|  |  |
| --- | --- |
| 3GPP TR 33.874 V0.2.0 (2021-05) | |
| 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 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.  © 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 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 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

6 Solutions 7

6.Y Solution #Y: <Solution Name> 7

6.Y.1 Introduction 7

6.Y.2 Solution details 7

6.Y.3 Evaluation 7

7 Conclusions 7

Annex A (informative): Change history 8

# 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”

# 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 33.832 [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 [2], 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.

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.

### 5.1.3 Potential security requirements

# 6 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.Y Solution #Y: <Solution Name>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 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 |