|  |  |
| --- | --- |
| 3GPP TR 33.847 V0.3.0 (2020-11) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of enhancement for proximity based services in the 5G System (5GS)  (Release 17) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal 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.  © 2020, 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 7

Introduction 8

1 Scope 9

2 References 9

3 Definitions of terms, symbols and abbreviations 10

3.1 Definitions 10

3.2 Abbreviations 10

4 Security Aspects of 5G ProSe 10

4.1 Architecture assumption 10

4.1.1 Introduction 10

4.1.2 Control Plane based architecture for direct discovery 10

4.2.1 User Plane based architecture for direct discovery 11

5 Key issues 12

5.1 Key Issue #1: Discovery message protection 12

5.1.1 Key issue details 12

5.1.2 Security threats 12

5.1.3 Potential security requirements 12

5.2 Key Issue #2: Keys in ProSe discovery scenario 13

5.2.1 Key issue details 13

5.2.2 Security threats 13

5.2.3 Potential security requirements 13

5.3 Key Issue #3: Security of UE-to-Network Relay 13

5.3.1 Key issue details 13

5.3.2 Security threats 14

5.3.3 Potential security requirements 14

5.4 Key issue #4: Authorization in the UE-to-Network relay scenario 15

5.4.1 Key issue details 15

5.4.2 Security threats 15

5.4.3 Potential security requirements 15

5.5 Key Issue #5: Privacy protection over the UE-to-Network Relay 16

5.5.1 Key issue details 16

5.5.2 Security threats 16

5.5.3 Potential security requirements 16

5.6 Key Issue #6: Integrity and confidentiality of information over the UE-to-UE Relay 16

5.6.1 Key issue details 16

5.6.2 Security threats 16

5.6.3 Potential security requirements 17

5.7 Key issue #7: Authorization in the UE-to-UE relay scenario 17

5.7.1 Key issue details 17

5.7.2 Security threats 17

5.7.3 Potential security requirements 17

5.8 Key Issue #8: Privacy of information over the UE-to-UE Relay 18

5.8.1 Key issue details 18

5.8.2 Security threats 18

5.8.3 Potential security requirements 18

5.9 Key Issue #9: Key management in 5G Proximity Services for UE-to-Network relay communication 18

5.9.1 Key issue details 18

5.9.2 Security threats 19

5.9.3 Potential security requirements 19

5.10 Key Issue #10: Key issue on secure data transfer between UE and 5GDDNMF 19

5.10.1 Key issue details 19

5.10.2 Security threats 20

5.10.3 Potential requirements 20

5.11 Key Issue #11: UE identity protection during ProSe discovery 20

5.11.1 Key issue details 20

5.11.2 Security threats 20

5.11.3 Potential security requirements 20

5.12 Key Issue #12: Security of one-to-one communication over PC5 21

5.12.1 Key issue details 21

5.12.2 Security threats 21

5.12.3 Potential security requirements 21

5.13 Key Issue #13: Security and privacy of groupcast communication 22

5.13.1 Key issue details 22

5.13.2 Security threats 22

5.13.3 Potential security requirements 22

5.14 Key Issue #14: security for support of Non-IP traffic 22

5.14.1 Key issue details 22

5.14.2 Security threats 23

5.14.3 Potential security requirements 23

5.15 Key Issue #15: privacy of ProSe entities while supporting Non-IP traffic 23

5.15.1 Key issue details 23

5.15.2 Security threats 24

5.15.3 Potential security requirements 24

5.16 Key Issue #x: Privacy protection of PDU session-related parameters for relaying. 24

5.16.1 Key issue details 24

5.16.2 Security threats 25

5.16.3 Potential security requirements 25

5.X Key Issue #X: <Key Issue Name> 25

5.X.1 Key issue details 25

5.X.2 Security threats 25

5.X.3 Potential security requirements 25

6 Solutions 25

6.0 Mapping of Solutions to Key Issues 26

6.1 Solution #1: Solution for key management in 5G Proximity Services relay communication 26

6.1.1 Introduction 26

6.1.2 Solution details 26

6.1.3 Evaluation 28

6.2 Solution #2: Secure data transfer between UE and 5GDDNMF 29

6.2.1 Introduction 29

6.2.2 Solution details 29

6.2.3 Evaluation 29

6.3 Solution #3: Reuse LTE security mechanism for 5G ProSe open discovery 30

6.3.1 Introduction 30

6.3.2 Solution details 30

6.3.3 Evaluation 32

6.4 Solution #4: Reuse LTE security mechanism for 5G ProSe restricted discovery 32

6.4.1 Introduction 32

6.4.2 Solution details 33

6.4.2.1 Model A restricted discovery 33

6.4.2.2 Model B restricted discovery 34

6.4.3 Evaluation 36

6.5 Solution #5: Protection of the PC3 interface using AKMA and TLS 37

6.5.1 Introduction 37

6.5.2 Solution details 37

6.5.3 Evaluation 38

6.6 Solution #6: Key management for UE-to-Network Relays and Remote UE’s 38

6.6.1 Introduction 38

6.6.2 Solution details 38

6.7 Solution #7: Security establishment of one-to-one PC5 communication 41

6.7.1 Solution overview 41

6.7.2 Solution details 41

6.7.3 Evaluation 42

6.8 Solution #8: Confidential protection against UE-to-UE relay using asymmetric cryptography 43

6.8.1 Introduction 43

6.8.2 Solution details 43

6.8.2.1 Procedure 43

6.8.3 Evaluation 44

6.9 Solution #9: Key management in discovery procedure 44

6.9.1 Solution overview 44

6.9.2 Solution details 44

6.9.3 Evaluation 45

6.10 Solution #10: Authorization and security with UE-to-Network relay using Remote UE network primary authentication 45

6.10.1 Solution overview 45

6.10.2 Solution details 45

6.10.3 Solution evaluation 48

6.11 Solution #11: Protection of the PC3 interface using GBA 48

6.11.1 Introduction 48

6.11.2 Solution details 48

6.11.3 Evaluation 48

6.12 Solution #12: Privacy handling for Layer-3 UE-to-UE Relay based on IP routing 48

6.12.1 Description 48

6.12.2 Solution details 48

6.12.3 Evaluation 50

6.13 Solution #13: Secondary Authentication for a Layer 3 Remote UE 50

6.13.1 Introduction 50

6.13.2 Solution details 51

6.13.2.1 Secondary Authentication after PC5 link setup 51

6.13.2.2 Secondary Authentication before PC5 link setup 53

6.13.3 Evaluation 54

6.14 Solution #14: A security solution for UE-to-Network Relay based on Layer 2 Relay 54

6.14.1 Introduction 54

6.14.2 Solution details 55

6.14.3 Evaluation 56

6.15 Solution #15: Key management in UE-to-Network Relay based on primary authentication 56

6.15.1 Introduction 56

6.15.2 Solution details 56

6.15.3 Evaluation 58

6.16 Solution #16: Security establishment procedures between two UEs in the UE-to-UE relay scenario 58

6.16.1 Introduction 58

6.16.2 Solution details 58

6.16.3 Evaluation 59

6.18 Solution #18: PC5 link setup for UE-to-Network relay 60

6.18.1 Introduction 60

6.18.2 Solution details 60

6.18.3 Evaluation 62

6.19 Solution #19: End-to-end security for the L3 UE-to-Network relay 62

6.19.1 Introduction 62

6.19.2 Solution details 63

6.19.3 Evaluation 63

6.20 Solution #20: PC5 link setup for UE-to-UE relay 63

6.20.1 Introduction 63

6.20.2 Solution details 64

6.20.3 Evaluation 65

6.21 Solution #21: AF for key management in PC5 communication 65

6.21.1 Introduction 65

6.21.2 Solution details 65

6.21.3 Evaluation 67

6.22 Solution #22: Masked representation of identities 67

6.22.1 Introduction 67

6.22.2 Solution details 68

6.22.2.1 Solution for Model A 68

6.22.2.2 Solution for Model B 69

6.22.3 Evaluation 71

6.23 Solution #23: Initial key with validity time 71

6.23.1 Introduction 71

6.23.2 Solution details 72

6.23.3 Evaluation 72

6.Y Solution #Y: <Solution Name> 72

6.Y.1 Introduction 72

6.Y.2 Solution details 72

6.Y.3 Evaluation 72

7 Conclusions 72

Annex <X> (informative): Change history 73

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

# 1 Scope

This document studies the security and privacy aspects of proximity based services (including public safety and commercial proximity services) in the 5G system. It ensures that the security solutions are aligned with the work in TR 23.752 [2], TS 22.278 [3] and TS 22.261 [4]. This document covers the following issues:

* Security and privacy key issues, threats and potential requirements of proximity based services in 5G system.
* 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 23.752: "Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS)".

[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 23.303: "Proximity-based services (ProSe); Stage 2".

[6] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[7] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[8] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[9] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[10] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[11] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[12] 3GPP TS 33.220: "Generic Authentication Architecture (GAA), Generic Bootstrapping Architecture (GBA)".

[13] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[14] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[15] 3GPP TS 23.501: "System Architecture for the 5G System".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions 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 UE-to-Network Relay:** A UE that provides functionality to support connectivity to the network for Remote UE(s).

## 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].

5GC 5G Core

ProSe Proximity-based Services

5G DDNMF 5G Direct Discovery Name Management Function

AF Application Function

AMF Access and Mobility management Function

AS layer Access Stratum layer

NG Next Generation

NG-RAN Next Generation RAN

NGAP NG Application Protocol

NR New Radio (5G)

PCF Policy Control Function

RAN Radio Access Network

RAT Radio Access Technology

REAR Remote UE Access via Relay UE

UDM Unified Data Management

# 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-17 security mechanisms.

## 4.1 Architecture assumption

### 4.1.1 Introduction

The following clauses describe the control plane based and user plane based architecture for supporting 5G ProSe direct discovery.

### 4.1.2 Control Plane based architecture for direct discovery

The Control Plane based architecture has been captured in TR 23.752[2] Annex B.



Figure 4.1.1-1: Control Plane based architecture

In Figure 4.1.1-1, 5G DDNMF is introduced into 5GC as a new network function. 5G DDNMF has similar functions from architecture point of view to the DDNMF part of ProSe Function as defined in TS 23.303[5].

Control Plane based 5G Prose architecture only reuses the PC5 interface comparing to the Prose Architecture defined in TS 23.303[5]. This means the UE will use NAS message to get discovery parameters for open discovery or restricted discovery.

### 4.2.1 User Plane based architecture for direct discovery

The User Plane based architecture has been captured in TR 23.752[2] Annex B.



Figure 4.2.1-1: User Plane based architecture

In Figure 4.2.1-1, 5G DDNMF is introduced into 5GC as a new network function. 5G DDNMF has similar functions from architecture point of view to the DDNMF part of ProSe Function as defined in TS 23.303[5].

User Plane based 5G Prose architecture tries to reuse Prose reference points defined in TS 23.303[5], especially for PC2 and PC3 reference points.

# 5 Key issues

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

## 5.1 Key Issue #1: Discovery message protection

### 5.1.1 Key issue details

The Open ProSe direct discovery procedure is used for a UE to discover or be discovered by other UE(s) in proximity over the PC5 interface. The UE can discover other UE(s) with interested application(s) and/or interested group(s) using the ProSe direct discovery procedure. In Open Discovery, a UE which wants to discover other UE’s does not require any explicit permission from the other UE’s in order to be allowed to discover them.

The Restricted ProSe direct discovery procedure is used for a UE to discover or be discovered by other UE(s) in proximity over the PC5 interface. In Restricted Discovery, a UE which wants to discover other UE’s requires an explicit permission from the other UE’s in order to be allowed to discover them.

There could be a case where a discoverer UE intends to discover two different discoveree UEs (called discoveree UE A and discoveree UE B) at a time. With the existing ProSe architecture, the three UEs have to have the same security keys to support the case.

There is a vulnerability with the model B architecture in this use case. Despite discoveree UE A allowing to be discovered by only the discoverer UE, discoveree UE B is also capable of detecting and decoding the discovery response message from discoveree UE A because it has the same keys, and thus discovering discoveree UE A.

Hence it needs to be studied how to protect the discovery response message of a UE in a restricted direct discovery model B architecture mode from being discovered by other discoveree UE(s).

Editor’s Note: Whether there is a case where a discoverer UE wants to discover more than one different discoveree UEs using same ProSe service at a time is FFS.

### 5.1.2 Security threats

If the discovery message cannot be confidentiality protected, integrity protected, and replay protected, the Prose APP Code can be intercepted, modified, or replayed by an attacker. The announcing UE or discoveree UE may connect with a UE that is not interested in that particular Prose service.

An attacker may impersonate the discoveree or the discovered UE.

A discoveree UE can detect the response message from other discoveree UE(s) that uses the same security keys in restricted direct discovery model B architecture, and may discover other discoveree UE(s), that are not supposed to be discoverable to it. This puts the privacy of other discoveree UE(s) at risk.

Editor’s Note: Whether this threat is valid is FFS.

### 5.1.3 Potential security requirements

The discovery message in open discovery shall support integrity protection and replay protection.

The discovery message in restricted discovery shall support confidentiality protection, integrity protection, and replay protection.

The entity which receives a restricted discovery message on the PC5 interface shall be able to verify the source authenticity.

Editor note: It is FFS in SA2 whether ProSe code or similar parameter will be used in discovery messages sent on PC5 interface. Any related privacy issues with the use of ProSe code or similar parameter needs to be further studied in restricted discovery.

The 5G System shall provide means to protect the discovery response message of a discoveree UE in the restricted direct discovery model B architecture from other discoveree UE(s).

Editor’s Note: In case that a discoverer UE wants to discover more than one different discoveree UEs using same ProSe service at a time, if security protection between different discoveree UEs is needed is FFS

## 5.2 Key Issue #2: Keys in ProSe discovery scenario

### 5.2.1 Key issue details

In TS 33.303[6], Prose Function sends discovery key to announce UE for calculating MIC in open discovery. In Restricted discovery, Prose Function also may send DUCK, DUIK, and DUSK to UEs.

In 5G, the functions of Prose Function are split into different network functions along with different network architecture approaches. Meanwhile, AKMA has been defined in TS 33.535[7], and GBA is under study to adapt to 5G system. The elements above have to be considered to calculate and share discovery key(s) to UEs in 5G Prose.

Following issues need to be addressed in this key issue:

- Which network function derives the discovery key.

- How to send the keys to the UEs.

### 5.2.2 Security threats

Not applicable

### 5.2.3 Potential security requirements

Not applicable

## 5.3 Key Issue #3: Security of UE-to-Network Relay

### 5.3.1 Key issue details

In KI#3 of TR 23.752[2], the UE maybe be able to access the network via the direct network communication or the indirect network communication as showing in figure 5.3.1-1. The path#1 is direct network communication path and the path#2 and path#3 are indirect network communication paths via different UE-to-network Relays.



Figure 5.3.1-1

The UE-to-Network relay is registered to the 5GS as a UE. In order to provide service to the remote UE, the UE-to-Network relay needs to establish an NR PC5 link with the Remote UE. Security for PC5 link establishment is documented for LTE Prose in TS 33.303 [6] and for eV2X in TS 33.536 [8]. However, it should be studied how to accommodate such procedures to 5G Prose.

For UE-to-Network relay, two options (Layer-2 UE-to-Network relay and Layer-3 UE-to-Network relay) are under consideration in TR 23.752 [2]. Both options commonly provide network access service to remote UE with the following differences.

* Layer 2 relay: remote UE is registered to the 5GC and has an AS security context established with the gNB in the connected mode.
* Layer 3 relay: remote UE may be registered to the 5GC, but does not have an AS security context.

Both options described above require PC5 unicast link between the remote UE and UE-to-Network relay. Therefore, it should be studied how to establish PC5 link securely (e.g., authentication and security context establishment) for both options.

TR 23.752 [2] in Clause 5.3, Key Issue #3: Support of UE-to-Network Relay has the following key issue:

*- How to transfer data between the Remote UE and the network over the UE-to-Network Relay.*

*NOTE 1: Security and privacy aspects will be handled by SA WG3.*

The UE-to-Network Relay in 5G is enhanced compared to LTE ProSe, to support commercial case. This may bring new security requirements compared to LTE Prose where the UE-to-Network Relay is only used in public safety scenario as defined in clause 4.4.3 of TS 23.303[5]. Public safety enabled UEs can be considered under control by police or government. When a UE-to-Network Relay is used in commercial case, the UE-to-network Relay may be a commercial UE that could belong to any person. In this case, the trust relationship between remote UE and relay UE is not as strong as the trust relationship between public safety enabled UEs.

### 5.3.2 Security threats

Lack of security during PC5 link establishment for UE-to-Network relay may cause to DoS attacks against the remote UE.

Lack of security during PC5 link establishment for UE-to-Network relay may allow MitM attack where the attacker can eavesdrop, modify, or inject messages into the remote UE data.

Failure to protect integrity and confidentiality of information exchanged between the Remote UE and the network over the UE-to-Network Relay will open vulnerability in 5GS and allow various attacks such as unauthorised access..If the UE-to-Network Relay is compromised, the security (i.e., the integrity and confidentiality) of information between the Remote UE and the network may be compromised.

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

### 5.3.3 Potential security requirements

The system shall support a secure means to establish a PC5 link between the remote UE and the UE-to-Network relay.

Confidentiality protection, Integrity protection and replay-protection shall be supported between the remote UE and the 3GPP network.

3GPP system shall provide means to protect security (i.e., the integrity and confidentiality) of information during UE-to-Network Relay path switch.

## 5.4 Key issue #4: Authorization in the UE-to-Network relay scenario

### 5.4.1 Key issue details

3GPP system has to be able to authorise a UE to access 5GC via a 5G UE-to-Network Relay and to authorise a UE to perform as a UE-to-Network Relay. Without a proper authorisation, unauthorised entities will be able to access 5GC via UE-to-Network Relay or act as UE-to-Network Relays creating a vulnerability and causing possible (D)DOS attacks or leading to unauthorised service usage on both 5GS and UE-to-Network Relay.

TR 23.752 [2], key issue #3 describes the issue on the support of UE-to-Network Relay, i.e.

*“-How to authorize a UE to be a 5G UE-to-Network Relay and how to authorize a UE to access 5GC via a 5G UE-to-Network Relay.*

*…*

*NOTE 1: Security and privacy aspects will be handled by SA WG3”*

From the security point of view, whether the UE can play the UE-to-Network Relay role should be assured by the Remote UE. On the contrary, whether the UE can play the remote UE role shouldl be assured by the UE-to-Network relay.

In addition, the following aspects on how the network authorizes the Remote UE via the UE-to-Network Relay need to be studied:

* Should there be different authorization mechanisms for L2 and L3 relay?
* Which Network Functions should be involved in the Remote UE authorization?
* What type of information (e.g. identifiers) should the Remote UE provide to the network via the UE-to-Network Relay and how should it be used for Remote UE authorization?

This key issue is to study the authorization issue in the UE-to-Network relay scenario.

### 5.4.2 Security threats

An attacker may impersonate the UE-to-Network Relay. If the authorization of the UE-to-Network relay role is not supported, the attacker UE could play the UE-to-Network relay role, and force a UE to camp on to it by passing all the message on between the UE and the network. It may then deny the UE services between the two UEs, such as drop the message.

An attacker may impersonate the Remote UE. If the authorization of the remote UE is not supported, the attacker UE could play the remote UE role, and arbitrarily consume the services provided by the UE-to-Network relay. The charging of the attacker UE as a remote UE may not be supported.

### 5.4.3 Potential security requirements

The 5GS shall support to authorize the UE as a UE-to-Network relay in the UE-to-Network relay scenario.

The 5GS shall support to authorize the UE as a Remote UE in the UE-to-Network relay scenario.

## 5.5 Key Issue #5: Privacy protection over the UE-to-Network Relay

### 5.5.1 Key issue details

3GPP system has to be able to protect privacy of the Remote UE that is using the UE-to-Network Relay. Failure to protect privacy of the Remote UE that is using the UE-to-Network Relay will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

TR 23.752 [2] in Clause 5.3, Key Issue #3: Support of UE-to-Network Relay has the following key issue:

*- How to transfer data between the Remote UE and the network over the UE-to-Network Relay.*

*NOTE 1: Security and privacy aspects will be handled by SA WG3.*

### 5.5.2 Security threats

Failure to protect privacy of the Remote UE that is using the UE-to-Network Relay will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

Path switch between UE-to-Network 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-Network 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 privacy of entities and identities during UE-to-Network Relay path change will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of entities and identities.

### 5.5.3 Potential security requirements

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

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

## 5.6 Key Issue #6: Integrity and confidentiality of information over the UE-to-UE Relay

### 5.6.1 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 unauthorised disclosure and modification of information. Protection of communications between the peer UEs should take into consideration that the UE-to-UE Relay is an untrusted node.

TR 23.752 [2] in Clause 5.4, Key Issue #4: Support of UE-to-UE Relay, has the following key issue:

*- How to enhance the system architecture to provide the security protection for relayed connection?*

### 5.6.2 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 unauthorised disclosure and modification of information.

The UE-to-UE Relay being an untrusted node may be compromised, allowing the security (i.e., the integrity and confidentiality) of information between the peer UEs to be compromised. Therefore, end-to-end security between the peer UEs communicating over the UE-to-UE Relay is needed.

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

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

### 5.6.3 Potential security requirements

3GPP system shall provide means to confidentially and integrity protect security end-to-end between the peer UEs during communications over the UE-to-UE Relay.

3GPP system shall provide means to protect security (i.e., the integrity, confidentiality, and replay protection) of user plane data and signalling information during UE-to-UE Relay path switch.

## 5.7 Key issue #7: Authorization in the UE-to-UE relay scenario

### 5.7.1 Key issue details

TR 23.752 [2], key issue #4 describes its Key Issue regarding support of UE-to-UE Relay:

*“- Whether and how for the network can control the 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 the Remote UE to access a UE-to-UE Relay?*

*…*

*NOTE 2: For security aspects, coordination with SA3 is needed.”*

From a security point of view, whether the UE can act as a UE-to-UE Relay is be assured by the Remote UE. On the contrary, whether the UE can act as a remote UE should be assured by the UE-to-UE relay.

3GPP system has to be able to autorise a UE to perform as UE-to-UE Relay and a UE to communicate with another UE via a UE-to-UE Relay. This key issue directs SA3 to study the authorization aspects in the UE-to-UE relay scenario.

### 5.7.2 Security threats

An attacker may impersonate the UE-to-UE Relay. If the authorization of the UE acting as UE-to-UE relay is not supported, the attacker UE may impersonate the UE-to-UE relay, and force a remote UE to camp on it by passing messages between two UEs. The attacker may then deny the UE services between the two UEs (e.g., arbitrary discard messages).

An attacker may impersonate the source UE or the target UE.

### 5.7.3 Potential security requirements

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

Authorisation of a UE that requests to be a source UE or a target UE discovering a UE-to-UE Relay, should be provided.

3GPP system shall provide means to authorise a UE to communicate with another UE via a UE-to-UE Relay.

## 5.8 Key Issue #8: Privacy of information over the UE-to-UE Relay

### 5.8.1 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 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 23.752 [2] in Clause 5.4, Key Issue #4: Support of UE-to-UE Relay, has the following key issue:

*- How to enhance the system architecture to provide the security protection for relayed connection?*

### 5.8.2 Security threats

Failure to protect 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.

Existing Link identifier update procedure specified in TS 33.536 [8] 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.

### 5.8.3 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 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 UE-to-UE Relay path switch.

## 5.9 Key Issue #9: Key management in 5G Proximity Services for UE-to-Network relay communication

### 5.9.1 Key issue details

This key issue covers both Layer-2 and Layer-3 relays in 5G Proximity Services.

TR 23.752 [2] has candidate solution for both layer 2 and layer 3 UE-to-network relay. There are security solutions which will be adapted for PC5 unicast communication for ProSe from 5G V2X.

Currently, V2X does not support relay communication (both UE-to-network or UE-to-UE relay).

Based on V2X security TS 33.536 [8], the Direct Provisioning Function (DPF) defined in TS 23.303 [5] is replaced by PCF, based on the V2X architecture as defined in TS 23.287 [9], and is not supported by the DDNMF. The architecture reference model as described in clause 2 User Plane based architecture, with the following additional considerations:

* each PLMN deploys one logical 5G DDNMF
* the 5G DDNMF interacts with PCF for the authorization of the ProSe discovery service



Figure 5.9.1-1: User Plane architecture for ProSe

In LTE ProSe, the ProSe Key Management Function supports the key derivation required to support the UE-to-network relay communication.

Whereas in 5G the existing entity can support the key derivation, authentication and authorization of the remote UE and UE-to-Network relay.

In order to attach to the network via a UE-to-network relay, a remote UE may have to authenticate to the network and vice versa. Because the UE-to-network relay sits in between the remote UE and the network, it may have the possibility to perform MitM, DoS, and replay attacks in between.

### 5.9.2 Security threats

Following are the possible threats

- A man-in-the-middle attack by the relay UE;

- A denial of service attack by the relay UE on the remote UE;

- Impersonation of the remote UE by the relay UE.

### 5.9.3 Potential security requirements

- 5GS shall support secure communication between the remote UE and the network via UE-to-Network relays.

- 5GS shall support generation of separate security contexts for remote UEs for ProSe relay communication.

## 5.10 Key Issue #10: Key issue on secure data transfer between UE and 5GDDNMF

### 5.10.1 Key issue details

This key issue describes about the issue in secure communication between UE and ProSe function (5GDDNMF).

The ProSe-enabled UEs have many interactions with the 5GDDNMFin the 5G ProSe solution currently described in SA2 study TR 23.752 [2]. For example, to retrieve ProSe Discovery parameters and provision of ProSe discovery related security parameters.

If not secured an attacker may manipulate or modify the data being transmitted between UE and 5GDDNMF, thus adversely affecting the ProSe communication.

### 5.10.2 Security threats

- An attacker may manipulate the data being transmitted between the UE and 5GDDNMF, thus adversely affecting the ProSe communication.;

- An attacker may eavesdrop on transmitted data and further utilize it for improper use.;

- An attacker may replay an intercepted data thus affecting an expected state of action at the ProSe-enabled UE. .

### 5.10.3 Potential requirements

The ProSe-enabled UE and 5GDDNMF shall mutually authenticate each other for secure ProSe communication.

The transmission of data between 5GDDNMF and the ProSe-enabled UE shall be integrity protected.

The transmission of data between 5GDDNMF and the ProSe-enabled UE shall be confidentiality protected

The transmission of data between 5GDDNMF and the ProSe-enabled UE shall be protected from replay attacks.

## 5.11 Key Issue #11: UE identity protection during ProSe discovery

### 5.11.1 Key issue details

During ProSe discovery a ProSe UE that is to be discovered needs to broadcast information via which it can be discovered. In some use cases the broadcasted information is uniquely associated to the (identity of the) ProSe UE. If this broadcasted information is not properly protected, the privacy of the UE can not be guaranteed in the sense that the UE can be traced and followed. Also impersonation of the ProSe UE can occur leading to identity theft.

### 5.11.2 Security threats

A ProSe UE identity broadcasted during ProSe discovery can be used to trace a ProSe.

A ProSe UE identity broadcasted during ProSe discovery can be used to impersonate the ProSe UE.

### 5.11.3 Potential security requirements

The 5GS shall provide means to mitigate against the use of the identity of a ProSe UE broadcasted during ProSe discovery to trace the ProSe UE.

The 5GS shall provide means to mitigate against the use of the identity of a ProSe UE broadcasted during ProSe discovery to impersonate the ProSe UE.

## 5.12 Key Issue #12: Security of one-to-one communication over PC5

### 5.12.1 Key issue details

One-to-one ProSe communication is realised by establishing a secure link over PC5 between initiating UE and peer UE, it is used by two UEs that want to directly exchange traffic or when a remote UE attaches to ProSe relay. The establishment of this secure link needs to be possible also when either one or both the ProSe UEs are out-of-coverage.

Editor’s Note: the one-to-one communication policy/parameter provisioning procedure should inline with SA2.

The LTE ProSe one-to-one communication may happen after discovery procedures, or after one-to-many ProSe communications. The detailed one-to-one (i.e. unicast) communication and the corresponding security aspects are defined for LTE ProSe in 3GPP TS 23.303 [5] and TS 33.303 [6], respectively. 2The architecture study in the TR 23.752 [2] proposes to introduce new features to 5G ProSe from 5G V2X, this may protentially reuse the security meshanisms from 5G V2X as defined in TS 33.536 [8]. Although the 5G V2X and the ProSe one-to-one communications both rely on the PC5 reference point, the ProSe may not be able to fully reuse the security mechanisms from 5G V2X scenario which is due to the fact that they may use different processing procedures. For this reason, it’s necessary to study the security of one-to-one communication which is dedicated for 5G ProSe scenario. 5G ProSe needs a reliable mechanism to establish and to use one-to-one communication over PC5.

### 5.12.2 Security threats

If the two UE cannot be mutually authenticated during one-to-one communication, a peer may connect to an attacker.

The signalling and user plane message exchanges during one-to-one communication may be seen in cleartext, modified or replayed by an attacker if lack of confidentiality protection and integrity protection.

If one-to-one communication (unicast) mechanism in 5G V2X is reused, an attacker may deploy bidding-down attack to force establishing unprotected connection between initiating UE and peer UE.

Failure to secure protect the security context refreshing may introduce potential vulnerability.

### 5.12.3 Potential security requirements

The initiating UE shall establish a different security context for each peer UE during the PC5 one-to-one communication establishment if the security is activated. It shall be possible to establish this security context also when either one or both the ProSe UEs are out-of-coverage.

The mutual authentication between two UEs during one-to-one communication shall be supported.

The one-to-one communication link security establishment shall be protected from MitM attacks.

The PC5 one-to-one communication signalling shall support confidentiality protection, integrity protection and anti-replay protection.

The PC5 one-to-one communication user plane shall support confidentiality protection, integrity protection and anti-replay protection.

The system shall support means of providing the signalling and user plane security policies to UEs for a particular PC5 one-to-one communication.

The initiating UE and peer UE shall provide a means to mitigate establishing unprotected connection caused by bidding-down attack.

The system shall support means for a secure refresh of the UE security context.

NOTE: The security context refresh may be triggered based on various options (e.g. validity time etc.)

## 5.13 Key Issue #13: Security and privacy of groupcast communication

### 5.13.1 Key issue details

In TR 23.752 [2], Solution #22 "V2X-based group communication for commercial services" mentions the following note:

*“NOTE 2: The mechanism for converting the ProSe application layer provided group identifier to the destination Layer-2 ID depends on the conclusion of KI#8.”*

Solution #37 “Groupcast mode communication for commercial services and public safety” and solution#4 “PC5 group communication for commercial services”, also mentions the provisioning of Application layer group ID and the corresponding Destination L2-IDs in collaboration with the application server.

Thus far solution #7, #35 and #36 have been proposed for KI#8 “Support of PC5 Service Authorization and Policy/Parameter Provisioning” but do not address the conversion mechanism for application layer group ID to the destination L2 ID.

This conversion/mapping procedure should be secured in terms of privacy and traceability. Unless the conversion is carefully performed, the group membership of specific UEs could be disclosed. For example, attackers might be able to make an inquiry whether any member of certain group are exists in some location.

Also, for group communications, UEs are able to start communication without first discovering the receiving UE(s). This means that a UE can unilaterally start sending encrypted one-to-many data packets, which may be successfully decrypted by other group members without knowing in advance which group members can actually receive the data. Security for one-to-many direct communication in LTE Prose is specified in TS 33.303 [6]. However, it should be studied how to accommodate such procedures to 5G Prose.

In 5GS, ProSe services can be used for both public safety services and commercial services (e.g. interactive service). In TR 23.752 [2], group communications for commercial services has been studied. Therefore, the security of ProSe group communications for commercial services needs to be considered.

### 5.13.2 Security threats

If the group IDs are not securely converted by the application layer, the intruder can link them back to UE groupcast memberships, revealing which UEs have been associated with a specific group and hence causes privacy attacks.

Failures to protect groupcastcommunications, the following threats are identified:

- Passive attackers can eavesdrop on data packets exchanged between UEs.

- Active attackers can intercept, modify or replay data packets exchanged between UEs.

- An UE as a group member may be impersonated by an attacker.

### 5.13.3 Potential security requirements

5G system shall ensure that the group IDs and L2 IDs are protected from linkability and traceability attacks for ProSe groupcast communications.

One-to-many communications between ProSe-enabled UEs shall be protected by confidentiality and integrity.

## 5.14 Key Issue #14: security for support of Non-IP traffic

### 5.14.1 Key issue details

3GPP system has to be able to preserve security (i.e., the integrity and confidentiality) while supporting Non-IP traffic. Failure to protect integrity and confidentiality of information while supporting Non-IP traffic will open vulnerability in 5GS and allow attacks such as unauthorised disclosure and modification of information.

TR 23.752 [2] in Clause 6.5.2, Procedures, states the following:

*The "Procedures for V2X communication over PC5 reference point" defined in TS 23.287 [5] clause 6.3 is reused to support ProSe communication over NR based PC5 reference point, and the differences are highlighted as followings.*

*- For broadcast and groupcast mode ProSe communication, the procedures as defined in TS 23.287 [5] clauses 6.3.1 and 6.3.2 are applied with the following differences are identified:*

*- The following data unit types are supported: IP, non-IP, Ethernet, Unstructured and Address Resolution Protocol (see RFC 826 [10]).*

*NOTE: Whether "non-IP type" is used for "Unstructured type" can be decided in normative phase.*

*- The ProSe Group IP multicast address for groupcast communication may be provisioned by PCF and is used to send and receive IP data.*

*- For unicast mode ProSe communication, the procedure as defined in TS 23.287 [5] clause 6.3.3 is applied with the following differences are identified:*

*- DHCPv4 based IP address allocation is supported.*

*- Both Ethernet and Unstructured data unit types are supported.*

Multiple solutions in TR 23.752 [2] address support of NoN-IP traffic and require security and privacy protection to be addressed in the present document.

### 5.14.2 Security threats

Failure to protect integrity and confidentiality of information while supporting NoN-IP traffic for unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays, will open vulnerability in 5GS and allow various attacks resulting in unauthorised disclosure and modification of information.

