|  |
| --- |
| 3GPP TR 33.743 V0.2.0 (2024-05) |
| 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 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 Overview and Security Assumptions 8

5 Key issues 9

5.1 Key issue #1: Security for multi-hop UE-to-Network Relay 9

5.1.1 Key issue details 9

5.1.2 Threats 9

5.1.3 Potential security requirements 9

5.2 Key Issue #2: Security for Multi-hop UE-to-UE Relay 10

5.2.1 Key issue details 10

5.2.2 Security threats 10

5.2.3 Potential security requirements 10

5.X Key Issue #X: <Key Issue Name> 10

5.X.1 Key issue details 10

5.X.2 Security threats 10

5.X.3 Potential security requirements 10

6 Solutions 10

6.1 Solution #1: Security for multi-hop UE-to-Network Relay using an intermediate key 11

6.1.1 Introduction 11

6.1.2 Solution details 11

6.1.2.1 Security procedure over User Plane 11

6.1.2.2 Security procedure over Control Plane 13

6.1.2.3 Key Hierarchy 13

6.1.3 Evaluation 14

6.2 Solution #2: Security of multi-hop UE-to-Network Relay discovery Model A 14

6.2.1 Introduction 14

6.2.2 Solution details 14

6.2.3 Evaluation 16

6.3 Solution #3: Security of multi-hop UE-to-Network Relay discovery Model B 16

6.3.1 Introduction 16

6.3.2 Solution details 16

6.3.3 Evaluation 18

6.4 Solution #4: Security of multi-hop UE-to-Network Relay communication 18

6.4.1 Introduction 18

6.4.2 Solution details 18

6.4.3 Evaluation 20

6.5 Solution #5: Security establishment for multi-hop UE-to-Network Relay 20

6.5.1 Introduction 20

6.5.2 Solution details 21

6.5.3 Evaluation 22

6.6 Solution #6: Security for multi-hop Layer-3 UE-to-Network Relay Communication 22

6.6.1 Introduction 22

6.6.2 Security procedure for each hop PC5 Link 22

6.6.3 Authorisation procedure for Remote UE access Network via multi-hop Relay (s) 23

6.6.3 Security procedure for 5G ProSe Multi-hop Layer-3 UE-to-Network Relay Communication with N3IWF support 24

6.6.4 Security procedure for 5G ProSe Multi-hop Layer-2 UE-to-Network Relay Communication 24

6.6.5 Evaluation 24

6.7 Solution #7: Multi-hop UE-to-network Relay discovery security procedure 24

6.7.1 Introduction 24

6.7.2 Solution details 25

6.7.2.1 Multi-hop UE-to-Network Relay Discovery security procedure with Model A 25

6.7.2.2 Multi-hop UE-to-Network Relay Discovery security procedure with Model B 26

6.7.3 Evaluation 27

6.8 Solution #8: Multi-hop UE-to-network Relay security establishment procedure 27

6.8.1 Introduction 27

6.8.2 Solution details 27

6.8.3 Evaluation 28

6.9 Solution #9: Multi-hop UE-to-Network Relay discovery security 28

6.9.1 Introduction 28

6.9.2 Solution details 28

6.9.2.1 Discovery with Model A 28

6.9.2.2 Discovery with Model B 29

6.9.3 Evaluation 31

6.10 Solution #10: Multi-hop UE-to-Network Relay communication security 31

6.10.1 Introduction 31

6.10.2 Solution details 31

6.10.3 Evaluation 32

6.11 Solution #11: Security establishment for multi-hop UE-to-UE Relay 32

6.11.1 Introduction 32

6.11.2 Solution details 32

6.11.2.1 Security mechanism with network assistance 32

6.11.2.2 Security mechanism without network assistance 33

6.11.3 Evaluation 33

6.12 Solution #12: Solution of multi-hop UE-to-UE Relay Communication 33

6.12.1 Introduction 33

6.12.2 Solution details 33

6.12.3 Evaluation 34

6.13 Solution #13: Solution of multi-hop UE-to-UE Relays Discovery Model B 34

6.13.1 Introduction 34

6.13.2 Solution details 35

6.13.3 Evaluation 37

6.14 Solution #14: Multi-hop UE-to-UE Relay discovery security 37

6.14.1 Introduction 37

6.14.2 Solution details 37

6.14.3 Evaluation 37

6.15 Solution #15: Multi-hop UE-to-UE Relay communication security 38

6.15.1 Introduction 38

6.15.2 Solution details 38

6.15.3 Evaluation 38

6.Y Solution #Y: <Solution Name> 38

6.Y.1 Introduction 38

6.Y.2 Solution details 38

6.Y.3 Evaluation 38

7 Conclusions 39

Annex A (informative): Change history 40

# 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.

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

As shown in the figure 4-2 above, the Layer-3 5G ProSe multi-hop UE-to-UE Relay allows the End UEs to communicate each other via more than one UE-to-UE relays.

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.

## 6.1 Solution #1: Security for multi-hop UE-to-Network Relay using an intermediate key

### 6.1.1 Introduction

This solution addresses "*Key issue #1: Security for multi-hop UE-to-Network Relay".*

The solution proposes to reuse mechanisms described in TS 33.503 [5], clauses 6.3.3.2 and 6.3.3.3 with the following enhancements:

* Remote UE that wishes to connect to U2N Relay via an Intermediate Relay, sends securely a PRUK ID and a new ProSe Intermediate Relay Key (PIRK), derived from (UP-PRUK or CP-PRUK), to the Intermediate Relay after PC5 link security is established between Remote UE and Intermediate Relay.
* The Intermediate Relay in direct proximity to the U2N Relay (i.e., last hop Intermediate Relay) establishes the PC5 link security based on the PIRK (i.e., derives PC5 link root key from PIRK). If not in direct proximity to the U2N, the Intermediate Relay forwards securely the PRUK ID and PIRK to the next Intermediate Relay in the path after PC5 link security is established between the Intermediate Relays.

Editor's Note: It’s FFS whether the security context for intermediate Hops can be reused for different pairs of Remote UE and U2N.

### 6.1.2 Solution details

#### 6.1.2.1 Security procedure over User Plane



Figure 6.1.2.1-1: PC5 security establishment procedure for multi-hop 5G ProSe UE-to-Network relay communication over User Plane

1. The Remote UE authorized for multi-hop discovery and communication is provisioned with U2N Relay discovery and communication parameters. Remote UE and Relays are provisioned with RSC, where RSC is configured with an indicator allowing multi-hop support indicator.
2. Remote UE sends a ProSe Remote User Key request to its PKMF. PKMF verifies that the Remote UE is authorized for U2N Relay services including via multi-hop. If the Remote UE is authorized, PKMF sends a response including UP-PRUK and UP-PRUK ID to the Remote UE as per existing provisioning mechanisms defined in TS 33.503 [5], clause 6.1.3.2.
3. The Remote UE discovers the U2N Relay via the Intermediate Relay discovery messages. It is assumed that U2N discovery is performed according to discovery solutions for KI#1.
4. The Remote UE sends a DCR message to the Intermediate Relay, including RSC, user info of U2N Relay and UP-PRUK ID.
5. The Remote UE and Intermediate Relay perform a mutual authentication using a Long-Term Credential (LTC). Alternatively, the Remote UE and Intermediate Relay can connect based on a mechanism with network assistance (based on TS 33.503 [5], clause 6.6.3.1), and skip mutual authentication in that case.

Editor's Note: how the Remote UE and Intermediate Relay performs a mutual authentication based on LTC and how LTC is provisioned is FFS.

Editor's Note: how a Remote UE and Intermediate Relay can perform the procedure in the clause 6.6.3.1 especially the CP procedure is FFS.

Editor's Note: It’s FFS whether and how security context is established for earlier hops beside the last hop.

1. The Remote UE receives a Direct Security Mode Command message from the Intermediate Relay that includes conventional security parameters (e.g., security policy, freshness parameters, etc) to initiate the PC5 link security establishment.

As the Remote UE is connecting to the U2N Relay via an Intermediate Relay, Remote UE derives a UP-PIRK using UP-PRUK and nonce1.

Remote UE sends a fully protected (encrypted, integrity, replay) Direct Security Mode Complete message to the Intermediate Relay including PIRK, nonce1.

If more than one Intermediate Relay are involved (not shown in the figure), the Intermediate Relay behave similarly to the Remote UE towards the next Intermediate Relay (except for the UP-PIRK derivation) and forwards securely the UP-PIRK to the next hop Intermediate Relay, up to the last hop Intermediate Relay.

Editor's Note: It’s FFS whether the security context for intermediate hops can be reused for different pairs of Remote UE and U2N.

1. The last hop Intermediate Relay sends a DCR message to the U2N Relay including UP-PRUK ID, RSC, U2N user info, nonce1 and a multi\_hop\_indication to indicate that the request is for a Remote UE multi-hop connection.
2. The U2N Relay sends a key request to the Remote UE PKMF via its PKMF. The request includes UP-PRUK ID, RSC, nonce1 and the multi\_hop\_indication.

If Remote UE PKMF receives a multi\_hop\_indication in the request, the Remote UE PKMF derives a UP-PIRK from UP-PRUK using nonce1 and derives a K\*NRP from UP-PIRK using RSC, and a nonce2 i.e., instead of deriving a KNRP using UP-PRUK. The corresponding key hierarchy for multi-hop U2N security is described in 6.Y.2.3.

Remote UE PKMF sends the K\*NRP and nonce2 to the U2N Relay via U2N Relay PKMF.

1. U2N Relay derives a session key using K\*NRP and security keys using the session key. U2N Relay sends a Direct Security Mode Command message integrity protected to the Intermediate Relay including nonce2.

Intermediate Relay derives K\*NRP from UP-PIRK using RSC and nonce2, the same way as Remote UE PKMF. Intermediate Relay derives a session key using K\*NRP and security keys using the session key. The Intermediate Relay verifies the security of the Direct Security Mode Command with the generated security keys. The Intermediate Relay determines that U2N Relay and Remote UE are authorized for multi-hop U2N Relay connectivity if the verification is successful.

Intermediate Relay sends a fully protected Direct Security Mode Complete message to the U2N Relay.

U2N Relay verifies the security of the Direct Security Mode Complete with the generated security keys. The U2N Relay determines that Intermediate Relay and Remote UE are authorized for multi-hop U2N Relay connectivity if the verification is successful.

1. The U2N Relay sends a DCA message to the Intermediate Relay confirming successful relayed connection.

The U2N Relay proceeds with the regular remaining steps to complete the procedure including sending UP-PRUK ID in a Remote UE Report procedure to identify the Remote UE that is using the multi-hop U2N Relay connectivity service.

The Intermediate Relay sends a DCA message to the Remote UE confirming successful establishment of multi-hop relayed connection.

#### 6.1.2.2 Security procedure over Control Plane

The security procedure over Control Plane applies the same principles as above to the mechanisms described in TS 33.503 [5], clause 6.3.3.3, with the following differences:

* If the Remote UE possesses a CP-PRUK/CP-PRUK ID from a previous direct U2N Relay connection, it uses CP-PRUK/CP-PRUK ID instead of UP-PRUK and UP-PRUK ID and derives a CP-PIRK from CP-PRUK.
* The last hop Intermediate Relay derives K\*NR\_ProSe from CP-PIRK.
* On the network side, AUSF derives CP-PIRK from CP-PRUK and K\*NR\_ProSe from CP-PIRK.

#### 6.1.2.3 Key Hierarchy



Figure 6.1.2.2-1: PC5 Key Hierarchy for multi-hop 5G ProSe UE-to-Network Relay security over User Plane (left) and Control Plane (right)

The key hierarchy for multi-hop U2N Relay (UP or CP) support shown in Figure 6.Y.2.2-1 is proposed in addition to the existing key hierarchy for single-hop connection (TS 33.503, clause 6.3.3.2.3 or 6.3.3.3.3). This key hierarchy applies when Remote UE connects to U2N via multi-hop, as follows:

* The proposed Intermediate Relay Key PIRK (respectively UP-PIRK and CP-PIRK) is derived from PRUK (respectively UP-PRUK and CP-PRUK) to enable the PC5 link security establishment between the last hop Intermediate Relay and the U2N Relay.
* PIRK is sent securely from the Remote UE to the last hop Intermediate Relay (directly or via other Intermediate Relay(s)).
* The network and last hop Intermediate Relay derive a PC5 root key (respectively K\*NRP or K\*NR\_ProSe) from the PIRK. The network sends the PC5 root key derived from PIRK to the U2N.
* K\*NRP is used instead of KNRP, and K\*NR\_ProSe instead of KNR\_ProSe for the derivation of the session key, used to derive the security keys for the connection security between the last hop Intermediate Relay and U2N relay.

### 6.1.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

## 6.2 Solution #2: Security of multi-hop UE-to-Network Relay discovery Model A

### 6.2.1 Introduction

This solution addresses key issue #1: Security for multi-hop UE-to-Network Relay.

The announcing 5G ProSe U2N and the monitoring 5G ProSe Remote UE performs protected relay discovery as specified in clause 6.3.2.3.2 of TS 23.304 [4] and clause 6.1.3.2.2.1 of TS 33.503 [5].

The intermediate U2N can relay and forward the discovery Announcement message sent by the announcing 5G ProSe U2N. The intermediate U2N can additionally insert necessary information (e.g. hop count) required to support multi-hop U2N relay in the forwarded messages.

To protect the integrity and/or confidentiality of the information inserted/updated by the intermediate U2N, the intermediate U2N needs to obtain also a set of relay discovery security material from its own HPLMN, called as intermediate relay discovery security material in this solution for brevity. So that the forwarded relay discovery message contains both original relay discovery announcement message protected by the relay discovery security material associated with the announcing U2N and also the additional information protected by the intermediate relay discovery security material associated with the intermediate U2N.

NOTE: The complete additional information (e.g. hop count) updated by the intermediate U2N that is required for multi-hop U2N relay discovery is to be defined by SA2.

NOTE: There could be one or more intermediate U2Ns in the discovery message path. The maximum number of intermediate U2N(s) in the path is to be defined by SA2. This solution shows only two intermediate U2Ns as example.

Editor’s Note: How to retrieve the corresponding relay discovery security material and the intermediate relay discovery security material is FFS.

Editor’s Note: How the solution protects the path information during the discovery of multi-hop U2N relay is FFS.

Editor’s Note: The reason for the two sets of security material and additional information protection based on intermediate relay discovery security materials is FFS.

### 6.2.2 Solution details

The security procedure for multiple hop 5G ProSe UE-to-Network Relay Discovery with Model A is described as follows.



Figure 6.2.2-1: Example Model A Discovery operation supporting multi-hop UE-to-Network Relay

0a. The announcing 5G ProSe U2N is provisioned with the relay discovery security materials from its HPLMN as specified in clause 6.1.3.2.2.1 of TS 33.503[5].

The intermediate 5G ProSe U2N(s) and the remote UE are provisioned with the relay discovery security materials associated with announcing U2N as Monitoring UE as specified in clause 6.1.3.2.2.1 of TS 33.503[5].

NOTE: The intermediate U2N needs to be provisioned with U2N discovery security material to understand RSC being announced by the Announcing U2N.

0b. The 5G ProSe intermediate U2N UE (e.g. U2N #1, U2N #2) is also provisioned with the intermediate relay discovery security material used for protection of the forwarded announcement message from its own HPLMN, acting as announcing UE as specified in clause 6.1.3.2.2.1 of TS 33.503 [5].

The 5G ProSe intermediate U2N and the remote UE are also provisioned with the intermediate relay discovery security materials associated with the neighbouring intermediate U2Ns, acting as Monitoring UE as specified in clause 6.1.3.2.2.1 of TS 33.503 [5].

1. The announcing U2N reuses the 5G ProSe UE-to-Network Relay Discovery Announcement message as specified in clause 6.1.3.2.2.1 of TS 33.503 [5] with the additional information (e.g. hop count) required for multi-hop U2N relay and protects the message with relay discovery security material obtained from step 0a.
2. The intermediate U2N #1 receives the protected announcement message, obtains the RSC and verifies the Announcement message based on the relay discovery security material associated with the announcing U2N obtained from step 0a. If the verification is successful, the intermediate U2N #1 updates the hop information (e.g. hop count) and forwards the original Announcement message with the additional information (e.g. updated hop count). The forwarded message is protected by the intermediate relay discovery security material that the intermediate U2N #1 obtained from its HPLMN from step 0b.
3. The intermediate U2N #2 received the protected message, obtains the RSC and verifies the original Announcement message based on the relay discovery security material associated with the announcing U2N obtained from step 0a and the additional information based on intermediate relay discovery security material associated with the intermediate U2N #1 which was obtained from step 0b. If the verification is successful, the intermediate U2N #2 updates the hop information (e.g. hop count) and forwards the original Announcement message with the additional information (e.g. updated hop count). The forwarded message is protected by the intermediate relay discovery security material that the intermediate U2N #2 obtained from its HPLMN from step 0b.

4. On receiving the Announcement message from the intermediate U2N #2 , the monitoring 5G ProSe Remote UE verifies the received Announcement message using the relay discovery security material associated with the announcing U2N obtained from step 0a and the additional information based on intermediate relay discovery security material associated with the intermediate U2N #2 which was obtained from step 0b. If the verification is successful, the monitoring 5G ProSe Remote UE shall process the relay announcement message as specified in clause 6.1.3.2.2.1 of TS 33.503[5].

### 6.2.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

## 6.3 Solution #3: Security of multi-hop UE-to-Network Relay discovery Model B

### 6.3.1 Introduction

This solution addresses key issue #1: Security for multi-hop UE-to-Network Relay.

The discoveree 5G ProSe U2N and the discoverer 5G ProSe Remote UE performs protected relay discovery as specified in clause 6.3.2.3.3 of TS 23.304[4] and clause 6.1.3.2.2.2 of TS 33.503[5].

The intermediate U2N can relay and forward the discovery Solicitation/Response messages sent by the discoveree 5G ProSe U2N and the discoverer 5G ProSe Remote UE. The intermediate U2N can additionally insert necessary information (e.g. hop count) required to support multi-hop U2N relay in the forwarded messages.

To protect the integrity and/or confidentiality of the information inserted/updated by the intermediate U2N, the intermediate U2N needs to obtain also a set of relay discovery security material from its own HPLMN, called as intermediate relay discovery security material in this solution for brevity. So that the forwarded relay discovery messages contain both original relay discovery Solicitation/Response message protected by the relay discovery security material associated with the discoveree U2N and also the additional information protected by the intermediate relay discovery security material associated with the intermediate U2N.

NOTE: The complete additional information (e.g. hop count) updated by the intermediate U2N that is required for multi-hop U2N relay is to be defined by SA2.

NOTE: There could be one or more intermediate U2Ns in the discovery message path. The maximum number of intermediate U2N(s) in the path is to be defined by SA2. This solution shows only two intermediate U2Ns as example.

Editor’s Note: How to retrieve the corresponding relay discovery security material and the intermediate relay discovery security material is FFS.

Editor’s Note: How the solution protects the path information during the discovery of multi-hop U2N relay is FFS.

Editor’s Note: The reason for the two sets of security material and additional information protection based on intermediate relay discovery security materials is FFS.

### 6.3.2 Solution details

The security procedure for multiple hop 5G ProSe UE-to-Network Relay Discovery with Model B is described as follows.



Figure 6.2.2-1: Example Model B Discovery operation supporting multi-hop UE-to-Network Relay

0a. The discoveree 5G ProSe U2N is provisioned with the relay discovery security materials from its HPLMN as specified in clause 6.1.3.2.2.2 of TS 33.503[5].

The intermediate 5G ProSe U2N(s) and the remote UE are provisioned with the relay discovery security materials associated with discoveree U2N as discoverer UE as specified in clause 6.1.3.2.2.2 of TS 33.503[5].

NOTE: The intermediate U2N needs to be provisioned with U2N discovery security material to understand RSC being discovered.

0b. The 5G ProSe intermediate U2N UE (e.g. U2N #1, U2N #2) is also provisioned with the intermediate relay discovery security material used for protection of the forwarded discovery Solicitation/Response messages from its own HPLMN, acting as discoveree UE as specified in clause 6.1.3.2.2.2 of TS 33.503[5].

The 5G ProSe intermediate U2N, the discoveree 5G ProSe U2N and the remote UE are also provisioned with the intermediate relay discovery security materials associated with the neighbouring intermediate U2Ns, acting as discoverer UE as specified in clause 6.1.3.2.2.2 of TS 33.503[5].

1. The discoverer Remote UE reuses the 5G ProSe UE-to-Network Relay Discovery Solicitation message as specified in clause 6.1.3.2.2.2 of TS 33.503[5] with the additional information (e.g. hop count) required for multi-hop U2N relay and protects the message with relay discovery security material obtained from step 0a.
2. The intermediate U2N #1 receives the protected Relay Discovery Solicitation message, obtains the RSC and verifies the Relay Discovery Solicitation message based on the relay discovery security material associated with the discoveree U2N obtained from step 0a. If the verification is successful, the intermediate U2N #1 updates the hop information (e.g. hop count) and forwards the original Relay Discovery Solicitation message with the additional information (e.g. updated hop count). The forwarded message is protected by the intermediate relay discovery security material that the intermediate U2N #1 obtained from its HPLMN from step 0b.
3. The intermediate U2N #2 received the protected message, obtains the RSC and verifies the original Relay Discovery Solicitation message based on the relay discovery security material associated with the discoveree U2N obtained from step 0a and the additional information based on intermediate relay discovery security material associated with the intermediate U2N #1 which was obtained from step 0b. If the verification is successful, the intermediate U2N #2 updates the hop information (e.g. hop count) and forwards the original Relay Discovery Solicitation message with the additional information (e.g. updated hop count). The forwarded message is protected by the intermediate relay discovery security material that the intermediate U2N #2 obtained from its HPLMN from step 0b.
4. On receiving the Relay Discovery Solicitation message from the intermediate U2N #2 , the discoveree 5G ProSe U2N verifies the received Relay Discovery Solicitation message using the relay discovery security material associated with the discoveree U2N obtained from step 0a and the additional information based on intermediate relay discovery security material associated with the intermediate U2N #2 which was obtained from step 0b. If the verification is successful, the discoveree 5G ProSe U2N shall process the Relay Discovery Solicitation message as specified in clause 6.1.3.2.2.2 of TS 33.503[5].

 The discoveree U2N reuses the 5G ProSe UE-to-Network Relay Discovery Response message as specified in clause 6.1.3.2.2.2 of TS 33.503[5] with the additional information (e.g. hop count) required for multi-hop U2N relay and protects the message with relay discovery security material obtained from step 0a and additionally with the intermediate relay discovery security material associated with the intermediate U2N #2 which was obtained from step 0b.

1. The intermediate U2N #2 verfies the protected Relay Discovery Response message and forward the message with the updated additional information and protect the forwarded message with the intermediate relay discovery security material that the intermediate U2N #2 obtained from its HPLMN from step 0b, same as step 3.
2. The intermediate U2N #1 verfies the protected Relay Discovery Response message and forward the message with the updated additional information and protect the forwarded message with the intermediate relay discovery security material that the intermediate U2N #1 obtained from its HPLMN from step 0b, same as step 2.

8. On receiving the Relay Discovery Response message from the intermediate U2N #1 , the discoverer 5G ProSe Remote UE verifies the received Relay Discovery Response message using the relay discovery security material associated with the discoveree U2N obtained from step 0a and the additional information based on intermediate relay discovery security material associated with the intermediate U2N #1 which was obtained from step 0b. If the verification is successful, the discoverer 5G ProSe Remote UE shall process the Relay Discovery Response message as specified in clause 6.1.3.2.2.2 of TS 33.503[5].

### 6.3.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

## 6.4 Solution #4: Security of multi-hop UE-to-Network Relay communication

### 6.4.1 Introduction

This solution addresses key issue #1: Security for multi-hop UE-to-Network Relay.

Each hop of multi-hop UE-to-Network Relay communication (e.g. between Remote UE and intermediate UE-to-Network Relay, between target UE-to-Network Relay and intermediate UE-to-Network Relay, or between two intermediate UE-to-Network Relays) performs PC5 link security establishment procedure and sets up PC5 security context, reusing the methods as specified in clause 6.6.3 of TS 33.503[5].

Once hop-by-hop security for PC5 link establishment has been performed, the Remote UE and the target UE-to-Network Relay triggers e2e security between them, reusing the security methods (UP based or CP based solution) as specified in clause 6.3.3 of TS 33.503[5]. The signaling of the selected security method is overlay over the secured PC5 link of each hop.

NOTE: There could be one or more intermediate UE-to-Network Relays in the discovery message path. The maximum number of intermediate UE-to-Network Relays in the path is to be defined by SA2. This solution shows only one intermediate UE-to-Network Relay as example.

### 6.4.2 Solution details

The security procedure for multi-hop 5G ProSe UE-to-Network Relay communication is described as follows.



Figure 6.4.2-1: Security for multi-hop UE-to-Network Relay communication

0. The 5G ProSe Remote UE, the intermediate UE-to-Network Relay(s) and the target 5G ProSe UE-to-Network Relay sets up hop by hop PC5 link security, reusing the methods as specified in clause 6.6.3 of TS 33.503[5].

 After this procedure, secured PC5 transport messages can be exchanged between PC5 links of each hop and protected by the PC5 link security context of each hop.

1. The 5G ProSe Remote UE is to set up e2e security with the target 5G ProSe UE-to-Network Relay and chooses a security method to be used (i.e. UP based or CP based solution). The 5G ProSe Remote UE forms U2N security container to be sent to the target 5G ProSe UE-to-Network Relay over intermediate UE-to-Network Relay(s) , which contains Direct Communication Request (DCR) messages that contains the UP-PRUK ID/CP-PRUK ID or SUCI, RSC and freshness parameter Nonce\_1, as specified in clause 6.3.3.2.2 or clause 6.3.3.2.3 of TS 33.503[5]. The 5G ProSe Remote UE protects U2N security container using the relay discovery security material associated with the target 5G ProSe UE-to-Network Relay, by reusing the protection method as specified in clause 6.3.5 of TS 33.503[5].

The 5G ProSe Remote UE sends the U2N security container and possible other additional information (e.g. hop counter) required for multi-hop UE-to-Network Relay over a secured PC5 transport message to the intermediate UE-to-Network Relay.

NOTE: The content of possible additional information (e.g. hop count) that is required for multi-hop UE-to-Network relay is to be defined by SA2.

1. The intermediate UE-to-Network Relay forwards the secured transport PC5 message to the target 5G ProSe UE-to-Network Relay.
	1. The target UE-to-Network Relay performs UP based solution (step 4 of clause 6.3.3.2.2 TS 33.503[5]) or CP based solution (step 3-13 of clause 6.3.3.3.2 TS 33.503[5]). The messages, if available, exchanged between the Remote UE and the target 5G ProSe UE-to-Network Relay are sent within the U2N security container over secured PC5 transport messages via PC5 link of each hop.
2. The 5G ProSe Remote UE and the target 5G ProSe UE-to-Network Relay performs Direct Security Mode Command procedure as specified in UP based solution (step 5 of clause 6.3.3.2.2 TS 33.503[5]) or CP based solution (step 14-17 of clause 6.3.3.3.2 TS 33.503[5]). The messages exchanged between the Remote UE and the target 5G ProSe UE-to-Network Relay are sent within the U2N security container over secured PC5 transport messages via PC5 link of each hop.

Successful verification of the Direct Security Mode Command assures the 5G ProSe Remote UE that the 5G ProSe UE-to-Network Relay is authorized to provide the relay service. Successful verification of the Direct Security Mode Complete message assures the 5G ProSe UE-to-Network Relay that the 5G ProSe Remote UE is authorized to get the relay service.

* 1. After successful verification, PC5 security context is also set up between the Remote UE and the target 5G ProSe UE-to-Network Relay. The 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message within U2N security container over secured PC5 transport messages via PC5 link of each hop. The U2N security container is protected by the PC5 security context between the Remote UE and the target 5G ProSe UE-to-Network Relay.
1. The Remote UE and the target 5G ProSe UE-to-Network Relay perform the rest of the UE-to-Network relay procedure, such as establishing a new PDU session or modifying an existing PDU session for relaying if needed or performing Remote UE Report etc, as specified in clause 6.3.3.2.2 and clause 6.3.3.2.3 of TS 33.503[5].

Editor’s Note: This solution needs to be aligned with SA2 conclusion.

Editor’s Note: Whether the E2E security between the Remote UE and the target 5G ProSe UE-to-network Relay needs to be set up is FFS.

### 6.4.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

## 6.5 Solution #5: Security establishment for multi-hop UE-to-Network Relay

### 6.5.1 Introduction

This solution addresses Key Issue #1: Security for multi-hop UE-to-Network Relay, aiming to provide a method to establish security between UEs in the multi-hop UE-to-Network (U2NW) Relay scenario.



In this solution, each of the Intermediate Relay needs to establish secured PC5 link with the node (Intermediate Relay or the U2NW Relay) in the next hop before it can serve the Remote UE. This solution is based on the following terminologies and assumptions:

* The term ‘Intermediate Relay’ in this solution refers to the relays located between the Remote UE and the U2NW Relay, while the U2NW Relay is the node which connects to the network.
* The hops are counted based on the path from the Remote UE to the U2NW Relay, i.e. the Intermediate Relay that connects to the Remote UE is assumed as the first hop of the multi-hop connection, while the U2NW Relay locates at the last hop.
* The ‘next hop’ of a node (i.e. Remote UE, Intermediate Relay or U2NW Relay) refers to the neighbour node facing to the network side, while the ‘previous hop’ refers to the neighbour node facing to the Remote UE side.
* The Remote UE and the Intermediate Relay in this solution can locate of network coverage, the U2NW Relay in this solution is required to be covered by the network.

### 6.5.2 Solution details



Figure 6.5.2-1: Example multi-hop U2NW Relay security establishment procedures

Each of the Intermediate Relay needs to establish secured PC5 link with the node (Intermediate Relay or the U2NW Relay) in the next hop before it can serve the Remote UE.

0. The multi-hop relay discovery procedure to discover the involvers, including the Remote UE, the Intermediate Relay(s) and the U2NW Relay.

1. After the multi-hop Relay discovery procedure, the Remote UE initiate the Direct Communication Request (DCR) message (i.e. DCR-1 on the figure) to request the security establishment between the intermediate relay in the next hop, including the RSC, CP/UP-PRUK ID or SUCI of the Remote UE as defiend in clause 6.3 of TS 33.503 [5].

2a-2b. The Intermediate Relay receives the DCR-1 and temporarily stores the DCR-1. The Intermediate Relay initiates another DCR (i.e. DCR-2 on the figure) to establish security establishment between the next hop node. When establishing the secured link between the next hop, the Intermediate Relay takes the role of a Remote UE and the DCR-2 includes the RSC, CP/UP-PRUK ID or SUCI of the Intermediate UE as defiend in clause 6.3 of TS 33.503 [5].

3. The Intermediate Relay and the U2NW Relay follow the procedures in 6.3 of TS 33.503 [5] to establish the secured PC5 link.

4-5. The Intermediate Relay uses the protected PC5 link established in step 3 to send intermediate key request message including the temporarily stored parameters in DCR-1. Based on the existing U2NW Relay security mechanism (i.e. steps 4a-4e of 6.3.3.2.2 or steps 3-13 of 6.3.3.3.2 of TS 33.503 [5]), the U2NW Relay uses the parameters in the Intermediate Key Request to interact with the network, in order to get the KNR\_ProSe/KNRP and freshness parameter to set up connection with the Remote UE.

NOTE: If more than one Intermediate Relays in the path, each Intermediate Relay needs to store the DCR message from its previous hop and establish secured link between its next hop. The parameters in the stored DCR message are sent to the next hop after the secured link is established. The secured link is also used to receive security parameters from next hop to set up security with previous hop.

Editor’s Note: It’s FFS how security is established between Remote UE and Intermediate Relay when there are more than one Intdermediate Relays.

6-7. The KNR\_ProSe/KNRP and freshness parameter are contained in the Intermediate Key Response and sent to the Intermediate Relay via the protected PC5 channel established in step 3. The Remote UE and the Intermediate Relay use existing mechanism to finish security link setup.

Editor’s Note: It’s FFS whether step 4/6 can interact with network directly when Intermediate Relay has network coverage.

Editor’s Note: It’s FFS whether and how Intermediate Relays are authorised to get KNR\_ProSe/KNRP.

Editor’s Note: It’s FFS whether step 4/6 are needed with UP-based solution.

8. The rest multi-hop U2NW communication procedures.

### 6.5.3 Evaluation

TBD.

## 6.6 Solution #6: Security for multi-hop Layer-3 UE-to-Network Relay Communication

### 6.6.1 Introduction

This solution addresses security requirements for communication scenarios in Key Issue #1 (as defined in clause 5.1) .



Figure 6-6: Example scenario of multi-hop UE-to-Network Relay

Security procedure for each hop PC5 Link as described in clause 6.6.2.

Authorisation procedure for Remote UE access Network via multi-hop Relay (s) as described in clause 6.6.3.

Security procedure for 5G ProSe Multi-hop Layer-3 UE-to-Network Relay Communication with N3IWF support as described in clause 6.6.4.

Security procedure for 5G ProSe Multi-hop Layer-2 UE-to-Network Relay Communication as described in clause 6.6.5.

Editor’s Note: Whether the authorisation procedure need is FFS.

Editor’s Note: How to authorize the intermediate relay in the multi-hop U2N scenario is FFS.

### 6.6.2 Security procedure for each hop PC5 Link

The security procedure with or without network assistance in clause 6.6.3 of TS 33.503 [5] is used to establish a secure PC5 link between the Remote UE and the intermediate Relay, the intermediate Relay and the intermediate Relay, the intermediate Relay and the UE-to-Network Relay.

Editor’s Note: Whether UP based and CP based PC5 security procedure as specified in clause 6.3.3 of TS 33.503[5] can be reused is FFS.

### 6.6.3 Authorisation procedure for Remote UE access Network via multi-hop Relay (s)



1. The hop-by-hop PC5 security has been established as described in clause 6.6.2.

1. The Remote UE sends a Multi-hop Communication Request to the UE-to-Network Relay via one or more Intermediate Relay, which includes information about the selected path, the SUCI or UP-/CP-PRUK ID of Remote UE, RSC and freshness\_parameter\_1.

2. Upon receiving the Multi-hop Communication Request from the remote UE via one or more Intermediate Relay, the UE-to-Network Relay perform the security procedure with network assistance as specified in step 4 of clause 6.3.3.2.2 of TS 33.503 [y] or step 3 to step 13 in clause 6.3.3.3.2 of TS 33.503 [5].

Editor’s Note: Whether UP based and CP based PC5 security procedure as specified in clause 6.3.3 of TS 33.503[5] can be reused is FFS.

3. The 5G ProSe UE-to-Network Relay shall derive the session key from KNRP/KNR\_ProSe and then derive the confidentiality key (if applicable) and integrity key. The 5G ProSe UE-to-Network Relay shall sends a Authorization Check Request message to the 5G ProSe Remote UE via one or more Intermediate Relay. This message shall also include the freshness Parameter 2 and shall be protected by integrity key.

4. Upon receiving the Authorization Check Request message, the Remote UE shall derive the KNRP/KNR\_ProSe from UP-/CP-PRUK. It shall then derive the session key and the confidentiality key (if applicable) and integrity key and process the Authorization Check Request message. Successful verification of the Authorization Check Request message assures the Remote UE that the UE-to-Network Relay is authorized to provide the Multi-hop U2N Relay service.

5. The Remote UE responds with a Authorization Check Response message to 5G ProSe UE-to-Network Relay via one or more Intermediate Relay if successfully verified the Authorization Check Request message. The Authorization Check Response message shall be protected by integrity key and confidentiality key (if applicable).

6. Upon receiving the Authorization Check Response message, the UE-to-Network Relay shall verify the this message. Successful verification of the Authorization Check Response message assures the 5G ProSe UE-to-Network Relay that the 5G ProSe Remote UE is authorized to get the Multi-hop U2N Relay service.

7. After the successful verification of the Authorization Check Response message, the 5G ProSe UE-to-Network Relay responds a Multi-hop Communication Accept message to the 5G ProSe Remote UE via one or more Intermediate Relay to finish the Multi-hop Communication establishment procedures. The Multi-hop Communication Accept message shall be protected by integrity key and confidentiality key (if applicable).

Editor’s Note: Whether the session key between the remote UE and U2N relay is used for security protection is FFS.

NOTE: The Multi-hop Communication Request/Accept message and Authorization Check Request/Response message are transmitted between the Remote UE and the UE-to-Network Relay over hop-by-hop PC5 link.

### 6.6.3 Security procedure for 5G ProSe Multi-hop Layer-3 UE-to-Network Relay Communication with N3IWF support

The 5G ProSe Layer-3 Remote UE selects N3IWF and performs the security procedures as specified in clause 7.2.1 of TS 33.501 [z].

NOTE: The N3IWF selects methods will be specified by SA2.

### 6.6.4 Security procedure for 5G ProSe Multi-hop Layer-2 UE-to-Network Relay Communication

The 5G ProSe Remote UE and NG-RAN node shall establish AS security as specified in TS 33.501 [z].

### 6.6.5 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

## 6.7 Solution #7: Multi-hop UE-to-network Relay discovery security procedure

### 6.7.1 Introduction

This solution is proposed to address Key Issue #1, which provides a method by which the Remote UE can securely discover the UE-to-network Relay via one or multiple Intermediate Relays.

For the multi-hop UE-to-Network Relay discovery, in addition to protecting the discovery message by reusing the UE-to-network Relay discovery security mechanism defined in TS 33.503 [5], the involved UE also needs to ensure the trustworthiness of path information before updating the stored record or forwarding the discovery message.

This is because the attacker can launch the replay attack by re-sending the detected discovery message, which may distort the real path information maintained by the Remote UE and Intermediate Relay. For example, the discovery message is captured by the attacker at Time 1 in location A. The attacker can re-send this discovery message at Time 2 (Time 2 is sufficiently close to Time 1) in location B. Once receiving the discovery message, the UE in location B supporting multi-hop UE-to-network relay service can successfully verify this message and forward it to all the UEs in proximity in location B, resulting in the failure of multi-hop UE-to-network relay discovery.

The path information verification can be achieved by authenticating the UE sent the discovery message, i.e. only if the link can be securely established, the UE received the discovery message can trust the included path information and forward this message during the multi-hop UE-to-network Relay discovery.

Editor’s Note: The need for Intermediate Relay to obtain the discovery security materials associated with its HPLMN and multiple sets of discovery security materials associated with the HPLMN of potential UE-to-network Relay(s)/Intermediate Relay(s) is FFS.

### 6.7.2 Solution details

#### 6.7.2.1 Multi-hop UE-to-Network Relay Discovery security procedure with Model A



Figure 6.7.2.1-1: Security procedure for multi-hop UE-to-Network Relay Discovery with Model A

0. The discovery security materials provisioning procedure for 5G ProSe UE-to-network Discovery defined in TS 33.503 [5] is reused for multi-hop UE-to-network relay discovery.

The UE-to-network Relay obtains the discovery security materials associated with its HPLMN. The Intermediate Relay obtains the discovery security materials associated with its HPLMN, and multiple sets of discovery security materials associated with the HPLMN of potential UE-to-network Relay(s)/Intermediate Relay(s). The Remote UE obtains multiple sets of discovery security materials associated with the HPLMN of potential UE-to-network Relay(s)/Intermediate Relay(s).

1. The UE-to-network Relay broadcasts the announcement message, which is protected by the discovery security materials associated with the RSC and its HPLMN ID.
2. The Intermediate Relay1 verifies the announcement message by using the discovery security material associated with the PLMN ID of UE-to-network Relay and RSC.

If the verification is passed, the Intermediate Relay1 determines whether to broadcast the announcement message for multi-hop UE-to-Network Relay based on the following principles:

* Whether the criteria defined in TR 23.700-03 [1] can be met or not, e.g. if the Hop-count value is smaller than the Hop-Limit value or not, if the Hop-Count value is smaller than the stored value in the record or not, etc.
* Whether the secure link between the announcing UE and monitoring UE can be established or has been established, e.g. whether the Intermediate Relay1 can successfully establish the link with the UE-to-network Relay by reusing the link establishment procedure defined in TS 33.503 [5] when there is no connection.

Editor’s Note: The need for Intermediate Relay to establish a link whenever an announcement is received is FFS and is to be aligned with SA2.

1. If the above principles are met, the Intermediate Relay1 broadcasts the announcement message, which is protected by the discovery security materials associated with the RSC and its HPLMN ID.
2. The Intermediate Relay2 verifies the announcement message and determines whether to forward it as step #2. If there is no connection between the Intermediate Relay2 and Intermediate Relay1, the Intermediate Relay2 initiates the link establishment procedure as defined in TS 33.503 [5].
3. Once the link is securely established, the Intermediate Relay2 broadcasts the protected announcement message.
4. The Remote UE may select one of the Intermediate Relay based on the received announcement message. For the selected Intermediate Relay, the Remote UE initiates the link establishment procedure. Only if the link is securely established, the Remote UE can initiate the communication establishment procedure with the UE-to-network Relay via the selected Intermediate Relay.

Editor’s Note: It is FFS whether the communication establishment between the Remote UE and the U2N relay is needed.

#### 6.7.2.2 Multi-hop UE-to-Network Relay Discovery security procedure with Model B



Figure 6.7.2.2-1: Security procedure for multi-hop UE-to-Network Relay Discovery with Model B

0. The discovery security materials provisioning procedure for 5G ProSe UE-to-network Discovery defined in TS 33.503 [5] is reused for multi-hop UE-to-network Relay discovery.

The Remote UE, Intermediate Relay, and UE-to-network Relay obtains the discovery security materials associated with its HPLMN, and multiple sets of discovery security materials associated with the HPLMN of potential UE-to-network Relay(s)/Intermediate Relay(s).

1. The Remote UE broadcasts the solicitation message, which is protected by the discovery security materials associated with the RSC and its HPLMN ID.
2. The Intermediate Relay verify the solicitation message by using the discovery security material associated with the PLMN ID of Remote UE and RSC. If the verification is passed, the Intermediate Relay further broadcasts the solicitation message, which is protected by the discovery security materials associated with the RSC and its HPLMN ID.
3. The UE-to-network Relay verifies the solicitation message and sends the response message.
4. Once receiving the response message, the Intermediate Relay verifies it by using the corresponding discovery security materials, and determines whether to forward the response message based on the following principles:
* Whether the criteria defined in TR 23.700-03 [1] can be met or not, e.g. if the Hop-count value is smaller than the Hop-Limit value or not, if the Hop-Count value is smaller than the stored value in the record or not, etc.
* Whether the secure link between the Intermediate Relay and UE-to-network Relay can be established or has been established, e.g. whether the Intermediate Relay1 can successfully establish the link by reusing the link establishment procedure defined in TS 33.503 [5] when there is no connection.
1. If the above principles are met, the Intermediate Relay sends the response message, which is protected by the discovery security materials associated with the RSC and its HPLMN ID.
2. The Remote UE may select one of the Intermediate Relay based on the received response message. For the selected Intermediate Relay, the Remote UE initiates the link establishment procedure. Only if the link is securely established, the Remote UE can initiate the communication establishment procedure with the UE-to-network relay via the selected Intermediate Relay.

### 6.7.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

## 6.8 Solution #8: Multi-hop UE-to-network Relay security establishment procedure

### 6.8.1 Introduction

This solution is proposed to address Key Issue #1, which provides a method by which the Remote UE can securely establish the communication with the UE-to-network Relay via one or multiple Intermediate Relay(s).

In this solution, it is assumed that the security of each hop (i.e. the link between the Remote UE and Intermediate Relay1, the link between the Intermediate Relay1 and Intermediate Relay2, the link between the Intermediate Relay2 and UE-to-network Relay) has been established during the multi-hop UE-to-network Relay discovery procedure.

For establishing the security for multi-hop UE-to-network Relay communication, the DCR message is sent by the Remote UE and is transmitted over the secure link. Once receiving the DCR message, the UE-to-network Relay can perform the Remote UE report procedure as defined in TS 33.503 [5].

### 6.8.2 Solution details



Figure 6.8.2-1: Security establishment procedure for multi-hop UE-to-network Relay communication

1. The Remote UE can securely discover the UE-to-network Relay by performing the multi-hop UE-to-network Relay discovery procedure.

It is assumed the final path selected by the Remote UE is Remote UE – Intermediate Relay1 – Intermediate Relay2 – UE-to-network Relay, and the security of each hop (i.e. the link between the Remote UE and Intermediate Relay1, the link between the Intermediate Relay1 and Intermediate Relay2, the link between the Intermediate Relay2 and UE-to-network Relay) has been established by reusing the existing procedure defined in TS 33.503 [5].

1. The Remote UE sends the DCR message, which may include RSC, user info ID of Remote UE, etc. The DCR message is transmitted over the secure link between the Remote UE and Intermediate Relay1.
2. The Intermediate Relay1 forwards the DCR message, which may include RSC, user info ID of Remote UE, etc. The DCR message is transmitted over the secure link between the Intermediate Relay1 and Intermediate Relay2.
3. The Intermediate Relay2 forwards the DCR message, which may include RSC, user info ID of Remote UE, etc. The DCR message is transmitted over the secure link between the Intermediate Relay2 and UE-to-Network Relay.
4. The UE-to-network Relay may establish the End-to-End security by reusing the UE-to-network Relay communication procedure defined in TS 33.503 [5]. The UE-to-network Relay returns the DCA message to the Remote UE via the Intermediate Relay(s).

Editor’s Note: Whether the E2E security is needed is FFS.

Editor’s Note: How to authorize the Remote UE, Intermediate Relay and UE-to-Network relay in the multi-hop UE-to-network relay scenario is FFS.

1. The UE-to-network Relay sends the Remote UE report to the SMF of Relay UE.

Editor's Note: whether this procedure is aligned with SA2 is FFS.

### 6.8.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

## 6.9 Solution #9: Multi-hop UE-to-Network Relay discovery security

### 6.9.1 Introduction

This solution addresses the first, second and fourth security requirements in the key issue #1 regarding the multi-hop UE-to-Network (U2N) Relay discovery. This solution proposes to reuse the security procedure for 5G ProSe UE-to-Network Relay discovery with Model A and Model B as specified in clause 6.3 of TS 33.503 [5]. In addition, it is proposed to mandate the integrity protection of discovery messages as the messages contain information related to path selection (e.g., hop count indicating the number of hops to reach the 5G ProSe UE-to-Network Relay). The proposed security procedure is based on the multi-hop UE-to-Network Relay discovery procedures in several solutions (e.g., solution #1, #2, and #7) of TR 23.700-03 [1].

### 6.9.2 Solution details

#### 6.9.2.1 Discovery with Model A

The security procedure for multi-hop UE-to-Network Relay discovery with Model A is shown in Figure 6.9.2.1-1.



Figure 6.9.2.1-1: Model A Discovery operation supporting multi-hop UE-to-Network Relay

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay are provisioned with the discovery security materials associated with an RSC based on the procedure specified in clause 6.3 of TS 33.503 [5]. The discovery security materials contain a Discovery User Integrity Key (DUIK) for the integrity protection of Relay Discovery Announcement.

 Editor’s Note: Which HPLMN provision the discovery security materials associated with RSC to the Remote UE, Intermediate Relay and UE-to-Network Relay is FFS.

1. The 5G ProSe UE-to-Network Relay protects a Relay Discovery Announcement using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the 5G ProSe UE-to-Network Relay broadcasts the Relay Discovery Announcement.

2. The Intermediate UE-to-Network Relay processes the received Relay Discovery Announcement message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. If the processing is successful, the Intermediate UE-to-Network Relay updates the path information (e.g., hop count, Relay Info.) and protects the updated message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the Intermediate UE-to-Network Relay broadcasts the message.

Editor’s Note: How the solution protects the path information during the discovery of multi-hop U2N relay is FFS.

3. Upon receiving the Relay Discovery Announcement message from the Intermediate UE-to-Network Relay, the 5G ProSe Remote UE processes the received message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5].

#### 6.9.2.2 Discovery with Model B

The security procedure for multi-hop UE-to-Network Relay discovery with Model B is shown in Figure 6.9.2.2-1.



Figure 6.9.2.2-1: Model B Discovery operation supporting multi-hop UE-to-Network Relay

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay are provisioned with the discovery security materials associated with an RSC based on the procedure specified in clause 6.3 of TS 33.503 [5]. The discovery security materials contain a Discovery User Integrity Key (DUIK) for the integrity protection of Relay Discovery Solicitation and Relay Discovery Response.

1. The 5G ProSe Remote UE protects a Relay Discovery Solicitation using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the 5G ProSe Remote UE broadcasts the Relay Discovery Solicitation.

2. The Intermediate UE-to-Network Relay processes the received Relay Discovery Solicitation using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. If the processing is successful, the Intermediate UE-to-Network Relay updates the path information (e.g., hop count) and protects the updated message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the Intermediate UE-to-Network Relay broadcasts the message.

3. Upon receiving the Relay Discovery Solicitation from the Intermediate UE-to-Network Relay, the 5G ProSe UE-to-Network Relay processes the received message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. If the processing is successful, the 5G ProSe UE-to-Network Relay constructs a Relay Discovery Response and protects it using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5].

 The 5G ProSe UE-to-Network Relay replies to the Intermediate UE-to-Network Relay with the Relay Discovery Response.

4. Upon receiving the Relay Discovery Response from the 5G ProSe UE-to-Network Relay, the Intermediate UE-to-Network Relay processes the received message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. If the processing is successful, the Intermediate UE-to-Network Relay updates the path information (e.g., hop count) and protects the updated message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the Intermediate UE-to-Network Relay replies to the 5G ProSe Remote UE with the message.

5. Upon receiving the Relay Discovery Response from the Intermediate UE-to-Network Relay, the 5G ProSe Remote UE processes the received message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5].

### 6.9.3 Evaluation

TBD

## 6.10 Solution #10: Multi-hop UE-to-Network Relay communication security

### 6.10.1 Introduction

This solution addresses the first, second and third security requirements in the key issue #1 regarding the multi-hop UE-to-Network (U2N) Relay communication. This solution proposes to reuse the security procedure over User Plane for PC5 security establishment for each hop among 5G ProSe Remote UE, Intermediate UE-to-Network Relay(s), and 5G ProSe UE-to-Network Relay as specified in clause 6.3.3.2 of TS 33.503 [5]. The proposed security procedure is based on the multi-hop UE-to-Network Relay communication procedures in the solutions (i.e., solution #1, #2, and #7) of TR 23.700-03 [1].

### 6.10.2 Solution details

The security procedure for multi-hop UE-to-Network Relay communication is shown in Figure 6.10.2-1.



Figure 6.10.2-1: Security procedure for multi-hop UE-to-Network Relay communication

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay are provisioned with the discovery security materials associated with an RSC based on the procedure specified in clause 6.3 of TS 33.503 [5]. In addition, the 5G ProSe Remote UE and Intermediate UE-to-Network Relay are provisioned with UP-PRUK and UP-PRUK ID from 5G PKMF as specified in step 1 in clause 6.3.3.2.2 of TS 33.503 [5].

1. The 5G ProSe Remote UE performs a multi-hop UE-to-Network Relay discovery procedure with the Intermediate UE-to-Network Relay and 5G ProSe UE-to-Network Relay.

2. If the Intermediate UE-to-Network Relay does not have an existing PC5 link with the 5G ProSe UE-to-Network Relay or an intermediate UE-to-Network relay on the path to the 5G ProSe UE-to-Network Relay, the Intermediate UE-to-Network Relay establishes a PC5 link with the 5G ProSe UE-to-Network Relay or the intermediate UE-to-Network relay based on the PC5 security establishment for 5G ProSe UE-to-Network relay communication over User Plane specified in clause 6.3.3.2.2 of TS 33.503 [5].

Editor’s Note: How to trigger the PC5 Link establishment with security is FFS.

3. The 5G ProSe Remote UE establishes a PC5 link with the Intermediate UE-to-Network Relay based on the PC5 security establishment for 5G ProSe UE-to-Network relay communication over User Plane specified in clause 6.3.3.2.2 of TS 33.503[5] with the Intermediate UE-to-Network Relay taking the role of the 5G ProSe UE-to-Network Relay.

NOTE 1: step 3 can start before step 2.

Editor’s Note: How the Intermediate Relay decides to connect to U2N Relay without connection request from Remote UE is FFS.

Editor’s Note: How the Intermediate Relay can play the role of U2N Relay to perform UP procedure while out of coverage is FFS.

Editor’s Note: How is the Remote UE authorized for connecting via U2N Relay as per UP procedure is FFS.

Editor’s Note: The need for a Remote UE to establish e2e security with the U2N relay is FFS.

Editor’s Note: Alignment with SA2 conclusion on the procedures is FFS.

### 6.10.3 Evaluation

TBD

## 6.11 Solution #11: Security establishment for multi-hop UE-to-UE Relay

### 6.11.1 Introduction

This solution addresses Key Issue #2: Security for multi-hop UE-to-UE Relay, aiming to provide a method to establish security between UEs in the multi-hop UE-to-UE (U2U) Relay scenario. In this solution, the existing mechanism to establish security in U2U scenario as specified in clauses 6.6.3 and 6.6.4 of TS 33.503 [5] is used as baseline. This solution is based on the following terminologies and assumptions:

* The term ‘Multi-hop UE-to-UE Relay’ in this solution refers to the relays located between the End UEs.
* The hops are counted based on the path from the source End UE to the target End UE, i.e. the Intermediate Relay that connects to the Source End UE is assumed as the first hop of the multi-hop connection, while the Target End UE locates at the last hop.
* The ‘next hop’ of a node refers to the neighbour node facing to the Target End UE side, while the ‘previous hop’ refers to the neighbour node facing to the Source End UE side.

### 6.11.2 Solution details

The mechanisms in clauses 6.6.3 and 6.6.4 are used as baseline of this solution, including mechanisms with and without network assistance.

Editor’s Note: Alignment with SA2 is FFS.

#### 6.11.2.1 Security mechanism with network assistance

Both UP-based and CP-based procedures as specified in clauses 6.3.3.2 and 6.3.3.3 of TS 33.503 [5] are used as baseline to provide authentication, authorisation and security establishment within the Multi-hop U2U Relay scenario with the following modificaitons:

For security establishment between the Source End UE and the Multi-hop U2U Relay:

- The Remote UE is replaced by the Source End UE.

- The U2NW Relay is replaced by the Multi-hop UE-to-UE Relay.

For security establishment between the Multi-hop U2U Relays:

- The Remote UE is replaced by the Multi-hop U2U Relay close to the Source End UE side.

- The U2NW Relay is replaced by the Multi-hop U2U Relay close to the Target End UE side.

For security establishment between the Multi-hop U2U Relay and the Target End UE:

- The Remote UE is replaced by the Target End UE.

- The U2NW Relay is replaced by the Multi-hop U2U Relay at the previous hop of the Target End UE.

- Upon receiving the Direct Communication Request (DCR) message from the Multi-hop U2U Relay which includes an RSC and if the Network Assistance Security Indicator associated with the RSC indicates the security procedures with network assistance are required, the Multi-hop U2U Relay needs to make sure it is inside network coverage prior to initiating the security procedure with network assistance. If the Multi-hop U2U Relay is not in network coverage, it shall reject the DCR message.

- The steps 4-5d in clause 6.3.3.2.2 of TS 33.503 [5] and the steps 3-16 in clause 6.3.3.3.2 of TS 33.503 [5] are not triggered by the DCR from the Multi-hop U2U Relay. Upon receiving the DCR message from the Multi-hop U2U Relay which includes an RSC with the Network Assistance Security Indicator indicating the security procedures with network assistance, the Target End UE shall inform the Multi-hop U2U Relay to initiate the above steps with the message pair Direct Communication Security Request and Direct Communication Security Accept. The Direct Communication Security Request message shall include the SUCI or UP-/CP-PRUK ID of Target End UE, the RSC and freshness parameter. Upon receiving the Direct Communication Security Request message, the Multi-hop U2U Relay shall make sure it is inside network coverage prior to initiating the security procedures with network assistance. If it is outside network coverage, it shall reject the Direct Communication Security Request message.

- The RSC in the DCR sent by Multi-hop U2U Relay to Target End UE is protected using the security mechanism in clause 6.3.5 of TS 33.503 [5] by modifying Annex A.5 to generate a keystream of the length of the RSC. The Direct Communication Security Request message is protected by reusing the protection method defined in clause 6.3.5 of TS 33.503 [5].

#### 6.11.2.2 Security mechanism without network assistance

The security procedure in clause 6.2 of TS 33.503 [5] is used to establish a secure PC5 link, using mechanism without network assistance, between the End UE and the Multi-hop U2U Relay, and between Multi-hop U2U Relays with the following modifications.

- The RSC is included in the DCR message.

- The DCR message is protected based on the security mechanism defined in clause 6.3.5 of TS 33.503 [5] with a modification that the length of the UP-PRUK ID/CP-PRUK ID is set to zero in clause 6.3.5.2 of TS 33.503 [5].

### 6.11.3 Evaluation

TBD.

## 6.12 Solution #12: Solution of multi-hop UE-to-UE Relay Communication

### 6.12.1 Introduction

This solution addresses key issue #2.

For the use of multi-hop UE-to-UE relays, multi-hop UE-to-UE relays can be within or outside the 3GPP coverage range. When the multi-hop UE-to-UE relay is without 3GPP coverage, this solution provides a mechanism for the PC5 security setting process between the Source End UE or the Target End UE and the multi-hop UE-to-UE Relay.

### 6.12.2 Solution details

The security procedure in clause 6.2 is used to establish a secure PC5 link between the End UE and the 5G ProSe Layer-3 multi-hop UE-to-UE Relay and between multiple 5G ProSe Layer-3 multi-hop UE-to-UE Relays without network assistance with the following modifications.

- The RSC is included in the DCR message.

- The DCR message is protected based on the security mechanism defined in clause 6.3.5 with a modification that the length of the UP-PRUK ID/CP-PRUK ID is set to zero in clause 6.3.5.2.

### 6.12.3 Evaluation

TBD

## 6.13 Solution #13: Solution of multi-hop UE-to-UE Relays Discovery Model B

### 6.13.1 Introduction

This Solution based on the solution #5 in TR 23.700-03 [1] and addressed the requirement of KI#2,

The 5G ProSe End UE are provisioned direct discovery security material associated with ProSe Code. The 5G ProSe End UE and U2U Relay are provisioned a set of discovery security material associated with RSC. The RSC related discovery security material is obtained from the HPLMN of discoveree 5G ProSe End UE.

Editor’s Note: It is FFS whether the whole discovery procedure in this solution is aligned with SA2.

Editor’s Note: It is FFS whether the discovery security materials provisioning procedure is aligned with single hop U2U Relay.

Editor’s Note: How the solution protects the path information during the discovery of multi-hop U2N relay is FFS.

### 6.13.2 Solution details



Figure 6.13.2-1 Security procedure for multi-hop UE-to-UE Relay Discovery Model B

1. The discoverer 5G ProSe End UE and discoveree 5G ProSe End UE are provisioned with the discovery security materials associated with a 5G ProSe Direct Discovery service based on the discovery security materials provisioning procedure for Restricted 5G ProSe Direct Discovery, as specified defined in clause 6.1.3.2.2.2.

The discoverer 5G ProSe End UE, discoveree 5G ProSe End UE and 5G ProSe UE-to-UE Relay are provisioned with the discovery security materials associated with a RSC based on the discovery security materials provisioning procedure for UE-to-Network Relay Discovery from the HPLMN of discoveree DDNMF, as specified in clause 6.1.3.2.2.2.

1. The discoverer 5G ProSe End UE shall construct a direct discovery set that contains two End UE discovery infos. Each End UE discovery info is protected using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3. The first protected End UE discovery info shall include User Info ID of the discoverer 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. The second protected End UE discovery info shall include the and User Info ID of the discoveree 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. Then, the discoverer 5G ProSe End UE shall include the above protected End UE discovery set and HPLMN id of the discoveree 5G ProSe End UE in the Solicitation message and protect the Solicitation message using the discovery security materials associated with RSC obtained from the HPLMN of discvoeree 5G ProSe End UE as specified in clause 6.1.3.2.3. The solicitation message is sent to the 5G ProSe UE-to-UE Relay 1.

Editor’s Note: How can the discoverer End UE knows the HPLMN ID of discoveree End UE is FFS.

3. On receiving the 5G ProSe UE-to-UE Relay Discovery Solicitation message from the discoverer 5G ProSe End UE, the 5G ProSe UE-to-UE Relay 1 shall extract the PLMN id from the Discovery Solicitation message and process the received UE-to-UE Relay Discovery Solicitation message using the discovery security materials identified by extracted PLMN id. The discovery security materials is obtained from the HPLMN of discoveree 5G ProSe End UE~~.~~

If the verification is successful, the 5G ProSe UE-to-UE Relay 1 shall modify the UE-to-UE Relay Discovery Solicitation message to include User Info ID of the 5G ProSe UE-to-UE Relay 1.

 The 5G ProSe UE-to-UE Relay Discovery Solicitation message is protected using the security materials associated with the RSC based on the extracted PLMN id as specified in clause 6.1.3.2.3.

Then, 5G ProSe UE-to-UE Relay 1 sends the message to the 5G ProSe UE-to-UE Relay 2 including the extracted PLMN id which is the HPLMN of discoveree DDNMF.

4.5. 5G ProSe UE-to-UE Relay 2…N repeat the step 3.

6. The discoveree 5G ProSe End UE shall extract the PLMN id and process the received UE-to-UE Relay Discovery Solicitation message using the discovery security materials associated with the RSC based on the extracted PLMN id which is the HPLMN of discoveree DDNMF,.

If the verification is successful, the discoveree 5G ProSe End UE shall extract the protected direct discovery set from the message and process the direct discovery set using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3.

The discoveree 5G ProSe End UE shall select a multi-hop relay path.

Editor Note: Whether path select procedure will be used is aligned with SA2.

7. The discoveree 5G ProSe End UE shall construct a direct discovery set that contains two End UE discovery infos. Each End UE discovery info is protected using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3. The first protected End UE discovery info shall include User Info ID of the discoverer 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. The second protected End UE discovery info shall include the and User Info ID of the discoveree 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. Then, the discoveree 5G ProSe End UE shall include the above protected direct discovery sets and HPLMN id of the discoveree 5G ProSe End UE in the Solicitation message and protect the Solicitation message using the discovery security materials associated with the RSC based on the extracted PLMN id which is the HPLMN of discoveree 5G ProSe End UE’s DDNMF as specified in clause 6.1.3.2.3. The discoveree 5G ProSe End UE replies to the 5G ProSe UE-to-UE Relay N with the UE-to-UE Relay Discovery Response message.

8. On receiving the UE-to-UE Relay Discovery Response message from the discoveree 5G ProSe End UE, the 5G ProSe UE-to-UE Relay N shall extract the PLMN id from the Discovery Response message and process the received UE-to-UE Relay Discovery Response message using the discovery security materials associated with the RSC based on the extracted PLMN id which is the HPLMN of discoveree 5G ProSe End UE’s DDNMF.

If the verification is successful, the 5G ProSe UE-to-UE Relay N shall modify the UE-to-UE Relay Discovery Response message to include User Info ID of 5G ProSe UE-to-UE Relay N.

 The UE-to-UE Relay Discovery Response message is protected using the security materials associated with the RSC based on the extracted PLMN id which is the HPLMN of discoveree 5G ProSe End UE’s DDNMF. Then, 5G ProSe UE-to-UE Relay N sends the UE-to-UE Relay Discovery Response message to UE-to-UE Relay 2.

Then, 5G ProSe UE-to-UE Relay N sends the message to the 5G ProSe UE-to-UE Relay 2 including the extracted PLMN id which is the HPLMN of discoveree DDNMF.

9. The 5G U2U Relay 2 repeat the step 8.

10. On receiving the UE-to-UE Relay Discovery Response message, the discoverer 5G ProSe End UE shall extract the PLMN id from the Discovery Response message and process the UE-to-UE Relay Discovery Response message using the discovery security materials associated with the RSC based on the extracted PLMN id which is the HPLMN of discoveree 5G ProSe End UE’s DDNMF.

If the verification is successful, the discoverer 5G ProSe End UE shall extract the protected direct discovery set from the UE-to-UE Relay Discovery Response message and process the protected End UE discovery infos using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3. If the verification of the first End UE discovery info is successful and the User Info ID of the discoverer matches, the discoverer 5G ProSe End UE processes the second End UE discovery info.

### 6.13.3 Evaluation

TBD

## 6.14 Solution #14: Multi-hop UE-to-UE Relay discovery security

### 6.14.1 Introduction

This solution addresses the first, third and fourth security requirements in the key issue #2 regarding the multi-hop UE-to-UE (U2U) Relay discovery. This solution assumes the architecture and procedures proposed in the solution #3 of TR 23.700-03 [1]. This means that 5G ProSe UE-to-UE Relays discover each other to form a 5G ProSe UE-to-UE Relay cloud, and 5G ProSe End UEs first discover nearby 5G ProSe UE-to-UE Relay and discover a target 5G ProSe End UE at IP layer (e.g., based on MANET routing protocol) via 5G ProSe UE-to-UE Relay cloud.

This solution proposes to reuse the security procedure for 5G ProSe UE-to-Network Relay discovery with Model A and Model B as specified in clause 6.1.3.2.2 of TS 33.503 [5]. That is, the discovery messages are protected based on the discovery security materials associated with an RSC for multi-hop UE-to-UE Relay.

### 6.14.2 Solution details

Based on the architecture and procedures in the solution #3 of TR 23.700-3 [1], this solution consists of two types of relay discovery: one for Relay discovery among 5G ProSe UE-to-UE Relays and the other one for Relay discovery between an 5G ProSe End UE and 5G ProSe UE-to-UE Relay.

1. Relay discovery among 5G ProSe UE-to-UE Relays

5G ProSe UE-to-UE Relays perform a Relay discovery to form a 5G ProSe UE-to-UE Relay cloud. For the provisioning of discovery security materials and discovery message protection based on the discovery security materials associated with an RSC for multi-hop UE-to-UE Relay, the security procedures for 5G ProSe UE-to-Network Relay discovery with Model A and Model B as specified in clause 6.1.3.2.2 of TS 33.503 [5] are used with the following changes:

- One 5G ProSe UE-to-UE Relay plays the role of a 5G ProSe Remote UE and the other 5G ProSe UE-to-UE Relay plays the role of a 5G ProSe UE-to-Network Relay.

2. Relay discovery between an 5G ProSe End UE and 5G ProSe UE-to-UE Relay

The 5G ProSe End UE performs a Relay discovery to discover a 5G ProSe UE-to-UE Relay that supports a multi-hop UE-to-UE Relay. For the provisioning of discovery security materials and discovery message protection based on the discovery security materials associated with an RSC for multi-hop UE-to-UE Relay, the security procedures for 5G ProSe UE-to-Network Relay discovery with Model A and Model B as specified in clause 6.1.3.2.2 of TS 33.503 [5] are used with the following changes:

- A 5G ProSe End UE plays the role of a 5G ProSe Remote UE and a 5G ProSe UE-to-UE Relay plays the role of a 5G ProSe UE-to-Network Relay.

Editor’s Note: How is privacy of End UE during discovery preserved when Relays share End UE User info (with associated IP address) to other Relays when using MANET based routing discovery is FFS.

Editor’s Note: Alignment with SA2’s conclusion about the procedure is needed.

### 6.14.3 Evaluation

TBD

## 6.15 Solution #15: Multi-hop UE-to-UE Relay communication security

### 6.15.1 Introduction

This solution addresses the first, second, and third security requirements in the key issue #2 regarding the multi-hop UE-to-UE (U2U) Relay communication. This solution assumes the architecture and procedures proposed in the solution #3 of TR 23.700-03 [1]. This means that UE-to-UE Relays establish a PC5 link with each other after the Relay discovery to form a 5G ProSe UE-to-UE Relay cloud, and a 5G ProSe End UE establishes a PC5 link with the 5G UE-to-UE Relay to discover a target 5G ProSe End UE and communicate with the discovered target 5G ProSe End UE at IP layer (e.g., based on MANET routing protocol).

For PC5 link security, this solution proposes to reuse the security procedure specified in clause 6.2 of TS 33.503 [5].

### 6.15.2 Solution details

Based on the architecture and procedures in the solution #3 of TR 23.700-3 [1], this solution consists of two types of PC5 link establishment: one for PC5 link establishment among 5G ProSe UE-to-UE Relays and the other one for PC5 link establishment between an 5G ProSe End UE and 5G ProSe UE-to-UE Relay.

1. PC5 link establishment among 5G ProSe UE-to-UE Relays:

After 5G ProSe UE-to-UE Relays perform a Relay discovery, they establish a secure PC5 link based on the security procedure for unicast mode 5G ProSe Direct Communication specified in clause 6.2 of TS 33.503 [5] with the following modifications:

- The RSC is included in the DCR message.

- The DCR message is protected based on the security mechanism defined in clause 6.3.5 with a modification that the UP-PRUK ID/CP-PRUK ID is not used in clause 6.3.5.2.

2. PC5 link establishment between an 5G ProSe End UE and 5G ProSe UE-to-UE Relay:

After the Relay discovery between an 5G ProSe End UE and 5G ProSe UE-to-UE Relay, the 5G ProSe End UE establishes a secure PC5 link with the 5G ProSe UE-to-UE Relay based on the security procedure for unicast mode 5G ProSe Direct Communication specified in clause 6.2 of TS 33.503 [5] with the following modifications:

- The RSC is included in the DCR message.

- The DCR message is protected based on the security mechanism defined in clause 6.3.5 with a modification that the UP-PRUK ID/CP-PRUK ID is not used in clause 6.3.5.2.

### 6.15.3 Evaluation

TBD

## 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 S3-241631 | 0.1.0 |
| 2024-05 | SA3#116 | S3-242521 |  |  |  | Included changes from S3-242072, S3-242156S3-242522, S3-242523, S3-242524, S3-242525, S3-242526, S3-242527, S3-242528, S3-242529, S3-242530, S3-242532S3-242650, S3-242651, S3-242652, S3-242653 | 0.2.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |