|  |
| --- |
| 3GPP TR 33.790 V0.1.0 (2024-03) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on the security support for the Next Generation Real Time Communication services phase 2;(Release 19) |
|   |
|  | 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 4

Introduction 5

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: Third party specific identities 8

5.1.1 Key issue details 8

5.1.2 Security threats 8

5.1.3 Potential security requirements 8

5.2 Key Issue #2: Security of IMS based Avatar Communication 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 9

6 9

6.0 Mapping between key issues and solutions 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

Annex A (informative): 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.

# Introduction

Editor's Note: The introduction clause content is left for future consideration.

# 1 Scope

The present document studies security impacts of the new features of the Next Generation Real Time Communication studied in TR 23.700-77[2], specifically, the security aspects that are to be covered in this study are as follows:

- IMS third party identity security handling

- the security handling of the enhancements to support the use cases of IMS based Metaverse services.

Editor’s Note: New objectives may be added to address security aspects of other key issues introduced in SA2 after further progress made in SA2.

# 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".

1. 3GPP TR 23.700-77: ""Study on system architecture for next generation real time communication services; Phase 2".
2. 3GPP TR 33.890: "Study on security support for next generation real time communication services".
3. 3GPP TR 24.229: " IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP);Stage 3".

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or 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

## 4.1 General

The following clauses include information about the Rel-18 Next Generation Real Time Communication security study results documented in TR 33.890 [3] and the related Rel-19 architecture study documented in TR 23.700-77 [2].

## 4.2 Architectural Assumptions and Principles

The following architectural assumptions and principles are considered during the study:

- The third party specific user identity handling work in TR 33.890 [3] and TR 23.700-77 [2] is taken into account if applicable. The existing Ms reference point and procedures as described in TS 24.229 [4] are to be reused.

- The security study of the IMS enhancements to support media handling of avatar calls considers alignment with the study in TR 23.700-77 [2].



Figure 4.2-1: Usage of Ms reference point (see TS 24.229 [4], Annex V.2)

# 5 Key issues

## 5.1 Key issue #1: Third party specific user identities

### 5.1.1 Key issue details

According to TR 23.700-77 [2], there are scenarios that the third party subscribers use third party IDs (e.g., enterprise employee ID). The IMS network can present the third party ID to the callee during subsequent calling process. The third party subscriber can access the IMS network directly or via a SIP trunk as well.

From the security point of view, the enhanced IMS network shall be able to support the identity verification and authorization of third-party user during an IMS call.

### 5.1.2 Threats

A malicious UE can use IDs belonging to others or forged IDs to initiate IMS calls in the IMS network;

A malicious UE can use an ID that no longer belongs to it to initiate IMS calls in the IMS network (e.g., the user use the ID allocated by a particular company even after leaving it).

The ID's transfer between IMS networks may be manipulated by intermediary network entities. Consequently, the callee may receive a wrong ID.

### 5.1.3 Potential security requirements

The IMS system shall be able to coordinate with the third party to verify and authorize the third-party specific user identities.

The IMS network shall be able to support the integrity protection of the third-party specific user identities on the originating side and terminating side.

Editor’s Note: The KI may be updated according to SA2’s progress.

## 5.2 Key issue #2: Security of IMS based Avatar Communication

### 5.2.1 Key issue details

According to TR 23.700-77 [2], there are scenarios that a UE uses an Avatar-ID to initiate an IMS based Avatar Communication. Then the Avatar-ID is used to fetch objects such as an Avatar representation which may include Avatar metadata and Avatar media.

The IMS network can present the Avatar to the callee during the subsequent calling process. The UE can access the IMS network directly or via a SIP trunk as well.

From a security point of view, the enhanced IMS network needs to be able to support the Avatar-ID authentication and authorization during an IMS Avatar call. Also, Avatar objects such as Avatar representations could be used by malicious users to impersonate other users. Therefore, it is essential to ensure that the Avatar objects are secure and cannot be tampered with or accessed by unauthorized entities.

### 5.2.2 Threats

A malicious UE can use Avatar-IDs belonging to other UEs or forged Avatar-IDs to initiate IMS avatar communication in the IMS network and therefore impersonate other UEs.

The potential transfer of the Avatar-IDs between IMS networks can potentially be tampered by intermediary network entities.

The potential transfer of the Avatar metadata between IMS networks can potentially be manipulated by intermediary network entities.

The potential transfer of the Avatar media between IMS networks can potentially be manipulated by intermediary network entities.

Avatar objects could be used for impersonating a IMS caller.

### 5.2.3 Potential security requirements

The 3GPP system shall support means to ensure that stored Avatar objects and Avatar-IDs are accessed only by authenticated and authorized entities, i.e. UEs and IMS network nodes. .

The IMS network shall support the integrity protection of the Avatar-ID on the originating side and terminating side.

The IMS network shall support the integrity protection of the Avatar objects such as the Avatar representation on the originating network and terminating network.

# 6 Solutions

Editor's Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.0 Mapping between key issues and solutions

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

## 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

# 7 Conclusions

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

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02-19 | SA3#115 | S3-240761 |  |  |  | TR skeleton | 0.0.0 |
| 2024-03-04 | SA3#115 | S3-240941 |  |  |  | pCRs approved at SA3#115: S3-240761, S3-240942, S3-240943, S3-240944, S3-240945 | 0.1.0 |