### 5.14.3 Potential security requirements

3GPP system shall provide means to protect security (i.e., the integrity, confidentiality, and replay protection) while supporting NoN-IP traffic for unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays.

## 5.15 Key Issue #15: privacy of ProSe entities while supporting Non-IP traffic

### 5.15.1 Key issue details

3GPP system has to be able to preserve privacy of ProSe entities while supporting NoN-IP traffic. Failure to protect privacy of identities while supporting NoN-IP traffic will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

TR 23.752 [2] in Clause 6.5.2, Procedures, states the following:

*The "Procedures for V2X communication over PC5 reference point" defined in TS 23.287 [5] clause 6.3 is reused to support ProSe communication over NR based PC5 reference point, and the differences are highlighted as followings.*

*- For broadcast and groupcast mode ProSe communication, the procedures as defined in TS 23.287 [5] clauses 6.3.1 and 6.3.2 are applied with the following differences are identified:*

*- The following data unit types are supported: IP, non-IP, Ethernet, Unstructured and Address Resolution Protocol (see RFC 826 [10]).*

*NOTE: Whether "non-IP type" is used for "Unstructured type" can be decided in normative phase.*

*- The ProSe Group IP multicast address for groupcast communication may be provisioned by PCF and is used to send and receive IP data.*

*- For unicast mode ProSe communication, the procedure as defined in TS 23.287 [5] clause 6.3.3 is applied with the following differences are identified:*

*- DHCPv4 based IP address allocation is supported.*

*- Both Ethernet and Unstructured data unit types are supported.*

Multiple solutions in TR 23.752 [2] address support of NoN-IP traffic and require security and privacy protection to be addressed in the present document.

### 5.15.2 Security threats

Failure to protect privacy of entities and identities while supporting NoN-IP traffic for unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of entities and identities.

### 5.15.3 Potential security requirements

3GPP system shall provide means to preserve privacy of entities and identities while supporting NoN-IP unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays.

NoN-IP traffic unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays.

unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays

## 5.16 Key Issue #x: Privacy protection of PDU session-related parameters for relaying.

## 5.16.1 Key issue details

As part of Key Issue #3 in TR 23.752 [2], SA2 studies layer-2 and layer-3 relays. One of the aspects to be studied as denoted in Key Issue #3 is:

*“- How to support end-to-end requirements between Remote UE and the network via a UE-to-Network Relay, including QoS (such as data rate, reliability, latency) and the handling of PDU Session related attributes (e.g. S-NSSAI, DNN, PDU Session Type and SSC mode).”*

In case of Layer-2 relays, the Remote UE itself is responsible to perform initial registration and set up the PDU session with the Core Network, and the UE-to-Network relay is expected to transparently forward all RRC and NAS messages to/from the network. Although privacy-sensitive slice information from a Remote UE may be revealed to a UE-to-Network relay if requested NSSAI information is included during the initial registration, it is assumed that the inclusion of the requested NSSAI information can be controlled in a similar manner as specified in clause 5.15.9 “Operator-controlled inclusion of NSSAI in Access Stratum Connection Establishment” of TS 23.501 [15]. The subsequent PDU session request is sent only after AS security is established between the UE and the network and hence the privacy sensitive information contained in that request (e.g. requested NSSAI, requested DNN) is not exposed to the UE-to-Network relay.

For Layer-3 relays, the UE-to-Network relay is responsible for setting up a PDU session to the Core Network on behalf of the Remote UE, in order to send the relayed traffic to the Core Network. To facilitate this, the UE-to-Network relay needs to be provided with the PDU session parameters that the Remote UE needs to use for its applications to make sure it connects to the correct DNN, slice, etc. However, if information about PDU session attributes, such as information about a particular slice and/or DNN that a Remote UE wishes to use, is exposed, pre-configured or otherwise made available to UE-to-Network relays or other Remote UEs, this may impose a privacy risk for the Remote UE. In particular, since relay UEs and remote UEs are typically end-user devices, and hence these may not be trusted at the same level as base stations or core network functions.

Several solutions in TR 23.752 [2] (such as solutions #16, #19, #28, #35) that are dealing with preconfiguring PDU session parameter related information to Remote UEs and UE-to-Network relays, dealing with discovery, and dealing with connection setup have already identified an action for SA WG3 to study the privacy concerns that were raised, e.g.:

*“Editor's note: The privacy protection for S-NSSAI information and group information in discovery message and the security of pre-configuring, storing and exposing all this privacy sensitive information with the UE-to-Network relay is FFS and in coordination with SA WG3.”*

*“NOTE: The privacy aspects of preconfiguring slicing information in UE-to-Network relays need to be coordinated with SA WG3.”*

*“NOTE 1: The privacy aspects of transporting PDU session parameters using an unsecured PC5 Direct Communication Request message need to be coordinated with SA WG3.”*

This key issue is to study the privacy issues related to the pre-configuration of PDU session parameter related information to UE-to-Network relays and Remote UEs, and privacy issues related to exposing PDU session parameter related information during discovery and/or connection setup messages.

Editor’s Note: It is FFS whether for Layer-2 relays existing mechanisms (as described above) can be assumed to be sufficient and do not need to be studied further.

### 5.16.2 Security threats

Information related to slices and DNNs that a UE uses or wishes to use for its relay operation (i.e. for the purpose of relay selection and/or setting up a relayed connection to the network), is privacy sensitive as it may reveal that a UE belongs a special subscription group, e.g. police/law enforcement/customs, or is linked e.g. to a healthcare facility. This leads to the following threats:

- Exposure of this information in the clear (e.g. in discovery or connection setup messages) enable eavesdroppers to perform privacy attacks on Remote UEs or UE-to-Network relays.

### 5.16.3 Potential security requirements

The 5G System shall provide a means to mitigate tracing and tracking privacy attacks on Remote UEs based on potential exposure of slicing information, DNN information, and other PDU session related persistent information.

## 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 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 1 |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |
| 3 | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |
| 6 |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |
| 8 |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |
| 9 |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  | X | X |  |  |  |  | X |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |  |
| 13 |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |
| 14 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 15 |  |  | X | X |  |  |  |  | X |  |  |  |  |  |  |  |
| 16 |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |
| 17 |  |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| 18 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 19 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 20 |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |
| 21 |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |
| 22 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| 23 |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |

## 6.1 Solution #1: Solution for key management in 5G Proximity Services relay communication

### 6.1.1 Introduction

This solution describes how the existing network function Authentication Server Function performs the key management instead of PKMF (ProSe Key Management Function) as done in TS 33.303 [6] in LTE ProSe. This solution addresses key issue #9.

### 6.1.2 Solution details

In this solution it is assumed that the 5GDDNMF is a functionality of PCF and not a separate entity. Proposed solution reuses the PCF discovery procedure as defined in 23.502[10] for provisioning or configuration of the relay discovery material and the required security material.



Figure 6.1.2-1: Procedural call flow for key management in 5G ProSe

Step 0a-0e: The remote UE seeking access via UE-to-Network relay, REAR (Remote Access via Relay) sends a UE policy provisioning request to the AMF. The request may include the Remote UE capability i.e., ProSe UE capability, PC5 capability.

AMF sends N5gddnmf\_UEpolicycontrol\_update or Npcf\_UEpolicycontrol\_update request over Service based interface to discover the corresponding PCF or 5GDDNMF and requests for the policy required for ProSe UE Discovery and security material.

5GDDNMF or PCF responds back with Npcf\_GetDiscovery\_info response message with ProSe relay UE discovery and security material to 5GDDNMF. The 5GDDNMF sends back N5gddnmf\_UEpolicycontrol\_update response with the required ProSe relay discovery and security material. AMF delivers the ProSe relay discovery and security material to the Remote UE.

The UE-to-Network relay gets authenticated and authorized by the network to support as a relay for ProSe communication. Editor's Note: Whether the security keys can be provided in step 0d is FFS.

Editor's Note: The definition of 5GDDNMF shouldbe aligned with SA2.

Step 1: The Remote UE sends a key request message to the AMF, where the message includes the ProSe Remote access indication and 5G-GUTI if already assigned or the SUCI. This solution based on single hop relay i.e., one UE-to-Network relay between Remote UE and the core network. The proposed solution also works for multiple hop relay communication.

The ProSe Remote access indication is set to 1, which indicates that there is only single hop UE-to-Network relay in between.

The AMF forwards the Key request to the AUSF instance which is capable of authentication, authorization and key derivation for the ProSe UE-to-Network relay communication.

Step 2: In order to authorize the UE requesting for keys for remote access, the AUSF sends Nudm\_UEAuthentication request to UDM and retrieves the UE details or subscription data. In this message the AUSF includes ProSe Remote access indication and 5G-GUTI or SUCI.

Step 3: On receiving the Nudm\_UEAuthentication request, the UDM verifies the 5G-GUTI or SUCI and sends the corresponding SUPI to the AUSF in Nudm\_UEAuthentication response message.

Step 4: On receiving the SUPI from UDM, the AUSF generates the REAR Key for Remote UE communication via UE-to-Network relay. REAR key will be used for deriving the ProSe key KNR\_ProSe.

Input to the Key Derivation Function for deriving the REAR key is as follows:

REAR Key = KDF (Latest KAUSF, SUPI of the Remote UE, Relay UE ID bound to SUPI of relay/TempID of relay, other possible parameters)

The generated key is 256 bits in which, the 128 bits MSB of key is the REAR Key and the other 128 bits is the REAR Key ID. The purpose of REAR Key ID is to identify the REAR key.

Editor's Note: The input parameters to derive the keys are FFS.

Step 5: AUSF sends the generated REAR key and Relay UE ID/TempID of Relay which is bound to UE-to-Network relays SUPI in the key response message to the Remote UE.

Step 6: Remote UE discovers the relay UE using any of Model A or Model B method. The discovery message must include the relay UE ID provided by the AUSF.

Step 7: After the discovery of the UE-to-Network relay, the Remote UE sends the Direct communication request to the discovered relay for establishing secure PC5 unicast link. The message should include Relay Service Code or ServiceID, 5G-GUTI of the Remote UE and Message Authentication Code MACREAR.

Step 8: On receiving the Direct Communication request, the UE-to-Network relay sends a key request message Relay Service Code or ServiceID, 5G-GUTI of the Remote UE and Message Authentication Code MACREAR received from the remote UE.

Step 9: AUSF authorizes the remote UE requesting for remote access by checking the MACREAR using the REAR key, and 5G-GUTI.

Step 10: After authorization the AUSF generates the ProSe key to be used for Remote access via Relay.

The input to the KDF for generating ProSe key is as follows:

KNR\_ProSe = KDF (REAR key, 5G-GUTI, Relay Service Code or ServiceID, KNR\_ProSe freshness parameter, other possible parameters). KNR\_ProSe freshness parameter can be any nonce or counter or random number.

Editor's Note: The purpose of KNR\_ProSe is FFS.

Step 11: AUSF sends the KNR\_ProSe freshness parameter in the key response message to the UE-to-Network relay.

Step 12: The UE-to-Network relay sends the received KNR\_ProSe freshness parameter to the Remote UE in Direct Security mode command message.

Step 13: The remote UE generates the ProSe key to be used for Remote access via Relay same as defined in step 10.

Step 14: Remote UE sends the Direct Security mode complete message to the UE-to-Network relay. Further communication between Remote UE and Network takes place securely via the UE-to-Network relay.

Editor's Note: This solution assumes and require network connectivity for both remote UE and relay UE.

Editor's Note: This solution may impact more than one key issue.

### 6.1.3 Evaluation

TBD

## 6.2 Solution #2: Secure data transfer between UE and 5GDDNMF

### 6.2.1 Introduction

This solution addresses key issue#10.

### 6.2.2 Solution details

In LTE ProSe, the protection of traffic between UE and ProSe Function is as specified in clause 5.3.3.2 in TS 33.303 [6]. For 5G ProSe the security can be established using Authentication and Key Management for Applications. Where AF is the ProSe Application Function (5GDDNMF) and AF should be authenticated and authorized by the operator network before providing the AKMA Application Key (KAF) to the AF.

Editor's Note: Whether 5GDDNMF is a functionality of PCF or an AF is based on conclusion from SA2.

It is proposed to use the AKMA network model and security procedure to have a secure data transfer between UE and the 5GDDNMF.



Figure 6.2.2-1: User plane architecture

Figure 6.2.2-1 is reference model for AKMA modified for supporting Proximity based services. The Application function in AKMA is 5GDDNMF in ProSe having a service-based interface N5gddnmf with other Network Functions, to consume or provide services from or to other NFs.

Editor's Note: Whether AKMA user plane architecture is used shall be based on conclusion from SA2.

The PC3 interface between UE and 5GDDNMF is considered as Ua\* interface and depends on Ua\* protocol.

However, the security requirement of PC3 interface should be aligned to satisfy the Ua\* interface. Also, the interface Ua\* needs to have new functionalities in addition to specified in clause 4.4.1 of TS 33.535 [7] for Ua\*.

Editor’s note: The need of new functionalities is FFS and whether the new functionalities can be used in Ua\* is FFS.

Editor’s note: The impact on Ua\* interface and PC3 interface are FFS.

### 6.2.3 Evaluation

TBD

## 6.3 Solution #3: Reuse LTE security mechanism for 5G ProSe open discovery

### 6.3.1 Introduction

This solution addresses Key Issue #1(Discovery message protection). It proposes to reuse the open discovery security mechanism specified in TS 33.303 [6] for 5G ProSe open discovery. This solution does not address UE-to-Network and UE-to-UE relay discovery.

In LTE ProSe, the ProSe function is used to provide the UE with the necessary security material in order to protect discovery messages transmitted over the air. In 5G ProSe, the 5G Direct Discovery Name Management Function (DDNMF) is used to replace the ProSe function in the open discovery.

This solution allows the discovery key to be provided to the DDNMF in the HPLMN of the monitoring UE and the monitoring UE in order to support out of coverage scenario and more security flexibility.

Editor’s note: It’s FFS about new security parameters for 5G that is different from LTE ProSe.

Editor’s note: The detailed security-related parameters in the announcing message are FFS.

Editor’s note: It’s FFS how to support the security flexibility.

### 6.3.2 Solution details

This solution does not address the discovery key generation and key delivery protocol used in the discovery procedure, which is up to the conclusion of key issue #2.

The open discovery security procedure is described as follows:

1. The announcing UE sends a Discovery Request message containing the ProSe Application ID to the DDNMF in its HPLMN in order to be allowed to announce a code on its serving PLMN (either VPLMN or HPLMN).
2. If the announcing UE wants to send announcements in the VPLMN, the DDNMF in the HPLMN requests authorization from the VPLMN DDNMF by sending Announce Auth.() message.
3. VPLMN DDNMF responds with an Announce Auth. Ack () message.
4. The DDNMF in HPLMN of the announcing UE returns the ProSe App Code that the announcing UE can announce and a Discovery Key associated with it. The DDNMF stores the Discovery Key with the ProSe App Code. In addition, the DDNMF provides the UE with a CURRENT\_TIME parameter, which contains the current UTC-based time at the DDNMF, a MAX\_OFFSET parameter, and a Validity Timer. The UE sets a clock which is used for ProSe authentication (i.e. ProSe clock) to the value of CURRENT\_TIME and the UE stores the MAX\_OFFSET parameter, overwriting any previous values. The announcing UE obtains a value for a UTC-based counter associated with a discovery slot based on UTC time. The counter is set to a value of UTC time in a granularity of seconds. The UE may obtain UTC time from any sources available, e.g. the RAN via SIB16, NITZ, NTP, GPS, via Ub interface (in GBA) (depending on which is available).
5. The UE starts announcing, if the difference between UTC-based counter provided by the system associated with the discovery slot and the UE’s ProSe clock is not greater than the MAX\_OFFSET and if the Validity Timer has not expired. For each discovery slot it uses to announce, the announcing UE calculates a 32-bit Message Integrity Check (MIC) to include with the ProSe App Code in the discovery message. Four least significant bits of UTC-based counter are transmitted along with the discovery message. The MIC is calculated as described in clause A.2 of TS 33.303 [6] using the Discovery Key and the UTC-based counter associated with the discovery slot.
6. The Monitoring UE sends a Discovery Request message containing the ProSe Application ID to the DDNMF in its HPLMN in order to get the Discovery Filters that it wants to listen for.
7. The DDNMF in the HPLMN of the monitoring UE sends Monitor Req. message to the DDNMF in the HPLMN of the announcing.
8. The DDNMF in the HPLMN of the announcing UE sends Monitor Resp. message to the DDNMF in the HPLMN of the monitoring. If MIC needs to be checked by the DDNMF in the HPLMN of the monitoring UE or the monitoring UE, the Discovery Key should be contained in the response message.
9. The DDNMF returns the Discovery Filter containing either the ProSe App Code(s), the ProSe App Mask(s) or both along with the CURRENT\_TIME and the MAX\_OFFSET parameters. The UE sets its ProSe clock to CURRENT\_TIME and stores the MAX\_OFFSET parameter, overwriting any previous values. The monitoring UE obtains a value for a UTC-based counter associated with a discovery slot based on UTC time. The counter is set to a value of UTC time in a granularity of seconds. The UE may obtain UTC time from any sources available, e.g. the RAN via SIB16, NITZ, NTP, GPS (depending on which is available). If MIC needs to be checked by the monitoring UE, the Discovery Key should be contained in the response message.
10. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter, if the difference between UTC-based counter associated with that discovery slot and UE’s ProSe clock is not greater than the MAX\_OFFSET of the monitoring UE's ProSe clock. If the monitoring UE has the Discovery Key, the MIC check is performed locally, and steps 11 to 15 are omitted.
11. On hearing such a discovery message, and if the UE needs to check the MIC for the discovered ProSe App Code, the Monitoring UE sends a Match Report message to the DDNMF in the HPLMN of the monitoring UE. The Match Report contains the UTC-based counter value with four least significant bits equal to four least significant bits received along with discovery message and nearest to the monitoring UE’s UTC-based counter associated with the discovery slot where it heard the announcement, and other discovery message parameters including the ProSe App Code and MIC. If the DDNMF in the HPLMN of the monitoring UE has the Discovery Key, the MIC check is performed locally, and steps 12 to 14 are omitted.
12. The DDNMF in the HPLMN of the monitoring UE passes the discovery message parameters including the ProSe App Code and MIC and associated counter parameter to the DDNMF in the HPLMN of the announcing UE in the Match Report message.
13. The DDNMF in the HPLMN of the announcing UE should check the MIC is valid.
14. The DDNMF in the HPLMN of the announcing UE should acknowledge a successful check of the MIC to the DDNMF in the HPLMN of the monitoring UE in the Match Report Ack message.
15. The DDNMF in the HPLMN of the monitoring UE acknowledges the check result to the monitoring UE.



