|  |
| --- |
| 3GPP TR 33.874 V0.3.0 (2021-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on enhanced security for Network Slicing Phase 2;(Release 17) |
|   |
| *5G-logo_175px* | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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.© 2021, 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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 3

Introduction 4

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 6

3.3 Abbreviations 6

4 Architectural and security assumptions 6

5 Key issues 6

5.1 Key Issue #1: privacy issue on broadcasting slice information 6

5.1.1 Key issue details 6

5.1.2 Security threats 6

5.1.3 Potential security requirements 7

5.2 Key Issue 2: DoS to NSAC procedure 7

5.2.1 Key issue details 7

5.2.2 Security threats 7

5.2.3 Potential security requirements 8

5.3 Key Issue #3: AF authentication and authorization 8

5.3.1 Key issue details 8

5.3.2 Security threats 8

5.3.3 Potential security requirements 8

6 Solutions 8

6.1 Solution #1: authentication and authorization for a third-party AF or an AF deployed within 3GPP systems 8

6.1.1 Introduction 8

6.1.2 Solution details 9

6.1.2.1 Number of UEs and PDU Sessions per network slice notification procedure 9

6.1.3 Evaluation 10

7 Conclusions 10

Annex A (informative): Change history 11

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

Editor’s Note: This clause contains some background information for the study.

# 1 Scope

The present document identifies key issues, potential security and privacy requirements and solutions with respect to network slicing Phase 2 work TS23.501 [2], TS23.502 [3], TS23.503 [4] and studies TR 23.700-40 [5] and TR 38.832 [6], specifically,

* Define the security requirements and security services for new NF(s) introduced for UEs’ network slice access control.
* Study potential security risks/threats (i.e. DoS, sensitive information leakage) and solutions if needed with respect to slice-related quota management, data rate limitation, and constraints on simultaneous use of slices.
* Study potential security risks/threats related to broadcasting slice-related cell selection/reselection info, and provide security solutions if needed.

# 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 (5GS)”

[3] 3GPP TS 23.502: “Procedures for the 5G System (5GS)”

[4] 3GPP TS 23.503: “Policy and charging control framework for the 5G System (5GS); Stage 2”

[5] 3GPP TR 23.700-40: “Study on enhancement of network slicing; Phase 2”

[6] 3GPP TR 38.832: “Study on enhancement of Radio Access Network (RAN) slicing”

[7] 3GPP TS 33.501: “Security architecture and procedures for 5G system”

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

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

<ABBREVIATION> <Expansion>

# 4 Architectural and security assumptions

Editor's note: This clause includes the architectural and security assumptions applicable for the study.

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: privacy issue on broadcasting slice information

### 5.1.1 Key issue details

A gNB may support multiple and different network slices, and on different frequencies in different regions.

In TR 38.832 [6], in order to support fast cell selection and cell reselection for particular network slices, solutions based on broadcasting slice related information are being studied. The broadcast slice related cell info may contain e.g. NSSAI, SST, slice grouping or slice associated information. In this key issue, the following questions are to be addressed:

- Whether broadcasting slice related information in this scenarios will cause any privacy issue

- If yes, mitigation solutions need to be provided

Editor’s Note: as per current TR 38.832 [6], NSSAI is not contained in the broadcast SIB. Whether NSSAI is already excluded from the broadcast SIB or not is to be confirmed by RAN2.

### 5.1.2 Security threats

According to TS 23.501 [1], SST refers to the expected Network Slice behaviour in terms of features and services. An SST could be represented with a standardised SST value or without a standardised SST value. The currently standardized SST values can indicate the slice types of eMBB, URLCC, MIoT and V2X, from which sensitive information of a specific slice can hardly be derived. Hence there is no privacy issue if SST is included in the broadcast SIB.

An S-NSSAI is comprised of a SST and an optional Slice Differentiator (SD), which is to differentiate amongst multiple network slices of the same Slice/Service type. An S-NSSAI may contain privacy-sensitive information, e.g. when dedicated to a group of users may expose the group identity. An S-NSSAI may also contain sensitive information, e.g. network topology that the operator may not want to share with others.

A cell broadcasting sensitive S-NSSAI may become a target of attackers interested in the S-NSSAI information. It is likely for an attacker to further link the S-NSSAI with its UEs/users together with other knowledge/tools, e.g. a frequency band supports only the sensitive S-NSSAI or a few allowing attackers to narrow down the scope. Broadcasting sensitive S-NSSAI should be avoided.

