services, entities, and interfaces 18

6.3 Solution #3: Access to SNPN services via Trusted non-3GPP access network 18

6.3.1 Introduction 18

6.3.2 Functional Description 19

6.3.3 Procedures 19

6.3.3.1 Access Network Selection procedure 19

6.3.3.2 Registration procedure 20

6.3.4 Impacts on services, entities, and interfaces 20

6.4 Solution #4: Support of onboarding over untrusted non-3GPP access in SNPN 21

6.4.1 Introduction 21

6.4.2 Functional Description 21

6.4.3 Procedures 22

6.4.4 Impacts on services, entities, and interfaces 22

6.5 Solution #5: Support of Credentials Holder scenarios over untrusted non-3GPP access in SNPN 22

6.5.1 Introduction 22

6.5.2 Functional Description 22

6.5.3 Procedures 23

6.5.4 Impacts on services, entities, and interfaces 23

6.6 Solution #6: Access to SNPN services via wireline access network 23

6.6.1 Introduction 23

6.6.2 Functional Description 23

6.6.3 Impacts on services, entities, and interfaces 23

6.7 Solution #7: High level flow for localized service support 24

6.7.1 Introduction 24

6.7.2 Functional Description 24

6.7.3 Procedures 25

6.7.4 Impacts on services, entities, and interfaces 26

6.8 Solution #8: Reuse existing mechanisms for Control Plane Load Control, Congestion and Overload Control 27

6.8.1 Introduction 27

6.8.2 Functional Description 27

6.8.3 Procedures 27

6.8.4 Impacts on services, entities, and interfaces 27

6.9 Solution #9: Prevention of overload build up at home network using AMF based congestion control when local service is over 27

6.9.1 Introduction 27

6.9.2 High-level Description 28

6.9.3 Procedures 29

6.9.3.1 UE in CM Idle-State and AMF configured to send "Network/service availability timer" 29

6.9.3.2 UE in CM-Idle State and AMF not configured to send Network/service availability timer 31

6.9.3.2 UE in CM-Connected State and AMF not configured to send Network/service availability timer 33

6.9.4 Impacts on existing services and interfaces 34

6.10 Solution #10: Solution for automatic discovery and selection of NPN hosting network and localized services 34

6.10.1 Introduction 34

6.10.2 Functional Description 35

6.10.2.1 SNPN hosting network for localized services 35

6.10.2.2 PNI-NPN hosting network for localized services 35

6.10.3 Procedures 36

6.10.3.1 Discovery and selection of SNPNs for access to localized services 36

6.10.3.2 Leaving SNPN Localized services mode 36

6.10.4 Impacts on services, entities, and interfaces 36

6.11 Solution #11: Access to localized service by using roaming architecture 37

6.11.1 Introduction 37

6.11.2 Functional Description 37

6.11.3 Procedures 38

6.11.4 Impacts on services, entities, and interfaces 39

6.12 Solution #12: Discovering services offered by SNPN while camping in a serving network 39

6.12.1 Introduction 39

6.12.2 Functional Description 39

6.12.3 Procedures 41

6.12.3.1 UE discovery, selection and access for hosting network 41

6.12.4 Impacts on services, entities and interfaces 42

6.13 Solution #13: Exposure enhancements to support providing access to localized services 42

6.13.1 Introduction 42

6.13.2 Functional Description 43

6.13.3 Procedures 45

6.13.4 Impacts on services, entities, and interfaces 45

6.14 Solution #14: Solution for hosting network selection 45

6.14.1 Introduction 45

6.14.2 Functional Description 45

6.14.3 Procedures 45

6.14.4 Impacts on services, entities, and interfaces 46

6.15 Solution #15: Local service provisioning via PLMN 46

6.15.1 Introduction 46

6.15.2 Functional Description 46

6.15.3 Procedures 46

6.15.4 Impacts on Services, Entities, and Interfaces 47

6.16 Solution #16: Access to SNPN with NG-RAN and to WLAN Access Network using the same credentials 48

6.16.1 Introduction 48

6.16.2 Functional Description 48

6.16.3 Procedures 49

6.16.3.1 WLAN Authentication with AAA Server 49

6.16.3.2 User plane aspects 51

6.16.4 Impacts on services, entities, and interfaces 51

6.17 Solution #17: UE Group specific NAS level congestion control 51

6.17.1 Introduction 51

6.17.2 Functional Description 51

6.17.3 Procedures 52

6.17.4 Impacts on services, entities and interfaces 52

6.18 Solution #18: Steering of UE to select hosting network for obtaining localized services 53

6.18.1 Introduction 53

6.18.2 Functional Description 53

6.18.3 Procedures 53

6.18.4 Impacts on services, entities, and interfaces 54

7 Evaluation 55

8 Conclusions 55

Annex A: Change history 56

# 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.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The scope of this Technical Report is to study further enhancements of the 5GS to support Non-Public Networks including the following aspects:

1. Support for enhanced mobility by enabling support for idle and connected mode mobility between SNPNs without new network selection.

2. Support for non-3GPP access for SNPN.

3. Address SA WG1 requirements in TS 22.261 [2] related to support for Providing Access to Localized Services.

NOTE: The TS 22.261 [2] requirements for Providing Access to Local Services related to Multicast/Broadcast are not part of the scope.

# 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 next generation new services and markets".

[3] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[4] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[5] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[6] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station in idle mode".

[7] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[8] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)"

[9] 3GPP TS 23.402: “Architecture enhancements for non-3GPP accesses”.

[10] 3GPP TS 33.501: “Security architecture and procedures for 5G System”.

[11] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1], TS 23.501 [3] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**Local service, Localized service:** Service, which is localized (i.e. provided at specific/limited area) and/or can be bounded in time. The service can be realized via applications (e.g. live or on-demand audio/video stream, electric game, IMS, etc), or connectivity (e.g. UE to UE, UE to Data Network, etc.).

**Localized service provider:** application provider or network operator who make their services localized and to be offered to end user via a hosting network.

**Hosting network:** A network providing access to Local/Localized services.

**Home network:** A network owning the current in use subscription/credential of the UE. Home network can be either PLMN or NPN.

NOTE 1: For SNPN case, TS 23.501 [3] defines UE access using credentials owned by a Credentials Holder separate from the SNPN.

**Home network service:** Service, which is offered to UE based on subscription agreed with home network operator.

**Return to home network:** UE leaves the hosting network (e.g. when the Local/Localized service is terminated), and resumes to use subscription/credential of home network. It can involve a network selection (e.g. select HPLMN or VPLMN) as specified in TS 23.122 [6], and can involve deactivation/activation of SNPN access mode.

NOTE 2: These are the definitions used in this TR, SA2 can consider if the definitions are used in the normative phase.

## 3.2 Void

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], TS 23.501 [3] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1], TS 23.501 [3].

Abbreviation format (EW)

<ABBREVIATION> <Expansion>

# 4 Architectural Assumptions and Requirements

Editor's note: This clause will list general architectural assumptions and principles for this study.

- Solutions shall build on the 5G System architectural principles as in TS 23.501 [3], including flexibility and modularity for newly introduced functionalities.

- Functionality to enable regulatory services like emergency services are assumed to re-use existing architecture mechanisms with no or limited impact.

NOTE: Any impacts to PWS or LI would be handled by other responsible WGs i.e. CT1 and SA3-LI respectively.

- Hosting network can be NPN, i.e. SNPN, or PNI-NPN.

- Home network can be NPN or PLMN.

- The term "home network" does not imply a roaming relationship.

- Only subscribers of a public network can roam into a PLMN.

# 5 Key Issues

## 5.1 Key Issue #1: Enabling support for idle and connected mode mobility between SNPNs without new network selection

### 5.1.1 Description

The NPN Phase 2 study item contains following work task that assumes the UE is in SNPN access mode: Support for enhanced mobility by enabling support for idle and connected mode mobility between SNPNs without new network selection. This KI aims at studying impacts to the 5G System for scenarios where the UE has a subscription with each of the source and target SNPN or can access both the source and target SNPN using credentials from a Credentials Holder:

- Study how to enable optimizations for idle mode mobility without new network selection in the inter-SNPN mobility case.

- Study how to enable optimizations for connected mode mobility without new network selection in the inter-SNPN mobility case.

- Whether and how session continuity can be supported in case of idle mode and connected mode mobility between SNPNs.

- Whether and which additional information transfer between SNPNs on top of Rel-17 is required for the above mentioned mobility scenarios.

## 5.2 Key Issue #2: Support of Non-3GPP access for SNPN

### 5.2.1 Description

Currently the 3GPP specifications do not support direct connection to SNPN via non-3GPP access networks. Indirect connection to SNPN via PLMN using untrusted non-3GPP access architecture is supported as shown in TS 23.501 Annex D.3 (PLMN as underlay network and SNPN as overlay network).

There are already non-3GPP access technologies which are in use in enterprises and campuses, and it is foreseen that use of such non-3GPP access technologies will continue to evolve. The integration of these existing technologies in the SNPN would add flexibility to the SNPN operators. In general, the solutions of this key issue aim to address the support for non-3GPP access for SNPN.

One objective of this key issue is to enable the 5GS to support direct connection of non-3GPP access networks to the SNPN's 5GC.

NOTE 1: Co-ordination with BBF and CableLabs will take place as needed during the study for solutions related to Wireline 5G Access Network.NOTE 2: Roaming for SNPN is out of scope of this key issue.

## 5.3 Key Issue #3: Enabling NPN as hosting network for providing access to localized services

### 5.3.1 Description

Providing access to local services refers to the capability to provide access to a hosting network and a set of services offered by the hosting network provider, and 3rd party service providers including other network operators and 3rd party application providers. The services may be localized (i.e. provided at specific/limited area) and may be bounded in time. The user may become aware of the available access to local services, and the process to gain and terminate access to the hosting network and local services. This process should be efficient, and convenient from a user experience standpoint.

Providing access to local services creates new opportunities for users and service providers. For example, access can be provided in areas where there is no coverage provided by other networks (for example, on a cargo ship out at sea), or the access and local services can be established as needed (on a short-term basis), without the need for long term business relationships, permanently installed equipment, etc.

The type of local services and access for localized services via a hosting network can be promoted and arranged through different channels. Principally the Localized service provider (e.g. brick and mortar businesses, construction contractors, first responder agencies, etc.) will provide information and proper incentive or instructions to potential users so that they will seek to access the local services via hosting networks.

The 5G network as hosting network offering access to such localized services can be either a PNI-NPN or an SNPN.

It is assumed that hosting network and the localized services can be operated by different entities. Localized services may provide more than just data connectivity to end users, e.g. additional information/incentive/instructions in order to seek access to the localized services in.

This key issue aims at addressing how to enable a NPN (i.e. a SNPN or a PNI-NPN) as a hosting network for providing access to localized services with the following aspects:

- Define hosting NPN and identify the difference(s) between hosting NPN and NPN defined in both Rel-16 and Rel-17.

- Define localized services and identify the difference(s) between localized services and regular services.

- Define where and when localized services are available based on localized service agreements (i.e. a service agreement for a localized service).

NOTE 1: SA WG2 works under the assumption that the relationships and the localized service agreements are already available by means outside SA2 scope i.e. SA2 is to agree where the information is made available.

- What is required to enable communication between a network operator deploying a hosting network and a localized services provider:

- Investigate which type of interaction (e.g., configuration of the hosting network, information reporting) is needed, in such relation to enable the localized services provider for making the best use of the hosting network; and

NOTE 2: Collaboration with SA WG5 and SA WG3 may be needed.

## 5.4 Key Issue #4: Enabling UE to discover, select and access NPN as hosting network and receive localized services

### 5.4.1 Description

For providing localized services to UE, the UE needs to be able to discover, select and access the hosting network for the localized services. The discovery mechanism can be based on provisioning the UE with appropriate information. TS 22.261 [2] has defined various requirements regarding discovery, selection and access of a hosting network in 6.41.2.3, 6.41.2.4 and 6.41.2.5.

NOTE: For the hosting network, only NPN (SNPN or PNI-NPN) is considered in this study.

The corresponding solutions need to consider following assumptions:

- The UE can, but not necessarily, have prior subscription with the hosting network and/or the localized services provider.

- The information for discovery of hosting network offering the localized services can be provided to the UE via either hosting network or UE's home network, or UE’s serving network or localized services provider. This information allows the UE to discover, select and access the hosting network offering the localized services.

- Reception and usage of configuration provided by a localized services provider to discover and access a hosting network and localized services is subject to home network operator’s policy and agreement between a localized services provider and hosting network operator, including the considerations of prior service agreement with a localized services provider and no prior subscription to hosting network.

- If the UE is able to obtain services from two networks simultaneously, it may additionally select the hosting network.

- The selection of a hosting network can be done on request by the user, i.e., using manual selection, unless the UE can, maintain the PDU Sessions established with the home network and retain the services provided by the home network on these PDU Sessions, while selecting the hosting network (see KI#5).

- Automatic selection of a hosting network needs to be allowed by the home network of the subscription/credentials used by the UE.

- A localized service agreement is established (see KI#3).

This key issue aims at addressing the following aspects:

- Investigate which type of information needs to be exchanged between hosting network and a localized services provider so that a UE can perform discovery, selection and connection of the hosting network and access the localized services provided via the hosting network.

NOTE 1: The hosting network can also act as a service provider for localized services.

- What is the provisioning mechanism and the information needed for the UE to discover, select and access suitable hosting network for localized services with possible validity conditions for accessing the hosting network offering the localized services, because of the nature of the localized service and hosting network (e.g., time and location constrains). This includes information enabling the UE to be aware of services that can be accessed via hosting NPN.

- Discovery and selection procedures of hosting network and localized services provided via the hosting network for UE to obtain localized services. Both automatic and end user manual selection apply.

- How a UE already registered in a network (PLMN or NPN) can discover a suitable hosting network and the localized services provided via the hosting network when the hosting network and/or localized services become available.

- How to ensure the localized services are accessed by UE according to the conditions when and where the localized services are allowed to be accessed by the UE.

- How the UE is provisioned with credentials (if required) to access the selected localised services provided via the hosting network.

- Mechanisms to authorize UE to access the hosting network.

NOTE 2: Security aspects (such as authentication of the UE and security aspects of provisioning) are addressed in SA WG3. The authentication architecture is addressed in both SA WG2 and SA WG3.

## 5.5 Key Issue #5: Enabling access to localized services via a specific hosting network

### 5.5.1 Description

Hosting NPN provides access to localized services. But home network operator of a UE can also utilize the hosting network based on a relationship established between hosting network operator and UE's home operator, so that it is possible to enable the UE with a subscription from home network to access home network services via the hosting network, in addition to the localized services. TS 22.261 [2] has defined the following requirements:

*- The 5G system shall be able to allow the home network to steer its UE(s) to a hosting network with the consideration of the location, times, coverage of the hosting network and services offered by the home network and hosting network.*

*- A localized service agreement is established (see KI#3).*

*- The 5G system shall enable the home network operator to indicate to the UE what services are preferred to be used from the home network when the UE connects to a hosting network and the requested services are available from both the hosting and the home network.*

*- Based on localized service agreements, the hosting network shall be able to provide required connectivity and QoS for a UE simultaneously connected to the hosting network for localized services and its home network for home network services.*

*- A UE shall be able to connect to its home network via the hosting network, if supported by the hosting network and the home network based on localized service agreements.*

This key issue aims at addressing the following aspects:

- How and whether the home network, determine the service availability of a hosting network, and interacts with hosting network to authorize home network's subscribers to access home network services via the hosting network, at certain time and location, coverage of the hosting network and services offered by the hosting network.

- How to enable UE to access both home network services and localized services via the hosting network, and seamless service continuity for home network services and localized services when UE moves between different networks providing the same services. This includes how to configure UE with information enabling the UE to be aware of services that can be accessed via a specific network (e.g. home network or hosting NPN).

- How home network determines the need to steer or instruct the UE, and how the home network steers or instructs the UE to select a hosting network for obtaining home network services or localized services or select a network for a specific service which is available from both hosting and home network.

- How to collect charging information for the use of localized services at the hosting network and provide the charging records to UEs' home operators.

NOTE 1: Charging aspects needs to be coordinated with SA WG5.

NOTE 2: It is assumed that existing mechanisms can be used to support Regulatory Services, e.g. PWS and emergency services.

## 5.6 Key Issue #6: Support for returning to home network

### 5.6.1 Description

According to SA WG1 TR 22.844, when local service is over, large number of UEs would attempt registration back to their home network. This may lead to a signaling peak in the home network and result in user plane and control plane overload causing for example longer waiting for users to re-register to/re-select their home network.

There are various load control mechanisms already defined e.g.:

- Access control and barring as defined in clause 5.2.5 of TS 23.501 [3];

- Control Plane Load Control, Congestion and Overload Control as defined in clause 5.19 of TS 23.501 [3];

- Prevention of signalling overload related to Disaster Condition and Disaster Roaming service as defined in clause 5.40.6 of TS 23.501 [3].

This key issue aims to study whether the existing mechanisms for overload control in the network can support all the requirements in TS 22.261 [2] clause 6.41 "Providing Access to Local Services" and whether any enhancements or additional mechanisms need to be defined. The following aspects will be considered:

- How to mitigate user plane and control plane overload caused by a high number of UEs returning from a temporary local access of a hosting network to their home network in a very short period of time.

- How to minimize the impact on the UE's communication e.g., to prevent user plane and control plane outages when returning to a home network together with other high number of UEs in a very short period of time, after terminating their temporary local access to a hosting network.

NOTE: The solution for this KI may need to consider mechanism developed for KI#5 "Enabling access to localized services via a specific hosting network".

# 6 Solutions

Editor's note: This clause is intended to document the agreed architecture solutions and a mapping of solutions to key issue(s) in clause 6.0. Each solution should clearly describe which of the key issues it covers and how.

## 6.0 Mapping Solutions to Key Issues

Table 6.0-1: Mapping Solutions to Key Issues

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Key Issues | | | | | |
| Solutions | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | X |  |  |  |  |  |
| 2 |  | X |  |  |  |  |
| 3 |  | X |  |  |  |  |
| 4 |  | X |  |  |  |  |
| 5 |  | X |  |  |  |  |
| 6 |  | X |  |  |  |  |
| 7 |  |  | X | X | X | X |
| 8 |  |  |  |  |  | X |
| 9 |  |  |  |  |  | X |
| 10 |  |  |  | X |  | X |
| 11 |  |  |  |  | X |  |
| 12 |  |  |  | X |  |  |
| 13 |  |  |  | X | X |  |
| 14 |  |  |  | X |  |  |
| 15 |  |  |  | X | X |  |
| 16 |  | X |  |  |  |  |
| 17 |  |  |  |  |  | X |
| 18 |  |  |  |  | X |  |

## 6.1 Solution #1: Enable efficient mobility via equivalent SNPNs

### 6.1.1 Introduction

The solution addresses key issue #1 "Enhanced mobility between SNPNs without new network selection".

The solution utilizes a list of SNPN identities (i.e. a list of combinations of PLMN ID and NID) to enable UE with one single SNPN subscription to efficiently access different SNPNs without performing new network selection. The list is implemented by the similar logic as the list of equivalent PLMNs, as specified in clause 5.18.2a of TS 23.501 [3].

The solution also re-use existing function as specified in clause 5.18.1 of TS 23.501 [3], where different combination of PLMN ID and NID can point to the same 5GC.

### 6.1.2 Functional Description

In existing specification, the UE can receive a list of equivalent PLMNs from core network. Such equivalent PLMN list will assist UE to select a cell from another PLMN during mobility without the need to perform new network selection.

In this solution, a list of equivalent SNPNs is proposed to facilitate the idle and connected mobility between SNPNs, reusing similar functions which are defined for PLMN:

- The core network can provide a list of SNPN identities to the UE that the UE consider as equivalent to the registered SNPN.

- The list of equivalent SNPNs can be prepared based on AMF local configuration.

- The UE stores the list of equivalent SNPNs, and update or delete the list at the end of each registration procedure in the same way as done with the list of equivalent PLMNs as described in TS 23.122 [6] and TS 24.501 [7].

- The stored list consists of a list of equivalent SNPNs' identities as downloaded by the network plus the SNPN identity of the registered SNPN that downloaded the list. When the UE is switched off, the UE shall keep the stored list so that it can be used for SNPN selection after switch on.

- The lists of equivalent SNPNs are stored and used per SNPN subscription by the UE.

- These SNPNs in the list shall be regarded by the UE as equivalent to each other for SNPN selection and cell (re)selection.

- The list can also be provided from AMF to NG-RAN for the purpose of connected mode mobility.

### 6.1.3 Procedures

When UE accesses multiple SNPNs using the credentials holder function as depicted in Figure 6.1.3-1, the following applies:

- SNPN-1 and SNPN-2 are identified by different SNPN identity, i.e. combination of PLMN ID and NID.

- SNPN-1 and SNPN-2 are the Credentials Holder(CH) for each other:

- UE of SNPN-1 can register in SNPN-2, where using SNPN-1 as the CH.

- UE of SNPN-2 can register in SNPN-1, where using SNPN-2 as the CH.

- NFs from one SNPN (e.g. SNPN-1) are only authorized to consume services from the other SNPN (e.g. SNPN-2) which is acting as CH, as depicted in Figure 5.30.2.9.3-1 of TS 23.501 [3].

- UE from each SNPN has only the subscription/credential from the respective SNPN:

- UE of SNPN-1 has only subscription/credential from SNPN-1.

- UE of SNPN-2 has only subscription/credential from SNPN-2.

- When UE holds the list of equivalent SNPNs (SNPN-1 and SNPN-2), it efficiently makes cell (re)selection when doing idle mode mobility between the SNPN-1's NG-RAN and SNPN-2's NG-RAN, without the need to perform network selection.



Figure 6.1.3-1 UE accesses multiple SNPNs using CH

When UE accesses multiple SNPNs belonging to the same administrative entity as depicted in Figure 6.1.3-2, the following applies:

- SNPN-1 and SNPN-2 are identified by different SNPN identity, i.e. combination of PLMN ID and NID.

- SNPN-1 and SNPN-2 belong to the same administrative entity. A common 5GC is used and can be managed by the same administrative entity to support both SNPN identities of SNPN-1 and SNPN-2.

- NFs of one SNPN (e.g. SNPN-1) can be authorized to consume services from NFs of the other SNPN (e.g. SNPN-2).

- UE from each SNPN has only the subscription from the respective SNPN.

- When UE is provided with the list of equivalent SNPNs (SNPN-1 and SNPN-2), it efficiently makes cell (re)selection when doing idle mode mobility between the SNPN-1's NG-RAN and SNPN-2's NG-RAN, with all the mobility and session context transferred, but without the need to perform network selection. PDU session continuity is supported.

- UE selects and attempts registration on available and allowable SNPNs by taking the equivalent SNPNs (if available) into account.

NOTE 1: CT1 will specify the details and final order of the network selection procedure.

- When NG-RAN is provided with the list of equivalent SNPNs(SNPN-1 and SNPN-2) in the MRL, it makes use of such info to achieve connected mode mobility between SNPN-1 and SNPN-2.

- In the case of handover or network controlled release to a shared network:

- When multiple SNPN IDs are broadcasted in a cell selected by NG-RAN, NG-RAN selects a target SNPN, taking into account the list of SNPN IDs which are equivalent to the serving SNPN in the Mobility Restriction List (MRL) from the AMF.

- For Xn based HO procedure, source NG-RAN indicates the selected SNPN ID to the target NG-RAN.

- For N2 based HO procedure, the source NG-RAN indicates a selected SNPN ID to the AMF in the HO required message. Source AMF uses the selected SNPN ID and target tracking area information supplied by the source NG-RAN to select the target AMF. The source AMF should forward the selected SNPN ID to the target AMF. The target AMF indicates the selected SNPN ID to the target NG-RAN so that the target NG-RAN can select target cells for future handover appropriately.

NOTE 2: It is up to RAN3 to decide how to add the selected SNPN ID in NGAP for connected mode mobility.

Serving SNPN ID if changed is indicated to the UE as part of the UE registration procedure.



Figure 6.1.3-2 UE accesses multiple SNPNs belonging to the same administrative entity

### 6.1.4 Impacts on services, entities, and interfaces

UE and AMF support of equivalent SNPN list in NAS.

NG-RAN and AMF support of equivalent SNPNs in NGAP.

UE/NG-RAN/AMF take equivalent SNPN list into consideration, for supporting relevant functions, e.g.:

- idle/connected network selection.

- cell (re)selection.

AMF to inform UE the registered SNPN ID change during mobility in Registration Accept message.

Minor impact on the following clauses in TS 23.501 [3]:

- clause 5.18.1, NOTE 3.

- clause 5.18.2a.

- clause 5.18.4.

NGAP impact for supporting connected mode mobility between SNPNs.

NOTE: It is up to RAN3 to decide how to extend NGAP for connected mode mobility.

## 6.2 Solution #2: Access to SNPN services via Untrusted non-3GPP access network

### 6.2.1 Introduction

Clause 5.30.2.8 and Annex D, clause D.3 of TS 23.501 [3] specify how the UE can access SNPN services via a PLMN.

This solution defines how the UE can access SNPN services via Untrusted non-3GPP access network.

### 6.2.2 Functional Description

To access SNPN services, a UE that has successfully obtained IP connectivity via an Untrusted non-3GPP access network may select the N3IWF of an SNPN and register with that SNPN (using the credentials of that SNPN) following the same N3IWF selection procedure as specified for access to stand-alone non-public network services via PLMN in clause 6.3.6.2a of TS 23.501 [3].

UE initiates N3IWF selection for emergency services when it detects a user request for emergency session and determines that Untrusted non-3GPP access shall be used for the emergency access. The UE with SNPN subscription follows the N3IWF selection procedure for Emergency services for UE not equipped with UICC, as defined in TS 23.501 [3] clause 6.3.6.4.2.

Editor's note: It is FFS whether the UE fully follows the selection procedure for UE not equipped with UICC as the UE's configured SNPNs can be available.

UE equipped with Default UE credentials only shall not attempt to register with an N3IWF. Instead, UE connects with a PVS using the IP connectivity from the local Untrusted non-3GPP access network (how the UE selects the PVS based on preconfigured information is out of 3GPP scope) and the PVS performs provisioning of the UE with SNPN credentials for primary authentication and other information to enable access to the desired SNPN, including N3IWF identifier configuration and Non-3GPP Access node selection information.

Editor's note: Other ways for UE to select the PVS are FFS.

### 6.2.3 Procedures

The procedure for selection of N3IWF of an SNPN for a UE connected to an untrusted non-3GPP access network is identical to the procedure for selection of N3IWF of an SNPN for a UE connected to a PLMN, the latter being described in clause 6.3.6.2a of TS 23.501 [3].

The [NGAP] INITIAL UE MESSAGE should be extended to indicate the “selected NID” in addition to the existing “Selected PLMN identity”. The encoding of this additional information is left to RAN3 WG to determine.

NOTE: The lack of “selected NID” in [NGAP] INITIAL UE MESSAGE in Rel-17 for untrusted non-3GPP access was omitted due to SNPN support was limited to 3GPP access.

### 6.2.4 Impacts on services, entities, and interfaces

UE impact:

- Ability to apply the existing procedures for selection of N3IWF of an SNPN for a UE connected to a PLMN (described in clause 6.3.6.2a of TS 23.501 [3]) when the UE is connected over Untrusted non-3GPP access.

N3IWF impact:

- Ability to select and to connect to the 5GC network of an SNPN and convey the “selected NID” to the AMF, in addition to the “Selected PLMN identity”.

NOTE: It is up to RAN3 to decide how NGAP is extended i.e. which IE is used for forwarding the selected NID.

## 6.3 Solution #3: Access to SNPN services via Trusted non-3GPP access network

### 6.3.1 Introduction

This solution defines how the UE can access SNPN services via a Trusted non-3GPP access network. It is based on clause 6.3.12.2 of TS 23.501 [3], which defines the access network selection procedure for access to PLMN services via a Trusted non-3GPP access network.

### 6.3.2 Functional Description

To access SNPN services via a Trusted non-3GPP access network, the UE follows the same procedures used for accessing a PLMN via a Trusted non-3GPP access network defined in clause 6.3.12.2 of TS 23.501 [3] with the following clarifications and additions:

- The UE initiates the access network selection procedure specified in clause 6.3.12.2 of TS 23.501 [3] and constructs a list of available SNPNs. This list contains the SNPNs advertised by all discovered non-3GPP access networks. A non-3GPP access network may advertise (e.g. with ANQP), not only the PLMNs with which 5G connectivity is supported (as specified in clause 6.3.12.2 of TS 23.501 [3]), but also the SNPNs with which 5G connectivity is supported.

- The UE selects an SNPN that is included in the list of available SNPNs.

- When the UE wants to perform UE onboarding via an SNPN, the UE may select an SNPN that is included in the pre-configured ON-SNPN selection information.

NOTE: If the same SNPN identifier is included in the lists advertised by multiple non-3GPP access networks and the UE has determined to connect to this SNPN, the UE selects the underlying non-3GPP access network through which to establish the connection based on UE implementation.

- The UE selects a non-3GPP access network that supports 5G connectivity to the selected SNPN and initiates the registration procedure via trusted non-3GPP access specified in clause 4.12a.2.2 of TS 23.502 [4] in order to register with the selected SNPN via the selected non-3GPP access network. During the EAP authentication procedure the NAI provided by the UE indicates that 5G connectivity to a specific SNPN is required, e.g. NAI = "<username>@nai.5gc.nid<NID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org".

Editor's note: It is FFS whether this solution supports SNPNs with self-assigned NID.

- If there are multiple non-3GPP access networks that support 5G connectivity to the selected SNPN as described in clause 6.3.3, then the UE places these non-3GPP access networks in a prioritized list and selects the highest priority non-3GPP access network from this list. To determine the priority of a non-3GPP access network, the UE shall apply the WLANSP rules (if provided), and the procedure specified in clause 6.6.1.3 of TS 23.503 [5], "UE procedure for selecting a WLAN access based on WLANSP rules". If the UE is not provided with WLANSP rules, the UE determines the priority of a non-3GPP access network by using implementation means.

- UE accessing the SNPN with credentials from CH is supported as described in clause 6.3.3.X.

- UE onboarding via Trusted non-3GPP access is supported as follows:

- The non-3GPP access network advertises (e.g. via ANQP) an Onboarding enabled indication, as defined in TS 23.501 clause 5.30.2.10.2.3 for the 3GPP access.

- As part of UE registration via Trusted non-3GPP access, in step 5 of TS 23.502 Figure 4.12a.2.2-1 the UE provides an onboarding indication inside the AN-Parameters.

- Emergency services via Trusted non-3GPP access to an SNPN are supported as follows:

- UE shall attempt Emergency services over Trusted non-3GPP access only if there is no 3GPP coverage.

- In presence of Trusted non-3GPPP access networks providing access to both SNPNs and PLMNs the UE initiates Emergency service with either an SNPN or a PLMN based on implementation.

- The non-3GPP access network advertises the support of Emergency service (e.g. via ANQP).

### 6.3.3 Procedures

#### 6.3.3.1 Access Network Selection procedure

The UE follows the existing procedures for network selection in SNPN access mode defined in TS 23.501 clause 5.30.2.4.2 (Automatic network selection) and clause 5.30.2.4.3 (Manual network selection). The prerequisite for these procedures is the following:

UE is configured with one or more of the following lists as defined in TS 23.501 clause 5.30.2.3:

- User controlled prioritized list of preferred SNPNs;

- Credentials Holder controlled prioritized list of preferred SNPNs;

- Credentials Holder controlled prioritized list of GINs.

A UE enabled to support UE Onboarding may be pre-configured with ON-SNPN selection information as described in TS 23.501 [3] clause 5.30.2.10.2.4.

The non-3GPP access network advertises (e.g. via ANQP) the following information:

- For SNPN supporting UE access using credentials from a CH, the indications defined in TS 23.501 clause 5.30.2.2 are used:

- An indication per SNPN of whether access using credentials from a Credentials Holder is supported;

- List of supported Group IDs for Network Selection (GINs) per SNPN;

- An indication per SNPN of whether the SNPN allows registration attempts from UEs that are not explicitly configured to select the SNPN, i.e. UEs that do not have any PLMN ID and NID nor GIN broadcast by the SNPN in the Credentials Holder controlled prioritized lists of preferred SNPNs/GINs.

- For SNPN supporting UE onboarding service, the Onboarding enabled indication as defined in TS 23.501 clause 5.30.2.10.2.3:

- An onboarding enabled indication that indicates whether onboarding is currently enabled for the SNPN.

- For SNPN supporting Emergency service via Trusted non-3GPP access:

- an Emergency service indication.

The [NGAP] INITIAL UE MESSAGE should be extended to indicate the “selected NID” in addition to the existing “Selected PLMN identity”. The encoding of this additional information is left to RAN3 WG to determine.

NOTE: The lack of “selected NID” in [NGAP] INITIAL UE MESSAGE in Rel-17 for Trusted non-3GPP access was omitted due to SNPN support was limited to 3GPP access.

#### 6.3.3.2 Registration procedure

The UE registers with the selected SNPN via the trusted non-3GPP access network using the procedure described in clause 4.12a.2 of TS 23.502 [4] with the enhancements to the following steps:

3. The UE requests "5G connectivity" to a specific SNPN, e.g. NAI = "<any\_username>@nai.5gc. nid<NID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org". The TNAP selects a TNGF which is associated with the requested SNPN ID.

5. In the Access Network parameters (AN parameters) container, the UE includes an Establishment cause set to a value corresponding to the service/functionality which the UE wants to use. For example, the Establishment cause may be set to 'UE onboarding'.

6a. The TNGF selects an AMF according to the included Establishment cause.

### 6.3.4 Impacts on services, entities, and interfaces

UE impact:

- Ability to read SNPN identifiers in the list of available networks with which 5G connectivity is supported, as advertised by the non-3GPP access network.

- Ability to select an SNPN that is included in the list of available SNPNs as described in clause 6.3.3.

- Support for Emergency services as described in clause 6.3.2.

- Support for UE onboarding as described in clause 6.3.2, notably the use of an onboarding indication inside the AN-Params.

- Support of accessing SNPN using credentials from a CH as described in clause 6.3.3.1.

Non-3GPP access network impact:

- Ability to advertise (e.g., via ANQP) the SNPNs with which 5G connectivity is supported and related parameters as described in clause 6.3.3.1.

- Support for UE onboarding as described in clause 6.3.2, notably the advertisement (e.g. via ANQP) of an Onboarding enabled indication.

TNGF impact:

- Ability to select and to connect to the 5GC network of an SNPN.

- Ability to select and to connect to the 5GC network of an SNPN and convey the “selected NID” to the AMF, in addition to the “Selected PLMN identity”.

NOTE: It is up to RAN3 to decide how NGAP is extended i.e. which IE is used for forwarding the selected NID.

## 6.4 Solution #4: Support of onboarding over untrusted non-3GPP access in SNPN

### 6.4.1 Introduction

Editor's Note: This clause lists the key issue(s) addressed by this solution, and briefly the main principles of the solution.

This solution aims at addressing key Issue #2 about support of Non-3GPP access for SNPN. In particular, this solution mainly focuses on how to support functionalities defined in R17 eNPN such as onboarding and remote provisioning over untrusted non-3GPP access. For UE accessing SNPN using credentials owned by the SNPN, Solution #2 specified in clause 6.2 can be applied.

This solution assumes that access to PVS is restricted inside the ON-SNPN and the PVS is not accessible from the public internet directly over the “untrusted non-3GPP access network”.

### 6.4.2 Functional Description

Editor's Note: This clause further details the solution principles and any assumptions made.

Before the UE registers to an SNPN over untrusted non-3GPP access for Onboarding, it shall select a N3IWF in the SNPN which supports Onboarding. Additionally, the SNPN shall support the Default Credentials Server belonging to a group identified by GINs.

Editor’s Note: How the UE can select non-3GPP access network that supports access to the N3IWF in the SNPN which supports Onboarding is FFS.

Therefore, clause 6.3.6.2a of TS 23.501[3] can be applied with following clarifications and additions:

* The configured N3IWF FQDN may consist of GIN that identifying a group the DCS belongs to.
* The FQDN constructed by the UE GIN that identifies a group the DCS belongs to and the Visited Country FQDN, indicating the query is for SNPN and performing a DNS query for the resulting FQDN. The example of N3IWF FQDN consisting of GIN is shown below:

n3iwf.5gc.GIN999123456789ABCDE..pub.3gppnetwork.org

* After UE selects a N3IWF that supports Onboarding, it shall include an Onboarding indication in the AN parameters included in the EAP-Res/5G-NAS message which are sent to N3IWF during registration procedure as specified in clause 4.12.2.2 in TS 23.502 [4]. The selected N3IWF shall select an AMF that supports Onboarding based on the Onboarding indication included in the AN parameters.

Editor’s Note: Whether GIN needs to be in the FQDN for N3IWF that supports onboarding is FFS.

Editor’s Note: Which authority will respond to the DNS query for FQDN that contains GIN and support onboarding is FFS.

### 6.4.3 Procedures

Editor's Note: This clause describes procedures and information flows for the solution.

### 6.4.4 Impacts on services, entities, and interfaces

Editor's Note: This clause lists impacts to services, entities, and interfaces.

UE impact:

- Ability to construct an FQDN consist of GINs used for selecting a preferred SNPN that supports onboarding.

- Ability to include Onboarding indication in the AN parameter sent to the N3IWF during registration procedure.

N3IWF impact:

- Ability to select an AMF that supports Onboarding based on the Onboarding indication included in the AN parameters.

## 6.5 Solution #5: Support of Credentials Holder scenarios over untrusted non-3GPP access in SNPN

### 6.5.1 Introduction

Editor's Note: This clause lists the key issue(s) addressed by this solution, and briefly the main principles of the solution.

This solution aims at addressing key Issue #2 about support of Non-3GPP access for SNPN. In particular, this solution mainly focuses on how to support functionalities defined in R17 eNPN such as accessing SNPN using credentials owned by Credentials Holder separate from the SNPN over untrusted non-3GPP access. For UE accessing SNPN using credentials owned by the SNPN, Solution #2 specified in clause 6.2 can be applied.

### 6.5.2 Functional Description

Editor's Note: This clause further details the solution principles and any assumptions made.

When UE accesses to a SNPN using credentials owned by Credentials Holder separate from the SNPN, if the UE is configured with GINs, it can select a N3IWF in the SNPN where UE accesses by using credentials owned by the Credentials Holder belonging to a group identified by GINs.

Editor's Note:It is FFS how GIN can help the UE select N3IWF of the serving SNPN it needs to receive service from.

Therefore, clause 6.3.6.2a of TS 23.501[3] can be applied with following clarifications and additions:

* The UE is configured with a GIN that identifies a group the CH belongs to.
* The FQDN constructed by the UE consists of GIN that identifies a group the CH belongs to and the Visited Country FQDN, indicating the query is for SNPN and performing a DNS query for the resulting FQDN.

The example of N3IWF FQDN consisting of GIN is shown below:

n3iwf.5gc.GIN999123456789ABCDE..pub.3gppnetwork.org

Editor's Note:Which authority will resolve the DNS query for N3IWF FQDN using GIN is FFS.

### 6.5.3 Procedures

Editor's Note: This clause describes procedures and information flows for the solution.

### 6.5.4 Impacts on services, entities, and interfaces

Editor's Note: This clause lists impacts to services, entities, and interfaces.

UE impact:

- Ability to construct an FQDN consisting of GINs used for selecting a preferred SNPN that supports connecting with Credentials Holder.

SNPN operator and/or GSMA:

- Use SNPN FQDN consisting of GINs.

## 6.6 Solution #6: Access to SNPN services via wireline access network

### 6.6.1 Introduction

This solution addresses KI#2.

The solution defines how the 5G-RG, FN-RG, and devices behind the RG (UE or N5GC devices behind an FN-RG or 5G-RG) can access SNPN services via a wireline access network. It is based on clause 4.2.1 of TS 23.316 [8], where the SNPN is implicitly selected by wired physical connectivity between 5G-RG or FN-RG and W-AGF. The only additional requirement is that the NID is included as part of the registration procedure for wireline access system.

### 6.6.2 Functional Description

To access SNPN services via a wireline access network, the RG follows the similar procedures used for accessing a PLMN via a wireline access network defined in clause 4.2.1 of TS 23.316 [8]. The procedure is as follows:

- SNPN is implicitly selected by wired physical connectivity.

- The 5G-RG, the W-AGF acting on behalf of the FN-RG and the W-AGF acting on behalf of the N5GC device shall consider both the PLMN ID and the SNPN Network Identifier (NID) configuration to access SNPN via the wireline access network.

- The 5G-RG that supports 5G connectivity to the SNPN initiates the registration procedure via a W-5GAN as specified in clause 7.2.1.1 of TS 23.316 [8] with the addition of SNPN NID. For example, the NAI format for a SUPI containing a GCI shall take the following form: "<GCI>@5gc.nid<NID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

- The FN-RG that supports 5G connectivity to the SNPN initiates the registration procedure via a W-5GAN as specified in clause 7.2.1.3 of TS 23.316 [8] with the addition of SNPN NID. For example, the NAI format for a SUPI containing a GCI shall take the following form: "<GCI>@5gc.nid<NID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

- The N5GC device behind RG (5G-RG or FN-RG) that supports 5G connectivity to the SNPN initiates the registration procedure via a W-5GAN as specified in clause 4.10a of TS 23.316 [8] with the addition of SNPN NID.

### 6.6.3 Impacts on services, entities, and interfaces

5G-RG impact:

- Ability to formulate the SUCI that includes the SUPI type as “IMSI” and the home network domain which will include the SNPN identifier (NID) and the PLMN ID to access an SNPN network.

W-AGF impact in case of an FN-RG:

- Ability to formulate the SUCI with NAI that includes the SNPN identifier (NID) and the PLMN ID in the realm portion of NAI to access an SNPN network.

## 6.7 Solution #7: High level flow for localized service support

### 6.7.1 Introduction

This solution provides a high level and overall flow to enable localized service, and covers key issues KI#3/#4/#5/#6.

### 6.7.2 Functional Description

The steps shown in the Figure 6.X.3-1 describe a sequence of events among the involved entities. Such sequence is assumed to be applicable for enabling localized service in a typical scenario. The order of the steps and the occurrences of each step are not necessarily restricted.

This solution is assumed to be an umbrella solution without further details on how each steps are implemented.

### 6.7.3 Procedures



Figure 6.7.3-1 High level procedures for providing access to local service

H1. For a hosting network to provide access to localized service, the service provider of the localized service needs to establish localized service agreement with the operator of a hosting network.

The service provider according to TS 22.261 [2] clause 6.41.2.2 can be network operators or 3rd party application providers. The services offered from service providers can be localized, and accessed via the hosting network based on the agreement between the different entities.

A service agreement with UE's home network operator is needed to enable, e.g.:

- UE to receive and use configuration provided by a 3rd party service provider to discover and access a hosting network and localized services.

- Charging for the use of localized service.

- The interworking scenarios described in TS 22.261 [2] Annex G1.

- Service/session continuity between home network and hosting network.

NOTE 1: The service level agreements established between different entities are work assumptions for SA2.

H2. The hosting network is configured based on the service agreements e.g., QoS, number of end users, time, location, network slicing, whether a subscriber of the home network is authorized to use localized service, whether home network services can be accessed via hosting network, etc.

Editor's note: It is FFS whether there is SA2 work related to the configuration of hosting network. Also how the configuration of the hosting network can be done e.g., via OAM or via other mechanisms involving interactions with service provider.

H3. End user/UE is prompted with localized service (e.g. via ticket of an event, commercial etc) , and starts to look for methods how to access the localized service. This could trigger activities on the application layer (e.g. login a web page, scan a QR code etc) and further triggers demand/request from the UE to obtain information related localized services.

NOTE 2: The application layer activities are outside of 3GPP scope.

H4. The service provider / hosting network / home network can co-ordinately deliver to the UE information related to localized service(s). This step can also involve the serving network of the UE in case UE is not currently served by home network. The information related to localized service(s) provided to UE in this step can also be unsolicited. In this case, step H3 can happen after, or during this step.

H5. Based on the received information related to localized service(s), the end user/UE decides to accept and starts the process to discover/select the hosting network when the conditions of the localized service are about to be met (e.g. event time is approaching, end user enters the physical location etc).

H6. UE connects to the hosting network, possibly with the authorization from home network, and prepares to access the localized service (e.g. User Plane setup, QoS negotiation, etc ).

H7. UE temporarily stays in the hosting network to obtain the desired localized service and optionally home network services that are available via the hosting network.

H8. When the temporary access to hosting network for localized service is about to be terminated due to for example event is over, end user has left the area, agreed quota is exhausted, etc, the UE returns from the hosting network.

H9. Hosting network and/or the service provider collect and provide charging information to UEs' home network operator, depends on the localized service agreement.

NOTE 3: Charging aspects is to be coordinated with SA5.

H10. When the localized service agreement is terminated, each entity shown in the figure may need to roll back the previous setup, in order to for example maintain the privacy of an end user against hosting network, prevent a UE to re-access hosting network, release network resources etc. The operation of roll back depends how the localized service is agreed between entities, e.g. if it is a time limited or a geographic limited service, whether it is an one-time service for a single event, etc.

### 6.7.4 Impacts on services, entities, and interfaces

Impacts are expected to be described in other solutions.

NOTE: Security aspects has dependences on SA3 work.

## 6.8 Solution #8: Reuse existing mechanisms for Control Plane Load Control, Congestion and Overload Control

### 6.8.1 Introduction

This solution addresses the scenario when UEs after having utilized localized services in a hosting network return to their home network. Due to the nature of localized services, this may involve large number of UEs in the same location at the same time. Large number of UEs that simultaneously attempt to re-register with their home network can cause a significant increase in signalling load, both in the Access Network (AN) and in the Core Network (CN). The proposed solution is to reuse existing mechanisms for Control Plane Load Control, Congestion and Overload Control, to mitigate signalling overload when large number of UEs return to their home network.

### 6.8.2 Functional Description

The solution assumes that the UEs have temporarily selected and registered with a hosting network for utilizing localized service, and that the UEs at some point leave the hosting network and return to their home network. The home network in this case can be a PLMN (HPLMN or VPLMN) or an SNPN.

The mechanism for Control Plane Load Control is a comparatively slow mechanism. It does not adapt quickly to changes of signalling load. The purpose of the mechanism is to distribute the load in relation to the relative capacity of the involved Network Functions. The load distribution is based on Weight Factors in AMFs.

AMF Control of Overload involves activation of NAS level congestion control, which is based on providing UEs with back-off time values. The UEs use the back-off time values to decide when to initiate NAS signalling. By providing different back-off time values to different UEs, the UE-initiated NAS-signalling is expected to be distributed over time, thereby reducing the peak signalling load. NAS level congestion control is described in 3GPP TS 23.501 [3] clause 5.19.7.

### 6.8.3 Procedures

Control Plane Load Control, Congestion and Overload Control, are described in:

* 3GPP TS 23.501 [3] clause 5.19.
* 3GPP TS 29.500 [11] clause 6.3: Load Control.
* 3GPP TS 29.500 [11] clause 6.4 Overload Control.

### 6.8.4 Impacts on services, entities, and interfaces

None.

## 6.9 Solution #9: Prevention of overload build up at home network using AMF based congestion control when local service is over

### 6.9.1 Introduction

The solution addresses the KI#6: Support for returning to the home network, by controlling the build-up of load due to the large-scale migration of multiple UEs from the local hosting network to the home network when the local hosting network decides to end its services.

The UEs that are registered to the local hosting network are deregistered in a staggered manner and completed before local hosting network goes out of service. The UEs are forced to enter into Network selection mode to choose the home network. In this manner the number of UE’s triggering simultaneous de-registration (and consequently then registering back to its home) are in the range of manageable capacity by the home network without causing congestion or overload.

This is achieved using either one of the two mechanisms

- Usage of Network availability timers

- Specific Cause code to trigger the controlled deregistration

### 6.9.2 High-level Description

The solution addresses KI#6 and the following principles are used:

- When a UE registers to the local hosting network, the AMF of the local hosting network, based on the valid duration of the local hosting services, will start a "Network/service availability timer" for the UE. The timer will have a random value and is based on the time at which the UE registers to the local hosting network and the duration for which such local hosting service will be available.

- There will be 2 separate timers for each UE started at the time of Registration– one to be applicable if the UE is in CM-Idle State when the timer expires and the other one if the UE is in CM-Connected State when the timer expires. The timer value for the CM-Connected State will be larger than the one for CM-Idle State.

- The "Network/service availability timer" will be restarted every time UE initiates Registration to the 5G Network.

- The "Network/service availability timer" for UE-Idle State will be applicable if the UE is in CM-Idle state at the expiry of this timer.

- The "Network/service availability timer" for UE-Connected State will be applicable if the UE is in CM-Connected state at the expiry of this timer.

- The "Network/service availability timer" is used to trigger the de-registration of UE from the local hosting network, before the local hosting services becomes unavailable.

- The timer values are chosen such that the de-registration procedures from the local hosting network are timed in a staggered manner and completed before the local hosting services terminates and the number of UE's triggered to initiate simultaneous de-registration (and consequently then registration back to its home network) are in the range of manageable capacity by the home network without causing overload build up at the home network

- The "Network/service availability timer" to be used in CM-Idle State could be send to the UE, during the Registration procedure to the local hosting network, in Registration accept message.

- Sending of "Network/service availability timer" is optional and based on configuration at the AMF.

- At the expiry of "Network/service availability timer"- Idle / Connected at AMF, RRC state of the UE will be checked, and appropriate actions will be taken based on the UE state (Idle or Connected) at that instant.

- When the "Network/service availability timer" for UE expires at the AMF and AMF is not configured to send the “Network/service availability timer” to the UE, AMF will initiate De-registration procedure for the UE with a specific cause code, that indicates the local hosting services are going to be unavailable.

- When the "Network/service availability timer" for UE expires at the AMF, and AMF is configured to send the “Network/service availability timer” to the UE, AMF will initiate implicit De-registration procedure for the UE without any signalling. This is applicable only when the UE is in CM Idle State as the "Network/service availability timer" for CM-Connected State is never send to the UE.

- If the UE becomes CM-Idle after the expiry of "Network/service availability timer" for CM-Idle State, but before the expiry of "Network/service availability timer" for CM-Connected State, then the AMF will immediately initiate De-registration procedure for the UE with a specific cause code, that indicates the local hosting services are going to be unavailable.

- When UE is provided with "Network/service availability timer" as part of the Registration Accept message, UE will move itself to RM-DEREGISTERED State without any signalling with the 5G Network, at the expiry of this timer.

- When the UE is de-registered from the local hosting services either due to the expiry of "Network/service availability timer" or due to the AMF initiated De-registration procedure for the UE, with a specific cause code, that indicates the local hosting services are going to be unavailable:

a. The UE may put the hosting network in a temporary forbidden list or temporary unavailable list, so that it does not try to re-register to the same hosting network again after this timer expiry.

b. UE would change the Network Selection mode to Automatic if it had connected to the hosting network through Manual selection mode and select network based on PLMN selection procedure as defined in 3GPP TS 23.122 [6], clause 4.4.

c. UE will initiate Registration to the Home Network as defined in 3GPP TS 23.502 [4], clause 4.2.2.2.2.

### 6.9.3 Procedures

#### 6.9.3.1 UE in CM Idle-State and AMF configured to send "Network/service availability timer"



Figure 6.9.3.1-1: UE in CM-Idle State and AMF configured to send “Network/service availability timer”

1. UE initiate registration with the local hosting network.

2. AMF assigns an appropriate "service availability timer" considering the service available timer (as configured by the OAM) and ensuring that all the UEs does not trigger de-registration at the same time. Thus, ensuring the UE also does not cause signalling overload at the home network when the UE connects back. AMF includes the "Network/service availability timer" in the Registration accept message as it is configured to send this timer in Registration accept message.

As an example, one of the methods is illustrated below to show how the "Network/service availability timer" is derived by AMF

a. Network/service availability timer = (Time at which the Hosting Network ends service) – (Time of UE registration) + x where x is chosen a random value to avoid all UEs accessing the Home Network at the same time.

3. AMF starts the "Network/service availability timer" for both CM-Idle and CM-Connected States.

4. UE initiates RRC release procedure before the expiration of the "Network/service availability timer" for CM-Idle State. UE enters into CM-Idle State.

5. "Network/service availability timer" for CM-Idle State expires at AMF and UE. AMF initiates Implicit De-registration of the UE without any additional Signalling.

6. UE moves to RM-DEREGISTERED STATE.

7. UE moves hosting network identity to the list of "temporarily forbidden SNPNs" or temporary unavailable list, if the local hosting network is SNPN, or move the CAG Identifiers of local hosting network out of "CAG Information list", if the local hosting network is a PNI-NPN.

8. UE would change the Network Selection mode to Automatic PLMN selection if it had connected to the hosting network through Manual mode and select network based on PLMN selection procedure as defined in 3GPP TS 23.122 [6], clause 4.4. UE will initiate Registration to the Home / Serving Network as defined in 3GPP TS 23.502 [4], clause 4.2.2.2.2. Since the de-registration from the hosting network and Registration to the Home/Serving Network happens in a staggered manner, the Home/Serving Network does not get overloaded.

#### 6.9.3.2 UE in CM-Idle State and AMF not configured to send Network/service availability timer



Figure 6.9.3.2-1: UE in CM-Idle State and AMF not configured to send “Network/service availability timer”.

1. UE initiates registration with the local hosting network.

2. AMF assigns an appropriate "service availability timer" considering the service available timer (as configured by the OAM) and ensuring that all the UEs does not trigger de-registration at the same time. Thus, ensuring the UE also does not cause signalling overload at the home network when the UE connects back. AMF does not include the "Network/service availability timer" in the Registration accept message as it is not configured to send this timer in Registration accept message.

3. AMF starts the "Network/service availability timer" for both CM-Idle and CM-Connected States.

4. UE initiates RRC release procedure before the expiration of the "Network/service availability timer" for CM-Idle State. UE enters the CM-Idle State.

5. "Network/service availability timer" for CM-Idle State expires at AMF. AMF initiates explicit De-registration procedure with the UE.

6. AMF sends Paging Request to the UE.

7. UE initiates Service Request to come to CM-Connected Mode.

8. AMF sends De-registration Request to the UE with cause code (eg: 5G Services going out of Service) indicating that local services are going to be terminated soon.

9. UE sends De-registration complete to the AMF.

10. UE moves hosting network identity to the list of "temporarily forbidden SNPNs" or temporary unavailable list, if the local hosting network is SNPN, or move the CAG Identifiers of local hosting network out of "CAG Information list", if the local hosting network is a PNI-NPN.

11. UE would change the Network Selection mode to Automatic if it had connected to the hosting network through Manual mode and select network based on PLMN selection procedure as defined in 3GPP TS 23.122 [6], clause 4.4. UE will initiate Registration to the Home / Serving Network as defined in 3GPP TS 23.502 [4], clause 4.2.2.2.2. Since the de-registration from the hosting network and Registration to the Home/Serving Network happens in a staggered manner, the Home/Serving Network does not get overloaded.

#### 6.9.3.2 UE in CM-Connected State and AMF not configured to send Network/service availability timer



Figure 6.9.3.2-1: UE in CM-Connected state and AMF not configured to send “Network / Service Availability” timer

1. UE initiates registration with the local hosting network.

2. AMF assigns an appropriate "service availability timer" considering the service available timer (as configured by the OAM) and ensuring that all the UEs does not trigger de-registration at the same time. Thus, ensuring the UE also does not cause signalling overload at the home network when the UE connects back. AMF does not include the "Network/service availability timer" in the Registration accept message as it is not configured to send this timer in Registration accept message.

3. AMF starts the "Network/service availability timer" for both CM-Idle and CM-Connected States.

4. "Network/service availability timer" for CM-Idle State expires at AMF. The UE is in CM-CONNECTED state, so the AMF does not take any action.

5. "Network/service availability timer" for CM-Connected State expires at AMF. AMF initiates explicit De-registration procedure with the UE.

6. AMF sends De-registration Request to the UE with cause code (eg: 5G Services going out of Service) indicating that local services are going to be terminated soon.

7. UE sends De-registration complete to the AMF.

8. UE moves hosting network identity to the list of "temporarily forbidden SNPNs" or temporary unavailable list, if the local hosting network is SNPN, or move the CAG Identifiers of local hosting network out of "CAG Information list", if the local hosting network is a PNI-NPN.

9. UE would change the Network Selection mode to Automatic if it had connected to the hosting network through Manual mode and select network based on PLMN selection procedure as defined in 3GPP TS 23.122 [6], clause 4.4. UE will initiate Registration to the Home / Serving Network as defined in 3GPP TS 23.502 [4], clause 4.2.2.2.2. Since the de-registration from the hosting network and Registration to the Home/Serving Network happens in a staggered manner, the Home/Serving Network does not get overloaded.

The same call flow is applicable for a UE in CM-Connected State, even if the AMF is configured to send "Network/service availability timer".

### 6.9.4 Impacts on existing services and interfaces

The solution has the following impacts:

UE:

- handling of new cause codes, service availability timer and related implementation.

AMF:

- handling of new timer for all the UEs accessing local services. Support for new cause code in network initiated UE deregistration request.

## 6.10 Solution #10: Solution for automatic discovery and selection of NPN hosting network and localized services

### 6.10.1 Introduction

This solution addresses the Key issue#4: Enabling UE to discover, select and access NPN as hosting network and receive localized services.

It also provides a solution for Key Issue #6: Support for returning to home network

It provides a different approach for discovery and selection for PNI-NPN case and for SNPN case.

### 6.10.2 Functional Description

#### 6.10.2.1 SNPN hosting network for localized services

SNPN selection for localized services is performed by a UE that supports access to localized services in SNPNs and that has been configured to access localized services in SNPNs. We will call this UE an “*SNPN-localized services-enabled UE*”.

An “*SNPN-localized services-enabled UE”* can be configured with a specific prioritized list of SNPNs for localized services. The UE can be pre-configured or dynamically configured by the subscribed SNPN or Home PLMN (e.g., using the SoR procedure as defined in Annex C of TS 23.122 [6]).

The reason to have a separate list for localised services instead of a common one like the one is defined in TS 23.501 [3] clause 5.30.2.4 is that there may be a case where the home SNPN or HPLMN or the UE is present in the same areas where localised services are provided and based on the existing selection procedures the UE will always prefer the home SNPN or HPLMN in this case.

The prioritized list of SNPNs for localized services is stored in the context of a given subscription. If the UE has multiple subscriptions, then the UE may have one prioritized list of SNPNs for localized services for each subscription.

Each entry in the prioritized list of SNPNs for localized services contains:

1. An identification of the SNPN and the localized service to access. This identification can be done in a few different ways:

- Identification Mode 1: SNPN ID (PLMN ID + NID) or a Group ID for Network Selection (GIN)

- This mode if identification assumes that the localized service is enabled in the whole SNPN with the SNPN ID or in every cell where GIN is broadcasted.

- Note that an SNPN operator could potentially use multiple SNPN IDs in different areas.

- Identification Mode 2: SNPN ID or GIN, plus an additional Subnetwork ID.

- The subnetwork ID is used to assign a specific area where the localized service is provided, and it is broadcasted in SIB together with SNPN ID or GIN.

- One or more localized services may be assigned the same subnetwork ID if they are offered in the same area.

2. Validity information:

- Validity time period.

- Additional location information (TAI list or geographical information).

The UE uses this prioritized list and the validity information to perform discovery and selection and to leave the SNPN as described in the Procedures section 6.10.3.

#### 6.10.2.2 PNI-NPN hosting network for localized services

For PNI-NPN case, Rel-17 automatic selection defined in TS 23.501 [3] applies with one additional enhancement:

- Entries in the Allowed CAG list of the UE can additionally contain the following validity information:

- Validity time period (from/to date and time)

- Location (e.g., list of tracking areas where the CAG list is valid)

NOTE: Location information for Allowed CAG list only needed if PNI-NPN as hosting network can be a subset of a CAG.

In the case of PNI-NPN (CAG) selection for access to localized services, the UE only considers an entry in the Allowed CAG list valid if and while all conditions for that entry are met.

For the case of time period, a UE will only attempt registration on a CAG cell if e.g. the current time lies within the time period of the related condition.

### 6.10.3 Procedures

#### 6.10.3.1 Discovery and selection of SNPNs for access to localized services

The UE performs the following steps:

- Step 1. UE is configured with a “prioritized list of SNPNs for localized services” and at least one entry in the validity information is met (e.g., current time is within the time period). This configuration allows the UE to start operating in "SNPN Localized services mode" when the right validity conditions are met. The UE may continue at this point be in either SNPN access mode or PLMN access mode until the conditions of validity information.

- Step2. When some validity information is met (e.g. time validity) in step 1, the UE scans for SNPNs in the background

NOTE: Details of how often to scan, etc. are out of scope of SA2.

- Step 3. If the UE finds at least one available and allowable SNPN which meets the validity conditions, then the UE switches to a new network selection mode "SNPN Localized services mode" and selects an available SNPN from the list of SNPNs for localized services.

- Step 4. The UE performs Initial registration in the SNPN and presents the SUPI of the currently active subscription (subscription that contains the prioritized list of SNPNs for localized services which the UE used to select the SNPN).

#### 6.10.3.2 Leaving SNPN Localized services mode

The UE performs the following steps:

- Step 1. If the validity information in the prioritized list of SNPNs for localized services for the currently registered SNPN are no longer met, then the UE disables “SNPN Localized services mode” and returns to the mode in which the UE was before activating SNPN Localized services mode (i.e., return to SNPN access mode or PLMN access mode). If the validity conditions that are no longer met is the Validity time period, this could occur to many devices at the same time and a large number of UEs may return to their HPLMN at the same time if measures are not taken. Therefore, two possible solutions to address this issue (key issue #6) can be taken:

- Option 1: The CH or HPLMN (depending on case) configures UEs with slightly different end time to the validity time period.

- Option 2: The UE applies a random delay before initiating step 2.

- Step 2. The UE performs SNPN selection or PLMN selection as defined in TS 23.122 [6] (depending on the mode).

### 6.10.4 Impacts on services, entities, and interfaces

UE:

- New configuration to incorporate location services validity information and in the case of SNPN prioritization.

- New SNPN for localized services selection mode.

- New triggers to enter/leave SNPN for localized selection mode.

RAN:

- In one of the options for SNPN for localized service identification, new Subnetwork ID broadcasted in SIB.

## 6.11 Solution #11: Access to localized service by using roaming architecture

### 6.11.1 Introduction

This solution addresses Key Issue #5: Enabling access to localized services via a specific hosting network. The basic principle of this solution is reusing existing roaming architecture and LADN mechanism. This solution does not resolves how the UE triggers, discovers and selects hosting network, which is in the scope of Key Issue #4.

### 6.11.2 Functional Description

In this solution, it is assumed that a UE's home network is a PLMN and hosting network is a PNI-NPN.

The following figure 6.11.2-1 and figure 6.11.2-2 depict the proposed architecture, which are reusing 5G System roaming architecture in case of local breakout and home routed scenario. When a UE registers to the selected hosting network and receives localized services provided by the hosting network, architecture in figure 6.11.2-1 is used. If the UE also need to get services from the home network, the UE may establish home routed PDU session as shown in figure 6.11.2-2. Whether the UE receives a specific service from the hosting network or home network is determined based on subscription of the UE by establishing a local breakout session, or a home routed session. The UE just follows the existing PDU Session Establishment procedure based on URSP rule provided by the home network.



Figure 6.11.2-1. Architecture when a UE uses localized services provided by the hosting network



Figure 6.11.2-2. Architecture when a UE uses services provided by the home network

When a UE registers to the hosting network and has the subscription to a specific LADN DNN for local service or a wild card DNN, the AMF provides LADN information (i.e. LADN DNN and LADN service area) to the UE according to the existing LADN mechanism. The UE uses the LADN information to access localized services provided by the hosting network.

NOTE: When hosting network operator configures LADN information in the AMF, the operator can provide associated validity time of LADN DNN so that the AMF provides LADN information when the validity time is satisfied.

Editor's note: It is FFS whether and how to support the scenario that PNI-NPN is in the HPLMN.

Editor's note: It is FFS how the UE discovers and selects PNI-NPN (including whether and how to support CAG) for local services.

### 6.11.3 Procedures



Figure 6.11.3-1. Registration in the hosting network

The Registration procedure in TS 23.502 [4] is used with following modifications:

- When a UE performs initial Registration procedure, Registration type indicates that the UE is accessing the network for localized services. Based on this information the AMF determine to provide LADN information to the UE.

- The AMF indicates to the UDM that the UE is registering for localized services. The UDM use the indication whether to accept UE registration.

### 6.11.4 Impacts on services, entities, and interfaces

**UE:**

- The UE indicates that the UE is accessing the network for localized services during the Registration procedure.

**AMF:**

- The AMF indicates to the UDM that the UE is registering for localized services.

**UDM:**

- The UDM determines whether to accept registration taking into account the indication that UE is registering for localized services.

## 6.12 Solution #12: Discovering services offered by SNPN while camping in a serving network

### 6.12.1 Introduction

The solution addresses key issue #4 "Enabling UE to discover, select and access NPN as hosting network and receive localized services" and proposes how UE becomes aware of hosting network for localized services.

UE may not actively search for available networks such as hosting network for localized services when UE is camped in home network.

This solution proposes that current serving network (PLMN or SNPN) may assist UE in discovering hosting network for localized services in specific conditions, such as when serving network determines that UE moves into area where localized services are available. For current serving network to able to assist UE in discovery of hosting network for localized services some level of co-operation between current serving network and hosting network is needed.

Once UE becomes aware of the hosting network with help of serving network, there can be several different alternatives for how the UE may connect to hosting network depending on the configuration of UE such as availability of credentials and configuration of hosting network.

### 6.12.2 Functional Description

This solution addresses KI#4 and the following principles are used:

- UE is assumed to have only single radio capability.

- When the UE is camping in the home network, the home network AMF determines the location of the UE, for instance, based on AMF determining change of Tracking Area (TA), e.g., Tracking Area Code (TAC) or gNB id, in Registration Request (Mobility Registration Update) received from UE as specified in TS 23.502 clause 4.2.2.2.

- The AMF is aware of availability of hosting network(s) that corresponds to (allowed) areas (such as tracking area) which represent the current UE location as indicated in the Mobility Registration Update sent by the UE.

Editor’s Note: How AMF is aware of availability and other information of hosting network (s) in the Tracking Area is FFS.

- Based on availability of the hosting network(s) in the location of the UE and considering other information such as subscription information, UE capability, roaming and local configuration/policies, AMF may decide to assist UE in discovering hosting network(s).

Editor’s Note: Other criteria for AMF to consider whether to assist UE in discovering Hosting network(s) is FFS.

- If the serving network decides to assist UE in discovering hosting network(s), the AMF may

- the AMF may include information on available hosting network(s) as part of Registration Accept message sent to UE.

- the UDM may as part of registration procedure initiate Steering of Roaming (SoR), as specified in TS 23.122 [6] Annex C, to update information of available hosting network(s) to UE.

- the AMF may initiate UE Configuration Update procedure, as specified in TS 23.502 clause 4.2.4.2, to update information on available hosting network(s).

Editor’s Note: It is FFS whether the existing information element in the SoR is sufficient to carry hosting network related information or what enhancements are needed.

- The AMF may invoke the Namf\_EventExposure\_Notify to provide mobility related event to (authorized) SMF(s) that have subscribed for the events by invoking Namf\_EventExposure\_Subscribe as specified in TS 23.501 clause 5.3.4.4 and TS 23.502 clause 4.15.4.2. Mobility event notification may include information of available hosting network(s) or could be mapped (e.g., PRA) to such information in SMF. SMF may use the information of available hosting network(s) received from AMF to initiate PDU Session Modification to inform UE, e.g., using PCO, about specific details of hosting network configuration such as URL and other information that UE may use to access localized sevices captive portal for UE onboarding and remote provisioning purposes.

Editor’s Note: How SMF is aware of UE configuration information for hosting network(s) is FFS.

- UE could use the localized sevices captive portal, e.g., for UE onboarding to hosting network (to obtain credentials) while still connected in home network (or current serving network) and using existing PDU session.

- Information of available hosting network(s) may include

- indication of availability of one or more hosting network(s),

- list of (PLMN ID, SNPN ID), GINs (as defined in TS 23.501 clause 5.30) or localized sevices specific identifier of available hosting network(s),

- N3IWF address and necessary credentials to access hosting network(s),

- Specific details of hosting network such as URL or other data for UE to be able to connect to the localized sevices captive portal page.

- The serving network may also broadcast GIN that is localized services specific or localized services specific broadcast indicator to indicate localized services availability with which the hosting network has an agreement with. In case of GIN is used, the serving network also broadcasts GIN when requested by the UE. In case of localized services, a new indicator is needed in the broadcast that a GIN can be used to select a hosting network. GIN, the localized services identifier and other information such as HRNN (Human readable network name) may also be displayed on the UE allowing for manual selection by the user.

Editor's Note: Scope of the GIN broadcast by serving network needs to be clarified (e.g., geographic, whether whole network, maximum number).

- Based on information of available hosting network(s) UE receives from current serving network (e.g., initiated by AMF or triggered by GIN broadcasted by the home network), UE may

Editor's Note: How “triggered by GIN broadcasted by the home network” triggers UE selection of a hosting network is FFS.

Editor's Note: Switch of SNPN/PLMN access mode for network selection is FFS.

- access hosting network using credentials owned by a Credentials Holder separate from the hosting network. Credentials Holder can be the home network or current serving network (e.g. the PLMN or the SNPN). UE authorization for hosting network services is checked by the serving network

Editor's Note: It is FFS how a serving network which is not holding the credential of the UE can take the Credentials Holder role.

- access hosting network by using UE onboarding and remote provisioning as specified in TS 23.501 clause 5.30.2.10 with onboarding SUCI/SUPI and other configuration information provisioned using UE Configuration Update (or SoR) procedure while connected to home network.

- access from the serving network to hosting network via NWu interface and N3IWF located in the hosting network using onboarding SUCI/SUPI in registration procedure. Onboarding SUCI/SUPI, N3IWF address, default credentials to establish connectivity via NWu to access hosting network and other data can be configured using UE Configuration Update procedure to the UE. The access credentials can be UE specific or usable by all UEs of a certain serving network. In this case hosting network acts as the overlay network, serving network acts as the underlay network. UE may use PDU session in (overlay) hosting network that is restricted to access only to the localized servicesportal page where the UE can be provisioned with service and network related data.

- access hosting network that offers free services for users in the area, e.g., using sponsored connectivity.

- access hosting network services for subscribers of the serving network (e.g., the PLMN or the SNPN) with which they have agreement. In this case, authorization to offer hosting network services is checked by the serving network.

### 6.12.3 Procedures

#### 6.12.3.1 UE discovery, selection and access for hosting network



Figure 6.12.3.1-1: UE discovery, selection and access for hosting network.

1. Registration Request (Mobility Update) update triggered due to TAC changes.

2. Serving Network detects that the UE moved to area (TA, cell id) where localized service is offered.

3. In TAs where localized servicesis available, the serving network includes hosting network info as part of Registration accept or UE Configuration Update or SoR. The serving network may also include necessary information regarding hosting network (SNPN ID, GIN, DNN, S-NSSAI) for it to obtain limited connectivity to hosting network.

4. UE initiates PDU Session using DNN, S-NSSAI that the network redirects to hosting network portal (PCF policies installed using PDR/FAR rules to redirect to localized services portal).

NOTE 1: UE can use internet PDU Session, reactivate UP and simply use the link provided by the network e.g. in the PCO to reach the hosting network.

5. Depending on information, subscription and authorization obtained for hosting network, UE may connect to hosting network using NWu connectivity or select hosting network directly

NOTE 2: If UE should use hosting network as the underlay network later on and the PLMN as overlay, it might be necessary to provide N3IWF address of the PLMN as well.

### 6.12.4 Impacts on services, entities and interfaces

Editor's note: This clause lists impacts to services, entities, and interfaces.

## 6.13 Solution #13: Exposure enhancements to support providing access to localized services

### 6.13.1 Introduction

Editor's Note: This clause lists the key issue(s) addressed by this solution, and briefly the main principles of the solution.

This solution aims at address key Issue #3 (Enabling NPN as hosting network for providing access to localized services) and Key Issue #5 (Enabling access to localized services via a specific hosting network), in particular:

- How localized service agreements (i.e. a service agreement for a localized service) for a specific occasion (time and location) are automatically established and terminated,

- What is required to enable communication between a network operator deploying a hosting network and a localized services provider: Investigate which type of interaction (e.g., configuration of the hosting network, information reporting) is needed, in such relation to enable the localized services provider for making the best use of the hosting network,

- How and whether the home network, determine the service availability of a hosting network, and interacts with hosting network to authorize home network's subscribers to access home network services via the hosting network, at certain time and location, coverage of the hosting network and services offered by the hosting network,

- How to enable UE to access both home network services and localized services via the hosting network, and seamless service continuity for home network services and localized services when UE moves between different networks providing the same services. This includes how to configure UE with information enabling the UE to be aware of services that can be accessed via a specific network (e.g. home network or hosting NPN).

- How home network determines the need to steer or instruct the UE, and how the home network steers or instructs the UE to select a hosting network for obtaining home network services or localized services or select a network for a specific service which is available from both hosting and home network.

The main principles of this solution are that:

- The localized service provider can act as the AF to manage the localized service agreements among Hosting Network operator, localized service provider, and Home Network or Credentials Holder via exposure interface;

- The localized service provider can act as the AF to manage the subscribed localized service information in subscription data within the Home Network or Credentials Holder or Hosting network via network exposure. This can be performed on a demand basis;

- The network selection information for the target Hosting Network is provisioned/signalled to the UE when the UE is registered in the Home Network; the network selection information is used for discovery and selection of the target Hosting Network; Optionally, the network selection information can be signalled to the UE under certain conditions e.g. when UE enters specific area and/or after certain time;

- When the UE registers in the Hosting Network, the Home Network or the Credentials Holder performs primary authentication and authorization for the UE;

- When the UE accesses to the localized service via Hosting Network, the Hosting Network initiates Network Slice-Specific Authentication and Authorization or PDU Session Secondary Authentication and Authorization to authorize the UE access to the localized service;

- When the UE accesses to the localized service via Hosting Network, the Hosting Network uses the time and location allowed for the UE to perform access control to the localized service;

### 6.13.2 Functional Description

Editor's Note: This clause further details the solution principles and any assumptions made.

Providing access to localized services refers to the capability to provide access to a hosting network (PNI-NPN or SNPN) and a set of services offered by the hosting network provider, other mobile network operators (PLMN or SNP) and 3rd party application providers. The services may be localized (i.e. provided at specific/limited area) and may be bounded in time.

The UE’s with or without prior subscription to the hosting network can access to the localized services via hosting network using access credentials from Home Network or Credentials Holder once the UE has subscribed successfully to the localized services of the hosting network. Then this solution assumes that:

- The localized service provider acting as the application function manages the service agreements among Hosting Network operator, localized service provider, and Home Network or Credentials Holder via network exposure. The service agreements include:

- Availability of the localized service (service identification, service parameters [DNN, S-NSSAI, QoS], service authorization methods [NSSAA or PDU Session SAA], service access methods [LBO or HR], time and location); and

- List of Supported Home Networks or Credentials Holders; and

- List of Supported Hosting Networks;

- UE/User can subscribe to the localized service for a specific Hosting Network via out-of-3GPP means, e.g. online store, portal:

- The UE should be a subscriber of the supported Home Network or should have credentials from the supported Credentials Holder in the service agreement; and

- The target Hosting Network should be one in the list of supported Hosting Networks; and

- The localized service provider should know localized service information selected by the UE/User, e.g., subscribed DNN, S-NSSAI, QoS, service authorization method, service access method, time and location, this information selected by the UE/Use should be covered by the Availability of the localized service in the service agreement. The localized service should also know the information of the subscribed Hosting Network and Home Network or Credentials Holder; and

- The UE/User can obtain the service credentials assigned by the localized service, the service credentials can be used to authenticate and authorize the UE access to the localized service;

- The localized service provider acting as the application function, updates subscription data in the subscribed Home Network or Credentials Holder or Hosting network via network exposure, so the subscription data can contain the localized service information subscribed by a single UE or a group of UEs:

- If the UE will access the Hosting Network using credential from Credentials Holder with AAA Server, then the localized service updates the subscription data in the subscribed Hosting Network, so the subscription data contains the indication that primary AA by AAA-S is required as well as the subscribed localized service information e.g., subscribed DNN, S-NSSAI, QoS, service authorization method, service access method, time and location.

- If the UE will access the Hosting Network using credential from Credentials Holder with AUSF and UDM, then the localized service updates the subscription data in the subscribed Home Network, so the subscription data contains the subscribed Hosting Network information as well as the subscribed localized service information e.g., subscribed DNN, S-NSSAI, QoS, service authorization method, service access method, time and location.

- If the UE will access the Hosting Network using credentials from Home Network, then the localized service updates the subscription data in the subscribed Home Network, so the subscription data contains the subscribed Hosting Network information as well as the subscribed localized service information e.g., subscribed DNN, S-NSSAI, QoS, service authorization method, service access method, time and location.

- The Home Network updates UE with the network selection information for the subscribed Hosting Network (e.g. service identification, Hosting Network ID, temporal validity condition, spatial validity condition) when subscribed time starts and/or when UE enters specific area indicated by the subscribed location contained in the subscription data:

- The temporal validity condition is derived from the subscribed time for the localized service, this indicates the time period when the network selection information is valid;

- The spatial validity condition is derived from the subscribed location for the localized service, this indicates the area where the network selection information is valid;

- The UE moves in the subscribed location for the localized service and the temporal validity condition is still valid, and starts discovery and selection of the Hosting Network.

- The UE registers in the Hosting Network with the access credentials and accesses to the localized services using the service credentials.

- The UE is authenticated and authorized by the Home Network or the Credentials Holder;

- The UE can be provisioned with information related with the subscribed localized service (Allowed NSSAI, service authorization method, URSP rules);

- The UE setups the connectivity to the localized service by establishing a PDU Session with the DNN, S-NSSAI associated with the localized service, the Hosting Network can allocate resources for the PDU Session according to the subscribed QoS or service access method;

- With the subscribed service authorization method, the Hosting Network performs the service authorization using the indicated authorization method;

- With the subscribed time and location, the Hosting Network performs access control to the localized service;

- When the UE moves out the subscribed location for the localized service or the temporal validity condition becomes out-dated,

- The UE de-registers from the Hosting Network, the UE may delete the network selection information for the subscribed Hosting Network and information related with the subscribed localized service;

- The Hosting Network de-registers the UE and releases network resources reserved for the UE;

- The localized service provider may delete the localized service information from subscription data in the Home Network or Credentials Holder or Hosting network;

Figure 6.13.2-1 depicts the scenarios for support of providing access to localized services.



Figure 6.13.2-1: Support of providing access to localized services via exposure enhancements

### 6.13.3 Procedures

Editor's Note: This clause describes procedures and information flows for the solution.

### 6.13.4 Impacts on services, entities, and interfaces

Editor's Note: This clause lists impacts to services, entities, and interfaces.

### 6.14 Solution #14: Solution for hosting network selection

### 6.14.1 Introduction

This solution solves several requirements listed in Key Issue#4.

### 6.14.2 Functional Description

In this solution, the hosting network sends Hosting Network Selection and Access Information to the local service provider, who provides service to UEs accessing the hosting network.

The Hosting Network Selection and Access Information consists the following information:

- Hosting Network Identifier, e.g. SNPN ID in case of the hosting network is an SNPN, CAG ID and PLMN ID in case of the hosting network is a PNI-NPN.

- The time condition information when the hosting network provides access service.

- The location condition information where the hosting network provides access service.

- Optionally, credential used for the UE to access the hosting network. Credential may be only provided in case hosting network is an SNPN.

The UE receives the Hosting Network Selection and Access Information from the localized service provider. The UE selects a hosting network when the time and location condition information is satisfied.

### 6.14.3 Procedures



Figure 6.14.3-1 UE receives hosting network selection and access information from local SP

1. The hosting network server sends Hosting Network Selection and Access Information to the NEF.

The hosting network (HN) server stores the Hosting Network Selection and Access Information and send it to the local service providers who provide services to the UEs accessing the hosting network.

2. The NEF sends the Hosting Network Selection and Access Information to the local service provider App.

Editor's note: The details of step 1 and 2 are FFS.

3. The UE establishes connection with the local service provider App.

The UE may establish a PDU Session via its home network and establishes connection via the PDU Session.

NOTE: How the UE knows the address of the local service provider App is out of 3GPP scope.

4. The UE selects a hosting network based on the Hosting Network Identifier in the Hosting Network Selection and Access Information when the corresponding time and location condition information is satisfied.

Editor's note: Whether the Hosting Network Selection and Access Information can trigger manual hosting network selection or not is FFS.

### 6.14.4 Impacts on services, entities, and interfaces

UE impact:

- Ability to receive Hosting Network Selection and Access Information from the local service provider App.

- Ability to perform hosting network selection based on the received Hosting Network Selection and Access Information.

Hosting Network impact:

- Ability to send Hosting Network Selection and Access Information to the local service provider.

## 6.15 Solution #15: Local service provisioning via PLMN

### 6.15.1 Introduction

This solution mainly addresses Key Issue #4 and #5. The local service platform generates and provides the local service access information and provides it to the UE, through the UE's serving PLMN.

### 6.15.2 Functional Description

This solution assumes that the local service provider has a business agreement with the PLMN operator. Its service platform utilizes the PLMN's network exposure framework for providing the local service access information to the requesting UE.

The local service platform monitors the Local Service Subscription events through the PLMN network exposure function. Such an event is triggered when a UE initiates subscription request (e.g., via NAS request) for a interested local service. The UE may have learned the desired local service information (e.g. local service name/identifier) via various channels that are out of 3GPP scope.

When the local service platform receives the Local Service Subscription event, and if it is acceptable, it generates the local service access information for the requesting UE and provides it to the UE through the PLMN network exposure function. The local service access information may include the hosting network identifier, temporary credential for accessing the hosting network and local service, etc.

With the local service information, the UE should be able to access the hosting network and may further obtain more configuration for accessing the local service from the hosting network.

### 6.15.3 Procedures



Figure 6.15.3-1 Local service provisioning via PLMN

1. The AF in the local service platform subscribes to the Local Service Subscription event notification from the 5GC. The AF indicates its local service identifier in the subscription request.

2. The NEF determines the AMFs that serve the areas where the local service is available and subscribes to the Local Service Subscription event notification from the AMF.

3. The UE has obtained the local service related information such as local service identifier through various channels that are out of 3GPP scope. The local service subscription request may be triggered, for example, by the user input or when entering the area where the local service is available.

4. The UE initiates local service subscription by sending a NAS request to the AMF. The UE indicates the desired local service identifier in the request.

5. The AMF detects the Local Service Subscription event and sends the event notification to the NEF.

6. The NEF forwards the event notification to the AF in the local service platform.

7. If the subscription request is acceptable, the local service platform generates the information necessary for accessing the local service, such as the initial credentials.

8. The local service platform uses the NEF/UDM 's external parameter provisioning procedure to deliver the local service access information to the UE that has requested the subscription.

### 6.15.4 Impacts on Services, Entities, and Interfaces

NEF, UDM and AMF need to support new Local Service Subscription event.

AMF and UE need to support new NAS message or IE that indicates local service subscription request.

## 6.16 Solution #16: Access to SNPN with NG-RAN and to WLAN Access Network using the same credentials

### 6.16.1 Introduction

The architecture defined for non-3GPP access in PLMNs for trusted and untrusted access relied on the assumption that the PLMN owns already a 3GPP based CN and therefore the 3GPP identities and credentials are used when the UE is also accessing over non-3GPP access e.g. WLAN. It is also assumed that the PLMN offers services e.g. IMS voice/SMS that the UE cannot access directly from the non-3GPP access and therefore it needs to connect to the 3GPP CN. This is achieved for example through connection to N3WIF in case of untrusted non-3GPP access architecture or for Trusted Non-3GPP access using the network elements of TNAP and TNGF.

These assumptions may though not hold true in “enterprise” environment that will possibly deploy 3GPP based “private cellular network”/SNPN while it already has a deployed WLAN infrastructure in place. For example in such enterprise environment the identities and credentials used for WLAN authentication could be already provisioned to the “enterprise” UEs before the SNPN is deployed. In such network environment also access to specific services can be restricted through using a VPN that runs on top of internet connection provided from WLAN or using application layer authentication and therefore there is possibly no need to have N3IWF in the “untrusted non-3GPP access” architecture and there is no need to upgrade the existing WLAN infrastructure to support what is required from TNAP and TGNF in the “trusted non-3GPP access” architecture.

The other two aspects that need consideration is the access network selection and mobility. For access network selection mechanisms standardised by 3GPP e.g. using ANDSP need to be enhanced for Non-Seamless WLAN Offload or rely on local UE configuration. Seamless mobility is not in scope of this solution since many applications can also work with nomadic mobility.

The solution describes how UE can access an SNPN with NG-RAN on one hand and a WLAN Access Network on the other hand using the same credentials. If the credentials use AKA and USIM authentication and are stored in UDM, the existing mechanisms for Non-Seamless WLAN Offload defined in TS 33.501 [10] and TS 23.501 [3] apply.

If the credentials are stored in a AAA Server possibly new authentication procedures and Non-Seamless WLAN Offload (NSWO) architecture need to be defined. After being authenticated the UE does not have access to 5GC via WLAN and it performs only Non-seamless WLAN offload traffic.

In summary this solution proposes the following enhancements:

1. in case of SNPN with non-3GPP credentials there has to be an association between the WiFi and cellular (non-3GPP) credentials that are stored in the cellular modem and
2. WLANSPs support for SNPN ID, GIN to identify WLAN AN associated with the SNPN

The details are described in the following sections.

### 6.16.2 Functional Description

The solution focuses on the case that the credentials are stored in a AAA Server and has the following properties:

* The same AAA Server that is used for WLAN access authentication in a WLAN Access Network is also used for primary authentication in SNPN with NG-RAN by re-using the architecture defined for “Credentials Holder for primary authentication and authorization” in TS 23.501 [3] clause 5.30.2.9.2.
* SWa interface that is based on Radius/Diameter is assumed between WLAN Access Network and AAA-S
* The UE uses the same permanent identity and credentials for primary authentication in SNPN and for WLAN access authentication in WLAN Access Network

- For example the identity and credentials already used for WLAN access authentication are also used in SNPN as SUPI in NAI format.

* WLAN network selection can be based on enhanced WLAN Selection Policy (WLANSP) rules from ANSDP used for Non-Seamless WiFi Offload i.e. as defined in TS 23.402 [9] clause 4.8.2.1.6 or local configuration in the UE.

NOTE: The WLANSP rules in rel.17 are only supported for PLMNs.

* The SNPN can configure the UE to use a specific identity (SUCI) and credentials for specific WLAN networks, e.g. by associating the conditions from WLANSP rules with a specific identity (SUPI) and credentials to be used for the specific WLAN network e.g. based on the PreferredSSIDList or the HomeNetwork attribute containing the SNPN-id .
* The WLAN Access Network and the SNPN provide access to the same Data Network e.g. internet or enterprise network
* Optionally assignment of IP addresses in the WLAN Access Network and in the SNPN can happen from same IP address pool, if needed, based on local policy.

Seamless mobility between the SNPN and the WLAN Access Network is not supported by this architecture. Seamless mobility can be provided if additionally N3IWF is deployed but this is out of scope of this specific solution.



Figure 6.16.2-1: Access to SNPN with NG-RAN and to WLAN Access Network using the same credentials

### 6.16.3 Procedures

##### 6.16.3.1 WLAN Authentication with AAA Server

The figure 6.16.3-1 describes the WLAN authentication using a AAA Server.



Figure 6.16.3-1: WLAN authentication sharing with AAA Server as in Figure 6.x.2-1

0) If the SNPN supports the architecture as in Figure 6.x.2-1 and wants the UE to use the same credentials for access to a WLAN Access Network and to this SNPN, then the SNPN configures in the UE the same permanent identity and credentials for primary authentication with the SNPN and for WLAN access authentication with the WLAN Access Network. WLAN network selection can be based on enhanced WLAN Selection Policy (WLANSP) rules from ANSDP used for Non-Seamless WiFi Offload i.e. as defined in TS 23.402 [9] clause 4.8.2.1.6.

The SNPN can configure the UE to use a specific identity (SUCI) and credentials for specific WLAN networks, e.g. by associating the conditions from WLANSP rules that in rel.17 are only supported for PLMNs with a specific identity (SUCI) and credentials to be used for the specific WLAN network e.g. based on the PreferredSSIDList or the HomeNetwork attribute containing the SNPN-id .

Steps 1-8 are out of scope of SA2 and are shown for information:

1. A connection is established between the UE and the WLAN AP, using a specific procedure based on IEEE 802.11.

2. The WLAN AP sends an EAP Identity Request to the UE.

3. The UE always sends the SUCI in NAI format.

4. The WLAN AP sends a SWa protocol message (could be over RADIUS or Diameter interface) with EAP identity response, NAI containing the SUCI to AAA Proxy.

5. If AAA Proxy is used it forwards the SWa message to AAA Server based on the NAI of the SUCI.

6. EAP authentication is performed. Any EAP method can be used for WLAN authentication between the UE and the AAA Server.

7, 8. AAA Server performs successful authentication. When AAA Proxy is used sends a SWa protocol message with EAP-success and possibly other security parameters to WLAN. EAP-success message is forwarded from WLAN AP to the UE.

Editor’s Note: New authentication procedures and Non-Seamless WLAN Offload (NSWO) architecture need to be defined. Security aspects are in SA3 scope.

##### 6.16.3.2 User plane aspects

The UE needs to acquire a local IP address on WLAN access that may optionally be from same IP address pool, if needed, based on local policy.

Following same principles as in TS 23.501 [3] for UE supporting non-seamless WLAN offload, while connected to WLAN access and registered in the SNPN via NG-RAN, the UE can route specific data flows via the WLAN access without traversing the 5GC of SNPN. The UE data flows are identified using URSP configuration for Non-Seamless Offload, or UE Local Configurations as defined in TS 23.503 [5]. For these data flows, the UE uses the local IP address allocated by the WLAN access network and no IP address preservation is provided between WLAN and SNPN.

### 6.16.4 Impacts on services, entities, and interfaces

UE:

* uses the same permanent identity (SUCI) and credentials for primary authentication in SNPN and for WLAN access authentication in a WLAN Access Network
* UE is optionally configured to associate the conditions from WLANSP rules that in rel.17 are only supported for PLMNs with specific identity (SUPI) and credentials to be used for the specific WLAN network e.g. based on the PreferredSSIDList or the HomeNetwork attribute containing the SNPN-id . Otherwise local configuration can be used.

-New authentication procedures and Non-Seamless WLAN Offload (NSWO) architecture need to be defined. Security aspects are in SA3 scope.WLAN AP (informative impact)

* Support compatible security mechanisms with 5GS
* SWa interface that is based on Radius/Diameter is assumed between WLAN Access Network and AAA-S

No other impacts in the UE, NG-RAN, and 5GC are identified.

## 6.17 Solution #17: UE Group specific NAS level congestion control

### 6.17.1 Introduction

One of the aspects of the Key Issue #6 is how to mitigate user plane and control plane overload caused by a high number of UEs returning from a temporary local access of a hosting network to their home network in a very short period of time.

This solution describes how the existing mechanisms defined in clause 5.19.7.5 of TS 23.501 can be enhanced to support NAS level congestion control for a specific group of UEs that has temporarily accessed to a local service(s) and has attempted to return their home network almost simultaneously.

### 6.17.2 Functional Description

The proposed solution focuses on using group specific NAS level congestion control mechanism to mitigate user plane and control plane overload caused by a higher number of UEs returning from a hosting network to their home network in a very short period of time.

Group specific NAS level congestion control is performed at the 5GC only, and it is transparent to UE. The AMF or SMF or both may apply NAS level congestion control for a UE associated to an Internal-Group Identifier described in clause 5.9.7 of TS 23.501.

The home network associates UEs temporarily accessing localized services to an Internal-Group Identifier, which can be specific to each local hosting network and/or service, and applies UE group-specific NAS level congestion control to mitigate user plane and control plane overload caused during the return of UEs. The home network removes the UE from the group after it has returned to the home network.

Editor's note: It is FFS for how long the home network maintains the grouping.

### 6.17.3 Procedures

The home network (HPLMN) and/or local hosting network (LHN) may group the UEs based on the information:

- when the UE-initiated de-registration request message sent from UE to its HPLMN in order to access to local services provided by a LHN, UE indicates in the de-registration message (i.e., “hosting network access” or “5GS local network access indication”) that the de-registration request is to access to local services provided by a LHN; or

- when the network-initiated de-registration request message sent from network to the UE in order to enable the UE to register with a LHN to access to local services, the network indicates in the de-registration message (i.e., “hosting network access” or “5GS local network access indication”) that the de-registration request is to enable UE to register with a LHN to access to local services.

The home network (HPLMN) may utilize:

- an application function (AF) residing in the local hosting network(s); or

- an exposure framework from local hosting network(s),

to receive information on users who requested access or has accessed to the local service(s) in order to associate users to an Internal-Group Identifier specific to local hosting network(s) and/or local service(s).

Editor's Note: It is FFS whether both options described above can be used at the same time for constructing the Internal-Group by the home network, and whether and how to coordinate between the options

Editor’s Note: It is FFS whether and how new mechanism(s) developed for KI#5 is considered in this solution.

Then, the network (AMF or SMF) applies UE group-specific NAS level congestion control to manage the return of UEs from the LHN to their home PLMN by spreading out the registration attempts over time and limiting the number of UEs attempting to register simultaneously when the UEs accessed to the local service(s) provided by the LHN(s) are returning back to their home network.

### 6.17.4 Impacts on services, entities and interfaces

UDM:

- Support for local hosting network and/or local service information in the Internal-Group Identifier.

UE:

- Shall support configuration and handling of the localized sevice related de-registration information (i.e., “hosting network access” or “5GS local network access indication”).

AMF:

* Shall support localized service related de-registration information element (i.e., “hosting network access” or “5GS local network access indication”).

AMF/SMF:

* Shall apply Group Specific NAS level congestion control when UEs temporarily accessed to local service(s).

NEF:

* Shall support exposure from local hosting networks

## 6.18 Solution #18: Steering of UE to select hosting network for obtaining localized services

### 6.18.1 Introduction

One of the aspects of the key issue #5 is how the network would determine the need to steer or instruct the UE to hosting network and other aspect is on how actually would network steer the UE toward the hosting network.

The proposed solution focuses on the case when based on location and time, certain localized services are available, which are being provided by the hosting network and using “Steering of Roaming” mechanism to allow service provider (PLMN or 3rd Party service provider) to update the UE with required information on availability of hosting networks along with the services they are providing. This information will assist the UE to make the switch to appropriate hosting network for obtaining localized services.

Steering of Roaming information container would carry the “operator defined hosting network selector list”, which will assist the UE to switch to hosting network for obtaining localized services.

### 6.18.2 Functional Description

The proposed solution will be using similar concept and mechanism to “Steering of Roaming” as defined in TS 23.122 [6].

As per the service level agreement between the PLMN operator and hosting network operator/service provider, UE’s HPLMN may create a “operator defined hosting network selector list” for the purpose of automatically steering the UE between PLMN and hosting networks.

HPLMN or the Service Provider will use the UE’s current location and time to trigger the steering information toward the UE.

The “operator defined hosting network selector list” may consist of following information:

- A prioritized list of hosting network identifiers (SNPN IDs).

- A validity time window may be associated with the SNPN ID in the “operator defined hosting network selector list”.

- A valid list of tracking areas (TAs) may be associated with the SNPN ID in the “operator defined hosting network selector list”.

Editor's Note: It is FFS which network(home network, serving network, hosting network) the information of tracking area belongs to.

Editor's Note: It is FFS whether the new list is per localized service, or it is applicable for all localized services.

### 6.18.3 Procedures

Figure XX shows the flow of steering of roaming information container with “operator defined hosting network selector list” to assist in UE with selection of hosting network. This procedure can be triggered during or after registration, UE’s location, and time window are critical factors in deciding when this procedure is triggered by the UDM/SoR-AF/SP (Service Provider).



Figure 6.X.3-1: Steering the UE with hosting network information

Procedure:

1. The SoR-AF/SP to HPLMN UDM: Nudm\_ParameterProvision is sent to the HPLMN UDM to trigger the update of the UE with new list of “operator defined hosting network selector list”.

2. The HPLMN UDM to the AMF: The UDM notifies the changes of the user profile to the affected AMF by the means of invoking Nudm\_SDM\_Notification service operation.

3. The AMF to the UE: the AMF sends a DL NAS TRANSPORT message to the served UE. The AMF includes in the DL NAS TRANSPORT message the steering of roaming information received from the UDM.

4. UE: Upon receiving the SoR information, UE shall perform the security check on it.

5. The UE to AMF: If the UDM has requested an acknowledgement from the UE in the DL NAS TRANSPORT message, the UE sends an UL NAS TRANSPORT message to the serving AMF with an SOR transparent container including the UE acknowledgement.

6. The AMF to the HPLMN UDM: If the UL NAS TRANSPORT message with an SOR transparent container is received, the AMF uses the Nudm\_SDM\_Info service operation to provide the received SOR transparent container to the UDM.

7. The HPLMN UDM to the SOR-AF: HPLMN UDM informs the SoR-AF/Service Provider (SP) about the successful delivery of the SoR information (i.e., “operator defined hosting network selector list”).

8. The UE will use the received steering of roaming information to assist in selection of the hosting network for obtaining localized services. The UE would select an SNPN if available and allowable for obtaining localized services, identified by an SNPN identity contained in the “operator defined hosting network selector list” in priority order.

Editor's Note: Switch between SNPN/PLMN access mode for network selection is FFS.

### 6.18.4 Impacts on services, entities, and interfaces

UDM:

- Support for additional list (i.e., “operator defined hosting network selector list”) in steering of roaming information.

SoR-AF/SP:

- Support for additional list (i.e., “operator defined hosting network selector list”) in steering of roaming information.

UE:

- Shall support configuration and handling of the new list (i.e., “operator defined hosting network selector list”)

- Use the “operator defined hosting network selector list for selection of hosting network.

# 7 Evaluation

Editor's note: This clause provides an evaluation of the solutions.

# 8 Conclusions

Editor's note: This clause will capture conclusions from the study.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **Tdoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA2#149e | S2-2200487 | - | - | - | Proposed skeleton agreed at SA2#149e | 0.0.0 |
| 2022-02 | SA2#149e |  | - | - | - | S2-2200488 (skeleton), S2-2200488, S2-2200489, S2-2201749, S2-2201750, S2-2201860, S2-2201752, S2-2201753, S2-2201850  Editorial changes by rapporteur. | 0.1.0 |
| 2022-04 | SA2#150e |  |  |  |  | S2-2203442, S2-2203443, S2-2203444, S2-2203445, S2-2203446, S2-2203447, S2-2203448, S2-2203449, S2-2203450, S2-2203451, S2-2203452, S2-2203453, S2-2202258, S2-2203454, S2-2203455, S2-2202457, S2-2203456, S2-2203457, S2-2203458, S2-2203459, S2-2202526, S2-2203460, S2-2203461, S2-2202931 | 0.2.0 |