|  |
| --- |
| 3GPP TR 33.873 V0.3.0 (2021-03) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on the security of the system enablers for devices having Multiple Universal Subscriber Identity Modules;(Release 17) |
|   |
|  |  |
|  |
| 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 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Overview of the MUSIM features in the 5G System 7

5 Key issues 7

5.1 Key issue #1: Security Aspects of Busy Indication 7

5.1.1 Key issue details 7

5.1.2 Threats 7

5.1.3 Potential security requirements 7

5.2 Key issue #2: UE and Paging Server Communication 8

5.2.1 Key issue details 8

5.2.2 Threats 8

5.2.3 Potential security requirements 8

5.X Key Issue #X: <Key Issue Name> 8

5.X.1 Key issue details 8

5.X.2 Security threats 8

5.X.3 Potential security requirements 8

6 Solutions 8

6.1 Solution #1: Security Solution for Busy Indication using NAS signaling 8

6.1.1 Introduction 8

6.1.2 Solution details 9

6.1.3 System impact 10

6.1.4 Evaluation 10

6.Y Solution #Y: <Solution Name> 10

6.Y.1 Introduction 10

6.Y.2 Solution details 10

6.Y.3 System impact 10

6.Y.4 Evaluation 10

7 Conclusions 10

Annex A (informative): Change history 11

**Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.**Error! Bookmark not defined.

# 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 contains the study of system enablers for devices having multiple Universal Subscriber Identity Modules (USIM) in the EPS and 5G system architecture are studied in 3GPP TR 23.761[2]. This document provides the security and privacy issues related to MUSIM architecture and lists potential solutions for identified key issues including.

- Security and privacy issues exposing the Paging Cause in cleartext in paging message

- Security aspects of the communication between UE and Paging Server and exposing Paging server address

- Security and Privacy implications if a Multi-USIM device needs to explicitly indicate to the MNO owning one USIM and that UE is also registered via another USIM at the same or different PLMNs.

- Security aspects of Paging Response with cause value busy indication.

Finally, the study provides some conclusions for potential normative work.

# 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 TR 23.761: " Study on system enablers for devices having multiple Universal Subscriber Identity Modules (USIM)"

[3] 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 Overview of the MUSIM features in the 5G System

Editor’s Note: This clause contains architectures agreed by SA2 and security assumptions relevant 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: Security Aspects of Busy Indication

### 5.1.1 Key issue details

In TR 23.761 [2], a Multi-USIM device with concurrent registrations over 3GPP RAT associated with multiple USIMs procedures is discussed. A multi-USIM device can efficiently perform some activity (e.g., listen to paging) in a system while communicating in another system. The network sends a paging request to notify the UE of a pending MT service. UE may monitor periodically for paging from another system. UE responds to the page (either by accepting the page request or by sending a busy indication), which allows the network to save paging resources due to not escalating the page across a larger area.

It was concluded in TR 23.761 [2] that if a Multi-USIM device in RRC\_Idle mode decides not to accept a received paging, a BUSY Indication is sent by the UE via a NAS message to network whenever the UE supports NAS BUSY indication.

Editor’s Note: RAN2’s conclusion on busy indication for RRC\_INACTIVE UE is to be added.

### 5.1.2 Threats

If the Busy indication is injected, modified or replayed by attackers, the network may be spoofed to believe the UE appears busy, which will mislead the network to stop paging the UE for the incoming MT service and causing Dos attack on the UE.

If the Busy indication sent by the UE in a NAS message is removed by an attacker before reaching the AMF, the network may be spoofed to believe that the UE accepted the paging without indicating busy (e.g. a normal Service Request responding to paging), which will mislead the network to process the request from the UE with the existing procedure to prepare for the UE to be transferred from Idle to Connected mode. This will waste the network resource and alter the real intention of the MUSIM device, which is a type of DoS attack on both the network and the UE.

### 5.1.3 Potential security requirements

3GPP system shall support a mechanism to protect BUSY indication against modification, replay, and fabrication attacks.

## 5.2 Key issue #2: UE and Paging Server Communication

### 5.2.1 Key issue details

As per 23.761[2], A Multi-USIM device is needed to monitor each connected system's paging channel for MT services destined to that device. UE's paging notification and reception need to be done with minimal interruption to ongoing services in the current system and without performing undesirable operations (e.g., Wasting resource, reaching misleading assumption of reachability). MUSIM devices which are unable to simultaneously monitor paging on all 3GPP RATs and systems in which it is in Idle state or RRC\_Inactive state (for 5GS) needs to choose the paging channel(s) to monitor, which can lead to unsuccessful paging on the other paging channel(s). There are two solutions, to prevent unnecessary interruption of the current service to receive paging (Solution #7, Solution #12, Solution #27), proposed in the 23.761[2]. While connected to a MUSIM system, all these solutions deliver paging notifications of 3GPP RATs and systems in which UE is in Idle or inactive state through a currently active network. Solutions to this key issue should study security and privacy aspects related to communication between UE and paging server..

### 5.2.2 Threats

Editor’s note: Security threats are FFS.

### 5.2.3 Potential security requirements

Editor’s Note: Potential security requirements are FFS.

## 5.X Key Issue #X: <Key Issue Name>

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

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

## 6.1 Solution #1: Security Solution for Busy Indication using NAS signaling

### 6.1.1 Introduction

This solution addresses key issue #1: Security Aspects of Busy Indication.

The key issue proposes to support a mechanism to prevent DoS attack caused by busy indication. Solution reduces the severity of the DoS attacks and identify the DoS attacks by handling the response to paging for MT service. Solution described proposes a solution allowing the UE to send a busy indication to the network in a NAS message as a response to a page.

### 6.1.2 Solution details

The procedure below assumes that UE-1 can periodically pause the RRC-connection allowing UE-2 to perform page monitoring.



**Figure 6.1.2-1 BUSY Indication using NAS Signaling**

0. A device with USIM, i.e., UE1, is in connected mode and UE2 is in IDLE mode.

1. The AMF-2 serving the UE-2 sends a paging request message to RAN-2. RAN-2 pages UE-2

2. Upon receiving the paging message UE-2, if UE supporting NAS Busy indication decides to send a NAS Busy Indication, responds with a BUSY indication vis NAS message after RACH procedure. RAN-2 forwards the NAS message to the AMF-2. 1.

a. The NAS message carrying the Busy Indication may be ciphered. The cipher mechanism as defined in clause 6.4.4 of TS 33.501 [3] can be reused to protect the in the NAS message.

b. The NAS message carrying the Busy Indication is integrity protected. The integrity protection mechanism as defined in clause 6.4 3 of TS 33.501 [3] can be reused to integrity protect the in the NAS message.

Editor’s Note: Whether the busy indication shall be confidentiality protected needs more justification.

Editor’s Note: It is FFS how GUTI re-allocation is done when GUTI gets revealed in the busy indication message.

Editor’s Note: It is FFS to verify with RAN whether UE can do a 3-way NAS exchange in network B, when it is in active state in network A.

### 6.1.3 System impact

UE:

- Uses existing NAS integrity and ciphering mechanism as per 33.501[3].

AMF:

- Uses existing NAS integrity and ciphering mechanism as per 33.501[3].

Note: Details of NAS message to send busy indication will be defined by SA2 or CT1 group.

### 6.1.4 Evaluation

Above solution relies on already defined mechanisms in TS 33.501[3] to send ciphered and integrity protected BUSY indication and fulfills security requirements of Key issue 1.

## 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 System impact

Editor’s Note: Each solution should clearly list which entities need new functionality and what functionality they need for the provided solution to work.

### 6.Y.4 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** |
| 2020-11-09 | SA3#101-e | S3-202863 |  |  |  | TR Skeleton | 0.0.0 |
| 2020-11-16 | SA3#101-E | S3- 203411 |  |  |  | Version after SA3#101-E incorporating changes from S3-203410, S3-203409,S3-203408 | 0.1.0 |
| 2021-01-25 | SA3#102-e | S3-210627 |  |  |  | Version after SA3#102-e incorporating changes from S3-210626, S3-210694 | 0.2.0 |
| 2021-03-05 | SA3#102-Bis-e | S3-211284 |  |  |  | Version after SA3#102-Bis-e incorporating changes from S3-211276, S3-211275, S3-211277, S3-211031, S3-211280 | 0.3.0 |