Figure 6.3.2-1: Open discovery security procedure

### 6.3.3 Evaluation

TBD

## 6.4 Solution #4: Reuse LTE security mechanism for 5G ProSe restricted discovery

### 6.4.1 Introduction

This solution addresses Key Issue #1(Discovery message protection). It proposes to reuse the restricted discovery security mechanisms of Model A and Model B specified in TS 33.303 [6] for 5G ProSe restricted discovery.

In LTE ProSe, the ProSe function is used to provide the UE with the necessary security material in order to protect discovery messages transmitted over the air. In 5G ProSe, the 5G Direct Discovery Name Management Function (DDNMF) is used to replace the ProSe function in the restricted discovery.

Editor’s note: It’s FFS about new security parameters for 5G that is different from LTE ProSe.

Editor’s note: The detailed security-related parameters in the announcing message are FFS.

Editor’s note: It’s FFS how to support the security flexibility.

### 6.4.2 Solution details

#### 6.4.2.1 Model A restricted discovery

This solution does not address the discovery key generation and key delivery protocol used in the discovery procedure, which is up to the conclusion of key issue #2.

The security procedure for Model A restricted discovery is described as follows:

Steps 1-4 refer to an Announcing UE.

1. Announcing UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to get the ProSe Code to announce and to get the associated security material.
2. The DDNMF may check for the announce authorization with the ProSe Application Server.
3. If the Announcing UE is roaming, the DDNMFs in the HPLMN and VPLMN of the Announcing UE exchange Announce Auth.
4. The DDNMF in the HPLMN of the Announcing UE returns the ProSe Code and the corresponding Code-Sending Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters.

Steps 5-10 refer to a Monitoring UE

1. The Monitoring UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to be allowed to monitor for one or more Restricted ProSe Application IDs.
2. The DDNMF in the HPLMN of the Monitoring UE sends an authorization request to the ProSe Application Server. If, based on the permission settings, the RPAUID is allowed to discover at least one of the Target RPAUIDs contained in the Application Level Container, the ProSe Application Server returns an authorization response.
3. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates a different PLMN, the DDNMF in the HPLMN of the Monitoring UE contacts the indicated PLMN’s DDNMF i.e. the DDNMF in the HPLMN of the Announcing UE, by sending a Monitor Request message.
4. The DDNMF in the HPLMN of the Monitoring UE may exchange authorization messages with the ProSe Application Server.
5. The DDNMF in the HPLMN of the Announcing UE responds to the DDNMF in the HPLMN of the Monitoring UE with a Monitor Response message including the ProSe Code, the corresponding Code-Receiving Security Parameters and an optional Discovery User Integrity Key (DUIK).
6. The DDNMF in the HPLMN of the Monitoring UE returns the Discovery Filter and the Code-Receiving Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters.

Steps 11 and 12 occur over PC5.

1. The UE starts announcing.
2. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter. If the Monitoring UE was asked to send Match Reports for MIC checking, it proceeds to step 13.

Steps 13-16 refer to a Monitoring UE that has encountered a match.

1. The Monitoring UE sends a Match Report message to the DDNMF in the HPLMN of the monitoring UE.
2. The DDNMF in the HPLMN of the Monitoring UE may exchange an Auth Req/Auth Resp with the ProSe App Server to ensure that Monitoring UE is authorised to discover the Announcing UE.
3. The DDNMF in the HPLMN of the monitoring UE returns to the Monitoring UE an acknowledgement that the integrity check passed.
4. The DDNMF in the HPLMN of the Monitoring UE may send a Match Report Info message to the DDNMF in the HPLMN of the Announcing UE.



Figure 6.4.2.1-1: Model A restricted discovery security procedure

#### 6.4.2.2 Model B restricted discovery

This solution does not address the discovery key generation and key delivery protocol used in the discovery procedure, which is up to the conclusion of key issue #2.

The security procedure for Model B restricted discovery is described as follows:

Steps 1-4 refer to a Discoveree UE.

1. Discoveree UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to get the ProSe Code to announce and associated security material.
2. The DDNMF may check for the announce authorization with the ProSe Application Server depending on DDNMF configuration.
3. The DDNMFs in the HPLMN and VPLMN of the Discoveree UE exchange Announce Auth. messages. If the Discoveree UE is not roaming, these steps do not take place.
4. The DDNMF in the HPLMN of the Discoveree UE returns the ProSe Response Code and the Code-Sending Security Parameters, Discovery Query Filter(s) and their Code-Receiving Security Parameters corresponding to each discovery filter along with the CURRENT\_TIME and MAX\_OFFSET parameters.

Steps 5-10 refer to a Discoverer UE

1. The Discoverer UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to be allowed to discover one or more Restricted ProSe Application IDs.
2. The DDNMF in the HPLMN of the Discoverer UE sends an authorization request to the ProSe Application Server. If the RPAUID is allowed to discover at least one of the Target RPAUIDs contained in the Application Level Container, the ProSe Application Server returns an authorization response.
3. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates a different PLMN, the DDNMF in the HPLMN of the Discoverer UE contacts the indicated PLMN’s DDNMF i.e. the DDNMF in the HPLMN of the Discoveree UE, by sending a Discovery Request message.
4. The DDNMF in the HPLMN of the Discoveree UE may exchange authorization messages with the ProSe Application Server.
5. The DDNMF in the HPLMN of the Discoveree UE responds to the DDNMF in the HPLMN of the Discoverer UE with a Discovery Response message including the ProSe Query Code(s) and their associated Code-Sending Security Parameters, ProSe Response Code and its associated Code-Receiving Security Parameters, and an optional Discovery User Integrity Key (DUIK) for the ProSe Response Code.
6. The DDNMFs in the HPLMN and VPLMN of the Discoverer UE exchange Announce Auth. messages. If the Discoverer UE is not roaming, these steps do not take place.
7. The DDNMF in the HPLMN of the Discoverer UE returns the Discovery Response Filter and the Code-Receiving Security Parameters, the ProSe Query Code and the Code-Sending Security Parameters along with the CURRENT\_TIME and MAX\_OFFSET parameters.

Steps 12 to 15 occur over PC5.

1. The Discoverer UE sends the ProSe Query Code and also listens for a response message.
2. The Discoveree UE listens for a discovery message that satisfies its Discovery Filter.
3. The Discoveree sends the ProSe Response Code associated with the discovered ProSe Query Code.
4. The Discoverer UE listens for a discovery message that satisfies its Discovery Filter.

Steps 16-19 refer to a Discoverer UE that has encountered a match.

1. The Discoverer UE sends a Match Report message to the DDNMF in the HPLMN of the Discoverer UE.
2. The DDNMF in the HPLMN of the Discoverer UE may exchange an Auth Req/Auth Resp with the ProSe App Server to ensure that Discoverer UE is authorised to discover the Discoveree UE.
3. The DDNMF in the HPLMN of the Discoverer UE returns to the Discoverer UE an acknowledgement that the integrity check passed.
4. The DDNMF in the HPLMN of the Discoverer UE may send a Match Report Info message to the DDNMF in the HPLMN of the Discoveree UE.



Figure 6.4.2.2-1: Model B restricted discovery security procedure

### 6.4.3 Evaluation

TBD

## 6.5 Solution #5: Protection of the PC3 interface using AKMA and TLS

### 6.5.1 Introduction

This solution describes how AF in AKMA TS 33.535 [7] can be used to generate the key to be used to protect the PC3 interface between the UE and the 5GDNNMF. This solution addresses key issue #10.

This solution can also be used with other AF’s used for ProSe services which are accessed in the user plane.

### 6.5.2 Solution details

This solution assumes that 5GDDNMF is a separate entity and not a functionality of the PCF. This solution assumes that the 5GDDNMF takes the role as the AF in AKMA and uses AKMA procedures as defined in TS 33.535 [7] to generate a symmetric key in the UE and the AF.

This solution proposes to use TLS 1.3 with PSK authentication as described in RFC 8446 [11].

The signaling flow in clause 6.5.2-1 describes the establishment of TLS 1.3 with PSK authentication.

There is no separate authentication of the UE to support AKMA functionality. Instead, it reuses the 5G primary authentication procedure executed e.g. during the UE Registration to authenticate the UE. A successful 5G primary authentication results in KAUSF being stored at the AUSF and the UE.

The AUSF generates KAKMA from KAUSF and generates a A-KID which is mapped to the new generated KAKMA and pushes the KAKMA and A-KID to the AAnF.



Figure 6.5.2-1: Procedure for security protection of the PC3 interface between the AF (e.g. 5GDDNMF) and the UE

Step 1) The UE mutually authenticates with and registers in the 5GC. As part of the UE authentication with the 5GC, the UE and the AUSF store a KAUSF. Additionally, the UE and the AUSF generate AKMA Key material (i.e. KAKMA and A-KID) and the AUSF sends this material to the AAnF as specified in the AKMA TS 33.535 [7]. The UDM will indicate whether the UE is allowed to use AKMA services. The PCF (or some other network function) provides the AF address (e.g 5GDNNMF address) to the UE and the UE establish PDU session with the network.

Step 2a) The UE initiates TLS 1.3 with PSK authentication with the AF server as described in RFC 8446 [11. The UE sends Client Hello where the ClientHello contains a pre\_shared\_key extension containg a PSK identity formatted from A-KID and 3GPP-akma hint together with a psk\_key\_exchange\_modes extension indicating e.g. psk\_dhe\_ke.

The following steps in 2 b)-c) are part of AKMA procedures defined in TS 33.535 [7].

Step 2b) The AF server contacts the AAnF with the A-KID.

Step 2c) The AAnF looks up the KAKMA key using the A-KID and generates a KAF key from the KAKMA key.

Step 2d) The AAnF server responds with the KAF key and the expiration time for the KAF key to the AF.

Step 2e) The AF server responds with a Server Hello with a pre\_shared\_key extension indicating the chosen PSK identity.

Step 2f) The UE generates KAF from KAKMA.

Step 2g) The UE responds with a Finished message.

Step 3 The UE and the AF server can exchange application data over a secured link.

### 6.5.3 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 user plane architecture is adopted by SA2 is FFS.

Editor’s Note: 3GPP TS 33.303 specifies the use of GBA to protect PC3 interface. The benefits to define additional solution to secure PC3 when GBA is already specified are FFS.

## 6.6 Solution #6: Key management for UE-to-Network Relays and Remote UE’s

### 6.6.1 Introduction

This solution describes how an AF in the user plane provisions security keys to the Remote UE and the UE-to-network relay, to be used for PC5 communication over PC5 interface between a Remote UE and a UE-to-NW Relay. This solution addresses key issue#4.

The AF could be a new key management function for example similar to the PKMF (ProSe Key Management Function) defined for in TS 33.303 [6] which is accessed in the user plane.

Editor’s note: This solution works when the UE is in 3GPP coverage. The use case when the Remote UE is out of coverage is FFS.

### 6.6.2 Solution details

The Remote UE needs to retrieve the address to the AF(s) from the network when it wants to act as a Remote UE.



Figure 6.6.2-1: Procedures for key management in ProSe UE-to-Network Relay

Step 1) The Remote UE gets authenticated and authorized by the network to act as a Remote UE. The Remote UE mutually authenticates with and registers in the 5GC. The network (e.g. PCF) provides the AF address to the Remote UE for the AF used for key management for PC5 communication in ProSe UE-to-Network Relay. The Remote AF could be e.g. a 5GDDNMF function or a new key management function similar to the PKMF (ProSe Key Management Function) defined for public safety in TS 33.303 [6]. The Remote UE establish a PDU session with the network.

Step 2) The Remote UE retrievs a discovery key for discovery of a UE-to-network relay from the network. The Remote UE sends a Key request message for discovery of a UE-to-network relay. The AF provides a Relay Discovery key together with a Relay Discovery key ID in the Key response message to the Remote UE.

These steps may take place together with steps 4 and 5.

Step 3) The Remote UE establishes a secure connection with the AF server.

Step 4) The Remote UE sends a Key request message for PC5 communication with a UE-to-network relay to the AF.

Editor’s note: The parameters included in the Key request message by the Remote UE to the AF are FFS.

Step 5) The AF generates a PC5 communication key and provides the PC5 communication key and a PC5 communication key ID in the Key response message to the Remote UE to be used for PC5 communication with a UE-to-network relay. The AF could generate the PC5 communication key from the AKMA key KAF.

Editor’s note: The parameters included from the AF to the Remote UE are FFS.

Editor’s note: It’s FFS whether the PC5 communication key can be generated from the AKMA key KAF.

Step 6) The UE-to-network relay gets authenticated and authorized by the network to act as a UE-to-network relay.

Step 7) The UE-to-network relay retrievs a discovery key for UE-to-network relay discovery from the network. The UE-to-network relay sends a Key request message and the network provides a Relay Discovery key together with a Relay Discovery key ID in the Key response message to the UE-to-network relay.

Editor’s note: For step 6) and step 7), if UE-to-network relay and the Remote UE support the same application they will connect to the same AF.  Different relays do not need to be connected to the same AF, it depends on the application. This needs to be further clarified in the solution. Also, it needs to be clarified how all the potential relay candidates get authorized.

Step 8) UE-to-network relay discovery is taken place on PC5 interface using either model A or model B discovery.

Step 9) When the The Remote UE and the UE-to-network relay discovery have discovered each other, the Remote UE sends a Direct Communication Request on PC5 interface. The Remote UE includes the PC5 communication key ID received from the AF together with a Relay Service Code. The PC5 communication key ID indicates the PC5 communication key which the Remote UE want to use to get relay connectivity. The Direct Communication Request contains the Relay Service Code that the Remote UE would like to access. The Remote UE generates a freshness parameter Nonce-1. The Remote UE calculates a message authentication code (MAC-PC5comm) over the included ProSe parameters using the PC5 communication key and the Nonce-1 and includes the message authentication code (MAC-PC5comm) in the Direct Communication Request.

Editor’s note: The parameters included in Direct Communication Request from Remote UE to UE-to-network relay are FFS.

Step 10) The Remote UE establishes a secure connection with the AF server.

Step 11) The UE-to-network relay sends a Key request message for PC5 communication with a Remote UE to the AF.

Editor’s note: The parameters included from UE-to-network relay to AF are FFS.

Step 12) The AF authenticates and authorize the Remote UE by verifying the message authentication code (MAC-PC5comm) using the PC5 communication key identified by the PC5 communication key ID and the Nonce-1. The AF checks the context of the Remote UE to confirm whether it can connect to the network via the selected ProSe UE-to-network Relay for the given Relay Service Code.

Step 13) If the AF confirms the Remote UE can connect to the network via the selected ProSe UE-to- network Relay, the AF generates a new freshness parameter (i.e. K-COMM freshness parameter). The AF generates a new key K-COMM from at least the PC5 communication key, Relay Service Code and a new freshness parameter (i.e. K-COMM freshness parameter).

Editor’s note: The generation of the K-COMM key is FFS.

Step 14) The AF sends the K-COMM key and the freshness parameter (K-COMM freshness) to the UE-to-network relay in the Key response message.

Editor’s note: The parameters included from AF to UE-to-network relay in the Key response message are FFS.

Step 15) Using the supplied K-COMM to protect the Direct Security Mode Command message, the UE-to-network relay sends a Direct Security Mode Command message to the Remote UE. This message contains the K-COMM freshness. The UE-to-network relay generates a Nonce-2 and calculates a MAC-COMM over the included ProSe parameters using the K-COMM key and includes the MAC-COMM and Nonce-2 in the Direct Security Mode Command message.

Editor’s note: The parameters included from the UE-to-network relay to the Remote UE are FFS.

