|  |  |
| --- | --- |
| 3GPP TR 33.847 V0.2.0 (2020-10) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Security Aspects of Enhancement for Proximity Based Services in 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 6

Introduction 7

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 9

3.1 Definitions 9

3.2 Abbreviations 9

4 Security Aspects of 5G ProSe 9

4.1 Architecture assumption 9

4.1.1 Control Plane based architecture for Direct Discovery 9

4.2.1 User Plane based architecture for Direct Discovery 10

5 Key issues 11

5.1 Key Issue #1: Discovery message protection 11

5.1.1 Key issue details 11

5.1.2 Security threats 11

5.1.3 Potential security requirements 11

5.2 Key Issue #2: Keys in ProSe discovery scenario 12

5.2.1 Key issue details 12

5.2.2 Security threats 12

5.2.3 Potential security requirements 12

5.3 Key Issue #3: Security of UE-to-Network Relay 12

5.3.1 Key issue details 12

5.3.2 Security threats 13

5.3.3 Potential security requirements 13

5.4 Key issue #4: Authorization in the UE-to-Network relay scenario 14

5.4.1 Key issue details 14

5.4.2 Security threats 14

5.4.3 Potential security requirements 14

5.5 Key Issue #5: Privacy protection over the UE-to-Network Relay 14

5.5.1 Key issue details 14

5.5.2 Security threats 15

5.5.3 Potential security requirements 15

5.6 Key Issue #6: Integrity and confidentiality of information over the UE-to-UE Relay 15

5.6.1 Key issue details 15

5.6.2 Security threats 15

5.6.3 Potential security requirements 15

5.7 Key issue #7: Authorization in the UE-to-UE relay scenario 16

5.7.1 Key issue details 16

5.7.2 Security threats 16

5.7.3 Potential security requirements 16

5.8 Key Issue #8: Privacy of information over the UE-to-UE Relay 16

5.8.1 Key issue details 16

5.8.2 Security threats 16

5.8.3 Potential security requirements 17

5.9 Key Issue #9: Key management in 5G Proximity Services for UE-to-Network relay communication 17

5.9.1 Key issue details 17

5.9.2 Security threats 18

5.9.3 Potential security requirements 18

5.10 Key Issue #10: Key issue on secure data transfer between UE and 5GDDNMF 18

5.10.1 Key issue details 18

5.10.2 Security threats 18

5.10.3 Potential requirements 18

5.11 Key Issue #11: UE identity protection during ProSe discovery 19

5.11.1 Key issue details 19

5.11.2 Security threats 19

5.11.3 Potential security requirements 19

5.12 Key Issue #12: Security of one-to-one communication over PC5 19

5.12.1 Key issue details 19

5.12.2 Security threats 19

5.12.3 Potential security requirements 20

5.13 Key Issue #13: Security and privacy of groupcast communication 20

5.13.1 Key issue details 20

5.13.2 Security threats 20

5.13.3 Potential security requirements 21

5.14 Key Issue #14: security for support of Non-IP traffic 21

5.14.1 Key issue details 21

5.14.2 Security threats 21

5.14.3 Potential security requirements 21

5.15 Key Issue #15: privacy of ProSe entities while supporting Non-IP traffic 22

5.15.1 Key issue details 22

5.15.2 Security threats 22

5.15.3 Potential security requirements 22

5.X Key Issue #X: <Key Issue Name> 23

5.X.1 Key issue details 23

5.X.2 Security threats 23

5.X.3 Potential security requirements 23

6 Solutions 23

6.0 Mapping of Solutions to Key Issues 23

6.1 Solution #1: Solution for key management in 5G Proximity Services relay communication 23

6.1.1 Introduction 23

6.1.2 Solution details 23

6.1.3 Evaluation 25

6.2 Solution #2: Secure data transfer between UE and 5GDDNMF 26

6.2.1 Introduction 26

6.2.2 Solution details 26

6.2.3 Evaluation 26

6.3 Solution #3: Reuse LTE security mechanism for 5G ProSe open discovery 27

6.3.1 Introduction 27

6.3.2 Solution details 27

6.3.3 Evaluation 29

6.4 Solution #4: Reuse LTE security mechanism for 5G ProSe restricted discovery 29

6.4.1 Introduction 29

6.4.2 Solution details 30

6.4.2.1 Model A restricted discovery 30

6.4.2.2 Model B restricted discovery 31

6.4.3 Evaluation 33

6.5 Solution #5: Protection of the PC3 interface using AKMA and TLS 34

6.5.1 Introduction 34

6.5.2 Solution details 34

6.5.3 Evaluation 35

6.6 Solution #6: Key management for UE-to-Network Relays and Remote UE’s 35

6.6.1 Introduction 35

6.6.2 Solution details 35

6.7 Solution #7: Security establishment of one-to-one PC5 communication 38

6.7.1 Solution overview 38

6.7.2 Solution details 38

6.7.3 Solution evaluation 39

6.8 Solution #8: Confidential protection against UE-to-UE relay using asymmetric cryptography 39

6.8.1 Introduction 39

6.8.2 Solution details 40

6.8.2.1 Procedure 40

6.8.3 Solution Evaluation 41

6.9 Solution #9: Key management in discovery procedure 41

6.9.1 Solution overview 41

6.9.2 Solution details 41

6.9.3 Solution evaluation 41

6.10 Solution #10: Authorization and security with UE-to-Network relay using Remote UE network primary authentication 41

6.10.1 Solution overview 41

6.10.2 Solution details 42

6.10.3 Solution evaluation 44

6.Y Solution #Y: <Solution Name> 44

6.Y.1 Introduction 44

6.Y.2 Solution details 45

6.Y.3 Evaluation 45

7 Conclusions 45

Annex <X> (informative): Change history 45

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

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

# Foreword

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

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

The technical report to study the security and privacy aspects of proximity based services (including public safety and commercial proximity services) in 5G system and ensure the security solutions are aligned with the work in SA2 (i.e. in TR 23.752 [2]) and SA1 (i.e. in TS 22.278 [3] and TS 22.261 [4]). The work is comprised of the following parts:

* Study the security and privacy key issues, threats and requirements of proximity based services in 5G system.
* Elaborate on the potential security solutions to cover these requirements.

Both non-roaming and roaming scenarios will be 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".

# 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

### The following clauses describe the control plane based and user plane based architecture for supporting 5G ProSe Direct Discovery.4.1.1 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 discoverying 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 the that particular Prose service.

An attacker may impersonate the discoveree or the discovered UE.

A malicious application running on 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 5G GBA is being addressed. 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 shall be assured by the Remote UE. On the contrary, whether the UE can play the remote UE role shall 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.

### 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.

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

## 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 shall 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 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

### 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.

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

## 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.

SA2 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, Rel-16 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 broadcastes 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.

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

Editor’s Note: it’s FFS whether this KI covers the out-of-coverage scenario.

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. During the 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.

### 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.

Editor’s Note: The validity and refresh mechanism of the security context are FFS.

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.

## 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 [1] 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 address support of NoN-IP traffic and require security and privacy protection that they provide to be studied in TR 33.847.

### 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 [1] 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 address support of NoN-IP traffic and require security and privacy protection that they provide to be studied in TR 33.847.

### 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.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 |
| 1 |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| 3 | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| 6 |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| 8 |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |
| 9 |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  | X | X |  |  |  |  | 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 shall be 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.

Editor’s note: It is FFS how this solution will perform out of coverage.

Editor’s note: How to derive the discovery key is FFS.

Editor’s note: Whether this solution based on CP or UP is FFS.

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

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.
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).
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.
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.
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 shall check the MIC is valid.
14. The DDNMF in the HPLMN of the announcing UE shall 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 announcing UE checks the MIC and acknowledges the check result to the DDNMF in the HPLMN of 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 is FFS how this solution will perform out of coverage.

Editor’s note: It’s FFS how this mechanism can be used in UE-to-Network and UE-to-UE relay discovery scenarios.

Editor’s note: How to derive the discovery key is FFS.

Editor’s note: Whether this solution based on CP or UP is FFS.

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

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

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 shall 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 shall 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.

Editor’s Note: It’s FFS how to protection the privacy of entities during one-to-one communication over PC5.

### 6.7.3 Solution evaluation

TBC

## 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 shall 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

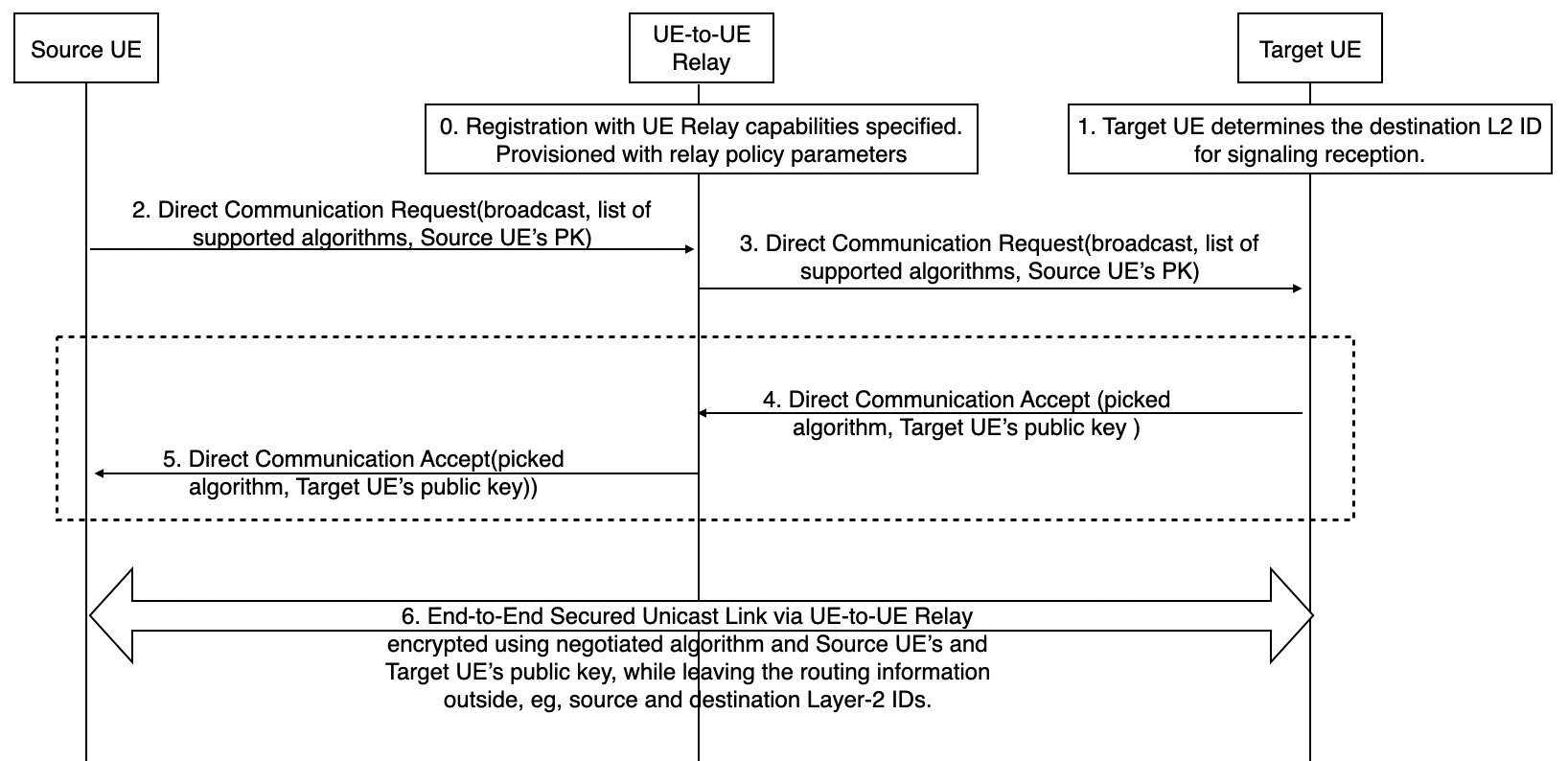


Figure 6.8.2.1-1. Security protection via UE-to-UE Relay using asymmetric cryptographyThe connection establishment procedure is based on TR 23.752, Clause 6.9. However, the seucirty procedure below is not limited to one connection establishment procedure defined in SA2.

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 clause 5.6.1.4. The destination Layer-2 ID is configured with the target UEs as specified in TS 23.287 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 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 shall 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 Solution 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.

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 user plane. 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.

Editor’s Note: What protocol is used between UE and 5G DDNMF and how to secure the protocol are FFS.

### 6.9.3 Solution evaluation

TBD

## 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.

### 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].

Editor's note: Details for how a Remote UE that is already authenticated and authorized reconnects for relay communication are 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.

Editor’s Note: Whether and how the AMF serving the Relay UE always be able to serve the remote UE is FFS.

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.

Editor's note: How the AMF and Relay UE determines whether the authentication messages are for to the Remote 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 1: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 shall 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.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, S3-202067implemented | 0.1.0 |
| 2020-09 |  |  |  |  |  | Wrong version of the specification was uploaded to the 3GU Portal | 0.1.1 |
| 2020-10 | SA3#100bis-e | S3-202145 |  |  |  | implemented | 0.2.0 |