|  |
| --- |
| 3GPP TR 33.700-28 V0.3.0 (2023-01) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of satellite access(Release 18) |
|   |
|  | 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.© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its 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

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 6

4 Assumptions 7

5 Key issues 7

5.1 Key issue #1: Protection of UE unreachability period retrieved by 5GC/EPC 7

5.1.1 Key issue details 7

5.1.2 Threats 7

5.1.3 Potential security requirements 7

5.X Key issue #X: <Title> 8

5.X.1 Key issue details 8

5.X.2 Threats 8

5.X.3 Potential security requirements 8

6 Solutions 8

6.1 Mapping of solutions to key issues 8

6.Y Solution #Y: <Title> 8

6.Y.1 Introduction 8

6.Y.2 Solution details 8

6.Y.3 Evaluation 8

7 Conclusions 9

Annex X: Change history 10

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# 1 Scope

The present document investigates the security and privacy aspects of satellite access/NTN. The study is based on the architectural and functional requirements on integration of satellite components in the 5GS/EPS architecture, so as to ensure that the proposed solutions address the security and privacy implications on the architecture enhancements agreed in TR 23.700-28 [x]. Specifically, it covers the following:

- The identified security and privacy issues, threats, and potential requirements for protecting the UE in the enhanced 5GS/EPS architecture supporting discontinuous coverage with satellite access;

- The potential solutions addressing the identified security and privacy issues as above.

# 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 23.700-28: "Study on Integration of satellite components in the 5G architecture; Phase 2".

[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 Assumptions

Discontinuous satellite coverage for satellite access in the context of this study is characterized by the fact that Uu interface is available for the UE less than 100% of the time, due to predictable patterns of satellite coverage.

According to TR 23.700-28 [x], the work on satellite access focuses on further 5GC/EPC enhancements to support discontinuous satellite access, which mainly aim for mobility enhancement and power saving optimizations. Therefore, security solutions should be applicable to both 5GS and EPS while minimizing the impact on 5GS and EPS protocols, and not adversely affect mobility enhancement and power saving optimizations.

# 5 Key issues

## 5.1 Key issue #1: Protection of UE unreachability period retrieved by 5GC/EPC

### 5.1.1 Key issue details

To support mobility enhancement and power saving optimization, multiple solutions were documented in TR 23.700-28 [2], which require 5GC/EPC to move the UE into CM-IDLE state and provide power saving parameters or mobility management parameters properly, when the UE is about to leave satellite coverage. This requires that UE unreachability period information to be made aware of by 5GC/EPC. According to the conclusions in TR 23.700-28 [2], such UE unreachability period information (timing information when UE moves out/in of NTN coverage or satellite coverage information at current and potential future locations of the UE) could be retrieved by 5GC/EPC from different potential sources, e.g. the OAM, the UE, the AF/external server (e.g. Coverage Map Server). While the sources like the OAM could be trusted, the sources like the AF/external server may not always be trusted.

In addition, it is concluded in TR 23.700-28 [2] clause 8.1 that the AMF/MME does not determine UE unreachability period by itself but obtains UE unreachability period information from an AF or the UE or the OAM. If the UE unreachability period information is provided by the AF, it requires the AF to determine per UE information for the AMF/MME. To authorize the AF by the network as defined in TS 33.501 [3], OAuth 2.0 based authorization is used, which is however an authorization on service level, not on per UE level.

### 5.1.2 Threats

If 5GC/EPC receives falsified or tampered UE unreachability period information, the 5GC/EPC may be misled to put a CM-CONNECTED UE into CM-IDLE state when the UE is still in satellite coverage, leading to service interruption; or the 5GC/EPC may be misled to provide inappropriate mobility management parameters and/or power saving parameters to the UE, which fails the optimization of power consumption. Both cases are a type of DoS attack on the UE.

If an AF authorized for satellite access service provides 5GC/EPC the unreachability period information of a UE that is not under its authority, the 5GC/EPC may also suffer from the above threat.

### 5.1.3 Potential security requirements

The 5GS/EPS shall provide a means to ensure that the AF/external server is authorized to provide UE unreachability period information.

Editor’s Note: Whether UE unreachability information will be provided by the AF/external server is subject to SA2 normative work. The security of the interface between the 5GC/EPC and the AF/external network is subject to SA2 normative work.

## 5.X Key issue #X: <Title>

### 5.X.1 Key issue details

### 5.X.2 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 Mapping of solutions to key issues

Editor's Note: This clause contains a table mapping between key issues and solutions.

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

### 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 X:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-10 | SA3#108 Adhoc-e | S3-222864 |  |  |  | Skeleton (approved at SA3#108Adhoc-e) | 0.0.1 |
| 2022-10 | SA3#108 Adhoc-e | S3-223043 |  |  |  | Inclusion of the documents approved at SA3#108Adhoc-e: S3-223040, S3-223041, S3-223042 | 0.1.0 |
| 2022-11 | SA3#109 | S3-224166 |  |  |  | Inclusion of the documents approved at SA3#109: S3-224072 | 0.2.0 |
| 2023-01 | SA3#109 Adhoc-e | S3-230563 |  |  |  | Inclusion of the documents approved at SA3#109Adhoc-e: S3-230563 | 0.3.0 |
|  |  |  |  |  |  |  |  |