Editor’s Note: In case the S-NSSAI supported by RAN node consists only of an SST field value (without SD field), the privacy implication of broadcasting SST is FFS.

Editor’s Note: the privacy issue of slice grouping and slice associated info is FFS depending on their definition to be made by RAN2.

Editor’s Note: It is FFS whether sensitive S-NSSAI can be broadcasted even if it is protected, as a protected S-NSSAI on its own is enough to link the users to that broadcast even if the actual name of the S-NSAAI is not known.

### 5.1.3 Potential security requirements

TBD

## 5.2 Key Issue 2: DoS to NSAC procedure

### 5.2.1 Key issue details

A new Network Slice Admission Control (NSAC) procedure has been introduced in TS23.501 [2] and TS23.502 [3], where the number of registered UEs is monitored for a network slice (i.e. S-NSSAI) and a UE will be rejected to access if the number of UE registered in the requested S-NSSAI has reached its quota. However, the NSAC procedure needs to be studied further to address potential security risks, for examples:

* In the current NSAC procedure, the number of registered UE in an S-NSSAI is updated independently from other S-NSSAIs during the registration procedure. In other words, the granularity level at registration is S-NSSAI. However, it is not the case in the de-registration procedure. The numbers are only updated when the UE exits from all network slices, i.e. de-registered. Since a UE may access multiple slices, e.g. eight, the UE would still be counted against quota usage of ALL S-NSSAIs even the UE is not using some or most of slices (“idly occupied” by the UE). This may lead to the quota reached fast which does not reflect the real usage of a slice. Other legitimate UEs will suffer from DoS – “dog in the mager”. It is notable that an attacker can use legitimate UEs to launch such attacks.
* Assuming NSSAA is executed before NSAC, then if NSSAA is successful but quota has been reached, UE will be rejected. The UE has to send registration request later and go through the same NSSAA procedure again. This is a significant waste of resource (has to serve fewer UEs given the same resource) when NSSAA is required, since NSSAA requires multiple rounds of message exchanges with the home PLMN.
* The Early Admission Control (EAC) mode has been introduced where the admission control can be inactive if the number of UE bellows a preconfigured threashold. This may pose a security risk that exceeds the slice quota when a sudden increase in the slice registration requests, maliciously or accidentally.

### 5.2.2 Security threats

TBD

### 5.2.3 Potential security requirements

TBD

## 5.3 Key Issue #3: AF authentication and authorization

### 5.3.1 Key issue details

As specified in TS23.501 [2] and TS23.502 [3], the current utilization state of a network slice, e.g. the number of UEs registered for a network slice or the current number of PDU Sessions established on a network slice, can be reported to an AF deployed within a 3GPP system or in a third party domain. In either case, the AF should be authenticated and authorized beforehand and the 5G system should make sure no sensitive information leakage.

In TS23.502 [3], a notification procedure has been specified to allow an AF to get access to the network slide information through NEF. However, it is not clear how the AF is authenticated and authorized. The authorization details (e.g. what parameters and whether slice-specific parameters need to be verified) need to be specified to avoid ambiguity and potential attacks. It is expected that the AF deployed within the 3GPP domain or a third party domain will be authenticated or authorized in a different way, which should be also studied and specified. In addition, the procedure needs to take into account the privacy issue of S-NSSAI since S-NSSAI may not be available at a third party AF due to concerns on the sensitivity information leakage (an S-NSSAI may not to be made known to a third-party AF).

### 5.3.2 Security threats

If an AF is not authenticated or authorized before accessing to the network slice information, a mischievous AF may collect such information for other purposes. If S-NSSAI is sent to a third party AF, sensitive information may leak out of 3GPP systems.

### 5.3.3 Potential security requirements

S-NSSAI information shall not be sent to a third party AF for network slice quota-usage notification.

# 6 Solutions

## 6.1 Solution #1: authentication and authorization for a third-party AF or an AF deployed within 3GPP systems

### 6.1.1 Introduction

AF authentication and authorization is subject to whether the AF lies in the 3GPP system or in a third party domain. Existing but different mechanisms are chosen for the two scenarios. In case AF is a third party NF, S-NSSAI is not required at AF to prevent sensitive information leakage.

