|  |
| --- |
| 3GPP TR 33.700-29 V0.1.0 (2024-03) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Security Aspects of 5G Satellite Accessin the 5G architecture;Phase 3 (Release 19) |
|   |
|  |  |
|  |
| 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.© 2024, 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 and abbreviations 6

3.1 Terms 6

3.2 Abbreviations 7

4 Architecture and security assumptions 7

5 Key issues 7

5.1 Key issue #1: Security protection in Store and Forward Satellite Operation 7

5.1.1 Key issue details 7

5.1.2 Security threats 8

5.1.3 Potential security requirements 8

5.X Key Issue #X: <Key Issue Name> 9

5.X.1 Key issue details 9

5.X.2 Security threats 9

5.X.3 Potential security requirements 9

6 Solutions 9

6.0 Mapping of Solutions to Key Issues 9

6.Y Solution #Y: <Solution Name> 9

6.Y.1 Introduction 9

6.Y.2 Solution details 9

6.Y.3 Evaluation 9

7 Conclusions 9

7.Z Key Issue #Z: <Key Issue Name> 9

Annex <A>: <Informative annex title for a Technical Report> 10

Annex <X>: 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.

# 1 Scope

The present document studies the security and privacy aspects of 5G satellite access phase 3. It is comprised of the following parts:

- Identify and study the security and privacy key issues of the regenerative payload generic architecture in 5GS/EPS.

- Identify and study the security and privacy key issues of the Store and Forward (S&F) Satellite operation both for NR NTN (5GS) and for IoT NTN (EPS).

- Identify and study the security and privacy key issues of UE-Satellite-UE communication enhancements for 5GS.

- The impact on regulatory services in the context of 5G satellite access. In particular, the assessment of the potential impact to lawful intercept in regenerative, Store and Forward (S&F), and UE-satellite-UE communication enhancement architecture.

# 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 23.700-29: "Study on integration of satellite components in the 5G architecture; Phase 3".

[3] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[5] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

[6] 3GPP TS 33.210: "Network Domain Security: IP network layer security".

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1], 3GPP TR 23.700-29[2] 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 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].

S&F Store and Forward

# 4 Architecture and security assumptions

The following architecture and security assumptions are applied to the study:

- The architecture assumptions and principles for EPS/5GS integrating of satellite components as defined in TR 23.700-29 [2] are used as architecture assumptions in this study.

- The security architecture, procedures, and security requirements for EPS/5GS as defined in TS 33.401 [3] / TS 33.501 [4] are used as a baseline.

- The IP Multimedia Subsystem (IMS) media plane security as defined in TS 33.328 [5] is used as a baseline.

- The physical security of 3GPP systems on board orbiting satellites is out of the scope of 3GPP.

- The feeder link and the inter-satellite link (ISL) are assumed to act only as transport layer links and are not specified in 3GPP.

- The use of feeder link and ISL is assumed to have no impact on the security of reference points (including the X2/Xn interface, S1-MME/N1 interface, S1-U/N3 interface, and the interfaces between the core network entities) by using the network domain security as defined in TS 33.210 [6].

Editor’s Note: Priority of the security study between IoT NTN (EPS) and NR NTN (5GS) and the scenario when two UEs are under the coverage of the same satellite are to be aligned with TR 23.700-29 [2]. The security study should be aligned with TR 23.700-29 [2].

Editor’s Note: Security of on board 3GPP system hosted by satellite requires further security assumptions. Such assumptions are FFS.

# 5 Key issues

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

## 5.1 Key issue #1: Security protection in Store and Forward Satellite Operation

### 5.1.1 Key issue details

In clause 4 of TR 23.700-29 [2], there is following description about the Store and Forward Satellite Operation:

*"The following architecture assumptions are applied to the study:*

*…*

*- Store and Forward Satellite Operation assumes that UE-satellite-ground network connectivity can be intermittent as defined in clause 3.1.*

*- Store and Forward Satellite Operation shall work without ISL.*

*…"*

From a security perspective, whether a UE can use Store and Forward Satellite service should be assured by the 3GPP network.

In S&F satellite operations, architectural assumption is that the UE-satellite-ground network connectivity is intermittent. 3GPP Network Functions and/or Network Elements which are located on a satellite may communicate with the ground infrastructure of 3GPP network over an intermittently available feeder link connection between the satellite and the ground network. S&F satellite operational mode is relevant for delay tolerant and non-real time communications via LEO/MEO space segment.

During the feeder link’s intermittent unavailability, the following risks arise.

1. The EPS/5G AKA procedure may not get fully completed or is partially completed. It results into incomplete procedure for mutual authentication between the network and the UE.

2. The Security Mode Command (SMC) procedure for Non-Access Stratum (NAS) may not fully complete because the NAS connection between UE and MME/AMF may have been interrupted. In turn it results into incomplete security capabilities negotiation between the UE and the EPS/5GC network.

This key issue is to study the authentication, authorization and data security in Store and Forward Satellite Operation.

### 5.1.2 Security threats

Editor’s Note: the feasibility of the denial of service (i.e. caused by false user-plane data or control-plane data) is FFS.

Editor’s Note: whether the availability issue is a security threat is FFS.

Editor’s Note: whether there are more security threats is FFS.

Editor’s note: The risk of resource depletion of 3GPP system due to UE's incomplete AKA procedure is dependent on agreed architecture solution direction of S&F KI in SA2.

Due to the nature of the S&F mode during the feeder link’s intermittent unavailability, the following threats can manifest themselves:

- When the UE and 3GPP network cannot mutually authenticate, such condition may cause availability issue.

- Without the authentication, confidentiality, integrity, and anti-replay protection there will be no security protection of the communication between UE, on board satellite 3GPP systems and ground-based 3GPP systems.

### 5.1.3 Potential security requirements

The 3GPP system shall support mutual authentication between the UE and the 3GPP network in the Store and Forward Satellite Operation.

The 3GPP system shall support means to provide confidentiality, integrity, and anti-replay protection for user-plane and control-plane messages between UE and the 3GPP network in the Store and Forward Satellite Operation.

Editor’s Note: whether there are more security requirements is 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.

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |
| --- | --- |
|  | Key Issues |
| Solutions | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

## 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

## 7.Z Key Issue #Z: <Key Issue Name>

Editor’s Note: This clause contains the agreed conclusions of Key Issue #Z.

Annex <A>:
<Informative annex title for a Technical Report>

 Annex <X>:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024 | SA3#115 | S3-240626 |  |  |  | Skeleton | 0.0.0 |
| 2024 | SA3#115 | S3‑240930 |  |  |  | S3-240931, S3-240932, S3-240933, S3-240934 | 0.1.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |