|  |
| --- |
| 3GPP TR 33.754 V0.1.0 (2024-04) |
| *Technical* *Report* |
| **3rd Generation Partnership Project;****Technical Specification Group Services and System Aspects;****Study on security aspects for Multi-Access(DualSteer + ATSSS Ph-4);****(Release** **19)** |
|   |
| *A logo with a green logo  Description automatically generated* | 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.© 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 6

Introduction 7

1 Scope 8

2 References 8

4 Security assumptions 9

5 Key issues 9

5.1 Key Issue #Y: Authentication of UE in ATSSS over Non-Integrated Non-3GPP Access 9

5.1.1 Key issue details 9

5.1.2 Security threats 10

5.1.3 Potential security requirements 10

5.2 Key Issue #Y: Confidentiality and integrity protection of the communication between UE and 5GCore in Non-Integrated Non-3GPP Access. 10

5.2.1 Key issue details 10

5.2.2 Security threats 10

5.2.3 Potential security requirements 11

5.X Key Issue #X: <Key Issue Name> 11

5.X.1 Key issue details 11

5.X.2 Security threats 11

5.X.3 Potential security requirements 11

6 Solutions 11

6.0 Mapping of solutions to key issues 11

6.Y Solution #Y: <Solution Name> 11

6.Y.1 Introduction 11

6.Y.2 Solution details 11

6.Y.3 Evaluation 11

7 Conclusions 11

Annex <X> (informative): Change history 12

# 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: The introduction clause content is left for future consideration.

# 1 Scope

The present document aims to address the security aspects of Multi-Access, focusing on DualSteer devices and ATSSS Phase 4 (ATSSS Ph-4) enhancements, as identified in the FS\_MASSS study in TR 23.700-54 [2].

The scope of this study includes the following key areas:

- Examine the security implications of a simplified architecture over non-3GPP access, where non-3GPP access does not rely on the current TNGF/N3IWF architecture. This involves assessing:

- Whether to keep NAS security context on non-3GPP access.

- Whether to keep IPsec on the user plane and/or control plane of non-3GPP access.

- Whether new security mechanisms are to be considered in UE procedures, particularly regarding registration and connectivity to the 5G system in the context of ATSSS between 3GPP and non-3GPP access without 5G NAS.

The study will leverage insights from the requirements and architectural considerations outlined in the FS\_MASSS study in TR 23.700-54 [2].

# 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 23.700-54 "Study on Multi-Access (DualSteer and ATSSS\_Ph4)".

[3] 3GPP TS 33.501: " Security architecture and procedures for 5G system"

[4] 3GPP TS 23.501: "System architecture for the 5G System (5GS) "

…

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

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>

clause includes the overview applicable for the study.

# 4 Security assumptions

Editor’s Note: This clause includes the security assumptions 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: Authentication of UE in ATSSS over Non-Integrated Non-3GPP Access

### 5.1.1 Key issue details

As specified in TS 33.501 [3], authentication of UE for non-3GPP access is done by the successfully running the primary authentication. However, TR 23.700-54 [2] introduces the concept of Non-Integrated Non-3GPP Access (NIN3A), a type of non-3GPP access network that provides direct IP connectivity between the UE and the UPF without any intermediate NF such as Non-3GPP Interworking Function (N3IWF) and Trusted Non-3GPP Gateway Function (TNFG). Here, UE does not register to the 5GC over this Non-Integrated Non-3GPP Access. However, the UE is still able to access 5G resources, i.e. UPF, SMF. NIN3A leverages direct connections between UE and UPF to streamline connectivity.

This Key Issue focuses on the security challenges associated with direct connectivity, particularly in the absence of N3IWF/TNGF. The primary concerns include:

- Authentication: Ensuring the UE's identity is securely verified and authenticated before establishing a direct connection to the UPF.

- Privacy and Identity Protection: Protecting the UE's identity during the connectivity process.

Editor’s note: The definition of UE identity in this context is FFS.

### 5.1.2 Security threats

Non-Integrated Non-3GPP Access (NIN3A) exposes a new IP communication endpoint in the 5G Core (UPF) to be reachable directly by the UE. The absence of authentication between the UE and UPF introduces significant security risks and threats, potentially compromising the UPF network element and the entire 5G Core. Here are some of those threats:

- Unauthorized Access: The lack of authentication would allow unauthorized UEs to gain access and connect directly to the UPF, compromising the network resources and potentially launching further attacks.

- Impersonation: Attackers can spoof the identity of legitimate UEs or masquerade as trusted entities to gain access to the network.

- Denial of Service (DoS) Attacks: Attackers can exploit the lack of authentication to launch DoS attacks against the UPF, overwhelming network resources and disrupting legitimate services.

### 5.1.3 Potential security requirements

The 5G System should support the means to authenticate a UE accessing the network via Non-Integrated Non-3GPP Access (NIN3A).

The authentication mechanism should not compromise the privacy of the UE.

## 5.2 Key Issue #2: Confidentiality and integrity protection of the communication between UE and 5GCore in Non-Integrated Non-3GPP Access.

### 5.2.1 Key issue details

TR 23.700-54 [2] introduces the concept of non-Integrated non-3GPP Access (NIN3A), a type of non-3GPP access network that provides direct IP connectivity between the UE and the UPF without any intermediate NF such as Non-3GPP Interworking Function (N3IWF) and Trusted Non-3GPP Gateway Function (TNFG). This access type should not compromise the security of the 5G network.

This key issue focuses on safeguarding the confidentiality and integrity of data exchanged between the UE and the 5G Core Network under NIN3A connectivity, within the ATSSS framework. It emphasizes the need for comprehensive security measures that encompass both the associated proxy functionalities, such as MPQUIC and MPTCP, as specified for ATSSS in TS 23.501 (clause 5.32) [4], and beyond.

### 5.2.2 Security threats

If the communication between UE and 5G Core Network via NIN3A is not confidentiality and integrity protected, an attacker could intercept and manipulate the traffic between both endpoints, leading to data theft, tampering or service disruption. These vulnerabilities could undermine the trust and reliability of the 5G network, especially in scenarios that leverage NIN3A for enhanced connectivity.

### 5.2.3 Potential security requirements

The new simplified ATSSS architecture over non-3GPP access should provide the mechanisms to protect the traffic (user plane and/or control plane) between the UE accessing the network via Non-Integrated Non-3GPP Access (NIN3A) and the 5G Core Network.

Editor’s note: Whether control plane protocol stack is needed in Non-3GPP access, and consequently the associated security requirement, will depend on the conclusions of TR 23.700-54 [2]

## 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

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

**Table 6.0-1: Mapping of solutions to key issues**

|  |  |
| --- | --- |
| **Solutions** | **KI#X** |
|  |  |

## 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. The evaluation of the solution should include the impact in the 5G system.

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04 | SA3#115Adhoc-e | S3-241591 |  |  |  | TR Skeleton | 0.0.0 |
| 2024-04 | SA3#115Adhoc-e | S3-241608 |  |  |  | Included changes from S3-241590, S3-241577, S3-241366, | 0.1.0 |