### 6.1.2 Solution details

If an AF is deployed within the 3GPP systems, authentication and authorization is based on the mechanisms defined for SBI, Clause 13 in TS33.501 [7], where the AF is authenticated by the NRF it registered within the same PLMN. For the Oauth 2.0 based authorization, the NRF takes the role of Authentication Server and the NEF takes the role of Resource Server.

If an AF a third party NF, authentication and authorization is based on the mechanisms defined in Clause 12 in TS33.501 [7], where mutual authentication is performed between the AF and the NEF. For the Oauth 2.0 based authorization, the NEF takes both roles of Authentication Server and the Resource Server.

In order to avoid sensitive information leakage involving S-NSSAI, S-NSSAI is not sent to or made available to a third party AF. Instead, NEF keeps a mapping between S-NSSAI and ENSI (External Network Slice Information) and ENSI (instead of S-NSSAI) is available at the third party AF. The notification procedure (adapted from the clause 4.15.3.2.10 of TS 23.502 [3]) with ENSI is described as below.

### 6.1.2.1 Number of UEs and PDU Sessions per network slice notification procedure

##

Figure 6.1.2.1-1: Number of UEs and PDU Sessions per network slice notification procedure

0. Authentication of AF: AF is authenticated by NRF or authenticated by NEF based on description above. A token is generated for AF after authentication. It is noted that the AF token includes claim for the authorized S-NSSAI or ENSI (if AF is a third party NF).

1. To subscribe or unsubscribe for the number of UEs or the number of PDU Sessions per network slice notification with the NSACF, the AF sends Nnef\_EventExposure\_Subscribe/Unsubscribe Request (Event ID, Event Filter, Event Reporting information) message to the NEF. The Event ID parameter defines the subscribed event ID, i.e. Number of Registered UEs or Number of Established PDU Sessions. The Event Filter parameter defines the S-NSSAI for which reporting is required. If the AF is a 3GPP NF, The Event Filter parameter is S-NSSAI whereas the Event Filter parameter is ENSI if the AF is a third party NF. The Event Reporting information parameter defines the mode of reporting, i.e. threshold based reporting with included a threshold value or periodic reporting with included periodicity time interval.

2. The NEF checks whether the AF is authorised for the requested subscription based on the AF token. It needs to check whether the token claims matches the AF’s identity and the Event Filter parameter. If authorised, the NEF may query the NRF to find the NSACF responsible for the requested S-NSSAI (NEF needs to map to S-NSSAI based on ENSI for a third party AF). The NEF forwards the request to the NSACF with Nnsacf\_SliceEventExposure\_Subscribe/Unsubscribe Request (Event ID, Event Filter, Event Reporting information). The Event Filter parameter is the mapped S-NSSAI for the third party AF.

3. The NSACF confirms with Nnsacf\_SliceEventExposure\_Subscribe/Usubscribe Response message to the NEF.

4. The NEF forwards the response from NSACF via the Nnef\_EventExposure\_Subscribe/Unsibscribe Response message to the AF. The Event Filter parameter is changed to the mapped ENSI for the third party AF.

5. When the reporting condition for a subscribed event is fulfilled, the NSACF triggers a notification towards the AF.

6. The NSACF sends the Nnsacf\_SliceEvent Exposure\_Notify (Event ID, Event Filter, Event Reporting information) message to the NEF. If the subscription is for event based notification (e.g. based on the monitored event reaching a threshold value), the Event Reporting information parameter contains confirmation for the event fulfilment. If the subscription is for periodic notification, the Event Reporting information parameter provides information for the current number of UEs registered with a network slice (e.g. represented in percentage of the maximum number of the UEs registered with the network slice) or information for the current number of PDU Sessions on a network slice (e.g. represented in percentage of the maximum number of the UEs established on the network slice) or both. It is

7. The NEF forwards the message to the AF in the Nnef\_EventExposure\_Notify (Event ID, Event Filter, Event Reporting information) message. The Event Filter parameter is changed to the mapped ENSI for the third party AF.

### 6.1.3 Evaluation

TBD

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-03 | SA3#102bis-e |  |  |  |  | TR Skeleton | 0.0.0 |
| 2021-03 | SA3#102bis-e |  |  |  |  | Incorporating S3-211264, S3-211265 | 0.1.0 |
| 2021-05 | SA3#103-e |  |  |  |  | Incorporating S3-212212 | 0.2.0 |
| 2021-08 | SA3#104-e |  |  |  |  | Incorporating S3-213133, S3-213030, S3-213134, S3-213140, S3-213144 | 0.3.0 |