|  |  |
| --- | --- |
| 3GPP TR xx.xxx V0.1.0 (2025-09) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Security Aspects of Satellite Access in 5G;  Phase 4  (Release 20) | |
|  | |
|  |  |
|  | |
| 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.  © 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 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 4

1 Scope 6

2 References 6

3 Definitions of terms and abbreviations 6

3.1 Terms 6

3.2 Abbreviations 6

4 Architecture assumptions 6

5 Key issues 7

5.1 Key Issue #1: Authenticated UE to exchange NAS messages with multiple satellites in split-MME architecture 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

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

6.0 Mapping of Solutions to Key Issues 8

6.Y Solution #Y: <Solution Name> 8

6.Y.1 Introduction 8

6.Y.2 Solution details 8

6.Y.3 Evaluation 8

7 Conclusions 8

7.Z Key Issue #Z: <Key Issue Name> 8

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

# 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 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[3] 3GPP TS 33.401: "3GPP System Architecture Evolution: Security Architecture".

…

[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] 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].

<ABBREVIATION> <Expansion>

# 4 Architecture assumptions

The following architecture assumptions are applied to the study:

- The general features and the Split MME architecture of Store and Forward Satellite operation are described in Annex O.2 of TS 23.401 [2] are used as architecture assumptions in this study.

# 5 Key issues

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

## 5.1 Key Issue #1: Authenticated UE to exchange NAS messages with multiple satellites in split-MME architecture

### 5.1.1 Key issue details

One of the architectural assumptions for Store and Forward Satellite operation is that when the service link is available, there is no feeder link and inter satellite link. There are two example deployment options for Store and Forward Satellite operation given in Annex O of TS 23.401 [2], i.e. Split MME architecture and Full EPC in each satellite.

For the split-MME architecture, S&F Satellite operation may involve multiple satellites allocated by an S&F Monitoring List. In this scenario, the UE context needs to be synchronized between the multiple MME-onboard(s) and the associated MME-ground. The synchronization of UE context between the MME-ground and MME-onboard(s) is out of the scope of 3GPP.

According to Annex N of TS 33.401 [3], regular LTE procedures are used to provide security between UE and network for the split-MME architecture. This means that once the UE completes an interaction with a satellite, the UE context in the satellite must be synchronized to other satellites before these satellites can perform any subsequent S&F Satellite operations with the UE. This significantly reduces the data exchange efficiency of the entire system.

Ideally, for an IoT device, once it is registered in the network and its UE context has been distributed to the satellites included in the S&F Monitoring List, the UE can exchange data with these satellites without the need for UE context synchronization between the satellites.

This key issue focuses on solutions that meet the following conditions:

- The UE context of the UE registered in the network has been provided to the satellites included in the S&F Monitoring List;

- The UE can perform Mobile Originated (MO) or Mobile Terminated (MT) data transmission with the satellites that have the UE context;

- The UE context does not need to be synchronized across the multiple satellites for supporting the MO/MT data transmissions. However, UE context synchronization may still be required for other changes not being associated with the MO/MT data transmission.

### 5.1.2 Security threats

If the NAS COUNTs are not synchronized across multiple satellites, an attacker may intercept and replay previously transmitted NAS messages. Since different satellites may accept outdated NAS COUNT values, the replay protection mechanism could be bypassed, leading to unauthorized actions.

Key stream may be reused if the security contexts are not well-managed across multiple satellites.

### 5.1.3 Potential security requirements

The 3GPP system shall support means to secure NAS messages exchange in the store and forward satellite operations.

## 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** |
| 2025 | SA3#123 | S3-252746 |  |  |  | Skeleton | 0.0.0 |
| 2025 | SA3#123 | S3‑253040 |  |  |  | S3-252746, S3-253039, S3‑253041 | 0.1.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |