3GPP TR 23.740 V16.0.0 (2018-12)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on Enhancement of Network Slicing

(Release 16)

** 

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

Keywords

3GPP, 5G System, Network Slicing

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

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

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

All rights reserved.

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

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

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

Contents

Foreword [6](#__RefHeading___Toc532994177)

1 Scope [7](#__RefHeading___Toc532994178)

2 References [7](#__RefHeading___Toc532994179)

3 Definitions and abbreviations [7](#__RefHeading___Toc532994180)

3.1 Definitions [7](#__RefHeading___Toc532994181)

3.2 Abbreviations [8](#__RefHeading___Toc532994182)

4 Architectural Assumptions and Requirements [8](#__RefHeading___Toc532994183)

5 Key Issues [8](#__RefHeading___Toc532994184)

5.1 Key Issue#1: Mutually exclusive access to Network Slices [8](#__RefHeading___Toc532994185)

5.1.1 Description [8](#__RefHeading___Toc532994186)

5.2 Key issue#2: Enabling interworking for slicing between EPC and 5GC [9](#__RefHeading___Toc532994187)

5.2.1 Description [9](#__RefHeading___Toc532994188)

5.3 Key Issue#3: Access to specific Network Slices authorized and authenticated through additional User Identifiers [9](#__RefHeading___Toc532994189)

5.3.1 Description [9](#__RefHeading___Toc532994190)

6 Solutions [10](#__RefHeading___Toc532994191)

6.1 Solutions for KI#1 [10](#__RefHeading___Toc532994192)

6.1.1 Solution #1.1: Mutually Exclusive Access to Network Slices via the use of URSP [10](#__RefHeading___Toc532994193)

6.1.1.1 Introduction [10](#__RefHeading___Toc532994194)

6.1.1.2 Functional description [10](#__RefHeading___Toc532994195)

6.1.1.3 Procedures [11](#__RefHeading___Toc532994196)

6.1.1.4 Impacts on existing entities and interfaces [11](#__RefHeading___Toc532994197)

6.1.1.5 Evaluation [11](#__RefHeading___Toc532994198)

6.1.2 Solution #1.2: Mutually Exclusive Access to Network Slices via UE configuration [11](#__RefHeading___Toc532994199)

6.1.2.1 Introduction [11](#__RefHeading___Toc532994200)

6.1.2.2 Functional description [12](#__RefHeading___Toc532994201)

6.1.2.3 Procedures [12](#__RefHeading___Toc532994202)

6.1.2.4 Impacts on existing entities and interfaces [12](#__RefHeading___Toc532994203)

6.1.2.5 Evaluation [13](#__RefHeading___Toc532994204)

6.1.3 Solution #1.3: Solution to Key issue#1: Mutual exclusion awareness in UE. [13](#__RefHeading___Toc532994205)

6.1.3.1 Introduction [13](#__RefHeading___Toc532994206)

6.1.3.2 Functional description [14](#__RefHeading___Toc532994207)

6.1.3.3 Procedures [15](#__RefHeading___Toc532994208)

6.1.3.4 Impacts on existing entities and interfaces [18](#__RefHeading___Toc532994209)

6.1.3.5 Evaluation [18](#__RefHeading___Toc532994210)

6.1.4 Solution#1.4: Slicing Group Support for Mutually Exclusive Access to Network Slices [19](#__RefHeading___Toc532994211)

6.1.4.1 Introduction [19](#__RefHeading___Toc532994212)

6.1.4.1.1 Design principles [19](#__RefHeading___Toc532994213)

6.1.4.1.2 Working Assumptions and Concepts of Mutually Exclusive Access Slicing Group [19](#__RefHeading___Toc532994214)

6.1.4.2 Functional description [20](#__RefHeading___Toc532994215)

6.1.4.2.1 Concepts of Mutually Exclusive Access Slicing Group [20](#__RefHeading___Toc532994216)

6.1.4.2.2 Identification of Mutually Exclusive Access Slicing Group [21](#__RefHeading___Toc532994217)

6.1.4.2.3 UE Support for Mutually Exclusive Access Slicing Group [22](#__RefHeading___Toc532994218)

6.1.4.2.4 Roaming Support for Mutually Exclusive Access Slicing Group [22](#__RefHeading___Toc532994219)

6.1.4.2.5 URSP/NSSP Support for Mutually Exclusive Access Slicing Group [23](#__RefHeading___Toc532994220)

6.1.2.4.6 AMF Support for Mutually Exclusive Access Slicing Group [23](#__RefHeading___Toc532994221)

6.1.4.3 Procedures [25](#__RefHeading___Toc532994222)

6.1.4.3.1 UE Registration with Mutually Exclusive Access Slicing Group [25](#__RefHeading___Toc532994223)

6.1.4.4 Impacts on existing entities and interfaces [28](#__RefHeading___Toc532994224)

6.1.4.5 Evaluation [28](#__RefHeading___Toc532994225)

6.1.5 Solution #1.5: Mutually Exclusive Access to Network Slices using existing mechanisms [28](#__RefHeading___Toc532994226)

6.1.5.1 Introduction [28](#__RefHeading___Toc532994227)

6.1.5.2 Functional description [28](#__RefHeading___Toc532994228)

6.1.5.2.1 General assumptions [28](#__RefHeading___Toc532994229)

6.1.5.2.2 Applying proposed logic to an example [29](#__RefHeading___Toc532994230)

6.1.5.3 Procedures [31](#__RefHeading___Toc532994231)

6.1.5.3.1 General [31](#__RefHeading___Toc532994232)

6.1.5.3.2 Signalling within the network [31](#__RefHeading___Toc532994233)

6.1.5.3.3 Interactions with Rel-15 usage of Allowed NSSAI [31](#__RefHeading___Toc532994234)

6.1.5.3.4 Characteristics of the solution [31](#__RefHeading___Toc532994235)

6.1.5.4 Impacts on existing entities and interfaces [31](#__RefHeading___Toc532994236)

6.1.5.5 Evaluation [32](#__RefHeading___Toc532994237)

6.1.6 Solution #1.6: Enabling access control to network slices that cannot be access simultaneously [32](#__RefHeading___Toc532994238)

6.1.6.1 Introduction [32](#__RefHeading___Toc532994239)

6.1.6.1.1 Design Principles [32](#__RefHeading___Toc532994240)

6.1.6.1.2 Working Assumptions [32](#__RefHeading___Toc532994241)

6.1.6.1.3 Network Slice Access Exclusion Rules [33](#__RefHeading___Toc532994242)

6.1.6.2 High-level Description [35](#__RefHeading___Toc532994243)

6.1.6.2.1 Services and Illustrated Procedures [35](#__RefHeading___Toc532994244)

6.1.6.2.1.1 Registration Procedure [35](#__RefHeading___Toc532994245)

6.1.6.2.1.2 Enforcement of mutually exclusive rules [36](#__RefHeading___Toc532994246)

6.1.6.2.1.2.1 PDU Establishment [37](#__RefHeading___Toc532994247)

6.1.6.3 Impacts on existing services and interfaces [37](#__RefHeading___Toc532994248)

6.1.6.4 Evaluation [38](#__RefHeading___Toc532994249)

6.1.7 Solution #1.7: Solutions for MEANS via Slicing Group Indication [38](#__RefHeading___Toc532994250)

6.1.7.1 Introduction [38](#__RefHeading___Toc532994251)

6.1.7.2 Functional description [38](#__RefHeading___Toc532994252)

6.1.7.2.1 UE configuration [38](#__RefHeading___Toc532994253)

6.1.7.2.2 UE subscription [38](#__RefHeading___Toc532994254)

6.1.7.2.3 Operations [38](#__RefHeading___Toc532994255)

6.1.7.2.4 Roaming support [39](#__RefHeading___Toc532994256)

6.1.7.3 Procedures [40](#__RefHeading___Toc532994257)

6.1.7.3.1 RAN configuration [40](#__RefHeading___Toc532994258)

6.1.7.3.2 Registration procedure [40](#__RefHeading___Toc532994259)

6.1.7.4 Impacts on existing entities and interfaces [41](#__RefHeading___Toc532994260)

6.1.7.5 Evaluation [42](#__RefHeading___Toc532994261)

6.1.8 Solution #1.8: Solution to Key issue#1: Access to new group of Network Slices. [42](#__RefHeading___Toc532994262)

6.1.8.1 Introduction [42](#__RefHeading___Toc532994263)

6.1.8.2 Functional description [42](#__RefHeading___Toc532994264)

6.1.8.3 Procedures [42](#__RefHeading___Toc532994265)

6.1.8.4 Impacts on existing entities and interfaces [42](#__RefHeading___Toc532994266)

6.1.8.5 Evaluation [43](#__RefHeading___Toc532994267)

6.2 Solutions for KI#2 [43](#__RefHeading___Toc532994268)

6.2.1 Solution#2.1: Network slice instance selection in initial AMF [43](#__RefHeading___Toc532994269)

6.2.1.1 Introduction [43](#__RefHeading___Toc532994270)

6.2.1.2 Functional description [43](#__RefHeading___Toc532994271)

6.2.1.3 EPS to 5GS handover Procedures [44](#__RefHeading___Toc532994272)

6.2.1.4 Impacts on existing entities and interfaces [45](#__RefHeading___Toc532994273)

6.2.1.5 Evaluation [45](#__RefHeading___Toc532994274)

6.2.2 Solution #2.2: Slice-aware mobility from EPC to 5GC [45](#__RefHeading___Toc532994275)

6.2.2.1 Introduction [45](#__RefHeading___Toc532994276)

6.2.2.2 Functional description [45](#__RefHeading___Toc532994277)

6.2.2.2.1 Idle Mode Mobility from EPC to 5GC [45](#__RefHeading___Toc532994278)

6.2.2.2.2 Connected Mode Mobility from EPC to 5GC [46](#__RefHeading___Toc532994279)

6.2.2.3 Procedures [47](#__RefHeading___Toc532994280)

6.2.2.4 Impacts on existing entities and interfaces [47](#__RefHeading___Toc532994281)

6.2.2.5 Evaluation [47](#__RefHeading___Toc532994282)

6.2.3 Solution #2.3: Inter RAT mobility Slice support [47](#__RefHeading___Toc532994283)

6.2.3.1 Introduction [47](#__RefHeading___Toc532994284)

6.2.3.2 Functional description [47](#__RefHeading___Toc532994285)

6.2.3.3 Procedures [49](#__RefHeading___Toc532994286)

6.2.3.3.1 Registration with AMF and V-SMF change during CONNECTED state mobility [49](#__RefHeading___Toc532994287)

6.2.3.3.2 Registration with AMF and V-SMF change during IDLE state mobility [50](#__RefHeading___Toc532994288)

6.2.3.4 Impacts on existing entities and interfaces [50](#__RefHeading___Toc532994289)

6.2.3.5 Evaluation [51](#__RefHeading___Toc532994290)

6.2.4 Solution #2.4: Connected mode mobility from EPC to 5GC [51](#__RefHeading___Toc532994291)

6.2.4.1 Introduction [51](#__RefHeading___Toc532994292)

6.2.4.2 Functional description [51](#__RefHeading___Toc532994293)

6.2.4.3 Procedures [52](#__RefHeading___Toc532994294)

6.2.4.3.1 Enhancement to PDN connection establishment [52](#__RefHeading___Toc532994295)

6.2.4.3.1 Enhancement to handover preparation from EPC to 5GC [52](#__RefHeading___Toc532994296)

6.2.4.4 Impacts on existing entities and interfaces [53](#__RefHeading___Toc532994297)

6.2.4.5 Evaluation [53](#__RefHeading___Toc532994298)

6.2.5 Solution#2.5: Using the NF discovery to find the S-NSSAI. [53](#__RefHeading___Toc532994299)

6.2.5.1 Introduction [53](#__RefHeading___Toc532994300)

6.2.5.2 Functional description [53](#__RefHeading___Toc532994301)

6.2.5.3 Procedures [54](#__RefHeading___Toc532994302)

6.2.5.3.1 EPS to 5GS handover using N26 interface [54](#__RefHeading___Toc532994303)

6.2.5.4 Impacts on existing entities and interfaces [55](#__RefHeading___Toc532994304)

6.2.5.5 Evaluation [55](#__RefHeading___Toc532994305)

6.3 Solutions for KI#3 [55](#__RefHeading___Toc532994306)

6.3.1 Solution #3.1: Slice Specific Authentication and Authorization using non 3GPP credentials based on secondary authentication [55](#__RefHeading___Toc532994307)

6.3.1.1 Introduction [55](#__RefHeading___Toc532994308)

6.3.1.2 Functional description [56](#__RefHeading___Toc532994309)

6.3.1.3 Procedures [57](#__RefHeading___Toc532994310)

6.3.1.3.1 Slice authentication at first PDU session establishment for the S-NSSAI [57](#__RefHeading___Toc532994311)

6.3.1.4 Impacts on existing entities and interfaces [58](#__RefHeading___Toc532994312)

6.3.1.5 Evaluation [58](#__RefHeading___Toc532994313)

6.3.2 Solution #3.2: Solution to KI#3 on Slice Specific Authentication and Authorization using non 3GPP credentials [58](#__RefHeading___Toc532994314)

6.3.2.1 Introduction [58](#__RefHeading___Toc532994315)

6.3.2.2 Functional description [59](#__RefHeading___Toc532994316)

6.3.2.3 Procedures [60](#__RefHeading___Toc532994317)

6.3.2.3.1 Secondary Authentication and Authorization During Registration [60](#__RefHeading___Toc532994318)

6.3.2.3.2 Secondary Re-Authentication and Re-Authorization after Registration [63](#__RefHeading___Toc532994319)

6.3.2.4 Impacts on existing entities and interfaces [63](#__RefHeading___Toc532994320)

6.3.2.5 Evaluation [63](#__RefHeading___Toc532994321)

6.3.3 Solution #3.3: Solution for configuration of network slice authentication [64](#__RefHeading___Toc532994322)

6.3.3.1 Introduction [64](#__RefHeading___Toc532994323)

6.3.3.2 Functional description [64](#__RefHeading___Toc532994324)

6.3.3.3 Procedures [64](#__RefHeading___Toc532994325)

6.3.3.4 Impacts on existing entities and interfaces [64](#__RefHeading___Toc532994326)

6.3.3.5 Evaluation [64](#__RefHeading___Toc532994327)

7 Evaluation [64](#__RefHeading___Toc532994328)

7.1 Evaluations Criteria for KI#1: Mutually Exclusive Access to Network Slices [64](#__RefHeading___Toc532994329)

7.2 Evaluations for KI#2: Enabling interworking for slicing between EPC and 5GC [66](#__RefHeading___Toc532994330)

8 Conclusions [67](#__RefHeading___Toc532994331)

8.1 Conclusions for key issue #1 - Mutually exclusive access to Network Slices [67](#__RefHeading___Toc532994332)

8.1.1 Enhancements for change of a set of Network Slices [68](#__RefHeading___Toc532994333)

8.2 Conclusions for key issue #2 - Enabling interworking for slicing between EPC and 5GC [69](#__RefHeading___Toc532994334)

8.3 Conclusions for key issue #3 - Access to specific Network Slices authorized and authenticated through additional User Identifiers [69](#__RefHeading___Toc532994335)

Annex A: Change history [70](#__RefHeading___Toc532994336)

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

# 1 Scope

The scope of this Technical Report is:

- Identify, prioritize and study the practical non-roaming and roaming deployment scenarios and system impacts when the 5GS is not able to support all possible combination of S-NSSAIs for the UE, and the aspects of mutually exclusive access to Network Slices.

- Study the possible enhancement for the Network Slicing interworking with EPC for Connected and Idle modes.

- Study how to provide Network Slice Access authentication and authorization specific for the Network Slice Access authorization that uses User Identities and Credentials different from the 3GPP SUPI and that takes place after the primary authentication which is still required between the UE and the 5GS for PLMN access authorization and authentication.

# 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 23.501: "System Architecture for the 5G System; Stage 2".

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

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[5] 3GPP TS 38.300: "NR and NG-RAN Overall Description; Stage 2".

[6] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[7] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

# 3 Definitions and abbreviations

## 3.1 Definitions

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

**Mutually Exclusive Access to Network Slices**: The access to Network Slices is considered to be mutually exclusive for a UE when their respective S-NSSAIs are both present in the UE's subscription and the UE is prevented from accessing both S-NSSAIs simultaneously.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] apply.

# 4 Architectural Assumptions and Requirements

For Mutually Exclusive Access to Network Slices the following assumptions apply:

- It is assumed that the support of mutually exclusive access to network slices uses Rel-15 network slicing feature as the baseline.

- Support of the Mutually Exclusive Access to Network Slices in a PLMN shall not impact Rel-15 5G UEs' behaviour.

- The network operator shall be able to ensure that the UE is prevented to access Network Slices which are mutually exclusive for that UE.

- It is assumed that a UE supporting mutually exclusive access to network slices shall be able to operate in a Rel-15 5GS.

- Rel-16 5G UE and core may support Mutually Exclusive Access to Network Slices.

For interworking for slicing between EPC and 5GC the following assumptions apply:

- It is assumed that the interworking for slicing between EPC and 5GC uses Rel-15 solution as the basis.

- The interworking for slicing between EPC and 5GC shall not impact Rel-15 5G UEs behaviour.

- The system shall support slicing interworking between EPC and 5GC for roaming case when the PGW-C+SMF is Rel-15.

# 5 Key Issues

## 5.1 Key Issue#1: Mutually exclusive access to Network Slices

### 5.1.1 Description

Several scenarios addressing access control to mutually exclusive Network Slices have been identified, i.e. due to deployment, regulation or per SLA, some UEs may be restricted from using two services (S-NSSAIs) simultaneously.

Such scenarios can include (but not limited to):

- by internal regulation (of the subscriber, of the employer, of the operator, etc): for example, it might be forbidden for a UE to access "regular" services and "specific" services, e.g. a UE used by a government officer might be restricted to be either in "off-duty" (regular) or "on-duty" (specific) mode. It is forbidden by regulation for the UE to access simultaneously the off-duty services and the on-duty services.

- by network capability: for example, a factory device may have two modes of operations: "maintenance mode" (used to perform updates, e.g. blueprints upload, check the status of the devices, monitoring and maintenance, etc) and a "ultra-low latency factory mode", where the device receives URLLC commands to perform its duty. In that case, the AMF instance used for the URLLC factory slice may be tailored specifically to that duty, and not be able to support other services such as file database access, etc. In that case, the device may have to select either mode and not connect to both simultaneously.

To address the above mentioned scenarios this key issue will:

1) Identify whether existing Release 15 System procedures are able to allow access control to mutually exclusive Network Slices.

2) Identify whether improvements to existing Release 15 System procedures are needed when controlling the access to mutually exclusive Network Slices, including aspects of both UE and network.

To achieve those results this key issue will answer (not limited to) the following questions:

- Which information is used to support mutually exclusive access to Network Slices in the UE and/or in the network?

- How to support the UE to select the particular network slice(s) that can serve the UE simultaneously?

- How the above information is used to support mutually exclusive access to Network Slices both in the non-roaming and in the roaming case?

- In roaming cases, how the solutions would work when the Serving PLMN supports mutually exclusive Network Slices, whereas the HPLMN does not (and vice versa)?

- Which network functions are involved in determining/providing the above information, and how?

- Should the above information be pre-configured in the UE or dynamically handled by the network for the UE?

- How can mutually exclusive access to Network Slices be enforced by the network?

- What are the System impacts, if any, to existing Release 15 procedures to enable the network to control simultaneous access from a UE to different Network Slices?

- How to ensure that introduction of support for mutually exclusive Network Slices does not disrupt the normal operation of Release 15 UEs?

## 5.2 Key issue#2: Enabling interworking for slicing between EPC and 5GC

### 5.2.1 Description

In Rel-15, when the UE has a set of PDN connections active in the EPC (for which the UE has been given a corresponding S-NSSAI by the CN), when the UE moves to the 5GC the serving AMF is not selected considering the slices associated to the active PDN connections. This may lead to scenarios where the AMF may not be able to serve all the PDU sessions that the UE intends to move to the 5GC. It is desirable for Rel-16 to study whether solutions are possible and worthwhile to minimize the impact of mobility procedures from EPC to 5GC on the slices corresponding to the PDN connective active in the EPC.

The key issue aims at addressing at least the following open aspects when the UE moves between EPC and 5GC, or vice versa:

- Selecting an AMF based on the slices associated to the active PDN connections the UE has in the EPC.

- Selecting an appropriate V-SMF based on the slices associated to the active PDN connections the UE has in the EPC.

- Transferring (in both idle and connected modes) multiple simultaneous PDU Sessions to the same DNN that are associated to different slices and served by different (H-)SMFs.

## 5.3 Key Issue#3: Access to specific Network Slices authorized and authenticated through additional User Identifiers

### 5.3.1 Description

This key issue will study how to provide Network Slice Access authentication and authorization specific for the Network Slice Access authorization that uses User Identities and Credentials different from the 3GPP SUPI and that takes place after the primary authentication which is still required between the UE and the 5GS for PLMN access authorization and authentication.

In particular, the KI will address: Access control to Network Slices that require additional authorization and authentication:

- How do the UE and the Network know that additional authorization and authentication is required for a Network Slice?

- How is the additional authorization and authentication triggered and performed? E.g. which procedures are used and when.

# 6 Solutions

## 6.1 Solutions for KI#1

### 6.1.1 Solution #1.1: Mutually Exclusive Access to Network Slices via the use of URSP

#### 6.1.1.1 Introduction

This is a solution to Key Issue #1, "Mutually Exclusive Access to Network Slices" (MEANS).This solution assumes the following:

- It is assumed that the network deployments in the home and the visited networks are designed according to the requirements for MEANS, and that the "mutually exclusive" network slices are not sharing resources (including no common AMF Set). This ensures that the NSSF will never grant access to both network slices simultaneously even if a UE requests it (e.g. due to SIM swap). As in Rel-15, NSSF internal policies dictate which network slice would be selected in this case.

- It is assumed that the "mutual exclusivity" of network slices is per network deployment, and is common to all UEs subscribed to both network slices.

- It is assumed that the UE has internal logic (e.g. MMI, or software support) to understand which applications are needed at a given time (e.g. "on duty" vs "off duty", "maintenance" vs "factory", etc), which is beyond the scope of this solution to address. If a SIM swap happens to a UE not understanding the purpose of the applications, it is expected that the UE would not use these applications anyway.

- This solution assumes that the supporting UE would parse the URSP to determine the S-NSSAIs to include in the Requested NSSAI. This behaviour is not required in Rel-15.

- It is assumed that PLMN are going to deploy their network slices in their networks so that all the services available to the users can be used simultaneously (i.e. there will be at least a set of network slice instances in the home network that can offer all the services (S-NSSAIs) that the UE can request simultaneously in its home network), except for network slices that are intended to be under mutually exclusive access by UEs.

- It is assumed that PLMNs are going to organise their SLAs so that network slices in the roaming partners' networks are going to offer all services available to the users simultaneously (i.e. there will be at least a set of network slice instances in the roaming partner network that can offer all the services (S-NSSAIs) that the UE can request simultaneously in that network), except for network slices that are intended to be under mutually exclusive access by UEs.

- This means that the enforcement of the MEANS in roaming scenarios is enforced via SLA (the roaming partner would not allow a UE to access MEANS slices simultaneously, e.g. via sharing the same AMF), and that when UEs needing MEANS in roaming partners' networks not supporting such SLA requirements would not receive the Subscribed S-NSSAIs of the UE that could result in such violation of the MEANS.

### 6.1.1.2 Functional description

This solution proposes to introduce a new (optional, to be ignored if not understood) sub-field, the S-NSSAI Group, in the URSP, as part of the Network Slice Selection field of the Route Selection component, with the following use:

- If an S-NSSAI value in the URSP is associated with an S-NSSAI Group, all instances of this S-NSSAI in the URSP shall be associated with the same S-NSSAI Group value.

- If the UE includes in the Requested NSSAI (or its associated mapping) an S-NSSAI value in the URSP is associated with an S-NSSAI Group, the UE shall not include in the Requested NSSAI another S-NSSAI value associated with a different S-NSSAI Group.

NOTE: This solution does not propose a specific encoding or limitation to the S-NSSAI Group, however, it is expected that very few groups will be needed, therefore an encoding allowing up to 2 ~ 8 group values is expected to be sufficient.

### 6.1.1.3 Procedures

No new procedures are required with this solution.

### 6.1.1.4 Impacts on existing entities and interfaces

UE impact:

- This solution only impacts UE supporting the feature. UEs not supporting the feature should not receive such URSP information (by design: since they do not need the "exclusion service", they do not need to receive configuration for such "exclusion"), and should ignore it if received nonetheless. The supporting UE would need to parse the URSP in order to fill the Requested NSSAI.

Network impact (serving and home):

- This solution does **not** impact the roaming 5GC networks, and can work in Rel-15 5GC networks. It is expected that supporting roaming partners will properly configure their networks to fulfil their SLAs. Enforcement of MEANS in the network is using the Rel-15 NSSF/AMF functionality for determining an appropriate set of S-NSSAI for the Allowed NSSAI.

- This solution does **not** impact the home 5GC network beyond the ability to send to the relevant UEs the URSP with the added field (i.e. it impacts the PCF and the UDR). It is expected that the home network operator will configure its network to fulfil the subscription requirements. Enforcement of MEANS in the network is using the Rel-15 NSSF/AMF functionality for determining an appropriate set of S-NSSAI for the Allowed NSSAI.

In this solution, Mutually Exclusive Access to Network Slices in the network is already supported in Rel-15 and does not require any further changes. Actual isolation of resources between network slices is supported by the underlying virtualisation environment and OAM (see SA5 specifications).

### 6.1.1.5 Evaluation

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

### 6.1.2 Solution #1.2: Mutually Exclusive Access to Network Slices via UE configuration

#### 6.1.2.1 Introduction

This is a solution to Key Issue #1, "Mutually Exclusive Access to Network Slices" (MEANS).

This solution incorporates parts of solution #5, in clause 6.1.5.

This solution assumes the following:

- It is assumed that the network deployments in the home and the visited networks are designed according to the requirements for MEANS, and that the "mutually exclusive" network slices are not sharing resources (including no common AMF Set). This ensures that the NSSF will never grant access to both network slices simultaneously even if a UE requests it (e.g. due to SIM swap). As in Rel-15, NSSF internal policies dictate which network slice would be selected in this case.

- It is assumed that the "mutual exclusivity" of network slices is per network deployment, and is common to all UEs subscribed to both network slices.

- It is assumed that the UE used for mutually exclusive network slices:

- either has internal logic (e.g. MMI, or software support) to understand which applications are needed at a given time (e.g. "on duty" vs "off duty", "maintenance" vs "factory", etc), which is beyond the scope of this solution to address. If a SIM swap happens to a UE not understanding the purpose of the applications, it is expected that the UE would not use these applications anyway. As this is UE local configuration, the network can update the information by existing means for UE local configuration, or can rely on application logic to update and perform the choice between two sets of network slices.

- or has internal logic (e.g. software support) to sort the S-NSSAIs to put in the Requested NSSAI in priority order.

- A UE not supporting the feature (e.g. with no application/MMI to perform the selection between several sets of slices or no internal logic to sort S-NSSAIs in priority order), but nonetheless subscribed to network slices that are mutually exclusive with each other will rely on the Rel-15 slice rejection mechanism.- It is assumed that PLMN are going to deploy their network slices in their networks so that all the services available to the users can be used simultaneously (i.e. there will be at least a set of network slice instances in the home network that can offer all the services (S-NSSAIs) that the UE can request simultaneously in its home network), except for network slices that are intended to be under mutually exclusive access by UEs.

- It is assumed that the PLMN's internal logic for NSSF/AMF network slice selection can include a mechanism to take in account the S-NSSSAIs from the Requested NSSAI in priority order during the network slice selection.

- It is assumed that PLMNs are going to organise their SLAs so that network slices in the roaming partners' networks are going to offer all services available to the users simultaneously (i.e. there will be at least a set of network slice instances in the roaming partner network that can offer all the services (S-NSSAIs) that the UE can request simultaneously in that network), except for network slices that are intended to be under mutually exclusive access by UEs.

- This means that the enforcement of the MEANS in roaming scenarios is enforced via SLA (the roaming partner would not allow a UE to access MEANS slices simultaneously, e.g. via sharing the same AMF), and that when UEs needing MEANS in roaming partners' networks not supporting such SLA requirements would not receive the Subscribed S-NSSAIs of the UE that could result in such violation of the MEANS.

#### 6.1.2.2 Functional description

This solution proposes that the UE expected to be able to select between network slices is configured (by mechanisms not to be defined in the specification, e.g. part of application configuration) in such a way that the UE knows whether two given S-NSSAIs can be requested simultaneously in the Requested NSSAI, or how to sort the S-NSSAIs in the Requested NSSAI in priority order (see solution #5, in clause 6.1.5, for more details)..

The solution proposes that the (not specified) internal logic of the AMF/NSSF regarding network slice selection can decide to consider the S-NSSAIs in the Requested NSSAI in priority order.

#### 6.1.2.3 Procedures

No new procedures are required with this solution.

#### 6.1.2.4 Impacts on existing entities and interfaces

Impacts compared to Rel-15:

- This solution has no normative specification impacts. It is already supported by Rel-15 specifications. Only a few informative statements are expected (e.g. a few notes) to clarify the expected behaviour of the UE and the network..

UE impact:

- This solution only impacts UE supporting the feature as part of the overall UE design and application configuration (i.e. no specification impact). UEs not supporting the feature would not need to be configured in such a way. The UE would need to understand its own configuration.

Network impact (serving and home):

- This solution does **not** impact the roaming 5GC networks, and can work in Rel-15 5GC networks. It is expected that supporting roaming partners will properly configure their networks to fulfil their SLAs. Enforcement of MEANS in the network is using the Rel-15 NSSF/AMF functionality for determining an appropriate set of S-NSSAI for the Allowed NSSAI.

- This solution does **not** impact the home 5GC network, and can work in home Rel-15 5GC network. It is expected that the home network operator will configure its network to fulfil the subscription requirements. Enforcement of MEANS in the network is using the Rel-15 NSSF/AMF functionality for determining an appropriate set of S-NSSAI for the Allowed NSSAI.

In this solution, Mutually Exclusive Access to Network Slices in the network is already supported in Rel-15 and does not require any further changes. Actual isolation of resources between network slices is supported by the underlying virtualisation environment and OAM (see SA5 specifications).

The impact to the specification work is expected to be as follows:

- An explanation that, the UE can optionally be locally (pre-)configured with information (by mechanisms not specified in 3GPP specifications) regarding the S-NSSAIs that can (or cannot) be requested simultaneously by the UE;

- An explanation that, the UE can optionally be locally configured (by mechanisms not specified in 3GPP specifications) to sort S-NSSAIs in the Requested NSSAI in a priority order;

- An explanation that the AMF/NSSF, when receiving a Requested NSSAI with S-NSSAIs that cannot be allowed simultaneously, can decide to consider the S-NSSAIs in the Requested NSSAI in priority order; and

- Possibly, an explanation how these mechanisms can allow an operator to fulfil the KI#1 scenarios.

It is expected that this work can be completed via a single CR to TS 23.501 [2].

#### 6.1.2.5 Evaluation

### 6.1.3 Solution #1.3: Solution to Key issue#1: Mutual exclusion awareness in UE.

#### 6.1.3.1 Introduction

As per definition of Mutually exclusive Network Slices:

*The access to Network Slices is considered to be mutually exclusive for a UE when their respective S-NSSAIs are both present in the UE's subscription and the UE is prevented from accessing both S-NSSAIs simultaneously.*

The case exists a UE may attempt to request in a Registration Request e.g. two S-NSSAIs in the Requested NSSAI are not compatible. It is assumed the network then detects this is an incorrect NSSAI, accepts the Registration request, places the UE in default slices as subscribed by the UE (possibly this causes a AMF change, and as a reminder the default NSSAIs must be mutually compatible), and indicates to the UE that there were incompatible S-NSSAIs. The automatic UE configuration procedures ought to also get triggered as per the existing TS 23.501 [2].

It is clear however that if the UE is not provided by the network with the exact S-NSSAIs that were incompatible and assuming the UE may subsequently request a number of S-NSSAIs >2, before the UE can eventually form a mutually compatible set of S-NSSAIs in a Requested NSSAIs, including one of the S-NSSAIs that were detected as incompatible, it may take a number of trials and errors. This would be the result of allowing a current Rel-15 UE to be provisioned with some S-NSSAIs that are mutually incompatible.

Hence, unless Rel-15 is updated e.g. in the late drop, in Rel-15 a UE cannot be provisioned with mutually incompatible S-NSSAIs unless the operator is ready to accept that a suboptimal behaviour and a number of trial and errors may be involved in using certain slices. However, these trials and errors may be unacceptable for the correct operation of a mutually exclusive slice (e.g. a public safety slice may not welcome a trial and error phase before some mission critical data or media can be exchanged over the public safety slice, but this slice may have to coexist with e.g. a V2X slice on a police car).

For this reason we need to specify some means by which:

1) A properly configured UE never requests mutually exclusive slices in a requested NSSAI.

2) Error cases can be handled in a way that the network can provide the UE with the rules that avoid future repetition of the error, for UEs that are compliant to the solution proposed.

3) There are no trial end errors once 1 and 2 are implemented in the system.

Whether a late Rel-15 change needs to be considered (aligned with the late Rel-15 drop) will be part of the conclusions of the study.

Editor's note: Compatibility with Rel-15 UEs and network needs to be assessed.

#### 6.1.3.2 Functional description

It is proposed that for each S-NSSAI in the UE subscription, Configured NSSAI and Default Configured NSSAI, a Mutual Exclusion Class Information is associated. This information identifies whether a certain S-NSSAI can be used with other S-NSSAIs and rules to define such coexistence.

It is proposed that in Rel-16 these classes of mutual exclusion are identified by means of Mutual Exclusion Class Information, which identifies classes of slices that can be used simultaneously:

Table 6.1.3.2-1: Mutual Exclusion Class Information

| S-NSSAI  Mutual exclusion class | Rule |
| --- | --- |
| 0 | No constraint defined for the S-NSSAI |
| 1 | S-NSSAI can be used alongside S-NSSAIs with same SST field value |
| 2 | S-NSSAI can be used alongside S-NSSAIs with same SD field value |
| 3 | S-NSSAI cannot be used alongside any other S-NSSAI |
| 4 | S-NSSAI can be used only alongside class 4 S-NSSAIs (Operator defined) |
| 5 | S-NSSAI can be used only alongside class 5 S-NSSAIs (Operator defined) |
| 6 | S-NSSAI can be used only alongside class 6 S-NSSAIs (Operator defined) |
| 7 | S-NSSAI can be used only alongside class 7 S-NSSAIs (Operator defined) |
| 8 | S-NSSAI can be used only alongside class 8 S-NSSAIs (Operator defined) |
| 9 | S-NSSAI can be used only alongside class 9 S-NSSAIs (Operator defined) |
| 10 | S-NSSAI can be used only alongside class 10 S-NSSAIs (Operator defined) |
| 11 | S-NSSAI can be used only alongside class 11 S-NSSAIs (Operator defined) |
| 12 | S-NSSAI can be used only alongside class 12 S-NSSAIs (Operator defined) |
| 13 | S-NSSAI can be used only alongside class 13 S-NSSAIs (Operator defined) |
| 14 | S-NSSAI can be used only alongside class 14 S-NSSAIs (Operator defined) |
| 15 | S-NSSAI can be used only alongside class 15 S-NSSAIs (Operator defined) |

Classes 0-3 are standardised, and offer global interoperability. They identify the obvious classes of slices that are compatible with any other slice, those that are isolated (so not compatible with any other slice) and:

- Those slices that can be used simultaneously with any other slice of the same type in the UE and share same dedicated AMFs for the SST in the CN.

- Those slices that can be used simultaneously with any other slice of the same SD filed (e.g. all slices from same tenant, e.g. from same vertical customer) by a the UE and e.g. can share same AMF dedicated for the SD in the CN.

Classes 4-15 are operator specific. They define coexistence classed valid across a PLMN.

An S-NSSAI cannot be used simultaneously with S-NSSAIs that do not belong to the same Mutual Exclusion Class or do not meet the related standardised Mutual Exclusion Class definition if applicable.

Based on the above proposal, it follows that there can be 12 operator specific coexistence classes and 4 standardised ones. If more (or fewer) classes were deemed needed can be discussed and so the total number can be decided in normative phase.

A VPLMN can decide, for inbound roamers, that some of the HPLMN coexistence classes are modified to other operator-specific values in VPLMN, and this information can be sent together with the configured NSSAI or Allowed NSSAI for the VPLMN, as long as this is consistent with the intended behaviour by the HPLMN (i.e. Network Slices that are incompatible in HPLMN, remain so in the VPLMN).

If the mutual exclusion rules specified in the S-NSSAI Mutual Exclusion Class Information, which the serving PLMN receives from the UDM as part of the UE subscription data, are not met by a Requested NSSAI in a Registration Request message, the Requested NSSAI is considered as not valid and the AMF shall return in the Registration accept to the UE (which includes only default S-NSSAIs in Allowed NSSAI, alongside their coexistence class information which is the same as all the Default S-NSSAIs shall be enabled to be used at the same time) a cause code indicating that the UE has provided an invalid Requested NSSAI due to Mutual Exclusion reasons, but the S-NSSAIs in the Requested NSSAI shall not be stored as Rejected S-NSSAIs unless the AMF detected some of them were not supported in the TA or in the PLMN for the UE, in which case these S-NSSAIs are indicated by the AMF as rejected S-NSSAIs.

Then, this triggers the UE configuration to be updated, e.g. the registration accept may also provide a Configured NSSAI including the UE the Mutual Exclusion class Information.

If a HPLMN requires the Mutual Exclusion to be supported while the UE is roaming, in a Rel-15 network, this can be supported by provisioning in the UE a Configured NSSAI for the HPLMN with the Mutual Exclusion Class Information for each S-NSSAI. and the UE shall respect these rules when using the S-NSSAIs in the Rel-15 network, with the standing assumption Rel-15 network can always support any set of S-NSSAIs. However the HPLMN cannot rely on the VPLMN to enforce the Mutual exclusion rules, or expect that the VPLMN is respecting the Mutual Exclusion by allocating dedicated functions (e.g. AMF) that are e.g. handling only S-NSSAIs belonging to the same Mutual exclusion class.

The Rel-15 VPLMN is also not able to use the Mutual exclusion information in the UE subscription.

#### 6.1.3.3 Procedures

This solution impacts existing procedures end to end by inclusion of the Mutual Exclusion Class Information in association of every S-NSSAI in the configured NSSAI when this is provided to the UE by the AMF in Registration Accept or in the UE Configuration Update. The Default Configured NSSAI S-NSSAIs, shall also be associated to Mutual Exclusion Class Information. The Association can be done e.g. with a separate new information element providing the mapping of each S-NSSAI in the (Default)Configured NSSAI to a Mutual Exclusion Class. Other than this, there is no impact except behavioural (as described in clause 6.2.3) in the nodes which have to evaluate this information: e.g. the Mutual Exclusion Class information to e.g. generate the Allowed NSSAI from the Requested and subscribed NSSAI in the network, of the UE that needs to evaluate this information in the Configured NSSAI or Default Configured NSSAI to form a Requested NSSAI with compatible slices only.

If the UE does not indicate any NSSAI in registration request, the Default S-NSSAIs received in the Allowed NSSAI has no Mutual exclusion class information. The S-NSSAIs in the allowed NSSAI are by definition compatible with one another.

Mutual Exclusion Class Information is also provided alongside subscriber information in the interaction between UDM and AMF, and between AMF and NSSF, for the determination of suitable allowed NSSAI which complies to Mutual exclusion constraints that are part of Subscriber data.

If a roaming partner network is known to not support rel-16, the HPLMN shall only provide subscription information to those PLMNs with S-NSSAIs that are mutually compatible.

A Rel-15 UE cannot use the Mutual Exclusion Class Information. If a subscription including this information is used for a Rel-15 UE, then the mutual exclusion of slice is not respected by this UE. It is therefore expected that a baseline subscription of compatible slices that can be used in a Rel-15 UE or a Rel-15 network or UE is defined for the event a rel-15 UE is used or a rel-15 network is used by a roaming partner. It is expected an explicit Indication of support of this feature is required by all UEs in rel-16 in the registration procedure.

The following procedures impacts are further clarified:



Figure 6.1.3.3-1: Registration with AMF re-allocation procedure

Step 1: the UE includes indication of support of the Mutual exclusivity feature and forms the Requested NSSAI based also on the Mutual Exclusion Class Information if available for the S-NSSAIs in the Configured NSSAI or Default Configured NSSAI.

Step 14: the UE subscription data includes the Mutual Exclusion Class Information.

Step 21: The Registration Accept message may include a Configured NSSAI with the Mutual Exclusion Class Information if the UE has sent a requested NSSAI with incompatible S-NSSAIs.



Figure 6.1.3.3-2: Registration with AMF re-allocation procedure

Step 4a: the AMF provides the NSSF with the Mutual Exclusion Class information to aid the NSSF to determine the Allowed NSSAI, in a network that supports Mutual Exclusion feature, if the UE supports the Mutual exclusion feature, If the UE does not support the Mutual exclusion feature, then the AMF only provides to the NSSF the Slices that are part of the basic set of compatible S-NSSAIs part of the UE subscription. If the network is rel-15, the HPLMN has passed to it no Mutual Exclusion Class Information and only the basic set of compatible S-NSSAIs part of the UE subscription, So, there is no particular action taken in a rel-15 network.



Figure 6.1.3.3-3: Refer to TS 23.502 [3], Figure 4.2.4.2-1: UE Configuration Update procedure for access and mobility management related parameters

Step 1: The Configured NSSAI may be provided alongside a Mutual Exclusion Class information if applicable. If the UE is not indicating support of the Mutual exclusion feature, the configured NSSAI only includes the S-NSSAIs corresponding to the basic set of compatible S-NSSAIs.

#### 6.1.3.4 Impacts on existing entities and interfaces

- UE: support of Mutual Exclusion Class Information and procedures that include it for its configuration in the UE from the network.

- AMF: enforcement of the Mutual Exclusion Class Information received from UDM and/or inclusion in NSSF queries as part of sending the Subscribed S-NSSAIs.

- NSSF: enforcement of the Mutual Exclusion Class Information.

- UDM: Handling of the Mutual Exclusion Class Information.

#### 6.1.3.5 Evaluation

### 6.1.4 Solution#1.4: Slicing Group Support for Mutually Exclusive Access to Network Slices

The intent of this solution is to support mutually exclusive access of network slices in 5GS as shown in Figure-6.4.2.1-1 below. Within a group of network slices, each network slice can serve the UE simultaneously with other network slice(s) within the 5GS. However, network slices that are not in the same group cannot serve the UE simultaneously within the 5GS.

#### 6.1.4.1 Introduction

##### 6.1.4.1.1 Design principles

The design principles of the proposed solution to support Mutually Exclusive Access of network slices are as follows:

- Minimum impact to the existing Rel-15 network slicing signalling procedures between the UE and the network:

- Minimum impact to the UE's registration and PDU Session Management procedures.

- Minimum impact to the slice selection procedure.

- No impact to Rel-15 UE.

- No impact to other basic system procedures such as the Mobility Management procedure, UE Configuration Update procedures, etc.

- No impact to Rel-15 roaming procedure.

- No impact to Rel-15 URSP/NSSP support for network slicing service mapping.

##### 6.1.4.1.2 Working Assumptions and Concepts of Mutually Exclusive Access Slicing Group

1) In this proposal, it assumes that different Mutually Exclusive Access Slicing Groups do NOT share the same serving AMF. Such assumption complies to the definition as defined in clause 3.1 of TR 23.740.

2) Given the consideration of the network slicing feature should be end-to-end, in the roaming scenario, this proposal expects that, UE, VPLMN and HPLMN are required to support Mutually Exclusive slicing access in order to enable Mutually Exclusive Slicing Access support in Rel-16.

3) For the Rel-16 UE, UE will be configured with UE capability to indicate whether it supports Mutually Exclusive Access to Network Slices.

4) For the Rel-16 5GC, if it does not support Mutually Exclusive Access to Network Slices, even when the Rel-16 UE presents its support for Mutually Exclusive Access to Network Slices during the UE Registration, such capability will be ignored by the Rel-16 5GC and no Mutually Exclusive Access to Network Slices are assigned to the UE.

5) Two scenarios when provisioning/configuring S-NSSAI(s) to the UE:

A. Provisioning/configuring S-NSSAIs to the UEs for the Network Slices that all serve the UE simultaneously if the UE does not support Mutually Exclusive Access to Network Slices.

B. Provisioning/configuring S-NSSAIs to the UEs for the Network Slices that do NOT all serve the UE simultaneously if the UE supports Mutually Exclusive Access to Network Slices.

Same as in today Rel‑15, during the UE Registration, the UDM may provide the Rel‑16 serving PLMN all or some of the UE's subscriptions, according to the local policy and/or SLA in case of roaming, the serving PLMN determines the applicable S-NSSAI(s) to be provided to the UE.

For the scenario A. above, there is only one set of provisioned/configured S-NSSAIs that all can serve the UE simultaneously.

For the scenario B. above, the set of provisioned/configured S-NSSAI configured by the HPLMN will be composed of two or more set of S-NSSAIs that do NOT serve the UE simultaneously. In case of roaming, the corresponding mapping S-NSSAI(s) configured by the VPLMN will also be composed of two or more set of S-NSSAIs that do not serve the UE simultaneously in the VPLMN.

#### 6.1.4.2 Functional description

##### 6.1.4.2.1 Concepts of Mutually Exclusive Access Slicing Group

The S-NSSAIs within the same Mutually Exclusive Access Slicing Group can serve the UE simultaneously, but not with the S-NSSAI(s) from different slicing groups.

The Figure-6.4.2.1-1 below presents the concept on how the serving PLMN organizes the Mutually Exclusive Access Slicing Groups, and how the Allowed NSSAI and the corresponding serving AMF are derived from the Mutually Exclusive Access Slicing groups.

During the Rel-16 UE registration with the Rel-16 5GC that supports Mutually Exclusive Access to Network Slices, the following four main scenarios to consider:

1) If the UE does not provide the Requested NSSAI and the UE's capability indicates that, the UE is capable of supporting Mutually Exclusive Access to Network Slices, if there is more than one Mutually Exclusive Access Slicing Groups configured for the UE according to UE's subscription as described in scenario B above, based on the local and/or the roaming policy, the serving PLMN (via serving AMF or NSSF) will select a particular slicing group and derive the Allowed NSSAI for the UE from the selected slicing group, and if applicable, any associated S-NSSAI mappings with the HPLMN are also determined. The unselected Mutually Exclusive Access Slicing Groups and the associated mappings with the HPLMN, if applicable, will also be provided to the UE as the Configured NSSAI as in Rel-15. The associated slicing group information is also included for each S-NSSAI in the Configured NSSAI as well as in the associated mapping, if applicable.

2) If the UE provides the Requested NSSAI during the UE registration and the UE's capability indicates that, the UE is capable of supporting Mutually Exclusive Access to Network Slices, the serving PLMN decides the Allowed NSSAI based on the Requested NSSAI as in Rel-15. In addition, if there is more than one Mutually Exclusive Access Slicing Groups configured for the UE according to the UE's subscription as described in scenario B. above, the unselected Mutually Exclusive Access Slicing Groups and the associated mappings with the HPLMN, if applicable, will also be provided to the UE as the Configured NSSAI as in Rel-15. The associated slicing group information is also included for each S-NSSAI in the Configured NSSAI as well as in the associated mapping, if applicable.

3) If the there is no indication that the UE is capable of supporting Mutually Exclusive Access to Network Slices, the serving network shall only provide the UE for the Allowed NSSAI and/or Configured NSSAI with the S-NSSAIs as described in scenario A. above, and, if applicable, the associated mappings with the HPLMN that call all be served by the same AMF simultaneously.

Fundamentally, Mutually Exclusive Access to Network Slices, if supported, is end-to-end.

Table 6.1.4.2.1-1 summarizes the end-to-end considerations for supporting the Mutually Exclusive Access for Network Slicing in Rel-16 network.

Table 6.1.4.2.1-1: Summary of Considerations End-to-end Mutually Exclusive Access Support for Network Slicing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| UE Mutually Exclusive Access Slicing capability | | Serving PLMN Mutually Exclusive Access Slicing capability | Home PLMN Mutually Exclusive Access Slicing capability | End-to-end Mutually Exclusive Access Support |
| Rel-15 UE | N/A | N/A | N/A | No |
| Rel-16 UE | No | N/A | N/A | No |
| Yes | No | No | No |
| Yes | No | Yes | No |
| Yes | Yes | No | No |
| Yes | Yes | Yes | Yes |

NOTE: The serving AMF is part of the network slice, same AMF/AMF Set cannot serve two different Mutually Exclusive Access Slicing Groups. Different Allowed NSSAIs from different Mutually Exclusive Access Slicing Groups are served by different AMF/AMF Set. Hence, once the UE is registered, the serving AMF is corresponding to the Allowed NSSAI for particular Mutually Exclusive Access Slicing Group. If UE, that supports Mutually Exclusive Access to Network Slices, wants to activate service not belonging to the same Mutually Exclusive Access Slicing Group, then the UE is required to re-register with the new Requested NSSAI that includes the S-NSSAIs from the Configured NSSAI corresponding to the target service, and any existing PDU session, if any, will be released according to clause 5.15.5.2.2 in TS 23.501 [2] before the UE is registered with the new set of S-NSSAI(s) in the new Mutually Exclusive Access Slicing Group.

Once Allowed NSSAI is identified, the subsequent PDU Session Establishment procedure is the similar to today Rel-15 procedures as described in clause 5.15.5 in TS 23.501 [2], except for the following:

- The UE should only include the S-NSSAI from the Allowed NSSAI in the Requested NSSAI for UE registration; and if using the S-NSSAI from the Configured NSSAI, it shall have the same Slicing Group ID as the S-NSSAI in the Allowed NSSAI.

- The serving AMF shall verify the Slicing Group ID of the S-NSSAI in the Requested NSSAI is the same as the Allowed NSSAI that has been provided to the UE. Otherwise, the PDU Session Establishment request will be rejected with the proper cause to indicate the inappropriate Slicing Group ID of the S-NSSAI in the Requested NSSAI.



Figure-6.1.4.2.1-1: Concepts of Mutually Exclusive Access Slicing Groups and their Corresponding NSSAIs

##### 6.1.4.2.2 Identification of Mutually Exclusive Access Slicing Group

In order to differentiate different slicing groups for mutually exclusive access, there are two options to consider:

(1) Reserving portion of the SD field from S-NSSAI as the Slicing Group Identifier. For example, as shown in Figure-6.1.4.2.2-1 below, the SD field could be extended to indicate the support for mutually exclusive access slicing group.

Pros:

- The Group identifier is imbedded into the S-NSSAI and no need for introducing new identifier.

- Significantly lesser impact to the existing interface and the slicing related procedures by the UE and by the Network given the Group Identifier is imbedded into the S-NSSAI and hence, no new parameter is needed.

Cons:

- The size of the SD field is reduced and hence, the number of slice descriptors are reduced.

(2) Introducing an additional Slicing Group Identifier which is used to associate with the S-NSSAI.

Pros:

- No need to modify the S-NSSAI and hence, the size of the SD field are not impacted.

Cons:

- Need to introduce additional identifier for the slicing group id.

- More significant impact to the existing interface and the slicing procedures given new parameter is needed to indicate the Group Identifier to be associated with the S-NSSAI for coordination.

The Mutually Exclusive Access Slicing Group ID is per PLMN. In case of roaming, Slicing Group ID in the serving PLMN may have different value from the home PLMN. This is no different in Rel-15, where serving PLMN and home PLMN will have own respective S-NSSAI for the given network slice. Similar to Rel-15, there will be SLA agreement on the mapping for the S-NSSAIs between the serving PLMN and home PLMN to support Mutually Exclusive Access.

This proposal does not preclude the scenario that operator may configure one or more S-NSSAI(s) that can serve the UE simultaneously together with any Mutually Exclusive Access Slicing Group. In this case, such S-NSSAI(s) are not tied to any specific slicing group and there should be special Slicing Group ID defined for such kind of S-NSSAI.

The exact definition on how to partition the SD field or to introduce new additional identifier to support slicing group identification is determined by the CT group. If option (1) approach is taken, only the SD field is affected, hence, there is no impact to the Standardized SST value. Therefore, operator can organize the given S-NSSAIs with Standardized SST values by leveraging the SD field to support the grouping for Mutually Exclusive Access to Network Slices.



Figure-6.1.4.2.2-1: Example of extending SD to identify the Mutually Exclusive Access Slicing Group

##### 6.1.4.2.3 UE Support for Mutually Exclusive Access Slicing Group

For the Rel-15 UE or the Rel-16 UE that is not capable of supporting Mutually Exclusive Slicing Access attaches to the Rel-16 5GC that is capable to support Mutually Exclusive Access to network slicing, such UE will be provided with S-NSSAI(s) that can serve the UE simultaneously (see clause 6.1.4. 1.2working assumptions above). There is no impact to Rel-15 UE.

For the Rel-16 UE that is capable of supporting Mutually Exclusive Slicing Access, and if the network supports also the Mutually Exclusive Slicing Access, the UE shall include the S-NSSAIs that are in the same Mutually Exclusive Access Slicing Group in the Requested NSSAI during the UE's registration and also during the UE Session Establishment procedures.

This proposal does not require any changes to clause 5.15.4, TS 23.501 [2] for the NSSAI storage aspects in the UE.

##### 6.1.4.2.4 Roaming Support for Mutually Exclusive Access Slicing Group

In case of roaming, in order to enable Mutually Exclusive Access, this proposal expects UE, serving network and home network are all capable of supporting Mutually Exclusive Slicing Access. Based on such working assumption, the serving and the home PLMN would have to coordinate the mapping of the S-NSSAI(s) with their respective Mutually Exclusive Access Slicing Group IDs according to the SLA and their respective local policy.

##### 6.1.4.2.5 URSP/NSSP Support for Mutually Exclusive Access Slicing Group

The URSP/NSSP in Rel-15 provides the service mapping between the Allowed/Configured S-NSSAIs in the UE to the UE's applications (refer to clause 6.6.2 in TS 23.503 [4] for more details). The same service mapping practice remains unchanged for Rel-16 as in Rel-15.

As described in 6.1.4.1.2 working assumption above, there are two scenarios of S-NSSAIs to be provisioned/configured by the Mutually Exclusive Access capable 5GC to the UEs dependent on UE's Mutually Exclusive Access capable and not capable.

In the case that the Mutually Exclusive Access capable UE is moving from Mutually Exclusive Access capable 5GC to incapable 5GC or vice versa, during the UE re-registration, the prior Allowed and Configured NSSAIs stored in the UE will be completely replaced by a new set of S-NSSAIs by following the procedures as described in clause 5.15.4 in TS 23.501 [2]. As a result, the UE will refer to the new set of S-NSSAI(s) (i.e. either scenario A. or scenario B. above) and the revised URSP/NSSP updated by the serving PCF for the service mapping to support the subsequent PDU Session Establishment procedures.

In the case that the UE replaces its SIM card from Rel-15 to Rel-16 which supports Mutually Exclusive Access to Network Slices while attaching to the same serving 5GC (in case of roaming, including both VPLMN and HPLMN):

- if the serving 5GC supports Mutually Exclusive Access to Network Slice, then the Mutually Exclusive Access support is enabled. The prior Allowed and Configured NSSAIs stored in the UE will be completely replaced by S-NSSAIs that support Mutually Exclusive Access by following the same procedures as described in clause 5.15.4 in TS 23.501 [2]. As a result, the UE will refer to the revised URSP/NSSP for the service mapping when initiating PDU Session Establishment procedures.

- if the serving 5GC does not support Mutually Exclusive Access to Network Slice, then the Mutually Exclusive Access support is not enabled. The prior Allowed and Configured NSSAIs stored in the UE may be replaced by S-NSSAI(s) that do not apply for Mutually Exclusive Access following the same procedures as described in clause 5.15.4 in TS 23.501 [2].

In the case that the UE replaces its SIM card from Rel-15 to Rel-16 which does not support Mutuallly Exclusive Access to Network Slices while attaching to the same serving 5GC (in case of roaming, including both VPLMN and HPLMN), irrespective the attached serving system supports Mutually Exclusive Access or not, the prior Allowed and Configured NSSAIs stored in the UE may be replaced by S-NSSAI(s) that do not apply for Mutually Exclusive Access by following the same procedures as described in clause 5.15.4 in TS 23.501 [2].

In the case that the UE replaces its SIM card from Rel-16 to Rel-15 while attaching to the same serving 5GC (in case of roaming, including both VPLMN and HPLMN), irrespective the attached serving 5GC supports Mutually Exclusive Access or not, the prior Allowed and Configured NSSAIs stored in the UE may be updated with S-NSSAI(s) that do not apply for Mutually Exclusive Access by following the same procedures as described in clause 5.15.4 in TS 23.501 [2].

In summary, the existing URSP/NSSP related procedures are unchanged, and this proposal makes no impact to the URSP/NSSP as defined in Rel-15.

##### 6.1.2.4.6 AMF Support for Mutually Exclusive Access Slicing Group

The following procedures are based on clause 5.15.5.2.1, in TS 23.501 [2] with the changes shown in italic fonts and the changes are based on the use of option (1) in clause 6.4.2.2 above for the identification of Mutually Exclusive Access Slicing Group.

**(A)** *During the UE's initial registration, once the UE's subscriptions for the network slicing are obtained from UDM, depending on AMF local configuration,* the AMF may be allowed to determine whether it can serve the UE, and the following is performed:

- AMF checks whether it can serve all the S-NSSAI(s) from the Requested NSSAI present in the Subscribed S-NSSAIs (potentially using configuration for mapping S-NSSAI values between HPLMN and Serving PLMN), or all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs in the case that no Requested NSSAI was provided or none of the S-NSSAIs in the Requested NSSAI were present in the Subscribed S-NSSAIs (see clause 5.15.3 *in TS 23.501 [2]*).

- *If Mutually Exclusive Access to Network Slices is supported and there is more than one slicing groups marked as default in the Subscribed S-NSSAIs, based on the operator's configuration, the AMF will then decide which particular Slicing Group is to be selected.*

- If the AMF can serve the S-NSSAIs in the Requested NSSAI, the AMF remains the serving AMF for the UE. The Allowed NSSAI is then composed of the list of S-NSSAI(s) in the Requested NSSAI permitted based on the Subscribed S-NSSAIs, or, if no Requested NSSAI was provided, all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs, *and if Mutually Exclusive Access to Network Slices is supported, the default Subscribed S-NSSAIs for the selected Slicing Group*. The AMF also determines the mapping if the S-NSSAI(s) included in the Allowed NSSAI needs to be mapped to Subscribed S-NSSAI(s) values.

If no Allowed NSSAI is determined from above, the AMF based on the Subscribed S-NSSAI(s) and operator's configuration may also determine the Configured NSSAI for the Serving PLMN or/and the associated mapping of the Configured NSSAI to the Configured NSSAI for the HPLMN, so these can be configured in the UE. Then Step (C) below is executed.

- *Otherwise*, the AMF queries the NSSF (see (B) below).

**(B)** When required as described above, the AMF needs to query the NSSF, and the following is performed:

- The AMF queries the NSSF, with Requested NSSAI, mapping of Requested NSSAI to Configured NSSAI for the HPLMN, the Subscribed S-NSSAIs (with an indication if marked as default S-NSSAI), any Allowed NSSAI it might have for the other Access Type (including its mapping to the Configured NSSAI for the HPLMN), PLMN ID of the SUPI and UE's current Tracking Area(s).

NOTE 1: When more than one UE's Tracking Area is indicated, the UE is using more than one Access Type.

- Based on this information, local configuration, and other locally available information including RAN capabilities in the current Tracking Area for the UE or load level information for a network slice instance provided by the NWDAF, the NSSF does the following:

- It verifies which S-NSSAI(s) in the Requested NSSAI are permitted based on comparing the Subscribed S-NSSAIs with the S-NSSAIs in the mapping of Requested NSSAI to Configured NSSAI for the HPLMN. It considers the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs in the case that no S-NSSAI from the Requested NSSAI are present in the Subscribed S-NSSAIs.

- It selects the Network Slice instance(s) to serve the UE. When multiple Network Slice instances in the UE's Tracking Areas are able to serve a given S-NSSAI, based on operator's configuration, the NSSF may select one of them to serve the UE, or the NSSF may defer the selection of the Network Slice instance until a NF/service within the Network Slice instance needs to be selected.

- It determines the target AMF Set to be used to serve the UE, or, based on configuration, the list of candidate AMF(s), possibly after querying the NRF.

- It determines the Allowed NSSAI(s) for the applicable Access Type(s), taking also into account the availability of the Network Slice instances as described in clause 5.15.8 *in TS 23.501 [2]* that are able to serve the S-NSSAI(s) in the Allowed NSSAI in the current UE's Tracking Areas. *If there is more than one slicing groups in the Subscribed S-NSSAIs, based on the operator's configuration and local policy, the NSSF will then decide which particular Slicing Group is to be selected as the Allowed NSSAI(s) for the applicable Access Type(s).*

- It also determines the mapping of each S-NSSAI of the Allowed NSSAI(s) to the Subscribed S-SNSSAIs if necessary.

- Based on operator configuration, the NSSF may determine the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s).

- Additional processing to determine the Allowed NSSAI(s) in roaming scenarios and the mapping to the Subscribed S-NSSAIs, as described in clause 5.15.6 *in TS 23.501 [2]*.

- If no Allowed NSSAI is determined from above, the NSSF based on the Subscribed S-NSSAI(s) and operator configuration may derive the Configured NSSAI for the Serving PLMN or/and the associated mapping of the Configured NSSAI to the Configured NSSAI for the HPLMN, so these can be configured in the UE.

- The NSSF returns to the current AMF the Allowed NSSAI for the applicable Access Type(s), the mapping of each S-NSSAI of the Allowed NSSAI to the Subscribed S-NSSAIs if determined and the target AMF Set, or, based on configuration, the list of candidate AMF(s). The NSSF may return the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s), and the NRF to be used to determine the list of candidate AMF(s) from the AMF Set. The NSSF may return NSI ID(s) to be associated to the Network Slice instance(s) corresponding to certain S-NSSAIs. NSSF may return the rejected S-NSSAI(s) as described in clause 5.15.4.1 *in TS 23.501 [2]*. The NSSF may return the Configured NSSAI for the Serving PLMN and the associated mapping of the Configured NSSAI to the Configured NSSAI for the HPLMN.

- Depending on the available information and based on configuration, the AMF may query the appropriate NRF (e.g. locally pre-configured or provided by the NSSF) with the target AMF Set. The NRF returns a list of candidate AMFs.

- If rerouting to a target serving AMF is necessary, the current AMF reroutes the Registration Request to a target serving AMF as described in clause 5.15.5.2.3 *in TS 23.501 [2]*.

- Step (C) is executed.

**(C)** The serving AMF shall determine a Registration Area such that all S-NSSAIs of the Allowed NSSAI for this Registration Area are available in all Tracking Areas of the Registration Area (and also considering other aspects as described in clause 5.3.2.3 *in TS 23.501 [2]*) and then return to the UE this Allowed NSSAI and the mapping of the Allowed NSSAI to the Subscribed S-NSSAIs if provided. The AMF may return the rejected S-NSSAI(s) as described in clause 5.15.4.1 *in TS 23.501 [2]*.

NOTE 2: As there is a single distinct Registration Area for Non-3GPP access in a PLMN, the S-NSSAIs in the Allowed NSSAI for this Registration Area (i.e. for Non-3GPP access) are available homogeneously in the PLMN.

When no Requested NSSAI was included, or when the mapping of the S-NSSAIs in Requested NSSAI to the corresponding values in the Configured NSSAI for the HPLMN is incorrect, or when an S-NSSAI was rejected in the PLMN, the AMF may update the UE slice configuration information for the PLMN as described in clause 5.15.4.2 in TS 23.501 [2].

#### 6.1.4.3 Procedures

##### 6.1.4.3.1 UE Registration with Mutually Exclusive Access Slicing Group

The following procedures are based on clause 4.2.2.2.3, in TS 23.502 [3] v15.2 with the changes shown in italic fonts and the changes are based on the use of option (1) in clause 6.4.2.2 above for the identification of Mutually Exclusive Access Slicing Group.

When an AMF receives a Registration request, the AMF may need to reroute the Registration request to another AMF, e.g. when the initial AMF is not the appropriate AMF to serve the UE. The Registration with AMF re-allocation procedure, described in figure 4.2.2.2.3-1 of TS 23.502 [3], is used to reroute the NAS message of the UE to the target AMF during a Registration procedure.



Figure 6.1.4.3.1-1: UE Registration Procedures to support Mutually Exclusive Access

1. Steps 1 and 2 of figure 4.2.2.2.2-1 *in TS 23.502 [3]* have occurred, and the (R)AN sends the Registration request message within an Initial UE message to the initial AMF; *and in case the UE is to re-register with Requested NSSAI corresponding to a different Mutually Exclusive Access Slicing Group, the UE shall not provide the 5G-GUTI in Access Stratum signalling when performing a Registration procedure*. *The Initial UE message may or may not include the Requested NSSAI, and the Initial UE message and re-registration message may or may not include the UE MM Core Network Capability that indicates its support for Mutually Exclusive Access to network slices.*

2. If the AMF needs the SUPI and/or UE's subscription information to decide whether to reroute the Registration Request or if the Registration Request was not sent integrity protected or integrity protection is indicated as failed, then AMF performs steps 4 to 9a of figure 4.2.2.2.2-1 in TS 23.502 [3].

3a. [Conditional] Initial AMF to UDM: Nudm\_SDM\_Get (SUPI, Slice Selection Subscription data).

If the initial AMF needs UE's subscription information to decide whether to reroute the Registration Request and UE's slice selection subscription information was not provided by old AMF, then initial AMF request UE's Slice Selection Subscription data from UDM by invoking the Nudm\_SDM\_Get (see clause 5.2.3.3.1 *in TS 23.502 [3]*) service operation. UDM may get this information from UDR by Nudr\_UDM\_Query(SUPI, Subscribed S-NSSAIs). *In addition, if the serving PLMN, and in case of roaming, the HPLMN and the UE are capable of supporting the Mutually Exclusive Access to Network Slices, the initial AMF includes also the UE's capability in Nudm\_SDM\_Get service operation.*

3b. UDM to initial AMF: Response to Nudm\_SDM\_Get. The AMF gets the Slice Selection Subscription data including Subscribed S-NSSAIs. The UDM may provide indication that the subscription data for network slicing is updated for the UE.

UDM responds with slice selection data to initial AMF *with the consideration for the support for the Mutually Exclusive Access to Network Slices in the serving PLMN, in the UE (i.e. indicated by the UE MM Core Network Capability provided by the initial AMF), and in case of roaming, in the Home PLMN*.

4a. [Conditional] Initial AMF to NSSF: Nnssf\_NSSelection\_Get (Requested NSSAI, [Mapping Of Requested NSSAI], Subscribed S-NSSAI(s) with the default S-NSSAI indication, TAI, Allowed NSSAI for the other access type (if any), [Mapping of Allowed NSSAI], PLMN ID of the SUPI).

If there is a need for slice selection, (see clause 5.15.2.1 of TS 23.501 [2]), e.g. the initial AMF cannot serve all the S-NSSAI(s) from the Requested NSSAI permitted by the subscription information, the initial AMF invokes the Nnssf\_NSSelection\_Get service operation from the NSSF by including Requested NSSAI, optionally Mapping Of Requested NSSAI, Subscribed S-NSSAIs with the default S-NSSAI indication, Allowed NSSAI for the other access type (if any), Mapping of Allowed NSSAI, PLMN ID of the SUPI and the TAI of the UE.

4b. [Conditional] NSSF to Initial AMF: Response to Nnssf\_NSSelection\_Get (AMF Set or list of AMF addresses, Allowed NSSAI for the first access type, [Mapping Of Allowed NSSAI], [Allowed NSSAI for the second access type], [Mapping of Allowed NSSAI], [NSI ID(s)], [NRF(s)], [List of rejected (S-NSSAI(s), cause value(s))], [Configured NSSAI for the Serving PLMN], [Mapping Of Configured NSSAI]).

The NSSF performs the steps specified in point (B) *in clause 6.2.4.6 above*. The NSSF returns to initial AMF the Allowed NSSAI for the first access type, optionally the Mapping Of Allowed NSSAI, the Allowed NSSAI for the second access type (if any), optionally the Mapping of Allowed NSSAI and the target AMF Set or, based on configuration, the list of candidate AMF(s). The NSSF may return NSI ID(s) associated to the Network Slice instance(s) corresponding to certain S-NSSAI(s). The NSSF may return the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s). It may return also information regarding rejection causes for S-NSSAI(s) not included in the Allowed NSSAI. The NSSF may return Configured NSSAI for the Serving PLMN, and possibly the associated mapping of the Configured NSSAI.

NOTE 1: The NRF(s) is returned by the NSSF, if any, belong to any level of NRF (see clause 6.2.6 of TS 23.501 [2]) according to the deployment decision of the operator.

5. [Conditional] Initial AMF to old AMF: Namf\_Communication\_RegistrationCompleteNotify (failure cause).

The initial AMF decides to reroute the NAS message to another AMF. The initial AMF sends a reject indication to the old AMF telling that the UE Registration procedure did not fully complete at the initial AMF. The old AMF continues as if the Namf\_Communication\_UEContextTransfer had never been received.

6a. [Conditional] Initial AMF to NRF: Nnrf\_NFDiscovery\_Request (NF type, AMF Set).

If the initial AMF does not locally store the target AMF address, and if the initial AMF intends to use direct reroute to target AMF or the reroute via (NG-R)AN message needs to include AMF address, then the initial AMF invokes the Nnrf\_NFDiscovery\_Request service operation from the NRF to find a proper target AMF which has required NF capabilities to serve the UE. The NF type is set to AMF. The AMF Set is included in the Nnrf\_NFDiscovery\_Request.

6b. [Conditional] NRF to AMF: Response to Nnrf\_NFDiscovery\_Request (list of (AMF pointer, AMF address, plus additional selection rules and NF capabilities)).

The NRF replies with the list of potential target AMF(s). The NRF may also provide the details of the services offered by the candidate AMF(s) along with the notification end-point for each type of notification service that the selected AMF had registered with the NRF, if available. As an alternative, it provides a list of potential target AMFs and their capabilities, and optionally, additional selection rules. Based on the information about registered NFs and required capabilities, a target AMF is selected by the initial AMF.

If the initial AMF is not part of the target AMF set, and is not able to get a list of candidate AMF(s) by querying the NRF with the target AMF set (e.g. the NRF locally pre-configured on AMF does not provide the requested information, the query to the appropriate NRF provided by the NSSF is not successful, or the initial AMF has knowledge that the initial AMF is not authorized as serving AMF etc.) then the initial AMF shall forward the NAS message to the target AMF via (R)AN executing step 7(B); the Allowed NSSAI and the AMF Set are included to enable the (R)AN to select the target AMF.

7(A). If the initial AMF, based on local policy and subscription information, decides to forward the NAS message to the target AMF directly, the initial AMF invokes the Namf\_Communication\_N1MessageNotify to the target AMF, carrying the rerouted NAS message. The Namf\_Communication\_N1MessageNotify service operation includes the information enabling (R)AN to identify the N2 terminating point and the NAS message carried at step 1, and the UE's SUPI and MM Context if available. If the initial AMF has obtained the information from the NSSF as described at step 4b, that information except the AMF Set or list of AMF addresses is included. The target AMF then updates the (R)AN with a new updated N2 termination point for the UE (step 7b), the (R)AN acknowledges the updated N2 termination point (step 7c). Step 7(B) is skipped.

NOTE 2: Steps 7b and 7c can occur separately or as part of the first subsequently required N2 interaction.

7(B). If the initial AMF, based on local policy and subscription information, decides to forward the NAS message to the target AMF via (R)AN, the initial AMF sends a Reroute NAS message to the (R)AN (7a). The Reroute NAS message includes the information about the target AMF and the Registration Request message carried at step 1. If the initial AMF has obtained the information as described at step 4b, that information is included. The (R)AN sends the Initial UE message to the target AMF (7b) indicating reroute due to slicing including the information from step 4b that the NSSF provided.

8. After receiving the Registration Request message transmitted at step 7(A)a or step 7(B)b, if no UE context is received from the initial AMF, the target AMF, based on rerouting due to slicing, continues with the Registration procedure from step 4 until 22 of figure 4.2.2.2.2-1 in TS 23.501 [2] (with the target AMF corresponding to the new AMF). If the UE context is received from the initial AMF, the target AMF continues with the Registration procedure from step 8 or 9b (depending on whether it decides to reauthenticate the UE) until step 22 of figure 4.2.2.2.2-1 in TS 23.501 [2], skipping step 10.

#### 6.1.4.4 Impacts on existing entities and interfaces

- UE: Support of Mutual Exclusive Access Group Information and procedures that include it for its configuration in the UE from the network.

- AMF: Enforcement of the Mutual Exclusive Access Group Information received from UDM and/or inclusion in NSSF queries as part of sending the Subscribed S-NSSAIs.

- NSSF: Enforcement of the Mutual Exclusive Access Group Information.

- UDM: Provision of the Mutual Exclusive Access Group Information in the UE based on UE's Mutually Exclusive Access capability and if applicable, the SLA roaming agreement with the UE's HPLMN.

#### 6.1.4.5 Evaluation

### 6.1.5 Solution #1.5: Mutually Exclusive Access to Network Slices using existing mechanisms

#### 6.1.5.1 Introduction

This is a solution to Key Issue #1, "Mutually Exclusive Access to Network Slices".

This solution is based on existing Rel-15 slice selection mechanisms and does not require any protocol impacts.

#### 6.1.5.2 Functional description

##### 6.1.5.2.1 General assumptions

This solution assumes the following:

- It is assumed that the UE has internal logic (e.g. MMI, or software support) to understand which applications are needed at a given time, and is able to prioritize the applications requiring different S-NSSAIs. The UE also orders the S-NSSAIs in the Requested NSSAI according to their priority from how the UE wants to use them (i.e. when an application is of highest priority the associated S-NSSAI is derived, e.g. from the URSP, and the S-NSSAI is put first in the Requested NSSAI). The UE continues to derive the priority of the subsequent S-NSSAIs based on the importance of the applications and places the resulting S-NSSAIs in priority order in the Requested NSSAI. The UE derives S-NSSAIs for all the applications the UE wants to use, and the UE should derive the priority order for all of the S-NSSAIs.

- It is assumed that the AMF/NSSF leverage on the understanding that the Requested NSSAI is sorted in a priority order, and that the AMF/NSSF does not include in the Allowed NSSAI S-NSSAIs of lower priority which are Mutuall Exclusive from higher priority S-NSSAIs.

- The UE understands that an S-NSSAI requested (i.e. it exists in the Configured NSSAI for the serving PLMN) which is not rejected nor in the Allowed NSSAI is mutual exclusive to one or more of the S-NSSAIs in the Allowed NSSAI. If the UE wants to access such an S-NSSAI, the UE puts it with high priority in a new Requested NSSAI.

##### 6.1.5.2.2 Applying proposed logic to an example

Example Network Configuration:



Figure 6.1.5.2.2-1: Example Network configuration for Mutually Exclusive Network Slices

Example UE configuration:

- Configured NSSAI: Slice A, B, C, D, E, F, G, H.

- URSP/NSSP: App1a, App1b, App1c->Slice A, App2a, App2b->Slice B, App3a, App3b->Slice C, App4->Slice D, App5->Slice E, App6->Slice F, App7->Slice G, App8->Slice H.

Scenario 1:

1. The UE wants to use 3 applications with priority App1a, App3a, App2a.

2. Requested NSSAI (Slice A, Slice C, Slice B).

3. Allowed NSSAI (Slice A, Slice B):

- The network does not include Slice C in the Allowed NSSAI as it is not allowed to be accessed at the same time as the higher prioritized Slice A.

4. From the Allowed NSSAI, the UE understands that Slice C may be mutually exclusive from Slice A.

5. Time pass and the UE wants to use App3a i.e. the UE puts the Slice C with higher priority: Requested NSSAI (Slice C, Slice A, Slice B).

6. Allowed NSSAI (Slice C):

- UE anticipated that Slice A and Slice C would not be accepted into the Allowed NSSAI but included them anyway to make network aware of UE wanted slices.

In the above scenario the optimal Network Slice configuration is achieved immediately.

Scenario 2:

1. The UE wants to use 6 applications App1a, App1b, App2a, App2b, App3a, App5 and highest priority is App1a. From URSP UE derives that App1a is to use Slice A and so is App1b. Second priority is App2a, and from URSP the UE derives the slice to be used and also that App2b is to use the same slice. The UE has no further preferences on priority between the other applications but derives the slices to be used and places these in the Requested NSSAI after the prioritized slices.

2. Requested NSSAI (Slice A, Slice B, Slice C, Slice E):

- The network handles the Requested NSSAI as the S-NSSAIs are in priority order.

3. Allowed NSSAI (Slice A, Slice B):

- The network does not include Slice C and Slice E in the Allowed NSSAI as it is not allowed to be accessed at the same time as the higher prioritized Slice A and Slice B.

4. From the Allowed NSSAI, the UE understands that Slice C and Slice E may be mutually exclusive from Slice A and Slice B.

5. Time pass and the UE wants to use App3a, and sends a new Requested NSSAI (Slice C, Slice A, Slice B).

6. Allowed NSSAI (Slice C):

- The network does not include Slice A and Slice B in the Allowed NSSAI as they are not allowed to be accessed at the same time as the higher prioritized Slice C.

Scenario 3:

1. The UE wants to use 1 application App1a.

2. Requested NSSAI (Slice A).

3. Allowed NSSAI (Slice A).

4. The UE establishes a PDU Session using Slice A.

5. Time pass and the UE wants to use App3a i.e. two options exist:

Option 1:

- the UE need to use App3a, but the current App1a is more important: Requested NSSAI (Slice A, Slice C);

- Allowed NSSAI (Slice A):

- the UE knows that Slice A and Slice C may be mutually exclusive and to be able to use App3 the UE needs to put Slice C with higher priority than Slice A.

Option 2:

- the UE really need to use App3a, i.e. it is more important than current App1a (even though it has an established PDU Session): Requested NSSAI (Slice C, Slice A).

- Allowed NSSAI (Slice C) and the network released the current PDU Session for Slice A as the PDU Session shall not be allowed to be used when UE is registered to the Slice C.

- the UE knows that Slice A and Slice C may be mutually exclusive.

- the UE establishes a PDU Session for Slice C.

In the above scenario the optimal Network Slice configuration is achieved immediately for both options.

The options 1 and 2 shows how to handle already established PDU Sessions.

It is unlikely that there are already deployed Rel-15 UEs, but if there are then it can be assumed that these UEs either can be updated to apply the logic described above or that these UEs simply add S-NSSAIs to the end of the Requested NSSAI and then there is no issue as they are seen as lower priority by the network.

#### 6.1.5.3 Procedures

##### 6.1.5.3.1 General

No new procedures are required with this solution.

##### 6.1.5.3.2 Signalling within the network

In principle this solution is independent from how information is signalled within the network, i.e. this solution can be combined with any other solution addressing the required signalling within the network.

NSSF and AMF are possible decision points. HPLMN and VPLMN input needed.

For V-NSSF, no need for any signalling for VPLMN considerations.

When AMF is the decision point, the VPLMN considerations is likely achieved by O&M in the AMF as otherwise why decide in AMF?

For HPLMN input, one may consider SLA or VPLMN getting input from UDM, H-PCF or H-NSSF.

Consequently, the only new signalled information that may be required is the signalling of HPLMN policies towards the VPLMN (unless derived by SLA). The most straightforward option seems to be to signal the HPLMN input from UDM to the AMF, and then if decision point is NSSF the AMF forwards the HPLMN input to the NSSF.

##### 6.1.5.3.3 Interactions with Rel-15 usage of Allowed NSSAI

In Rel-15, the S-NSSAIs that the UE proposed in the Requested NSSAI which were not included in the Allowed NSSAI nor rejected are subscribed S-NSSAIs (as included in the Configured NSSAI) but currently not available for usage (e.g. not available in the RA). The UE does not have more information than that why the S-NSSAI was not registered, i.e. there is no defined procedure in Rel-15 for allowing the UE to discover when an S-NSSAI becomes available in the new area for the UE. One could propose a similar logic as for LADN, in which the UE gets notified which LADNs are available for the UE in the new RA. Such logic could be seen as new functionality and therefore not agreeable.

Under current circumstances, as the UE does not know when an S-NSSAI becomes available the UE has no other choice than to propose the same S-NSSAI again in the Requested NSSAI. Combining the proposed logic for handling mutually exclusive slices, it would mean that the UE should propose the S-NSSAI in the order of priority the UE wants the S-NSSAI to be registered.

##### 6.1.5.3.4 Characteristics of the solution

This solution has no impacts to the protocol towards the UE, and in case SLA covers the agreements of MEANS for Network Slices then there is no need for any signalling within the network. In case SLA is not enough as a solution, then signalling of HPLMN requirement for MEANS to VPLMN would be required, and that is assumed to be covered by another solution.

The solution achieves an optimal combination of network slice configuration for a UE without the need to signal any additional MEANS information from the network to the UE.

The logic that the UE order the S-NSSAIs in priority order could be efficient when the information the UE has available is outdated, i.e. the solution can be used also when MEANS information is standardized as to allow a network decision already before sending the updated MEANS information to the UE.

The UE does not know whether the Slices really are mutually exclusive, but there is no need for the UE to know as the UE can act the same way independently.

The Requested NSSAI becomes larger than necessary as the UE always provides the slices the UE wants to use (derived by wanted applications and the URSP), but thereby the network gets aware of which slices the UE really wants to access and the network operator may try to address the customer needs by creating new slice configuration accordingly (MEANS groups).

#### 6.1.5.4 Impacts on existing entities and interfaces

Impacts compared to Rel-15:

- This solution has no protocol impacts, but only a few logical assumptions.

UE impact:

- The UE provides the list of S-NSSAIs in the Requested NSSAI in priority order.

- The UE understands that an S-NSSAI requested (i.e. it exists in the Configured NSSAI for the serving PLMN) which is not rejected nor in the Allowed NSSAI is mutual exclusive to one or more of the S-NSSAIs in the Allowed NSSAI. If the UE wants to access such an S-NSSAI, the UE puts it with high priority in a new Requested NSSAI.

5GC impact (serving and home):

- The AMF/NSSF assumes that the UE provides the list of S-NSSAIs in the Requested NSSAI in priority order.

- If the Requested NSSAI includes Mutually Exclusive S-NSSAIs, then the AMF/NSSF does not include the S-NSSAIs of lower priority in the Allowed NSSAI until all S-NSSAIs of the Allowed NSSAI are allowed to be access together.

- Impacts to make VPLMN aware of HPLMN policies for MEANS and for applying VPLMN policies in the VPLMN.

In this solution, Mutually Exclusive Access to Network Slices in the network is already supported in Rel-15 and does not require any further changes. Actual isolation of resources between network slices is supported by the underlying virtualisation environment and OAM (see SA5 specifications).

#### 6.1.5.5 Evaluation

### 6.1.6 Solution #1.6: Enabling access control to network slices that cannot be access simultaneously

#### 6.1.6.1 Introduction

##### 6.1.6.1.1 Design Principles

The following consideration constitute the Design Principles substantiating this solution:

- It should be possible for an operator to decide whether two or more Network Slices can be configured to be accessed within the same PLMN and whether they can be accessed simultaneously or not on a per UE basis.

- The current Rel-15 Configured NSSAI concept, which establishes that a Configured NSSAI "may either be configured by a Serving PLMN and apply to the Serving PLMN, or may be a Default Configured NSSAI configured by the HPLMN and that applies to any PLMN" should be preserved.

- Rel-15 baseline should be used for basic enforcement of Access to Network Slices whereby a UEs use the Requested NSSAI to signal what Network Slices the UE is requesting to access in the current PLMN. As such the Requested NSSAI should be based on the (Default) Configured NSSAI and Allowed NSSAI when available.

##### 6.1.6.1.2 Working Assumptions

Operator defined Access to Network Slices: The proposal assumes that an operator should be able to determine what Network Slices should or should not be accessed together at all and what Network Slices can be accessed within the same PLMN but not simultaneously on a per UE basis.

During the Registration procedure the UE is provided with an Allowed NSSAI, and information on whether two or more S-NSSAIs in the Configured NSSAI cannot be supported by the 5GS to serve the UE simultaneously and information whether two or more S-NSSIAs, contained in the Allowed NSSAI can be used simultaneously. This information is provided as part of the Registration Accept message and in this proposal, this information is referred to as Network Slice exclusion rules. The UE can then use this information (i.e., Network Slice exclusion rules, Configured NSSAI and Allowed NSSAI) to determine whether the 5GS supports a combination of S-NSSAIs from the Configured NSSAI which the UE uses when constructing the Requested NSSAI. In addition, the UE can determine whether two or more Network Slices can be used simultaneously, when requesting access to UP resources, e.g. through a PDU Session Establishment procedure or a CP resources, e.g., through a Service Request procedure.

Network Slice exclusion rules proposed in this solution also supports the case where an operator chooses to configure an AMF or NSSF to provide only non-mutually exclusive Network Slices in the Allowed NSSAI, if it is so desired.

The solution sticks to current Rel. 15 definition of Allowed NSSAI: "NSSAI provided by the Serving PLMN during e.g. a Registration procedure, indicating the S-NSSAIs values the UE could use in the Serving PLMN for the current registration area"

Therefore, the solution assumes an operator may configure the AMF to include the Allowed NSSAI combinations of S-NSSAIs that are allowed in the current registration area but that may or may not be used simultaneously, in contrast with the Allowed NSSAI used in Rel-15 where Network Slices can always be used simultaneously.

The enforcement of mutually exclusive rules, e.g. when the Allowed NSSAI includes combinations of S-NSSAIs referring to Network Slices that may and may not be used simultaneously, takes place during PDU Session Establishment and Service Request procedures.

As per Rel-15 principles, upon the establishment of a NAS Signalling connection, a single N1 termination point is located in the AMF and the AMF may keep the NAS signalling connection until the UE de-registers from the network. The AMF is therefore in the position to enforce exclusion rules for messages intended to Network Slices that that should not be used simultaneously with other already serving Network Slices.

The solution assumes that different Network Slice exclusion rules affecting the same set of slices could be provided to different UEs.

The solution assumes that a common AMF may be shared by two or more Network Slices that are configured so that they cannot be accessed simultaneously.

NOTE: It is FFS whether solutions should address Network Slice exclusion aspects of all procedures that take place prior to the establishment of a PDU Session.

Editor's note: This solutions focuses on the FS\_eNS Objective pertaining to "Identify, prioritize and study the practical non-roaming and roaming deployment scenarios and system impacts when the 5GS is not able to support all possible combination of S-NSSAIs for the UE". The solution addresses this aspect by providing Network Slice exclusion rules for all S-NSSIs from the Subscribes S-NSSAIs. In addition, this solution allows the enforcing of Network Slice exclusion rules for S-NSSAIs referring to Network Slices that cannot be accessed simultaneously, during a PDU Session Establishment procedure and Service Request procedure to prevent simultaneous use of Network Slices that are mutually exclusive but which S-NSSAI combination can still be supported by the 5GS.These rules may be configured at the AMF or NSSF

The solution assumes during the SMF selection, that the NSSF (or AMF if configured accordingly) is configured to apply Network Slice exclusion rules. The application of relevant Network Slice exclusion rules will ensure that the UE only accesses slices that can be access simultaneously according to the Network Slice exclusion rules. If a UE, which requests access to a Network Slice that is mutually exclusive to slices that are already accessed, the Network (i.e., the AMF) will reject the request with an appropriate code. A UE may request access to Network Slices that are mutually exclusive e.g. due to USIM swap.

##### 6.1.6.1.3 Network Slice Access Exclusion Rules

Exclusion rules are configured in the subscriber record within the UDM on a per S-NSSAI basis. The exclusion rule can be either preconfigure in the UE or provided via the Registration procedure or Configuration Update procedure. The exclusion rules provided to the UE convey the following information on a per S-NSSAI basis:

1) S-NSSAIs that are mutually exclusive to this S-NSSAI. This effectively yields combinations of S-NSSAI that can be accessed simultaneously. This combination can be configured or tagged as groups but the proposals does not mandate this.

2) Whether a mutually exclusive S-NSSAI can be used sequentially (if a two mutually exclusive S-NSSAI are included in the Allowed NSSAI, this indicates that two or more Network Slices can be sequentially used without the need to re-register as long as they are not accessed simultaneously. When no entries in the Allowed are mutually exclusive as per the provided exclusion rules, the UE can use all entries in the Allowed NSSAI simultaneously.

NOTE: This proposal assumes that exclusion rules are provided as a separate information element (e.g., not necessarily part of the Configured NSSAI). Furthermore, the proposal does not mandate that non- mutually exclusive S-NSSAI be grouped but it does not precluded grouping. This is left to Stage 3 to decide.

A S-NSSAI that is not defined/tagged as mutually exclusive to any other S-NSSAI can be used in simultaneously with any other S-NSSAI. If grouping were to be used this would correspond to the case where such an S-NSSAI would be part of all Non-Mutually Exclusive groups. Likewise, a S-NSSAI for which all other S-NSSAI have marked it as mutually exclusive, would correspond to a single S-NSSA|I group.

Editor's note: Need further clarification on the practicality of your proposal to justify the support for mutually exclusive access in Rel‑16 5GS when a S-NSSAI that is not tagged. Per the descriptions above, it can be used simultaneously with any other S-NSSAI, especially such S-NSSAI is the one to be used by the Rel‑15 UE. Does it imply that Rel‑15 UE can actually get better services than the Rel‑16 UE if it is capable of supporting mutually exclusive access?

6.1.6.1.3.1 Roaming Consideration

Exclusion rules follow the same Rel-15 model with regards to roaming scenarios, whereby S-NSSAI information in the visited network is mapped to the Home counterpart. As such, exclusion rules from HPLMN are mapped to exclusion rules from VPLMN based on operators Service Level Agreement dictating the treatment of S-NSSAI information in the visited PLMNs.

The use of Exclusion rules by the VPLM specifying whether S-NSSAI can be used sequentially can be mapped to HPLMN rules. However local policies in the VPLMN may prohibit the use of S-NSSAI in the Allowed NSSI that are mutually exclusive.

#### 6.1.6.2 High-level Description

##### 6.1.6.2.1 Services and Illustrated Procedures

###### 6.1.6.2.1.1 Registration Procedure



Figure 6.1.6.2.1-1: Registration procedure

1-21. As per current specification.

22. The Network (AMF if configured to do so or NSSF) derives the set of Network Slices that can and cannot be accessed simultaneously and/or the combination(s) of Network Slices that are not supported in the 5GS.

If the Allowed NSSAI contains S-NSSAIs that may or may not be configured to be used simultaneously as specified in the exclusion rules, the UE then uses these Network Slice exclusion rules to determine what Network Slices can be accessed during a PDU Session Establishment of Service Request procedure.

NOTE 1: If the Network Slice Exclusion rules provided to the UE in the Registration Accept message do not indicate any Network Slice combination that cannot be used simultaneously, that means that all S-NSSAIs in the Allowed NSSAI correspond to Network Slices that the UE can access at any time.

Network Slice Exclusion rules for Network Slices that cannot be accessed simultaneously (i.e. through the same AMF) apply to the S-NSSAIs within the Allowed NSSAI provided to the UE by the current AMF and they may also apply to S-NSSAIs entries in the Configured NSSAI, which the UE uses to construct a Requested NSSAI.

In roaming scenarios, the use of exclusion rules by the VPLMN specifying whether S-NSSAI can be used sequentially can be mapped to HPLMN rules. However local policies in the VPLMN may prohibit the use of S-NSSAI in the Allowed NSSI that are mutually exclusive.

If the UE wants to request access to Network Slices, corresponding to S-NSSAIs not present in the Allowed NSSAI, the UE applies Network Slice exclusion rules applicable to all S-NSSAIs included UE in the Configured NSSAI and UE re-registers without providing the 5G GUTI in the AS message.

NOTE 2: Similar to the derivation and construction of the Allowed NSSAI which is provided upon successful registration, a new set of Network Slice exclusion rules may also be provided at any time, e.g. upon a successful Registration procedure or through a UCU procedure.

###### 6.1.6.2.1.2 Enforcement of mutually exclusive rules

For the case when the Allowed NSSAI includes S-NSSAIs that are mutually exclusive, the following cases apply:

1) The UE attempts to establish a PDU Session on a Network Slices that is mutually exclusive (clause 6.1.6.2.1.2.1 applies.

NOTE: If the NAS transaction is not network slice specific (e.g. Sending of SMS over NAS) the solution assumes that all slices are applicable for this this transaction.

6.1.6.2.1.2.1 PDU Establishment



Figure 6.1.6.2.1.2-1: PDU Establishment

0. Based on the Allowed NSSAI, URSP/NSSP rules (e.g., Network Slice exclusion rules from VPLMN received during Registration procedure) and local configuration, the UE can select S-NSSAIs to form Allowed NSSAI request the establishment of a PDU Session, considering the S-NSSAI Network Slice exclusion rules from VPLMN.

1. If in Step 0 the UE chooses a S-NSSAI that cannot be used simultaneously (according to the Network Slice exclusion rules from VPLMN) with other S-NSSAI(s) where PDU Sessions are already established, the UE initiates a PDU Session Release procedure of those PDU Sessions selected in step 0.

2. The UE initiates a PDU Session Establishment procedure, providing the S-NSSAIs for PDU Session to be established selected in step 0.

Editor's note: PDU Session Release has nothing to do with to the NAS session connectivity over the N1. Need further clarification on how the network prevents the UE to access the other mutually exclusive slices simultaneously while the NAS (the control plane) remains active to communicate with all slices which are served by the same AMF.

#### 6.1.6.3 Impacts on existing services and interfaces

The AMF/NSSF may determine that set of rules the UE needs to follow when selecting slices that are mutually exclusive. The Network (the AMF) sends this rules during the Registration procedure or through a Configuration Update procedure.

The AMF may invoke PDU Session Release operation (Nsmf\_PDUSession\_ReleaseSMContext) to release PDU Session on network slices that are mutually exclusive.

Editor's note: PDU Session Release has nothing to do with to the NAS session connectivity over the N1. Need further clarification on how the network prevents the UE to access the other mutually exclusive slices simultaneously while the NAS (the control plane) remains active to communicate with all slices which are served by the same AMF.

Editor's note: Need further clarification on the impacts to specific functional elements

#### 6.1.6.4 Evaluation

### 6.1.7 Solution #1.7: Solutions for MEANS via Slicing Group Indication

#### 6.1.7.1 Introduction

This is a solution to Key Issue #1, "Mutually Exclusive Access to Network Slices" (MEANS).

In this solution, each Network Slice is deployed to belonging to a Mutually Exclusive Access Network Slice Group (MEAG). Each Mutually Exclusive Access Network Slice Group represents a set of network slices which can share a common AMF.

#### 6.1.7.2 Functional description

##### 6.1.7.2.1 UE configuration

The UE is configured with Configured NSSAI and MEAG IDs associated with each S-NSSAI from the Configured NSSAI. Figure 6.1.7.2.1-1 shows the UE configuration. Rel 15 UE not supporting MEANS feature can ignore the MEAG IDs and uses Configured NSSAI only when it generates Requested NSSAI. Rel 16 UE supporting MEANS feature can interpret MEAG IDs as well as Configured NSSAI and considers both information when it generates Requested NSSAI.

|  |  |
| --- | --- |
| Configured NSSAI | MEAG ID |
| S-NSSAI1 | MEAG#1 |
| S-NSSAI2 | MEAG#1 |
| S-NSSAI3 | MEAG#2 |
| S-NSSAI4 | MEAG#2 |
| S-NSSAI5 | MEAG#3 |
| **\ /**  **\\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**  **Rel-15 UE** |  |
| **\ /**  **\\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**  **Rel-16 UE** | |

Figure 6.1.7.2.1-1: S-NSSAI and MEAG associated with the S-NSSAI

Editor's note: It is FFS whether a S-NSSAI including SD field in the S-NSSAI can belong to multiple MEAGs or not belong to any MEAG.

##### 6.1.7.2.2 UE subscription

The UE subscription in UDM also includes subscribed S-NSSAIs and MEAG IDs associated with each subscribed S-NSSAI.

##### 6.1.7.2.3 Operations

When a UE requests network slices during registration, the UE shall generate Requested NSSAI including S-NSSAIs only belonging to the same MEAG, i.e. not include S-NSSAIs belonging to different MEAGs. The UE also provides MEAG ID together with Requested NSSAI. The Allowed NSSAI provided to the UE during registration procedure shall not include S-NSSAIs from different MEAGs in Allowed NSSAI, together.

5G CN may configure a UE with Configured NSSAI which includes S-NSSAI(s) with associated MEAG IDs during registration or update Configured NSSAI for the UE after registration at any time. Specifically in Registration Request, if UE does not include Requested NSSAI or UE includes S-NSSAIs from different MEAGs in Requested NSSAI, 5G CN should configure a UE with S-NSSAI(s) with associated MEAG IDs.

When AMF is selected for supporting network slice, the selected AMF can be shared with other S-NSSAIs of same MEAG but not shared with other S-NSSAIs from different MEAGs.

The Allowed NSSAI provided to the UE during registration procedure shall not include S-NSSAIs from different MEAGs together.

When UE requests S-NSSAI different from MEAG which current active network slice is belonging to, UE shall deregister from current network slice, first.

6.1.7.2.3.1 Coexistence with Rel-15 UE

Figure 6.1.7.2.3.1-1 shows MEANS deployment in a PLMN. The left side of the figure illustrates Rel-15 Network Slice deployments. In Rel-15 network, it is assumed that AMF can support all S-NSSAIs provided by the PLMN and requested by a UE. The right side of the figure illustrates Rel-16 Network Slice deployments with MEANS feature. The set of S-NSSAIs supported in the Rel 15 network on the left side of the figure is considered as one MEAG (i.e. Rel-15 MEAG) in Rel16 network because it seems not reasonable to say that the set of S-NSSAIs which can be supported at the same time in Rel 15 network becomes no longer supported at the same time in Rel 16 network.When a Rel-15 UE registers to a Rel.16 network, it will not include MEAG ID in Requested NSSAI and the gNB will select AMF based on the received Requested NSSAI.



Figure 6.1.7.2.3.1-1: MEANS deployment

##### 6.1.7.2.4 Roaming support

When UE performs registration procedure in roaming, if it has neither Configured NSSAI nor Allowed NSSAI for the PLMN, it does not provide Requested NSSAI in the Registration Request. When a gNB in VPLMN receives a Registration Request without Requested NSSAI, it may select a default AMF for forwarding the Registration Request message. In this case, NSSF is assumed to provide Configured NSSAI and MEAG IDs associated with the S-NSSAI of the Configured NSSAI for the serving PLMN if Mutually Exclusive Access for network slices are supported; otherwise, only Configured NSSAI without MEAG ID is provided. When NSSF is not deployed, it is assumed that the selected default AMF is capable of providing Configured NSSAI and MEAG IDs associated with the S-NSSAI of the Configured NSSAI for the serving PLMN if Mutually Exclusive Access for network slices are supported; otherwise, only Configured NSSAI without MEAG ID is provided.

When a default AMF receives Registration Request, it may determine the Configured NSSAI and/or the Allowed NSSAI which may include the associated MEAG ID(s) and the mapping information. When an AMF different from the default AMF is selected as a serving AMF, the default AMF may forward the Configured NSSAI, and mapping information and possible the MEAG IDs for the UE to the new serving AMF; alternately, the new serving AMF, which may be supported by NSSF, determines the Configured and/or the Allowed NSSAI that may include the associated MEAG ID(s) if Mutually Exclusive Access for network slices are supported. And the serving AMF provides the Configured and/or the Allowed NSSAI, the mapping information and possible the MEAG IDs to the UE in the Registration Accept.

For roaming case, Serving PLMN may provide Configured NSSAI including associated MEAG ID per included S-NSSAI for roamer UE and mapping of each S-NSSAI in the Configured NSSAI in Serving PLMN to corresponding S-NSSAI(s) values for the HPLMN.

When Serving PLMN provides Configured NSSAI including MEAG ID for each S-NSSAI, it shall be kept that S-NSSAIs belonging to corresponding MEAGs in HPLMN.

When UE supporting MEANS roams to the network not supporting MEANS(e.g. Rel-15), the UE will be aware of the serving network not supporting MEANS based on capability negotiation during registration and the UE will be configured only with NSSAIs without MEAG. When the UE compose Requested NSSAI based on Configured NSSAI, the UE shall include NSSAIs belonging to the same MEAG which was assigned in HPLMN.

#### 6.1.7.3 Procedures

##### 6.1.7.3.1 RAN configuration

NG setup procedure between gNB and AMF is specified in clause 16.4.3 of TS 38.300 [5]. The gNB and the AMF exchange the list of supported S-NSSAIs. In addition to clause 16.4.3 of TS 38.300 [5], the AMF provides to the RAN the MEAG ID along with the list of supported S-NSSAIs as shown in Figure 6.1.7.3.1-1.



Figure 6.1.7.3.1-1: RAN configuration procedure

##### 6.1.7.3.2 Registration procedure

Figure 6.1.7.3.2-1 shows a Registration procedure.



Figure 6.1.7.3.2-1: Registration procedure

The Registration procedure is performed as defined in TS 23.502 [3] with the following additions:

1. The UE generates Requested NSSAI including S-NSSAIs only within the same MEAG ID. The Slice Group ID is also included along with the Requested NSSAI in Registration Request message.

3. The RAN selects AMF based on Requested NSSAI as specified in TS 23.502 [3]. If the RAN is not able to find an AMF which can support all S-NSSAIs in the Requested NSSAI, then it forwards the message to an AMF belonging to the requested MEAG ID.

6. AMF reallocation may happen within the same slice group.

The AMF or NSSF may verify whether all S-NSSAIs in the Requested NSSAI are correctly associated with the same MEAG ID. If some of the S-NSSAIs in the Requested NSSAI are not belonging to the same MEAG ID, then AMF or NSSF considers that the UE configuration is not up-to-date and triggers UE configuration update.

7. If UE configuration update is required as described in step 6, the Registration Accept message includes Configured NSSAI and the associated MEAG IDs.

#### 6.1.7.4 Impacts on existing entities and interfaces

To support MEANS, below are the impacted entities and interfaces listed:

- Support for UE generating Requested NSSAI within a same slice group and providing MEAG ID in Registration Request.

- Support for RAN selecting AMF based on MEAG ID.

- Support for AMF triggering UE configuration update by verifying the Requested NSSAI against the MEAG ID.

- Support for NSSF reallocating AMF within a same slice group.

Impacted interfaces: N1, N2.

#### 6.1.7.5 Evaluation

### 6.1.8 Solution #1.8: Solution to Key issue#1: Access to new group of Network Slices.

#### 6.1.8.1 Introduction

There are several solutions in the TR addressing the key issue#1. Most solution in some way provides the UE with information about which MEANS (different names in the different solutions) group a Network Slice belongs to.

#### 6.1.8.2 Functional description

In Rel-15 a UE likely will simply try to add another S-NSSAI from the Configured NSSAI while the UE is in CM-CONNECTED or from CM-IDLE while still indicating the valid GUAMI. However, MEANS seems to drive the need for the UE to access the network again from CM-IDLE without indicating GUAMI from old registration as to allow the 5G-AN to select 5GC based on Requested NSSAI. The other option would be to allow re-allocation to new slices while the UE is in state CM-CONNECTED which is not yet fully functional. The FS\_ETSUN study may solve it (or other studies), but it seems uncertain whether that will be enabled in Rel-16. Independent if it is enabled by FS\_ETSUN, it is not certain that such functionality will be possible to use for moving a UE between MEANS groups e.g. in case isolation between MEANS groups is required.

However, as to not requiring the UEs to go through CM-IDLE when re-allocation of slices are possible while in CM-CONNECTED it is proposed that the network should be able to indicate whether the UE shall request access to other MEANS group from CM-IDLE without indicating GUAMI or 5G-S-TMSI in 5G-AN signalling (i.e. to trigger the 5G-AN to do the selection) or whether UE can request it while in CM-CONNECTED (i.e. as 5GS will enable re-allocation even if e.g. PDU Session for another MEANS group is established). The indication is either provided together with information about the MEANS groups provided to the UE (i.e. see each solution for the key issue#1), or the indication can be sent by the AMF separately. If sent separately the information could be to which MEANS group(s) the UE may use the more efficient change while being connected to the current AMF i.e. while in CM-CONNECTED.

Such indication can be used together with any of the existing solutions in the TR i.e. it should be seen as an add on (complement) to any available solution (unless the specific solution explicitly addresses the issue).

#### 6.1.8.3 Procedures

The procedure for the main adopted solution applies, and together with that adopted solution additional information/indication can be sent as whether the MEANS group can or shall be accessed while in CM-IDLE without indicating GUAMI or 5G-S-TMSI in 5G-AN signalling.

As an option or additional enhancement, the network, e.g. AMF, may indicate to which MEANS groups the UE can use the more efficient re-allocation while staying in CM-CONNECTED for the current Registration (Allowed NSSAI). The network, e.g. AMF, may provide such information as part of the Registration Accept message or as part of UE Configuration Update procedure.

#### 6.1.8.4 Impacts on existing entities and interfaces

- UE: Impacts as per main solution to be adopted by the study, and in addition receiving indication whether an S-NSSAI or group of network slices supports being accessed via CM-CONNECTED (or UE needs to do it from CM-IDLE without indicating GUAMI/5G-S-TMSI in 5G-AN signalling).

- Network: Impacts as per main solution to be adopted by the study and in addition sending to the UE an indication or information whether an S-NSSAI or group of network slices (MEANS group) supports being accessed via CM-CONNECTED (or UE needs to do it from CM-IDLE without indicating GUAMI/5G-S-TMSI in 5G-AN signalling).

#### 6.1.8.5 Evaluation

This solution is complementing any of the existing solutions in the TR. The solution enables the UE to know whether an efficient re-allocation/change of Network Slices (e.g. changing the Requested NSSAI compared to Allowed NSSAI by e.g. adding more S-NSSAIs from the Configured NSSAI) or MEANS group can be enabled while the UE is in CM-CONNECTED or whether the UE has to go through CM-IDLE state.

## 6.2 Solutions for KI#2

### 6.2.1 Solution#2.1: Network slice instance selection in initial AMF

#### 6.2.1.1 Introduction

This solution address the key issue#2: Enabling interworking for slicing between EPC and 5GC.

#### 6.2.1.2 Functional description

The PGW-C+SMF knows the S-NSSAI or each PDN connection. In connected mode, Initial AMF uses the Nsmf\_PDUSessionCreateSMContext service operation with the PGW-C+SMF that returns the S-NSSAI and PDU Session ID to the Initial AMF selected by the source MME. Then the Initial AMF determines the set of network slices supported for the UE, and, if required, selects the Target AMF and forward the handover message to the target AMF . The rest are same procedure as normal EPS to 5GS handover procedure using N26 interface.

For IDLE mode mobility from EPS to 5GS using N26 interface, the Target AMF uses the Nsmf\_PDUSessionCreateSMContext service operation with the PGW-C+SMF to retrieve the S-NSSAI of the transferred PDU Connection. The S-NSSAI of the PDU session returned by PGW-C+SMF is used to select a correct V-SMF as described in clause 4.11.1.3.3 of TS 23.502 [3].

NOTE 1: This solution uses existing solution in Release 15 to correlate the EBI and S-NSSAI of the PDU session as described in clause 4.11.1.2.2 and clause 4.11.1.3.3 in TS 23.502 [3]. The AMF sends UE EPS PDN Connection received from MME to SMF and the SMF return the EBI information and the S-NSSAI of the PDU session.

#### 6.2.1.3 EPS to 5GS handover Procedures



Figure-6.2.1.3-1: EPS to 5GS handover using N26 interface

1. Step 1 to step 6 are same as normal EPS to 5GS handover using N26 interface.

Editor's note: Step 4 must be aligned with TS 23.502 [3] to use CreateSMContext.

7. The SMF + PGW-C sends a Nsmf\_PDUSessionCreateSMContext Response (PDU Session ID, N2 SM Information (PDU Session ID, QoS Rules, EPS Bearer Setup List, H-CN Tunnel-Info, S-NSSAI), S-NSSAI) to the initial AMF. SMF includes mapping between QoS flows and EPS bearers as part of N2 SM Information container.

8. The Initial AMF performs network slice instance selection and the target AMF based on the S-NSSAI received in step 7.

In home-routed roaming case, if the VPLMN and HPLMN have an SLA to support non-standard S-NSSAI values in the VPLMN, the Initial AMF uses the NSSF of the VPLMN to map the S-NSSAI values to the respective S-NSSAI values to be used in the VPLMN.

9. The Initial AMF sends Namf\_Communication\_CreateUEContext service operation (Target 5GAN Node ID, Source to Target Transparent Container, EPS MM Context, EPS Bearer Context(s), N2 SM Information received in step 7, S-NSSAI received in step 7) message to the target AMF. Based on the S-NSSAI the target AMF may reselect a new V-SMF2. In case of no change of V-SMF, step 10-12 are skipped and in step 13 the target AMF uses the N2 SM Information received in step 7.

10. If the Target AMF reselects a new V-SMF2, it sends Nsmf\_PDUSessionCreateSMContext Request(UE EPS PDN Connection, N2 SM Information) to V-SMF2.

11-12. The V-SMF2 establishes the N4 session with V-UPF2. The V-UPF2 allocates CN tunnel information. The V-SMF2 updates N2 SM Information with the S-NSSAI and the CN tunnel information of V-UPF2. The V-SMF2 then sends Nsmf\_PDUSessionCreateSMContext Response (PDU Session ID, N2 SM Information) towards target AMF.

13-31. Step 13 to step 31 are same procedure as normal EPS to 5GS handover procedure using N26 interface in clause 4.11.1.2.2 of TS 23.502 [3]. In additional, in step 19, the initial AMF initiates resource release of V-SMF1 and V-UPF. The Forward Relocation Complete notification message is relayed by an initial AMF in case that the target AMF does not support N26 interface.

#### 6.2.1.4 Impacts on existing entities and interfaces

No impact on EPC.

No impacts on UE.

In connected mode, the Initial AMF selects the target network slice instance and the target AMF based on the S-NSSAI received from the PGW-C+SMF. Then it sends the Namf\_Communication\_CreateUEContext service operation with the EPS MM Context , EPS Bearer Context(s)and the N2 SM Info received from V-SMF1 to target AMF. The initial AMF removes the resources in V-SMF1 and V-UPF1 after the UE context has been transferred to target AMF.

The target AMF sends N2 SM Info received from initial AMF to V-SMF2 if new V-SMF2 is selected.

The V-SMF2 updates the N2 SM Info received from target AMF with S-NSSAI and CN tunnel information of V-UPF2 and sends the new N2 SM Info to the 5G-AN.

#### 6.2.1.5 Evaluation

This solution is based on Rel-15 solution and can provide slicing interworking between EPC and 5GC for both Rel-15 UE and Rel-16 UE. This solution has no impact on the PGW-C+SMF, therefore it can also work for roaming case when the PGW-C+SMF is Rel-15.

Additional enhancement (i.e. network slicing selection) is introduced in handover preparation phase which may add more handover latency. However the additional enhancement is within the VPLMN, i.e. no need for interaction across PLMNs.

The solution requires Rel-16 AMF and Rel-16 V-SMF.

### 6.2.2 Solution #2.2: Slice-aware mobility from EPC to 5GC

#### 6.2.2.1 Introduction

The solution addresses key issue number 2.

#### 6.2.2.2 Functional description

For mobility from EPC to 5GC, IDLE mode and CONNECTED mode mobility are addressed separately.

##### 6.2.2.2.1 Idle Mode Mobility from EPC to 5GC

The SM context in the EPC that is provided to the 5GC in case of mobility from EPC to 5GC does not contain any slicing information. This applies regardless if the UE initially registers and establishes connectivity in 5GC and then moves to EPC, or the UE initially registers and establishes connectivity in EPC.

As a result, when the UE moves to the 5GC from EPC, the AMF will have no information about the slice (identified by S-NSSAI) associated the UE's PDN connections moved from EPC. Consequently, the AMF will also not be able to verify whether the AMF selected during the mobility from EPC to 5GC is appropriate for the slices that the UE is connected to for its active PDU sessions.

To address this scenario, a solution is proposed based on the following.

6.2.2.2.1.1 Usage of slice mapping information for single-registration mode UEs

The solution uses the mapping of slices to PDN Connections. The UE determines the slice mapping per current release 15 mechanisms:

- For PDU sessions originally established over 5GC (i.e. before the UE has moved to EPC) the UE applied NSSP to determine S-NSSAI and DNN. When moving to EPC, the UE locally keeps the S-NSSAI information for those PDU sessions moved from 5GC.

- For PDN connections established over EPC, during PDN connection establishment in the EPC, the UE is provided by the PGW-C+SMF via PCO the S-NSSAI associated with the PDN connection, together with a PLMN ID that the S-NSSAI relates to. The UE stores this S-NSSAI and the PLMN ID associated with the PDN connection.

When moving from EPC to 5GC, for each PDU session single-registration mode UEs provide the AMF with slice mapping information containing the S-NSSAIs associated to the PDU Sessions active in the UE, together with the EPS bearer identity of the default EPS bearer corresponding to the PDN connection. The UE sends the slice mapping information in the Registration request when mobility from EPC to 5GC mobility happens.

The UE sends the slice mapping information and in the roaming case:

- In the AMF: When the AMF receives the slice mapping information from the UE in the Registration request, the AMF maps S-NSSAIs sent by the UE to S-NSSAIs for the Serving PLMN. AMF selects V-SMFs and V-UPFs based on slice mapping information (instead of default V-SMFs / default V-UPFs as in Rel-15).

- In the UE: When the UE receives the Configured NSSAI for the Serving PLMN (which includes the S-NSSAI values which can be used in the Serving PLMN and a mapping to the corresponding S-NSSAI values in the Configured NSSAI for the HPLMN) in the Registration Accept from the AMF, the UE updates the S-NSSAIs locally stored for sessions created in EPC to reflect the correct S-NSSAI for the current PLMN.

##### 6.2.2.2.2 Connected Mode Mobility from EPC to 5GC

Selecting the target AMF, and by that a set of network slices, based on information available at the source MME introduces a risk that the UE gets served by an AMF that is not appropriate and possibly by network slice(s) that are not in the UE's subscription. Even though this is corrected by a subsequent Registration procedure, if network slice isolation is supported it gets violated, and there may be service interruption for the UE. It is necessary to select an AMF that supports the network slices (S-NSSAI) associated to the UE's PDN connections and allowed by the UE's subscription. This requires information on the UE's subscribed S-NSSAIs, and network slices (S-NSSAI) associated to the UE's PDN connections which the MME does not have.

It is therefore proposed that:

- for each active PDN connection the UE associates an S-NSSAI with the EPS Bearer ID for the default bearer of the PDN connection. The UE then sends to the serving MME a transparent handover container comprising, for each PDN connection, the EPS Bearer ID for the default bearer of the PDN connection (which identifies the PDN connection) and the associated S-NSSAI per each created PDN connection. The UE sends the information to the MME during an Attach procedure, if PDN connections were established in the 5GS, Tracking Area Update procedures, and upon establishment of a PDN connection in the EPS.

- At handover from EPS to a 5GS network, the source MME select an AMF based on current mechanisms and ensuring the selected AMF is capable of performing AMF selection (e.g. based on appropriate DNS configuration). The MME provides the transparent handover container to the AMF selected by the MME. The AMF selected by the MME, together with the NSSF, selects a target AMF and forwards the signalling from the source MME to the target AMF. The target AMF is selected considering the S-NSSAIs associated to PDN connections that are in the transparent handover container. The UE does not get registered in the AMF selected by the MME, but only by the target AMF. The target AMF selects V-SMFs and V-UPFs based on slice mapping information provided by the MME (instead of default V-SMFs / default V-UPFs as in Rel-15).

#### 6.2.2.3 Procedures

#### 6.2.2.4 Impacts on existing entities and interfaces

Impacts on EPC: MME must be enhanced to support the transfer of transparent handover container from UE in EPC Attach and Tracking Area Update procedures. The MME must be enhanced to store the transparent handover container to the UE context and update the container whenever updated by the UE. The MME must be enhanced to support the transfer of transparent handover container in S10 interface to the Target MME or Initial AMF.

Impacts on UE: The UE must be enhanced to include the association of default EPS Bearer ID and S-NSSAI in transparent handover container in EPC Attach and Tracking Area Update request. The UE must send the updated transparent handover container in Tracking Area Update request to MME whenever a new PDN connection has been established, or the old one has been released. The UE must be enhanced to include the association of default EPS Bearer ID and S-NSSAI in Registration Request.

The AMF must be enhanced to support the reception of S-NSSAI and default EPS Bearer ID from MME (connected mode) and from UE (idle-mode). The Initial/Target AMF uses the default EPS Bearer ID to map the S-NSSAI to the PDN Connection(s) received from the MME.

#### 6.2.2.5 Evaluation

The proposed solution supports deployments with and without Decor/eDecor.

The solution requires Rel-16 UE, Rel-16 MME and Rel-16 AMF.

### 6.2.3 Solution #2.3: Inter RAT mobility Slice support

#### 6.2.3.1 Introduction

The solution solves the key issue #2, especially on the below item:

- Selecting an AMF based on the slices associated to the active PDN connections the UE has in the EPC.

- Selecting an appropriate V-SMF based on the slices associated to the active PDN connections the UE has in the EPC.

#### 6.2.3.2 Functional description

**AMF/V-SMF selection during CONNECTED state mobility:**

An interim AMF is selected by MME during handover phase as in Rel-15. The interim AMF/SMF can connect to all possible slices that support interworking with EPS. After handover is completed, the UE initiates the registration procedure. The interim AMF selects the final AMF based on S-NSSAI of established PDN connections. And the AMF is relocated during the registration procedure if it is needed.

The interim AMF gets the S-NSSAI of serving PLMN of established PDN connection either from PGW-C during handover procedure (LBO or non Roaming case), or from UE in registration request (HR case). For home routed roaming case, if the AMF is not provided with S-NSSAI of VPLMN by the UE, based on received S-NSSAI of HPLMN from PGW-C+SMF, the AMF determines the S-NSSAI of VPLMN itself via local mapping information exist or NSSF.

The registration procedure needs to be enhanced to support AMF relocation as well as V-SMF change in CM-CONNECTED state.

**AMF selection during IDLE state mobility:**

In idle mobility, the UE has S-NSSAI and the associated PLMN of established PDN connections sent by the PGW-C+SMF. In local breakout roaming case or non-roaming case, i.e. the associated PLMN is the serving PLMN, the UE can include the S-NSSAI of established PDN connections in RRC message. 5G AN selects correct AMF based on the S-NSSAI of established PDN connections in RRC message.

In case the PDN connection is home routed, i.e. the associated PLMN is the home PLMN, the S-NSSAI provided by PGW-C to UE is S-NSSAI in HPLMN. In this case, UE sends the S-NSSAI in HPLMN to AMF in NAS. The AMF determine the corresponding S-NSSAI in VPLMN, e.g. via local provision mapping information or query from NSSF, and select a final AMF, which may be different from the one selected by 5G AN, based on the S-NSSAI (in VPLMN) of established PDN connections.

**V-SMF selection during IDLE state mobility:**

With N26 case:

The UE includes the S-NSSAI of corresponding PDN connection together with default EBI into registration request. The Context retrieved from MME includes default EBI. Thus, the AMF can correlate the S-NSSAI with corresponding PDN connection.

For home routed roaming case, the UE provides the S-NSSAI of HPLMN to AMF in NAS and the AMF determines the S-NSSAI of VPLMN, e.g. via local provision information or NSSF.

The AMF selects the V-SMF(s) based on the S-NSSAI(s) of the VPLMN associated with the established PDN connection(s).

Without N26 case:

The UE includes HPLMN value of S-NSSAI(s) associated to the PDU Session ID of each established PDN connection(s) in registration request. The AMF determines its corresponding VPLMN value of the S-NSSAI, e.g. via NSSF or local provision information. In Registration Accept message, the AMF includes the VPLMN value of the S-NSSAI(s) associated to PDU Session ID of each established PDU Session(s) in the message. Hence, UE knows VPLMN value of S-NSSAI associated to each established PDU Session, and can include S-NSSAI in PDU Session Establishment Request. The AMF selects V-SMF based on S-NSSAI received in PDU Session Establishment Request.

#### 6.2.3.3 Procedures

##### 6.2.3.3.1 Registration with AMF and V-SMF change during CONNECTED state mobility



Figure 6.2.3.3.1-1: AMF/V-SMF relocation during registration procedure when UE is in CM-CONNECTED state

1. UE sends Registration request to the interim AMF. The UE includes HPLMN value of S-NSSAI(s) associated with established PDN connection(s) and its corresponding default EBI in Registration request. This is for the case that the UE get the S-NSSAI from the HPLMN and not able to map it to the S-NSSAI of VPLMN.

3. A final AMF is selected by interim AMF based on subscribed S-NSSAI(s), S-NSSAI(s) associated with established PDN connection(s) which can be the S-NSSAI of HPLMN, and UE requested NSSAI. The interim AMF may query NSSF or based on the local provision mapping information for Allowed S-NSSAI determination. If the interim AMF is not provided with VPLMN value of S-NSSAI(s) associated with established PDN connection(s) by the UE, the interim AMF provides the HPLMN value of S-NSSAI(s) associated with established PDN connection(s) to NSSF, and NSSF will provide its corresponding VPLMN value to the interim AMF in response.

4. The interim AMF forwards the registration request to final AMF as in step 7a of figure 4.2.2.2.3-1 in clause 4.2.2.2.3 of TS 23.502 [3], with the following enhancement:

An indication is included in the message to indicate that the registration is in CM-CONNECTED state, so that the final AMF will not retrieve UE context based on mapped GUTI in the registration request.

5. TS 23.502 [3] Steps 4 ~ 16 of figure 4.2.2.2.2-1 or step 8~16 of figure 4.2.2.2.2-1, excluding step 10, are performed.

6. The final AMF selects the final V-SMF(s) based on VPLMN value of S-NSSAI(s) associated with the established PDN connection(s).

7. For each established PDU Session, the final AMF determine the related final V-SMF based on the VPLMN value of S-NSSAI. If the selected final V-SMF is different from the interim V-SMF, the final AMF invokes Nsmf\_PDUSession\_CreateSMContext to the selected final V-SMF, including the interim V-SMF ID in the message.

8. The final V-SMF retrieves SM context from interim V-SMF based on V-SMF ID received from AMF.

10~16. Handover the PDU session user plane path to the final V-UPF. After step 12, the uplink path has been switched, and after step 15, the downlink path has been switched. The PGW-U+UPF sends end marker via interim V-SMF after step 15.

Editor's note: The exact procedure how to relocate the V-SMF should be aligned with the conclusions in ETSUN study.

Editor's note: whether the AMF need to be relocated when the UE initiates a new PDU Session that is not using any of the existing S-NSSAI(s) is FFS.

21. The final AMF notifies the interim AMF by invoking Namf\_Communication\_RegistrationCompleteNotify after the sessions have been switched to final V-SMF/V-UPF. The interim AMF can release session in interim V-SMF and V-UPF.

##### 6.2.3.3.2 Registration with AMF and V-SMF change during IDLE state mobility

See the related description in clause 6.2.3.2.

In addition, if the UE does not include the S-NSSAI of corresponding PDN connection together with default EBI into registration request (i.e. Rel-15 UE), the AMF reselects V-SMF based on S-NSSAI received from PGW-C+SMF, and triggers V-SMF change. For home routed roaming case, the AMF first maps the S-NSSAI value of HPLMN received from PGW-C+SMF to S-NSSAI value of VPLMN, and selects V-SMF based on S-NSSAI value of VPLMN.

#### 6.2.3.4 Impacts on existing entities and interfaces

AMF:

- AMF is enhanced to support the AMF reallocation.

- Based on the default EBI and the associated S-NSSAI.

- In the Registration Request message and a new indication to the final AMF for not to retrieve UE context based on mapped GUTI.

- For each PDU Session, at the Registration Accept message, the associated S-NSSAI of VPLMN is returned to UE.

- AMF must be enhanced to support V-SMF relocation procedures.

UE:

- The UE must include the default EBI and the associated S-NSSAI, which can be either the HPLMN value or serving PLMN value, in the Registration Request message.

SMF:

- SMF must be enhanced to support V-SMF relocation procedures.

Editor's note: The exact procedure how to relocate the V-SMF should be aligned with the conclusions in ETSUN study.

#### 6.2.3.5 Evaluation

### 6.2.4 Solution #2.4: Connected mode mobility from EPC to 5GC

#### 6.2.4.1 Introduction

Key issue 2 raises questions on AMF selection and V-SMF selection during the mobility procedure from EPC to 5GC. As there is no assumption that the mechanisms of AMF selection and V-SMF selection for Idle state UE and Connected state UE are same, this solution only considers Connected mode mobility from EPC to 5GC.

#### 6.2.4.2 Functional description

In order to select appropriate AMF and V-SMF based on the information of network slices that the UE is using, this solution makes following assumptions:

- The S-NSSAIs that the UE is using need to be known by the NF that executes the selection.

- Legacy EPC nodes are not required to be enhanced to support S-NSSAI-based AMF or V-SMF selection.

- Current EPC and 5GC interworking procedure should be used as the baseline.

Based on such assumptions, this solution proposes an S-NSSAI based AMF and V-SMF selection mechanism.

In this solution, it is assumed that only combo nodes in EPC are allowed to be enhanced, i.e. PGW-C+SMF and HSS+UDM.

During the PDN connectivity establishment procedure, as described in current specification TS 23.501 [2], the PGW-C+SMF will receive from the UE an ePCO containing PDU session ID, and determines the S-NSSAI corresponding to the PDN connection based on the operator policies, e.g. PGW address and APN. Therefore, the PGW-C+SMF can know the information of the slice the UE is accessing. In order to let the 5GC NFs obtain such information, this solution proposes to store the default EPS Bearer ID and S-NSSAI associated with the PDU Session ID into the HSS+UDM.

When the inter-system handover from EPC to 5GC is performed, during the handover preparation phase, the MME selects AMF as defined in the TS 23.502 [3] (Rel 15). The selected AMF firstly fetches UE subscription data containing pairs of default EPS bearer ID and S-NSSAI associated with the PDU Session ID from the HSS+UDM, and then determines whether it can serve all slices identified by S-NSSAIs fetched from the HSS+UDM. If the selected AMF can not serve all S-NSSAIs, it requests NSSF to select a target AMF/AMF set based on the S-NSSAIs.

After the target AMF is determined, the old selected AMF initiates an AMF relocation procedure as specified in the TS 23.502 [3]. The old selected AMF also provide the target AMF the pair of default EBI and S-NSSAI information. The target AMF can select a correct V-SMF based on S-NSSAI for each PDU session which is anchored in another PLMN.

#### 6.2.4.3 Procedures

##### 6.2.4.3.1 Enhancement to PDN connection establishment



Figure 6.2.4.3.1-1: PDN connection establishment enhancement

For each PDN connection, after the PGW-C+SMF determines the associated S-NSSAI based on operator policies, it registers with the UDM and stores the identity of the PDN connection (default EPS Bearer ID) and the S-NSSAI associated with the PDN PDU Session ID into the HSS+UDM.

The S-NSSAI stored in the HSS+UDM will be used for AMF selection and V-SMF selection.

##### 6.2.4.3.1 Enhancement to handover preparation from EPC to 5GC

The enhancement to the handover procedure is quite similar as the AMF relocation procedure defined in the clause 4.2.2.2.3 in TS 23.502 [3].



Figure 6.2.4.3.1-1: Enhancement for Handover preparation from EPC to 5GC

According to the existing handover procedure from EPC to 5GC, the MME selects an AMF and sends Forward Relocation Request to the AMF. This AMF is called initial AMF in this solution.

In order to determine a suitable serving AMF, the initial AMF uses the step 3 of "Registration with AMF re-allocation" procedure in TS 23.502 [3] to fetch slice interworking related subscription data first, i.e. pairs of EBI and S-NSSAI associated with the PDU Session ID, and then the initial AMF knows the S-NSSAIs that the UE is using. The initial AMF selects the target AMF based on these S-NSSAIs.

The target AMF completes the handover preparation in the target side, and responds the MME with a Forward Relocation Response.

#### 6.2.4.4 Impacts on existing entities and interfaces

No impact on EPC.

No impacts on UE.

The Initial AMF uses the Nudm\_SDM\_Get service operation to retrieve the S-NSSAI associated with the default Bearer ID and the PDU Session ID.

The PGW-C+SMF must register to UDM for each PDN Connection established in EPC. The PGW-C+SMF updates the default EPS Bearer ID and the S-NSSAI associated with the PDU Session ID to the HSS+UDM.

HSS+UDM must be enhanced to support the storage of default EPS Bearer ID and the associated S-NSSAI.

#### 6.2.4.5 Evaluation

Extra step is required in the handover preparation to retrieve the S-NSSAI from the UDM.

The solution requires Rel-16 AMF, Rel-16 PGW-C+SMF, and Rel-16 HSS+UDM.

### 6.2.5 Solution#2.5: Using the NF discovery to find the S-NSSAI.

#### 6.2.5.1 Introduction

This solution addresses the key issue#2: Enabling interworking for slicing between EPC and 5GC, and especially how to select the target AMF and V-SMF based on the S-NSSAI of the ongoing PDN connection in mobility from EPC to 5GC.

#### 6.2.5.2 Functional description

The solution is based on following principles on how to find out the S-NSSAI for the ongoing PDN connections:

As specified in Rel-15, when the UE moves from EPC to 5GC, the AMF uses the Nnrf\_NFDiscovery service operation and PGW-C address (FQDN) as an input parameter to discover the corresponding SMF address (FQDN or IP address).

In this solution, the NRF is used to map the PGW-C address to SMF address and corresponding S-NSSAI. For example, the NF discovery service (Nnrf\_NFDiscovery) is enhanced to include also the S-NSSAI that is served by the SMF. The NRF returns the S-NSSAI of the SMF, along the SMF address, when the AMF discovers the SMF via Nnrf\_NFDiscovery service operation. As the Nnrf\_NFDiscovery service operation is generic, it could return the S-NSSAI also in general SMF discovery not related to EPC interworking. In this case, the S-NSSAI is not used.

As it may be the SMF serves multiple S-NSSAIs, the mapping of S-NSSAI may be based on following methods:

Option#A: The PGW-C may be configured with TEID ranges, one TEID range per S-NSSAI served by the SMF. The NRF is configured with the mapping from PGW-C address and TEID range to SMF address and S-NSSAI. The AMF uses the PGW-C address and TEID received from MME as an input to find out the corresponding SMF address and S-NSSAI. Nnrf\_NFDiscovery service operation is enhanced to include also the PGW-C TEID as an input parameter for SMF discovery.

Option#B: The different PGW-U+UPF IP address might be associated with different S-NSSAI. The NRF is configured with the mapping from PGW-U+UPF IP address to the S-NSSAI, the mapping information between PGW-U+UPF IP address and the corresponding S-NSSAI shall be provided to the NRF by the UPF or OA&M. The PGW-C+SMF selects PGW-U+UPF based on S-NSSAI associated with a PDN connection, and the AMF uses the PGW-U+UPF IP address received from MME as an input parameter to find out the corresponding S-NSSAI.

Rest of the procedures follow the principles in Solutions 2.1 and 2.2 on how to select the Target AMF and V-SMF:

- In connected mode, the MME selects the AMF as currently specified in Rel-15. This AMF then acts as an Initial AMF and uses the above procedure to find out the S-NSSAI for each PDN Connection. Based on the list of S-NSSAIs, the Initial AMF can select the Target AMF, using the NSSF service as in Rel-15. The Initial AMF forwards the list of PDN Connections associated with the S-NSSAI and SMF address to the Target AMF. In home-routed roaming case, the Target AMF selects the V-SMF based on the S-NSSAI received from the Initial AMF.

- In idle mode, in home-routed roaming case, once the Target AMF has used the above procedure to find out the S-NSSAI for each PDN connection it received from the MME, the Target AMF selects the V-SMF based on the S-NSSAI.

It should be noted, that although the above description uses the NRF for SMF discovery, depending on the conclusions in FS\_eSBA, also the common Service Framework may be used for service instance discovery.

#### 6.2.5.3 Procedures

##### 6.2.5.3.1 EPS to 5GS handover using N26 interface



Figure-6.2.5.3.1-1: EPS to 5GS handover using N26 interface

1. Step 1 to step 3 are the same as in Rel-15 EPS to 5GS handover using N26 interface. The AMF selected by the MME becomes an Initial AMF in this solution.

4. The Initial AMF uses the PGW-C address and TEID in PDN Connections received from the MME as an input parameter to NRF (e.g. Nnrf\_NFDiscovery) service to discover the SMF address. The NRF returns also the S-NSSAI for the SMF for each PDN Connection.

If the Initial AMF cannot serve all the S-NSSAI(s), the Initial AMF invokes the Nnssf\_NSSelection\_Get service operation from the NSSF to select the Target AMF.

In home-routed roaming case, if the VPLMN and HPLMN have an SLA to support non-standard S-NSSAI values in the VPLMN, the Initial AMF uses the NSSF of the VPLMN to map the S-NSSAI values to the respective S-NSSAI values to be used in the VPLMN.

5. In case the Target AMF is different to Initial AMF, the Initial AMF sends Namf\_Communication\_CreateUEContext service operation (Target 5GAN Node ID, Source to Target Transparent Container, EPS MM Context, EPS Bearer Context(s), , list of S-NSSAI(s) and SMF addresses received in step 4) message to the Target AMF. In home-routed roaming case, the Target AMF selects the V-SMF based on the S-NSSAI associated with the PDN Connection.

Steps 6-27 are the same as in Rel-15 EPS to 5GS handover procedure using N26 interface in clause 4.11.1.2.2 of TS 23.502 [3].

#### 6.2.5.4 Impacts on existing entities and interfaces

No impact on EPC.

No impacts on UE.

The Initial AMF uses the NRF, e.g. Nnrf\_NFDiscovery service to map the PGW-C address and TEID to SMF address and the S-NSSAI.

For example, the Nnrf\_NFDiscovery service operation is enhanced to include also the S-NSSAI that is served by the SMF. The NRF returns the S-NSSAI of the SMF, along the SMF address, when the AMF discovers the SMF via Nnrf\_NFDiscovery service operation.

If the SMF serves multiple S-NSSAIs, then the PGW-C must be configured with TEID ranges, one TEID range per S-NSSAI served by the SMF. In this case, the NRF is configured with the association from PGW-C address and TEID range to SMF address and S-NSSAI.

Option#B: The different PGW-U+UPF IP address might be associated with different S-NSSAI, the AMF need to extract the IP address from the EPS bearer context.

#### 6.2.5.5 Evaluation

The solution requires Rel-16 AMF and Rel-16 PGW-C+SMF.

## 6.3 Solutions for KI#3

### 6.3.1 Solution #3.1: Slice Specific Authentication and Authorization using non 3GPP credentials based on secondary authentication

#### 6.3.1.1 Introduction

The solution addresses key issue#3.

The 5GS system has introduced secondary authentication at the establishment of a PDU session. Specifically, during the establishment of a PDU session, Release 15 has defined that a DN-specific identity (TS 33.501 [6]) of a UE may be authenticated/authorized by the DN, via a DN-AAA server that may belong to the 5GC or to the DN. This solution assumes that the secondary authentication is performed between the 5GC and the external DN-AAA server with the support the NEF.

The procedure allows both the authentication triggering by the UE (with the UE providing authentication information during the Establishment of the PDU Session), or by the SMF that can reject the PDU Session Establishment if the UE has not provided authentication/authorization information. At any time, a DN-AAA server may revoke the authorization for a PDU Session or update DN authorization data for a PDU Session. According to the request from DN-AAA server, the SMF may release the PDU Session.

Such secondary authentication takes place in 5GS in addition to (and after) the 5GC access authentication handled by AMF.

In this solution it is assumed that connectivity to a slice implies the establishment of at least one PDU session.

#### 6.3.1.2 Functional description

It is proposed to re-use the secondary authentication introduced in Release 15 to enable slice authentication.

Specifically, the secondary authentication is used and enhanced as follows:

- If access to a specific network slice (i.e. a specific S-NSSAI) needs to be authenticated based on non 3GPP network slice credentials, the slice provider/customer provisions such network slice credentials (slice-specific User ID and security credentials) to the UE with mechanisms out of scope of this solution.

- If access to a specific network slice (i.e. a specific S-NSSAI) needs to be authenticated based on non 3GPP network slice credentials, at the establishment of the first PDU session corresponding to the S-NSSAI that requires authentication, the UE provides the non 3GPP credentials required for the authentication. If the UE does not provide such credentials and the SMF determines that the PDU session corresponding to the S-NSSAI needs to be authenticated, the SMF retrieves the credentials from the UE with an EAP Identity Request as defined in TS 33.501 [6].

- The SMF authenticates just the first PDU session established corresponding to an S-NSSA with a Slice-AAA function which, similarly to the DN-AAA for UE secondary authentication, may be in the 5GC network or external.

- Ths SMF may authenticate all the PDU sessions corresponding to the S-NSSAI, depending on network policies.

- When the SMF performs the authentication for a PDU session establishment corresponding to an S-NSSAI, the GPSI itself is used as external UE identifier and is provided to the Slice-AAA. This can be achieved by allocating a GPSI to any UE for which, based on subscription information, UE secondary authentication is required for one of the subscribed S/NSSAI(s)/DNN(s).

- During the UE secondary authentication, the authentication SMF (H-SMF or V-SMF for LBO) provides the GPSI, S-NSSAI, and optionally PDU Session ID to the Slice-AAA in addition to the information currently provided. This enable an external Slice-AAA to create a context related to the authentication of a slice that may have one or more PDU sessions for triggering re-authentication and de-authorization.

- When secondary authentication is performed successfully, the Slice-AAA subscribes with the NEF (with GPSI, S-NSSAI, and PDU Session ID) for notification of the change of SMF the SMF should contact to enable re-authentication. This is needed in order to ensure that the Slice-AAA contacts the correct SMF considering that a slice may have multiple PDU sessions which may be activated and released while the UE is authenticated for a slice (i.e. the PDU session that triggered the authentication may be released, and the Slice-AAA should be able to reach a different SMF for a PDU session corresponding to the S-NSSAI to trigger re-authentication).

- for Rel. 15 secondary authentication, the information on a successful secondary authentication/authorization between a UE and an SMF may be saved in SMF and/or UDM. In this solution, it is assumed that the information on successful authentication of a slice is stored in the UDM, and contains both the information on a previous successful authentication for a slice (S-NSSAI) and for a DN.

- Upon establishment of a PDU session corresponding to an S-NSSAI, the SMF checks whether the UE has already been authenticated and/or authorized for the same S-NSSAI by an SMF, in addition of checking if the UE has already been authenticated and/or authorized for the same DN.

- if DNN authentication/authorization is required in addition to slice authentication, the secondary authentication is executed twice by the SMF within the same PDU session establishment procedure, based on the network slice credentials first, and based on the DNN-specific secondary authentication information. The SMF shall not authorize the PDU session establishment unless both authentication/and authorization succeed. If both authentications are needed, the UE in addition to the current SM PDU DN request container provides also the network slice credentials.

- The slice-AAA may be part of the 5GC or may belong to the DN of the service provider offering the slice services.

- De-authorization of a slice by the slice-AAA will trigger the PDU session release of all the PDU sessions corresponding to the slice.

- When the Slice-AAA indicates revocation of a slice authorization, the Slice-AAA sends an indication to the NEF associated to the received GPSI, which in turn informs the SMF(s) serving the slice, and the PDU session(s) corresponding to that slice, that the PDU session(s) needs to be released.

- A failed slice authentication or a slice de-authentication triggers the SMF to inform the AMF that the S-NSSAI corresponding to one or more PDU sessions is not authorized. The AMF decides based on local policies whether to update the Allow NSSAI and indicate to the UE that the S-NSSAI is rejected.

#### 6.3.1.3 Procedures

##### 6.3.1.3.1 Slice authentication at first PDU session establishment for the S-NSSAI



Figure 4.3.2.3-1: PDU Session Establishment authentication/authorization by a DN-AAA server

1. The UE registers with the network. Primary authentication is performed during the registration procedure.

2. The UE triggers PDU session establishment for an S-NSSAI (or for none and one is selected by the network).

3. The SMF determines that slice authentication is required and triggers secondary UE authentication for the S-NSSAI. Upon successful authentication, the SMF stores in the UDM for the S-NSSAI the status of the slice authentication and the SMF ID as the slice authenticator.

4. [Optional] If DN authentication is also needed, the UE secondary authentication for the DNN is performed upon successful slice authentication.

5. The Slice AAA server subscribes for event notification via the NEF to be informed of a change of SMF, in order to enable the AAA server to reach the correct entity for re-authentication and de-authorization.

6. The UE may establish an additional PDU session for the same S-NSSAI.

7. Since the SMF for this PDU session may be different from the SMF of previous PDU sessions for the same S-NSSAI, the SMF checks the slice authentication status in the UDM. If no slice authentication is required, the SMF ID is stored in the UDM as serving the S-NSSAI in addition to other SMF IDs serving the same S-NSSAI.

8. [Optional] If slice authentication or DN authentication is needed, the SMF triggers the secondary authentication.

#### 6.3.1.4 Impacts on existing entities and interfaces

Impacted functions:

- UE:

- support of S-NSSAI-based secondary authentication in addition/parallel to secondary authentication for a DN.

- provisioning of multiple SM PDU containers at PDU session establishment to support both slice authentication and DNN authentication, when needed.

- AMF: if slice authentication fails, SMF may inform AMF that the authentication for the S-NSSAI failed and the AMF may, based on local policies, remove the S-NSSAI from the Allowed NSSAI.

- SMF: support slice authentication in addition to secondary authentication for DN. SMF to verify slice authentication status in UDM to avoid unnecessarily re-authenticating a slice if authentication took place at a previous PDU session establishment.

- AAA server: support of interaction with NEF for subscription to slice and DN related events (e.g. change of PSA) in order to allow the AA server to be up to date with the PSA where to send re-authentication requests or de-authorization requests.

#### 6.3.1.5 Evaluation

The solution does not require a slice to which the UE may never connect (i.e. establish connectivity to via a PDU session) to be authorized/authenticated until the UE requires the connectivity.

The solution does not impact the registration procedure in terms of MM timers, e.g. in case of failed authentications/retries due to EAP failure.

The solution re-uses existing NAS signalling. The solution re-uses the existing architecture and existing interfaces.

### 6.3.2 Solution #3.2: Solution to KI#3 on Slice Specific Authentication and Authorization using non 3GPP credentials

#### 6.3.2.1 Introduction

The scenario considered for the solution is that there is an Authentication, Authorisation and Accounting Server (AAA-S) deployed in a PLMN or in a third-party network that allows Slice-Specific secondary authentication and authorisation of users who have the right of access to certain slices. The AAA Server handles the User IDs and credentials for a Secondary authentication at a non 3GPP User ID level, after the UE has been authenticated by the 3GPP system for PLMN access. A AAA proxy function (AAA-F) is also defined to provide a single point of interaction from the PLMN with the third parties. The AAA-F can be a standalone or its services could be supported by other NFs (i.e. AUSF or NEF).

#### 6.3.2.2 Functional description

If a UE subscription includes an S-NSSAI of a slice that requires Slice-Specific Secondary Authentication and Authorisation, the UDM stores a flag indicating that this step is needed for the S-NSSAI. The IP address or FQDN/realm of the AAA Server that would perform the authentication and authorisation may be stored in the AAA-F per S-NSSAI. Alternately, if the User ID in the third party is defined as a NAI (see RFC 4282 [8]), i.e. the User ID is in the form user@domain, the IP Address is not needed in AAA-F and the correct AAA-S is derived at AAA-F by resolving the domain part of the NAI.

When a UE performs a registration request which includes S-NSSAI(s) in the Requested NSSAI which needs Slice-Specific Secondary Authentication and Authorisation (as detected based on the subscription information, as outlined above), the AMF executes on top of any required PLMN specific Authentication and Authorization step, an Authentication and Authorization step that is run with the UE and involves the AAA Server for the specific S-NSSAI(s). In the worst case, one such step is needed for each S-NSSAI. In general, there can be a mix of slices requiring Slice-Specific Secondary Authentication and Authorisation, and slices that do not require this.

For the S-NSSAIs which require Slice-Specific Secondary Authentication and Authorisation, the UE needs to be provided with the necessary credentials and algorithms necessary to authenticate itself with the AAA Server. This aspect is left out of the scope of this solution.

In addition, the UE includes a security capability indicating its support for Slice-Specific Secondary Authentication and Authorisation in the registration request facilitating the AMF to determine whether it can execute Slice-Specific Secondary Authentication and Authorisation or not. If the security capability is not included in the registration request (e.g. in case of Rel-15 UEs), the AMF shall not allow UE to access to any Network Slice for which Slice-specific Secondary authentication is required.

The proposal assumes that the assumed transport protocol is EAP and is summarized by the following figure:



Figure 6.3.2.2-1: Registration with Slice-Specific Secondary Authentication and Authorisation for Slice Access (high level concept)

Step 4 is conditional to both the UE security capability and the S-NSSAI subscription data, checked at step 3, including a flag that indicates Slice-Specific Secondary Authentication and Authorisation is needed. If this is needed and UE supports it, this step is executed. The start of this step suspends the current Registration procedure timer. This timer is restarted when all the pending EAP procedure for slices that are subject to Slice-Specific Secondary Authentication are completed.

Editor's note: This approach needs to be checked whether it is acceptable by CT1 and based on the feedback changes to the solution may be done in normative phase to align with the preferred way to handle NAS and EAP timers interaction.

Once it is executed, status can be kept by the AMF in the UE context, so extra authentication is not repeated at subsequent registrations until a re-authentication is required by the AAA Server or the PLMN, based on policy. If this is needed but UE does not support it, this step is skipped and the AMF shall not include an NSSAI to the Allowed NSSAI in step 5.

Explicit challenges used to re-authenticate the UE, or a request to revoke the authorization of the UE may come from the AAA Server and the AAA-F routes to the current serving AMF based on a binding between the User ID and the GPSI of the UE established when the UE is authorised. The AAA Server keeps a coupling between the User ID of the UE and the UE GPSI so it can pinpoint the UE for the User ID when it needs to be re-authenticated or its authorization status changes and needs to be revoked.

Once step 4 is executed successfully, and the registration accepted, the UE, after optional NSSF interaction (not explicitly shown above), is provided an allowed NSSAI including the slices that were successfully authorised. SM procedures can take place in the authorised slices for the UE.

It the UE fails Slice-Specific Secondary Authentication, and this results in the UE not having any Allowed NSSAI, the UE may be Accepted, as per rel-15 behaviour in the case of a misconfigured UE, with no Allowed NSSAI and, depending on operator policy, remain registered with operator-specific service restriction in the same AMF or it may be re-allocated to a specific AMF which applies specific service restrictions. The AMF then may e.g. deregister the UE after a certain time configurable by the operator.

If the UE fails Slice-Specific Secondary Authentication for a specific slice, how the UE obtains fresh/valid credentials from third parties is outside the scope of 3GPP.

NOTE: A UE may gain access to a slice that needs Slice-Specific Secondary Authentication and Authorisation and not trigger any PDU session establishment (e.g. SMS only device) or require a PDU session only after SMS trigger after is assigned an Allowed NSSAI and is successfully registered.

#### 6.3.2.3 Procedures

##### 6.3.2.3.1 Secondary Authentication and Authorization During Registration

During the registration procedure, before step 15 occurs, in figure 6.3.2.3.1-1, the AMF knows whether some S-NSSAIs require Slice-Specific Secondary Authentication and Authorisation based on information from the UDM.



Figure 6.3.2.3.1-1: TS 23.502 [3] Figure 4.2.2.2.2-1: Registration procedure

If the AMF detects the need to execute the Slice-Specific Secondary Authentication and Authorisation, the steps marked as "2" in Figure 6.3.2.3.1-2 are executed. In the event the Allowed NSSAI needs to be computed and potential new AMF determined by a NSSF, then these Authentication and Authorization steps are executed upfront so that the NSSF receives from the AMF only the authorized by Slice-Specific Secondary Authentication and Authorisation and subscribed-to slices.



Figure 6.3.2.3.1-2: Registration with third party Authentication and Authorisation

1. Steps 1-14 of the Registration procedure. Steps 2 are not executed if no S-NSSAI in the UE subscription is requiring Slice-Specific Secondary Authentication and Authorization or the UE does not have a security capability.

2a. [Conditional] The AMF requests the UE User ID for the S-NSSAI. The NAS message includes the S-NSSAI value so the right Network Slice authentication is executed and so the related User ID and credentials are used by the UE. The AMF may start in parallel several such authentication and Authorisations procedures if more than one S-NSSAI is subject to Secondary Slice-Specific Authentication and Authorisation. This step suspends the current Registration procedure timer, which is resumed when all the pending EAP interactions for Slice-Specific Secondary Authentication complete.

Editor's note: This approach needs to be checked whether it is acceptable by CT1 and based on the feedback changes to the solution may be done in normative phase to align with the preferred way to handle NAS and EAP timers interaction.

2b. [Conditional] The UE provides the User ID for the S-NSSAI alongside the S-NSSAI.

2c-2d. [Conditional] The AMF contacts the AAA Server via AAA-F. It includes also the S-NSSAI and the UE GPSI for binding of Network Slice User ID to the UE GPSI (so the AAA Server is allowed to contact the UE for further reauthentication based on its policy, or to revoke the UE authorisation, or to optimise future Authorisations based on the AAA server trusting the GPSI presented by the PLMN. If the AAA Server trusts the GPSI provided, by the PLMN, and it had if it had a previous mapping of the GPSI to the User ID, the AAA Server may go directly to step 2k.

2e-2j. [Conditional] The UE EAP based authentication happens. The number of steps is indicative, more may occur.

2k-2m. [Conditional] The EAP authentication completes successfully. Optionally, in steps 2k and 2l the AAA Server and the AAA-F convey to the AMF a list of S-NSSAIs the successful Authentication and Authorisation applies to, so the AMF can avoid executing multiple Authentications and Authorisations towards the same AAA Server for the same User ID for the S-NSSAIs in the list. This option should not be used if the AAA-s intends to collect accounting information for S-NSSAI usage by the UE.

3. The AMF stores in the UE context the outcome of steps 2 and if a list of S-NSSAIs was provided sharing the same User ID, then the AMF stores that also. The AMF can now determine, assisted by NSSF if needed, the Allowed NSSAI and this may trigger selection of another AMF.

4. The registration completes, and eventually a Registration Accept is sent to the UE including the Allowed NSSAI and the GUTI allocated by the target AMF if the AMF is relocated in step 3.

##### 6.3.2.3.2 Secondary Re-Authentication and Re-Authorization after Registration

The AAA-S may, based on application layer event, prompt the network to Re-authenticate and Re-authorize the user by sending a request to the AAA-F. For example, the AAA-S may initiate the request based on security policies, in order to revoke the User's authorization to access the slice.

In response to the request from the AAA-S, the AAA-F will initiate re-authentication and re-authorization by sending a request to the AMF. Upon receiving the request, the AMF initiates step 2 of Figure 6.3.2.3.1-2. If the purpose of the request is to revoke the User's authorization to access the slice, then the UE's Allowed NSSAI is updated accordingly via a Configuration Update per clause 4.2.4.2 of TS 23.502 [3].

#### 6.3.2.4 Impacts on existing entities and interfaces

Impacted functions:

UE: to be able to participate in Slice-Specific Secondary Authentication and Authorisation per S-NSSAI. Indicating UE's security capability to support the Slice-Specific Secondary Authentication and Authorisation.

AMF: triggering of Secondary Authentication and Authorisation per slice and ability to store outcome and any list of S-NSSAIs sharing the same authorised User ID. The Change of AMF happens to match the allowed NSSAI may happen after evaluation of the Secondary Authorisation Status. This happens after the UE is detected to be authorised for 3GPP access in the source AMF. The AMF takes into account of UE's security capability to trigger the Slice-Specific Secondary Authentication and Authorisation towards the UE.

UDM: Slice-Specific Support of Secondary Authentication info.

#### 6.3.2.5 Evaluation

This solution describes slice-based authentication/authorisation when UE requests registration to the associated S-NSSAI (e.g. during Registration procedure). The network (e.g. AMF) determines if the requested S-NSSAI(s) are subject to Slice-Specific Secondary Authentication and Authorisation. It allows for upfront determination whether the requested S-NSSAI is allowed to be used, and thus, the network grants Allowed NSSAI to the UE before any PDU session is established.

Considering that a Serving AMF is part of the used network slices (i.e. slices part of the Allowed NSSAI), this solution allows to selection a serving AMF after the successful slice-based authentication/authorisation.

The approach of nesting EAP interactions for Slice-Specific Secondary Authentication in the registration procedure NAS procedure needs to be checked whether it is acceptable by CT1 for the aspect of the interaction of EAP and NAS timers as described in the proposed solution. Based on the feedback, changes to the solution may be done in normative phase to align with the preferred way to handle NAS and EAP timers interaction.

### 6.3.3 Solution #3.3: Solution for configuration of network slice authentication

#### 6.3.3.1 Introduction

This solution applies to Key Issue 3 (Access to specific Network Slices authorized and authenticated through additional User Identifiers).

It is assumed that particular application(s) or service(s) in the UE has been configured with User ID and security credentials for slice authentication and authorization. Also, the network has been configured that a particular Network Slices(s) require authentication and authorization.

#### 6.3.3.2 Functional description

The main feature of this solution is the dynamic configuration for Network Slice authentication and authorisation in the network. In order to allow dynamic configuration update, the network may expose a service API (e.g. via North Bound APIs or via N33 interface) which supports provisioning of Network Slice authentication required indication from a service provider application function (SP-AF, similar to SCS/AS from TS 23.682 [7]).

Editor's note: It is FFS whether the configuration for Network Slice authentication in the network is performed per service/SP-AF (meaning per S-NSSAI), or per UE, or both.

The UE usually stores the User ID and the security information (e.g. security credentials) at the application layer (e.g. in a particular application). The application should register with the NAS layer (or EAP client) in order to bind the User ID with the particular S-NSSAI.

#### 6.3.3.3 Procedures

#### 6.3.3.4 Impacts on existing entities and interfaces

#### 6.3.3.5 Evaluation

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

# 7 Evaluation

## 7.1 Evaluations Criteria for KI#1: Mutually Exclusive Access to Network Slices

The following set of evaluation criteria are used to evaluate the proposed solutions for KI#1 to support UE for mutually exclusive accessing to network slices:

1) Comply to the definition of Mutually Exclusive Access to Network Slices as described in clause 3.1.

2) Comply to the working assumptions and requirements as described in clause 4.

3) Address all the objectives of the KI#1 as described in clause 5.1.

4) Impact to the UE, the serving PLMN, the home PLMN, e.g. AMF, NSSF, UDM, SMF, PCF in term of signalling interfaces, control flows and internal logic etc. including changes to the semantics of existing services/parameters.

5) Impact to (R)AN.

## 7.2 Evaluations for KI#2: Enabling interworking for slicing between EPC and 5GC

There are 5 solutions (Solutions 2.1 – 2.5) for Key Issue #2 (Enabling interworking for slicing between EPC and 5GC).

Table 7.2-1: Key impacts of the solutions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Solution 2.1 | Solution 2.2 | Solution 2.3 | Solution 2.4 | Solution 2.5 |
| UE impact | Idle:  N/A.  Connected:  No impact. | Idle:  Yes (default EBI in registration request)  Connected:  Yes  (send S-NSSAI to MME as container) | Idle:  Yes (default EBI in registration request)  Connected:  No impact | Idle:  N/A.  Connected:  No impact | Idle:  No impact.  Connected:  No impact |
| EPC impact | Idle:  N/A.  Connected:  No impact. | Idle:  No impact.  Connected:  Yes  (UE send S-NSSAI to MME, and from MME to AMF) | Idle:  No impact.  Connected:  No impact | Idle:  N/A.  Connected:  No impact. | Idle:  No impact.  Connected:  No impact. |
| PGW-C+SMF impact | Idle:  N/A.  Connected:  No impact. | Idle:  No impact  Connected:  No impact | Idle:  No impact.  Connected:  No impact | Idle:  N/A.  Connected:  Yes  (S-NSSAI storing to UDM) | Idle:  No impact.  Connected:  Yes (allocated TEID-C based on S-NSSAI) |
| V-SMF  impact | Idle:  N/A.  Connected:  No impact. | Idle:  No impact.  Connected:  No impact. | Idle:  No impact.  Connected:  Yes  (V-SMF relocation, depending on ETSUN conclusion). | Idle:  N/A.  Connected:  No impact. | Idle:  No impact.  Connected:  No impact. |
| AMF impact | Idle:  N/A.  Connected:  Yes (retrieve S-NSSAI from PGW-C, AMF selection and redirection during preparation phase) | Idle:  Yes (receive default EBI from UE)  Connected:  Yes (AMF selection and redirection during preparation phase, also impact N26) | Idle:  Yes (receive default EBI from UE)  Connected:  Yes (reselect and redirect AMF during registration procedure after handover) | Idle:  N/A  Connected:  Yes (retrieve S-NSSAI from UDM, AMF selection and redirection during preparation phase) | Idle:  No impact.  Connected:  Yes (retrieve S-NSSAI from NRF, and AMF selection/redirection during preparation phase) |
| UDM impact | Idle:  N/A  Connected:  No impact | Idle:  No impact.  Connected:  No impact | Idle:  No impact.  Connected:  No impact | Idle:  N/A  Connected:  Yes  (S-NSSAI storing to UDM) | Idle:  No impact.  Connected:  No impact |
| NRF impact | Idle:  N/A.  Connected:  No impact. | Idle:  No impact  Connected:  No impact. | Idle:  No impact  Connected:  No impact. | Idle:  N/A.  Connected:  No impact. | Idle:  Yes, (the PGW-C+SMF TEID or UPF plane information need be stored)  Connected:  (the PGW-C+SMF TEID or UPF plane information need be stored |
| Extra delay in handover preparation | Yes  (S-NSSAI query from SMF, AMF reselection/redirection) | Yes (AMF reselection and redirection) | No impact  (since, UE is moved to final AMF after the handover) | Yes  (UDM query, AMF reselection/redirection) | Yes (AMF reselection and redirection) |
| Relocation after handover | no | no | Yes(first select default AMF, then it may be reallocated to the final dedicated AMF ) | no | No |
| NOTE: The "Idle" in the table means the Idle state mobility. The "Connected" in the table means the Connected state mobility. | | | | | |

None of the listed solutions avoids the need for default 5GS default NF resources while complying to assumptions for the key issue. The solution 2.1 complies with the assumptions and it has limited impacts, but the solution adds some delay to the HO procedure and while it avoids default V-SMF resources it does not avoid default AMF resources.

# 8 Conclusions

## 8.1 Conclusions for key issue #1 - Mutually exclusive access to Network Slices

Editor's note: For the Key Issue#1, Mutually exclusive access to Network Slices, the conclusions of the study and the resulting normative specifications should describe whether and how the following aspects are covered:

- Whether the standard support the possibility for a Network Slice (S-NSSAI) to be associated to more than one group of Network Slices for which the access to the group of Network Slices are Mutually Exclusive from each other.

- Whether it is possible to deploy an AMF Set which supports Network Slices that are mutually exclusive from each other.

Editor's note: START of INTERIM Table for evaluation.

|  |  |  |
| --- | --- | --- |
| Key attributes | Approach 1 (Soln 3,4,7) | Approach 2+3 (Soln 2+5) |
| Handling of UE requesting incompatible slices | New cause code is needed for rel-16 to signal that some S-NSSAIs are rejected due to incompatibility | The AMF uses existing rel-15 procedures. |
| How is the UE aware of compatibility among S-NSSAIs so it forms a correct Requested NSSAI from the outset. | The CN configures the UE with information that the UE uses to assess whether a S-NSSAI is compatible with other S-NSSAIs on the configured NSSAI.  The UE shall have the same per S-NSSAI compatibility information as the CN, so it can locally (e.g. by local MMI interaction outside the scope of 3GPP) form a compatible and acceptable by the user set of requested S-NSSAIs before it is sent to the network. | The UE is preconfigured with method outside the scope of 3GPP if needed. Otherwise, can sort S-NSSAIs in priority order. |
| How does the Serving PLMN understand the requested S-NSSAIs are compatible | Identify compatibility as a subscription attribute of the S-NSSAI so roaming partners and a PLMN can define which S-NSSAIs are compatible and map these to the Allowed NSSAI provided by NSSF to AMF or by an AMF, even if the AMF supports more S-NSSAIs the UE also subscribes to. In other words, the incompatibility among slices should not impose AMF Set deployment constraints. | AMF sets are deployed to match each and every compatibility groups. |
| Compatibility between UE and network | The UE signals to the network whether it support Mutually incompatible slices handling.  If the UE does not support incompatible slices handling the UE is configured only with compatible Slices.  The subscription information shall include a basic set of compatible Network Slices S-NSSAIs to be used if the UE the subscriber uses does not signal support of mutually incompatible slices. | It is assuming using rel-15 compliant UE and Rel-15 compliant network |
| Support in roaming to PLMNs that are not upgraded to support handling of incompatible slices | The subscription information sent to PLMNs of roaming partners which do not support incompatible slices handling shall only contain mutually compatible Network Slices S-NSSAIs. | As per Rel-15 The deployment of the VPLMN has to match requirements from HPLMN as per an SLA (i.e. the VPLMN deploys AMF Sets that satisfy the SLA for compatibility Groups of the inbound roamers) |

Editor's note: END of INTERIM Table for evaluation.

### 8.1.1 Enhancements for change of a set of Network Slices

It is recommended to, during normative phase, address the issue of how the UE performs a change of S-NSSAIs in the Requested NSSAI e.g. whether the UE does it always from CM-IDLE or also from CM-CONNECTED.

## 8.2 Conclusions for key issue #2 - Enabling interworking for slicing between EPC and 5GC

Connected Mode:

- The solution 2.1 is recommended as basis for normative specifications.

NOTE: It is assumed that ETSUN will develop mechanisms to allow re-selection of V-SMFs which can be re-used for re-selecting a V-SMF dedicated to a Network Slice.

Idle Mode:

‐ To support Rel-15 UE, the AMF may reselect a V-SMF based on S-NSSAI received from PGW-C+SMF. For the V-SMF reallocation, the same mechanism defined at the ETSUN can be reused.

## 8.3 Conclusions for key issue #3 - Access to specific Network Slices authorized and authenticated through additional User Identifiers

For KI#3 it is concluded that Solution in clause 6.3.2 shall be the basis of normative work.

Editor's note: Solution 6.3.2 has an open issue that needs resolution in normative phase with CT WG1 interactions. Base on the outcome of these interactions it will be possible to update the procedure, but the guiding principle is that this is based on AMF-UE interaction with no SMF interaction.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2018-04 | SA2#127 | S2-183922 | - | - | - | TR skeleton (approved in S2-183922) | 0.0.0 |
| 2018-04 | SA2#127 | S2-183921  S2-183923  S2-184594 | - | - | - | S2-183921  S2-183923  S2-184594 | 0.1.0 |
| 2018-06 | SA2#127bis | S2-186275  S2-186276 |  |  |  | S2-186275  S2-186276 | 0.2.0 |
| 2018-07 | SA2#128 | S2-186450  S2-187247  S2-187248  S2-187249  S2-187288  S2-187251 |  |  |  | S2-186450  S2-187247  S2-187248  S2-187249  S2-187288  S2-187251 | 0.3.0 |
| 2018-07 | SA2#128 | S2-187177  S2-187178  S2-187179  S2-187180 |  |  |  | S2-187177  S2-187178  S2-187179  S2-187180 | 0.4.0 |
| 2018-08 | SA2#128bis | S2-188410  S2-188471  S2-188472  S2-188486  S2-188414  S2-188485  S2-189004  S2-188484  S2-188222  S2-188483  S2-188317  S2-189056 |  |  |  | S2-188410  S2-188471  S2-188472  S2-188486  S2-188414  S2-188485  S2-189004  S2-188484  S2-188222  S2-188483  S2-188317  S2-189056 | 0.5.0 |
| 2018-10 | SA2#129 | S2-1810324  S2-1810724  S2-1811059  S2-1811060  S2-1811168  S2-1811169  S2-1811170  S2-1811171  S2-1811199  S2-1811200  S2-1811205  S2-1811206  S2-1811445  S2-1811598  S2-1811599  S2-1811600 |  |  |  | S2-1810324  S2-1810724  S2-1811059  S2-1811060  S2-1811168  S2-1811169  S2-1811170  S2-1811171  S2-1811199  S2-1811200  S2-1811205  S2-1811206  S2-1811445  S2-1811598  S2-1811599  S2-1811600 | 0.6.0 |
| 2018-12 | SA2#129bis | S2-1812153  S2-1812819  S2-1813209  S2-1813210  S2-1813354  S2-1813356  S2-1813360  S2-1813380 |  |  |  | S2-1812153  S2-1812819  S2-1813209  S2-1813210  S2-1813354  S2-1813356  S2-1813360  S2-1813380 | 0.7.0 |
| 2018-12 | SP#82 | SP-181103 | - | - | - | MCC editorial update for presentation to TSG SA#82 | 1.0.0 |
| 2018-12 | SP#82 | - | - | - | - | MCC editorial update for publication after approval at TSG SA#82 (Release 16) | 16.0.0 |