|  |
| --- |
| 3GPP TR 33.740 V0.2.0 (2022-08) |
| 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Security Aspects of 5G ProSe 8

4.1 General 8

4.2 Architecture assumption 8

5 Key issues 8

5.1 Key Issue #1: Security for UE-to-UE Relay discovery 8

5.1.1 Key issue details 8

5.1.2 Security threats 9

5.1.3 Potential security requirements 9

5.2 Key Issue #2: Security of UE-to-UE Relay 9

5.2.1 Key issue details 9

5.2.2 Security threats 9

5.2.3 Potential security requirements 10

5.3 Key issue #3: Authorization in the UE-to-UE Relay Scenario 10

5.3.1 Key issue details 10

5.3.2 Security threats 10

5.3.3 Potential security requirements 10

5.4 Key Issue #4: Privacy of information over the UE-to-UE Relay 10

5.4.1 Key issue details 10

5.4.2 Security threats 11

5.4.3 Potential security requirements 11

5.X Key Issue #X: <Key Issue Name> 11

5.X.1 Key issue details 11

5.X.2 Security threats 11

5.X.3 Potential security requirements 11

6 Solutions 11

6.0 Mapping of Solutions to Key Issues 12

6.1 Solution #1: Restricted Peer UE IP Discovery with Layer-3 UE-to-UE Relay 12

6.1.1 Introduction 12

6.1.2 Solution details 12

6.1.3 Evaluation 13

6.2 Solution #2: Privacy handling for Layer-3 UE-to-UE Relay based on IP routing 14

6.2.1 Introduction 14

6.2.2 Solution details 14

6.2.3 Evaluation 15

6.3 Solution #3: PC5 security establishment when L3 UE-to-UE relay is in coverage 16

6.3.1 Introduction 16

6.3.2 Solution details 16

6.3.3 Evaluation 18

6.4 Solution #4: PC5 security establishment when L3 UE-to-UE relay is out of coverage 18

6.4.1 Introduction 18

6.4.2 Solution details 18

6.4.3 Evaluation 20

6.5 Solution #5: PC5 link security establishment for Layer-3 U2U Relay 20

6.5.1 Introduction 20

6.5.2 Solution details 20

6.5.2.1 PC5 link security establishment procedure over User Plane 20

6.5.2.2 PC5 link security establishment procedure over Control Plane 22

6.5.3 Evaluation 24

6.6.2.1 End-to-end security establishment for Layer-2 UE-to-UE relay 25

6.6.2.2 Key Hierarchy for UE-to-UE relay 26

6.6.2.3 Key derivation functions 27

6.7 Solution #7: Non-network-assited Security Establishment Procedure for 5G ProSe Layer-3 UE-to-UE Relay 27

6.7.1 Introduction 27

6.7.2 Solution details 28

6.7.3 Evaluation 29

6.8 Solution #8: Restricted 5G ProSe UE-to-UE Relay Discovery Model A 29

6.8.1 Introduction 29

6.8.2 Solution details 30

6.8.2.1 Restricted 5G ProSe UE-to-UE Relay Discovery Model A over Control Plane 30

6.8.2.2 Restricted 5G ProSe UE-to-UE Relay Discovery Model A over User Plane 32

6.8.3 Evaluation 32

6.9 Solution #9: Restricted 5G ProSe UE-to-UE Relay Discovery Model B 32

6.9.1 Introduction 32

6.9.2 Solution details 33

6.9.2.1 Restricted 5G ProSe UE-to-UE Relay Discovery Model B over Control Plane 33

6.9.2.2 Restricted 5G ProSe UE-to-UE Relay Discovery Model B over User Plane 35

6.9.3 Evaluation 35

6.10 Solution #10: PAKE-based security for UE-to-UE relay 35

6.10.1 Introduction 35

6.10.2 Solution details 36

6.10.3 Evaluation 37

6.Y Solution #Y: <Solution Name> 37

6.Y.1 Introduction 37

6.Y.2 Solution details 37

6.Y.3 Evaluation 37

7 Conclusions 37

7.Z Key Issue #Z: <Key Issue Name> 37

Annex <X> (informative): Change history 38

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".

# 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].

Definition format (Normal)

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

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format (EW)

<symbol> <Explanation>

## 3.3 Abbreviations

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

Abbreviation format (EW)

<ABBREVIATION> <Expansion>

# 4 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.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 |  |  |  |  |  |

## 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.

Editor’s Note: further details on how the token is generated, distributed and revoked are FFS.

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).

Editor’s Note: further details on token protection are FFS.

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 procedure defined in TS 23.304 [8]) 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. 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.

Editor's Note: whether the IP address change should be specified in SA3 is FFS.

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

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



Figure 6.3.2-1: 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/or PRUK when they are in coverage.

Editor’s Note: Further provisioned parameters e.g., PC5 security policies of UE-to-UE relay are FFS.

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.

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.

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].

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: 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.

Editor’s Note: Further input parameters in the Key Response message are FFS.

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. The 5G ProSe Source UE and 5G ProSe UE-to-UE Relay continues the rest of procedure for the UE-to-UE relay service over the secure PC5 link.

Editor’s Note: Further and remaining messages needs to be updated and clarified in step 6.

7. Step 1-6 are repeated for PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay.

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.

Editor’s Note: PC5 security set up procedure between target UE and Relay UE (step7) can be performed in parallel to the PC5 security set up procedure between source UE and Relay UE (step 1-6).

8. The 5G ProSe Source UE and the 5G ProSe Target UE may establish an end-to-end Security via 5G ProSe UE-to-UE relay. The detail is not described in this solution.

Editor’s Note: The method for providing End to End IP security is FFS.

### 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.

Editor’s Note: Which network function provides authorization token and how the UEs get the public key of token signing entity are FFS.

### 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 request authorization tokens when they are in coverage.

Editor’s Note: Further provisioned parameters e.g., PC5 security policies of UE-to-UE relay, public keys are FFS.

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.

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.

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

Editor’s Note: Its FFS how token freshness is guaranteed as any peer UE can replay the token (since sent in the clear in DCR).

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.

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 Source UE and 5G ProSe UE-to-UE Relay continue with the rest of procedure for the UE-to-UE relay service over the secure PC5 link.

Editor’s Note: Further and remaining messages needs to be updated and clarified in step 8.

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

Editor’s Note: It is FFS whether PC5 security set up procedure between target UE and Relay UE is performed after or in parallel to the PC5 security set up procedure between source UE and Relay UE.

10. The 5G ProSe Source UE and the 5G ProSe Target UE may establish an end-to-end Security via 5G ProSe UE-to-UE relay. The detail is not described in this solution.

Editor’s Note: The method for providing End to End IP security is FFS.

Editor’s Note: The need of End-to-end security in L3 relay is FFS,

Editor’s Note: The impact on the protocol stack to support end-to-end security for a L3 relay is FFS.

### 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 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 6.6.2.1-1: End to end security establishment for Layer-2 UE-to-UE relay

Before Step 0, the source UE and target UE have discovered and attached to the UE-to-UE relay. Source UE and Target UE have also discovered each other.

0. During the UE-to-UE relay authentication, 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: How the source UE and the target UE generate the shared key KD is not addressed in this solution.

1. The source UE sends a Direct Security Mode Command message to the target UE through the UE-to-UE relay, which contains Source UE’s security capabilities, Nonce\_1, MSB of KD ID chosen by source UE to uniquely identify KD at source UE.

2a. Upon reception of the Direct Security Mode Command message from the UE-to-UE Relay, target UE generates the session key KD-sess as specified in clause 6.6.2.3.1, and 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 chooses the LSB of KD ID to uniquely identify KD at target 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.

2b. The target UE activates the integrity protection before sending the Direct Security Mode Response message.

3. The target UE sends the Direct Security Mode Response message to source UE through UE-to-UE relay, including Nonce\_2, LSB of KD ID, chosen MSB of KD-sess ID, chosen\_algs, and MAC for integrity protection, Source UE’s security capabilities, Source UE’s security policy.

4a. Upon reception of the Direct Security Mode Response 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 ID from the received LSB of KD ID and chosen MSB of KD ID, and stores the complete KD ID with KD. The source UE chooses the LSB of KD-sess ID, forms KD-sess ID from the received MSB of KD-sess ID and chosen LSB of KD-sess ID, and stores KD-sess ID with KD-sess.

4b. 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.

5. The source UE sends the Direct Security Mode Complete message to target UE through the UE-to-UE Relay, which contains the LSB of KD-sess ID.

6. 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 using the key and algorithm indicated in the chosen\_algs. The target UE forms the KD-sess ID and stores it with KD-sess.

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.

Editor’s Note: These Security Mode Command messages’ name shall be consistent with TR 23.700-33, which is FFS.

Editor’s Note: How to protect the privacy information in DSMC request message is FFS.

Editor’s Note: The need of Nounce-1 and Nounce-2 needs more justification.

Editor’s Note: Which peer UE starts the SMC procedure is FFS.

#### 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

When deriving the session key KD-sess from KD in source UE and target UE the following parameters shall be used to form the input S to the KDF.

- FC = 0xXX

- P0 = Nonce\_1

- L0 = length of Nonce\_1

- P1 = Nonce\_2

- L1 = length of Nonce\_2

The input key KEY shall be the KD.

6.6.2.3.2 Integrity and encryption keys derivation function

When deriving the keys KD-int, KD-enc from KD-sess in source UE and target UE, the following parameters shall be used to form the input S to the KDF.

- FC = 0xXX

- P0 = 0x00 if KD-enc is being derived or 0x01 if KD-int is being derived

- L0 = length of P0 (i.e. 0x00 0x01)

- P1 = algorithm identity

- L1 = length of algorithm identity (i.e. 0x00 0x01)

The algorithm identity shall be set as described in TS 33.501 [2].

The input key KEY shall be the 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:

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.

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 (UE1) and the Target UE (UE2) can discover each other by selecting the same UE-to-UE Relay.

Editor’s Note: Details of key pre-configuration is FFS.

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.

Editor’s Note: How the U2U relay determine to send DCR to UE2 is FFS.

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.

Editor’s Note: Which specific PAKE protocols can be used is FFS.

Editor’s Note: How to provision passwords is FFS.

### 6.10.3 Evaluation

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

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

## 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 | S3-221643 |  |  |  | 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 |