Step 16) The Remote UE derives K-COMM key in the same way as the AF in step 13.

Editor’s note: The generation of the K-COMM key is FFS.

Step 17-18) The Remote UE processes the Direct Security Mode Command by verifying the MAC-COMM using the generated K-COMM key and the Nonce-2. If this verification is successful, the Remote UE responds with a Direct Security Mode Complete message and the Remote UE and UE-to-network relay can start to exchange user data.

## 6.7 Solution #7: Security establishment of one-to-one PC5 communication

### 6.7.1 Solution overview

This solution addresses the Key Issue #12: Security of one-to-one communication over PC5.

The initiating UE initiates the one-to-one communication establishment procedures to the receiving UE and the security-related information (e.g. security protection methods, security algorithms, keys if applicable, etc) are confirmed or created during the one-to-one communication establishment procedures.

The one-to-one communication establishment starts with a Direct Communication Request (DCR) message to send the initiating UE’s security capabilities and to trigger the mutual authentication. In order to perform the Direct Communication Request, the ProSe one-to-one communication may happen after discovery procedures, or after one-to-many ProSe communications. After DCR and mutual authentication, the Direct Security Mode Command and the Direct Security Mode Complete messages are emitted to inform the selected security protection algorithms for the connection and the initiating UE’s user plane security policies (i.e. user plane confidentiality and integrity protection policies), respectively. Finally, the receiving UE replies a Direct Communication Accept (DCA) message to confirm the user plane protection methods and finish the one-to-one communication establishment procedures.

### 6.7.2 Solution details

Initiating UE

Receiving UE

2. Direct Communication Request ( Initiating UE's security capabilities )

3. Direct Auth and Key Establishment

4. Direct Security Mode Command( Chosen\_algs, Initiating UE's security capabilities )

5. Direct Security Mode Complete (Initiating UE's user plane security policies)

1. Discovery Procedures, or One-to-Many Communication

6. Direct Communication Accept ( User plane security indication )

0. ProSe Parameter pre-configuration and previsioning

Figure 6.7.2-1 Procedures for one-to-one communication security establishment over PC5

0. ProSe security-related parameter (for one-to-one secure communication over PC5) pre-configuration and previsioning, the signalling integrity protection should be used and the signalling ciphering protection is a configuration option.

1. Discovery procedures or after one-to-many ProSe communications for getting initial parameters (e.g. L2 IDs).

2. The initiating UE starts Direct Communication Request (DCR) message contains and the initiating UE’s security capabilities. The initiating UE’s security capabilities are the confidentiality and integrity protection algorithms that the initiating UE accepts for this connection.

3. The receiving UE may initiate the Direct authentication and key establishment procedures with the initiating UE.

4. The receiving UE uses the Chosen\_algs to indicate the selected confidentiality and integrity protection algorithms of this link and contains the Chosen\_algs in the Direct Security Mode Command message. The initiating UE’s security capabilities are sent back to the initiating UE to mitigate the bidding down attack. The receiving UE should integrity protect the Direct Security Mode Command message before sending it to the initiating UE.

5. The initiating UE sends its user plane security policies to the receiving UE by using Direct Security Mode Complete message.

6. The receiving replies the Direct Communication Accept message to accept the DCR message and one-to-one communication establishment including the user plane security indication. The user plane security protection methods (the user plane confidentiality protection activated or not, and the user plane integrity protection activated or not) are explicitly indicated by using user plane security indication.

NOTE: The privacy protection of entities is not addressed in this solution.

### 6.7.3 Evaluation

The Solution #7 addresses the security requirements of key issue #12. The mutual authentication between two UEs during one-to-one communication is supported in step 3. MitM attacks during link establishment and bidding-down attacks are mitigated by mandatory activation of the signalling integrity protection. The system supports providing the signalling and user plane security policies to UEs for a particular PC5 one-to-one communication in step 0. According to the step 0 and 5, PC5 signalling and user plane confidentiality protection, integrity protection and anti-replay protection are assumed to be supported by the system as they can be negotiated or pre-configured to be activated.

The privacy protection is not addressed in this solution.

Editor’s Note: Futher evaluation is FFS.

## 6.8 Solution #8: Confidential protection against UE-to-UE relay using asymmetric cryptography

### 6.8.1 Introduction

This solution is targeting to address key issue#6, which is proposing that the communication via the UE-to-UE Relay between source UE and target UE should be confidentially and integrity protected. This solution proposes a method to protect the communication between source UE and target UE using asymmetric cryptography. To be more specific, the Source UE and Target UE use their public key and private key to confidentially protect the communication.

The authentication between source UE and target UE is not included in this solution.

### 6.8.2 Solution details

#### 6.8.2.1 Procedure

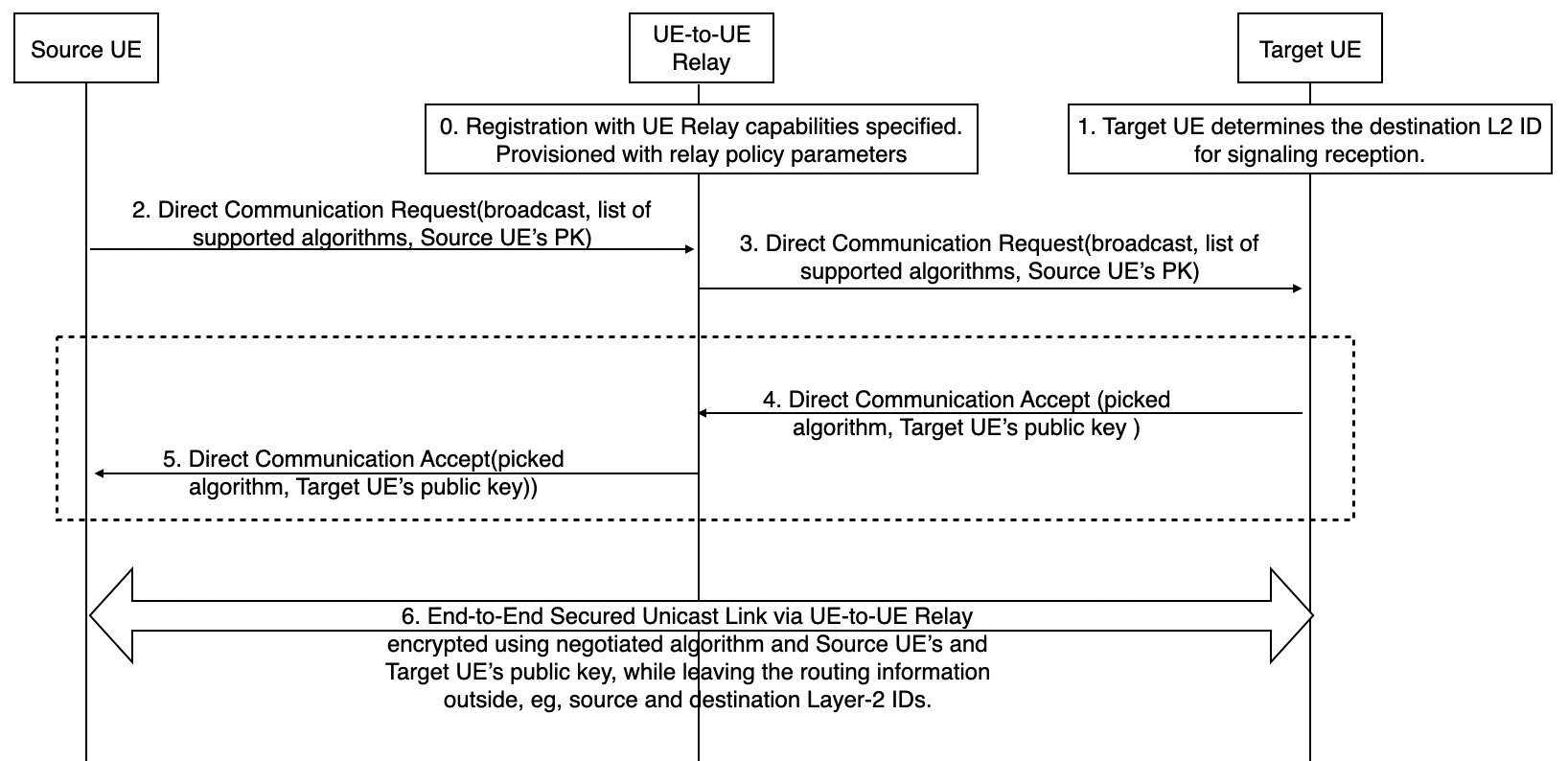


Figure 6.8.2.1-1: Security protection via UE-to-UE Relay using asymmetric cryptography

The connection establishment procedure is based on TR 23.752 [2], Clause 6.9. However, the security procedure below is not limited to one connection establishment procedure defined in TR 23.752 [2].

The security procedure details are as following:

0. UE-to-UE Relay registers with the network and specifies its UE-to-UE Relay capabilities. UE-to-UE Relay is provisioned from the network with relay policy parameters and with a unique Relay identifier (RID). The assumption in this solution is source UE and target UE are presumed already authenticated.

1. The target UE determines the destination Layer-2 ID for signalling reception for PC5 unicast link establishment as specified in TS 23.287 [9] clause 5.6.1.4. The destination Layer-2 ID is configured with the target UEs as specified in TS 23.287 [9] clause 5.1.2.1.

2. On the source UE, the application layer provides information to the ProSe layer for PC5 unicast communication (e.g. broadcast Layer-2 ID, ProSe Application ID, UE's Application Layer ID, target UE's Application Layer ID, relay applicable indication), as specified in TS 23.287 [9] clause 6.3.3.1. ProSe layer triggers the peer UE discovery mechanism by sending a broadcast Direct Communication Request message. The message is sent using the source Layer-2 ID and broadcast Layer-2 ID as destination, and includes other parameters related to the application offered. Source UE should also include 2 IEs, which are list of source UE’s supported algorithms and the source UE’s public key.

3. The UE-to-UE Relay receives the broadcast Direct Communication Request message and verifies if it's configured to relay this application, i.e. it compares the announce ProSe Application ID with its provisioned relay policy/parameters and, if it matches, the UE-to-UE Relay assigns itself a Relay-Layer-2 ID (e.g. R-L2 ID-a) for source UE (i.e. related to source UE 's L2 ID).The UE-to-UE Relay proceeds in forwarding the broadcast Direct Communication Request message, which includes list of source UE’s supported algorithms and the source UE’s public key, received from the source UE.

4.Target UE is interested in the announced application thus, target UE will check whether it could support the security algorithms in the list of source UE’s supported algorithms, if yes, then it sends the Direct Communication Accept message to source UE, including the chosen algorithm, and also target UE’s public key.

5. UE-to-UE Relay forwarded the Direct Communication Accept message to source UE.

6. An "extended" unicast link is established between source UE and target UE, via the UE-to-UE Relay. The extended link is secured end to end using source UE’s and target UE’s public key, while the routing information will be left in the clear.

Editor’s Note: it is FFS how to bind the public key with a specific UE and how to revoke public keys.

Editor’s Note: it is FFS whether and (if yes, then)how to protect the privacy of the routing information.

Editor’s Note: it is FFS on how to make sure the DCA message can be trusted.

Editor’s Note: public/private keys provisioning into the peer UEs is FFS

Editor’s Note: The solution is under the assumption that only a single (ProSe) application is supported.

### 6.8.3 Evaluation

TBD.

## 6.9 Solution #9: Key management in discovery procedure

### 6.9.1 Solution overview

This solution addresses the key issue #2: Keys in ProSe discovery scenario.

This solution proposes to generate discovery root key from AUSF and the 5G DDNMF derives the discovery keys. At the UE side, UE generates both discovery root key and discovery keysl.

### 6.9.2 Solution details

In control plane architecture as illustrated in clause 4.1.1, a UE reaches the 5G DDNMF via AMF. The 5G DDNMF allocates the Prose APP code and gets the discovery root key from AUSF. The AUSF will generate the discovery root key based on the KAUSF. The 5G DDNMF will further generate discovery IK based on the discovery root key for open discovery and will further generate discovery IK and discovery CK for restricted discovery. The 5G DDNMF will send the key material to the UE via AMF. On UE side, the UE will generate the same keys as the network side based on the key material sent from the 5G DDNMF. The 5G DDNMF and AMF will relay on the security of SBI.

NOTE: the detail of SBI used between 5G DDNMF and AMF is not introduced in this solution.

In user plane architecture as illustrated in clause 4.1.2, a UE reaches the 5G DDNMF via user plane. The 5G DDNMF allocates the Prose APP code and gets the discovery root key from AAnF. The AAnF will generate the discovery root key based on the KAKMA as described in TS 33.535[7]. The 5G DDNMF will further generate discovery IK based on the discovery root key for open discovery and will further generate discovery IK and discovery CK for restricted discovery. The 5G DDNMF will send the key material to the UE via Ua\* protocol. On UE side, the UE will generate the same keys as the network side based on the key material sent from the 5G DDNMF

Editor’s Note: The details of key derivation for both CP and UP solutions are FFS.

### 6.9.3 Evaluation

This solution does not specifiy the protocol used between UE and 5G DDNMF.

## 6.10 Solution #10: Authorization and security with UE-to-Network relay using Remote UE network primary authentication

### 6.10.1 Solution overview

The contribution proposes a solution to address the following Key Issues:

- KI #3: Security of UE-to-Network Relay

- KI #4: Authorization in the UE-to-Network relay scenario

- KI #9: Key management in 5G Proximity Services for UE-to-Network relay communication

This solution builds on top of common high-level principles from existing solution #46 and solution #47 specified in TR 23.752 [2]. These solutions address Remote UE and UE-to-Network authorization aspects in the case of L3 relay. This solution leverages a Remote UE primary authentication run to establish keys used to secure the PC5 link between the Remote UE and the UE-to-Network relay.

This solution assumes that the Remote UE selects a relay based on the connectivity service (e.g., S-NSSAI, DNN) that the relay can provide. The Remote UE learns about the connectivity service as part of the discovery procedure. It is assumed that the relay's Allowed NSSAI includes the S-NSSAIs needed to provide the connectivity service. The UE-to-Network relay either has a PDU session or is able to establish a new one without having to request a S-NSSAI (same assumption as solution #6 in TR 23.752 [2]). Therefore, in the context of the connectivity service provided by the relay, the AMF serving the relay is always able to serve the Remote UE.

### 6.10.2 Solution details

The procedure for Authorization and security with UE-to-Network relay using Remote UE network primary authentication is depicted in Figure 6.10.2-1.



Figure 6.10.2-1: Procedure for Authorization and security with UE-to-Network relay using Remote UE network primary authentication

0. The Relay UE is registered and authorized to operate as a UE-to-Network relay.

1. The Remote UE sends a Direct Communication request message to the Relay UE. The Remote UE includes its SUCI in the message to request UE-to-Network relay service. The Remote UE also provides its security capabilities and security policy as in TS 33.536[8]. If the Remote UE is reconnecting to the same Relay UE and is already authenticated and authorized for relay communication via that Relay UE, it includes the Krelay ID (instead of SUCI) established during the previous connection using this procedure. If the Relay UE has the Krelay and Krelay ID it skips steps 2 to 12, otherwise the Relay UE rejects the connection request.

NOTE 1:Krelay and Krelay ID are reused during reconnection the same way as KRNP and KRNP ID in TS 33.536[8].Editor's note: Whether and how the Remote UE may use its 5G native security context to connect via the Relay UE is FFS.

2. The Relay UE sends a NAS Relay Authorization request message to its serving AMF. The Relay UE includes the Remote UE's SUCI in the message.

3. The Relay UE's AMF checks that the Relay UE is authorized to act as a Relay based on subscription information obtained during Relay UE's registration

4-8. The Relay UE's AMF initiates Remote UE authentication with Remote UE's AUSF according to existing primary authentication procedures. The authentication messages are exchanged transparently via the Relay UE. Authentication messages between AMF and AUSF and AMF and Relay UE include an indication that it is for a relayed authentication i.e. to authenticate Remote UE via Relay UE.

Editor's note: Whether UDM is made aware that the Remote UE is being authenticated via a Relay UE is FFS.

9. Upon successful authentication of the network, the Remote UE derives a PC5 link root key Krelay and its Krelay ID from KAMF

NOTE 2:Krelay and its Krelay ID can be considered as equivalent to KRNP and KRNP ID in TS 33.536[8].

Editor's note: Details for how Krelay and Krelay ID are derived are FFS

10. Upon successful authentication of the Remote UE, Relay UE's AMF checks with Remote UE's UDM that Remote UE is authorized to use UE-to-Network relaying. Upon successful authorization check, Relay UE's AMF registers with Remote UE's UDM as its Relay's AMF, providing the Relay UE identity (SUPI or GPSI).

11. Relay UE's AMF derives a PC5 link root key Krelay and its Krelay ID from KAMF asperformed by Remote UE in step 9.

12. Relay UE's AMF sends a NAS Relay Authorization response message to the Relay UE. The Relay UE's AMF includes the PC5 link root key Krelay and its Krelay ID in the message. The Relay UE stores the key and its id and associates them with the PC5 link with Remote UE.

13. The Relay UE initiates PC5 link security establishment with Remote UE based on PC5 link root key Krelay. The Relay UE derives PC5 session key Krelay-sess from Krelay, and confidentiality and integrity keys from Krelay-sess the same way KNRP-sess is derived from KNRP, and confidentiality and integrity keys from KNRP-sess in TS 33.536[8]. The Relay UE integrity protects the Direct Security Mode Command and includes parameters as in TS 33.536[8]. The Relay UE includes the Krelay ID to indicate that the PC5 security establishment should be based on Remote UE's primary authentication run.

Editor's note: Details for key hierarchy used for PC5 link security above is FFS

14. The Remote UE checks that the received Krelay ID matches the one derived in step 9. If the provided key id matches, then the Remote UE proceeds with PC5 session, confidentiality, and integrity keys derivation using Krelay as the PC5 link root key as performed by the Relay UE. The Remote UE performs security checks of the Direct Security Mode Command message as in TS 33.536[8].

15. The Remote UE sends integrity and confidentiality protected Direct Security Mode Complete message to Relay UE as in TS 33.536[8].

16. Procedure continues as per L3 relay setup procedure as defined in TR 23.752 [2] (e.g., in step 3 in solution#6).

Editor's note: PC5 link security handling during changes of Relay UE's AMF and/or Remote UE re-authentication is FFS

Editor's note: Authorization revocation of Remote UE to use Relay is FFS

### 6.10.3 Solution evaluation

## 6.11 Solution #11: Protection of the PC3 interface using GBA

### 6.11.1 Introduction

This solution addresses key issue #10.

This solution proposes to protect the PC3 interface thanks to the use of TLS with PSK, where the Pre-Shared Key is established thanks to GBA (Generic Boostrapping Architecture).

### 6.11.2 Solution details

This solution assumes that the 5GDDNMF takes the role of the NAF (Network Application Function) in GBA.

GBA (Generic Boostrapping Architecture), as specified in 3GPP TS 33.220 [12], is a generic mechanism enabling the establishment of shared keys between the UE and any Application Function (named Network Application Function in GBA description) thanks to 3GPP user authentication (AKA-based authentication).

The UE and an Application Function can establish a TLS tunnel using GBA-based secret as specified in clause 4 of 3GPP TS 33.222 [13]. Then, the UE and the Application Function can exchange application data over the secure tunnel.

Consequently, the UE and the 5GDDNMF can exchange applicative data thanks to TLS tunnel established with GBA-based-secret.

### 6.11.3 Evaluation

## 6.12 Solution #12: Privacy handling for Layer-3 UE-to-UE Relay based on IP routing

### 6.12.1 Description

This solution addresses Key Issue #8: Privacy of information over the UE-to-UE Relay and describes operations of the 5G ProSe UE-to-UE Relay in support of privacy.

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 IP address/prefix and/or other identifiers, e.g., for privacy reasons.

When a Source UE 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 and/or other new identifiers since communication between UE1 and the UE-to-UE Relay is over a PC5 unicast link and the UE-to-UE Relay also handles the IP routing of messages exchanged between the peer UEs. Moreover, since the PC5 unicast link used by UE1 is established with the UE-to-UE Relay, this UE-to-UE Relay also needs to update its identifiers at the same time as the Source UE.

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.

### 6.12.2 Solution details

Figure 6.12.2-1 illustrates the IP address/prefix change procedure between the Source UE (UE1), the Target UE (UE2), and the UE-to-UE Relay. The Link Identifier Update procedure defined in TS 23.287 [9] is reused between UE1 and the UE-to-UE Relay and a new procedure is defined between the UE-to-UE Relay and UE2 (i.e., Target UE(s)).

This solution applies to Layer-3 based Solution #10 and Solution #32 described in TR 23.752[2]. Since Solution #10 and Solution #32 described in TR 23.752[2] are similar, this proposed solution applies to both of them. The main difference between Solution #10 and Solution #32 described in TR 23.752[2] is the proposed method of IP address/prefix allocation. In Solution #10, the UE-to-UE Relay allocates the IP address/prefix to the UE. In Solution #32, 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.

For simplicity, Figure 6.12.2-1 and the detailed text below focus on the change of IP addresses/prefixes. However, it is understood that other identifiers that are updated and exchanged during the Link Identifier Update procedure as specified in TS 23.287 [9] are also included in this proposed procedure. For example, Layer-2 IDs (source/destination) and security information IEs are changed on the PC5 unicast link between UE1 and the UE-to-UE Relay although not shown in Figure 6.12.2-1.



Figure 6.12.2-1: Privacy handling for Layer-3 based UE-to-UE Relay

0) A PC5 unicast link is established between UE1 and the UE-to-UE Relay. Another PC5 unicast link is established between the UE-to-UE Relay and UE2. The Relay maintains a mapping table that includes its PC5 peer UEs’ user info, their IP addresses/prefixes, and associated PC5 unicast links. Both Source/Target UEs learn their peer UE’s IP addresses/prefixes via the Relay UE using 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, timer expiration) that its IP address/prefix, Layer-2 ID, and possibly other identifiers (e.g., Application ID) must be changed. UE1 triggers the Link Identifier Update procedure, as defined in TS 23.287 [9], with some changes added for the support of UE-to-UE Relay.

2) UE1 sends a Link Identifier Update Request message to the UE-to-UE Relay over the PC5 unicast link, which includes a “new IP address needed” indication and its peer UE info (i.e., UE2 IP address, UE2 User Info), in addition to the usual parameters sent on the Link Identifier Update request message, e.g., Layer-2 ID and security info.

1. The “new IP address needed” indication is used when the UE-to-UE Relay assigns the IP address/prefix to its peer UEs, as defined in sol#10. If the UE uses a link-local IP address, as defined in sol#32, a new link-local IP address is self-allocated on UE1 and sent to the UE-to-UE Relay using the Link Identifier Update Request message.

3) UE-to-UE Relay assigns a new IP address/prefix to UE1 and saves it locally, while still preserving UE1’s current IP address/prefix. UE-to-UE Relay fetches UE2’s entry from its local table based on the peer UE info specified on the Link Identifier Update Request message. UE-to-UE Relay sends a new PC5 Relay Update Request message to UE2 (including UE1’s old IP address/prefix, UE1’s User Info, and UE1’s new IP address/prefix) to inform UE2 about UE1’s new IP address/prefix.

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

1. At this point, UE2 still sends/receives IP data using UE1’s old IP address/prefix until an IP packet using UE1’s new IP address/prefix is received. At that point, UE2 starts using UE1’s new IP address/prefix and forgets UE1’s old IP address/prefix.

5) UE-to-UE Relay sends a Link Identifier Update Response message to UE1 including UE1’s new IP address/prefix (and UE-to-UE relay new info e.g., new IP address/prefix, new Layer-2 ID, new security info).

6) UE1 saves its new IP address/prefix and UE-to-UE Relay new IP address/prefix and other new info. UE1 sends back a Link Identifier Update ACK message to the UE-to-UE Relay including all parameters received on the Link Identifier Update Response message. UE1 may start using its new IP address/prefix. The new Layer-2 IDs associated with the PC5 unicast link (i.e., for UE1 and UE-to-UE Relay, as well as new security info) are also used at that point. Once UE1 has received data using UE1’s new IP address/prefix, the old IP address/prefix may be released or deleted.

Editor’s Note: The IP addresses for both UE1 and UE2 should be updated at the same time. Otherwise the changed IP could be indirectly traced using other parameters that are associated with the Link ID Update request/response. It is FFS how to provide such IP addresses update in this solution.

Editor’s Note: Whether IP address change for privacy is always needed is FFS.

### 6.12.3 Evaluation

## 6.13 Solution #13: Secondary Authentication for a Layer 3 Remote UE

### 6.13.1 Introduction

This solution addresses KI#4, Authorization in the UE-to-Network relay scenario. This solution especially describes how to perform the secondary authentication for Remote UE. It is necessary to develop a mechanism to support the secondary authentication for Remote UE in UE-to-Network Relay communication for the case where a DN requires the secondary authentication. Because the DN cannot distinguish whether a UE is connected directly to the 5GC or connected to the 5GC via UE to Network Relay, so the DN may block the Remote UE access if the network does not support secondary authentication for a Remote UE. There are two proposed solutions specified in the following clauses for the secondary authentication of Remote UE, where one is performed after PC5 link setup, and the other is performed before finishing the PC5 link setup. These solutions are only applicable for Layer 3 UE-to-Network Relay.

### 6.13.2 Solution details

#### 6.13.2.1 Secondary Authentication after PC5 link setup



Figure 6.13.2.1-1: Secondary authentication procedure for a Remote UE (after PC5 link setup)

1. During the Registration procedure, Authorization and provisioning is performed for the ProSe UE-to-NW relay(0a) and Remote UE(0b).

Editor's note: It is FFS how the Remote UE is authorized and provisioned when it is out of coverage.

1. The ProSe 5G UE-to-Network Relay may establish a PDU session for relaying with default PDU session parameters received in step 0 or pre-configured in the UE-to-NW relay, e.g. S-NSSAI, DNN, SSC mode or PDU Session Type.

2. Based on the Authorization and provisioning in step 0, the Remote UE performs discovery of a ProSe 5G UE-to-Network Relay. As part of the discovery procedure the Remote UE learns about the connectivity service the ProSe UE-to-Network Relay provides.

3. The Remote UE selects a ProSe 5G UE-to-Network Relay and establishes a connection for One-to-one ProSe Direct Communication.

If there is no PDU session satisfying the requirements of the PC5 connection with the remote UE, e.g. S-NSSAI, DNN, QoS, the ProSe 5G UE-to-Network Relay initiates a new PDU session establishment or modification procedure for relaying.

4. For IP PDU Session Type and IP traffic over PC5 reference point, IPv6 prefix or IPv4 address is allocated for the remote UE. From this point the uplink and downlink relaying can start.

5. The ProSe 5G UE-to-Network Relay sends a Remote UE Report (Remote User ID, IP info) message to the SMF for the PDU session associated with the relay.

6. When the SMF received Remote UE Report, based on local configuration of the SMF, the SMF may retrieve subscription data of the Remote UE from the UDM and may perform Secondary authentication/authorization for the Remote UE. The SMF sends PDU Session Authentication Command message to the 5G ProSe UE-to-Network Relay including Remote User ID.

7. The 5G ProSe UE-to-Network Relay sends EAP message to the Remote UE via PC5 signalling. The Remote UE sends EAP message to the 5G ProSe UE-to-Network Relay via PC5 signalling.

Editor's note: whether a PDU session can be shared with other Remote UEs when DN requires PDU secondary A&A is FFS

8. The 5G ProSe UE-to-Network Relay sends PDU Session Authentication Complete message to the SMF including Remote User ID and EAP message received from the Remote UE.

9. The SMF sends EAP message to the DN-AAA.

10. The DN AAA server and the UE should exchange EAP messages, as required by the EAP method.

11. If the authentication/authorization success, the DN-AAA sends EAP-Success to the SMF.

12. If the authentication/authorization fails, the DN-AAA sends EAP-Failure to the SMF. The SMF sends NAS message (e.g. PDU Session Modification, Remote UE Release Command) to the 5G ProSe UE-to-Network Relay. The NAS message includes Remote User ID to indicate the Remote UE and the 5G ProSe UE-to-Network Relay releases the PC5 link with the Remote UE.

NOTE 1: It is possible to perform secondary authentication procedure in parallel when multiple Remote UEs are connected to the 5G ProSe UE-to-Network Relay almost at the same time.

NOTE 2: The DN-AAA does not know whether a UE is connected via 5G ProSe UE-to-Network Relay or connected directly to the network.

Editor's note: Whether forwarding EAP message via UE-to-Network Relay meets security requirements is FFS.

#### 6.13.2.2 Secondary Authentication before PC5 link setup



Figure 6.13.2.2-1: Secondary authentication procedure for a Remote UE (before PC5 link setup)

1. During the Registration procedure, Authorization and provisioning is performed for the ProSe UE-to-NW relay(0a) and Remote UE(0b).

Editor's note: It is FFS how the Remote UE is authorized and provisioned when it is out of coverage.

1. The ProSe 5G UE-to-Network Relay may establish a PDU session for relaying with default PDU session parameters received in step 0 or pre-configured in the UE-to-NW relay, e.g. S-NSSAI, DNN, SSC mode or PDU Session Type.

2. Based on the Authorization and provisioning in step 0, the Remote UE performs discovery of a ProSe 5G UE-to-Network Relay. As part of the discovery

3. Remote UE establishes PC5 connection towards the 5G ProSe UE-to-Network Relay UE. When requesting UE-to-Network relaying over PC5, the Remote UE provides its Remote User ID to the 5G ProSe UE-to-Network Relay UE.

4. The 5G ProSe UE-to-Network Relay UE sends PDU Session Establishment or PDU Session Modification Request to the SMF and provides the Remote UE ID of the Remote UE.

5. When the SMF received Remote User ID, based on local configuration of the SMF, the SMF may retrieve subscription data of the Remote UE from the UDM and may perform Secondary authentication/authorization for the Remote UE. The SMF sends PDU Session Authentication Command message to the 5G ProSe UE-to-Network Relay including Remote User ID.

6. The 5G ProSe UE-to-Network Relay sends EAP message to the Remote UE via PC5 signalling. The Remote UE sends EAP message to the 5G ProSe UE-to-Network Relay via PC5 signalling.

Editor's note: whether a PDU session can be shared with other Remote UEs when DN requires PDU secondary A&A is FFS

7. The 5G ProSe UE-to-Network Relay sends PDU Session Authentication Complete message to the SMF including Remote User ID and EAP message received from the Remote UE.

8. The SMF sends EAP message to the DN-AAA.

9. The DN AAA server and the UE should exchange EAP messages, as required by the EAP method.

10. If the authentication/authorization success, the DN-AAA sends EAP-Success to the SMF.

11. The SMF sends PDU Session Establishment Accept or PDU Session Modification Command to accept Remote UE's request.

12. The 5G ProSe UE-to-Network Relay UE sends PC5 connection accept message to the Remote UE.

13. The ProSe 5G UE-to-Network Relay sends a Remote UE Report (Remote User ID, IP info) message to the SMF for the PDU session associated with the relay.

14. If the authentication/authorization fails, the DN-AAA sends EAP-Failure to the SMF.

15. The SMF sends PDU Session Establishment Reject or PDU Session Modification Command to the 5G ProSe UE-to-Network Relay UE to reject Remote UE's request.

16. The 5G ProSe UE-to-Network Relay UE rejects PC5 connection establishment.

NOTE 1: It is possible to perform secondary authentication procedure in parallel when multiple Remote UEs are connected to the 5G ProSe UE-to-Network Relay almost at the same time.

NOTE 2: The DN-AAA does not know whether a UE is connected via 5G ProSe UE-to-Network Relay or connected directly to the network.

Editor's note: Whether forwarding EAP message via UE-to-Network Relay meets security requirements is FFS.

### 6.13.3 Evaluation

TBD.

## 6.14 Solution #14: A security solution for UE-to-Network Relay based on Layer 2 Relay

### 6.14.1 Introduction

This solution addresses Key Issue #3 on Security of UE-to-Network Relay. The solution is based on TR 23.752[2] solution #7 which is a Layer 2 Relay solution.

### 6.14.2 Solution details



Figure 6.14.2-1: UE-to-Network Relay solution for Layer2

Editor’s Note: The function of this solution out of coverage is FFS

0. If the Remote UE is in the coverage, the Remote UE perform initial registration to the network according to the registration procedure in TS 23.502[10]. If the Remote UE is not in the coverage, the Remote UE will perform the Initial Registration via the UE-to-Network Relay in step 7.

1. If in coverage, the Remote UE and UE-to-Network Relay UE independently get the service authorization for indirect communication from the network. If the Remote UE is not in coverage, the pre-configured information will be used.

2-3. The Remote UE and UE-to-Network Relay UE perform UE-to-Network Relay UE discovery and selection. For details of UE-to Network Relay discovery and selection for Layer2 UE-to-Network Relay see clause see clause 6.7.2.9 and Solution #19, Solution #41 of TR 23.752[2].

4. Remote UE initiate a one-to-one communication connection with the selected UE-to-Network Relay UE over PC5 using the procedure as described in clause 6.7 in this study.

5. If the UE-to-Network Relay UE is in CM\_IDLE state, triggered by the communication request received from the Remote UE, the UE-to-Network Relay UE sends a Service Request message to its serving AMF. The relay UE transitions to the connected state by sending a service request.

Editor’s Note: security for PC5 is FFS

6. The Remote UE initials AS connection with NG-RAN via the UE-to-Network Relay UE to establish AS Connection with the same NG-RAN serving the Relay UE.

7. The Remote UE sends a NAS message to the serving AMF. The NAS message is encapsulated in an RRC message that is sent over PC5 to the UE-to-Network Relay UE, and the UE-to-Network Relay UE forwards the message to the NG-RAN. The NG-RAN derives Remote UE's serving AMF and forwards the NAS message to this AMF.

If the Remote UE has registered to the network in step0, then the NAS message is integrity protected by using the NAS security context derived in step0, and the UE puts 5G-GUTI in the NAS message. Both the UE and AMFshould perform the procedures defined in TS 33.501[14].

If the Remote UE has not registered to the network, then the UE should send a NAS message with a SUCI and perform primary authentication with the Remote UE’s AMF. Both the UE and AMF should perform the procedures defined in TS 33.501[14].

8. Remote UE may trigger the PDU Session Establishment procedure as defined in clause 4.3.2.2 of TS 23.502 [10]. The user plane security between the Remote UE and the gNB should reuse the procedure defined in clause 6.6 of TS 33.501[14].

9. The data is transmitted between Remote UE and UPF via UE-to-Network Relay UE and NG-RAN. The UE-to-Network Relay UE forwards all the data messages between the Remote UE and NG-RAN using RAN specified L2 relay method.

Editor’s Note: this step needs to be revisited based on the RAN WG progress

### 6.14.3 Evaluation

## 6.15 Solution #15: Key management in UE-to-Network Relay based on primary authentication

### 6.15.1 Introduction

This solution addresses the KI #3, KI#4 and KI#9. This solution provides a mechanism setup a PC5 link security between a remote UE and UE-to-network relay based on primary authentication.

Editor’s note: whether this solution supporting out of coverage being FFS.

### 6.15.2 Solution details

The procedure for key management in UE-to-Network relay using primary authentication is depicted in Figure 6.15.2-1.

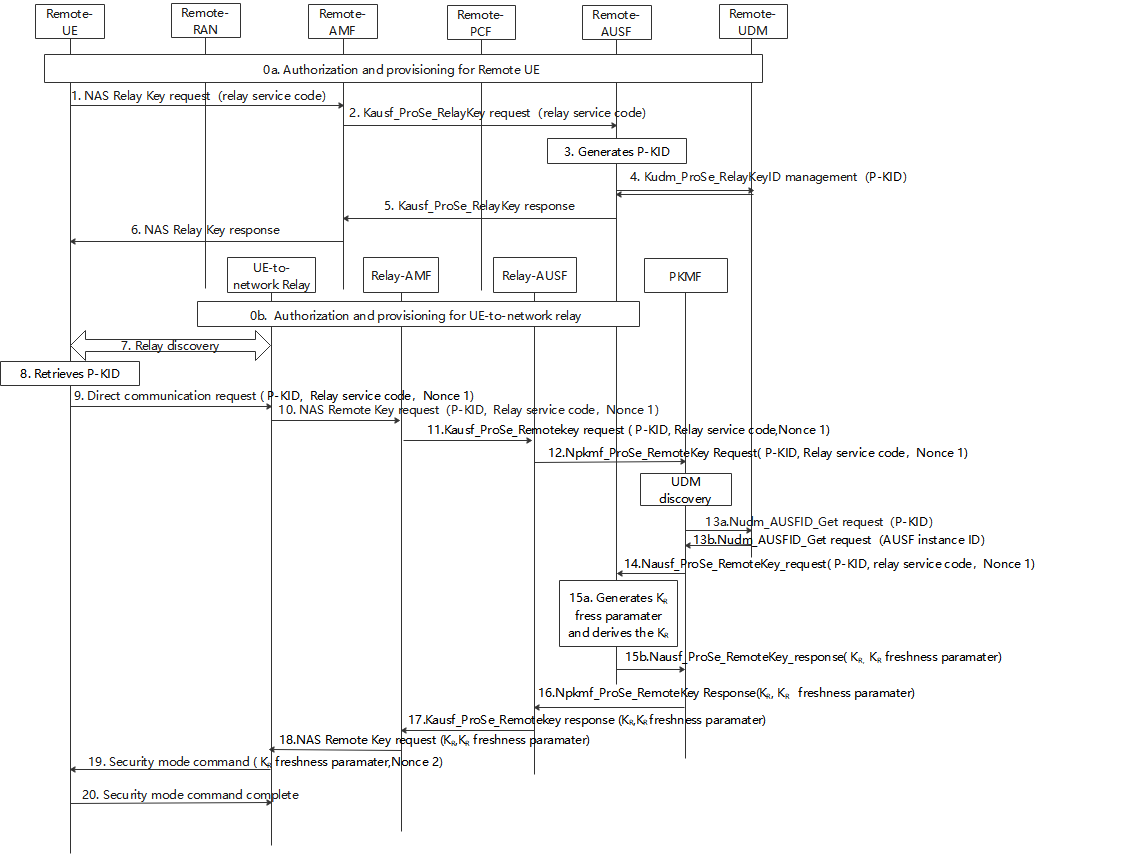


Figure 6.15.2-1: Procedures for key management in ProSe UE-to-Network Relay based on primary authentication

0. During Registration procedure, authorization and provisioning is performed for the Remote UE (0a) and ProSe UE-to-NW relay (0b).

1. The Remote UE sends a NAS relay Key request message with relay service code for PC5 communication with a UE-to-network relay.

2. After receiving the NAS relay key request from UE, the Remote AMF that serves the remote UE first checks whether the UE is authorized to be as a remote UE. If it is authorized, the Remote AMF further sends Nausf\_ProSe\_RelayKey request with relay service code.

3. The Remote AUSF that serves the remote UE generates P-KID for the relay service code in the Nausf\_ProSe\_RelayKey request.

Editor’s note: The generation of the P-KID in AUSF is FFS.

4. The Remote AUSF further stores P-KID in UDM via Kudm\_ProSe\_RelayKey service.

5. The Remote AUSF sends Nausf\_ProSe\_RelayKey response to the AMF.

6. The Remote AMF sends NAS relay Key response to the UE.

Editor’s note: how the procedure (i.e step 1~6 ) works in Kausf change (e.g., due to reauthentication) is FFS.

7. The Remote UE discovers the UE-to-network Relay using either model A or model B discovery.

8. The Remote UE retrieves P-KID based on the relay service code the Remote UE would like to access.

Editor’s note: The retrieval of the P-KID in UE is FFS.

9. The Remote UE sends a Direct Communication Request. The Direct Communication Request contains the Relay Service Code, P-KID and Nonce1.

Editor’s note: It’s FFS whether P-KID or other user ID e.g. SUCI should be used in PC5.

10. The UE-to-Network relay triggers the PC5 root key (i.e PC5 root key for communicating with the remote UE) retrieval procedure. The Relay sends NAS remote Key request with P-KID, Relay service code, Nonce 1.

11. The relay AMF that serves the relay UE first check whether the relay UE is authorized to be a relay. If authorized, the relay AMF sends Nausf\_ProSe\_RemoteKey request with P-KID, Relay service code, Nonce 1.

Editor’s note: The role of relay-AUSF is unclear. I.e. step11 could be invoked directly towards home NF, e.g. remote AUSF.

12. The relay AUSF discovers the PKMF and sends Npkmf\_ProSe\_RemoteKey request with P-KID, Relay service code, Nonce 1.

Editor’s note: The role of the PKMF is unclear. If AUSF of Remote UE is responsible for generating the key, then what is the role of PKMF.

13. The PKMF discovers the UDM based on the P-KID, and sends Nudm\_AUSFID\_Get request with P-KID. The UDM response to PKMF via Nudm\_AUSFID\_Get with AUSF instance ID of the AUSF serving remote UE.

Editor’s note: Whether PKMF can interface with the Remote UDM or Remote AUSF, in particular in the roaming case, is FFS.

14. PKMF further sends the remote AUSF Nausf\_ProSe\_RemoteKey request with P-KID, Relay service code, Nonce 1.

15. The remote AUSF generates KR freshness parameter and derives KR using at least Kausf, relay service code,KR freshness parameter and Nonce 1 as input.

Editor’s note: The generation of the KR key is FFS.

16. The PKMF sends Npkmf\_ProSe\_RemoteKey response with KR, KR freshness parameter to AUSF.

17. The relay AUSF sends Nausf\_ProSe\_RemoteKey response with KR, KR freshness parameter to the relay AMF.

18. The relay AMF sends NAS remote Key response KR, KR freshness parameter to the UE-to-network relay.

19. The UE-to-network relay sends a Direct Security Mode Command message to the Remote UE, KR freshness parameter and Nonce 2 are included in the message.

Editor’s note: The parameters included in Direct Security Mode Command message are FFS.

20. The Remote UE derives KR key in the same way as the remote AUSF in step 15.

Editor’s note: how the DSMC messages are being protected is FFS.

### 6.15.3 Evaluation

TBD.

## 6.16 Solution #16: Security establishment procedures between two UEs in the UE-to-UE relay scenario

### 6.16.1 Introduction

This solution addressed the key issue #6 by establishing the security context between the two remote UEs. Generally, protection key negotiation procedures defined in TS 33.536 [8] eV2X will be reused as the baseline.

### 6.16.2 Solution details

This clause gives out the procedure for the security establishment.



Figure 6.16.2-1: Security establishment procedure between UE1 and UE2 in the UE-to-UE relay scenario

The procedure assumes the UE1 and UE2 has preconfigured with the shared key ID and Key (i.e. K-ID, Key).

Editor’s Note: what protocol is used for the e2e messages protection is FFS

Step 1: UE1 performs the discovery procedure based on the Model A or Model B. It is possible that two potential UE-to-UE relays that can be selected for the services between UE1 and UE 2 are identified.

Editor’s Note: The relay selection should be aligned with SA2.

Step 2: UE1 selects UE-to-UE relay1 to relay the following ProSe service data based on its local policy.

Step 3: (Optional) UE1 may establish the direct security establishment with the UE-to-UE relay1.

Step 4: (Optional) UE-to-UE relay1 may establish the direct security establishment with the UE2.

NOTE: Details on Step 1-4 can be found in the other solutions of this document.

Editor’s Note: how to protect messages over PC5 between the remote UE and the relay is FFS.

Step 5-6: UE1 sends the indirect communication request to UE2 via the UE-to-UE relay1, including the K-ID, UE1 security capability, UE-to-UE relay1 ID, a security info, where the security info can be used by the UE2 to verify the UE1 authenticity.

Editor’s Note: Security parameters needs to be clarified.

Step 7: UE2 verified the security info to assure the correctness of the indirect communication request message, and may verify that the authenticity of UE-to-UE relay identified by the UE-to-UE relay ID.

Editor’s Note: Detail on authenticating UE-to-UE relay needs to be clarifed.

Step 8: UE1 and UE2 perform the indirect security mode command procedure to establish the security connection, including the protection key and security algorithms.

Editor’s Note: whether the direct SMC procedure defined in the TR 33.536 [8] can be reused here for indirect communicaton mode is FFS.

Step 9-10: UE2 sends indirect communication response message to the UE1.

The following data transferred between the two UEs could be protected based on the security connection estabhlished in the above.

### 6.16.3 Evaluation

TBD

6.17 Solution #17: Solution on securely creating destination Layer-2 ID in groupcast communication

6.17.1 Introduction

This solution addresses the KI #13 "Security and privacy of groupcast communication".

6.17.2 Solution details

The detailed solution is illustrated in Figure.

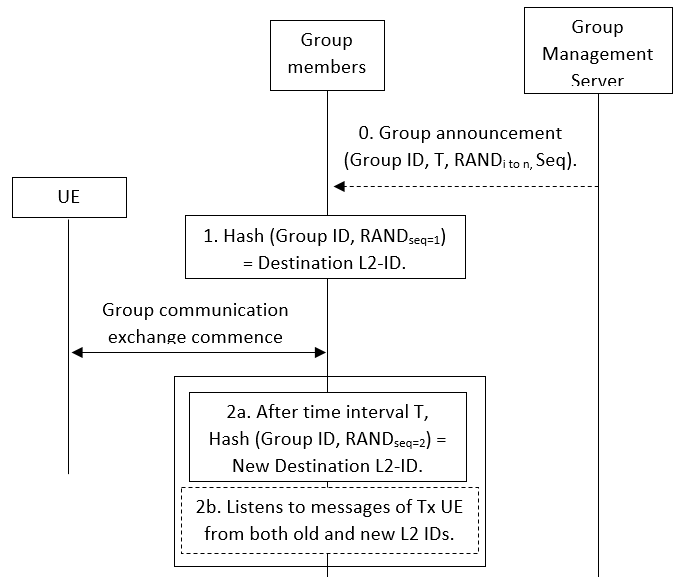


Figure 6.17.2-1: Procedure for secure conversion of application layer group ID to destination Layer-2 ID

0. Group Setup: Once the group is created, the group management server will send the application layer group ID to the associated UEs and a timer T. It will also send a set of random numbers and a specific sequence in which these random number are to be used. It is assumed that the application layer signalling is protected.

1. ID Conversion: All the UEs use the application layer group ID and the first random number according to the sequence as an input to a hash function to generate the destination Layer-2 ID.

2. ID Update: When the timer T expires, a new destination Layer-2 ID is calculated using the next random number according to the sequence. The UEs can listen to both old a new destination Layer-2 IDs, to avoid any time synchronization issues, for a certain period of time or until receives a message with the new ID.

The destination Layer-2 ID is updated until the ProSe application layer changes the group ID.

The group management server can also send the corresponding materials to generate random numbers rather than sending the random numbers itself.

Editor’s Note: security for group management (including message 0 in the figure) is FFS

Editor’s Note: time synchronization among group members is FFS

6.17.3 Evaluation

TBA.

## 6.18 Solution #18: PC5 link setup for UE-to-Network relay

### 6.18.1 Introduction

This solution addresses the KI #3. This solution provides a mechanism to setup a PC5 link between a remote UE and UE-to-network relay. This solution assumes 5G Prose function and Prose Key Management Function as in LTE Prose. This solution only describes the PC5 link setup procedure that is common for both L2 and L3 UE-to-network relay.

### 6.18.2 Solution details



Figure 6.18.2-1: Secure PC5 link establishment procedure for UE-to-network relay

Editor’s Note: Out of coverage is FFS.

0a-d. The Remote UE and the UE-to-network (U2N) relay get the discovery parameters and Prose Key management function (PKMF) address from the 5G Prose function and the discovery security material from the PKMF respectively.

Editor’s Note: How the remote UE is configured to access the PKMF of the relay UE is FFS.

Editor’s Note: The location of PKMF is FFS.

Editor’s Note: Security of communication with PKMF is FFS.

Editor’s Note: It is FFS when Remote UE and Relay are served by different 5G DDNMF

1a. The Remote UE sends a Prose Remote User Key (PRUK) Request message to the PKMF of the UE-to-network relay.

1b. The ProSe Key Management Function checks that the Remote UE is authorised to receive UE-to-network Relay service. If the Remote UE is authorised to receive the service, the PKMF sends a PRUK and PRUK ID to the Remote UE.

2. The discovery procedure is performed between the Remote UE and the UE-to-network Relay using the discovery parameters and discovery security material.

Editor’s Note\_3: The detail of discovery security material is FFS, and how it impacts on discovery procedure needs to be clarified

3. The Remote UE sends a Direct Communication Request that contain the PRUK ID, Relay Service Code (RSC) of the UE-to-network relay service and KNRP freshness parameter 1.

4a. The UE-to-network relay sends a Key Request message that contains PRUK ID, RSC and KNRP freshness parameter 1 to the PKMF.

4b. The PKMF generates KNRP freshness parameter 2 and derives KNRP using PRUK identified by PRUK ID, KNRP freshness parameter 1 and KNRP freshness parameter 2. sends a Key Response message that contains KNRP and KNRP freshness parameter 2 to the UE-to-network relay.

5a. The UE-to-network relay sends a Direct Security Mode Command message to the Remote UE (see 6.5.2.2). This message contains the KNRP Freshness Parameter 2 and protected based on the session key (KNRP-SESS) derived from KNRP.

Editor’s Note: How to support flexibility between remote UE and relay UE is FFS.

5b. The Remote UE derives KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2. It then derives the session key (KNRP-SESS) in the same manner as the UE-to-network relay and processes the Direct Security Mode Command. Then, the Remote UE responds with a Direct Security Mode Complete message to the UE-to-network relay.

6. The remote UE and UE-to-network relay continues the rest of procedure for the relay service over the secure PC5 link.

NOTE: the rest of procedure is determined depending on the UE-to-network relay types (i.e., L2 or L3 relay).

### 6.18.3 Evaluation

TBD.

## 6.19 Solution #19: End-to-end security for the L3 UE-to-Network relay

### 6.19.1 Introduction

This solution addresses the KI #3. This solution provides a mechanism to provide an end-to-end security between a remote UE and the network for Layer 3 UE-to-network relay.

### 6.19.2 Solution details



Figure 6.19.2-1: Secure PC5 link establishment procedure for UE-to-network relay

1. The Remote UE establishes a secure PC5 link with the UE-to-network (U2N) relay.

2. The remote UE performs a registration procedure to 5GC via N3IWF as specified in clause 7.2.1 of TS 33.501 [14]. The only difference from the untrusted non-3GPP access procedure is that the UE-to-network relay and the serving network of the UE-to-network relay take the role of untrusted access network. As a result of successful registration via the N3IWF, IPsec tunnel is established between the remote UE and N3IWF and all traffic between the remote UE and N3IWF is end-to-end protected.

3. The remote UE may establish a PDU session via N3IWF for the traffic that requires end-to-end security between the remote UE and 5GC.

Editor’s Note: The protocol stack is FFS.

Editor’s Note: It is FFS how Remote UE connects to N3IWF after step 1.

### 6.19.3 Evaluation

TBD.

## 6.20 Solution #20: PC5 link setup for UE-to-UE relay

### 6.20.1 Introduction

This solution addresses the KI #6. This solution provides a mechanism to setup a connection between remote UEs via the UE-to-UE relay. This solution is a L3 relay solution and assumes 5G Direct Discovery Name Management Function (DDNMF) and Prose Key Management Function (PKMF) as in LTE Prose. This solution only describes the PC5 link setup procedure between the remote UE and the UE-to-UE relay and end-to-end security setup between remote UEs.

### 6.20.2 Solution details



Figure 6.20.2-1:. Secure PC5 link establishment procedure for UE-to-network relay

Editor’s Note: How this solution will work out of coverage is FFS.

NOTE: This solution assumes a peer UE discovery mechanism (e.g., DNS based).

0. The Remote UEs and the UE-to-UE (U2U) relay get the discovery parameters and Prose Key management function (PKMF) address from the 5G DDNMF and the discovery security material from the PKMF respectively. Furthermore, the Remote UEs can be provisioned with the security materials for end-to-end security setup by the PKMF. For example, the security materials for end-to-end security setup include the Prose Service Code (PSC) and associated key. The service code may be used as a key ID when IKEv2 PSK based authentication is used.

1. Remote UE 1 performs the discovery procedure and PC5 unicast link setup procedure with the UE-to-UE relay.

a. The Remote UE performs discovery of a U2U relay.

b. The Remote UE sends a Direct Communication Request that includes Relay Service Code (RSC) and Nonce1.

c. Authentication and key agreement may be performed between the remote UE and U2U relay. As a result of successful authentication, KNRP is derived.

d. The U2U relay generates Nonce2 and derives KNRP-SESS using KNRP, Nonce1 and Nonce2. The U2U relay sends a Direct Security Mode Command that contains Nonce 2 to the Remote UE. The Direct Security Mode Command is integrity protected based on KNRP-SESS.

e. The Remote UE derives KNRP-SESS using KNRP, Nonce1 and Nonce2 and checks the integrity of the Direct Security Mode Command. If the verification is successful, the Remote UE sends a Direct Security Mode Complete to the U2U relay. From this point, all PC5 unicast traffic between the Remote UE and the U2U relay can be protected based on the KNRP-SESS.

Editor’s Note: How to support flexibility between remote UE1 and relay UE, and between Relay and Remote UE 2 are FFS.

Editor’s Note: The location of PKMF and how the remote UEs and relay UE use the PKMF is FFS.

2. Remote UE 2 performs the discovery procedure and PC5 unicast link setup procedure with the UE-to-UE relay in the same manner as Remote UE 1.

3. Remote UE 1 and Remote UE 2 can establish an end-to-end IPsec connection via U2U relay. To establish an end-to-end IPsec connection, Remote UE1 and Remote UE2 may perform IKEv2 authentication using the keying materials provisioned in step 0.

Editor’s Note: whether IPsec will be always used needs to be clarified.

### 6.20.3 Evaluation

TBD.

## 6.21 Solution #21: AF for key management in PC5 communication

### 6.21.1 Introduction

This solution describes how the Remote UE and the UE-to-network relay finds out the address of the common key management server (AF) to be able to communicate over PC5 interface. This solution addresses key issue#4.

This solution is for commercial services. The Remote UE and the UE-to-network Relay have no knowledge of each other beforehand.

### 6.21.2 Solution details

In this solution the Remote UE has an AF (AF-1) in it’s home PLMN for ProSe key management. The UE-to-network relay has an AF (AF-2) in its home PLMN for ProSe key management. These two AF’s (AF-1 and AF-2) can be located in the same or different PLMN’s and can communicate with each other.

The Remote UE receives the address of the AF in its home PLMN (AF-1(Remote UE)) from the home 5GDNNMF of the Remote UE. The UE-to-network Relay receives the address of the AF in its home PLMN (AF-2(UE-to-network relay)) from the home 5GDNNMF of the UE-to-network relay.

When the Remote UE has discovered a UE-to-network relay in its vicinity, it either sends the address of the AF-1(Remote UE) explicitly on the PC5 interface or includes the address of the AF-1(Remote UE) into the *Remote UE info* (described in solution #6 in TR 23.752 [2]) sent on PC5 interface to the UE-to-network relay.

The UE-to-network relay contacts the AF-1(Remote UE) via the AF-2(UE-to-network relay) (as described in Option 1 in Figure 6.21.2.-1) or the UE-to-network relay contacts the AF-1(Remote UE) directly (as described in Option 2 in Figure 6.21.2-2).

A third option could be that the UE-to-network relay uses the *Remote UE info* to query the AF-1(Remote UE) address from its 5GDDNMF in it’s home PLMN. The third option is not described below in the signaling flow.

Editor’s note: How this solution would work when Remote UE is out of 3GPP coverage is FFS.



Figure 6.21.2-1: AF for key management in PC5 communication

Step 0) The Remote UE contacts the 5GDNNMF in it’s home PLMN to retrieve the address of the AF-1(Remote UE) used for ProSe key management located in its home PLMN.

The UE-to-network Relay contacts the 5GDNNMF in it’s home PLMN to retrieve the address of the AF-2 (UE-to-network Relay) used for ProSe key management located in its home PLMN.

Step 1) The Remote UE retrievs the discovery keys for discovery of the UE-to-network relay.

Editor’s note: its FFS how the Remote UE retrieves the discovery keys in advance for commercial services.

Step 2) The Remote UE establishes a secure connection with the AF-1 (Remote UE) server.

Editor’s note: How to protect the UE - AF-1 (Remote UE) interface is FFS. This is similar to protection of PC3 interface if its via user plane.

Step 3a) The Remote UE contacts the AF-1(Remote UE) by initiating a Key Request message for PC5 communication including the Relay Service Code.

Step 3b) The AF-1(Remote UE) generates the Key for PC5 communication and provides it in the Key Response message together with a Key ID to the Remote UE.

Step 4) The UE-to-network relay retrievs the discovery keys for discovery of the Remote UE.

Editor’s note: its FFS how the UE-to-network relay retrieves the discovery keys in advance for commercial services.

Step 5) The UE-to-network relay discovery is taken place on PC5 interface using either model A or model B discovery.

Step 6) The Remote UE sends a Direct Communication Request on PC5 interface. The Remote UE includes the address of the AF-1(Remote UE) and the Key ID received from the AF-1 (Remote UE) together with the Relay Service Code and Key ID.

When the Remote UE discovers a UE-to-network relay in its vicinity, it can either send the address of the AF-1(Remote UE) explicitly on the PC5 interface or it can include the address of the AF-1(Remote UE) into the *Remote UE info* (described in solution #6 in TR 23.752 [2]) sent on PC5 interface, to the UE-to-network relay.

Editor’s note: The privacy of the address of the AF-1(Remote UE) sent over PC5 interface needs to be considered.

A third option could be that the UE-to-network relay uses the *Remote UE info* to query the AF-1(Remote UE) address from its 5GDDNMF in it’s home PLMN. The third option is not described below.

**Option 1:**

Step 7) The UE-to-network Relay contacts the AF-2(UE-to-network Relay) and includes the address of the AF-1(Remote UE) in the Key Request message for PC5 communication including the Key ID.

Step 8) The AF-2(UE-to-network Relay) contacts the AF-1(Remote UE) and forwards the Key Request message.

Editor’s note: In Option 1, the communication between AF-1(Remote UE) and AF-2(UE-to-network Relay) is out of 3GPP scope.

Step 9) The AF-1(Remote UE) includes the Key for PC5 communication identified by Key ID in the Key Response message to the AF-2(Remote UE).

Step 10) The AF-2(UE-to-network Relay) forwards the Key Response message to the UE-to-network Relay.

**Option 2:**

Step 7a) The UE-to-network Relay uses the address of the AF-1(Remote UE) and contacts directly the AF-1(Remote UE) by initiating a Key Request message for PC5 communication including the Key ID.

Editor’s note: In Option2, further details needs to be added to the solution. The Remote UE needs to provide its Remote UE ID to the UE-to-network Relay in order for the UE-to-network Relay to provide its own ID and the Remote UE ID to the AF-1(Remote UE). The AF-1(Remote UE) needs to authenticate the UE-to-network Relay and check whether the Remote UE and the UE-to-network Relay are allowed to communicate with each other.

Step 7b) The AF-1(Remote UE) includes the Key for PC5 communication identified by Key ID in the Key Response message to the UE-to-network Relay.

**Option 1 and Option 2:**

Editor’s note: The details of the security establishment (e.g. DSMC) between steps 6-10 are FFS.

Step 11) the UE-to-network Relay responds with a Direct Communication Accept on PC5.

### 6.21.3 Evaluation

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

## 6.22 Solution #22: Masked representation of identities

### 6.22.1 Introduction

This solution addresses Key Issue #11, UE identity protection during ProSe discovery.

The solution is based on the idea to use a temporary UE identity, called a Temporary Broadcast Identifier (TBI), which is masked before being broadcast, by using representations of the identifiers during announcing (i.e. broadcasting) and monitoring (i.e. filtering). The masking ensures that the TBI cannot be used to trace the UE and it cannot be used to impersonate the UE. The use of a temporary identifier ensures that no long-term permanent identifier is used which could be linked to the UE.

Editor's note: the need for a Temporary Broadcast Identifier is FFS.

The solution is described using the framework and terminology of ProSe Direct Discovery as described in TS 23.303 [5], i.e. for Model A discovery, the terms Announcing UE and Monitoring UE are used, and for Model B discovery, the terms Discoverer UE and Discoveree UE are used.

Editor's note: the applicability and working of the solution in out-of-coverage scenarios is FFS.

### 6.22.2 Solution details

#### 6.22.2.1 Solution for Model A

The solution for Model A consists of the following components:

- The assignment of a temporary UE identity, called a Temporary Broadcast Identifier (TBI), to the Announcing UE by the 5GC;

- The use of a Discovery Code (DC), representing the TBI, that is broadcast by the Announcing UE for announcing its presence and its identity;

- The use of a Discovery Filter (DF), that can be used by Monitoring UEs for recognizing and identifying the Announcing UE.

The corresponding information flows are described in Figure 6.22.2.1-1 for the Announcing UE and in Figure 6.22.2.1-2 for the Monitoring UE.



Figure 6.22.2.1-1 Direct discovery flows for Announcing UE

The steps performed by the Announcing UE during direct discovery are as follows, see also Figure 6.22.2.1-1.

0. Before performing direct discovery the Announcing UE is provisioned with a Temporary Broadcast Identifier (TBI); this provisioning can take place during earlier phases of direct discovery, e.g. during service authorization;

1. At the start of direct discovery the Announcing UE requests and receives from the 5GC a Discovery Code (DC) which is a masked representation of its TBI;

Editor's note: how a Discovery Code can be created from a Temporary Broadcast Identifier is FFS.

2. The Announcing UE broadcasts its DC so that it can be discovered by other UEs; in case of restricted discovery only authorized UEs should be able to use the DC they receive.



Figure 6.22.2.1-2 Direct discovery flows for Monitoring UE

The steps performed by the Montoring UE during direct discovery are as follows, see also Figure 6.22.2.1-2.

1. At the start of direct discovery the Monitoring UE requests and receives from the 5GC a Discovery Filter (DF) which is a representation of the Discovery Code broadcast by Announcing UEs that can be used to check for a match;

2. The Monitoring UE uses the DF in order to try to match it against any received DCs; in case of a match it has discovered the Announcing UE that it looked for.

#### 6.22.2.2 Solution for Model B

The solution for Model B consists of the following components:

- The assignment of temporary UE identities, called Temporary Broadcast Identifiers (TBI), to the Discoverer UE and the Discoveree UE;

- The use of a Query Code (QC), representing the TBI of the Discoverer UE, that is broadcast by the Discoverer UE for announcing its query in search for (one or more) Discoveree UEs; the Query Code both identifies the (properties of the) Discoveree UE and the Discoverer UE;

- The use of a Query Filter (QF), that can be used by Discoveree UEs for recognizing the query sent by the Discoverer UE; it also can be used to identity the Discoverer UE (and based on that authorize the discovery of the Discoveree UE);

- The use of a Response Code (RC), representing the TBI of the Discoveree UE, that is broadcast by Discoveree UE for announcing its response to the query received from the Discoverer UE; the Response Code also identifies the Discoveree UE;

- The use of a Response Filter (RF), that can be used by Discoverer UEs for recognizing the response sent by the Discoveree UE; it also can be used to identify the Discoveree UE.

The corresponding information flows are described in Figure 6.22.2.2-1 for the Discoverer UE and in Figure 6.22.2.2-2 for the Discoveree UE.



Figure 6.22.2.2-1 Direct discovery flows for Discoverer UE

The steps performed by the Discoverer UE during direct discovery are as follows, see also Figure 6.22.2.2-1.

0. Before performing direct discovery the Discoverer UE is provisioned with a Temporary Broadcast Identifier (TBI) by the 5GC; this provisioning can take place during earlier phases of direct discovery, e.g. during service authorization;

1. At the start of direct discovery the Discoverer UE requests and receives from the 5GC a Query Code (QC) and a Response Filter (RF); the Query Code is a masked representation of the TBI of the Dicoverer UE and of the Discoveree UEs that it wants to discover; the Response Filter is a representation of the Response Code broadcast by Discoveree UEs that can be used to check for a match;

2. The Discoverer UE broadcasts its QC so that it can be received by the Discoveree UEs that it looks for;

3. The Discoverer UE uses the RF in order to try to match it against any received RCs; in case of a match it has discovered a Discoveree UE that it looked for.



Figure 6.22.2.2-2 Direct discovery flows for Discoveree UE

The steps performed by the Discoveree UE during direct discovery are as follows, see also Figure 6.22.2.2-2.

0. Before performing direct discovery the Discoveree UE is provisioned with a Temporary Broadcast Identifier (TBI) by the 5GC; this provisioning can take place during earlier phases of direct discovery, e.g. during service authorization;

1. At the start of direct discovery the Discoveree UE request and receives from the 5GC a Query Filter (QF) and a Response Filter (RC); the Query Filter is representation of the Query Code broadcast by Discoverer UEs that can be used to check for a match; the Response Code is a masked representation of the TBI of the Discoveree UE;

Editor's note: how a Query Filter is created is FFS.

2. The Discoveree UE uses the QF in order to try to match it against any received QCs; in case of a match it has received a query from an interested Discoverer UE;

3. The Discoveree UE broadcasts its RC so that it can be received by the interested Discoverer UE.

### 6.22.3 Evaluation

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

## 6.23 Solution #23: Initial key with validity time

### 6.23.1 Introduction

This solution addresses Key Issue #12 Security of one-to-one communication over PC5. This solution assumes that the security context is established based on keys derived from a shared initial key provided by the 5GC. In order to prevent unbounded direct communication between ProSe UEs, the initial key and keys derived from it should have a validity time.

### 6.23.2 Solution details

The solution involves the following steps:

1. A shared initial key is provisioned to a selected set of authenticated and authorised ProSe UEs by the 5GC. This initial key has a validity time.

NOTE 1: The provisioning of the shared initial key can occur when ProSe UEs are authenticated/authorized or when ProSe UEs request access to perform ProSe direct communication.

Editor’s Note: Whether the initial key lifetime is same as the security context lifetime of a PC5 communication link is ffs.

2. As long as the initial key is valid, it can be used to derive keys needed for the security context. This security context enables establishment of a secure link between ProSe UEs with confidentiality and integrity protection.

NOTE 2: Derivation of keys from initial key can take place even when the ProSe UEs are outside the coverage area.

3. Upon expiration of the intial key, all keys derived from it will become invalid. In order to continue secure communication ProSe UEs need to request for a new initial key from the 5GC.

Editor’s Note: The behaviour of this solution if validity expires when the ProSe UEs are out-of-coverage is FFS.

### 6.23.3 Evaluation

TBD

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

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

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

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

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions.

Annex <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-08 | SA3#100e | S3-201804 |  |  |  | Skeleton | 0.0.0 |
| 2020-08 | SA3#100e | S3-202145 |  |  |  | S3-201804, S3-202144, S3-201826, S3-201756, S3-202129, S3-201757, S3-202130, S3-202147, S3-201616, S3-202157, S3-202146, S3-201618, S3-202064, S3-202066, S3-202065, S3-202067 implemented | 0.1.0 |
| 2020-09 |  |  |  |  |  | Wrong version of the specification was uploaded to the 3GU Portal | 0.1.1 |
| 2020-10 | SA3#100bis-e | S3-202775 |  |  |  | S3-202381, S3-202472, S3-202666, S3-202754, S3-202755, S3-202705, S3-202706, S3-202763, S3-202673, S3-202773, S3-202774, S3-202708, S3-202713, S3-202689, S3-202780, S3-202769, S3-202700, S3-202701, S3-202683, S3-202684, S3-202714 implemented | 0.2.0 |
| 2020-11 | SA3#101-e | S3-203459 |  |  |  | S3-203358, S3-203362, S3-203369, S3-203351, S3-203425, S3-203426, S3-203430, S3-203431, S3-203448, S3-203015, S3-203016, S3-203440, S3-203019, S3-203432, S3-203442, S3-203462, S3-203416, S3-203417, S3-203418, S3-203373, S3-203341, S3-203391, S3-203307, S3-203340, S3-203396, S3-203334 implemented | 0.3.0 |