|  |  |
| --- | --- |
| 3GPP TR 33.700-32 V0.1.0 (2024-04) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of User Identities and Authentication  (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 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 Symbols 6

3.3 Abbreviations 6

4 Architecture and security assumptions 6

5 Key issues 7

5.X Key Issue #X: <Key Issue Name> 7

5.X.1 Key issue details 7

5.X.2 Security threats 7

5.X.3 Potential security requirements 7

6 Solutions 7

6.0 Mapping of Solutions to Key Issues 7

6.Y Solution #Y: <Solution Name> 7

6.Y.1 Introduction 7

6.Y.2 Solution details 7

6.Y.3 Evaluation 7

7 Conclusions 7

Annex <A>: <Informative annex title for a Technical Report> 8

Annex <X>: Change history 9

# 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 for the creation and usage of user identities as studied in 3GPP TR 23.700-32 [2], with the following focus:

1. Study authentication and authorization of:
   1. a user identifier associated with a subscription and used on a UE (i.e., human user) and
   2. an identifier associated with a non-3GPP device behind a UE or 5G-RG.
2. Study privacy and security impacts of usage of user identifiers associated with a subscription or with a non-3GPP device behind a UE or 5G-RG, including exposure of user profile related information.

# 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 23.700-32: "Study on User Identities and Authentication 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], TR 23.700-32 [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].

**Non-3GPP device identifier:** an identifier of a non-3GPP device applies to a non-3GPP device connecting to network via a UE or 5G-RG.

Editor’s Note: the non-3GPP device identifier and user identifier may be updated according to the progress in TR 23.700-32 [2].

## 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 Architecture and security assumptions

This study should be based on the following assumptions:

- The architecture requirements and assumptions as described in TR 23.700-32[2] apply.

- The security architecture, procedures, and security requirements for 5GS as defined in TS 33.501 [x] are used as a baseline.

- For the non-3GPP device behind a UE or 5G-RG:

- Credentials are assumed to be provisioned in the non-3GPP device by an operator, human user or a 3rd party.

NOTE: How this is performed is not in scope of this study. The authentication of the non-3GPP device is not done by the 5GC.

- For the human user of the UE:

- The user authentication and primary authentication are independent. The user authentication procedure will not impact UE primary authentication procedure.

# 5 Key issues

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

## 5.1 Key Issue #1: Authentication and Authorization of Human User ID

### 5.1.1 Key issue details

TR 23.700-32 [2], *Key Issue #2: "Authentication and Authorization of Users and Restrictions on Users"* focuses on:

* authentication and authorization of a human user of a subscription and
* restriction on number of simultaneously active user identifiers of a subscription.

With the following NOTE:

*NOTE: Aspects of this key issue will depend on interaction with SA WG3. For example, authentication and Authorization methods are in the remit of SA WG3.*

The architecture assumption and requirement in TR 23.700-32 [2], clause 4.1 related to linkage and activation of user identifier with a UE subscription apply in the human user scenario.

This key issue is to study the authentication and authorization of a user identifier in the human user scenario.

### 5.1.2 Security threats

Without support for an authentication and authorization mechanism for the human user, an attacker may impersonate the human user of a subscription and gain unauthorized access to services normally available for that subscription legitimate user.

### 5.1.3 Potential security requirements

The 3GPP system shall provide means to support authentication and authorization of human user based on a User identifier linked to a 3GPP subscription.

## 5.2 Key Issue #2: User privacy

### 5.2.1 Key issue details

User identifier is a piece of information used to identify one specific User Identity, which is privacy sensitive.

In clause 5.3 of TR 23.700-32 [2], exposure of User Identity Profile information is documented as a key issue, with a NOTE as following:

"*NOTE 1: Aspects of this key issue will depend on interaction with SA WG3. For example, privacy protections related to exposure of User Identity Profile information and authorization/authentication results need to be coordinated with SA WG3.*"

This key issue focuses on the privacy aspect of User Identifier and User Identity Profile information.

### 5.2.2 Security threats

Either during the communication using User Identifier or during the exposure of User Identity Profile information, without proper protection against linkability and trackability attack, the privacy sensitive information may be leaked to undesired party so that the privacy of the user is violated.

### 5.2.3 Potential security requirements

The 5G system shall provide mechanisms for mitigating privacy attacks (e.g. trackability, linkability) against user identifier during the communication between the UE and the network, including the procedures for user authentication and service access.

The 5G system shall provide mechanisms for mitigating privacy attacks (e.g. disclosure) during the exposure of User Identity Profile information by the network to entities outside operator domain.

## 5.3 Key issue #3: Authentication and Authorization of one or more non-3GPP devices behind one gateway UE or 5G-RG

### 5.3.1 Key issue details

This key issue is going to address Authentication and Authorization of one or more non-3GPP devices behind one gateway UE or 5G-RG. It is to address the security issues related to the key issue #4 in the TR 23.700-32 [2], i.e. Identifying non-3GPP Devices Connecting behind a UE or 5G-RG.

### 5.3.2 Security Threats

If the non-3GPP devices behind one gateway UE or 5G-RG are not authenticated and authorized through means supported by the network, the attacker can access the network as a non-3GPP device via one gateway UE or 5G-RG without any authorization and restriction.

### 5.3.3 Potential security requirements

The 3GPP system shall provide means to support authentication and authorization of a non-3GPP device behind UE or 5G-RG based on a non-3GPP device identifier.

## 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

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions |  | | |
|  | <Key Issue #1> | <Key Issue #2> | <Key Issue #3> |
| #1 |  |  |  |
| #2 |  |  |  |
| #3 |  |  |  |

## 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 to the 3GPP system.

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions of the study.

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** |
| 2024-04 | SA3#115Adhoc-e | S3-241221 |  |  |  | Draft TR 33.700-32 skeleton | 0.0.0 |
| 2024-04 | SA3#115Adhoc-e | S3-241565 |  |  |  | Draft TR 33.700-32 skeleton (revised) | 0.0.1 |
| 2024-04 | SA3#115Adhoc-e | S3-241545 |  |  |  | S3-241565, S3-241122, S3-241556, S3-241514, S3-241515, S3-241543, S3-241566 | 0.1.0 |
|  |  |  |  |  |  |  |  |