|  |
| --- |
| 3GPP TR 33.743 V0.1.0 (2024-04) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Security Aspects of Enhancement for Proximity-based Services (ProSe) in 5GS Phase 3;(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 3

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 5

3.3 Abbreviations 6

4 Overview and Security Assumptions 6

5 Key issues 7

5.1 Key issue #1: Security for multi-hop UE-to-Network Relay 7

5.1.1 Key issue details 7

5.1.2 Threats 7

5.1.3 Potential security requirements 7

5.2 Key Issue #2: Security for Multi-hop UE-to-UE Relay 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

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.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.

# 1 Scope

The present document investigates and identifies the security (including privacy) threats, corresponding security (including privacy) requirements and potential solutions for Proximity Based Services (ProSe) in 5G System (5GS) phase 3, based on the architecture and system level enhancements studied in 23.700-03 [1], including

* ProSe multi-hop UE-to-Network Relay (both Layer-2 and Layer-3 Relays).
* ProSe multi-hop UE-to-UE Relay (Layer-3 Relay only).

# 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 23.700-03: "Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS) Phase 3".

[2] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

 [3] 3GPP TS 22.261: "Service requirements for next generation new services and markets; Stage 1".

[4] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[5] 3GPP TS 33.503: " Security aspects of 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 [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 [2].

**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 [2] 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 [2].

<ABBREVIATION> <Expansion>

# 4 Overview and Security Assumptions

Based on the normative Stage-1 requirements in TS 22.261 [3] and 5G ProSe architecture principles as defined in TS 23.304 [4], TR 23.700-03 [1] aims to enhance the architecture aspects of 5G system to support multi-hop over NR PC5 reference point for Layer-2 and Layer-3 UE-to-Network Relays, and support multi-hop over NR PC5 reference point for Layer-3 UE-to-UE Relays.



Figure 4-1: Example scenario of multi-hop UE-to-Network Relay

As shown in the figure 4-1 above, the Layer-2 and Layer-3 5G ProSe multi-hop UE-to-Network Relay allow the Remote UE to communicate with the network via multi-hop Relay(s) and UE-to-Network Relay, and vice versa. While the Layer-3 5G ProSe multi-hop UE-to-UE Relay allows the End UE to communicate each other via more than one UE-to-UE relays.

Note1: 5G ProSe Intermediate Relay or 5G ProSe multi-hop UE-to-Network Relay refers to the relay participated in multi-hop U2N relaying which is located between Remote UE and UE-to-Network Relay.



Figure 4-2: Example scenario of support of Layer-3 multi-hop UE-to-UE Relay

The security architecture and procedures for 5G ProSe are specified in TS 33.503 [5]. The current mechanisms of TS 33.503 [5] cover the scenarios of "single-hop Relay" (i.e. UE-to-Network Relay and UE-to-UE Relay) and hence potential enhancements are needed for the scenarios above.

The architecture with the following security assumption:

- The architecture assumptions and principles as defined in TR 23.700-03 [1] are used as architecture assumptions in this study.

- The security architecture defined in TS 33.503 [5] is used as basis security architecture for supporting 5G ProSe security phase 3.- The security architecture needs to enable secure multi-hop UE-to-UE relay discovery and communication when the Source UE, Target UE as well as the Layer-3 UE-to-UE relay(s) can be in coverage and out of coverage.

- The security architecture needs to enable secure multi-hop UE-to-Network relay discovery and communication when the Remote UE as well as the multi-hop UE-to-Network Relay(s) can in coverage and be out of coverage.

- It is assumed that the multi-hop UE-to-Network Relay(s) and the multi-hop Layer-3 UE-to-UE relay(s) are trusted entities.

# 5 Key issues

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

## 5.1 Key issue #1: Security for multi-hop UE-to-Network Relay

### 5.1.1 Key issue details

Based on the information exchange between Remote UE and network via the UE-to-Network Relay in previous releases, the multi-hop UE-to-Network Relay scenario in TR 23.700-03 [1] further allows the Remote UE connecting to the network via one or more Intermediate Relay(s) in proximity, by using either Layer-2 or Layer-3 connection methods. The Key Issue #1 (Support of multi-hop UE-to-Network Relays) in TR 23.700-03 [1] has the following note:

*NOTE 3: Security and privacy aspects will be handled by SA WG3.*

The 5GS is supposed to be able to provide security (and privacy) protection of messages from the Remote UE, via Intermediate Relay(s) and UE-to-Network Relay, to the network and vice versa. Failure to provide security (and privacy) protection of these messages may lead to various attacks, e.g. information manipulation or information leakage. Therefore, the security and privacy aspects of the discovery and communication messages in 5G ProSe multi-hop UE-to-Network Relay should be investigated.

This key issue focuses on the security (and privacy) issues for 5G ProSe multi-hop UE-to-Network Relay over NR PC5 reference point, including both discovery and communication scenarios.

### 5.1.2 Threats

If the exchanged messages are not confidentiality protected, integrity protected or replay protected, the parameters included can be obtained, modified or replayed by an attacker. Consequently, it may lead to various attacks such as information manipulation (e.g. Relay Service Code, hop count), privacy information (e.g. Relay Service Code) leakage or unable to discover each other for an intended service.

An attacker may impersonate the Remote UE, Intermediate Relay or UE-to-Network Relay. If the authentication and authorisation of UEs cannot be verified, an attacker UE may impersonate the Remote UE, Intermediate Relay or UE-to-Network Relay.

### 5.1.3 Potential security requirements

The 5G System shall provide a means for confidentiality protection, integrity protection and replay protection of discovery and communication messages in multi-hop UE-to-Network Relay discovery and communication scenarios.

The 5G System shall provide a means for mitigating trackability and linkability attacks on UEs in multi-hop UE-to-Network Relay discovery and communication scenarios.

The 5G System shall provide a means for authentication and authorisation of the UEs in multi-hop UE-to-Network Relay communication scenarios.

The 5G system shall provide a means to securely provision the security materials for multi-hop UE-to-Network Relay discovery.

Editor’s Note: the specific E2E information, and support of E2E protection of the E2E information between the Remote UE and the UE-to-Network Relay at the last hop are FFS, the alignment with architecture aspects in SA2 need to be considered.

## 5.2 Key Issue #2: Security for Multi-hop UE-to-UE Relay

### 5.2.1 Key issue details

When a pair of 5G ProSe End UEs cannot establish PC5 communication via one Layer-3 UE-to-UE Relay, they can still communicate by transmitting their messages through multiple Layer-3 UE-to-UE Relays. These UE-to-UE Relays act as intermediate relay nodes, receiving messages from one UE and forwarding them to the next until the message reaches the intended 5G ProSe End UE. To support the multi-hop UE-to-UE Relay service, relevant solutions are studied in TR 23.700-03 [1].

The 5G System is supposed to be able to protect security (and privacy) of message exchange between End UEs, via more than one Layer-3 UE-to-UE Relays. Unsecured message exchange in multi-hop UE-to-UE Relay scenario will open vulnerability to allow different attacks such as information manipulation or privacy leakage. Thus the discovery and communication messages are needed to be protected in order to protect the security (and to preserve privacy).

Therefore, it is necessary to study how to secure the multi-hop relay discovery and communication and protect the UE privacy in the multi-hop UE-to-UE relay service.

### 5.2.2 Security threats

Failure to protect discovery messages or communication messages will open vulnerability in 5GS and allow various attacks such as modification of information (e.g. Relay Service Code, hop count), replay attack, etc.

An attacker may impersonate the End UE or multi-hop UE-to-UE Relay if the authentication and authorisation of UEs are not performed during multi-hop UE-to-UE Relay communication scenario.

Failure to protect the privacy of the involved UEs during the multi-hop UE-to-UE Relay discovery procedure or multi-hop UE-to-UE Relay communication procedure will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

### 5.2.3 Potential security requirements

The 5G System shall provide a means for confidentiality protection, integrity protection and replay protection of discovery messages and communication messages in the multi-hop UE-to-UE Relay discovery and communication scenarios.

The 5G System shall provide a means for authentication and authorization of the UEs in multi-hop UE-to-UE Relay communication scenarios.

The 5G System shall provide a means for mitigating trackability and linkability attacks on UEs in multi-hop UE-to-UE Relay discovery and communication scenarios.

The 5G system shall provide a means to securely provision the security materials for multi-hop UE-to-UE relay discovery.

## 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.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

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** |
| 2024-04 | SA3#115 Adhoc-e | S3-241321 |  |  |  | Skeleton of TR33.743 | 0.0.0 |
| 2024-04 | SA3#115 Adhoc-e | S3-241618 |  |  |  | Included changes from S3-241558, S3-241619, S3-241620 and S3-241458-r3 | 0.1.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |