|  |  |
| --- | --- |
| 3GPP TR 33.740 V0.3.0 (2022-10) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of Proximity Based Services (ProSe) in 5G System (5GS) phase 2  (Release 18) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 9

3.1 Terms 9

3.2 Abbreviations 9

4 Security Aspects of 5G ProSe 9

4.1 General 9

4.2 Architecture assumption 9

5 Key issues 10

5.1 Key Issue #1: Security for UE-to-UE Relay discovery 10

5.1.1 Key issue details 10

5.1.2 Security threats 10

5.1.3 Potential security requirements 10

5.2 Key Issue #2: Security of UE-to-UE Relay 10

5.2.1 Key issue details 10

5.2.2 Security threats 10

5.2.3 Potential security requirements 11

5.3 Key issue #3: Authorization in the UE-to-UE Relay Scenario 11

5.3.1 Key issue details 11

5.3.2 Security threats 11

5.3.3 Potential security requirements 11

5.4 Key Issue #4: Privacy of information over the UE-to-UE Relay 12

5.4.1 Key issue details 12

5.4.2 Security threats 12

5.4.3 Potential security requirements 12

5.X Key Issue #X: <Key Issue Name> 13

5.X.1 Key issue details 13

5.X.2 Security threats 13

5.X.3 Potential security requirements 13

6 Solutions 13

6.0 Mapping of Solutions to Key Issues 13

6.1 Solution #1: Restricted Peer UE IP Discovery with Layer-3 UE-to-UE Relay 14

6.1.1 Introduction 14

6.1.2 Solution details 14

6.1.3 Evaluation 15

6.2 Solution #2: Privacy handling for Layer-3 UE-to-UE Relay based on IP routing 15

6.2.1 Introduction 15

6.2.2 Solution details 16

6.2.3 Evaluation 17

6.3 Solution #3: PC5 security establishment when L3 UE-to-UE relay is in coverage 17

6.3.1 Introduction 17

6.3.2 Solution details 17

6.3.2.1 Procedure for PC5 security establishment between the 5G ProSe Source UE and 5G ProSe UE-to-UE Relay 17

6.3.2.2 Procedure for PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay 20

6.3.3 Evaluation 20

6.4 Solution #4: PC5 security establishment when L3 UE-to-UE relay is out of coverage 21

6.4.1 Introduction 21

6.4.2 Solution details 21

6.4.3 Evaluation 23

6.5 Solution #5: PC5 link security establishment for Layer-3 U2U Relay 23

6.5.1 Introduction 23

6.5.2 Solution details 23

6.5.2.1 PC5 link security establishment procedure over User Plane 24

6.5.2.2 PC5 link security establishment procedure over Control Plane 25

6.5.3 Evaluation 27

6.7 Solution #7: Non-network-assited Security Establishment Procedure for 5G ProSe Layer-3 UE-to-UE Relay 33

6.7.1 Introduction 33

6.7.2 Solution details 34

6.7.3 Evaluation 35

6.8 Solution #8: Restricted 5G ProSe UE-to-UE Relay Discovery Model A 35

6.8.1 Introduction 35

6.8.2 Solution details 36

6.8.2.1 Restricted 5G ProSe UE-to-UE Relay Discovery Model A over Control Plane 36

6.8.2.2 Restricted 5G ProSe UE-to-UE Relay Discovery Model A over User Plane 38

6.8.3 Evaluation 38

6.9 Solution #9: Restricted 5G ProSe UE-to-UE Relay Discovery Model B 38

6.9.1 Introduction 38

6.9.2 Solution details 39

6.9.2.1 Restricted 5G ProSe UE-to-UE Relay Discovery Model B over Control Plane 39

6.9.2.2 Restricted 5G ProSe UE-to-UE Relay Discovery Model B over User Plane 41

6.9.3 Evaluation 41

6.10 Solution #10: PAKE-based security for UE-to-UE relay 41

6.10.1 Introduction 41

6.10.2 Solution details 42

6.10.2.1 Parameter provisioning in-coverage and out-of coverage 43

6.10.2.2 PAKE protocols 43

6.10.2.3 Parameters exchanged prior to the PAKE execution 44

6.10.2.4 PAKE execution 44

6.10.2.5 Secure exchange of data 44

6.10.3 Evaluation 44

6.11 Solution #11: Security for UE-to-UE Relay (Model A) discovery 44

6.11.1 Introduction 44

6.11.2 Solution details 45

6.11.3 Evaluation 47

6.12 Solution #12: Security of Layer-2 UE-to-UE Relay and Adaptation Layer 47

6.12.1 Introduction 47

6.12.2 Solution details 48

6.12.3 Evaluation 49

6.13 Solution #13: E2E authentication with Layer-3 UE-to-UE Relay 49

6.13.1 Introduction 49

6.13.2 Solution details 50

6.13.3 Evaluation 51

6.14 Solution #14: path switching with Layer-2 UE-to-UE Relay 51

6.14.1 Introduction 51

6.14.2 Solution details 51

6.14.3 Evaluation 53

6.15 Solution #15: Selection and authorization of in-coverage and out-of-coverage authentication and key establishment 53

6.15.1 Introduction 53

6.15.2 Solution details 54

6.15.3 Evaluation 55

6.16 Solution #16: Centralized discovery key management and U2U relay authorization 55

6.16.1 Introduction 55

6.16.2 Solution details 55

6.16.3 Evaluation 56

6.17 Solution #17: U2U relay discovery security material retrieval and authorization across PLMNs 56

6.17.1 Introduction 56

6.17.2 Solution details 57

6.17.3 Evaluation 58

6.18 Solution #18: UE-to-UE Relay security 58

6.18.1 Introduction 58

6.18.2 Solution details 58

6.18.3 Evaluation 59

6.19 Solution #19: End-to-end security establishment over the Layer-3 UE-to-UE Relay 59

6.19.1 Introduction 59

6.19.2 Solution details 59

6.19.3 Evaluation 61

6.20 Solution #20: Network-assisted security establishment procedure for 5G ProSe Layer-3 UE-to-UE Relay 61

6.20.1 Introduction 61

6.20.2 Solution details 62

6.20.3 Evaluation 63

6.21 Solution #21: E2E security establishment procedure for 5G ProSe Layer-3 UE-to-UE Relay 63

6.21.1 Introduction 63

6.21.2 Solution details 64

6.21.3 Evaluation 64

6.Y Solution #Y: <Solution Name> 64

6.Y.1 Introduction 64

6.Y.2 Solution details 65

6.Y.3 Evaluation 65

7 Conclusions 65

7.Z Key Issue #Z: <Key Issue Name> 65

Annex <X> (informative): Change history 65

For definitive guidance on drafting 3GPP TSs and TRs, see [3GPP TS 21.801](http://www.3gpp.org/DynaReport/21801.htm) supplemented by the 3GPP web page <http://www.3gpp.org/specifications-groups/delegates-corner/writing-a-new-spec>.

Ensure all blue guidance text is removed before submitting the TS/TR to the TSG for approval.

# Foreword

This clause is mandatory; do not alter the text in any way other than to choose between "Specification" and "Report".

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 drafting the TS/TR, pay particular attention to the use of modal auxiliary verbs! TRs shall not contain any normative provisions.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies the security and privacy aspects of proximity based services in 5G system phase 2. It ensures that the security solutions are aligned with the work in SA2 (i.e., TR 23.700-33 [2]), RANs, SA1 (i.e., TS 22.278 [3], TS 22.261 [4], and TS 22.115 [5]) and SA3 (i.e., TS 33.503 [6] and TR 33.870 [7]). The present document covers the following issues:

- Security and privacy key issues, threats and potential requirements of proximity based services in 5G system phase 2.

- Potential security solutions to cover these potential requirements.

Both roaming and non-roaming scenarios are considered.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-33: "Study on System enhancement for Proximity based Services (ProSe) in the 5G System (5GS); Phase 2".

[3] 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS)".

[4] 3GPP TS 22.261: "Service requirements for the 5G system; Stage 1".

[5] 3GPP TS 22.115: " Service aspects; Charging and billing".

[6] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[7] 3GPP TR 33.870: "Study of privacy of identifiers over radio access".

[8] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[9] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[10] IRTF “CPace, a balanced composable PAKE” available online at <https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/>

[11] IRTF “The OPAQUE Asymmetric PAKE Protocol” available online at <https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/>

[12] IRTF “SPAKE2, a PAKE” available online at <https://datatracker.ietf.org/doc/draft-irtf-cfrg-spake2/>

[13] IRTF “SPAKE2+, an Augmented PAKE” available online at <https://datatracker.ietf.org/doc/draft-bar-cfrg-spake2plus/>

[14] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[15] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

# 3 Definitions of terms, symbols and abbreviations

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

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**5G ProSe U2U UE:** A 5G ProSe-enabled UE that discovers or is discovered by a 5G ProSe-enabled UE(s) via a 5G ProSe UE-to-UE Relay; or a 5G ProSe-enabled UE that communicates with other 5G ProSe-enabled UE(s) via a 5G ProSe UE-to-UE Relay.

**5G ProSe UE-to-UE Relay:** A 5G ProSe-enabled UE that provides functionality to support connectivity between 5G ProSe U2U UEs.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5G DDNMF 5G Direct Discovery Name Management Function

RSC Relay Service Code

PAKE Password-based key establishment

# 4 Security Aspects of 5G ProSe

Editor’s Note: This clause contains a high-level overview of the 5G ProSe features, the security aspects and the potential impacts on the current Rel-18 security mechanisms.

## 4.1 General

Security solutions should build on the 5G ProSe architecture principles as defined in TS 23.304 [8] and 5G ProSe security architecture principles as defined in TS 33.503 [6], including flexibility and modularity for newly introduced functionalities.

## 4.2 Architecture assumption

- Security architecture defined in TS 33.503 [6] is used as basis security architecture for supporting 5G ProSe Security phase 2.

- The security architecture needs to enable secure UE-to-UE relay discovery and communication when the Source UE, Target UE as well as the UE-to-UE relay can be out of coverage.

- The 5G ProSe UE-to-UE Relay is specified in TS 23.304 [8].

- It is assumed that the 5G ProSe UE-to-UE Relay is a trusted entity.

# 5 Key issues

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

## 5.1 Key Issue #1: Security for UE-to-UE Relay discovery

### 5.1.1 Key issue details

In case of UE-to-UE Relay communication, a source UE discovers a target UE via a UE-to-UE Relay in proximity. The discovery messages to discover either a UE-to-UE Relay or a target UE via UE-to-UE Relays in proximity need to be security protected. Failure to protect the security of these discovery messages for UE-to-UE Relay communication may lead to various attacks by unauthorized UEs, e.g., discovery message manipulation, or potential leakage of privacy sensitive information. Therefore, the security aspects of the discovery messages broadcasted in UE-to-UE Relay discovery should be studied.

### 5.1.2 Security threats

If the discovery messages are not integrity protected and replay protected, the parameters included in the discovery messages (e.g., Relay Service Code and ProSe Restricted Code) can be modified, or replayed by an attacker. Consequently, a source UE may fail to find a relay UE or a target UE for an intended service.

If the discovery messages are not confidentiality protected, the privacy sensitive parameters (e.g., Relay Service Code and ProSe Restricted Code) can be eavesdropped by an attacker.

### 5.1.3 Potential security requirements

The 5G System shall provide a means for confidentiality protection, integrity protection and replay protection of discovery messages for UE-to-UE Relay discovery.

The 5G System shall provide a means to protect the privacy sensitive information of source UE and target UE during UE-to-UE Relay discovery procedure.

The 5G System shall provide a means to securely provision the security materials for UE-to-UE Relay discovery.

## 5.2 Key Issue #2: Security of UE-to-UE Relay

### 5.2.1 Key issue details

3GPP system has to be able to protect security (i.e., the integrity and confidentiality) of information between the peer UEs over the UE-to-UE Relay. Failure to protect integrity and confidentiality of information exchanged between the peer UEs over the UE-to-UE Relay will open vulnerability in 5GS and allow various attacks such as unauthorized disclosure and modification of information. Protection of communications between the peer UEs should take into consideration that the UE-to-UE Relay is a trusted node.

TR 23.700-33 [2], key Issue #1: Support of UE-to-UE Relay, has the following key issue:

*- How to enhance the system architecture to provide security/privacy protection for a relayed connection.*

*...*

NOTE 3: For security/privacy protection aspects, coordination with SA WG3 is needed.”

### 5.2.2 Security threats

Failure to protect integrity and confidentiality of information exchanged between the peer UEs over the UE-to-UE Relay will open vulnerability in 5GS and allow various attacks such as unauthorized disclosure and modification of information.

A malicious Relay UE that can establish a unicast link with the source UE, as well as the target UE may conduct an MITM attack.

Failure to protect integrity and confidentiality of information during path change will open vulnerability in 5GS and allow various attacks resulting in unauthorized disclosure and modification of information.

### 5.2.3 Potential security requirements

The 3GPP system shall support a means to provide confidentiality, integrity and replay protection of end-to-end information exchanged between the peer UEs over the UE-to-UE Relay.

The 3GPP system shall support a means to protect security (i.e., the integrity, confidentiality, and replay protection) of user-plane and control-plane messages, including during UE-to-UE Relay path switch.

The 3GPP system shall support a means to establish a secure connection between the source UE and the target UE in the UE-to-UE relay scenario.

## 5.3 Key issue #3: Authorization in the UE-to-UE Relay Scenario

### 5.3.1 Key issue details

TR 23.700-33 [2], key issue #1 describes its key Issue regarding support of UE-to-UE Relay:

*"- Whether and how the network can control UE-to-UE Relay operation, at least including how to:*

*- Authorize the UE-to-UE Relay, e.g. authorize a UE as UE-to-UE Relay.*

*- Authorize Source/Target UEs to use a UE-to-UE Relay.*

*…*

*NOTE 3: For security/privacy protection aspects, coordination with SA WG3 is needed."*

From a security point of view, whether the UE can act as a UE-to-UE Relay should be assured by the Source UE or Target UE. Similarly, whether the UE can act as a Source UE or Target UE should be assured by the UE-to-UE relay.

3GPP system should be able to authorize a UE to perform as UE-to-UE Relay and a UE to communicate with another UE via a UE-to-UE Relay.

### 5.3.2 Security threats

An attacker may impersonate the UE-to-UE Relay. If the Source/Target UE cannot verify if the UE acting as UE-to-UE relay is authorized, the attacker UE may impersonate the UE-to-UE relay. The attacker may then deny the UE services between the two UEs (e.g., arbitrary discard messages).

Similarly, an attacker may impersonate the Source UE or the Target UE.

### 5.3.3 Potential security requirements

The 5GS shall support authorization of the UE as a UE-to-UE relay in the UE-to-UE relay scenario.

The 5GS shall support authorization of the UE as a Source UE or a Target UE in the UE-to-UE relay scenario.

## 5.4 Key Issue #4: Privacy of information over the UE-to-UE Relay

### 5.4.1 Key issue details

3GPP system has to be able to protect the privacy of identities exchanged in the communications between peer UEs over a UE-to-UE Relay. Failure to protect the privacy of identities of peer UEs communicating over the UE-to-UE Relay will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

TR 23.700-33 [2] Key Issue #1: Support of UE-to-UE Relay, has the following key issue:

*‘- How to enhance the system architecture to provide security/privacy protection for relayed connections.*

*...*

*NOTE 3: For security/privacy protection aspects, coordination with SA WG3 is needed.’*

### 5.4.2 Security threats

Failure to protect the privacy of identities exchanged in the communications between the peer UEs over the UE-to-UE Relay will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

The existing Link identifier update procedure specified in TS 33.536 [9] provides privacy of the identities on a per unicast link basis (e.g., the link between a UE and the UE-to-UE Relay). Therefore an attacker may be able to link identities exchanged over the link between a UE and the UE-to-UE Relay to those exchanged over the corresponding link between the peer UE and the UE-to-UE Relay

Path switch between UE-to-UE Relay UEs is a new feature aiming to preserve user experience. Such preservation may be achieved by making certain elements (e.g., IP addresses) of user experience persistent across sessions and UE-to-UE Relays. Persistent parameters may leak unique attributes associated with UEs and other ProSe entities and allow privacy attacks on these entities (e.g., UEs). Failure to protect the privacy of entities and identities during UE to UE Relay path change will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of entities and identities.

### 5.4.3 Potential security requirements

The 5G System should provide means for mitigating trackability attacks on peer UEs during communications over a UE-to-UE Relay including during the UE-to-UE Relay path switch.

The 5G System should provide means for mitigating linkability attacks on peer UEs during communications over a UE-to-UE Relay including during the UE-to-UE Relay path switch.

5.5 Key Issue #5: Security of source and target UE communication via U2U relay

5.5.1 Key issue details

3GPP system has to be able to protect security (i.e., the integrity and confidentiality) of information transmitted between the source and target UEs over the UE-to-UE Relay. With the U2U relay being trusted, the protection of security between source and target UEs connected via the U2U relay can be realized either hop-by-hop or end-to-end or both. However, from an efficiency point of view, it does not make sense to do both hop-by-hop and end-to-end at the same time, especially since the U2U relay scenario most likely focuses on the case where the UEs are out of network coverage and therefore out of power source.

This key issue addresses the need for the U2U relay and the source and target UEs to negotiate and agree on a protection scheme, whether it is hop-by-hop or end-to-end. It is independent of the need to apply integrity-, confidentiality-, and replay-protection once the protection scheme is negotiated. Key issue is for L3 relay.

5.5.2 Security threats

If source and target UEs communicating with each other via U2U relay are not using the same protection scheme (i.e., hop-by-hop or end-to-end), the source and target UEs will not be able to communicate with each other or the traffic between the source and target UEs may not be protected at all.

Editor’s Note: Threat requires further study.

5.5.3 Potential security requirements

TBD

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

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

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

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Key Issues | | | | | | | |
| Solutions | 1 | 2 | 3 | 4 |  |  |  |  |
| 1 | X |  | X |  |  |  |  |  |
| 2 |  |  |  | X |  |  |  |  |
| 3 |  | X | X |  |  |  |  |  |
| 4 |  | X | X |  |  |  |  |  |
| 5 |  | X | X |  |  |  |  |  |
| 6 |  | X |  |  |  |  |  |  |
| 7 |  | X |  |  |  |  |  |  |
| 8 | X |  |  |  |  |  |  |  |
| 9 | X |  |  |  |  |  |  |  |
| 10 |  | X | X |  |  |  |  |  |
| 11 | X |  |  |  |  |  |  |  |
| 12 |  | X |  | X |  |  |  |  |
| 13 | X | X | X |  |  |  |  |  |
| 14 |  | X |  | X |  |  |  |  |
| 15 |  | X | X |  |  |  |  |  |
| 16 | X |  | X |  |  |  |  |  |
| 17 | X |  | X |  |  |  |  |  |
| 18 |  | X |  |  |  |  |  |  |
| 19 |  | X | X |  |  |  |  |  |
| 20 |  | X |  |  |  |  |  |  |
| 21 |  | X |  |  |  |  |  |  |

## 6.1 Solution #1: Restricted Peer UE IP Discovery with Layer-3 UE-to-UE Relay

### 6.1.1 Introduction

This solution is for the 5G ProSe Layer-3 UE-to-UE Relay case. It addresses Key Issue #3: Authorization in the UE-to-UE Relay Scenario and 2nd requirement of Key Issue #1: Security for UE-to-UE Relay discovery (protection of privacy sensitive information of source and target UE).

TR 23.700-33[2] describes several solutions for Layer-3 based which are all based on IP routing functionality at the UE-to-UE Relay. As part of the PC5 unicast link establishment procedure, the ProSe 5G UE-to-UE Relay allocates an IP address/prefix to the UE or is informed of the UE's IP address/prefix. The Relay stores the association of the UE's Application layer ID (also called User Info) and UE's IP address/prefix (e.g. into its DNS entries). When a source UE needs to communicate with a target UE via the ProSe 5G UE-to-UE Relay, it sends a request (e.g., DNS query) to the ProSe 5G UE-to-UE Relay, over the unicast link, to obtain the target UE's IP address/prefix (based on Target User Info). The Relay returns the IP address/prefix of the target UE. The source UE sends IP data to the target UE via the PC5 unicast link to UE-to-UE Relay. The UE-to-UE Relay acts as an IP router and forwards the packets to the corresponding PC5 unicast link towards the target UE.

When using the IP based routing, a UE connected to a UE-to-UE Relay may wish to restrict the discovery of its IP address/prefix for privacy reasons, such as only authorized peer UEs can discover the UE. This is similar to the restricted discovery mechanism where only an authorized Discoverer UE may discover a Discoveree UE. Besides IP address/prefix privacy aspect, the UE-to-UE Relay also needs to ensure that only authorized peer UEs can communicate with the UE.

To enable the support of Restricted IP address/prefix discovery, a UE indicates to the UE-to-UE Relay during the PC5 link establishment procedure if its IP address/prefix may be discovered/shared with peer UEs without seeking the UE authorization or if a prior authorization from the UE is required. In addition, to minimize the PC5 signaling needed to support Restricted IP address/prefix discovery, the UE may provide a token to the UE-to-UE Relay to delegate IP address/prefix sharing authorization to the UE-to-UE Relay using this token.

### 6.1.2 Solution details

This procedure enables a UE (UE1) to indicate to the UE-to-UE Relay if its IP address/prefix may be shared with a peer UE (UE2) without seeking its authorization or if its authorization is required. It also enables UE1 to provide information to the UE-to-UE Relay to verify directly if UE2 is authorized to receive IP address/prefix information of UE1.



Figure 6.1.2-1: "Restricted" IP discovery procedure for 5G ProSe Layer-3 UE-to-UE Relay

1. UE1 provides an indication (*IP discovery* *authorization required*) and may provide an authorization token during the PC5 Link Establishment procedure with the UE-to-UE Relay. UE-to-UE Relay stores this indication and token (if received) along with other UE1 and PC5 link information. UE1 may be pre-provisioned with the IP discovery authorization token. The token may be generated by UE1 to allow UE2 to discover its IP address. The validity of the token can be associated with the current PC5 unicast link, particular target UE(s), for a particular period, etc. The token is sent protected over the secure PC5 link using the security keys established with the relay.

2. UE-to-UE Relay receives a DNS query from UE2 including UE1's User Info and possibly a token. UE-to-UE Relay retrieves UE1's info and if the *IP discovery* *authorization required* indication is set, UE-to-UE Relay validates the token received from UE2 with UE1's saved token, if a token is received on Query and if a token from UE1 is saved on the UE-to-UE Relay.

The distribution of such token to the UE2 may be performed out of band or in band, e.g., by UE-to-UE Relay after/during a successful DNS query (as specified at step 5).

3. If no token is received from UE2 and/or no token has been provided by UE1 during the link establishment procedure, UE-to-UE Relay sends a PC5-S IP Discovery Authorization Request message with UE2's User Info, UE2's IP address, and the token from UE2 (if received on the Query) to UE1, requesting authorization to share UE1's IP address with UE2.

4. UE1 receives the PC5-S IP Discovery Authorization Request message and replies with a PC5-S IP Discovery Authorization Accept or Reject message, specifying UE2's User Info. UE1 may provide a token at this point for future DNS query messages to be authorized directly at the UE-to-UE Relay using this token. UE1's decision to authorize IP disclosure via the UE-to-UE Relay or provide an authorization token to the UE-to-UE Relay may be based on policies, Application's layer authorization, etc.

5. UE-to-UE Relay sends a DNS response to UE2 with UE1's IP address (if token matches at the UE-to-UE Relay or if a PC5-S IP Discovery Authorization Accept message is received from UE1) or doesn't reply to the Query message (if no match with token or if a PC5-S IP Discovery Authorization Reject message is received from UE1). UE-to-UE Relay stores the token, if provided by UE1, and may send it to the UE2 with the response. UE2 may use this token the next time it needs to send a DNS query message to discover UE1's IP address.

### 6.1.3 Evaluation

TBD

## 6.2 Solution #2: Privacy handling for Layer-3 UE-to-UE Relay based on IP routing

### 6.2.1 Introduction

This solution addresses Key Issue #4: Privacy of information over the UE-to-UE Relay and in the case of the 5G ProSe Layer-3 UE-to-UE Relay.

A Source UE (UE1) communicating with a Target UE (UE2) over PC5 unicast links, via a UE-to-UE Relay, may need to change its Layer-ID, MSB of Knrp-sess ID and potentially IP address/prefix and other identifiers, e.g., for privacy reasons.

When a Source UE changes its identifiers, the UE-to-UE Relay also needs to update its identifiers at the same time (as per the Link Identifier Update (LIU) procedure defined in TS 23.304 [8] and TS 33.536 [9]) since the PC5 link is established between UE1 and the UE-to-UE Relay. In the case where UE1 changes its IP address/prefix, its Target UE must be informed of UE1’s new IP address/prefix since communication between UE1 and UE2 is IP-based. Note that the UE IP address is protected over PC5, however existing LIU procedure mandates the change of IP address for IP communications, as per TS 24.554, clause 7.3.2.4. Furthermore, the UE-to-UE Relay must as well be informed of UE1’s new IP address/prefix since the UE-to-UE Relay handles the IP routing of messages exchanged between the UE1 and UE2. In other words, when used in the UE-to-UE Relay scenario, current LIU procedure would lead to breaking the communication between Source UE and Target UE without proper IP change handling. Therefore, LIU procedure needs enhancements for the UE-to-UE Relay scenario to correctly handle the Source UE IP address change (or Target UE IP address change if LIU procedure is run between Target UE and the UE-to-UE Relay) to avoid this issue.

Likewise, UE1 may be communicating with more than one Target UE over the PC5 unicast link via the UE-to-UE Relay. In that case, all Target UEs must be informed of UE1’s new IP address/prefix.

### 6.2.2 Solution details

Figure 6.2.2-1 illustrates the procedure between the Source UE (UE1), the UE-to-UE Relay, and the Target UE (UE2) handling the change of identifiers at the Source UE. The Link Identifier Update procedure defined in TS 23.304 [8] is reused between UE1 and the UE-to-UE Relay complemented with additional messages between the UE-to-UE Relay and UE2 (i.e., Target UE(s)).

The new procedure between the Relay and the Target UE(s) is needed to inform the Target UE(s) about UE1’s new IP address/prefix. The Target UE(s) do not need to change their IDs at this point since they are using a distinct PC5 link with the UE-to-UE Relay. The UE-to-UE Relay however needs to inform UE2 of UE1’s new IP address/prefix during the Link Identifier Update procedure between UE1 and UE-to-UE Relay to avoid disruption and loss of communication between UE1 and UE2.

This solution applies to Layer-3 based Solutions #2, #3, #11, #12 and #34 described in TR 23.700-33[2]. These solutions are all based on IP routing functionality at the UE-to-UE Relay with a difference related to the proposed method for IP address/prefix allocation. With some solutions, the UE-to-UE Relay allocates the IP address/prefix to the UE, while for other solutions, a link-local IP address that is assigned by the UE itself is used and sent to the UE-to-UE Relay. Differences in the procedure detailed below are explained when needed.



Figure 6.2.2-1: Privacy handling procedure for 5G ProSe Layer-3 UE-to-UE Relay

0) A PC5 unicast link is established between UE1 and the UE-to-UE Relay. A distinct PC5 unicast link is established between the UE-to-UE Relay and UE2. Both Source/Target UEs learn their peer UE’s IP addresses/prefixes via the Relay UE using e.g. DNS. IP data is exchanged between UE1 and UE2 via the UE-to-UE Relay over the PC5 unicast links. The UE-to-UE Relay handles the routing of IP packets to another PC5 unicast link based on the destination IP address/prefix.

1) UE1 is informed (e.g., via the application layer, privacy timer expiration) that its Layer-2 ID, Knrp-sess ID, and IP address/prefix, must be changed. UE1 sends a Link Identifier Update Request message to the UE-to-UE Relay, which includes the usual parameters sent on the Link Identifier Update Request message, e.g., new Layer-2 ID and new MSB of Knrp-sess ID. In addition, information related to the change of IP address/prefix may also be included e.g. “new IP address needed” and “inform peer UE” indications as well as UE2’s specific information needed at step 2, i.e. UE2’s IP address/prefix, UE2’s user info.

1. The “new IP address needed” indication is included to request a new IP address/prefix for UE1 from the UE-to-UE Relay.
2. If UE1 uses a link-local IP address, a new link-local IP address is self-allocated on UE1, sent to the UE-to-UE Relay using the Link Identifier Update Request message and, in this case, the “new IP address needed” indication is not included.

2) If the “new IP address needed” indication is included, UE-to-UE Relay assigns a new IP address/prefix to UE1, otherwise, the UE-to-UE Relay saves the new IP address/prefix provided by UE1. If the “inform peer UE” indication is included, the UE-to-UE Relay uses UE2’s specific information received at steps 1 to retrieve the PC5 link established with UE2 and sends a new PC5 Relay Update Request message to UE2 over the PC5 link including UE1’s new IP address/prefix.

3) UE2 saves UE1’s new IP address/prefix. UE2 sends a new PC5 Relay Update Response message to the UE-to-UE Relay including all parameters received on the PC5 Relay Update Request message to ACK them.

4) UE-to-UE Relay sends a Link Identifier Update Response message to UE1 including the usual parameters sent on the Link Identifier Update Response message, e.g., new Layer-2 ID and new LSB of Knrp-sess ID and including UE1’s new IP address/prefix.

5) UE1 completes the Link Identifier Update procedure by sending a Link Identifier Update ACK message to the UE-to-UE Relay. UE1 starts using its new IP address/prefix. The new Layer-2 IDs and Knrp-sess ID associated with the PC5 unicast link are also used at that point.

### 6.2.3 Evaluation

TBD

## 6.3 Solution #3: PC5 security establishment when L3 UE-to-UE relay is in coverage

### 6.3.1 Introduction

This solution addresses Key issue #2: Security of UE-to-UE Relay and Key issue #3: Authorization in the UE-to-UE Relay Scenario. This solution addresses a L3 UE-to-UE relay.

For L3 UE-to-UE relay use cases, the L3 UE-to-UE relay may be in or out of 3GPP coverage. This solution provides a mechanism for PC5 security setup procedure between a source UE or target UE and a L3 UE-to-UE relay when the L3 UE-to-UE relay is in 3GPP coverage.

This solution assumes 5GC NFs e.g., 5GDDNMF and PKMF are deployed in the network.

### 6.3.2 Solution details

#### 6.3.2.1 Procedure for PC5 security establishment between the 5G ProSe Source UE and 5G ProSe UE-to-UE Relay

Figure 6.3.2,1-1 illustrates the high-level procedure of the proposed solution.



Figure 6.3.2.1-1: High-level procedure of PC5 security between Source/Target UE and UE-to-UE relay

0. The 5G ProSe Source/Target UE and UE-to-UE relay are provisioned with the discovery security materials, PC5 security policies and/or PRUK when they are in coverage.

NOTE 1: 5GC NF(s) that provision PC5 security policies are to be determined during normative work.

1. The discovery procedure for UE-to-UE Relay is performed by the 5G ProSe Source UE using the discovery parameters and discovery security material, based on the Relay Service Code for UE-to-UE Relay. If the UE-to-UE Relay is in 3GPP coverage, it also indicates whether network-based Relay service authentication and authorization is supported for UE-to-UE relay in the discovery announcement message.

Editor’s Note: how to verify the service authorization information if relay UE uses the same security materials for both in-coverage and out-of-coverage mode.

NOTE 2: In case the Relay UE is capable to support more security methods (e.g., as described in Solution #4) when the Relay UE is in 3GPP coverage, it is preferrable to use the security method described in this solution.

2. If the discovered UE-to-UE Relay supports network-based Relay service authentication and authorization, the 5G ProSe Source UE sends a Direct Communication Request (DCR) that contains PRUK ID or SUCI, Relay Service Code (RSC) of the 5G ProSe UE-to-UE Relay service and KNRP freshness parameter 1 to the 5G ProSe UE-to-UE Relay. Protection of PRUK ID and RSC in DCR can be done same as described in TS33.503 [6].

3. The 5G ProSe UE-to-UE Relay sends a Key Request message that contains PRUK ID or SUCI, RSC and KNRP freshness parameter 1 to the 5GC.

NOTE 3: 5GC NFs and internal signalling are not described in detail.here for brevity. The similar security procedure as Security for 5G ProSe Communication via 5G ProSe Layer-3 UE to-Network Relay as defined in TS33.503 [6] can be reused.

4. The 5GC sends the Key Response message to the 5G ProSe UE-to-UE Relay, which includes KNRP, KNRP freshness parameter 2. The message may also contain GPI, EAP message exchange depending on the selected security methods (UP or CP) as defined in TS33.503 [6]

5a. The 5G ProSe UE-to-UE Relay shall derive the session key (KNRP-SESS) from KNRP and then derive the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies as specified in TS 33.536 [9]. The 5G ProSe UE-to-UE Relay sends a Direct Security Mode Command message to the 5G ProSe Source UE and include KNRP Freshness Parameter 2 in the message.

5b. The 5G ProSe Source UE shall derive KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2 and then derive the session key (KNRP-SESS) and the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies in the same manner as the 5G ProSe UE-to-UE Relay and process the Direct Security Mode Command. Successful verification of the Direct Security Mode Command assures the 5G ProSe Source UE that the 5G ProSe UE-to-UE Relay is authorized to provide the UE-to-UE relay service.

5c. The 5G ProSe Source UE responds with a Direct Security Mode Complete message to the 5G ProSe UE‑to-UE Relay.

5d. On receiving the Direct Security Mode Complete message, the 5G ProSe UE-to-UE Relay shall verify the Direct Security Mode Complete message. Successful verification of the Direct Security Mode Complete message assures the 5G ProSe UE-to-UE Relay that the 5G ProSe Source UE is authorized to get the UE-to-UE relay service.

6. After successful verification, the 5G ProSe UE-to-UE Relay responds a Direct Communication Accept message to the 5G ProSe Source UE to complete the PC5 connection establishment procedure.

7. PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay is performed according to the procedure described in clause 6.3.2.2.

Editor’s Note: Its FFS how target UE determines whether this PC5 link is used for direct communication with U2U relay or for U2U communication with Source UE.

#### 6.3.2.2 Procedure for PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay



Figure 6.3.2.2-1 PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay

1. If the target UE is not discovered by the 5G ProSe UE-to-UE Relay yet, the discovery procedure is performed.

2. The 5G ProSe UE-to-UE Relay sends a Direct Communication Invite that contains Relay Service Code to the 5G ProSe Target UE.

Editor’s Note: The need for the new Direct Communication Invite message is FFS in coordination with SA2.

3-7. Step 3-7 are same as step 2-6 of clause 6.3.2.1, where the 5G ProSe Target UE acts the role of the 5G ProSe Source UE.

### 6.3.3 Evaluation

## 6.4 Solution #4: PC5 security establishment when L3 UE-to-UE relay is out of coverage

### 6.4.1 Introduction

This solution addresses Key issue #2: Security of UE-to-UE Relay and Key issue #3: Authorization in the UE-to-UE Relay Scenario. This solution addresses a L3 UE-to-UE relay.

For UE-to-UE relay use cases, the L3 UE-to-UE relay may be in or out of 3GPP coverage. This solution provides a mechanism for PC5 security setup procedure between a source UE or target UE and a L3 UE-to-UE relay when the L3 UE-to-UE relay is out of 3GPP coverage.

This solution assumes long term credentials are provisioned into the UE(s) and form the root of the security of the PC5 unicast link as specified in TS 33.536 [9].

This solution proposes to use authorization tokens as in OAuth 2.0 to indicate that a source UE or a target UE or a L3 UE-to-UE relay is authorized to use a specific UE-to-UE service or to serve a specific UE-to-UE service. When the source UE or the target UE or the L3 UE-to-UE relay registers in the 3GPP network and is authorized to use the UE-to-UE service, the network provides a token stating what kind of UE-to-UE service it can use or serve. The token has an expiration time and is signed with a private key. The network also provides the public key to the UEs to be used for verifying the token from other parties.

This solution assumes the peer UEs retrieve authorization token and public key for token verifying from the Prose Application server. The method how the UEs retrieve tokens and public keys is application specific and not described in 3GPP specification.

### 6.4.2 Solution details

Figure 6.4.2-1 illustrates the high-level procedure of the proposed solution.



Figure 6.4.2-1: High-level procedure of PC5 security between Source/Target UE and UE-to-UE relay

0. The 5G ProSe Source/Target UE and UE-to-UE relay are provisioned with the discovery security materials and PC5 security policies, and request authorization tokens when they are in coverage.

1. The discovery procedure for UE-to-UE Relay is performed by the 5G ProSe Source UE using the discovery parameters and discovery security material, based on the Relay Service Code for UE-to-UE Relay.

2. If discovery result indicates the UE-to-UE Relay supports Direct Relay service authentication and authorization, the 5G ProSe Source UE sends a Direct Communication Request (DCR) that contains Relay Service Code (RSC) of the 5G ProSe UE-to-UE Relay service and Authorization token of 5G ProSe Source UE which is retrieved from step 0, and also the Key\_Est\_Info used for direct authentication and key establishment. Protection of Authorization token and RSC in DCR can be done in a similar way as described in TS33.503 [6].

Editor’s Note: The details regarding the ciphering algorithm for the token are FFS.

Editor’s Note: The need for authorization token is FFS”.

3. Direct Auth and Key Establish procedure as specified in TS 33.536 [9] is performed.

4. The 5G ProSe UE-to-UE Relay uses the public key provided by the network to verify the token of the 5G ProSe Source UE that the 5G ProSe Source UE is authorized to get the UE-to-UE relay service.

5. The 5G ProSe UE-to-UE Relay derives KNRP and other security material as specified in TS 33.536 [9]. The 5G ProSe UE-to-UE Relay sends a Direct Security Mode Command message to the 5G ProSe Source UE including the Authorization token of 5G ProSe UE-to-UE Relay which is retrieved from step 0. The protection of the Authorization token is applied in the same way as step 2.

6. The 5G ProSe Source UE uses the public key provided by the network to verify the token of the 5G ProSe UE-to-UE Relay that the 5G ProSe UE-to-UE Relay is authorized to provide the UE-to-UE relay service. The 5G ProSe Source UE derives KNRP and other security material similar as the 5G ProSe UE-to-UE Relay in step5.

7. The 5G ProSe Source UE sends the Direct Security Mode Complete message to the 5G ProSe UE-to-UE.

8. The 5G ProSe UE-to-UE Relay responds a Direct Communication Accept message to the 5G ProSe Source UE to complete the PC5 connection establishment procedure.

9. Step 1-8 are repeated for PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay.

### 6.4.3 Evaluation

## 6.5 Solution #5: PC5 link security establishment for Layer-3 U2U Relay

### 6.5.1 Introduction

This solution addresses Key Issue #2 and Key Issue #3. This solution provides a means to establish the secure PC5 link between the source UE/target UE and the UE-to-UE Relay. When UE-to-UE Relay is in coverage, the source UE/target UE may establish the secure PC5 link with the UE-to-UE Relay by using the same security procedure as 5G ProSe UE-to-Network Relay communication.

NOTE: How to select the PC5 link security procedure proposed by this solution for the source UE/target UE and the UE-to-UE Relay is not addressed in the present document.

### 6.5.2 Solution details

Both user-plane (UP) based and control-plane (CP) based procedures of 5G ProSe UE-to-Network Relay can be reused for 5G ProSe UE-to-UE Relay authorization and PC5 link security establishment. 5G ProSe UE-to-UE Relay service and 5G ProSe UE-to-Network Relay service can be distinguished by Relay Service Code.

#### 6.5.2.1 PC5 link security establishment procedure over User Plane

The PC5 link security establishment procedure over User Plane for 5G ProSe UE-to-UE Relay is as follows:



Figure 6.5.2.1-1: PC5 link security establishment procedure over User Plane for 5G ProSe UE-to-UE Relay

NOTE 1: Figure 6.5.2.1-1 shows the security procedure of the non-roaming for 5G ProSe UE-to-UE Relay services. In this figure, the source UE and the target UE and UE-to-UE Relay use a subscription of the same PLMN.

0. The source UE and the target UE is provisioned with the discovery security materials and Prose Remote User Key (PRUK) when it is in coverage. The UE-to-UE Relay is provisioned with the discovery security materials when it is in coverage. These security materials are associated with an expiration time, after which they become invalid. If the UE does not have valid discovery security materials, it needs to connect to the 5G PKMF and obtain fresh ones to use the 5G ProSe UE-to-UE Relay services. The UE gets the 5G PKMF address from the 5G DDNMF.

NOTE 2: The detail of discovery procedure is not addressed in the present document.

1. The source UE performs the discovery procedure and discover the target UE via UE-to-UE Relay.

Editor’s Note: UE-to-UE Relay discovery and communication establish will align with SA2 WG2.

2a. The source UE sends a Direct Communication Request (DCR) that contains the PRUK ID or a SUCI if the source UE does not have a valid PRUK, Relay Service Code (RSC) of the 5G ProSe UE-to-UE Relay service and KNRP freshness parameter 1 to the 5G ProSe UE-to-UE Relay.

Editor’s Note: Its FFS whether the included parameters in Direct Communication Request message in step 2 can be protected by the discovery keys similar as to the Direct Communication Request message when establishing a secure PC5 link in between Remote UE and UE-to-network relay as described in TS 33.503 [6].

2b. The source UE and the UE-to-UE Relay perform the same authorization and key establishment procedure over User Plane as 5G ProSe UE-to-Network Relay. According the PC5 key hierarchy over user plane as defined in clause 6.3.3.2.3 of TS 33.503[6], the PRUK of source UE (Remote UE) will be shared by 5G ProSe UE-to-Network Relay service and 5G ProSe UE-to-UE Relay service. And the PKMF of source UE use the PRUK identified by PRUK ID, KNRP freshness parameter 1, KNRP freshness parameter 2 and the RSC indicating the UE-to-UE Relay service to derive the KNRP different from the 5G ProSe UE-to-Network service.

2c. The UE-to-UE Relay derive the session key (KNRP-SESS) from KNRP and then derive the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on PC5 policies. The UE-to-UE Relay sends a Direct Security Mode Command message to the source UE. This message also include the KNRP freshness parameter 2 and be protected as specified in TS 33.536 [9].

2d. If the source UE receives the message containing the GPI, it processes the GPI and derive the PRUK and obtain the PRUK ID from the GPI.

The source UE derive KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2. It then derive the session key (KNRP-SESS) and the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies in the same manner as the UE-to-UE Relay and process the Direct Security Mode Command. Successful verification of the Direct Security Mode Command assures the source UE that the UE-to-UE Relay is authorized to provide the relay service.

The source UE responds with a Direct Security Mode Complete message to the UE-to-UE Relay as specified in TS 33.536 [9].

2e. On receiving the Direct Security Mode Complete message, the UE-to-UE Relay shall verify the Direct Security Mode Complete message. Successful verification of the Direct Security Mode Complete message assures the UE-to-UE Relay that the source UE is authorized to get the relay service.After successful verification, the UE-to-UE Relay responds a Direct Communication Accept message to the source UE to complete the PC5 connection establishment procedure.

3. The target UE performs the secure PC5 link establishment procedure with the UE-to-UE relay in the same manner as source UE.

4. The source UE and the target UE establish a secure connection between them.

NOTE 3: How to establish a secure connection between the source UE and the target UE is not addressed in the present document.

#### 6.5.2.2 PC5 link security establishment procedure over Control Plane

The PC5 link security establishment procedure over Control Plane for 5G ProSe UE-to-UE Relay, as follows:



Figure 6.5.2.2-1: PC5 link security establishment procedure over Control Plane for 5G ProSe UE-to-UE Relay

NOTE 1: Figure 6.5.2.2-1 shows the security procedure of the non-roaming for 5G ProSe UE-to-UE Relay services. In this figure, the source UE and the target UE and UE-to-UE Relay use a subscription of the same PLMN.

0. The source UE and the target UE and the UE-to-UE Relay shall be registered with the network. The UE-to-UE Relay shall be authenticated and authorized by the network to provide UE-to-UE Relay service. The source UE and the target UE shall be authenticated and authorized by the network to receive UE-to-UE Relay service. Discovery security material and PC5 security policies are provisioned to the source UE and the target UE and the UE-to-UE Relay respectively during this authorization and information provisioning procedure.

NOTE 2: The detail of discovery procedure is not addressed in the present document.

1. The source UE performs the discovery procedure and discover the target UE via UE-to-UE Relay.

Editor’s Note: UE-to-UE discovery and communication establish will align with SA2 WG2.

2a. The source UE sends a Direct Communication Request (DCR) that contains its security capabilities and PC5 signalling security policy, the PRUK ID or a SUCI if the source UE does not have a valid PRUK, RSC of the 5G ProSe UE-to-UE Relay service and Nonce\_1.

Editor’s Note: Its FFS whether the included parameters in Direct Communication Request message in step 2 can be protected by the discovery keys similar as to the Direct Communication Request message when establishing a secure PC5 link in between Remote UE and UE-to-network relay as described in TS 33.503 [6].

2b. The source UE and the UE-to-UE Relay perform the same authorization and key establishment procedure over Control Plane as 5G ProSe UE-to-Network Relay. According the PC5 key hierarchy over control plane as defined in clause 6.3.3.3.3 of TS 33.503 [6], the PRUK of source UE (Remote UE) will not be shared by 5G ProSe UE-to-Network Relay service and 5G ProSe UE-to-UE Relay service. The source UE performs an 5G ProSe Remote UE specific authentication independent of 5G ProSe UE-to-Network Relay service and derive the PRUK from KAUSF-P by using the RSC of 5G ProSe UE-to-UE Relay service.

2c. When receiving a KNR\_ProSe from the AUSF of the source UE via the AMF of UE-to-UE Relay, the UE-to-UE Relay derive the PC5 session key (Krelay-SESS) from KNR\_ProSe and then derive the confidentiality key (Krelay-enc) (if applicable) and integrity key (Krelay-int) based on PC5 policies. The UE-to-UE Relay sends a Direct Security mode command message to the source UE. This message also include the received Nonce\_2 and source UE’s PC5 signalling security policy and be integrity protected using Krelay-int. EAP Success message also be included if received from the AMF.

2d. The source UE generate the KNR\_ProSe key in the same way as its AUSF, and derive the PC5 session key Krelay-sess and confidentiality and integrity keys from KNR\_ProSe and process the Direct Security Mode Command. Successful verification of the Direct Security Mode Command assures the source UE that the UE-to-UE Relay is authorized to provide the relay service.

The source UE send the Direct Security Mode Complete message containing its PC5 user plane security policies to the UE-to-UE relay, which is protected by Krelay-int or/and Krelay-enc according to the negotiated PC5 signalling policies between the source UE and the UE-to-UE Relay.

2e. After the successful verification of the Direct Security Mode complete message, the UE-to-UE Relay responds a Direct Communication Accept message to the source UE to finish the PC5 connection establishment procedures and store the 5GPRUK ID in the security context associated to the PC5 link with the source UE.

3. The target UE performs the secure PC5 link establishment procedure with the UE-to-UE relay in the same manner as source UE.

4. The source UE and the target UE establish a secure connection between them.

NOTE 3: How to establish a secure connection between the source UE and the target UE is not addressed in the present document.

### 6.5.3 Evaluation

TBD

6.6 Solution #6: End-to-end security establishment for Layer-2 UE-to-UE relay

6.6.1 Introduction

This solution addresses security requirement for providing confidentiality, integrity protection of end-to-end information exchanged between the peer UEs over the L2 UE-to-UE Relay in key issue #2.

6.6.2 Solution details

6.6.2.1 End-to-end security establishment for Layer-2 UE-to-UE relay



Figure 6.6.2.1: End to end security establishment for Layer-2 UE-to-UE relay

1. Service authorisation and policy provisioning is performed for the Source UE, Target UE and UE-to-UE Relay.

2. Source UE has selected a suitable UE-to-UE Relay and received the Layer-2 ID of the target UE after Model A or Model B discovery. Source UE decides to connect with target UE via the selected UE-to-UE Relay.

3. The Source UE and Target UE may need to setup or modify the PC5 link with UE-to-UE Relay.

4. After PC5 link between source UE and UE-to-UE relay, UE-to-UE relay and target UE sets up, the E2E PC5 link establishment performs. The source UE sends a Direct Communication Request message to initiate the E2E PC5 link establishment procedure with the target UE.

Editor’s Note: In addition to the security end-to-end information, what information is included in the DCR message is determined by SA2.

To establish the End-to-End security between source UE and target UE, the message includes RSC, source UE’s security capability and source UE’s security policy. This message may include shared security credential ID between source UE and target UE to generate KD, or if there exists a shared key KD between source UE and target UE, the message may include KD ID, Nonce\_1 (for session key KD-sess generation), and the most significant 8-bits of the KD-sess ID (for uniquely identifying KD-sess at source UE).

Note 1: The provisioning of security credentials and security credential ID in the Source UE and Target UE is out of 3GPP scope.

The privacy information of source UE such as source UE’s security capability and security policy, Nonce\_1 can be protected by these security per-hop links between source UE and UE-to-UE relay, UE-to-UE relay and target UE.

5. During the Direct Auth and Key Establishment, several authentication signallings are exchanged between the peer UEs to derive the shared key KD based on the shared credential between source UE and target UE.

Note 2: How the source UE and the target UE generate the shared key KD is not addressed in this solution.

6a. In case the target UE decides to active the End-to-End security protection, based on source UE’s security policy, target UE choose Nonce\_2 and generates the session key KD-sess as specified in clause 6.6.2.3.1, selects integrity and encryption algorithms from Source UE’s capability, generates integrity and encryption keys as specified in clause 6.6.2.3.2. The target UE may choose LSB of KD-sess ID, forms KD-sess ID, and stores KD-sess ID with KD-sess. The target UE may choose the MSB of KD ID to uniquely identify KD at target UE if a new KD is generated.

6b. The target UE activates the integrity protection before sending the Direct Security Mode message if the U2U relay integrity key KD-int has been derived.

7. The target UE sends the Direct Security Mode message to source UE through UE-to-UE relay, including Source UE’s security capabilities, Source UE’s security policy to protect from bidding down attack. The message also includes Nonce\_2, LSB of KD-sess ID, chosen\_algs, and MAC for integrity protection, or the message may include MSB of KD ID.

8a. Upon reception of the Direct Security Mode message from the UE-to-UE Relay, the source UE generates the session key KD-sess as specified in clause 6.6.2.3.1. According to the chosen\_algs from target UE, source UE generates integrity and encryption keys as specified in clause 6.6.2.3.2. The source UE forms KD-sess ID from the received LSB of KD-sess ID and chosen MSB of KD-sess ID, and stores KD-sess ID with KD-sess. Or, if a new KD is generated, the source UE forms KD ID from the received MSB of KD ID and chosen LSB of KD ID, and stores the complete KD ID with KD.

8b. The source UE verifies the integrity protection using the indicated integrity algorithm in chosen\_algs and the generated integrity key. After the successful verification, source UE starts integrity and encryption protection before sending the Direct Security Mode Complete message.

9. The source UE sends the Direct Security Mode Complete message to target UE through the UE-to-UE Relay, which may contain the LSB of KD ID if a new KD is generated.

10. Upon reception of the Direct Security Mode Complete message from the UE-to-UE Relay, the target UE deciphers and checks the integrity protection on the Direct Security Mode Complete message. The target UE may form the KD ID and store it with KD.

11. The Target UE sends a Direct Communication Accept message to the Source UE. The Direct Communication Accept message includes User Info ID of Source UE, User Info ID of Target UE, QoS Info (PFI and PC5 QoS parameters) and RSC.

Editor’s Note: Whether to activate the integrity or confidentiality protection is based on the security policy of source UE and target UE, which is FFS.

Note 3: How the PC5-S messages in steps 4, 5, 7, 9, 11 are forwarded by the UE-to-UE Relay is to be determined by RAN2, such as based on an Adaptation layer.

6.6.2.2 Key Hierarchy for UE-to-UE relay

There are 4 different layers of keying material as shown in figure 6.6.2.2-1.



Figure 6.6.2.2-1: Key Hierarchy for UE-to-UE relay

* Security Credentials: Upon successful configuration procedure, each UE will be configured with the credentials which include a public/private key pair. Authentication signallings are exchanged between source UE and target UE via UE-to-UE relay to derive the KD.
* KD: This is a root key that is shared between source UE and target UE that communicating using UE-to-UE relay link. It may be refreshed by re-running the authentication signallings using the security credentials. Nonces are exchanged between the UEs and used with the KD to generate a KD-sess (the next layer of keys). The KD ID is used to identify KD.
* KD-sess: This key is derived by source UE and target UE from KD and is used derive keys that to protect the transfer of data between the peer UEs. The actual keys (see next bullet) that are used in the confidentiality and integrity algorithms are derived directly from KD-sess. The KD-sess ID identifies the KD-sess ID.
* KD-enc, KD-int: The U2U relay Encryption Key (KD-enc) and Integrity Key (KD-int) are used in the chosen confidentiality and integrity algorithms respectively for protecting control plane data and user plane data between source UE and target UE.

6.6.2.3 Key derivation functions

6.6.2.3.1 KD-sess derivation function

The KD-sess derivation function is specified in clause A.3 of TS 33.536 [2], and the input key is KD.

6.6.2.3.2 Integrity and encryption keys derivation function

The integrity key KD-int and encryption key KD-enc derivation function are specified in clause A.2 of TS 33.536 [2], and the input key is KD-sess.

6.6.3 Evaluation

TBD.

## 6.7 Solution #7: Non-network-assited Security Establishment Procedure for 5G ProSe Layer-3 UE-to-UE Relay

### 6.7.1 Introduction

The solution addresses Key Issue #2: Security of UE-to-UE Relay. It largely reuses the mechanism of Direct Security Establishment procedure defined in TS 33.503 [6] to ensure the security of UE-to-UE Relay Communication.

For Layer-3 UE-to-UE Relay, the full security of a UE-to-UE PC5 link depends on the security of two separate PC5 links, i.e. the link between the Source UE and UE-to-UE Relay and the link between UE-to-UE Relay and Target UE. The security of these two separate PC5 link relies on the security materials (i.e. the long term credential), which can be pre-configured on the 5G ProSe UE (incl. Source UE, Target UE and UE-to-UE Relay) or provisioned by the network during the service authorization procedure. In other words, all the ProSe UEs can obtain the security materials without the assistance of network. Therefore, the Source UE and the Target UE can establish the UE-to-UE PC5 link via Layer-3 UE-to-UE Relay regardless of whether they are within or out of network coverage.

### 6.7.2 Solution details

 Figure 6.7.2-1: Non-network-assited PC5 link security establishment procedure for 5G ProSe Layer-3 UE-to-UE Relay

0. The long term credential and long term credential ID are associated with RSC, which could be pre-configured on the 5G ProSe UE (incl. Source UE, Target UE and UE-to-UE Relay) or provisioned by the network e.g. during Service Authorization and Provisioning procedure before the U2U discovery procedure.

Note 1: How to pre-configure the long term credential to UE is out of the 3GPP scope.

1. The Discovery & Relay Selection procedure is performed between the peer UEs and the UE-to-UE Relay.

Note 2: It is assumed that after the Discovery & Relay Selection procedure, the Source UE (UE1) and the Target UE (UE2) can discover each other by selecting the same UE-to-UE Relay.

2. The Source UE sends a Direct Communication Request that contains the long term credential ID, Source UE’s security capabilities, RSC and nonce 1 to the UE-to-UE Relay as specified in the TS 33.503 [6]. The message may also include a Knrp ID if the Source UE has an existing Knrp with this UE-to-UE Relay for the same RSC.

3. The UE-to-UE Relay may initiate a Direct Auth and Key Establish procedure with Source UE to generate the Knrp. If the Knrp ID is included in the Direct Communication Request, this step is skipped.

4. The UE-to-UE Relay derives the session key (KNRP-SESS) from KNRP and then derives the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies as specified in TS 33.503 [6]. The UE-to-UE Relay sends a Direct Security Mode Command message to the Source UE. This message also includes the chosen security algorithm and nonce 2.

5. The Source UE responds with a Direct Security Mode Complete message to the UE-to-UE Relay.

6. The UE-to-UE Relay sends a Direct Communication Request that contains the long term credential ID, the chosen security algorithm, RSC and nonce 1' to the Target UE as specified in the TS 33.503 [6]. The message may also include a Knrp ID' if the UE-to-UE Relay has an existing Knrp' with this Target UE under the same RSC.

Note 3: How the U2U relay determiness to send DCR to UE2 is determined by SA2.

7. The Target UE may initiate a Direct Auth and Key Establish procedure with UE-to-UE Relay to generate the Knrp'. If the Knrp ID' is included in the Direct Communication Request, this step is skipped.

8. The Target UE derives the session key (KNRP-SESS’) from KNRP’ and then derives the confidentiality key (NRPEK') (if applicable) and integrity key (NRPIK') based on the PC5 security policies. The Target UE sends a Direct Security Mode Command message to the UE-to-UE Relay. This message also includes the nonce 2'.

9. The UE-to-UE Relay responds with a Direct Security Mode Complete message to the Target UE.

10. The Target UE sends the Direct Communication Accept message to the UE-to-UE Relay.

11. Only receiving the Direct Communication Accept message from the Target UE, the UE-to-UE Relay then responds with the Direct Communication Accept message to the Source UE.

Editor’s Note: Solution details will be studied based on SA2’s conclusion about the KI#1 in TR 23.700-33 [2].

12. The secure Layer-3 PC5 link between the Source UE and the Target UE via the UE-to-UE Relay is established. The UE-to-UE Relay can forward the traffic between the peer Prose UEs.

### 6.7.3 Evaluation

TBD

## 6.8 Solution #8: Restricted 5G ProSe UE-to-UE Relay Discovery Model A

### 6.8.1 Introduction

The solution addresses Key Issue #1: Security for UE-to-UE Relay discovery. It largely reuses the mechanism of Prose Discovery defined in TS 33.503 [6] to ensure the security of UE-to-UE Relay Discovery.

If the Source UE cannot reach the Target UE directly, it will try to discover a UE-to-UE Relay, which is responsible for providing relay service in connecting two Remote UEs over PC5. In the Model A method of the ProSe discovery, the UE-to-UE Relay plays the role of the Announcing UE and broadcasts the announcement message to all the UEs in proximity. To protect the announcement message, the UE-to-UE relay needs to request the security parameters from the DDNMF in the control plane or the PKMF in the user plane.

The solution meets all the security requirements in Key issue #1 by achieving privacy protection, protection of messages and security materials provisioning.

### 6.8.2 Solution details

#### 6.8.2.1 Restricted 5G ProSe UE-to-UE Relay Discovery Model A over Control Plane

 Figure 6.8.2.1-1:

According to TS 23.304 [8], the ProSe Application Server allocates a Restricted ProSe Application User ID (RPAUID) for each ProSe UE and returns the RPAUID to the application client in the UE.

As defined in the TR 23.700-33 [2] Solutions 10, 12, 30 and 33, the UE-to-UE Relay can discover other UEs in proximity via the previous U2U discovery or U2U communication procedures, the UE-to-UE Relay may buffer their RPAUID as Discovered UE ID. The Discovered UE ID will be removed by UE-to-UE Relay in case the buffer timer expired.

Steps 1-3 refer to the Relay Discovery Key Request procedure of UE-to-UE Relay. For the 5G ProSe UE-to-UE Relay Discovery, the UE-to-UE Relay plays the role of the Announcing UE.

1. UE-to-UE Relay sends a Relay Discovery Key Request message containing its Restricted ProSe Application User ID (RPAUID) and Relay Service Code (RSC) to its 5G DDNMF in order to get the associated security material. In addition, the UE-to-UE Relay includes its PC5 UE security capability that contains the list of supported ciphering algorithms by the UE-to-UE Relay in the Relay Discovery Key Request message.

Note a: The RSC may either be pre-configured on the UE or provisioned by the network during the service authorization and provisioning procedure.

Editor’s Note: Detailed parameters used in Relay Discovery Key Request procedure is FFS.

2. The 5G DDNMF of the UE-to-UE Relay may check for the announcement authorization with the PCF/UDM of the UE-to-UE relay or the ProSe App Server.

Note b: If the UE-to-UE relay is roaming, the 5G DDNMFs in the HPLMN and VPLMN of the UE-to-UE Relay may exchange Announcement Auth, which is omitted in the above figure.

3. The 5G DDNMF of the UE-to-UE Relay returns the corresponding Code-Sending Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters. The Code-Sending Security Parameters are stored with the RSC, which provide the necessary information for the UE-to-UE Relay. The 5G DDNMF of the UE-to-UE Relay includes the chosen PC5 ciphering algorithm in the Relay Discovery Key Response message, which is determined by the RSC and the received PC5 UE security capability in step 1.

Steps 4-9 refer to the Relay Discovery Key Request procedure of Source UE/Target UE. For the 5G ProSe UE-to-UE Relay Discovery, the Source UE and Target UE play the role of the Monitoring UE.

4. The Source UE/Target UE sends a Relay Discovery Key Request message containing its RPAUID, RSC, its PC5 UE security capability and the Relay RPAUID(s) to its 5G DDNMF in order to be allowed to monitor for one or more UE-to-UE Relay.

Note c: The application client provides the Source UE/Target UE with the list of potential UE-to-UE Relay containing the Relay RPAUID(s). The Relay RPAUID(s) of Source UE/Target UE to be monitiored are passed in an Application Lever Container.

5. The 5G DDNMF of the Source UE/Target UE sends an authorization request to the PCF/UDM of the Source UE/Target UE or the ProSe App Server. If the Source UE/Target UE is allowed to monitor the announcement message under this specific U2U relay service, the PCF/UDM of the Source UE/Target UE or the ProSe App Server returns an authorization response.

6. If the Relay Discovery Key Request is authorized, and the PLMN ID in the Relay RPAUID(s) indicates a different PLMN, the 5G DDNMF of the Source UE/Target UE contacts the indicated PLMN's 5G DDNMF (i.e. the 5G DDNMF of the UE-to-UE Relay) by sending a Monitor Request message including the PC5 UE security capability received in step 4.

7. The 5G DDNMF of the UE-to-UE Relay may exchange authorization messages with the ProSe App Server. The ProSe Application Server may check whether the Source UE/Target UE and the UE-to-UE Relay are authorized to perform the U2U discovery under the specific U2U relay service.

8. If the Monitor Request is authorized and the PC5 UE security capability in step 4 includes the chosen PC5 ciphering algorithm, the 5G DDNMF of the UE-to-UE Relay responds to the 5G DDNMF of the Source UE/Target UE with a Monitor Response message including the corresponding Code-Receiving Security Parameters and the chosen PC5 ciphering algorithm. The Code-Receiving Security Parameters provide the information needed by the Source UE/Target UE to undo the protection applied by the UE-to-UE relay. The 5G DDNMF of the Source UE/Target UE stores the RSC and the Code-Receiving Security Parameters.

9. The 5G DDNMF of the Source UE/Target UE returns the Code-Receiving Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters and the chosen PC5 ciphering algorithm. The Source UE/Target UE stores Code-Receiving Security Parameters, and the chosen PC5 ciphering algorithm together with the RSC.

Steps 10 and 11 occur over PC5:

10. The UE-to-UE relay broadcasts the U2U Relay announcement message and protects it by using the corresponding Code-sending security parameters. The U2U announcement message may contain the Type of Discovery (i.e. U2U relay), RSC and Discovered UE ID (i.e. RPAUID of discovered UEs in proximity via the previous U2U Discovery or U2U Communication), etc..

11. The Source UE/Target UE listens to the announcement message that satisfies its RSC if the UTC-based counter associated with that discovery slot is within the MAX\_OFFSET of the Source UE/Target UE's ProSe clock. In order to find such a matching message, it processes the message. Only if the integrity check is passed, the UE can decide if it can use this UE-to-UE relay according to RSC and Discovered UE ID(s). If the UE wants to communicate with other UEs via this relay, the UE may initiate the U2U relay link establishment procedure.

Note d: The Source UE/Target UE may check the integrity of the announcement message on its own or check the integrity by sending a Match Report as defined in TS 33.503 [6].

Editor’s Note: Solution details will be studied based on SA2’s conclusion about the KI#1 in TR 23.700-33[2].

#### 6.8.2.2 Restricted 5G ProSe UE-to-UE Relay Discovery Model A over User Plane

When the user-plane based security procedure for the UE-to-UE Relay discovery is used, the 5G PKMF takes the role of the 5G DDNMF as described in 6.8.2.1 of the present document.

Editor’s Note: It is FFS whether both CP and UP based procedures are needed for security materials provisioning.

### 6.8.3 Evaluation

TBD

## 6.9 Solution #9: Restricted 5G ProSe UE-to-UE Relay Discovery Model B

### 6.9.1 Introduction

The solution addresses Key Issue #1: Security for UE-to-UE Relay discovery. It largely reuses the mechanism of Prose Discovery defined in TS 33.503 [6] to ensure the security of UE-to-UE Relay Discovery.

If the Source UE cannot reach the Target UE directly, it will try to discover a UE-to-UE Relay, which is responsible for providing relay service in connecting two Remote UEs over PC5. In the Model B method of the ProSe discovery, the Source UE plays the role of the Discoverer UE, the Target UE plays the role of the Discoveree UE and the UE-to-UE Relay forwards all the messages between the Source UE and the Target UE. To achieve the security of UE-to-UE Relay Discovery, the UEs need to request the security parameters from the DDNMF in the control plane or the PKMF in the user plane.

The solution meets all the security requirements in Key issue #1 by achieving privacy protection, protection of messages and security materials provisioning.

### 6.9.2 Solution details

#### 6.9.2.1 Restricted 5G ProSe UE-to-UE Relay Discovery Model B over Control Plane

 Figure 6.9.2.1-1:

According to TS 23.304 [8], the ProSe Application Server allocates a Restricted ProSe Application User ID (RPAUID) for each Prose UE and returns the RPAUID to the application client in the UE.

Steps 1-3 refer to the Discovery Key Request procedure of UE-to-UE Relay.

1. UE-to-UE Relay sends a Relay Discovery Key Request message containing its RPAUID and Relay Service Code (RSC) to its 5G DDNMF in order to get associated security materials. In addition, the UE-to-UE Relay includes its PC5 UE security capability that contains the list of supported ciphering algorithms by the UE in the Relay Discovery Key Request message.

Note a: The RSC may either be pre-configured on the UE or provisioned by the network during the service authorization and provisioning procedure.

Editor’s Note: Detailed parameters used in Relay Discovery Key Request procedure is FFS.

2. The 5G DDNMF of the UE-to-UE Relay may check for the announcement authorization with the PCF/UDM of the UE-to-UE Relay or the ProSe App Server depending on the local configuration.

Note b: If the UE-to-UE relay is roaming, the 5G DDNMFs in the HPLMN and VPLMN of the UE-to-UE Relay may exchange Announcement Auth message, which is omitted in the above figure.

3. The 5G DDNMF of the UE-to-UE Relay returns the Code Security Parameters along with the CURRENT\_TIME and MAX\_OFFSET parameters and the chosen PC5 ciphering algorithm. The Code Security Parameters are stored with the RSC, which provides the necessary information for the UE-to-UE relay. The 5G DDNMF of the UE-to-UE Relay includes the chosen PC5 ciphering algorithm in the Relay Discovery Key Response message, which is determined by the RSC and the received PC5 UE security capability in step 1.

Steps 4-9 refer to the Relay Discovery Key Request procedure of Discoveree UE/Discoverer UE. For the 5G ProSe UE-to-UE Relay Discovery, the Source UE plays the role of the Discoverer UE and the Target UE plays the role of the Discoveree UE.

4. The Source UE/Target UE sends a Relay Discovery Key Request message containing the RPAUID, RSC, its PC5 UE security capability and the Relay RPAUID(s) to its 5G DDNMF in order to be allowed to discover one or more UE-to-UE Relay.

Note c: The application client provides the Source UE/Target UE with the list of potential UE-to-UE Relay containing the Relay RPAUID(s). The Relay RPAUID(s) of Source UE/Target UE to be monitiored are passed in an Application Lever Container.

5. The 5G DDNMF of the Source UE/Target UE sends an authorization request to the PCF/UDM of the Source UE/Target UE or the ProSe App Server. If the Source UE/Target UE is allowed to perform UE-to-UE Relay Discovery procedure under this specific U2U relay service, the PCF/UDM of the Source UE/Target UE or the Prose App Server returns an authorization response.

6. If the Relay Discovery Key Request is authorized, and the PLMN ID in the Relay RPAUID indicates a different PLMN, the 5G DDNMF of the Source UE/Target UE contacts the indicated PLMN's 5G DDNMF (i.e. the 5G DDNMF of the UE-to-UE Relay) by sending a Discovery Request message including the PC5 UE security capability in step 4.

7. The 5G DDNMF of the UE-to-UE Relay may exchange authorization messages with the ProSe Application Server. The ProSe Application Server may check whether the Source UE/Target UE and the UE-to-UE relay are authorized to perform the UE-to-UE Relay Discovery under the specific U2U relay service.

8. If the Discovery Request is authorized and the PC5 UE security capability in step 4 includes the chosen PC5 ciphering algorithm, the 5G DDNMF of the UE-to-UE Relay responds to the 5G DDNMFof the Source UE/Target UE with a Discovery Response message including the Code Security Parameters and a chosen PC5 ciphering algorithm. The Code Security Parameters provide the information needed by the Source UE/Target UE to protect/unprotect all discovery messages under the specific U2U relay service. The 5G DDNMF of the Source UE/Target UE stores the RSC and Code Security Parameters.

9. The 5G DDNMF of the Source UE/Target UE returns the Code Security Parameters along with the CURRENT\_TIME, MAX\_OFFSET parameters and the chosen PC5 ciphering algorithm. The Source UE/Target UE stores the Code Security Parameters together with the RSC.

Steps 10 and 13 occur over PC5:

10. The Source UE broadcasts the Solicitation Message and protects it by using the corresponding code security parameters. The Solicitation Message may contain the Type of Discovery (i.e. U2U relay), RSC, source UE info (i.e. RPAUID of the Source UE) and target UE info (i.e. RPAUID of Target UE), etc..

11. The UE-to-UE Relay listens to a solicitation Message that satisfies the RSC if the UTC-based counter associated with that discovery slot is within the MAX\_OFFSET of the UE-to-UE Relay's ProSe clock. On receiving the solicitation message including the supported RSC, UE-to-UE Relay(s) process it by using the corresponding code security parameters. If the integrity check/confidentiality check is passed, the UE-to-UE Relay adds the relay information in the solicitation message and broadcasts the new solicitation message, which is protected by the corresponding code security parameters. The new solicitation message may contain the Type of Discovery, Relay Info (i.e. RPAUID of UE-to-UE Relay), RSC, Relay indication (to indicate ProSe direct discovery forwarding), original Discoverer Info (i.e. RPAUID of Source UE) and target discoveree info (i.e. RPAUID of Target UE).

12. The Target UE listens to the solicitation Message that satisfies its RSC if the UTC-based counter associated with that discovery slot is within the MAX\_OFFSET of the Target UE's ProSe clock. If the integrity check/ confidentiality check is passed, the Target UE responds to the solicitation message via a response message.

Note d: The Source UE/Target UE may check the integrity of the discovery message on its own or check the integrity by sending a Match Report as defined in TS 33.503 [6].

13. On receiving the response message, UE-to-UE Relay(s) checks its integrity and confidentiality based on the security policies. If the check is passed, UE-to-UE relay forwards response message containing the Type of Discovery, Relay Info (i.e. RPAUID of Relay), RSC, Relay indication (to indicate ProSe direct discovery forwarding), original Discoveree Info (i.e. RPAUID of Target UE) and Discoverer Info (i.e. RPAUID of Source UE).

On receiving the response message from UE-to-UE relay, Source UE checks its integrity and confidentiality based on the security policies and determines if it can use this relay. If the Source UE wants to communicate with the Target UE via this Relay, the Source UE may initiate the U2U relay link establishment procedure.

Note e: The UE-to-UE relay selection may be performed on the Target UE or Source UE.

Editor’s Note: Solution details will be studied based on SA2’s conclusion about the KI#1 in TR 23.700-33 [2].

#### 6.9.2.2 Restricted 5G ProSe UE-to-UE Relay Discovery Model B over User Plane

When the user-plane based security procedure for the UE-to-UE Relay discovery is used, the 5G PKMF takes the role of the 5G DDNMF as described in 6.9.2.1 of the present document.

Editor’s Note: It is FFS whether both CP and UP based procedures are needed for security materials provisioning.

### 6.9.3 Evaluation

TBD

## 6.10 Solution #10: PAKE-based security for UE-to-UE relay

### 6.10.1 Introduction

This solution addresses Key Issue #2 and Key Issue #3.

This solution proposes the usage of a password-based key establishment (PAKE) for UE-to-UE relay security and authorization. A PAKE allows establishing a secure channel while authenticating the peers based on a password. The PAKE is used to setup the security between:

* the source UE (S-UE) and the UE-to-UE Relay (UE2UE),
* the target UE (T-UE) and the UE2UE and
* the S-UE and the T-UE.

The password(s) may be configured in an initial authorisation and parameter provisioning phase when the UEs are in coverage. When this is done, it is ensured that the network remains on control of the UE-to-UE relay secure communication. However, the password(s) may also be entered by a user or generated by the involved devices, e.g., when one of more of the devices are out-of-coverage. This option ensures that the security requirements can be fulfilled even in challenging operational cases.

Furthermore, the usage of a PAKE provides a reasonable approach authentication/authorization of the communicating parties:

* using a balanced PAKE authenticates two peers in a similar role, e.g., source and target UE;
* using an augmented PAKE can be used to differentiate roles, e.g., the role of a UE-to-UE relay and the role of a source/target UE preventing impersonation.

For cases in which these authorisation capabilities are not enough, this solution proposes the optional use of authorization tokens and policies -- deployed in the initial authorisation and parameter provisioning phase – for enhanced authorization capabilities.

### 6.10.2 Solution details

Figure 6.10.2-1 depicts the steps of this solution.



**Figure 6.10.2-1**

The required steps are as follows:

* Step 0 is the initial authorization and parameter provisioning of S-UE, UE2UE and T-UE.
* Steps 1 and 2 involve the exchange of an initial Direct Communication Request (DCR) message.
* Step 3 involves the setup of a secure authenticated channel between UE2UE and T-UE based on a PAKE.
* Step 4 involves an optional authorization phase.
* Step 5 involves the exchange of Direct Communication Accept (DCA) from T-UE to UE2UE.
* Step 6 involves the setup of a secure authenticated channel between S-UE and UE2UE based on a PAKE.
* Step 7 involves an optional authorization phase.
* Step 8 involves the exchange of DCA from UE2UE to S-UE.
* Step 9 involves the setup of a secure authenticated channel between S-UE and T-UE based on a PAKE.
* Step 10 involves an optional authorization phase.
* Step 11 involves the exchange of DCA from T-UE to S-UE.

The PAKE in Steps 3, 6, and 8 may rely on a password shared amongst both UEs (in case of balanced PAKE), or a password and a password derived value (in case of augmented PAKE) that might be, e.g., pre-configured in Step 0. This password may also be entered in the involved devices by the users or generated by the devices and exchanged out-of-band.

The PAKE in Steps 3 and 6 may be an augmented PAKE in which, e.g., the Target UE (or Source UE) does not have access to the password itself, but a password-derived value used in the augmented PAKE and from which the actual password can only be retrieved by means of an offline dictionary attack. This prevents the target UE (or Source UE) from impersonating the UE2UE.

The PAKE in Steps 3, 6, and 8 allow the communicating parties to authenticate to each other and establishing symmetric-cryptographic keys used to protect the communication link. This process provides a certain level of authorization, e.g., if two UEs share a same password (-derived) value, the authentication will be successful fulfilling authorization requirements in many scenarios.

Note 1: The PAKE choice and details are left to normative phase.

The optional authorization phase in Steps 4, 7, and 9 might be required when one of the devices requires further authorisation assurances. This phase relies on the exchange of authorization tokens and policies configured in Step 0. For instance, in Step 4, the target UE can send an authorization token so that the UE2UE can verify that the target UE is indeed entitled to use the UE2UE relay.

Note 2: Details on the optional authorization phase in Steps 4, 7, and 9 are left to normative phase.

The message flow in Figure 6.Y.2-1 can be adapted to other message flows, e.g., relying on discovery messages. For instance, the S-UE can send a Discovery Solicitation message towards the T-UE through the UE2UE. The T-UE replies with a Discovery Response message towards the S-UE through the UE2UE. Next, S-UE and UE2UE can establish a secure PC5 interface relying on a PAKE. Next, UE2UE and T-UE can establish a secure PC5 interface relying on a PAKE. And finally, S-UE and T-UE can establish a secure PC5 interface (assuming an L2 UE2UE) based on a PAKE.

This PAKE based solution can be either fully in ProSe scope or partial ProSe scope. In partial ProSe scope, it is required the ProSe definition of at least (1) parameters to be provisioned, (2) parameters exchanged prior to the PAKE itself, and (3) method to provision a password in out-of-coverage situations. In full ProSe scope, it is required the choice of at least a PAKE protocol. Full ProSe scope provides increased interoperability.

#### 6.10.2.1 Parameter provisioning in-coverage and out-of coverage

The provisioning of passwords can be done either in coverage or out-of-coverage in Step 0.

When the provisioning is done when a UE is in coverage, the UE is configured with one or multiple passwords “raw-passwords” or “password-derived tokens”.

Each “raw-password” or “password-derived token” is associated to “metadata”. The “metadata” includes “password hint”, “expiration date”, and “access rights”. The field “password hint” indicates which password to use; the field “expiration date” indicates how long a password is valid; the field “access rights” indicates which authorization provides a password. The bitstring used as “password” in a PAKE is computed as the KDF of the “raw-password” and the associated metadata fields. In the case of an augmented PAKE, the “password-derived token” is derived from the “password” itself.

As in other solutions, the parameters can be received from the 5G PKMF and 5G DDNMF when the UE is in coverage.

During provisioning in-coverage, a UE is also provisioned with an “out-of-coverage policy” determining whether a UE may use a temporary password entered or provisioned by the user when the UE is out-of-coverage. When the UE is then out-of-coverage, a UE can be provisioned with a temporary password entered by the user if “out-of-coverage policy” allows for it.

Note 3: Details on how a UE can be provisioned with a temporary password in an out-of-coverage situation (out of band, keyboard, QR code,…) are left to normative phase.

#### 6.10.2.2 PAKE protocols

There are many PAKE protocols in the literature. Specific PAKE protocols that are of special interest are IETF PAKE protocols in discussion and/or standardization at IRTF CFRG, e.g., CPAKE[10], OPAQUE[11], SPAKE2[12] or SPAKE2+[13]. CPAKE and SPAKE2 are balanced PAKE protocols. OPAQUE and SPAKE2+ are augmented PAKE protocols. While CPAKE and OPAQUE have been formally endorsed in the PAKE selection process by IRTF CFRG as balanced and augmented options, the choice of SPAKE2 and SPAKE2+ as balanced and augmented PAKE protocols, respectively, is also meaningful due to the similarity between.

#### 6.10.2.3 Parameters exchanged prior to the PAKE execution

Several parameters need to be exchanged prior to the PAKE execution in Steps 3, 6, and 9. These parameters include:

* The Relay Service Code,
* A “password hint” used to identify the “raw password”. In the absence of an explicit password hint, then the RSC that serves as password hint, i.e., the password is linked to the RSC.

In particular,

* The DCR message in Step 1 includes the RSC and password-hints for the PAKEs in Steps 6 and 9.
* The DCR message in Step 2 includes the RSC and password-hints for the PAKEs in Steps 3 and 9.

When the UE2UE relay receives message of Step 1, the UE2UE relay may remove the password hint for the PAKE in Step 6. Furthermore, the UE2UE relay adds its password hint for the PAKE to the DCR message in Step 2.

When the target UE receives message in Step 2, the target UE starts the PAKE in Step 3 based on the received password hint.

#### 6.10.2.4 PAKE execution

This subsection explains how a PAKE can be executed in the context of SPAKE2 and SPAKE2+ that involve the exchange of four messages as explained in Clause 3.1 in [x3][x4].

The first and second PAKE messages are exchanged in a *Direct Auth and Key Establish Request* and a *Direct Auth and Key Establish Response* messages, respectively.

The third and fourth messages are exchanged in the *Direct Security Mode Command* and the *Direct Security Mode Complete*, respectively.

#### 6.10.2.5 Secure exchange of data

The secure exchange of data relies on a shared key Ks between two UEs result of the PAKE. This key Ks is K\_shared as defined in Clause 3.4 in [x4] or TT as defined in Clause 4 in [x3].

For a L2 UE2UE relay, Ks is used as shared secret to derive PC5 keys for user/control planes and encryption/integrity by means of a key derivation function according to TS 33.220.

For a L3 UE2UE relay, Ks is used to derive a PSK hint and a PSK. PSK and PSK hint are used in IKE-PSK to secure the L3 communication by means of a key derivation function according to TS 33.220.

Note: Details related to the inputs to the KDF such FC value or other identifiers are left to normative phase.

### 6.10.3 Evaluation

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

Note: Whether PAKE based authentication is in Prose or Application layer scope is FFS.

## 6.11 Solution #11: Security for UE-to-UE Relay (Model A) discovery

### 6.11.1 Introduction

This solution addresses Key Issue #1 (as defined in clause 5.1). This solution is based on the solutions in TR23.700-33[2], the UE-to-UE Relay may perform Direct Discovery Model A or Model B to discover Target UE in advance.

In this solution, during UE-to-UE Relay model A discovery, the announcement discovery message sent and received between the source/target UE and the UE-to-UE Relay can be protected by using the discovery key associated with the RSC, which is obtained from the DDNMF of the HPLMN of the UE-to-UE Relay pointed by Relay’s RPAUID, and the RSC can carry one or more the ProSe Application information or associate with the ProSe Application information.

### 6.11.2 Solution details

6.11.2.1 Restricted 5G ProSe UE-to-UE Relay discovery Model A



Figure 6.11.1: Security procedure for UE-to-UE Relay discovery with Model A

NOTE 1: Figure shows the security procedure of the non-roaming for 5G ProSe UE-to-UE Relay discovery. In this figure, the source UE and the target UE and UE-to-UE Relay are in HPLMN.

Editor’s Note: Details parameters for relay discovery is FFS and it is based on SA2’s conclusion about the KI#1 TR23.700-33.

Editor’s Note: Details network function involved in relay discovery is FFS and it is based on SA2’s conclusion about the KI#1 TR23.700-33.

Step 1-4 refer to the Security procedure of UE-to-UE Relay

1. UE-to-UE Relay sends Relay Discovery Key Request message containing the Restricted ProSe Application User ID(RPAUID) and RSC to the 5G DDNMF in order to get the associated security material. In addition, the UE-to-UE Relay includes its PC5 UE security capability that contains the list of supported ciphering algorithms by the UE-to-UE Relay in the Relay Discovery Key Request message.

2. The 5G DDNMF may check for the UE-to-UE Relay authorization with the ProSe Application Server.

3. The 5G DDNMF of the UE-to-UE Relay returns the corresponding Code-Sending Security Parameter and Code-Receiving Security Parameter, along with the CURRENT\_TIME and MAX\_OFFSET parameters. The UE-to-UE Relay takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Announcing UE in step 4 of clause 6.1.3.1 of the TS 33.503 specification. The 5G DDNMF of the UE-to-UE Relay shall include the chosen PC5 ciphering algorithm in the Relay Discovery Key Response message. The 5G DDNMF determines the chosen PC5 ciphering algorithm based on the received PC5 UE security capability in step 1. The UE stores the chosen PC5 ciphering algorithm, Code-Sending Security Parameter and Code-Receiving Security Parameter together with the RSC.

Steps 4a-9a refer to Security procedure for Source UE

4a. The Source UE sends a Relay Discovery Key Request message containing the RPAUID, RSC and its PC5 UE security capability to the 5G DDNMF in order to be allowed to monitor for one or more RPAUIDs of UE-to-UE Relay UEs.

5a. The 5G DDNMF of the Source UE sends an authorization request to the ProSe Application Server. If, based on the RPAUID and RSC of Source UE, the RPAUID is allowed to discover at least one of the UE-to-UE Relay RPAUIDs contained in the Application Level Container, the ProSe Application Server returns an authorization response.

6a. If the Authorization Request is authorized in Step5a, and the PLMN ID in the UE-to-UE Relay RPAUID indicates a different PLMN, the 5G DDNMF of the Source UE contacts the indicated PLMN’s 5G DDNMF of UE-to-UE Relay by sending a Discovery Request message including the PC5 UE security capability and RSC received in step 4a.

7a. The 5G DDNMF of the UE-to-UE Relay may exchange authorization messages with the ProSe Application Server. ProSe Application Server may check whether the Source UE is authorised to implement UE-to-UE Relay Discovery under specific UE-to-UE Relay Service.

8a. If the PC5 UE security capability in step 4a includes the chosen PC5 ciphering algorithm, the 5G DDNMF of the UE-to-UE Relay responds to the 5G DDNMF of the Source UE with a Discovery Response message including the corresponding Code-Receiving Security Parameters, an optional Discovery User Integrity Key (DUIK), and the chosen PC5 ciphering algorithm. The Code-Receiving Security Parameters provide the information needed by the Source UE to undo the protection applied by the UE-to-UE Relay. The 5G DDNMF of the Source UE stores the RSC and the Code-Receiving Security Parameters.

9a. The 5G DDNMF of the Source UE returns the Code-Receiving Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters and the chosen PC5 ciphering algorithm. The Source UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Monitoring UE in step 9 of clause 6.1.3.1 of the TS 33.503 specification. The Source UE stores Code-Receiving Security Parameters and the chosen PC5 ciphering algorithm together with the RSC.

Steps 4b-9b refer to Security procedure for Target UE

NOTE 2: UE-to-UE Relay may perform Direct Discovery Model A or Model B to add UEs in Target UE list based on previous discovery.

4b. The Target UE sends a Relay Discovery Key Request message containing the RPAUID, RSC and its PC5 UE security capability to the 5G DDNMF in order to be allowed to monitor/discover for one or more RPAUIDs of UE-to-UE Relay UEs.

5b. The 5G DDNMF of the Target UE sends an authorization request to the ProSe Application Server. If, based on the RPAUID and RSC of Target UE, the RPAUID is allowed to monitor/discover at least one of the UE-to-UE Relay RPAUIDs contained in the Application Level Container, the ProSe Application Server returns an authorization response.

6b. If the Authorization Request is authorized in Step5b, and the PLMN ID in the UE-to-UE Relay RPAUID indicates a different PLMN, the 5G DDNMF of the Target UE contacts the indicated PLMN’s 5G DDNMF of UE-to-UE Relay by sending a Discovery Request message including the PC5 UE security capability and RSC received in step 4b.

7b. The 5G DDNMF of the UE-to-UE Relay may exchange authorization messages with the ProSe Application Server. ProSe Application Server may check whether the Target UE is authorised to implement UE-to-UE Relay Discovery under specific UE-to-UE Relay Service.

8b. If the PC5 UE security capability in step 4b includes the chosen PC5 ciphering algorithm, the 5G DDNMF of the UE-to-UE Relay responds to the 5G DDNMF of the Target UE with a Discovery Response message including the corresponding Code-Sending Security Parameters, Code-Receiving Security Parameters, an optional Discovery User Integrity Key (DUIK), and the chosen PC5 ciphering algorithm. The Code-Receiving Security Parameters provide the information needed by the Target UE to undo the protection applied by the UE-to-UE Relay. The 5G DDNMF of the Target UE stores the RSC, Code-Sending Security Parameters and the Code-Receiving Security Parameters.

9b. The 5G DDNMF of the Target UE returns Code-Sending Security Parameters, the Code-Receiving Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters and the chosen PC5 ciphering algorithm. The Target UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Monitoring UE in step 9 of clause 6.1.3.1 of the TS 33.503 specification. The Target UE stores Code-Sending Security Parameters, Code-Receiving Security Parameters, and the chosen PC5 ciphering algorithm together with the RSC.

10. UE-to-UE Relay broadcasts Relay Announcement message with a Target UE list and protect it.

11a. The UE-to-UE Relay may perform Discovery procedure with the RSC it supports to discover target UEs it can announce.

In this procedure, Target UE monitors Relay Announcement message, after receiving Relay Announcement message, if Target UE wants to use the relay to be discovered by other UEs, the Target UE will send a Response message and use Code-Sending Security Parameters to protect it.

NOTE 3: There are two methods for Target UE adding into UE lists. 1. When Target UE adds into UE list by previous discovery. The UE-to-UE Relay may perform Direct Discovery procedure (either Model A or Model B) with the RSC it supports to discover target UEs it can announce. Previous discovery is not shown in this solution. 2. When Target UE adds into UE list after receiving Relay announcement message, the step 11a will be implemented

11b. Source UE receives Announcement message, if the Source UE wants to communicate with the UEs in Target UE list, the UE will implement UE-to-UE relay link establishment procedure.

### 6.11.3 Evaluation

TBD

## 6.12 Solution #12: Security of Layer-2 UE-to-UE Relay and Adaptation Layer

### 6.12.1 Introduction

This contribution proposes a solution to address KI #2: Security of UE-to-UE Relay and Key Issue #4: Privacy of information over the UE-to-UE Relay. Most specifically, this contribution provides a solution for E2E security establishment during E2E PC5 unicast link establishment via a Layer-2 UE-to-UE Relay and privacy when using such E2E PC5 unicast link. The solution uses the new Adaptation Layer on the Control Plane and User Plane protocol stacks as specified in TR 23.700-33 [2], Annex A2 as a baseline.

A PC5 unicast link (also called per-hop link or management link), is established with the UE-to-UE Relay by source/target UEs to send E2E messages such as DSMC messages via the Relay. The management link is secured between the source/target UEs and the UE-to-UE Relay using existing procedures and doesn't use an adaptation layer.

### 6.12.2 Solution details



**Figure 6.12.2-1: End-to-End PC5 unicast link establishment and data forwarding using Relay-specific identifiers.**

1. UE-to-UE Relay registers with the network and specifies its relay capabilities. UE-to-UE Relay is provisioned with relay security policy parameters from the network based on existing procedures as described in TS 23.304 [8], TS 33.503 [6].
2. UE1 establishes a secure per-hop PC5 unicast link with the UE-to-UE Relay using existing procedures.
3. UE1 sends a DCR message which includes security parameters (i.e., UE1 MSB of KNRP-sess ID, KNRP ID, nonce1, etc.) as specified in TS 33.536 [9], clause 5.3.3.1.4 to establish an E2E PC5 unicast link via the UE-to-UE Relay.
4. The UE-to-UE Relay retransmits the DCR message if it is authorized to relay for this application based on provisioned relay policy/parameters. The UE-to-UE Relay adds an adaptation header containing info identifying UE1 and includes its unique Relay ID and relay-specific MSB of KNRP-sess ID in the DCR. The UE-to-UE Relay keeps the association of its relay-specific MSB of KNRP-sess ID and MSB of KNRP-sess ID received from UE1. Any subsequent E2E messages (i.e. PC5-S and data) are forwarded based on UE identifier info specified in the adaptation header.

Editor's Note: the details of handling of messaging via L2 UE-to-UE Relay (i.e., with adaptation layer) need to be coordinated with SA2/RAN2

1. Interested Target UE (i.e. UE3) receives the DCR message via the UE-to-UE Relay, establishes a PC5 unicast link establishment with the UE-to-UE Relay, if such link does not already exist.
2. Authentication between UE1 and UE3 via the Relay is performed to establish KNRP/KNRP ID pair if UE3 does not have a KNRP and KNRP ID pair as indicated in DCR from UE1.

Editor's Note: details of key establishment are FFS

1. UE3 sends a Direct Security Mode Command message to UE1 via the Relay (i.e. over the direct PC5 unicast link to the UE-to-UE Relay). UE3 generates and includes its LSB of KNRP-sess ID. UE3 forms the KNRP-sess ID from the MSB of KNRP-sess ID received from the Relay in step 4, and its LSB of KNRP-sess ID. UE3 derives KNRP-sess fromKNRP to create the e2e security context used with UE1 and NRPEK/ NRPIK as described in TS 33.536 [9]. UE3 adds an adaptation header including its LSB of KNRP-sess ID, and the info identifying UE1 as received with the DCR message. UE3 includes the Relay ID in the adaptation header when sending the first message to UE1 (i.e., Direct Link Authentication Request or Direct Security Mode Command).

The UE-to-UE Relay retransmits the DSMC message to UE1 (over PC5 unicast link with UE1) including info identifying UE3 in the adaptation header. The UE-to-UE Relay also includes in the adaptation header a relay-specific LSB of KNRP-sess ID associated with the E2E link between UE3 and UE1 (i.e., associated to MSB of KNRP-sess ID as received in step 3). UE-to-UE Relay puts its Layer-2 ID as the source and UE1 Layer-2 ID as the destination. The UE-to-UE Relay keeps the association of UE3 LSB of KNRP-sess ID and its relay-specific LSB of KNRP-sess ID associated with UE3. When receiving a DSMC message from the Relay, UE1 extracts the Relay ID. UE1 forms KNRP-sess ID using LSB of KNRP-sess ID specified in the adaptation header and its MSB of KNRP-sess ID sent in step 2. UE1 derives KNRP-sess fromKNRP to create the e2e security context used with UE3 and NRPEK/ NRPIK as described in TS 33.536 [9].

1. UE1 sends a Direct Security Mode Complete message to UE3 via the Relay (i.e. over the direct PC5 unicast link to the UE-to-UE Relay) protected using the established e2e security context. UE3 processes the security of the DSM Complete message which completes the E2E link security establishment procedure between UE1 and UE3.
2. UE3 sends a DCA message to UE1 via the Relay to complete the secure e2e link establishment between UE1 and UE3.
3. UE1 and UE3 exchange E2E data via the UE-to-UE Relay. UE-to-UE Relay replaces the fields specified in the PDCP header with relay-specific identifiers, based on the mapping established in steps 2 and 5, before forwarding the E2E messages.

Editor's Note: details on how to provide privacy of identifiers over the E2E link via the L2 UE-to-UE Relay are FFS

### 6.12.3 Evaluation

TBD

## 6.13 Solution #13: E2E authentication with Layer-3 UE-to-UE Relay

### 6.13.1 Introduction

This solution is for the 5G ProSe Layer-3 UE-to-UE Relay case. It addresses Key Issue #2: Security of UE-to-UE Relay, Key Issue #3: Authorization in the UE-to-UE Relay Scenario and 2nd requirement of Key Issue #1: Security for UE-to-UE Relay discovery (protection of privacy sensitive information of source and target UE).

TR 23.700-33[2] describes several solutions for Layer-3 based UE-to-UE Relay which are all based on IP routing functionality at the UE-to-UE Relay. As part of the PC5 unicast link establishment procedure, the ProSe 5G UE-to-UE Relay allocates an IP address/prefix to the UE or is informed of the UE's IP address/prefix. The Relay stores the association of the UE's Application layer ID (also called User Info) and UE's IP address/prefix (e.g. into its DNS entries). When a source UE needs to communicate with a target UE via the ProSe 5G UE-to-UE Relay, it sends a request (e.g., DNS query) to the ProSe 5G UE-to-UE Relay, over the unicast link, to obtain the target UE's IP address/prefix (based on Target User Info). The Relay returns the IP address/prefix of the target UE. The source UE sends IP data to the target UE via the PC5 unicast link to UE-to-UE Relay. The UE-to-UE Relay acts as an IP router and forwards the packets to the corresponding PC5 unicast link towards the target UE.

When using the IP based routing, the UE and UE-to-UE Relay may wish to allow E2E communication only with a peer UE that is authenticated and authorized by the UE for both privacy reasons and to prevent unauthorized usage of UE-to-UE Relay resources (e.g., due to unauthorized IP traffic). To enable this, a UE informs the UE-to-UE Relay during the PC5 link establishment procedure whether E2E authentication/authorization with peer UEs is required before allowing communications via the UE-to-UE Relay. The Relay enforces the E2E authentication/authorization between peer UEs accordingly.

### 6.13.2 Solution details

This solution describes how E2E authentication and authorization is enforced prior to allowing user data traffic. Key\_Est\_Info used in the procedure below is a generic authentication container as defined in TS 33.536 [9]. This container is transparent to the PC5 interface and used to transport different data required for key establishment depending on the authentication method used by the application.



Figure 6.13.2-1: End-to-end authentication via Layer-3 UE-to-UE Relay

1. PC5 unicast links are established between UE1 and the Relay, UE2 and the Relay. During PC5 link establishment, UE1 and/or UE2 informs the Relay that E2E authentication and authorization is required prior to E2E communication, i.e. DNS resolution/E2E IP communication is not allowed before E2E authentication and authorization is successfully run. The Relay stores the E2E authentication and authorization requirement information along with UE1 and/or UE2 user info.
2. UE1 sends DNS query to Relay including target UE2 user info, UE1 user info, and Key\_Est\_Info.

Editor's Note: whether the E2E authentication and key establishment is triggered by DNS message or other message is to be determined in coordination with SA2.

1. Relay determines that E2E authentication and authorization is required based on stored UE1 and UE2 user info and triggers E2E authentication and authorization.

The following steps 4 and 5 may be run multiple times depending on the authentication method used.

1. (a) Relay sends a Relayed Auth and Key Establishment Request message to UE2 including UE1 user info, UE2 user info, and Key\_Est\_Info. (b) UE2 sends a Relayed Auth and Key Establishment Response message to Relay including UE1 user info, UE2 user info, and Key\_Est\_Info. The final response indicates to the relay the authentication is complete with the corresponding result.
2. (a) Relay sends a Relayed Auth and Key Establishment Request message to UE1 including UE2 user info, UE1 user info, and Key\_Est\_Info. (b) UE1 sends a Relayed Auth and Key Establishment Response message to Relay including UE1 user info, UE2 user info, and Key\_Est\_Info. The final response indicates to the relay the authentication is complete with the corresponding result.
3. Once a final successful authentication result is received by the Relay from UE1 and UE2, Relay replies to the DNS Query message from UE1 by sending a DNS Response message including UE2’s IP address. If the E2E authentication and authorization fails, the Relay sends a DNS Response indicating failure.

### 6.13.3 Evaluation

TBD

## 6.14 Solution #14: path switching with Layer-2 UE-to-UE Relay

### 6.14.1 Introduction

This contribution proposes a solution to address KI #2: Security of UE-to-UE Relay and Key Issue #4: Privacy of information over the UE-to-UE Relay. Most specifically, this contribution provides a solution for path switching between two Layer-2 UE-to-UE Relays (i.e., relay re-selection).

This solution proposes to enable the preparation of the new security keys between the Source UE and Target UE using the existing PC5 unicast link via the first Relay and associated existing security association. The new security keys are then used for the security of a new PC5 unicast link that the UEs establish for path switching via a second relay. New security keys are necessary since the KNRP-sess is derived per unicast link as per TS 33.536, clause 5.3.3.1.2.1.

As in the UE-to\_Network Relay scenario, it is assumed that PC5 signalling integrity security policy is set to "REQUIRED".

Details related to the establishment of the new security keys for the new PC5 unicast link using the existing security association from the existing PC5 unicast link are specified in the following section.

### 6.14.2 Solution details

Figure 6.14.2-1 illustrates the high-level procedure of the proposed solution.



**Figure 6.14.2-1: Layer-2 based UE-to-UE Relay Path Switching**

1. A PC5 unicast link is established between Source UE and Target UE via Relay\_1. Traffic is exchanged between the Source UE and the Target UE over the PC5 unicast link, via Relay\_1.
2. Source UE triggers path switching, i.e. change of UE-to-UE Relay. The Source UE has obtained a list of candidate UE-to-UE Relay IDs (i.e. RIDs).
3. Source UE sends a Link Modification Request message to Target UE (via Relay\_1) including a list of candidate RIDs and a source UE link ID, which is used on the Source UE to associate the existing PC5 unicast link via Relay\_1 to the new PC5 unicast link with the selected Relay (e.g. Relay\_2). Security parameters (i.e., nonce\_1, MSB of KNRP-sess ID) to enable the establishment of new KNRP-sess and its ID and security keys are included as well.

The Source UE link ID is a locally generated random number by the Source UE. To avoid replay and linkability/trackability attacks across path switching procedures, a new Source UE link ID is generated and used each time a new path switch is initiated, i.e., each time a Link Modification message for path switching is sent. To preserve the privacy of the transmitted ids (Source UE link ID, MSB of KNRP-sess ID) the Link Modification Request message is protected for confidentiality, using current PC5 link security context.

1. Target UE selects a Relay from the received list of candidate RIDs (e.g. Relay\_2). Target UE uses the security parameters received from Source UE in the Link Modification Request message and its own security parameters to generate a new KNRP-sess (from current KNRP) and KNRP-sess ID and new security keys for the link to be established via the selected Relay. The new keys are stored to be later located when a DCR message for new link establishment is received (at step 8).
2. Target UE sends a Link Modification Accept message to Source UE (via Relay\_1) including its selected RID and a Target UE link ID, which is used on the Target UE to associate the existing PC5 unicast link via Relay\_1 to the new PC5 unicast link with the selected Relay (i.e. Relay\_2). Target UE’s security parameters (i.e., nonce\_2, LSB of KNRP-sess ID) used to establish a new KNRP-sess and KNRP-sess ID and new security keys for the link to be established via the selected Relay are also included. The Target UE link ID is generated as described for the Source UE link ID in step 3. To preserve the privacy of the transmitted ids (Target UE link ID, LSB of KNRP-sess ID) the Link Modification Accept message is protected for confidentiality, using current PC5 link security context.
3. Source UE uses the security parameters received from the Target UE on the Link Modification Accept message and its own security parameters to generate a new KNRP-sess (from current KNRP) and KNRP-sess ID and new security keys for the link to be established via the selected Relay. Source UE protects for integrity the Target UE link ID using the new security keys.
4. Source UE sends a broadcast Direct Communication Request (DCR) message including the selected RID (i.e. Relay\_2), Target UE link ID received from Target UE at step 5. Relay\_2 receives the DCR message and forwards it to Target UE.
5. Target UE receives the DCR message and uses the Target UE link ID to locate the new security keys derived in step 4. Target UE uses the new security keys to verify the integrity of the received Target UE link ID parameter. A successful verification by the Target UE validates the new PC5 unicast link establishment request used for path switching. Target UE associates the new security context with the new PC5 unicast link.
6. Target UE sends a Direct Communication Accept message protected using the new security context. Target UE includes the Source UE link ID from Source UE as received at step 3 in the message. Relay\_2 receives the DCA message and forwards it to Source UE.
7. Source UE verifies the security of the DCA message using the new security keys. A successful verification by source UE completes the establishment of the new PC5 unicast link used for path switching. Source UE associates the new security context with the new PC5 unicast link.
8. Source UE and Target UE use the newly established PC5 unicast link via the Relay\_2 for path switching.

### 6.14.3 Evaluation

Editor’s Note: additional complexity/logic to the UEs are FFS.

## 6.15 Solution #15: Selection and authorization of in-coverage and out-of-coverage authentication and key establishment

### 6.15.1 Introduction

This solution addresses Key Issue #2 and Key Issue #3.

Different types of solutions and configurations may be available to establish a secure and authorized PC5 communication link. For instance, Solution #3 and #5 address in-coverage scenarios while Solution #4, #6 and #7 address out-of-coverage scenarios, and Solution #10 may be used in both in-coverage and out-of-coverage.

Since more than a single solution might be needed to address different scenarios, it is required to determine which solution is allowed to be used when. For instance, an out-of-coverage source UE might attempt to use a solution for out-of-coverage when the UE-to-UE relay is in-coverage. In this exemplary situation, the UE-to-UE relay should be able to determine – based on a policy -- that an in-coverage solution is (not) required and indicate this to the source UE.

This solution describes the configuration of a policy that allows source/target UEs and UE-to-UE relay to agree on the type of solution and parameters that is preferred and/or authorized to be used.

### 6.15.2 Solution details



**Figure 6.15.2-1**

The message flow and steps of this solution are as outlined in Figure 6.15.2-1.

* In Step 0, the UEs perform an initial authorization and parameter provisioning for in-coverage and out-of-coverage situations. This step includes the configuration of parameters for different solutions for in-coverage and out-of-coverage security establishment and authorization.

Note 1: the configured parameters for in-coverage and out-of-coverage solution depend on the configured solution.

* In Step 1, the source UE and UE-to-UE relay perform a discovery phase.
* In Step 2, the source UE determines its out-of-coverage (in-coverage) situation, and choses a security solution and/or security parameters for its out-of-coverage (in-coverage) situation. This choice can be based on multiple reasons, e.g., application requirements such as performance or an in-coverage (out-of-coverage) indication received from the UE-to-UE relay during discovery, etc. The source UE builds correspondingly a Direct Communication Request based on the chosen out-of-coverage (in-coverage) solution and security parameters.

Editor’s Note: Its FFS why the source UE cannot select in-coverage solution if UE-to-UE relay is in-coverage.

* In Step 3, the UE-to-UE relay receives the DCR message and determines whether the DCR message either implicitly or explicitly contains parameters for an out-of-coverage (in-coverage) solution. The UE-to-UE relay then checks that the requested solution and security parameters fit its out-of-coverage (in-coverage) situation and whether a policy deployed in Step 0 together with any authorization information received in Step 2 allow the usage of said solution and security parameters. Once this policy is evaluated and if the result is positive, the UE-to-UE relay will proceed executing the requested out-of-coverage (in-coverage) solution. Alternatively, if the result is negative, the UE-to-UE relay may – based on configuration – indicate the source UE policy mismatch, and potentially request a different DCR message including a requested solution and security parameters.
* In Step 4, the UE-to-UE relay may take one of the following alternative steps:
  + Step 4-A, send a message to the Source UE to go on with an in-coverage solution.
  + Step 4-B, send a message to the core network to go on with an out-coverage solution.
  + Step 4-C, send a message to the Source UE indicating that the security establishment based on the exchanged parameters is not feasible and requesting alternative parameters.

Note 2: The above steps can be repeated for the security establishment process and authorization between Target UE and UE-to-UE relay.

Note 3: The above process illustrates how UEs signal and agree on solution and security parameters to use by means of the DCR message. This signalling and agreement phase might also be carried out in the discovery phase.

### 6.15.3 Evaluation

TBD

## 6.16 Solution #16: Centralized discovery key management and U2U relay authorization

### 6.16.1 Introduction

This solution addresses Key Issue #1: Security for UE-to-UE Relay discovery and Key issue #3: Authorization in the UE-to-UE Relay Scenario. For Key Issue #1, this solution specifically addresses the security requirement: The 5G System shall provide a means to securely provision the security materials for UE-to-UE Relay discovery.

This solution assumes that the discovery security materials used for direct discovery and U2U relay discovery are different. Therefore, U2U relay authorization can be executed during the U2U relay discovery key provision process. Otherwise this solution does not address the Key Issue #3.

This solution needs to extend the existing specification as follows:

- Permit multiple roles in the restricted discovery request. (Currently, there is only one role (Announce, Monitor, Query or Response) in the restricted discovery request.)

- Permit to return more than two sets security materials in the restricted discovery response. (Currently, the restricted discovery response can return code-sending-security-parameter, code-receiving-security-parameter or both.

This solution assumes that only one ProSe Key Management Function (PKMF) is used to generate and provision discovery security materials for direct discovery and U2U relay discovery. The PKMF in this solution is also called 5G U2U Relay PKMF to distinguish it from other kinds of PKMFs. A 5G U2U Relay PKMF can provision various discovery security materials based on a 5G ProSe UE’s roles in U2U relay discovery procedures.

### 6.16.2 Solution details

 Figure 6.16.2-1: Centralized discovery key management and U2U relay authorization procedure

Note: This solution only covers the parameters related to security material retrieval.

0. The 5G ProSe UE (Source UE/Target UE/Relay UE) gets the 5G U2U Relay PKMF address from the PCF/5G DDNMF of its HPLMN, which is responsible for provisioning discovery security materials related to direct discovery and U2U relay discovery.

Editor’s Note: Discovery request with PKMF instead of DDNMF or PCF is FFS (to be aligned with SA2 if needed).

Editor’s Note: Whether or not to use Discovery Request or other message is FFS.

1. The 5G ProSe UE establishes a secure connection with the 5G U2U Relay PKMF and sends a U2U Relay Discovery Request to the 5G U2U Relay PKMF. The request includes User Info ID, Security capability, and UE's roles in RSC-specified relay service. The request should include RSC if discovery security materials for U2U relay discovery are required.

Security for the interface between the 5G ProSe UE and the 5G U2U Relay PKMF relies on Ua security if GBA specified in TS 33.220 [14] is used (see clause 5.2.3.4) or Ua\* security if AKMA specified in TS 33.535 [15] is used (see clause 5.2.5.4).

Editor’s Note: Role representation is FFS and should be aligned with SA2.

2. 5G U2U Relay PKMF checks whether the 5G ProSe UE is authorized to play these roles in RSC-specified relay service.

3. The 5G U2U Relay PKMF provides a set of discovery security materials corresponding to the authorized roles to the 5G ProSe UE through U2U Relay Discovery Response. The discovery security materials related to U2U relay discovery are associated with the RSC. The 5G U2U Relay PKMF may include relay discovery security policies specifying how the provided security material is used in the U2U relay discovery procedure in the response. For example, a security policy can specify whether end-to-end protection needs to be enabled in relay discovery messages.

### 6.16.3 Evaluation

TBD

## 6.17 Solution #17: U2U relay discovery security material retrieval and authorization across PLMNs

### 6.17.1 Introduction

This solution addresses Key Issue #1: Security for UE-to-UE Relay discovery and Key issue #3: Authorization in the UE-to-UE Relay Scenario. For Key Issue #1, this solution specifically addresses the security requirement: The 5G System shall provide a means to securely provision the security materials for UE-to-UE Relay discovery.

This solution assumes that the discovery security materials used for direct discovery and U2U relay discovery are different. Therefore, U2U relay authorization can be executed during the U2U relay discovery key provision process. Otherwise this solution does not address the Key Issue #3.

This solution needs to extend the existing specification as follows:

- Permit multiple roles in the restricted discovery request. (Currently, there is only one role (Announce, Monitor, Query or Response) in the restricted discovery request.)

- Permit to return more than two sets security materials in the restricted discovery response. (Currently, the restricted discovery response can return code-sending-security-parameter, code-receiving-security-parameter or both.

This solution assumes that multiple ProSe Key Management Functions (PKMFs) are used to generate and provision discovery security materials for direct discovery and U2U relay discovery. The PKMF in this solution is also called 5G U2U Relay PKMF to distinguish it from other kinds of PKMFs. A 5G U2U Relay PKMF can provision various discovery security materials based on a 5G ProSe UE’s roles in U2U relay discovery procedures. 5G ProSe UEs will always retrieve discovery security materials from one 5G U2U Relay PKMF which address is provided by the PCF or 5G DDNMF. It is possible for a 5G U2U Relay PKMF to retrieve discovery security materials from other 5G U2U Relay PKMFs.

### 6.17.2 Solution details

 Figure 6.17.2-1: U2U relay discovery security material retrieval and authorization procedure across PLMNs

Note: This solution only covers the parameters related to security material retrieval.

0. The 5G ProSe UE (Source UE/Target UE/Relay UE) gets the 5G U2U Relay PKMF address from the PCF/5G DDNMF of its HPLMN, which is responsible for provisioning discovery security materials related to direct discovery and U2U relay discovery.

Editor’s Note: Discovery request with PKMF instead of DDNMF or PCF is FFS (to be aligned with SA2 if needed).

Editor’s Note: Whether or not to use Discovery Request or other message is FFS.

1. The 5G ProSe UE establishes a secure connection with the 5G U2U Relay PKMF in its HPLMN and sends a U2U Relay Discovery Request to the 5G U2U Relay PKMF. The request includes User Info ID, Security capability, and UE's roles in RSC-specified relay service. The request should include RSC if discovery security materials for U2U relay discovery are required.

Security for the interface between the 5G ProSe UE and the 5G U2U Relay PKMF relies on Ua security if GBA specified in TS 33.220 [14] is used (see clause 5.2.3.4) or Ua\* security if AKMA specified in TS 33.535 [15] is used (see clause 5.2.5.4).

Editor’s Note: Role representation is FFS and should be aligned with SA2.

2. The 5G U2U Relay PKMF in the HPLMN may need to send an Authorization Check Request to the ProSe App Server or UDM to check whether the UE is allowed to play its declared roles. The request includes User Info ID and the role list. The request should include RSC if discovery security materials for U2U relay discovery are required.

Editor’s Note: What functional entity is responsible for authorization checks is FFS.

3. The ProSe App Server or UDM checks whether the UE is allowed to play the roles it claims, and returns the allowed roles through Authorization Check Request

4. If the security materials for the roles are not available locally, the 5G U2U Relay PKMF in the HPLMN may need to send an U2U Relay Discovery Security Material Request to another 5G U2U Relay PKMF in a VPLMN to obtain the security materials. The request includes User Info ID and role list. The request should include RSC if discovery security materials for U2U relay discovery are required.

5-6. The 5G U2U Relay PKMF in the VPLMN may need to send an Authorization Check Request to the ProSe App Server to check whether the UE is allowed to play its declared roles.

7. The 5G U2U Relay PKMF in the VPLMN gets the discovery security materials for the allowed roles in the RSC-specific U2U relay service, and returns them through U2U Relay Discovery Security Material Response. The discovery security materials related to U2U relay discovery are associated with the RSC. The 5G U2U Relay PKMF may include relay discovery security policies specifying how the provided security material is used in the U2U relay discovery procedure in the response. For example, a security policy can specify whether end-to-end protection needs to be enabled in relay discovery messages.

8. The 5G U2U Relay PKMF in the HPLMN returns the discovery security materials obtained from the local and other PLMNs to the UE through U2U Relay Discovery Response. The discovery security materials related to U2U relay discovery are associated with the RSC. If there are Relay Discovery Security Policies for the RSC-specific U2U relay service, the 5G U2U Relay PKMF includes these policies in the response.

### 6.17.3 Evaluation

TBD

## 6.18 Solution #18: UE-to-UE Relay security

### 6.18.1 Introduction

This solution addresses Key Issue #2: Security of UE-to-UE Relay.

This solution uses PC5 security mechanism defined in in TS 33.536 [9] for the security between Remote UE and Relay UE.

This solution uses IPsec for the security between Remote UEs in Layer-3 UE-to-UE Relay scenario.

This solution uses PC5 security mechanism defined in TS 33.536 [9] for the security between Remote UEs in Layer-2 UE-to-UE Relay scenario.

### 6.18.2 Solution details

 Figure 6.18.2-1: UE-to-UE relay security procedure

0. The Source UE, Relay UE and Target UE discover each other, and then establish connections between them. This solution does not address the key issue of U2U relay discovery security.

1. According to the U2U relay security policy configured locally, the Source UE and Target UE may use the unicast mode security mechanism defined in clause 5.3 of TS 33.536 [9] to establish secure connections with the Relay UE respectively.

Editor’s Note: The security policy for whether perform hop-by-hop link security and E2E security in U2U relay is FFS.

2. For the Layer-3 UE-to-UE relay scenario, establishing a secure connection between the Source UE and the Target UE is out of the scope of 3GPP.

For the Layer-2 UE-to-UE relay scenario, the Source UE and the Target UE can reuse the unicast mode security mechanism defined in clause 5.3 of TS 33.536 [9] to establish a secure connection via the Relay UE.

Editor’s Note: Further details for e2e security over L2 U2U relay are FFS.

### 6.18.3 Evaluation

TBD

## 6.19 Solution #19: End-to-end security establishment over the Layer-3 UE-to-UE Relay

### 6.19.1 Introduction

This solution addresses Key Issue #2 and Key Issue #3. When Source/Target UEs and a Relay UE are in the network coverage, they are authorized and provisioned with the required information for security establishments during the registration procedure that includes the primary authentication (i.e., 5G-AKA and EAP-AKA).

The Source UE sends a Direct Communication Request to the Target UE over the UE-to-UE Relay, so that the direct authentication takes place and an end-to-end session key is established regardless of whether the UEs (Source UE, Target UE and/or UE-to-UE Relay) are within or outside the network coverage.

Editor’s note: The need of end-to-end security in Layer-3 solution is FFS.

### 6.19.2 Solution details

Figure 6.19.2-1 illustrates the end-to-end security establishment procedure between the Source UE and the Target UE over the UE-to-UE Relay.

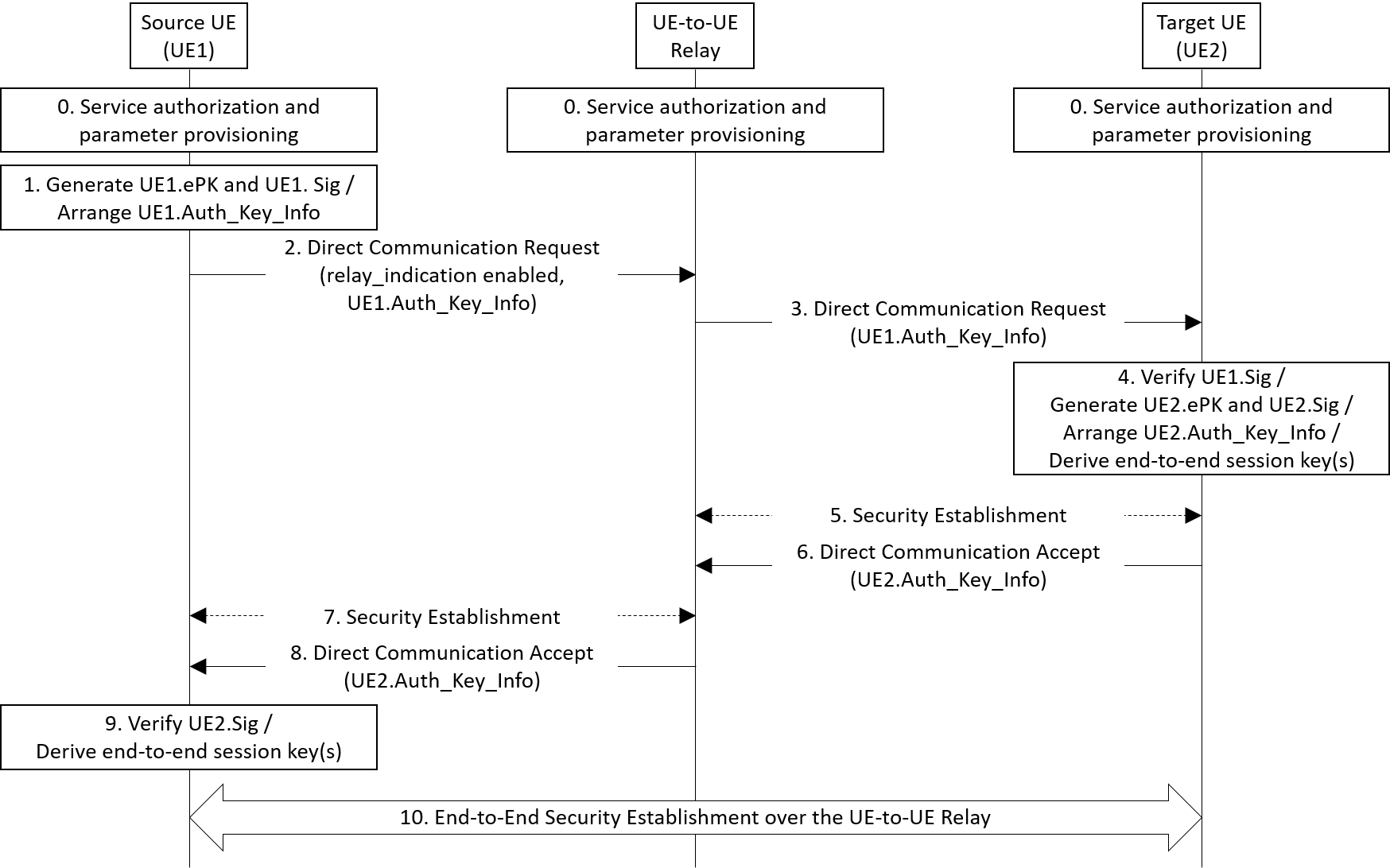


Figure 6.19.2-1: End-to-end security establishment procedure over the UE-to-UE Relay

1. The Source/Target UEs and the UE-to-UE Relay shall be registered with the network.

The Source/Target UE shall be authenticated and authorized by the network during the primary authentication procedure (i.e., 5G AKA or EAP-AKA’). The Source/Target UE initiates the procedure by sending a Registration Request message to the network, and the UDM checks the subscription information related to the UE-to-UE relay service, which indicates:

* whether the Source/Target UE is authorized to receive UE-to-UE Relay service;
* whether the Source/Target UE requires end-to-end security establishment;
* available methods for Direct Authentication and Key Establishment between the Source UE and the Target UE (e.g., Certification-based approach, Identity-based approach, etc).

Based on the subscription information, the Source/Target UE may send its information to the network (i.e., the AUSF) to get provisioned with security materials for the Direct Authentication and Key Establishment. For examples, ID and public key of the Source/Target UE shall be provisioned to the network in Certificate-based approach and ID of the Source/Target UE shall be provisioned to the network in Identity-based approach.

Note 1: the security materials provisioned to the Source/Target UE by the network are associated with an expiration time after which they become invalid.

Based on the subscription information from the UDM and the information provisioned by the Source/Target UE, the network decides whether to generate and provision the security materials to the Source/Target UE: the authorized Source/Target UE is provisioned with the security materials when it has not been provisioned with the security materials or when the validity of the security materials is expired.

The UE-to-UE Relay shall also be authenticated and authorized by the network to provide UE-to-UE Relay service.

Editor’s note: How the public key is provisioned to the network is FFS.

Editor’s note: How the security material is generated is FFS.

1. There are various authentication and key establishment methods to be used between the Source UE and the Target UE over a UE-to-UE Relay. Hence, all the authentication is specified to be carried in a generic container called Auth\_Key\_Info in the following steps.

The Source UE generates ephermeral public key (UE1.ePK) and secret key (UE1.eSK), and UE1.Sig using the security materials provisioned in step 0. The Source UE arranges the data for the direct authentication and key establishment with the Target UE (UE1.Auth\_Key\_Info), e.g., by carrying UE1.ID, UE1.ePK, and UE1.Sig. At each step of the flow, the Auth\_Key\_Info may contain different data required for key establishment.

The solution, for example, may employ certificated-based approach or identity-based approach. For the certificate-based approach, a UE is provisioned with its certificate and root CA’s public key to verify the certificate as security materials. Then, the UE puts a digital signature signed with its private key and its certificate to verify the signature into the Auth\_Key\_Info. For the Identity-based approach, a UE is provisioned with its identity, secret signing key (SSK), public validation token (PVT), and KMS public authentication key (KPAK) as security materials. Then, the UE puts a digital signature signed with SSK, PVT to verify the signature, and its identity into the Auth\_Key\_Info.

1. The Source UE wants to establish unicast communication with the Target UE via a UE-to-UE Relay. The Source UE sends to the UE-to-UE Relay a Direct Communication Request message with its Auth\_Key\_Info included and relay\_indication enabled. The message includes the source UE information, target UE information, Application ID, as well as Relay Service Code (RSC), if there is any.

Note 2: The relay\_indication is a newly proposed field in Sol#8 for KI#4 from TR 23.752 [3] to indicate whether a relay can be used in the communication and to integrate the relay discovery/selection into the unicast link establishment procedure. The relay discovery/selection step can be added before step 2 to replace the relay\_indication field.

Editor’s note: The solution needs SA2 coordination.

1. The UE-to-UE Relay receives the Direct Communication Request with the relay\_indication set and forwards the message to the Target UE with the relay\_indication disabled.
2. Upon reception of the Direct Communication Request message, the Target UE verifies the Source UE with the UE1.Sig included in UE1.Auth\_Key\_Info. If the verification test is successful and the Target UE decides to accept the request, the Target UE generates ephermeral public key (UE2.ePK) and secret key (UE2.eSK), and UE2.Sig using the security materials provisioned in step 0.

The Target UE arranges the data for the direct authentication and key establishment with the Source UE (UE2.Auth\_Key\_Info), e.g., by carrying UE2.ID, UE2.ePK, and UE2.Sig.

In this step, the Target UE derives the end-to-end session key(s) to protect the data between the Source UE and the Target UE using the Source UE’s public key (UE1.ePK) and its own secret key (UE2.eSK).

1. In this step, the PC5 unicast link security can be established between the Target UE and the Relay UE as defined in clause 5.3 of TS 33.536 [4].

Note 3: this solution focus on end-to-end security establishment between the Source UE and the Target UE, as the security establishment between the Source/Target UE and the UE-to-UE Relay can be achieved by reusing the unicast mode direct communication mechanism defined in TS 33.503 [5] or by repeating this solution.

1. The Target UE sends to the UE-to-UE Relay a Direct Communication Accept message with its Auth\_Key\_Info included.
2. In this step, the PC5 unicast link security can be established between the Target UE and the Relay UE as defined in clause 5.3 of TS 33.536 [4].
3. The UE-to-UE Relay receives the Direct Communication Accept message and retrieves the source UE information stored in step 2. The UE-to-UE Relay forwards the Direct Communication Accept message to the Source UE.
4. Upon reception of the Direct Communication Accept message, the Source UE verifies the Target UE with the UE2.Sig included in UE2.Auth\_Key\_Info. If the verification test is successful, the Source UE derives the end-to-end session key(s) to protect the data between the Source UE and the Target UE using the Target UE’s public key (UE2.ePK) and its own secret key (UE1.eSK).
5. The Source UE and the Target UE finish setting up the secure communication link over the UE-to-UE Relay with the shared end-to-end session key. The encryption key and integrity key are derived from the end-to-end session key and used in the chosen confidentiality and integrity algorithms, respectively.

Editor's note: The impact on protocol stack for end-to-end security is FFS.

### 6.19.3 Evaluation

TBD

## 6.20 Solution #20: Network-assisted security establishment procedure for 5G ProSe Layer-3 UE-to-UE Relay

### 6.20.1 Introduction

The solution addresses Key Issue #2: Security of UE-to-UE Relay. It largely reuses the mechanism of Direct Security Establishment procedure defined in TS 33.503 [6] to ensure the security of UE-to-UE Relay Communication.

In the UE-to-UE relay scenario, two options (Layer-2 UE-to-UE Relay and Layer-3 UE-to-UE Relay) are under consideration. For Layer-3 UE-to-UE Relay, the full security of a UE-to-UE PC5 link depends on the security of two separate PC5 links, i.e. the link between the Source UE and UE-to-UE Relay and the link between UE-to-UE Relay and Target UE. The security of these two separate PC5 link relies on the UE-to-UE Relay’s security materials, which are provided by the network after passing the authorization check. With the assistance of network, the UE-to-UE PC5 link via 5G ProSe Layer-3 UE-to-UE Relay can be securely established.

### 6.20.2 Solution details

Figure 6.20.2-1: Network-assited PC5 link security establishment procedure for 5G ProSe Layer-3 UE-to-UE Relay

0. The long term credential and long term credential ID are associated with RSC, which could be pre-configured on the Source UE and Target UE or provisioned by the network before the U2U discovery procedure.

1. The Discovery & Relay Selection procedure is performed between the peer UEs and the UE-to-UE Relay.

NOTE 1: It is assumed that after the Discovery & Relay Selection procedure, the Source UE and the Target UE can discover each other by selecting the same UE-to-UE Relay.

2. The Source UE sends a Direct Communication Request that contains the long term credential ID, Source UE’s security capabilities, RSC and nonce 1 to the UE-to-UE Relay. The message may also include a Knrp ID if the Source UE has an exisiting Knrp with this UE-to-UE Relay for the same RSC.

3a. If the UE-to-UE Relay already has the long term credential identified by the long term credential ID, step 3a and step 3b are skipped. Otherwise, the UE-to-UE Relay sends a Prose Key Request message that contains UE-to-UE Relay Identity, long term credential ID, RSC to its PKMF, indicates that the UE-to-UE Relay is requesting the long term credential. If the requested long term credential is stored in the ProSe Application server, the PKMF needs to obtain the long term credential from the ProSe Application Server (not shown in the figure).

Editor’s Note: How to provide credential in the CP based security procedure is FFS.

NOTE 2: In the user plane based security procedure, the PKMF is responsible for providing the long term credential.

NOTE 3: In this solution, the U2U relay is in the network coverage

3b. Once receiving the Prose Key Request message, the PKMF of the UE-to-UE Relay checks if the UE-to-UE Relay is authorized to provide relay service based on the UE-to-UE Relay identity and the received RSC. If the UE-to-UE Relay’s authorization information is not locally available, the PKMF shall request the authorization information to the UDM of the UE-to-UE Relay (not shown in the figure). If the UE-to-UE Relay is authorized to provide the relay service, the PKMF of the UE-to-UE Relay returns the long term credential.

4. The UE-to-UE Relay may initiate a Direct Auth and Key Establish procedure with Source UE to generate the Knrp. If the Knrp ID is included in the Direct Communication Request, this step is skipped.

5. The UE-to-UE Relay derives the session key (KNRP-SESS) from KNRP and then derives the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies as specified in TS 33.503 [6]. The UE-to-UE Relay sends a Direct Security Mode Command message to the Source UE. This message also includes the chosen security algorithm and nonce 2.

6. The Source UE responds with a Direct Security Mode Complete message to the 5G ProSe UE-to-UE Relay.

7. Based on the User Info ID or Layer-2 ID of Target UE obtained after the UE-to-UE Relay discovery, the UE-to-UE Relay sends a Direct Communication Request that contains the long term credential ID, the Chosen security algorithm, RSC and nonce 1' to the Target UE. The message may also include a Knrp ID' if the UE-to-UE Relay has an exisiting Knrp' with the Target UE that it trying to communicate with.

8. The Target UE may initiate a Direct Auth and Key Establish procedure with UE-to-UE Relay to generate the Knrp'. If the Knrp ID' is included in the Direct Communication Request, this step is skipped.

9. The Target UE derives the session key (KNRP-SESS') from KNRP' and derives the confidentiality key (NRPEK') (if applicable) and integrity key (NRPIK’) based on the PC5 security policies as specified in TS 33.503 [6]. The Target UE sends a Direct Security Mode Command message to the UE-to-UE relay. This message also includes the nonce 2'.

10. The UE-to-UE Relay responds with a Direct Security Mode Complete message to the Target UE.

11. The Target UE sends the Direct Communication Accept message to the UE-to-UE Relay.

12. Only after receiving the Direct Communication Accept message from the Target UE, the UE-to-UE Relay then responds the Direct Communication Accept message to the Source UE.

13. The secure L3 PC5 link between the Source UE and the Target UE via the UE-to-UE Relay is established. The UE-to-UE Relay can forward the traffic between the peer Prose UEs.

### 6.20.3 Evaluation

TBD

## 6.21 Solution #21: E2E security establishment procedure for 5G ProSe Layer-3 UE-to-UE Relay

### 6.21.1 Introduction

The solution addresses Key Issue #2: Security of UE-to-UE Relay. It largely reuses the IKEv2 protocol and the mechanism of Direct Security Establishment procedure defined in TS 33.503 [6] to ensure the end-to-end security between the Source UE and Target UE.

After the per-hop links (i.e. the PC5 link between Source UE and UE-to-UE Relay, as well as the PC5 link between UE-to-UE Relay and Target UE) are established, the peer UEs may exchange their security materials and associate the end-to-end security keys to establish E2E security. The Source UE and Target UE perform the IKEv2 protocol, which enables the end-to-end security in the UE-to-UE relay communication.

### 6.21.2 Solution details

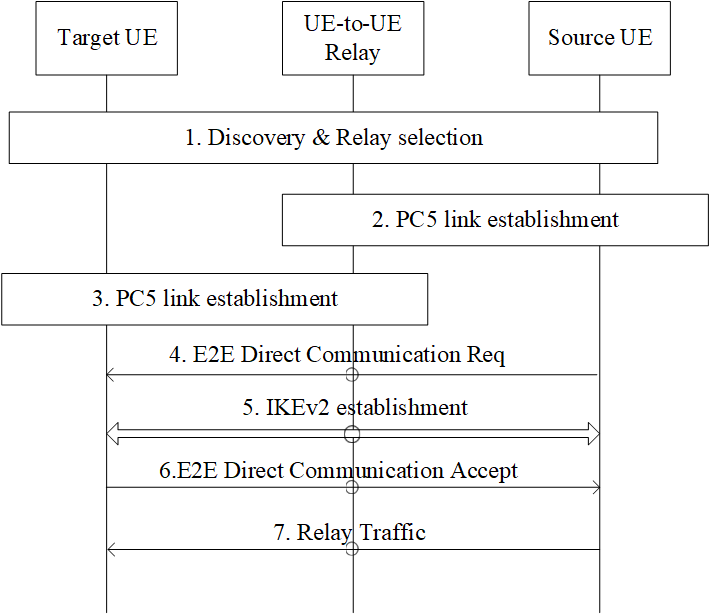


Figure 6.21.2-1: PC5 link security establishment procedure for 5G ProSe Layer-3 UE-to-UE Relay

1. The Discovery & Relay Selection procedure is performed between the peer UEs and the UE-to-UE Relay.

2. The Source UE initiates the PC5 link setup with UE-to-UE Relay by performing the Direct Communication procedures specified in TS 33.503 [6].

3. After the PC5 link between the Source UE and UE-to-UE Relay is established, the UE-to-UE Relay initiates the PC5 link setup with the Target UE based on the Direct Communication procedure specified in TS 33.503 [6].

4. The Source UE sends E2E Direct Communication Request to the Target UE, which is forwarded by the Layer-3 U2U relay. The E2E Direct Communication Request is protected by the NRPIK/NRPEK of each hop (i.e the link between Source UE and Layer-3 U2U Relay and the link between Layer-3 U2U Relay and Target UE).

5. [Optional]The Target UE initiates the security negotiation procedure with the Source UE to establish an end-to-end IPSec connection by performing IKEv2 authentication procedure. After the IKEv2 authentication, the Source UE and the Target UE generate the E2E security keys. The details of IKEv2 protocol is out of the scope of 3GPP.

NOTE: The detail of IKEv2 protocol is out of the scope of 3GPP.

6. The Target UE responds with the E2E Direct Communication Accept forwarded by the Layer-3 U2U Relay. The E2E Direct Communication Accept is protected by the E2E security keys generated in step5.

7. The End-to-End PC5 link between the Source UE and the Target UE via the UE-to-UE Relay is established. The UE-to-UE Relay can forward the traffic between the peer UEs.

### 6.21.3 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

## 7.Z Key Issue #Z: <Key Issue Name>

Editor’s Note: This clause contains the agreed conclusions of Key Issue #Z.

Annex <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-05 | SA3#107e | S3-221021 |  |  |  | Skeleton | 0.0.0 |
| 2022-07 | SA3#107 Adhoc-e | S3-221643 |  |  |  | S3-221489, S3-221640, S3-221693, S3-221609, S3-221608, S3-221677 implemented | 0.1.0 |
| 2022-08 | SA3#108-e | S3-222344 |  |  |  | S3-222364, S3-222365, S3-222354, S3-222355, S3-222402, S3-221927, S3-222341, S3-222371, S3-222372, S3-222373, S3-222296, S3-222306 implemented | 0.2.0 |
| 2022-08 | SA3#108Adhoc-e | S3-223054 |  |  |  | S3-222969, S3-223116, S3-222592, S3-222943, S3-222944, S3-222945, S3-222946, S3-222993, S3-222628, S3-222665, S3-222666, S3-222947, S3-222948, S3-223051, S3-223052, S3-223053, S3-222791, S3-222794, S3-222986, S3-222796, S3-222987, S3-222798, S3-222799, S3-222989, S3-223060, S3-223109, S3-223110, S3-223111 | 0.3.0 |