|  |
| --- |
| 3GPP TS 33.xxx V0.1.0 (2021-10) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)(Release 17) |
|   |
|  |  |
|  |
| 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.© 2021, 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, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Overview 7

4.1 General 7

4.2 Reference points and functional entities 7

5 Common security procedures 7

5.1 General 7

6 Security for 5G ProSe features 7

6.1 Security for 5G ProSe Discovery 7

6.1.1 General 7

6.1.2 Security requirements 7

6.1.3 Security procedures 7

6.2 Security for Groupcast mode 5G ProSe Direct Communication 7

6.2.1 General 8

6.2.2 Security requirements 8

6.2.3 Security procedures 8

6.3 Security for Unicast mode 5G ProSe Direct Communication 8

6.3.1 General 8

6.3.2 Security requirements 8

6.3.3 Security procedures 8

6.4 Security for 5G ProSe UE-to-Network Relay Communication 8

6.4.1 General 8

6.4.2 Security requirements 8

6.4.3 Security for 5G ProSe Communication via 5G ProSe Layer-3 UE-to-Network Relay 8

6.4.3.1 General 8

6.4.3.2 Security procedure over User Plane 8

6.4.3.3 Security procedure over Control Plane 8

6.4.4 Security for 5G ProSe Communication via 5G ProSe Layer-2 UE-to-Network Relay 8

6.4.4.1 General 8

Annex <A> (normative): <Normative annex for a Technical Specification> 9

Annex <B> (informative): <Informative annex for a Technical Specification> 10

Annex <X> (informative): Change history 10

# Foreword

This Technical Specification 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 specifies the security and privacy aspects of the Proximity based Services (ProSe) in the 5G System (5GS). 5G ProSe security features include: 5G ProSe Direct Discovery security, 5G ProSe Direct communication security, and 5G ProSe UE-to-Network Relay security.

# 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 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

# 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].

Definition format (Normal)

**<defined term>:** <definition>.

**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 format (EW)

<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 format (EW)

<ABBREVIATION> <Expansion>

# 4 Overview

Editor’s Notes: This clause contains the overview of 5G ProSe security and links to other specifications, reference points and functional entities, etc.

## 4.1 General

The overall architecture for 5G ProSe is given in TS 23.304 [2]. 5G ProSe includes several features that may be deployed independently of each other. For this reason, no overall security architecture is provided and each feature describes its own architecture.

Security for the 5G ProSe common procedures is described in clause 5, while the overall security of the 5G ProSe features is described in clause 6.

## 4.2 Reference points and functional entities

**PCx**: The reference point between the UE and the 5G ProSe Key Management Function. PCx relies on 5GC user plane for transport (i.e. an "over IP" reference point). It is used to transport security material to UEs for Groupcast mode 5G ProSe Direct Communication and 5G ProSe UE-to-Network Relay Communication.

# 5 Common security procedures

Editor’s Notes: This clause contains security procedures that are used by more than one ProSe feature.

## 5.1 General

# 6 Security for 5G ProSe features

Editor’s Notes: This clause contains 5G ProSe features.

## 6.1 Security for 5G ProSe Discovery

Editor’s Notes: This clause contains the description of the security for open 5G ProSe Direct Discovery and restricted 5G ProSe Direct Discovery and 5G ProSe UE-to-Network Relay Discovery.

### 6.1.1 General

### 6.1.2 Security requirements

### 6.1.3 Security procedures

## 6.2 Security for Groupcast mode 5G ProSe Direct Communication

Editor’s Notes: This clause contains the description of the security for Groupcast mode (one-to-many) 5G ProSe Direct Communication.

### 6.2.1 General

### 6.2.2 Security requirements

### 6.2.3 Security procedures

## 6.3 Security for Unicast mode 5G ProSe Direct Communication

Editor’s Notes: This clause contains the description of the security for Unicast mode (one-to-one) 5G ProSe Direct Communication.

### 6.3.1 General

### 6.3.2 Security requirements

### 6.3.3 Security procedures

## 6.4 Security for 5G ProSe UE-to-Network Relay Communication

Editor’s Notes: This clause contains the description of the security for 5G ProSe UE-to-Network Relay Communication.

### 6.4.1 General

### 6.4.2 Security requirements

### 6.4.3 Security for 5G ProSe Communication via 5G ProSe Layer-3 UE-to-Network Relay

#### 6.4.3.1 General

#### 6.4.3.2 Security procedure over User Plane

Editor’s Notes: This clause describes the security procedure that uses ProSe Key Management Function to authenticate/authorize UE during 5G ProSe UE-to-Network Relay Communication.

#### 6.4.3.3 Security procedure over Control Plane

Editor’s Notes: This clause describes the security procedure that relies on primary authentication procedure to authenticate/authorize UE during 5G ProSe UE-to-Network Relay Communication.

### 6.4.4 Security for 5G ProSe Communication via 5G ProSe Layer-2 UE-to-Network Relay

#### 6.4.4.1 General

Annex <A> (normative):
<Normative annex for a Technical Specification>

Start each annex on a new page.

Annexes are labelled A, B, C, etc. and designated either "normative" or "informative" depending on their content.

Normative annexes only to appear in Technical Specifications. Use style "Heading 8".

Annex <B> (informative):
<Informative annex for a Technical Specification>

Informative annexes may appear in both Technical Specifications and Technical Reports. Use style "Heading 8" for use in TSs.

Informative annexes shall not contain requirements for the implementation of the Technical Specification.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-10 | SA3#104e Ad-hoc | S3-213638 |  |  |  | Skeleton for this TS (approved in S3-213638 at SA3#104e Ad-hoc) | 0.0.0 |
| 2021-10 | SA3#104e Ad-hoc | S3-213639 |  |  |  | Inclusion of documents approved at SA3#104e Ad-hoc: S3-213636, S3-213637. | 0.1.0 |
|  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |