|  |  |
| --- | --- |
| 3GPP TR 33.847 V0.8.0 (2021-10) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of enhancement for proximity based services in the 5G System (5GS)  (Release 17) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 9

Introduction 10

1 Scope 11

2 References 11

3 Definitions of terms, symbols and abbreviations 12

3.1 Definitions 12

3.2 Abbreviations 12

4 Security Aspects of 5G ProSe 12

4.1 Architecture assumption 12

4.1.1 Introduction 12

4.1.2 Control Plane based architecture for direct discovery 12

4.1.3 User Plane based architecture for direct discovery 13

5 Key issues 14

5.1 Key Issue #1: Discovery message protection 14

5.1.1 Key issue details 14

5.1.2 Security threats 14

5.1.3 Potential security requirements 14

5.2 Key Issue #2: Keys in ProSe discovery scenario 14

5.2.1 Key issue details 14

5.2.2 Security threats 15

5.2.3 Potential security requirements 15

5.3 Key Issue #3: Security of UE-to-Network Relay 15

5.3.1 Key issue details 15

5.3.2 Security threats 16

5.3.3 Potential security requirements 16

5.4 Key issue #4: Authorization in the UE-to-Network relay scenario 16

5.4.1 Key issue details 16

5.4.2 Security threats 17

5.4.3 Potential security requirements 17

5.5 Key Issue #5: Privacy protection over the UE-to-Network Relay 17

5.5.1 Key issue details 17

5.5.2 Security threats 17

5.5.3 Potential security requirements 17

5.6 Key Issue #6: Integrity and confidentiality of information over the UE-to-UE Relay 18

5.6.1 Key issue details 18

5.6.2 Security threats 18

5.6.3 Potential security requirements 18

5.7 Key issue #7: Authorization in the UE-to-UE relay scenario 18

5.7.1 Key issue details 18

5.7.2 Security threats 19

5.7.3 Potential security requirements 19

5.8 Key Issue #8: Privacy of information over the UE-to-UE Relay 19

5.8.1 Key issue details 19

5.8.2 Security threats 19

5.8.3 Potential security requirements 19

5.9 Key Issue #9: Key management in 5G Proximity Services for UE-to-Network relay communication 20

5.9.1 Key issue details 20

5.9.2 Security threats 21

5.9.3 Potential security requirements 21

5.10 Key Issue #10: Key issue on secure data transfer between UE and 5GDDNMF 21

5.10.1 Key issue details 21

5.10.2 Security threats 21

5.10.3 Potential requirements 21

5.11 Key Issue #11: UE identity protection during ProSe discovery 21

5.11.1 Key issue details 21

5.11.2 Security threats 22

5.11.3 Potential security requirements 22

5.12 Key Issue #12: Security of one-to-one communication over PC5 22

5.12.1 Key issue details 22

5.12.2 Security threats 22

5.12.3 Potential security requirements 22

5.13 Key Issue #13: Security and privacy of groupcast communication 23

5.13.1 Key issue details 23

5.13.2 Security threats 23

5.13.3 Potential security requirements 23

5.14 Key Issue #14: security for support of Non-IP traffic 24

5.14.1 Key issue details 24

5.14.2 Security threats 24

5.14.3 Potential security requirements 24

5.15 Key Issue #15: privacy of ProSe entities while supporting Non-IP traffic 24

5.15.1 Key issue details 24

5.15.2 Security threats 25

5.15.3 Potential security requirements 25

5.16 Key Issue #16: Privacy protection of PDU session-related parameters for relaying 25

5.16.1 Key issue details 25

5.16.2 Security threats 26

5.16.3 Potential security requirements 26

5.17 Key Issue #17: Supporting security policy handling for PC5 connection of 5G ProSe services 26

5.17.1 Key issue details 26

5.17.2 Security threats 27

5.17.3 Potential security requirements 27

5.X Key Issue #X: <Key Issue Name> 27

5.X.1 Key issue details 27

5.X.2 Security threats 27

5.X.3 Potential security requirements 27

6 Solutions 27

6.0 Mapping of Solutions to Key Issues 28

6.1 Solution #1: Solution for key management in 5G Proximity Services relay communication 29

6.1.1 Introduction 29

6.1.2 Solution details 29

6.1.3 Evaluation 32

6.2 Solution #2: Secure data transfer between UE and 5GDDNMF 32

6.2.1 Introduction 32

6.2.2 Solution details 32

6.2.3 Evaluation 33

6.3 Solution #3: Reuse LTE security mechanism for 5G ProSe open discovery 33

6.3.1 Introduction 33

6.3.2 Solution details 33

6.3.3 Evaluation 36

6.4 Solution #4: Reuse LTE security mechanism for 5G ProSe restricted discovery 36

6.4.1 Introduction 36

6.4.2 Solution details 36

6.4.2.1 Model A restricted discovery 36

6.4.2.2 Model B restricted discovery 38

6.4.3 Evaluation 41

6.5 Solution #5: Protection of the PC3 interface using AKMA and TLS 42

6.5.1 Introduction 42

6.5.2 Solution details 42

6.5.3 Evaluation 44

6.6 Solution #6: Key management for UE-to-Network Relays and Remote UE’s 44

6.6.1 Introduction 44

6.6.2 Solution details 44

6.6.3 Evaluation 47

6.7 Solution #7: Security establishment of one-to-one PC5 communication 48

6.7.1 Solution overview 48

6.7.2 Solution details 48

6.7.3 Evaluation 49

6.8 Solution #8: Confidential protection against UE-to-UE relay using asymmetric cryptography 50

6.8.1 Introduction 50

6.8.2 Solution details 50

6.8.2.1 Procedure 50

6.8.3 Evaluation 51

6.9 Solution #9: Key management in discovery procedure 51

6.9.1 Introduction 51

6.9.2 Solution details 51

6.9.3 Evaluation 52

6.10 Solution #10: Authorization and security with UE-to-Network relay using Remote UE network primary authentication 52

6.10.1 Introduction 52

6.10.2 Solution details 52

6.10.2.1 Connection with UE-to-Network relay using Remote UE network primary authentication via the UE-to-Network relay 52

6.10.2.2 Connection with UE-to-Network relay using the 5G native security context of the Remote UE 54

6.10.2.3 Key hierarchy, key derivation, and distribution 57

6.10.2.4 Remote UE authorization revocation/re-authentication 58

6.10.3 Evaluation 59

6.11 Solution #11: Protection of the PC3 interface using GBA 60

6.11.1 Introduction 60

6.11.2 Solution details 60

6.11.3 Evaluation 60

6.12 Solution #12: Privacy handling for Layer-3 UE-to-UE Relay based on IP routing 60

6.12.1 Introduction 60

6.12.2 Solution details 61

6.12.3 Evaluation 62

6.13 Solution #13: Secondary Authentication for a Layer 3 Remote UE 62

6.13.1 Introduction 62

6.13.2 Solution details 63

6.13.2.1 Secondary Authentication after PC5 link setup 63

6.13.2.2 Secondary Authentication before PC5 link setup 65

6.13.3 Evaluation 66

6.14 Solution #14: A security solution for UE-to-Network Relay based on Layer 2 Relay 67

6.14.1 Introduction 67

6.14.2 Solution details 67

6.14.3 Evaluation 68

6.15 Solution #15: Key management in UE-to-Network Relay based on primary authentication 68

6.15.1 Introduction 68

6.15.2 Solution details 69

6.15.2.1 Procedure 69

6.15.2.2 Derivation of P-TID 70

6.15.3 Solution Evaluation 71

6.16 Solution #16: Security establishment procedures between two UEs in the UE-to-UE relay scenario 71

6.16.1 Introduction 71

6.16.2 Solution details 71

6.16.3 Evaluation 72

6.17 Solution #17: Solution on securely creating destination Layer-2 ID in groupcast communication 72

6.17.1 Introduction 72

6.17.2 Solution details 72

6.17.3 Evaluation 73

6.18 Solution #18: Authorization and PC5 link setup for UE-to-Network relay 73

6.18.1 Introduction 73

6.18.2 Solution details 74

6.18.3 Evaluation 76

6.19 Solution #19: End-to-end security for the L3 UE-to-Network relay 76

6.19.1 Introduction 76

6.19.2 Solution details 76

6.19.2.1 Procedure 76

6.19.2.2 Protocol Stack 77

6.19.3 Evaluation 78

6.20 Solution #20: PC5 link setup for UE-to-UE relay 78

6.20.1 Introduction 78

6.20.2 Solution details 78

6.20.3 Evaluation 79

6.21 Solution #21: 5G PKMF for key management in PC5 communication 79

6.21.1 Introduction 79

6.21.2 Solution details 80

6.21.3 Evaluation 84

6.22 Solution #22: Representation of identities during broadcast 86

6.22.1 Introduction 86

6.22.2 Solution details 86

6.22.2.1 Solution for Model A 86

6.22.2.2 Solution for Model B 88

6.22.3 Evaluation 89

6.23 Solution #23: Initial key with validity time 90

6.23.1 Introduction 90

6.23.2 Solution details 90

6.23.2.1 Overview 90

6.23.2.2 Procedures 90

6.23.3 Evaluation 92

6.24 Solution #24: NSSAA for Remote UE with L3 UE-to-Network relay 93

6.24.1 Introduction 93

6.24.2 Solution details 93

6.24.2.1 PC5 link establishment with L3 UE-to-Network relay to use an S-NSSAI subject to NSSAA 93

6.24.2.2 NSSAA of Remote UE connecting via L3 UE-to-Network relay 96

6.24.2.3 AAA-S triggered Authorization Revocation to use S-NSSAI for Remote UE 97

6.24.2.4 AAA-S triggered Authorization Revocation to use S-NSSAI for Relay UE 98

6.24.3 Evaluation 100

6.25 Solution #25: Secondary authentication of Remote UE with L3 UE-to-Network relay 100

6.25.1 Introduction 100

6.25.2 Solution details 100

6.25.2.1 PC5 link establishment with L3 UE-to-Network relay to use a PDU Session subject to secondary A&A 100

6.25.2.2 PDU Session secondary A&A of Remote UE via L3 UE-to-Network relay 102

6.25.2.3 DN-AAA triggered PDU Session Authorization Revocation for Remote UE 103

6.25.2.4 DN-AAA triggered PDU Session Re-Authentication/Authorization for Remote UE 104

6.25.3 Evaluation 105

6.26 Solution #26: Protecting PDU session-related parameters for L2 relay with existing mechanism 106

6.26.1 Introduction 106

6.26.2 Solution details 106

6.26.3 Evaluation 107

6.27 Solution #27: Mitigating the conflict between security policies using match report procedures 107

6.27.1 Introduction 107

6.27.2 Solution details 107

6.27.2.1 Open discovery scenario 107

6.27.2.2 Restricted discovery scenario 109

6.27.3 Evaluation 110

6.28 Solution #28: Mitigating the conflict between security policies using restricted discovery procedures on network side 110

6.28.1 Introduction 110

6.28.2 Solution details 110

6.28.3 Evaluation 112

6.29 Solution #29: Security flow for Layer-3 UE-to-Network Relay 112

6.29.1 Introduction 112

6.29.2 Solution details 113

6.29.3 Evaluation 114

6.30 Solution #30: UE-to-Network Relay security based on primary authentication 115

6.30.1 Introduction 115

6.30.2 Solution details 115

6.30.3 Evaluation 117

6.31 Solution #31: Use of authorization tokens in UE-to-UE relay 118

6.31.1 Introduction 118

6.31.2 Solution details 118

6.31.3 Evaluation 121

6.32 Solution #32: Mitigating privacy issues of relay service codes and PDU parameters for L3 UE-to-NW relays 121

6.32.1 Introduction 121

6.32.2 Solution Details 122

6.32.3 Evaluation 126

6.33 Solution #33: Security establishment of one-to-one PC5 communication rekeying 127

6.33.1 Introduction 127

6.33.2 Solution Details 128

6.33.3 Evaluation 129

6.34 Solution #34: Authorization of the remote UE in L3 U2N relay 129

6.34.1 Introduction 129

6.34.2 Solution details 129

6.34.3 Evaluation 129

6.35 Solution #35: Discovery procedures for UE-to-network relays 130

6.35.1 Introduction 130

6.35.2 Solution details 130

6.35.2.1 Commercial applications are dependent on the VPLMNs 130

6.35.2.2 Commercial applications are dependent on the HPLMNs of the relays 131

6.35.3 Evaluation 132

6.36 Solution #36: UE-to-Network Relay security based on AKMA 133

6.36.1 Introduction 133

6.36.2 Solution details 133

6.36.3 Evaluation 135

6.37 Solution #37: Keying procedures for Group Member and Relay discovery: public safety case 135

6.37.1 Introduction 135

6.37.2 Solution details 135

6.37.2.1 Group member discovery case 135

6.37.2.2 Relay discovery case 137

6.38 Solution #38: Mitigating the conflict between security policies using restricted discovery procedures on network side 138

6.38.1 Introduction 138

6.38.2 Solution details 138

6.38.3 Evaluation 139

6.39 Solution #39: Key management in UE-to-Network Relay based on shared key generated during primary authentication 140

6.39.1 Introduction 140

6.39.2 Solution details 140

6.39.2.1 Procedure 140

6.39.2.2 Derivation of P-TID 141

6.39.3 Evaluation 142

6.40 Solution #40: Protection with Security Policies for PC5 Direct Communication 142

6.40.1 Introduction 142

6.40.2 Solution details 142

6.40.2.1 Security policy configuration and provisioning 142

6.40.2.2 Security policy negotiation and enforcement 143

6.40.3 Evaluation 143

6.41 Solution #41: Security protection for 5G ProSe indirect network communication 143

6.41.1 Introduction 143

6.41.2 Solution details 143

6.41.2.1 Framework of security protection for 5G ProSe indirect network communication 143

6.41.2.2 Secure provisioning of UP security policies for 5G ProSe indirect network communication 144

6.41.2.3 Enforcement of UP security policies for 5G ProSe indirect network communication 144

6.41.3 Evaluation 146

6.42 Solution #42: Privacy enhancements during PC5 link setup for UE-to-Network relay 146

6.42.1 Introduction 146

6.42.2 Solution details 146

6.42.2.1 General 146

6.42.2.2 Protection of PRUK ID and RSC over the PC5 interface 147

6.42.2.3 Calculation of message-specific confidentiality keystream 147

6.42.2.4 Calculation of time-hash-bitsequence 148

6.42.3 Evaluation 148

6.43 Solution #43: Improved LTE security mechanism for 5G ProSe restricted discovery to ensure source authentication in out of coverage use cases 148

6.43.1 Introduction 148

6.43.2 Solution details 149

6.43.2.1 Basic idea 149

6.43.2.2 Message flows for restricted discovery model A 150

6.43.2.3 Applicability to restricted discovery mode B 151

6.43.3 Evaluation 151

6.Y Solution #Y: <Solution Name> 151

6.Y.1 Introduction 151

6.Y.2 Solution details 151

6.Y.3 Evaluation 151

7 Conclusions 151

7.1 Key Issue #1: Discovery message protection 151

7.2 Key Issue #2: Keys in ProSe discovery scenario 151

7.3 Key Issue #3: Security of UE-to-Network Relay 151

7.4 Key issue #4: Authorization in the UE-to-Network relay scenario 153

7.5 Key Issue #5: Privacy protection over the UE-to-Network Relay 153

7.6 Key Issue #6: Integrity and confidentiality of information over the UE-to-UE Relay 153

7.7 Key issue #7: Authorization in the UE-to-UE relay scenario 153

7.8 Key Issue #8: Privacy of information over the UE-to-UE Relay 153

7.9 Key Issue #9: Key management in 5G Proximity Services for UE-to-Network relay communication 154

7.10 Key Issue #10: Key issue on secure data transfer between UE and 5GDDNMF 154

7.11 Key Issue #11: UE identity protection during ProSe discovery 154

7.12 Key Issue #12: Security of one-to-one communication over PC5 154

7.13 Key Issue #13: Security and privacy of groupcast communication 155

7.14 Key Issue #14: security for support of Non-IP traffic 155

7.15 Key Issue #15: privacy of ProSe entities while supporting Non-IP traffic 155

7.16 Key Issue #16: Privacy protection of PDU session-related parameters for relaying 155

7.17 Key Issue #17: Supporting security policy handling for PC5 connection of 5G ProSe services 155

Annex <X> (informative): Change history 156

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

# 1 Scope

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

* Security and privacy key issues, threats and potential requirements of proximity based services in 5G system.
* Potential security solutions to cover these potential requirements.

Both roaming and non-roaming scenarios are considered.

# 2 References

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

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

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

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

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

[2] 3GPP TR 23.752: "Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS)".

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

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

[5] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

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

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

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

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

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

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

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

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

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

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

[16] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[17] 3GPP TS 23.503: " Policy and charging control framework for the 5G System (5GS); Stage 2".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Definitions

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

**5G ProSe UE-to-Network Relay:** A UE that provides functionality to support connectivity to the network for Remote UE(s).

## 3.2 Abbreviations

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

5GC 5G Core

ProSe Proximity-based Services

5G DDNMF 5G Direct Discovery Name Management Function

AF Application Function

AMF Access and Mobility Management Function

AS layer Access Stratum layer

NG Next Generation

NG-RAN Next Generation RAN

NGAP NG Application Protocol

NR New Radio (5G)

PCF Policy Control Function

RAN Radio Access Network

RAT Radio Access Technology

REAR Remote UE Access via Relay UE

UDM Unified Data Management

# 4 Security Aspects of 5G ProSe

Editor’s Note: This clause contains a high-level overview of the 5G ProSe features, the security aspects and the potential impacts on the current Rel-17 security mechanisms.

## 4.1 Architecture assumption

### 4.1.1 Introduction

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

### 4.1.2 Control Plane based architecture for direct discovery

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



Figure 4.1.2-1: Control Plane based architecture

In Figure 4.1.2-1, 5G DDNMF is introduced into 5GC as a new network function. 5G DDNMF has similar functions from an 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 the NAS message to get discovery parameters for open discovery or restricted discovery.

### 4.1.3 User Plane based architecture for direct discovery

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



Figure 4.1.3-1: User Plane based architecture

In Figure 4.1.3-1, 5G DDNMF is introduced into 5GC as a new network function. 5G DDNMF has similar functions from an 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.

### 5.1.2 Security threats

In case of open discovery, if the discovery messages are not integrity protected and anti-replay protected, the discovery parameters (e.g. ProSe Application ID, Source Layer-2 ID, Prose APP Code) can be intercepted, removed, modified, or replayed by an attacker. The announcing UE may connect with a UE that is not interested in that particular Prose service or fail to connect with any monitoring UE, which is a form of DoS attack.

In case of restricted discovery, if the discovery messages are not integrity protected and anti-replay protected, the discovery parameters (e.g. User Info ID, ProSe Restricted Code, ProSe Query Code, ProSe Response Code) can be intercepted, removed, modified, or replayed by an attacker. Consequently, the announcing/discoverer UE may connect with a monitoring/discoveree UE that is expecting a different ProSe service or fail to connect with any monitoring/discoveree UE, which is a form of DoS attack. If the discovery messages are not confidentiality protected, the privacy sensitive parameter (e.g. User Info ID, ProSe Restricted Code) can be eavesdropped on by an attacker, hence the privacy of announcing/discoverer UE is violated.

If the authenticity of the discovery message cannot be verified, an attacker can impersonate the discoveree or the discover UE.

### 5.1.3 Potential security requirements

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

The discovery messages 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.

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

### 5.2.1 Key issue details

In TS 33.303[6], the Prose Function sends a 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 the Prose Function are split into different network functions along with different network architecture approaches. Meanwhile, AKMA has been defined in TS 33.535[7], and GBA is under study to adapt to the 5G system. The elements above have to be considered to calculate and share discovery key(s) to UEs in 5G Prose.

Following issues need to be addressed in this key issue:

- Which network function derives the discovery key.

- How to send the keys to the UEs.

- Provisioning of keys to support discovery when the UE is out of coverage.

### 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 direct network communication or indirect network communication as showing in figure 5.3.1-1. Path #1 is a direct network communication path and 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 the 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 a 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 use cases. 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 e.g., police or government. When a UE-to-Network Relay is used in a 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 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 proper authorisation, unauthorised entities will be able to access 5GC via UE-to-Network Relay or act as UE-to-Network Relays creating a vulnerability and causing possible (D)DOS attacks or leading to unauthorised service usage on both 5GS and UE-to-Network Relay.

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

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

*…*

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

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

In addition, the following aspects of 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 messages 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 the authorisation of the UE as a UE-to-Network relay in the UE-to-Network relay scenario.

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

Path switch between UE-to-Network Relay UEs is a new feature aiming to preserve user experience. Such preservation may be achieved by making certain elements (e.g., IP addresses) of user experience persistent across sessions and UE-to-Network Relays. Persistent parameters may leak unique attributes associated with UEs and other ProSe entities and allow privacy attacks on these entities (e.g., UEs).

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

### 5.5.3 Potential security requirements

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

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

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

### 5.6.1 Key issue details

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

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

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

### 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 a unicast link with the source UE, as well as the target UE may conduct an MITM attack.

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

### 5.6.3 Potential security requirements

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

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

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

### 5.7.1 Key issue details

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

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

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

*- Authorize the Remote UE to access a UE-to-UE Relay?*

*…*

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

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

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

### 5.7.2 Security threats

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

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

### 5.7.3 Potential security requirements

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

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

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

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

### 5.8.1 Key issue details

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

TR 23.752 [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 security protection for relayed connections?*

### 5.8.2 Security threats

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

The existing Link identifier update procedure specified in TS 33.536 [8] provides privacy of the identities on a per unicast link basis (e.g., the link between a UE and the UE-to-UE Relay). Therefore an attacker may be able to link identities exchanged over the link between a UE and the UE-to-UE Relay to those exchanged over the corresponding link between the peer UE and the UE-to-UE Relay

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

### 5.8.3 Potential security requirements

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

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

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

### 5.9.1 Key issue details

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

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

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

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

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



Figure 5.9.1-1: User Plane architecture for ProSe

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

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

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

### 5.9.2 Security threats

Following are the possible threats

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

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

- Impersonation of the remote UE by the relay UE.

### 5.9.3 Potential security requirements

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

- 5GS shall support the 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 the issue with secure communication between UE and the 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 with 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 UE.

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

### 5.11.3 Potential security requirements

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

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

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

### 5.12.1 Key issue details

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

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. The architecture study in the TR 23.752 [2] proposes to introduce new features to 5G ProSe from 5G V2X, this may potentially reuse the security mechanisms 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 the 5G V2X scenario 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 to the 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 UEs 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 the one-to-one communication (unicast) mechanism in 5G V2X is reused, an attacker may deploy a bidding-down attack to force establishing an unprotected connection between initiating UE and peer UE.

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

### 5.12.3 Potential security requirements

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

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

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

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

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

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

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

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

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

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

### 5.13.1 Key issue details

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

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

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

Thus far solutions #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 inquire whether any member of a certain group is present 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 have 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 groupcast communications, 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., integrity and confidentiality) while supporting Non-IP traffic. Failure to protect integrity and confidentiality of information while supporting Non-IP traffic will open vulnerability in 5GS and allow attacks such as unauthorised disclosure and modification of information.

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

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

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

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

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

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

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

*- DHCPv4 based IP address allocation is supported.*

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

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

### 5.14.2 Security threats

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

### 5.14.3 Potential security requirements

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

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

### 5.15.1 Key issue details

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

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

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

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

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

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

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

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

*- DHCPv4 based IP address allocation is supported.*

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

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

### 5.15.2 Security threats

Failure to protect the 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 the privacy of entities and identities while supporting NoN-IP unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays.

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

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

## 5.16 Key Issue #16: Privacy protection of PDU session-related parameters for relaying

### 5.16.1 Key issue details

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

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

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

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

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

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

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

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

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

For Layer-2 relays transparently forwarding all RRC/NAS messages between the remote UE and the network, although the PDU session request containing privacy-sensitive information (e.g. requested NSSAI, requested DNN) is protected by NAS and AS security established between the remote UE and the network, the use of confidentiality protection of signalling messages is, however, a configuration option. Hence it is still possible that the information may be exposed in clear text if NAS/AS signalling confidentiality is not activated. This is an existing issue not related to the Layer-2 relay.

### 5.16.2 Security threats

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

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

### 5.16.3 Potential security requirements

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

## 5.17 Key Issue #17: Supporting security policy handling for PC5 connection of 5G ProSe services

### 5.17.1 Key issue details

User-plane security policy provisioning and enforcement for PDU sessions is a new feature in 5GS. This security policy handling feature is extended to 5G V2X in one-to-one communication (i.e. unicast).

To align with the security policy handling in 5GS, 5G V2X one-to-one communication specifies the handling of the security policy provisioned by the PCF in TS 33.536 [8]. Due to the similarity of service features between ProSe services and V2X services, it is deemed necessary for 5GS to be able to provision and enforce security policies of PC5 in 5G ProSe scenarios.

This key issue is to study how to support security policy handling in 5G ProSe, including security policy provisioning and security enforcement based on the provisioned security policies.

### 5.17.2 Security threats

Without secure provisioning of PC5 security policies for 5G ProSe services, PC5 connections can be downgraded or cannot be set up.

Without negotiation on security policies over PC5 connection for security enforcement,

* PC5 communication may fail
* Or PC5 communication may fail to meet the security requirements of various 5G ProSe services

### 5.17.3 Potential security requirements

5G ProSe system shall support a means to configure PC5 security policies for 5G Prose services at the network.

5G ProSe system shall support a means to securely provision the configured PC5 security policies to the UE for 5G Prose services.

5G ProSe system shall support negotiation on the provisioned PC5 security policies for security enforcement by the UEs to meet security requirements of 5G Prose Services.

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

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

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

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Key Issues | | | | | | | | | | | | | | | | |
| Solutions | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 1 |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |
| 3 | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |
| 6 |  |  |  | X |  |  |  |  | X |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| 8 |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| 9 |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  | X | X | X |  |  |  | X |  |  | X |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |
| 13 |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 14 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 15 |  |  | X | X |  |  |  |  | X |  |  |  |  |  |  |  |  |
| 16 |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| 17 |  |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |
| 18 |  |  | X | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 19 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 20 |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| 21 |  |  |  | X |  |  |  |  | X |  |  |  |  |  |  |  |  |
| 22 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |
| 23 |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| 24 |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 25 |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 26 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | X |  |
| 27 | X |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| 28 | X |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| 29 |  |  | X | X |  |  |  |  | X |  |  |  |  |  |  |  |  |
| 30 |  |  | X | X |  |  |  |  | X |  |  |  |  |  |  |  |  |
| 31 |  |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |
| 32 |  |  |  |  | X |  |  |  |  |  | X |  |  |  |  | X |  |
| 33 |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| 34 |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 35 |  | X |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |
| 36 |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 37 | X | X |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 38 | X |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| 39 |  |  | X | X |  |  |  |  | X |  |  |  |  |  |  |  |  |
| 40 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | X |
| 41 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 42 |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |
| 43 | 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 the proposed solution the PCF provisions the UE with necessary policies and parameters to use 5G ProSe services, as part of the UE ProSe Policy information as defined in TS 23.503 [17] clause 4.2.2. PCF provisions the authorization policy and parameters for 5G UE-to-Network Relay Discovery and Communication and the related discovery security materials are provisioned by 5GDDNMF.



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

Step 1: 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 Npcf\_UEpolicycontrol\_update request over Service based interface to discover the corresponding PCF and requests for the required ProSe authorization policy.

PCF sends back Npcf\_UEpolicycontrol\_update response with the required ProSe authorization policy. AMF delivers the ProSe related policies to the Remote UE.

The UE-to-Network relay gets authenticated and authorized by the network to support as a relay for ProSe communication.

Step 2: The Remote UE sends a key request message to the remote AMF, where the message includes the ProSe Remote access indication and 5G-GUTI if already assigned or the SUCI. This solution is 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.

If SUCI is included in the Key request, the AMF may forward the Key request to the AUSF instance for primary authentication and AUSF may initiate primary authentication and perform required operations.

If 5G-GUTI is included and AMF succeed to verify UE and retrieve the UE context from 5G-GUTI, AMF may proceed to step 3. Otherwise, AMF may forward the Key request to the AUSF for primary authentication.

Step 3: In order to authorize the UE requesting for keys for remote access, the AMF retrieves the UE details or subscription data from UDM.

Step 4: 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 5: The AUSF generates the REAR Key for Remote UE communication via UE-to-Network relay. The 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 long out of which, the 128 bits MSB of the key is the REAR Key and the other 128 bits is the REAR Key ID. The purpose of the REAR Key ID is to identify the REAR key.

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

Step 6-9: 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 AMF. The remote AMF includes the REAR key in the security context of the remote UE. Step 10: Remote UE discovers the relay UE using any of Model A or Model B methods. The discovery message must include the relay UE ID provided by the AUSF.

Step 11: After the discovery of the UE-to-Network relay, the Remote UE sends the Direct communication request to the discovered relay for establishing a secure PC5 unicast link. The message should include Relay Service Code or ServiceID, 5G-GUTI of the Remote UE.

Step 12: On receiving the Direct Communication request, the UE-to-Network relay sends a key request message to the relay AMF along with the Relay Service Code or ServiceID, 5G-GUTI of the Remote UE received from the remote UE.

Step 13-16: Relay AMF authorizes the relay UE and retrieves the ProSe security context if the key request includes 5G-GUTI. The AMF authorizes the remote UE by checking with the UDM and acquires the REAR key through the security context. A restricted security context (only ProSe related security context) transfer is performed between remote AMF and relay AMF to avoid the reallocation of AMF.

Editor's Note: Further details on restricted security context transfer is FFS.

Step 17-18: If the security context retrieval fails, the relay AMF sends a reject message to the remote AMF with an indication to re-try the key request using SUCI. This request is forwarded to the remote UE.

Step 19-24: The Remote UE sends a direct communication request to the relay using the SUCI parameter. Relay UE sends the relay key request to the relay AMF sends, relay AMF authorizes the UE and forwards the key request to the AUSF. The AUSF retrieves the Authentication Vectors from the UDM and triggers primary authentication of remote UE.

Step 25-26: The REAR key is generated at the AUSF same as in step 5. The remote UE and relay AMF acquire the REAR key from the key response message received from AUSF. The relay AMF authorizes the remote UE by checking with the UDM.

Step 27-29: The Relay AMF now generates the KNR\_ProSe key. The input to the KDF for generating the 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. KNR\_ProSe is used as a root key. The Relay UE derives PC5 session key Krelay-sess from KNR-ProSe, and confidentiality and integrity keys from Krelay-sess, in a similar way as KNRP-sess is derived from KNRP, and confidentiality and integrity keys from KNRP-sess in TS 33.536[8].

Step 30: The Relay AMF sends the KNR\_ProSe and freshness parameter in the key response message to the UE-to-Network relay.

Step 31-32: The UE-to-Network relay stores the received KNR\_ProSe and sends the freshness parameter to the Remote UE in the Direct Security Mode command message.

Step 33: The remote UE generates the ProSe key to be used for Remote access via Relay same as defined in step 29. 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: The privacy protection of Remote UE is FFS when its 5G-GUTI is used in DCR.

### 6.1.3 Evaluation

The proposed solution addresses key issue#4 and key issue#9 for key management in ProSe. This solution assumes and require network connectivity for both remote UE and relay UE. The proposed solution supports authorization policy provisioning by PCF as concluded by SA2. Also, this solution may impact more than one key issue. This solution depends on other solutions to be concluded in TR 33.847 for security material provisioning. Therefore, this solution needs to combine with other solutions on security for the discovery of ProSe UEs.

This solution has an impact on both the serving network and the HPLMN. The AUSF has a new role in this solution as a Key Management Function along with the functionality of an authentication server. No new NF is introduced for the key management and the already available key from primary authentication is used. This is a major change to the 5G architecture in Rel-15/Rel-16. It is unclear how the UE-to-network relay discovers the AUSF which holds the latest Kausf key.

Editor’s Note: Further Evaluation is FFS

## 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 a 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 the 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 the conclusion from SA2.

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

However, the security requirements of the 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 for new functionalities is FFS and whether the new functionalities can be used in Ua\* is FFS.

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

### 6.2.3 Evaluation

TBD

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

### 6.3.1 Introduction

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

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

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

NOTE: The security flexibility is addressed in other solutions. (e.g. Solution #27)

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.

### 6.3.2 Solution details

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

The open discovery security procedure is described as follows:

1. The announcing UE sends a Discovery Request message containing the ProSe Application ID to the DDNMF in its HPLMN in order to be allowed to announce a code on its serving PLMN (either VPLMN or HPLMN).
2. If the announcing UE wants to send announcements in the VPLMN, it needs to be authorised from the VPLMN ProSe Function. 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, if authorization is granted. There are no changes to these messages for the purpose of protecting the transmitted code for open discovery. If the Announcing UE is not roaming, these steps do not take place.
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 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).

NOTE 1: The UE may use unprotected time to obtain the UTC-based counter associated with a discovery slot. This means that the discovery message could be successfully replayed if a UE is fooled into using a time different from the current time. The MAX\_OFFSET parameter is used to limit the ability of an attacker to successfully replay discovery messages or obtain correctly MICed discovery message for later use. This is achieved by using MAX\_OFFSET as a maximum difference between the UTC-based counter associated with the discovery slot and the ProSe clock held by the UE.

NOTE 2: A discovery slot is the time at which an announcing UE sends the announcement.

1. 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. The 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.
2. 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.
3. The DDNMF in the HPLMN of the monitoring UE sends Monitor Req. message to the DDNMF in the HPLMN of the announcing.
4. The DDNMF in the HPLMN of the announcing UE sends Monitor Resp. message to the DDNMF in the HPLMN of the monitoring.IfMIC needs to be checked by the DDNMF in the HPLMN of the monitoring UE or the monitoring UE, the Discovery Key should be contained in the response message.
5. 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 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).IfMIC needs to be checked by the monitoring UE, the Discovery Key should be contained in the response message.
6. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter, if the difference between UTC-based counter associated with that discovery slot and UE’s ProSe clock is not greater than the MAX\_OFFSET of the monitoring UE's ProSe clock. If the monitoring UE has the Discovery Key, the MIC check is performed locally, and steps 11 to 15 are omitted.
7. On hearing such a discovery message, and if the UE needs to check the MIC for the discovered ProSe App Code, the Monitoring UE sends a Match Report message to the DDNMF in the HPLMN of the monitoring UE. The Match Report contains the UTC-based counter value with four least significant bits equal to four least significant bits received along with discovery message and nearest to the monitoring UE’s UTC-based counter associated with the discovery slot where it heard the announcement, and other discovery message parameters including the ProSe App Code and MIC. If the DDNMF in the HPLMN of the monitoring UE has the Discovery Key, the MIC check is performed locally, and steps 12 to 14 are omitted.
8. 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.
9. The DDNMF in the HPLMN of the announcing UE should check the MIC is valid. The relevant Discovery Key is found using the ProSe App Code.
10. The DDNMF in the HPLMN of the announcing UE should acknowledge a successful check of the MIC to the DDNMF in the HPLMN of the monitoring UE in the Match Report Ack message. The DDNMF in the HPLMN of the announcing UE includes a Match Report refresh timer in the Match Report Ack message. The Match Report refresh timer indicates how long the UE will wait before sending a new Match Report for the ProSe App Code.
11. The DDNMF in the HPLMN of the monitoring UE acknowledges the check result to the monitoring UE. The DDNMF returns the parameter ProSe Application ID to the UE. It also provides the CURRENT\_TIME parameter, by which the UE (re)sets its ProSe clock The DDNMF in the HPLMN of the monitoring UE may optionally modify the received Match Report refresh timer based on local policy and then include the Match Report refresh timer in the message to the Monitoring UE.



**Figure 6.3.2-1: Open discovery security procedure**

### 6.3.3 Evaluation

This solution supports the integrity protection of the discovery message.

This solution mitigates replay attack against the discovery message.

As defined in TS 23.303 [5], the User Identity, IMSI, is sent in the discovery request message. The proposed solution lacks details on how to protect the discovery request message, especially how to protect IMSI. There could be several solutions that can address IMSI protection (e.g., activation of the ciphering protection for the PC3 interface). Therefore, this solution needs to combine other solutions to make sure that IMSI is not sent in cleartext.

Editor’s Note: Further Evaluation is FFS

## 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.

NOTE: The security flexibility is addressed in other solutions. (e.g. Solution #28)

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.

### 6.4.2 Solution details

#### 6.4.2.1 Model A restricted discovery

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

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

Steps 1-4 refer to an Announcing UE.

1. Announcing UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to get the ProSe Code to announce and to get the associated security material.
2. The DDNMF may check for the announced 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. The Code-Sending Security Parameters provide the necessary information for the Announcing UE to protect the transmission of the ProSe Code and are stored with the ProSe Code. The Announcing UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Announcing UE in step 4 of subclause 6.3.2 of the current specification.

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 User 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). The Code-Receiving Security Parameters provide the information needed by the Monitoring UE to undo the protection applied by the announcing UE. The DUIK be included as a separate parameter if the Code-Receiving Security Parameters indicate that the Monitoring UE uses Match Reports for MIC checking. The DDNMF in the HPLMN of the Monitoring UE stores the ProSe Code and the Discovery User Integrity Key (if it received one outside of the Code-Receiving Security Parameters).

NOTE 1: There are two configurations possible for integrity checking, namely, MIC checked by the DDNMF, and MIC checked at the UE side. Which of the configuration is used is decided by the DDNMF that assigned the ProSe Code being monitored, and signalled to the Monitoring UE in the Code-Receiving Security Parameters.

1. 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. The Monitoring UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Monitoring UE in step 9 of subclause 6.3.2 of the current specification. The UE stores the Discovery Filter and Code-Receiving Security Parameters.

Steps 11 and 12 occur over PC5.

1. The UE starts announcing, if the UTC-based counter provided by the system associated with the discovery slot is within the MAX\_OFFSET of the announcing UE's ProSe clock and if the Validity Timer has not expired. The UE forms the discovery message and protects it. The four least significant bits of the UTC-based counter are transmitted along with the protected discovery message.
2. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter, if the UTC-based counter associated with that discovery slot is within the MAX\_OFFSET of the monitoring UE's ProSe clock. In order to find such a matching message, it processes the message. If the Monitoring UE was not asked to send Match Reports for MIC checking, it stops at this step from a security perspective. Otherwise, it proceeds to step 13.

NOTE 2: The UE checking the integrity of the discovery message on its own does not prevent the UE from sending a Match Report due to requirements in TS 23.303 [5]. If such a Match Report is sent, then there is no security functionality involved.

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

1. If the UE has either not had the DDNMF check the MIC for the discovered ProSe Code previously or the DDNMF has checked a MIC for the ProSe Code and the associated Match Report refresh timer (see step 15 for details of this timer) has expired, then 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 Code and MIC. The DDNMF checks the MIC.
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 acknowledgment that the integrity check passed. It also provides the CURRENT\_TIME parameter, by which the UE (re)sets its ProSe clock. The DDNMF in the HPLMN of the Monitoring UE includes the Match Report refresh timer in the message to the Monitoring UE. The Match Report refresh timer indicates how long the UE will wait before sending a new Match Report for the ProSe Code.
4. The DDNMF in the HPLMN of the Monitoring UE may send a Match Report Info message to the DDNMF in the HPLMN of the Announcing UE.



**Figure 6.4.2.1-1: Model A restricted discovery security procedure**

#### 6.4.2.2 Model B restricted discovery

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

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

Steps 1-4 refer to a Discoveree UE.

1. Discoveree UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to get Discovery Query Filter(s) to monitor a query, the ProSe Response Code to announce and associated security materials. The command indicates that this is for ProSe Response (Model B) operation, i.e. for a Discoveree UE.
2. The DDNMF may check for the announced 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. The Code-Sending Security Parameters provide the necessary information for the Discoveree UE to protect the transmission of the ProSe Response Code and are stored with the ProSe Response Code. The Code-Receiving Security Parameters provide the information needed by the Discoveree UE to undo the protection applied to the ProSe Query Code by the Discoverer UE. The Code-Receiving Security Parameters indicate a Match Report will not be used for MIC checking. The UE stores each Discovery Filter with its associated Code-Receiving Security Parameters. The Discoveree UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Announcing UE in step 4 of subclause 6.3.2 of the current specification.

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 User 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. The Code-Receiving Security Parameters provide the information needed by the Discoverer UE to undo the protection applied by the Discoveree UE. The DUIK be included as a separate parameter if the Code-Receiving Security Parameters indicate that the Discoverer UE uses Match Reports for MIC checking. The DDNMF in the HPLMN of the Discoverer UE stores the ProSe Response Code and the Discovery User Integrity Key (if it received one outside of the Code-Receiving Security Parameters). The Code-Sending Security Parameters provide the information needed by the Discoverer UE to protect the ProSe Query Code.

NOTE 1: There are two configurations possible for integrity checking, namely, MIC checked by the DDNMF, and MIC checked at the UE side; this is decided by the DDNMF that assigned the ProSe Code being monitored, and signalled to the Monitoring UE in the Code-Receiving Security Parameters.

1. 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.
2. 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. The Discoverer UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Monitoring UE in step 9 of subclause 6.3.2 of the current specification. The UE stores the Discovery Response Filter and its Code-Receiving Security Parameters and the ProSe Query Code and its Code-Sending Security Parameters.

Steps 12 to 15 occur over PC5.

1. The Discoverer UE sends the ProSe Query Code and also listens for a response message, if the UTC-based counter provided by the system associated with the discovery slot is within the MAX\_OFFSET of the announcing UE's ProSe clock and if the Validity Timer has not expired. The Discoverer UE forms the discovery message and protects it. The four least significant bits of UTC-based counter are transmitted along with the protected discovery message.
2. The Discoveree UE listens for a discovery message that satisfies its Discovery Filter, if the UTC-based counter associated with that discovery slot is within the MAX\_OFFSET of the Discoverer UE's ProSe clock. In order to find such a matching message, it processes the message.

NOTE 2: Match Reports are not used for the MIC checking of ProSe Query Codes.

1. The Discoveree sends the ProSe Response Code associated with the discovered ProSe Query Code. The Discoveree UE forms the discovery message and protects it. The four least significant bits of UTC-based counter are transmitted along with the protected discovery message.
2. The Discoverer UE listens for a discovery message that satisfies its Discovery Filter. In order to find such a matching message, it processes the message. If the Discoverer UE was not asked to send Match Reports for MIC checking, it stops at this step from a security perspective. Otherwise, it proceeds to step 16.

NOTE 3: The UE checking the integrity of the discovery message on its own does not prevent the UE from sending a Match Report due to requirements in TS 23.303 [5]. If such a Match Report is sent, then there is no security functionality involved.

NOTE 4: The security keys in the Code-Sending Security Parameters of discover UE and the security keys in the Code-Sending Security Parameters of discoveree UE need to be generated independently and randomly. This ensures that the impersonation of the discoveree UE is not feasible when the discoverer UEs make use of match reports.

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

1. If the Discoverer UE has either not had the DDNMF check the MIC for the discovered ProSe Response Code previously or the DDNMF has checked a MIC for the ProSe Response Code and the associated Match Report refresh timer (see step 18 for details of this timer) has expired, then the Discoverer UE sends a Match Report message to the DDNMF in the HPLMN of the Discoverer 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 Response Code and MIC. The DDNMF checks the MIC.
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. It also provides the CURRENT\_TIME parameter, by which the UE (re)sets its ProSe clock. The DDNMF in the HPLMN of the Discoverer UE includes the Match Report refresh timer in the message to the Discoverer UE. The Match Report refresh timer indicates how long the UE will wait before sending a new Match Report for the ProSe Response Code.
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

This solution supports integrity protection, confidentiality protection, and replay protection of the discovery message.

As defined in TS 23.303[5], the User Identity, IMSI, is sent in the discovery request message. The proposed solution lacks details on how to protect the discovery request message, especially how to protect IMSI. There could be several solutions that can address IMSI protection (e.g., activation of the ciphering protection for the PC3 interface). Therefore, this solution needs to combine other solutions to make sure that IMSI is not sent in cleartext.

This solution can ensure source authentication of the discovery messages when match reports are used. Devices that are out of coverage cannot use match reports, and therefore, source authentication is not supported in those applications that involve out of coverage UEs, without risking impersonation attacks due to sharing of the DUIK.

Editor’s Note: Further Evaluation is FFS

## 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 of the AF in AKMA and uses AKMA procedures as defined in TS 33.535 [7] to generate a symmetric key (i.e. KAF) in the UE and the AF.

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

Editor's Note: It is FFS whether other Ua\* protocol profiles may be identified to protect the PC3 interface along with AKMA.

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 an 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 establishes 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 containing 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.

Editor's Note: It is FFS how this solution supports roaming.

### 6.5.3 Evaluation

SA2 has adopted the user plane architecture described in TR 23.752 [2].

This solution resolves key issue #10 and can secure the PC3 interface using AKMA which is specified in TS 33.535 [7] in Rel-17.

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

### 6.6.1 Introduction

This solution describes a 5G PKMF which is an NF (network function) which resides in Remote UE’s HPLMN that is accessed by the Remote UE via user plane (like the 5G DDNMF). The 5G PKMF 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 and key issue #9.

This solution assumes that the Remote UE and the UE-to-network relay belong to the same home PLMN and are accessing the 5G PKMF used for PC5 key management located in HPLMN of Remote UE.

Solution #6 [in step 9] is originally based on solution #1 [in step 6 – MACREAR]  where the Remote UE calculates a message authentication code (MACREAR) over the included ProSe parameters and includes the MACREAR in the Direct Communication Request to the UE-to-network relay. The difference between solution #1 and solution #6 is that the key management for security key used for PC5 communication takes place in the user plane in solution #6 but in solution #1 it takes place in the control plane. Also in solution #1, the key for PC5 communication is generated from Kausf in AUSF, but in solution #6 the generation of the key for PC5 communication in 5G PKMF is out of scope.

The Remote UEs and UE-to-network relay are assumed to be provisioned with the discovery security materials when they are in 3GPP coverage.

The Remote UE needs to connect to the 5G PKMF in HPLMN in order to get a key for PC5 communication, prior to being able to discover and initiate PC5 communication with a UE-to-network relay.

### 6.6.2 Solution details

The Remote UE needs to retrieve the address to the 5G PKMF(s) in its HPLMN 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 provides the 5G PKMF address and the Relay Service Code to the Remote UE. The Remote UE establishes a PDU session with the network.

NOTE 1: SA2 has concluded that PCF provisions the Relay Service Code to the Remote UE.

Step 2) The Remote UE retrieves a discovery key for the discovery of a UE-to-network relay from the network as e.g. is described in solution #35.

Step 3) The Remote UE establishes a secure connection with the 5G PKMF. As this connection is established in the user plane, the same mechanism as used to protect the PC3 interface can be re-used. Either solution #5 or solution #11 can be used for securing the connection.

Step 4) The Remote UE sends a Key request message for PC5 communication with a UE-to-network relay to the 5G PKMF. The Remote UE includes the Relay Service Code and the Remote UE ID in the Key request message.

Editor’s note: It’s FFS whether the Remote UE ID consists of one or more of the following parameters: ProSe application id, ProSe application user id and/or GPSI of the Remote UE.

Step 5) The 5G PKMF generates a KPC5 key and provides the KPC5 key and a KPC5 key ID in the Key response message to the Remote UE to be used for PC5 communication with a UE-to-network relay.

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 retrieves a discovery key for UE-to-network relay discovery from the network as e.g. described in solution #35.

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 5G PKMF.  Different relays do not need to be connected to the same 5G PKMF, 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 the PC5 interface using either model A or model B discovery.

Step 9) When the Remote UE and the UE-to-network relay have discovered each other, the Remote UE sends a Direct Communication Request on the PC5 interface. The Remote UE generates a Nonce\_1. The Remote UE includes the KPC5 key ID received from the 5G PKMF together with Relay Service Code, the Remote UE ID, Nonce\_1 and its HPLMN ID. The Remote UE’s HPLMN ID is used by the UE-to-network relay’s 5G PKMF to determine the 5G PKMF in the Remote UE’s HPLMN. In this message flow, the Remote UE and the UE-to-network relay belong to the same HPLMN. The KPC5 key ID indicates the KPC5 key which the Remote UE wants to use to get relay connectivity. The Remote UE derives a temporary key KPC5-TEMP key from KPC5 key and Nonce\_1 and calculates a message authentication code (MACPC5-TEMP) over the included ProSe parameters using the KPC5-TEMP key and includes the message authentication code (MACPC5-TEMP) in the Direct Communication Request. Additional input parameters could be used in the calculation of the MACPC5-TEMP. This needs to be determined in the normative work.

Step 10) The UE-to-network relay establishes a secure connection with the 5G PKMF. As this connection is established in the user plane, the same mechanism as used to protect the PC3 interface can be re-used. Either solution #5 or solution #11 can be used for securing the connection.

Step 11) The UE-to-network relay sends a Key request message for PC5 communication with a Remote UE to the 5G PKMF, identified by the Remote UE’s HPLMN ID received on the PC5 interface. The Key request message includes the KPC5 key ID, the HPLMN ID of Remote UE, the Relay Service Code, Nonce\_1, the Remote UE ID, the UE-to-network relay ID, and the MACPC5.

Step 12) The 5G PKMF authenticates the Remote UE by verifying the message authentication code (MACPC5) using the KPC5 key identified by the KPC5 key ID and the Nonce-1. The 5G PKMF needs to check that the Nonce-1 is not replayed. The 5G PKMF 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. The 5G PKMF checks if the Remote UE and the UE-to-network relay are allowed to communicate by checking the Remote UE ID and the UE-to-network relay ID. The 5G PKMF may contact UDM to retrieve subscription data if it is not already stored in the 5G PKMF.

Step 13) If the 5G PKMF confirms the Remote UE can connect to the network via the selected ProSe UE-to- network Relay, the 5G PKMF generates a new freshness parameter (i.e. KPC5-COM freshness parameter). The 5G PKMF generates a new key KPC5-COM from at least the KPC5 key, Nonce\_1, Relay Service Code, and the new KPC5-COM freshness parameter. The generation of the KPC5-COM key can be done in a similar way as described in Annex A.7 in TS 33.303 if PRUK is replaced by KPC5 key.

Step 14) The 5G PKMF sends the KPC5-COM key, Remote UE ID and the KPC5-COM freshness parameter to the UE-to-network relay in the Key response message.

Step 14a) The UE-to-network Relay generates a Nonce\_2. The UE-to-network Relay generates the KSESS key for PC5 communication from the KPC5-COM key received from the 5G PKMF and the Nonce\_2.

Step 15) The UE-to-network Relay initiates a Direct Security Mode Command integrity protected with the KSESS-IK key generated from the KSESS key. The UE-to-network Relay calculates a MAC over the parameters included in the Direct Security Mode Complete message.

The UE-to-network Relay includes the KPC5-COM key ID, KPC5-COM freshness parameter together with calculated MAC and the Nonce\_2 in the Direct Security Mode Complete message.

Step 16) The Remote UE derives the KPC5-COM key in the same way as the 5G PKMF in step 13 using the KPC5-COM freshness parameter and then generates the KSESS key from the KPC5-COM key and Nonce\_2.

Step 17-18) The Remote UE processes the Direct Security Mode Command by verifying the MAC using a KSESS-IK key generated from the KSESS key. 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.

### 6.6.3 Evaluation

This solution resolves key issue #4 and key issue #9 and proposes to perform the key management for PC5 communication between the 5G PKMF and the Remote UE/UE-to-network relay over the user plane. The 5G PKMF is an NF located in the Remote UE’s HPLMN.

This solution assumes and requires 3GPP network connectivity for both Remote UE and UE-to-network relay.

The key for PC5 communication is retrieved from the 5G PKMF in the Remote UE’s HPLMN. How the key is generated in the 5G PKMF is out of scope.

The Remote UE provides its HPLMN ID on the PC5 interface to the UE-to-network relay and UE-to-network relay can connect to the 5G PKMF in Remote UE’s HPLMN via the UE-to-network relay’s 5G PKMF. The Remote UE’s HPLMN ID is used by the UE-to-network relay’s 5G PKMF to determine the 5G PKMF in the Remote UE’s HPLMN. In this solution though, the Remote UE and the UE-to-network relay belong to the same HPLMN.

If the Remote UE wants to connect a Relay UE, it means the Remote UE is almost out of coverage of the network, then its FFS how steps 3, 4, and 5 can be performed as this solution may not work when the remote UE is not in 3GPP coverage.

Which network function provides the 5G PKMF address to the Remote UE is still to be decided.

“UE-to-network relay can connect to the 5G PKMF in Remote UE’s HPLMN via the UE-to-network relay’s 5G PKMF” adds a new requirement to the PKMF’s holder which is out of the scope of the 3GPP.

The new changes compared to PKMF in LTE in TS 33.303 are as follows:

* The Remote UE’s HPLMN ID needs to be sent to the 5G PKMF.
* The Remote UE needs to generate the MACpc5temp (i.e. MACREAR ) and the 5G PKMF needs to verify. This seems useless because the Remote UE has been authenticated by 5G PKMF in step 3. And step 10 has established another secure link.

Solution #6 [in step 9] is originally based on solution #1 [in step 6]  where the Remote UE calculates a message authentication code (MACREAR) over the included ProSe parameters and includes the MACREAR in the Direct Communication Request to the UE-to-network relay. In solution #6, the UE-to-network relay forwards the MACPC5-TEMP, received from Remote UE on PC5, to the 5G PKMF in the Remote UE’s HPLMN and the 5G PKMF is able to verify that the Remote UE has the correct key for PC5 communication.

This solution aligns with the key management for the discovery keys for the UE-to-network relay which is also performed over the user plane.

Solution #6 is similar to Solution #21, but differs as described below:

* In Solution #6, the Remote UE calculates a message authentication code (MACREAR) over the included ProSe parameters and includes the MACREAR in the Direct Communication Request to the UE-to-network relay. In Solution #21, no message authentication code (similar to MACREAR) is included in the Direct Communication Request.
* In Solution #6, the Remote UE and UE-to-network relay belongs to the same HPLMN. In Solution #21, the Remote UE and UE-to-network relay belongs to different HPLMN’s.

Editor’s note: Further evaluations of impact on PC5 link security establishment are FFS.

This solution has no impact on network nodes as RAN, AMF, and AUSF.

This solution has an impact on the NF (network function) - 5G PKMF and potentially UDM.

SA2 has not defined the network function 5G PKMF in the architecture for the UE-to-network relay scenario as proposed in this solution, as SA2 does not define PKMF in LTE. The 5G PKMF could interact with the UDM and 5G DDNMF via SBI.

In LTE, the PKMF is only used for Public Safety.  However, in 5G we need also to support the commercial use case. It is very hard to have a single PKMF for all the applications that are independent of PLMNs. It’s unclear which authority should be responsible for maintaining the function for commercial use cases. This solution is proposing to reuse the logic of the 5G DDNMF (or the ProSe Function in LTE) or the 5G PKMF which is bound with the PLMN.

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

### 6.7.1 Solution overview

This solution addresses 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

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 messages are integrity protected and the signalling ciphering protection is a configuration option.

NOTE: Step 0 is done only in coverage. After step 0, the following steps 1-6 are done either within coverage or out-of-coverage.

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 integrity protects 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 the user plane security indication.

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

### 6.7.3 Evaluation

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

This solution requires network coverage for pre-configuration and provisioning of the ProSe security-related parameters.

Privacy protection is not addressed in this solution.

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

### 6.8.1 Introduction

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

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

### 6.8.2 Solution details

#### 6.8.2.1 Procedure

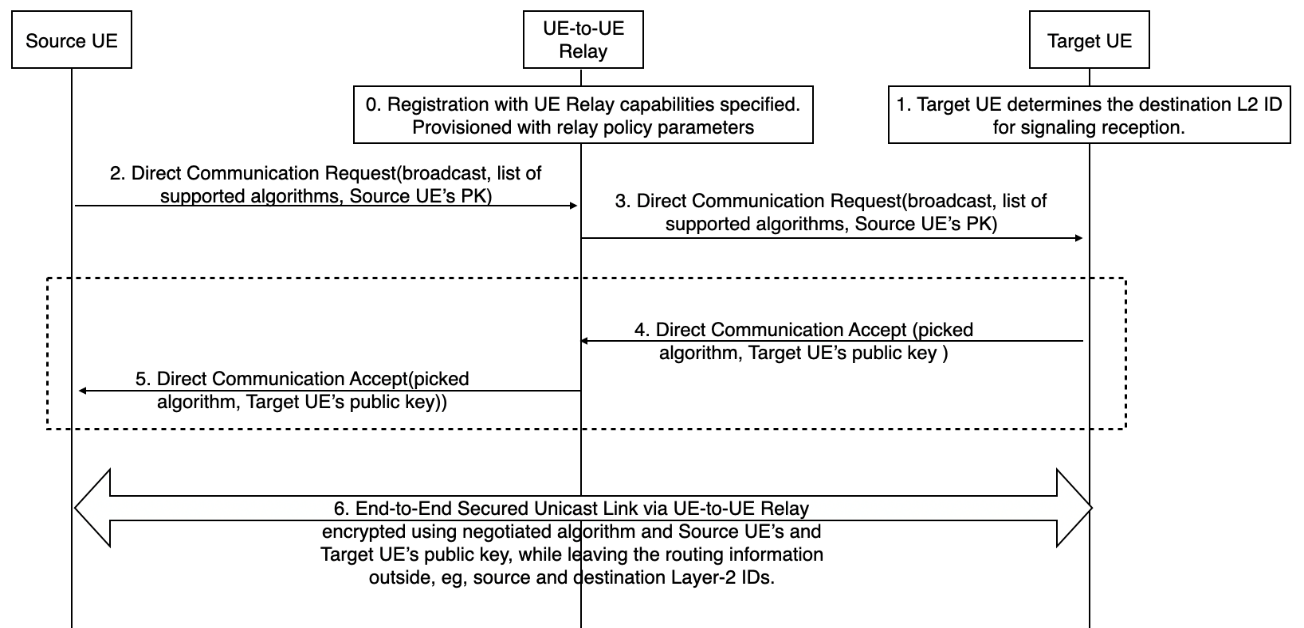


Figure 6.8.2.1-1: Security protection via UE-to-UE Relay using asymmetric cryptography

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

The security procedure details are as following:

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

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

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

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

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

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

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

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

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

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

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

### 6.8.3 Evaluation

TBD.

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

### 6.9.1 Introduction

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

This solution proposes to generate a 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 keys.

### 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 the UE side, the UE will generate the same keys as the network side based on the key material sent from the 5G DDNMF. The 5G DDNMF and AMF will rely on the security of SBI.

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

In user plane architecture as illustrated in clause 4.1.2, a UE reaches the 5G DDNMF via user plane. The 5G DDNMF allocates the Prose APP code and gets the discovery root key from AAnF. The AAnF will generate the discovery root key based on the KAKMA as described in TS 33.535[7]. The 5G DDNMF will further generate discovery IK based on the discovery root key for open discovery and will further generate discovery IK and discovery CK for restricted discovery. The 5G DDNMF will send the key material to the UE via the PC3a protocol. On the UE side, the UE will generate the same keys as the network side based on the key material sent from the 5G DDNMF

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

### 6.9.3 Evaluation

This solution does not specifiy the protocol used between UE and 5G DDNMF for the control plane based approach.

The user plane based approach lacks the details of keys (including discovery root key and discovery keys) derivation by the AAnF, the 5G DDNMF and the 5G ProSe UE for UP solution. It also lacks the details of security material provisioning.

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

### 6.10.1 Introduction

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

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

- KI #12: Security of one-to-one communication over PC5

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. If the Remote UE has already successfully performed a primary authentication with the network prior to connecting with the relay, the solution enables the Remote UE to reuse its 5G native security context to be authorized and establish a secure connection via the UE-to-Network relay.

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

### 6.10.2 Solution details

#### 6.10.2.1 Connection with UE-to-Network relay using Remote UE network primary authentication via the UE-to-Network relay

The procedure for Authorization and security with UE-to-Network relay using Remote UE network primary authentication is depicted in Figure 6.10.2.1-1.



Figure 6.10.2.1-1: 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 the UE-to-Network relay service. The Remote UE also provides its security capabilities and security policy as in TS 33.536[8]. If the Remote UE is reconnecting to the same Relay UE and is already authenticated and authorized for relay communication via that Relay UE, it includes the Krelay ID (instead of SUCI) established during the previous connection using this procedure. If the Relay UE has the Krelay and Krelay ID it skips steps 2 to 12, otherwise the Relay UE rejects the connection request.

NOTE 1:Krelay and Krelay ID are reused during reconnection in the same way as KNRP and KNRP ID in TS 33.536[8]. In case of reconnection with the relay, privacy protection of Krelay ID procedure reuses the same mechanism used for KNRP ID as described in TS 33.536 [8], clause 5.3.3.2.

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

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

4-8. The Relay UE's AMF initiates Remote UE authentication with Remote UE's AUSF according to existing primary authentication procedures. The authentication messages are exchanged transparently via the Relay UE. Authentication messages between AMF and AUSF and AMF and Relay UE include an indication that it is for a relayed authentication i.e. to authenticate Remote UE via Relay UE. The UDM does not need to be aware that the authentication is for a Remote UE as the AMF verifies (in subsequent step 10) with UDM that Remote UE is authorized to use UE-to-Network relaying.

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

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

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 AMF may include the Remote UE identity (e.g., GPSI). The Relay UE stores the key and its id, Remote UE identity and associates them with the PC5 link with Remote UE.

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

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 3-4 in solution#6, and if N3IWF is used with solution#23 subsequent steps 5-6).

#### 6.10.2.2 Connection with UE-to-Network relay using the 5G native security context of the Remote UE

The procedure for Authorization and security with UE-to-Network relay using the 5G native security context of the Remote UE is depicted in Figure 6.10.2.2-1.

Figure 6.10.2.2-1: Procedure for Authorization and security with UE-to-Network relay using 5G native security context of Remote UE

0. The Remote UE has registered with the network and established a 5G native security context with a source AMF. The Relay UE is registered and authorized to operate as a relay.

1. The Remote UE performs a discovery procedure with a Relay UE and decides to connect with the Relay UE using its 5G native security context.

2. If the Remote UE is aware of the PLMN ID of the Relay UE's serving PLMN, the Remote UE verifies that its 5G native security context was established with the Relay UE's serving PLMN before sending its 5G-GUTI to the Relay UE. If the PLMN ID of the Relay UE's serving PLMN and the PLMN ID part in its 5G-GUTI are different or if the current 5G-GUTI was used in a prior DCR with another Relay, the Remote UE sends its SUCI instead (as described in clause 6.10.2.1, step 1). If the Remote UE is not aware of the PLMN ID of the Relay UE's serving PLMN, the Remote UE may choose to send no identifier (i.e. neither SUCI nor 5G-GUTI). If a 5G-GUTI is sent, the Remote UE sends a DCR message to the Relay UE including Remote UE's core network identity (e.g., 5G-GUTI), ngKSI identifying the KAMF being used, the Remote UE's NAS security capabilities, and current UL NAS COUNT. These parameters may be included in a message integrity protected using Remote UE's 5G native security context.

NOTE 1: Remote UE has the option to use the knowledge of Relay PLMN ID to select a Relay (e.g., select Relay 1 with the same PLMN over Relay 2 with different PLMN). This option of PLMN ID based selection of Relay is to be confirmed with SA2.

3. If the request includes a 5G-GUTI, the Relay UE checks whether the PLMN ID of its serving PLMN and in Remote UE's 5G-GUTI are equal. If they are not equal, the Relay UE sends an Identity Request message to the Remote UE including Relay UE's serving PLMN ID, to obtain the Remote UE's identifier (SUCI or 5G-GUTI). If the Remote UE provides a SUCI in the Identity Response, Relay UE proceeds with the procedure as described in clause 6.10.2.1, from step 2. Otherwise, the Relay UE sends the Remote UE's 5G-GUTI and integrity protected message from Remote UE to its serving AMF (target AMF) in a NAS request message.

4. The target AMF checks that Relay UE is authorized to act as a relay.

5. The target AMF identifies the source AMF serving the Remote UE using the provided 5G-GUTI. If the source and target AMFs are different, the target AMF sends a request message to the source AMF to obtain security parameters for the Remote UE. The target AMF includes the integrity protected message from Remote UE and Remote UE's identity received from the Relay UE. The target AMF indicates that the access type and reason for the request are for relay access. If the source and target AMFs are the same (i.e., Remote UE has registered with target AMF), the target AMF retrieves the Remote UE’s context directly from its local storage instead.

6. [option 1] The source AMF locates the Remote UE's security context using the received Remote UE's 5G-GUTI. The source AMF checks the integrity protection of the message from the Remote UE using the Remote UE's security context. If the security checks are successful, the source AMF derives a Krelay and Krelay ID from KAMF identified by the ngKSI. [option 2] Alternatively, the source AMF may generate a new 5G security context. The derivation of the new KAMF is specified in TS 33.501 [14] (Annex A.13). The source AMF sends a response message to the target AMF that includes the Remote UE SUPI. The message may include a Krelay and Krelay ID, a new 5G security context to be used for Remote UE with a KAMF change indication or current Remote UE's 5G security context, and Remote UE's context.

NOTE 2: In the first option, the Remote UE's registration remains with Remote UE's (source) AMF which provides Relay UE's (target) AMF with Krelay and Krelay ID (and SUPI). In the second option, the Remote UE context is transferred to the Relay UE's AMF, with a KAMF change (using the same mechanisms as in TS 33.501[14], clause 6.9.2.3.3). In that case, the target AMF derives Krelay and Krelay ID. Source AMF uses its local policy to determine whether to transfer the Remote UE context and perform horizontal key derivation. If the Remote UE’s 5G security context is moved from the source AMF to the target AMF, then if the Remote UE has simultaneously access to the 3GPP network then this connection with the source AMF (of Remote UE) will be dropped. Following the context transfer, source and target AMF registration update with UDM is handled according to existing AMF change mechanisms (see TS 23.502, clause 4.2.2.2.2).

NOTE 3: Whether Option 2 (with Remote UE context transfer to Relay's AMF) can be used is to be confirmed with SA2.

7. The target AMF checks from Remote UE's context (e.g., obtained from source AMF or locally) or with Remote UE's UDM (e.g., using SUPI provided by source AMF) for authorization to use the Relay UE. If not provided by the source AMF, the target AMF derives a Krelay and Krelay ID using Remote UE's security context.

8. The target AMF sends a NAS response message to the Relay UE that includes the Remote UE id (e.g., GPSI), Krelay and Krelay ID. [Option 2] The message may include a KAMF change flag and new ngKSI if a new security context was generated by source AMF in the previous step.

9. The Relay UE sends a Direct Security Mode Command message to the Remote UE that includes Krelay ID and, if provided by the target AMF, KAMF change flag and new ngKSI. The message is integrity protected using a security key derived from Krelay.

10. If the KAMF change flag is set, the Remote UE derives a new KAMF from the KAMF indicated by the value of ngKSI. The Remote UE derives a Krelay and Krelay ID from the existing KAMF or the newly derived KAMF. The Remote UE verifies the DSMC message security using security derived from Krelay. A successful security verification indicates to the Remote UE that the Relay UE is authorized to provide the relay service for Remote UE. The new KAMF is derived the same way as described for NAS SMC procedure when KAMF change flag is set as described in TS 33.501 [14] clause 6.7.2 step 2a and Annex A.13. If the verification of the DSMC message is unsuccessful, the Remote UE replies with a Direct Security Mode Reject message. In that case, Remote UE discards the new security context if it was derived, continues the use of the existing security context, and the Relay UE aborts the link establishment procedure.

Editor's note: When there is a KAMF change (option 2), how to deal with desynchronization of K\_AMF is FFS.

11. If the security verification is successful, the Remote UE sends a Direct Security Mode Complete message to the Relay UE with security protection (integrity, confidentiality) using security keys derived from Krelay. The Relay UE verifies the Direct Security Mode Complete message security using security derived from Krelay. A successful security verification indicates to the Relay UE that the Remote UE is authorized to use the relay service provided by Relay UE.

12. [Option 2] If a new KAMF derivation was indicated (in step 9), the Relay UE sends a NAS complete message to inform the AMF of the key establishment result. If the Relay indicates a successful KAMF derivation then AMF registers with Remote UE's UDM causing UDM to deregister source AMF and removal or Remote UE context (as per TS 23.502, clause 4.2.2.2.2). If the KAMF derivation fails (e.g., verification of DSMC fails) then the PC5 link setup is aborted and the Remote UE discards the new security context if it was derived and continues the use of the existing security context.

13. The Remote UE receives a DCA message completing the successful PC5 link establishment.

NOTE 4: The purpose of the 5G GUTI reallocation is to preserve the privacy of the subscription temporary identifier. In the above procedure using the first option (i.e., Remote UE context remains with source AMF), the Remote UE transmits its 5G-GUTI only once (in the DCR). In that case, 5G-GUTI re-allocation by source AMF over Uu is performed as per TS 33.501 [14], clause 6.12.3. If the Remote UE has already a prior connection with the Relay it can send the Krelay ID (see 6.10.2.1 step 1) instead of 5G-GUTI. An attacker cannot track the Remote UE using the 5G-GUTI during communication with the Relay UE. Therefore, 5G-GUTI re-assignment is not necessary for this procedure for these scenarios. For 5G-GUTI reallocation when option 2 is used, the Remote UE triggering a connection via a Relay using DCR is considered to be similar to the case of "Service Request message triggered from the UE not triggered by the network" in TS 33.501 [14] clause 6.12.3. In that case, it is left to implementation (i.e., not required) to re-assign a 5G-GUTI. For Registration Update (option 2), the Remote UE is considered to be in a "connected" state and Relay UE's AMF is aware of Remote UE whereabouts as long as a PC5 link between the Remote UE and the Relay UE is up. Therefore, it is not necessary for the Remote UE to perform either mobility or periodic Registration Update procedures for the Relay UE's AMF to keep track of the Remote UE.

Editor's note: How 5G-GUTI reallocation and Registration Update is performed when Remote UE is transferred to Relay’s AMF (option 2) is FFS.

#### 6.10.2.3 Key hierarchy, key derivation, and distribution

The Key Hierarchy for the PC5 unicast link with the UE-to-Network relay is shown in Figure 6.10.2.3-1. Details for Krelay andKrelay ID derivation are described next.

Overall, the keys Krelay, Krelay-sess, Krelay-enc, Krelay-int serve a similar function respectively asKNRP, KNRP-sess, NRPEK, and NRPIK in TS 33.536 [8] clause 5.3.3.1.2.1.

The key derived for access via UE-to-Network relay is Krelay, which is used by UE-to-Network relay and Remote UE to derive Krelay-sess.

Krelay-sess is derived from Krelay using noncesexchanged during the PC5 link establishment similarly to how KNRP-sess is derived fromKNRP in Annex A.3 of TS 33.536 [8].



Figure 6.10.2.3-1: Key Hierarchy for PC5 unicast link with UE to Network relay

When deriving the key Krelay from KAMF and the uplink NAS COUNT in the UE and the AMF the following parameters are used to form the input S to the KDF.

- FC = 0xXX

- P0 = Uplink NAS COUNT

- L0 = length of uplink NAS COUNT (i.e. 0x00 0x04)

- P1 = Access type distinguisher

- L1 = length of Access type distiguisher (i.e. 0x00 0x01)

The access type distinguisher is set to the value for non-3GPP (0x02) (see Annex A.9 in TS 33.501 [14]).

The input key KEY is KAMF.

When deriving the Krelay ID from KAMF, the following parameters are used to form the input S to the KDF:

- FC = 0xYY;

- P0 = "R-KID";

- L0 = length of "R-KID"; (i.e. 0x00 0x05)

- P1 = SUPI;

- L1 = length of SUPI.

The input key KEY is KAMF.

SUPI has the same value as parameter P0 in Annex A.7.0 of TS 33.501 [14].

#### 6.10.2.4 Remote UE authorization revocation/re-authentication

After a successful authorization of Remote UE to use the relay, the Relay UE's AMF may initiate a re-authentication/authorization of the Remote UE at any time. For example, during Relay UE mobility with a change of AMF, the new Relay UE's AMF obtains from the old Relay's AMF the Relay UE context that includes Remote UE information (Krelay, Krelay ID, etc) as described in clause 6.10.2.1. The new AMF may decide to initiate a re-authentication/authorization of Remote UE and derive a new Krelay, Krelay ID as described in clause 6.10.2.1 steps 4-8 and 11. When a re-authentication/authorization is performed, the Remote UE generates a new Krelay, Krelay ID and the relay obtains the same from its serving AMF in a NAS message. The Relay UE replaces the old Krelay, Krelay ID with the new ones and initiates a re-key procedure over the PC5 link with the Remote UE to generate fresh new Krelay-session, Krelay-enc, Krelay-int similar to the procedure described in TS 33.536 [8] clause 5.3.3.1.4.4 for generating a fresh KNRP-sess, etc.

After a successful authorization of Remote UE to use the relay, the Relay UE's AMF may initiate revocation of authorization of the Remote UE at any time. For example, the AMF may receive an update message from the Remote UE's UDM to revoke authorization for the Remote UE to use the relay (e.g., due to Remote UE subscription change). The message includes the identity of the Relay UE serving the Remote UE as registered by the AMF in clause 6.10.2.1 step 10. The AMF sends a NAS message to the Relay UE to revoke authorization for the Remote UE to use the relay. The AMF may include the associated Krelay ID and the Remote UE identity (e.g., GPSI). The Relay UE locates the PC5 link context based on Krelay ID (or Remote UE's GPSI) and initiates a link release procedure for the PC5 link with the Remote UE.

### 6.10.3 Evaluation

The solution fulfils requirements of KI#3 (secure means to establish a PC5 link) using keys from the primary authentication to derive PC5 related keys. This solution can be combined with a solution using N3IWF (e.g., sol#19) to fulfil the second requirement of KI#3 (end to end security).

NOTE 1: The third requirement of KI#3 (i.e., security for path switch) is not considered within Rel-17 timeframe in line with TR 23.752 [2] conclusion ( clause 8.6).

The solution fulfils the requirements of KI#4 (authorization of Remote UE/ UE-to-Network relay) using a network-controlled authorization procedure based on primary authentication of Remote UE (building on TR 23.752 [2] sol#47 principles). The solution fulfils the requirements of KI#9 (PC5 key management for relay communication) by supporting derivation /distribution of PC5 related keys based on keys from the primary authentication, using existing 5GC entities (AMF, AUSF).

The solution fulfils the requirements of KI#12 (Security of one-to-one communication over PC5) including support of the Remote UE out of coverage scenario by reusing PC5 link communication security procedure as defined in TS 33.536 [8]. Specifically, the solution fulfils the 1st (separate security context per peer UE in and out of coverage), 3rd (link setup protection against MiTM), 4th (signalling protection) and 5th requirement (user plane protection).

The solution fulfils the requirements of KI#5 (privacy protection of Remote UE) by reusing existing privacy protection mechanisms for identifiers transmitted by Remote UE (e.g., SUCI, KNRP ID).

Editor’s Note: When Remote UE uses its 5G-GUTI in DCR with option 1 (no Remote UE context transfer) fulfilment of privacy protection of 5G-GUTI requirement is FFS.

When Remote UE uses its 5G-GUTI in DCR and considering option 2 (with Remote UE context transfer), the support for 5G-GUTI reallocation, Registration Update and handling of desynchronization of K\_AMF are not covered in the current specification.

Option 1 is the selected option for when Remote UE wishes to use its 5G-GUTI in DCR.

This solution requires a new relayed primary authentication procedure (aka "network controlled authorization" based on TR 23.752 [2] sol#47) to enable Remote UE to perform primary authentication with the AUSF of Remote UE via the AMF of Relay UE and Relay UE which both need to support a corresponding new NAS procedure.

In this solution, the UE-to-Network relay's AMF is responsible for PC5 link root key Krelay and its Krelay ID derivation from KAMF, as the Remote UE. The AMF stores Remote UE information (Remote UE id, PC5 link root key) in the Relay UE context. The Relay UE uses the PC5 root key and associated id to establish the security of the PC5 link with the Remote UE.

Another impact on 5GC and the existing procedure is documented in TR 23.752 [2] sol#47, clause 6.47.3. In addition and as an optimization to skip primary authentication, the Remote UE may optionally provide its 5G-GUTI when connecting for relayed communication authorization.

This solution assumes that NAS confidentiality is activated for the relay. In this solution, the PC5 link root key Krelay is sent over the air interface to the Relay UE. It requires that the NAS message carrying Krelay is both integrity and confidentiality protected. Otherwise, there is the risk that the root key Krelay is exposed in clear text if confidentiality protection of the NAS signaling is not activated. Therefore, the use of NAS signaling encryption needs to be properly configured for key provisioning.

NOTE: In general, NAS confidentiality is assumed to be required for any L3 relay scenario, as sensitive information/parameters may be exposed during provisioning by PCF or PDU Session management procedures.

Editor’s Note: Further evaluation is FFS.

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

### 6.11.1 Introduction

This solution addresses key issue #10.

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

### 6.11.2 Solution details

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

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

The UE and an Application Function can establish a TLS tunnel using GBA-based secret as specified in clause 5.4.0 of 3GPP TS 33.222 [13]. Then, the UE and the Application Function can exchange application data over the secure tunnel.

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

### 6.11.3 Evaluation

This solution addresses the requirement in Key Issue#10.

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

### 6.12.1 Introduction

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

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

When a Source UE changes its IP address/prefix, its Target UE must be informed of UE1’s new IP address/prefix since communication between UE1 and UE2 is IP-based. Furthermore, the UE-to-UE Relay must as well be informed of UE1’s new IP address/prefix and/or other new identifiers since communication between UE1 and the UE-to-UE Relay is over a PC5 unicast link and the UE-to-UE Relay also handles the IP routing of messages exchanged between the peer UEs. Moreover, since the PC5 unicast link used by UE1 is established with the UE-to-UE Relay, this UE-to-UE Relay also needs to update its identifiers at the same time as the Source UE.

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

### 6.12.2 Solution details

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

This solution applies to Layer-3 based Solution #10 and Solution #32 described in TR 23.752[2]. Since Solution #10 and Solution #32 described in TR 23.752[2] are similar, this proposed solution applies to both of them. The main difference between Solution #10 and Solution #32 described in TR 23.752[2] is the proposed method of IP address/prefix allocation. In Solution #10, the UE-to-UE Relay allocates the IP address/prefix to the UE. In Solution #32, a link-local IP address that is assigned by the UE itself is used and sent to the UE-to-UE Relay. Differences in the procedure detailed below are explained when needed.

As defined for the Layer-3 based Solution #10 and Solution #32 described in TR 23.752[2], each UE uses the same IP address with all its peer UEs which are connected to the same UE-to-UE Relay. UE1’s IP address is thus not associated or linked to UE2’s IP address thus UE2’s IP address cannot indirectly be used to track UE1 after the Link Identifier Update procedure is run between UE1 and the UE-to-UE Relay. For this reason, UE2 does not need to change its IP address at the same time as UE1. UE2 however needs to be informed of UE1’s new IP address since IP communication is used between UE1 and UE2.

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



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

0) A PC5 unicast link is established between UE1 and the UE-to-UE Relay. Another PC5 unicast link is established between the UE-to-UE Relay and UE2. The Relay maintains a mapping table that includes its PC5 peer UEs’ user info, their IP addresses/prefixes, and associated PC5 unicast links. Both Source/Target UEs learn their peer UE’s IP addresses/prefixes via the Relay UE using DNS. IP data is exchanged between UE1 and UE2 via the UE-to-UE Relay over the PC5 unicast links. The UE-to-UE Relay handles the routing of IP packets to another PC5 unicast link based on the destination IP address/prefix.

1) UE1 is informed (e.g., via the application layer, timer expiration) that its IP address/prefix, Layer-2 ID, and possibly other identifiers (e.g., Application ID) must be changed. UE1 triggers the Link Identifier Update procedure, as defined in TS 23.287 [9], with some changes added for the support of UE-to-UE Relay.

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

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

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

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

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

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

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

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

### 6.12.3 Evaluation

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

### 6.13.1 Introduction

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

### 6.13.2 Solution details

#### 6.13.2.1 Secondary Authentication after PC5 link setup



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

1. During the Registration procedure, Authorization and provisioning are performed for the ProSe UE-to-NW relay(0a) and Remote UE(0b). When the Remote UE is not in the coverage, the Remote UE may use its preconfigured policy and parameter for PC5 discovery and communication to establish a PC5 connection with a UE-to-Network Relay.

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

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

3. The Remote UE selects a ProSe 5G UE-to-Network Relay and establishes a connection for One-to-one ProSe Direct Communication. When requesting UE-to-Network relaying over PC5, the Remote UE provides its Remote User ID (e.g. SUCI) to the 5G ProSe UE-to-Network Relay UE, which then triggers a Remote UE authorization procedure to validate if the Remote UE is authorized to access the network over the UE-to-Network Relay UE.

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

NOTE 1: The secondary authentication of the UE-to-Network Relay UE takes part in the general PDU session establishment.

NOTE 2: How the Remote UE is authorized to access the network over the UE-to-Network Relay UE is not part of this solution but it is assumed that the AMF can get the Remote UE's SUPI during the authorization / authentication procedure using any solutions for KI#4 (e.g. Sol#10).

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

5. The ProSe 5G UE-to-Network Relay sends a Remote UE Report (Remote User ID, IP info) message to the SMF for the PDU session associated with the relay. The SMF receives the Remote UE's SUPI from the AMF, obtained during step 3.

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

NOTE 3: The local configuration of the SMF is set by the operator. If it indicates that secondary A&A is not required, the SMF does not perform secondary authentication/authorization for the Remote UE.

NOTE 4: As described in clause 4.3.2.3 of TS 23.502, secondary authentication can be supported in the case of a local breakout scenario. Similarly, the secondary authentication procedure for the remote UE can be performed even if remote UE's HPLMN is different from that of relay UE as long as there is a secure connection between relay UE's PLMN and the DN-AAA where the remote UE needs to perform the secondary authentication.

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

NOTE 5: When a PDU session being shared by multiple UEs is revoked or changed due to any reason, how to handle this is not introduced in this solution.

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

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

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

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

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

NOTE 6: It is possible to perform a secondary authentication procedure in parallel when multiple Remote UEs are connected to the 5G ProSe UE-to-Network Relay almost at the same time.

NOTE 7: The DN-AAA does not know whether a UE is connected via 5G ProSe UE-to-Network Relay or connected directly to the network.

NOTE 8: The solution assumes that the used EAP method provides the necessary security (e.g., for user id privacy protection).

#### 6.13.2.2 Secondary Authentication before PC5 link setup



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

1. During the Registration procedure, Authorization and provisioning are performed for the ProSe UE-to-NW relay(0a) and Remote UE(0b). When the Remote UE is not in the coverage, the Remote UE may use its preconfigured policy and parameter for PC5 discovery and communication to establish a PC5 connection with a UE-to-Network Relay.

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

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

3. Remote UE establishes PC5 connection towards the 5G ProSe UE-to-Network Relay UE. When requesting UE-to-Network relaying over PC5, the Remote UE provides its Remote User ID (e.g. SUCI) to the 5G ProSe UE-to-Network Relay UE, which then triggers a Remote UE authorization procedure to validate if the Remote UE is authorized to access the network over the UE-to-Network Relay UE.

NOTE 1: The secondary authentication of the UE-to-Network Relay UE takes part in the general PDU session establishment.

NOTE 2: How the Remote UE is authorized to access the network over the UE-to-Network Relay UE is not part of this solution but it is assumed that the AMF can get the Remote UE's SUPI during the authorization / authentication procedure using any solutions for KI#4 (e.g. Sol#10).

4. The 5G ProSe UE-to-Network Relay UE sends PDU Session Establishment or PDU Session Modification Request to the SMF and provides the Remote UE ID of the Remote UE. The SMF receives the Remote UE's SUPI from the AMF, obtained during step 3.

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

NOTE 3: The local configuration of the SMF is set by the operator. If it indicates that secondary A&A is not required, the SMF does not perform secondary authentication/authorization for the Remote UE.

NOTE 4: As described in clause 4.3.2.3 of TS 23.502, secondary authentication can be supported in the case of a local breakout scenario. Similarly, the secondary authentication procedure for the remote UE can be performed even if remote UE's HPLMN is different from that of relay UE as long as there is a secure connection between relay UE's PLMN and the DN-AAA where the remote UE needs to perform the secondary authentication.6. The 5G ProSe UE-to-Network Relay sends an EAP message to the Remote UE via PC5 signalling. The Remote UE sends an EAP message to the 5G ProSe UE-to-Network Relay via PC5 signalling.

NOTE 5: When a PDU session being shared by multiple UEs is revoked or changed due to any reason, how to handle this is not introduced in this solution.

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

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

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

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

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

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

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

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

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

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

NOTE 6: It is possible to perform a secondary authentication procedure in parallel when multiple Remote UEs are connected to the 5G ProSe UE-to-Network Relay almost at the same time.

NOTE 7: The DN-AAA does not know whether a UE is connected via 5G ProSe UE-to-Network Relay or connected directly to the network.

NOTE 8: The solution assumes that the used EAP method provides the necessary security (e.g., for user id privacy protection).

### 6.13.3 Evaluation

Solution #13 proposes to support secondary authentication of the Remote UE. With this solution, the AAA server in the DN can authorize the Remote UE to give access to the services using the PDU session of the L3 UE-to-NW Relay UE via the PC5 link. In this solution, the Remote UE and the UE-to-Network Relay UE exchange the EAP message via PC5 signalling and the UE-to-Network Relay UE relays the message between the Remote UE and SMF. SMF obtaining Remote UE's SUPI is assumed to be performed as part of a procedure addressed in solutions for KI#4.

This solution works in both cases where the remote UE and the relay UE have subscriptions to the same PLMN or different PLMNs.

This solution re-uses the EAP framework used in the secondary authentication procedure specified in clause 4.3.2.3 of TS 23.502 [6] with a modification on the triggering condition as the Relay UE’s SMF triggers the Remote UE’s secondary authentication when it receives Remote UE report from the Relay UE.

NOTE: Whether new messages will be defined or the existing messages for the secondary authentication will be reused for the remote UE secondary authentication will be determined by CT1.

In this solution, the secondary authentication for the Remote UE is not involved in whether the PDU session can be established or not and the Relay UE’s SMF has to create the Remote UE context when the secondary authentication for the Remote UE is needed.

From the Remote UE's point of view, the Remote UE may have to run two different authentication procedures to access UE to Network Relay services, i.e. one is between the Remote UE and the Relay UE, and the other is the secondary authentication, which is optional.

The name of this procedure may be called differently if this solution is adopted to the normative work.

Performing the secondary authentication for the remote UE over L3 UE-to-NW Relay UE may increase both NAS and PC5 signalling compared to not performing but it can be performed only when it is needed based on the subscription of the Remote UE and local configuration of the SMF.

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

### 6.14.1 Introduction

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

### 6.14.2 Solution details



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

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

1. If in coverage, the Remote UE and UE-to-Network Relay UE independently get the service authorization for indirect communication from the network. If the Remote UE is not in coverage, the pre-configured information will be used, and the service authorization and relevant parameters can be updated after step 7.

2-3. The Remote UE and UE-to-Network Relay UE perform UE-to-Network Relay UE discovery and selection. For details of UE-to Network Relay discovery and selection for Layer2 UE-to-Network Relay see clause 6.3.2.3 of TS 23.304 [16].

4. The Remote UE initiates a one-to-one communication connection with the selected UE-to-Network Relay UE over PC5 using the solutions to address KI#12 in this document.

NOTE 1: when the remote UE is out of coverage, how to authorize the remote UE is addressed in key issue#4.

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

6. The Remote UE initiates RRC connection with NG-RAN via the UE-to-Network Relay UE to establish RRC Connection with the same NG-RAN serving the Relay UE. The NG-RAN triggers the AS SMC procedure to establish AS security with the remote UE during RRC connection establishment.

NOTE 2: RRC connection establishment between the Remote UE and the NG-RAN is to be defined by RAN2.

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

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

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

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

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

### 6.14.3 Evaluation

The solution shows that the L2 solution can reuse the existing security mechanism from TS 33.501 [14].

How AS security between the Remote UE and the NG-RAN is established is not detailed in the solution.

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

### 6.15.1 Introduction

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

NOTE: Remote UE needs to be in coverage to request relay key from AUSF (i.e. NAS messages step1-6).

### 6.15.2 Solution details

#### 6.15.2.1 Procedure

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

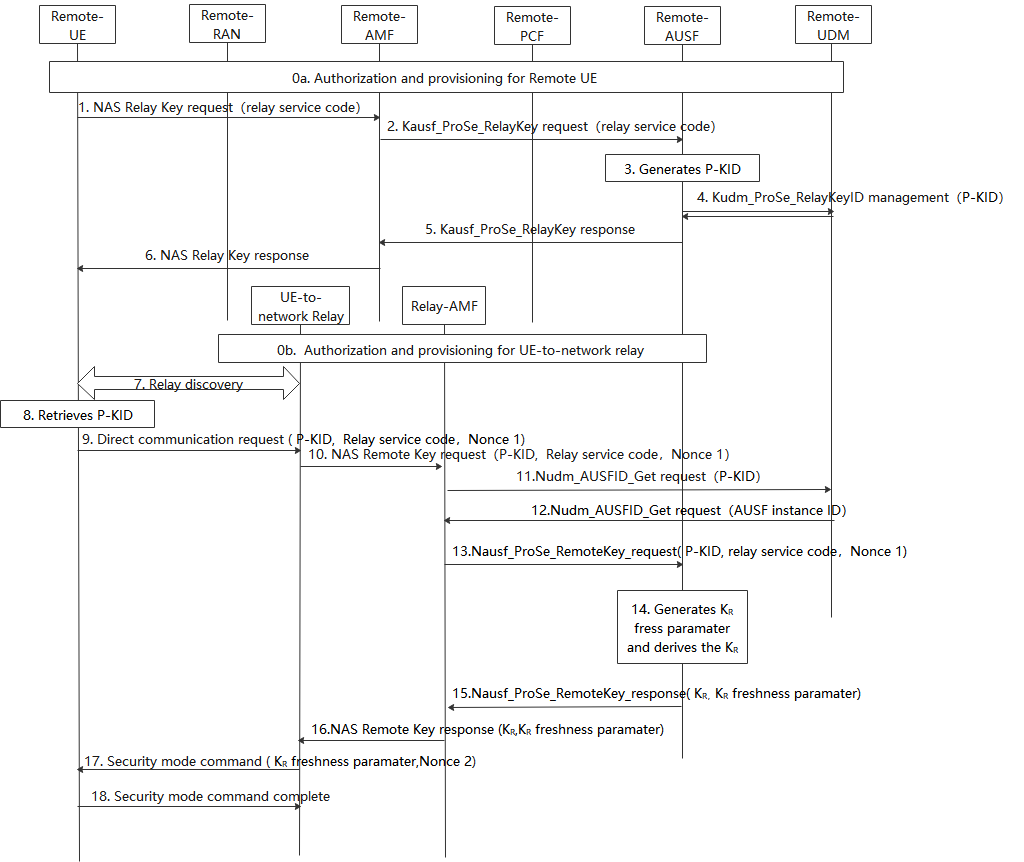


Figure 6.15.2-1: Procedures for key management in ProSe UE-to-Network Relay based on primary authentication

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

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

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

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

P-KID is in NAI format as specified in clause 2.2 of IETF RFC 7542 [6], i.e. username@realm. The username part includes the Routing Identifier and the P-TID (ProSe Temporary UE Identifier), and the realm part includes Home Network Identifier.

The P-TID is derived from KAUSF as specified in 6.15.2.2.

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

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

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

Note: If the Kausf changes, the UE initiates steps 1~6 to trigger the AUSF to derive the new P-KID and stores the new P-KID in the UDM.

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

8. The Remote UE derives P-KID based on the relay service code the Remote UE would like to access using the same method as the remote AUSF.

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

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

11. The relay AMF that serves the relay UE first check whether the relay UE is authorized to be a relay. If authorized, The AMF discovers the UDM based on the P-KID, the relay AMF sends Nudm\_AUSFID\_Get request with P-KID to the UDM.

12. UDM response to relay AMF via Nudm\_AUSFID\_Get with AUSF instance ID of the AUSF serving remote UE.

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

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

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

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

NOTE: This solution requires integrity and confidentiality protected NAS messages.

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

18. The Remote UE derives KR key in the same way as the remote AUSF in step 14. The DSMC message is integrity and confidentiality protected as in TS 33.536[8].

NOTE: This solution assumes the NAS confidentiality protection is activated.

#### 6.15.2.2 Derivation of P-TID

When deriving the P-TID from KAUSF, the following parameters are used to form the input S to the KDF:

- FC = xxxx (to be allocated by 3GPP);

- P0 = SUPI;

- L0 = length of SUPI.

- P1 = relay service code;

- L1 = length of relay service code.

The input key KEY is KAUSF.

SUPI has the same value as parameter P0 in Annex A.7.0 of TS 33.501 [2].

### 6.15.3 Solution Evaluation

This solution#15 addresses the requirements in KI#3, KI#4, and KI#9. The remote UE triggers the 5GC network to derive the P-KID per service relay code and the remote UE derives the PKID locally. The remote UE sends the P-KID to Relay UE for retrieving the shared key from the AUSF that serving remote UE, and the remote UE derives the shared key locally based on the primary authentication key Kausf. During the shared key obtaining procedure, the 5GC check whether the relay UE is authorized to be a relay UE. After the remote UE and relay UE retrieve the shared key, they can establish the PC5 security based on the existing mechanism defined in TS33.536.

This solution requires Remote UE to be in coverage to request a relay key from AUSF.

The AUSF is responsible for the ProSe key management function in this solution. This solution requires the AMF and the UE (including the Remote UE and Relay UE) to support new NAS procedures.

In this solution, the PC5 link root key KR is sent over the air interface to the Relay UE. It requires that the NAS message carrying KR is both integrity and confidentiality protected. Otherwise, there is the risk that the root key KR is exposed in clear text if confidentiality protection of the NAS signaling is not activated. Therefore, the use of NAS signaling encryption needs to be properly configured for key provisioning, this solution assumes the NAS confidentiality protection is activated.

Editor’s Note: Further evaluation is FFS.

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

### 6.16.1 Introduction

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

### 6.16.2 Solution details

This clause gives out the procedure for the security establishment.



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

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

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

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

Note X: As concluded in TR 23.752, alternative 2 (i.e. Model B) of solution #8 is selected for the normative work, in which if more than one candidate Relay UEs responding discovery response message, UE-1 can select one Relay UE based on e.g. implementation or link qualification.

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

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

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

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

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

Step 5-6: UE1 sends the indirect communication request to UE2 via the UE-to-UE relay1, including the K-ID, UE1 security capability, UE1 ID, UE2 ID, UE-to-UE relay1 ID, security info, where the security info can be used by the UE2 to verify the UE1 authenticity. The security info could be a message authentication code, which is generated by the Key, the UE1 ID, UE-to-UE relay1 ID, UE2 ID, and a freshness parameter.

Editor’s Note: What type of ID is used as a UE or relay ID is FFS.

Step 7: UE2 verified the security info to assure the correctness of the indirect communication request message, may check that the received UE2 ID matches with its own identity, and may verify that the authenticity of UE-to-UE relay by comparing the received UE-to-UE relay1 ID in step 6, and the UE-to-UE relay1 ID stored in step8.

Step 8: UE1 and UE2 perform the indirect security mode command procedure to establish a secure connection, including the protection key and security algorithms. Steps 4b and 5b of direct security mode complete procedures in TS 33.536 [8] clause 5.3.3.1.4.4 could be reused here for the indirect SMC between UE1 and UE2.

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

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

### 6.16.3 Evaluation

TBD

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

### 6.17.1 Introduction

This solution addresses the KI #13 "Security and privacy of groupcast communication". This solution ensures that the group IDs and the L2 IDs are protected in terms of linkability, traceability, and privacy even when the groupcast security is not enabled. The group creation and management, including the group announcement message is the scope of the application layer.

### 6.17.2 Solution details

The detailed solution is illustrated in Figure.

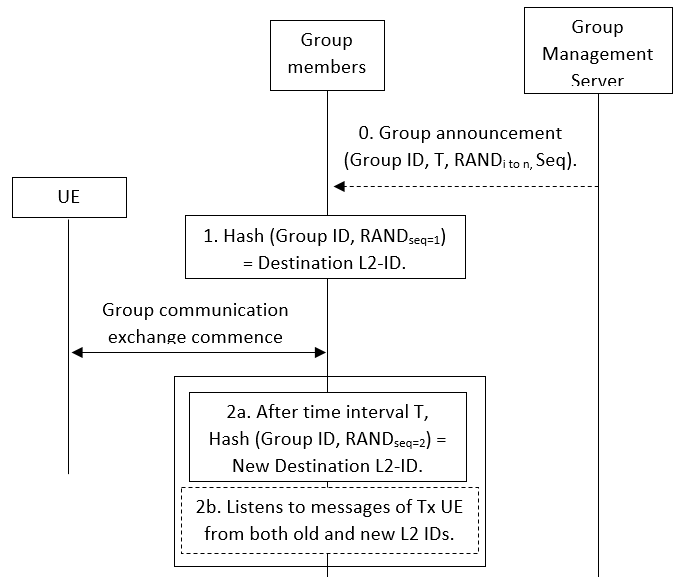


Figure 6.17.2-1: Procedure for secure conversion of application layer group ID to destination Layer-2 ID

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

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

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

The message 0 as presented in the figure is from the application layer specification. Hence the time synchronization for the members of the group while calculating the destination L2 IDs during the first conversion is not in the scope of this solution.

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

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

### 6.17.3 Evaluation

The solution fulfils the first security requirement outlined by key issue #13. The solution provides a mechanism to securely convert the group ID to destination L2 ID as well as preserve the privacy of the destination L2 ID by regularly updating it.

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

### 6.18.1 Introduction

This solution addresses KI #3 and KI #4. This solution provides a mechanism to set up a PC5 link between a remote UE and UE-to-network relay. In addition, this solution describes how a Remote UE and UE-to-network relay get authorized by the ProSe Key Management Function and verify each other’s roles. This solution assumes the 5G Prose function and Prose Key Management Function as in LTE Prose. This solution only describes the PC5 link setup procedure that is common for both L2 and L3 UE-to-network relay.

### 6.18.2 Solution details



Figure 6.18.2-1: Authorization and secure PC5 link establishment procedure for UE-to-network relay

NOTE: In this solution, the remote UE needs to be provisioned with the discovery security materials and Remote User Key when it is in coverage. Also, those security materials are associated with an expiration time, after which they become invalid. When the security materials become invalid the Remote UE needs to be in coverage to obtain fresh ones to be able to connect via relay.

Editor’s Note: The architecture of this solution needs to be aligned with SA2.

0a. The Remote UE gets the discovery parameters and ProSe Key management function (PKMF) address from the 5G DDNMF.

NOTE: The Remote UE may get multiple PKMF addresses for different PLMNs. If the Remote UE receives multiple PKMF addresses, it will contact each of the PKMFs separately. The remote UE may contact those PKMFs directly or via the PKMF of its home PLMN.

0b. The Remote UE is authorized to receive UE-to-network relay service and gets the discovery security material from the PKMF

0c. The UE-to-network relay gets the discovery parameters and ProSe Key management function (PKMF) address from the 5G DDNMF.

0d. The UE-to-network relay is authorized to act as a relay and gets the discovery security material from the PKMF.

The remote UE and relay UE communicate with the PKMF via PC8 reference point (like in LTE Prose [6]). Security for PC8 interface relies on Ua security if GBA [12] is used or Ua\* when AKMA [7] is used.

NOTE: For commercial services, the PKMF is located in the operator’s network. For Public Safety use cases, the PKMF can be managed by the Public Safety service provider.

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

1b. The ProSe Key Management Function checks that the Remote UE is authorised to receive UE-to-network Relay service. This is done by using the Remote UE’s identity that is bound to the keys that established the secure connection between the Remote UE and PKMF in step 0b. If the Remote UE is authorised to receive the service, the PKMF sends a PRUK and PRUK ID to the Remote UE.

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

NOTE: The details on the discovery security material will be determined in the normative phase based on the solutions and conclusions of KI #1 and KI #2.

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

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

4b. On receiving the Key Request message, the PKMF checks that the UE-to-network relay is authorized to act as a relay to the Remote UE. This is done by using the relay’s identity that is bound to the keys that established the secure connection between the relay and PKMF in step 0d. If the UE-to-network relay is authorized to provide the relay service, the PKMF generates KNRP freshness parameter 2 and derives KNRP using PRUK identified by PRUK ID, KNRP freshness parameter 1 and KNRP freshness parameter 2. Then, the PKMF sends a Key Response message that contains KNRP and KNRP freshness parameter 2 to the UE-to-network relay.

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

NOTE: The details on the security negotiation other than key derivation and its use would be based on the solutions for KI #12.

5b. The Remote UE derives KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2. It then derives the session key (KNRP-SESS) in the same manner as the UE-to-network relay and processes the Direct Security Mode Command. The Remote UE further derives the integrity protection key (KNRPIK) and encryption key (KNRPEK) from the session key (KNRP-SESS). Then, the Remote UE checks the integrity of the Direct Security Mode Command message. If the integrity check is successful, the Remote UE is assured that the UE-to-network relay is authorized to provide the relay service.

5c. The Remote UE responds with a Direct Security Mode Complete message to the UE-to-network relay. The Direct Security Mode Complete message is ciphered and integrity protected.

5d. On receiving and processing the Direct Security Mode Complete message, the UE-to-network relay checks the integrity of the Direct Security Mode Complete message. If the integrity check is successful, the UE-to-network relay is assured that the Remote UE is authorized to get the relay service.

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

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

### 6.18.3 Evaluation

This solution fulfils the security requirements of KI#3 as follows:

* This solution supports a secure means to establish a PC5 link between the remote UE and the U2N relay based on the security materials provisioned by the PKMF.

This solution fulfils the security requirements of KI#4 based on the PKMF’s authorization of the remote UE and the U2N relay. The UE authorization by PKMF in this solution is different from the UE authorization specified in TS 23.304 [16].

This solution reuses the ProSe UE-to-network relay security defined for LTE in TS 33.303 [6], which involves the ProSe Key Management Function (PKMF) of the Relay UE. The PKMF is only used for Public Safety in LTE. Introducing PKMF for commercial Prose services in 5G may require a different deployment model than in LTE.

This solution requires the Remote UE to be in coverage to get provisioned with the discovery security materials and Remote User Key.

Editor’s Note: Further evaluation is FFS.

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

### 6.19.1 Introduction

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

### 6.19.2 Solution details

#### 6.19.2.1 Procedure



Figure 6.19.2.1-1: Secure PC5 link establishment procedure for UE-to-network relay

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

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

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

The Relay Service Code (RSC) used for discovery and PC5 link setup is associated with the PDU session for the Remote UE to access the N3IWF. The Remote UE determines the N3IWF address and accesses the N3IWF over the PDU session established by the U2N relay UE based on the procedure in TS 23.304 [16].

NOTE: This solution assumes that the Remote UE is authorized to access the PDU Session associated with RSC according to KI#4 solutions.

#### 6.19.2.2 Protocol Stack

The protocol stacks for remote UE’s control-plane and user-plane via N3IWF are shown in Figure 6.19.2.2-1 and 6.19.2.2-2 respectively.



Figure 6.19.2.2-1 Control-plane protocol stack



Figure 6.19.2.2-2 User-plane protocol stack

### 6.19.3 Evaluation

This solution fulfils the second security requirement of KI#3:

* This solution supports the confidentiality, integrity, and replay protection of the traffic between the remote UE and the 3GPP network in an end-to-end manner between the remote UE and the N3IWF.

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

### 6.20.1 Introduction

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

### 6.20.2 Solution details



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

NOTE: In this solution, the remote UEs and relay UE are assumed to be provisioned with the discovery security materials when they are in coverage. Also, those security materials are associated with an expiration time, after which they become invalid. When the security materials become invalid the Remote UE needs to be in coverage to obtain fresh ones to be able to connect via relay.

Editor’s Note: the detail of discovery security materials is FFS.

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

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

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

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

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

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

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

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

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

NOTE: For commercial services, the PKMF is located in the operator’s network. For Public Safety use cases, the PKMF can be managed by the Public Safety service provider.

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

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

NOTE: Whether the end-to-end IPsec is needed is configured at the remote UEs by the PKMF.

### 6.20.3 Evaluation

This solution provides end-to-end confidentiality and integrity protection of communication between the peer UEs over the UE-to-UE Relay at the IP layer.

This solution provides confidentiality and integrity protection of user-plane data and control-plane signaling between the remote UE and the UE-to-UE relay based on PC5 unicast security.

Editor’s Note: Further evaluation is FFS.

## 6.21 Solution #21: 5G PKMF for key management in PC5 communication

### 6.21.1 Introduction

This solution describes how the Remote UE and the UE-to-network relay find out the address of the common key management server (5G PKMF) to be able to communicate over the PC5 interface. This solution addresses key issue #4 and key issue #9. This solution describes a 5G PKMF which is an NF (network function) which resides in Remote UE’s HPLMN that is accessed by the Remote UE via user plane (like the 5G DDNMF). The 5G PKMF provisions security keys to the Remote UE and the UE-to-network relay, to be used for PC5 communication.

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

The different layers of keys are the following:

* KPC5 key is a key with a key lifetime generated by the 5G PKMF-1(Remote UE) and provisioned to the Remote UE. KPC5 key is not provisioned to the UE-to-network relay.
* KPC5-COM key is generated from the KPC5 key and is a key shared between the two entities (Remote UE and UE-to-network relay) that are communicating over the PC5 unicast link. The KPC5-COM ID identified the KPC5-COM key.
* KSESS: This is a key that is derived by Remote UE and UE-to-network relay from KPC5-COM key and is used to protect the transfer of data between the Remote UE and UE-to-network relay. The actual keys (see next bullet) that are used in the confidentiality and integrity algorithms are derived directly from KSESS.
* KSESS-IK and KSESS-CK: The NR PC5 Encryption Key (KSESS-CK) and NR PC5 Integrity Key (KSESS-IK) are used in the chosen confidentiality and integrity algorithms respectively for protecting PC5-S signalling, PC5 RRC signalling, and PC5 user plane data. They are derived from KSESS and are refreshed automatically every time KSESS is changed.

### 6.21.2 Solution details

In this solution, the Remote UE has a 5G PKMF (5G PKMF-1) in its home PLMN for ProSe key management. The UE-to-network relay has a 5G PKMF (5G PKMF-2) in its home PLMN for ProSe key management. These two 5G PKMF’s (5G PKMF-1 and 5G PKMF-2) can communicate with each other. The 5G PKMF in this solution could be similar to the PKMF in 4G ProSe (TS 33.303).

The Remote UE receives the Relay Service Code from the PCF.

When the Remote UE has discovered a UE-to-network relay in its vicinity, it sends its HPLMN ID, explicitly on the PC5 interface to the UE-to-network relay.

There are two options:

* In Option 1, the UE-to network relay contacts the Remote UE’s 5G PKMF-1 via its 5G PKMF-2. The UE-to-network relay provides the HPLMN ID of the Remote UE, received on PC5 together with the Relay Service Code to its 5G PKMF-2 which can resolve the address of the Remote UE’s 5G PKMF-1.
* In Option 2, the UE-to-network relay retrieves the address of the Remote UE’s 5G PKMF-1 from its 5GDDNMF and contacts thereafter the Remote UE’s 5G PKMF-1 directly. The UE-to-network relay provides the HPLMN ID together with the Relay Service Code to its 5GDDNMF which can resolve the address of the Remote UE’s 5G PKMF-1.

It is expected that the Remote UE has been provisioned with the Relay Service Code when it is in 3GPP coverage. The Remote UE must be authenticated and authorized by its home PLMN before its provisioned with the Relay Service Code. The Remote UE retrieves the discovery key and the key for PC5 communication while in 3GPP coverage.

The Remote UEs and UE-to-network relay are assumed to be provisioned with the discovery security materials when they are in 3GPP coverage. If the discovery keys expire when the Remote UE is not in 3GPP coverage, then the Remote UE needs to find a cell which provides 3GPP access as this solution requires Remote UE to be in 3GPP coverage in order to obtain discovery security material.



Figure 6.21.2.1-1: 5G PKMF for key management in PC5 communication

Step 0) The Remote UE retrieves the address of the 5G PKMF-1(Remote UE) used for ProSe key management located in its home PLMN and the Relay Service Code from the network.

The UE-to-network Relay retrieves the address of the 5G PKMF-2 (UE-to-network Relay) used for ProSe key management located in its home PLMN and the Relay Service Code from the network.

NOTE: How the Remote UE and UE-to-network relay receives the address of the 5G PKMF-1(Remote UE) used for ProSe key management located in its home PLMN, and which function provides this parameter to the Remote UE is for SA2 to decide.

Step 1) The Remote UE retrieves the discovery keys for the discovery of the UE-to-network relay as described in solution #35 (Discovery procedures for UE-to-network relays).

Step 2) The Remote UE establishes a secure connection with the 5G PKMF-1 (Remote UE) server. The Remote UE ID is authenticated and authorized by the 5G PKMF-1 (Remote UE) server. As this connection is established in the user plane, the same mechanism as used to protect the PC3 interface can be re-used. Either solution #5 or solution #11 can be used for securing the connection.

Step 3a) The Remote UE contacts the 5G PKMF-1(Remote UE) by initiating a Key Request message for PC5 communication including the Relay Service Code and the Remote UE ID. The 5G PKMF-1(Remote UE) generates a KPC5 key and a KPC5 key ID.

NOTE: Whether the Remote UE ID consists of one or more of the following parameters: ProSe application id, ProSe application user id and/or GPSI of the Remote UE is for SA2 to decide

Step 3b) The 5G PKMF-1(Remote UE) provides the KPC5 key and the KPC5 key ID in the Key Response message to the Remote UE to be used for PC5 communication with a UE-to-network relay.

Step 4) The UE-to-network relay retrieves the discovery keys for the discovery of the Remote UE as described in solution #35 (Discovery procedures for UE-to-network relays).

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

Step 6) The Remote UE sends a Direct Communication Request on the PC5 interface. The Remote UE includes its HPLMN ID, the Nonce\_1, the Remote UE ID and the KPC5 key ID received from the 5G PKMF-1 (Remote UE) together with the Relay Service Code. The Remote UE’s HPLMN ID is used by the UE-to-network relay’s 5G PKMF-2 to find the 5G PKMF-1 in the Remote UE’s HPLMN.

One option could be that the Remote UE uses the discovery key to confidentiality protect the KPC5 key ID over the PC5 interface due to privacy issues. This would imply that other Remote UEs belonging to different PLMNs and being authorized to access the same UE-to-network relay can decrypt and get access to the KPC5 key ID. But these other Remote UEs should not succeed in establishing a secure connection to the 5G PKMF-1(Remote UE).

There are two options described below: Option 1 and Option 2:

* In Option 1, the UE-to network relay contacts the Remote UE’s 5G PKMF-1 via its 5G PKMF-2. The Remote UE provides its HPLMN ID over the PC5 interface to the UE-to-network relay and the UE-to-network relay provides the HPLMN ID together with the Relay Service Code to its 5G PKMF-2 which can resolve the address of the Remote UE’s 5G PKMF-1.
* In Option 2, the UE-to-network relay retrieves the address of the Remote UE’s 5G PKMF-1 from its 5GDDNMF and contacts thereafter the Remote UE’s 5G PKMF-1 directly. The Remote UE provides its HPLMN ID over the PC5 interface to the UE-to-network relay and the UE-to-network relay provides the HPLMN ID together with the Relay Service Code to its 5GDDNMF which can resolve the address of the Remote UE’s 5G PKMF-1.

**Option 1: The UE-to network relay contacts the Remote UE’s** 5G **PKMF-1 via its** 5G **PKMF-2.**

Step 7) UE-to-network Relay establishes a secure connection with the 5G PKMF-2 (UE-to-network Relay) server. As this connection is established in the user plane, the same mechanism as used to protect the PC3 interface can be re-used e.g. either solution #5 or solution #11.

NOTE 3: There are business agreements between 5G PKMF-1(Remote UE) and 5G PKMF-2(UE-to-network relay) and therefore implicit trust in between 5G PKMF-1(Remote UE) and 5G PKMF-2(UE-to-network relay) so that 5G PKMF-1(Remote UE) relies on 5G PKMF-2(UE-to-network relay) having authenticated the UE-to-network relay.

Step 8) The UE-to-network Relay contacts the 5G PKMF-2(UE-to-network Relay) and includes the HPLMN ID of Remote UE, the Relay Service Code, Nonce\_1, the Remote UE ID and the UE-to-network relay ID in the Key Request message for PC5 communication including the KPC5 key ID. If the Remote UE’s HPLMN ID is provided then it is used by the UE-to-network relay’s 5G PKMF-2 to determine the 5G PKMF-1 in the Remote UE’s HPLMN, if configured.

NOTE 4: Whether the UE-to-network relay ID consists of one or more of the following parameters: ProSe application id, ProSe application user id and/or GPSI of the Remote UE is for SA2 to decide.

Step 9) The 5G PKMF-2(UE-to-network Relay) contacts the 5G PKMF-1(Remote UE) and forwards the Key Request message including the Relay Service Code, Nonce\_1, the Remote UE ID, KPC5 key ID and the UE-to-network relay ID to the 5G PKMF-1(Remote UE).

NOTE 5: The interface between the 5G PKMF-2(UE-to-network Relay) and the 5G PKMF-1(Remote UE) is out of the 3GPP scope.

Step 10a) The 5G PKMF-1(Remote UE) needs to contact the 5GDDNMF(Remote UE) to check if the Remote UE and the UE-to-network relay are allowed to communicate with each other by checking the Remote UE ID and the UE-to-network relay ID.

NOTE 6: The check of whether the Remote UE and the UE-to-network relay are allowed to communicate with each other could also be performed by the 5G PKMF-1 itself, if the 5G PKMF-1 (of Remote UE) has an SBI to the UDM (of Remote UE). In this case, the 5G PKMF-1 does not contact the 5GDDNMF (of Remote UE) as described in steps 10a and 10c. The 5G PKMF-1 (of Remote UE) performs step 10b instead of the 5GDDNMF.

Step 10b) If the 5GDDNMF(Remote UE) has not received the subscription information from the UDM, then the 5GDDNMF(Remote UE) contacts the UDM(Remote UE) in Nudm\_SDM\_Get to check if the Remote UE and UE-to-network relay are allowed to communicate with each other. The UDM(Remote UE) provides the subscription information to the 5GDDNMF(Remote UE) in Nudm\_SDM\_Get\_Response.

Step 10c) The 5GDDNMF(Remote UE) responds to the 5G PKMF-1(Remote UE) whether the authorization is successful or not.

Step 11) If the 5G PKMF-1(Remote UE) confirms the Remote UE can connect to the network via the selected ProSe UE-to- network Relay, 5G the PKMF-1(Remote UE) generates a new freshness parameter (i.e. KPC5-COM freshness parameter). The 5G PKMF-1 generates a new key KPC5-COM key from at least the KPC5 key, Nonce\_1, Relay Service Code and the new KPC5-COM freshness parameter. The generation of the KPC5-COM key can be done in a similar way as described in Annex A.7 in TS 33.303 if PRUK is replaced by KPC5 key. The 5G PKMF-1(Remote UE) includes the Remote UE ID, KPC5-COM freshness parameter, the KPC5-COM key ID and the KPC5-COM key in the Key Response message to the 5G PKMF-2(Remote UE).

NOTE 7: The interface between the5G PKMF-2(UE-to-network Relay) and the 5G PKMF-1(Remote UE) is out of the 3GPP scope.

Step 12) The 5G PKMF-2(UE-to-network Relay) forwards the Key Response message to the UE-to-network Relay.

**Option 2: The UE-to-network relay retrieves the address of the Remote UE’s** 5G **PKMF-1 and contacts** 5G **PKMF-1 directly**

Step 7a) UE-to-network Relay establishes a secure connection with the 5GDDNMF of the Relay UE. As this connection is established in the user plane, the same mechanism as used to protect the PC3 interface can be re-used. Either solution #5 or solution #11 can be used for securing the connection.

Step 7b) The UE-to-network Relay contacts the 5GDDNMF of the UE-to-network relay and includes the HPLMN ID of the Remote UE and the Relay Service Code.

Step 7c) The 5GDDNMF of the UE-to-network relay is using the HPLMN ID of the Remote UE and the Relay Service Code to determine the address of the 5G PKMF-1(Remote UE) and includes the address of the 5G PKMF-1(Remote UE) in the response message to the UE-to-network Relay.

NOTE 8: The 5GDDNMF of the Relay UE could be pre-configured with the address of the 5G PKMF-1(Remote UE) but this is for SA2 to decide.

Step 8a) The UE-to-network Relay uses the address of the 5G PKMF-1(Remote UE) and contacts directly the 5G PKMF-1(Remote UE). The UE-to-network Relay establishes a secure connection with the 5G PKMF-1 (Remote UE) server. As this connection is established in the user plane, the same mechanism as used to protect the PC3 interface can be re-used. Either solution #5 or solution #11 can be used for securing the connection. The UE-to-network relay is implicitly authenticated by the 5G PKMF-1(Remote UE) server when establishing the secure connection.

Editor’s note: Roaming aspects are not specified for AKMA yet. This is FFS in work item AKMA which is still specified in Rel-17. This applies only to Option 2 in this solution and not to Option 1.

Step 8b) The UE-to-network Relay initiates a Key Request message for PC5 communication including the KPC5 key ID, the Relay Service Code, Nonce\_1, the Remote UE ID and the UE-to-network relay ID. The 5G PKMF-1(Remote UE) checks if the Remote UE and the UE-to-network relay are allowed to communicate by checking the Remote UE ID and the UE-to-network relay ID.

Step 9a) The 5G PKMF-1(Remote UE) needs to contact the 5GDDNMF(Remote UE) to check if the Remote UE and UE-to-network relay are allowed to communicate with each other.

NOTE 9: The check of whether the Remote UE and the UE-to-network relay are allowed to communicate with each other could also be performed by the 5G PKMF-1 itself, if the 5G PKMF-1 has an SBI to the UDM (of Remote UE). In this case, the 5G PKMF-1 does not contact the 5GDDNMF-1 as described in step 9a. The 5G PKMF-1 performs step 9b instead of the 5GDDNMF.

Step 9b) If the 5GDDNMF (Remote UE) has not received this information earlier from the subscription in the UDM, then the 5GDDNMF (Remote UE) contacts the UDM (Remote UE) in Nudm\_SDM\_Get to check if the Remote UE and UE-to-network relay are allowed to communicate with each other. The UDM (Remote UE) provides the subscription information to the 5GDDNMF (Remote UE) in Nudm\_SDM\_Get\_Response.

Step 9c) The 5GDDNMF (Remote UE) responds to the 5G PKMF-1(Remote UE) regarding whether the authorization is successful or not.

Step 10) If the 5G PKMF-1(Remote UE) confirms the Remote UE can connect to the network via the selected ProSe UE-to- network Relay, the 5G PKMF-1(Remote UE) generates a new freshness parameter (i.e. KPC5-COM freshness parameter). The 5G PKMF-1 generates a new key KPC5-COM key from at least the KPC5 key, Nonce\_1, Relay Service Code and the new KPC5-COM freshness parameter. The generation of the KPC5-COM key can be done in a similar way as described in Annex A.7 in TS 33.303 if PRUK is replaced by KPC5 key. The 5G PKMF-1(Remote UE) includes the Remote UE ID, the KPC5-COM key, the KPC5-COM key ID and the KPC5-COM freshness parameter for PC5 communication identified by KPC5 key ID in the Key Response message to the UE-to-network Relay.

**Option 1 and Option 2:**

Step 13) The UE-to-network Relay generates a Nonce\_2. The UE-to-network Relay generates KSESS key from the KPC5-COM key and Nonce\_2. The UE-to-network Relay initiates a Direct Security Mode Command integrity protected with KSESS-IK key generated from the KSESS key. The UE-to-network Relay includes the KPC5-COM key ID and the KPC5-COM freshness parameter together with calculated MAC and the Nonce\_2 in the Direct Security Mode Command message.

Step 14) The Remote UE generates the KPC5-COM key in the same way as the 5G PKMF-1(Remote UE) in step 11 in Option 1 using the KPC5-COM freshness parameter. The Remote UE then generates the KSESS key from the KPC5-COM key and Nonce\_2. The Remote UE checks the integrity of the received Direct Security Mode Command by verifying the received MAC using a KSESS-IK key generated from the KSESS key. If the verification is successful, then the Remote UE sends a Direct Security Mode Complete message which is integrity protected and encrypted using the KSESS-IK key and the KSESS-CK key.

Step 15) The UE-to-network Relay responds with a Direct Communication Accept on the PC5 interface.

### 6.21.3 Evaluation

This solution resolves key issue #4 and key issue #9 and proposes to perform the key management for PC5 communication between the 5G PKMF and the Remote UE/UE-to-network relay over the user plane.

This solution is for commercial services. This solution describes how the Remote UE and the UE-to-network relay find out the address of the key management server (5G PKMF) which resides in Remote UE’s HPLMN, in order to be able to retrieve a common key for PC5 to communicate over the PC5 interface.

This solution assumes and requires 3GPP network connectivity for both Remote UE and UE-to-network relay.

There are two options described in this solution: Option 1 and Option 2.

In Option 1, the UE-to network relay contacts the Remote UE’s 5G PKMF-1 via its 5G PKMF-2. The Remote UE provides its HPLMN ID over the PC5 interface to the UE-to-network relay and the UE-to-network relay provides the HPLMN ID together with the Relay Service Code to its 5G PKMF-2 which can resolve the address of the Remote UE’s 5G PKMF-1.

In Option 2, the UE-to-network relay retrieves the address of the Remote UE’s 5G PKMF-1 from its 5GDDNMF and contacts thereafter the Remote UE’s 5G PKMF-1 directly. The Remote UE provides its HPLMN ID over the PC5 interface to the UE-to-network relay and the UE-to-network relay provides the HPLMN ID together with the Relay Service Code to its 5GDDNMF which can resolve the address of the Remote UE’s 5G PKMF-1. Security between Remote UE with Relay’s PKMF lists AKMA as a possible solution, but if Remote and Relay in Option 2 belong to different PLMNs it is not clear how this can be supported since roaming aspects are not specified for AKMA yet. Option 2 in this solution requires that roaming is specified in AKMA in Rel-17.

Option 1 seems more desirable than Option 2, as in Option 1, the UE-to-network relay does not need to retrieve the address of the Remote UE’s 5G PKMF-1 from its 5GDDNMF. Option 1 is more aligned with the direct discovery procedures where the 5GDDNMF’s in different PLMN’s have interfaces and communicate directly in between each other. The same approach could be used for the 5G PKMF’s in different PLMN’s as described in Option 1.

This solution aligns with the key management for the discovery keys for the UE-to-network relay which is also performed over the user plane.

In this solution, which is similar to the ProSe solution in 4G, if the Remote UE **re-connects to the same Relay UE** as it was previously connected to, then even if the Remote UE has a KPC5-COM key stored (previously used with the same Relay UE), the Remote UE provides the same KPC5 key ID to the Relay UE. The Relay UE connects to the PKMF and the network needs to perform the authorization and provide new keys as only the PKMF can calculate a new KPC5-COM key. In this case, the previously used KPC5-COM key is not re-used. This solution is different compared to the eV2X solution for PC5 communication, where the KNRP (equivalent to Prose KD in 4G or KPC5-COM key in this solution) can be reused if the Remote UE re-connects to the same Relay UE as it was previously connected to without having the Relay UE to connect to the PKMF in order to get a new KNRP (equivalent to Prose KD in 4G or KPC5-COM key in this solution)

This solution has no impact on network nodes as RAN, AMF, and AUSF.

This solution has an impact on network nodes; potentially 5GDDNMF and potentially UDM.

Solution #21 is similar to Solution #6, but differs as described below:

* In Solution #6, the Remote UE calculates a message authentication code (MACREAR) over the included ProSe parameters and includes the MACREAR in the Direct Communication Request to the UE-to-network relay. In Solution #21, no message authentication code (similar to MACREAR) is included in the Direct Communication Request.
* In Solution #21, the Remote UE and UE-to-network relay belongs to different HPLMN’s. In Solution #6, the Remote UE and UE-to-network relay belongs to the same HPLMN.

If the Remote UE wants to connect to a Relay UE, it means the Remote UE is almost out of coverage of the network, then it’s FFS how steps 2, 3a, and 3b can be performed as this solution may not work when the remote UE is not in 3GPP coverage.

Which network function provides the 5G PKMF address to the Remote UE is still to be decided.

“UE-to-network relay can connect to the 5G PKMF in Remote UE’s HPLMN via the UE-to-network relay’s 5G PKMF” adds a new requirement to the PKMF’s holder which is out of the scope of 3GPP.

The new changes compared to PKMF in LTE in TS 33.303 are as follows:

* The Remote UE’s HPLMN ID needs to be sent to the UE-to-network relay’s 5G PKMF.

SA2 has not defined the 5G DDNMF in the architecture for the UE-to-network relay scenario as proposed in this solution.

SA2 has not defined the 5G PKMF which manages security keys for PC5 communication in the architecture for the UE-to-network relay, as SA2 does not define PKMF in LTE. The 5G PKMF could interact with 5G DDNMF and UDM via SBI as described in the solution.

In LTE, the PKMF is only used for Public Safety.  However, in 5G we need also to support the commercial use case. It is very hard to have a single PKMF for all the applications that is independent of PLMNs. It’s unclear which authority should be responsible for maintaining the function for commercial use cases. This solution is proposing to reuse the logic of the 5G DDNMF (or the ProSe Function in LTE) or the 5G PKMF which is bound with the PLMN.

## 6.22 Solution #22: Representation of identities during broadcast

### 6.22.1 Introduction

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

The solution is based on the idea to use representations of the ProSe applications UEs provide - via announcing (i.e. broadcasting) and UEs want to discover - via monitoring (i.e. listening and filtering). Using a representation enables resistance to tracing and impersonation of UEs.

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

ProSE Direct Discovery procedure can partially work in out-of-coverage scenarios in the following sense: at the start of the discovery process, codes and filters are provided through a required connection with the 5GC. The connection with the 5GC can be direct or via a relay. After this step, the discovery process can continue out of coverage.

Provided codes and filters can have an associated validity timer. As long as these validity timers have not yet expired, ProSe Direct Discovery using these codes and filters can take place, even in out-of-coverage scenarios. After the expiry of the validity timers, the ProSE UEs need to (re)connect to the 5GC and request new codes and filters. Hence, after expiry, the ProSe Direct Discovery procedure can no longer be performed in out-of-coverage scenarios. The expired codes and filters need to be discarded both in the ProSe UEs and in the 5GC.

### 6.22.2 Solution details

#### 6.22.2.1 Solution for Model A

The solution for Model A consists of the following components:

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

- The use of a Discovery Filter (DF), which can be used by Monitoring UEs for recognizing and identifying the Announcing UE based on the ProSe application broadcast.

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



Figure 6.22.2.1-1 Direct discovery flows for Announcing UE

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

1. At the start of direct discovery the Announcing UE requests and receives from the 5GC a Discovery Code (DC) which is a representation of the ProSe application it provides; the DC originates in the 5G DDNMF in the 5GC and is carried in the Discovery Request message over the PC3 interface;

NOTE 1: The DC is carried in the response to the Discovery Request message, which is protected according to the solutions for Key Issue #10.

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



Figure 6.22.2.1-2 Direct discovery flows for Monitoring UE

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

1. At the start of direct discovery the Monitoring UE provides information on the ProSe application it wants to discover and receives from the 5GC a Discovery Filter (DF) which is to match the Discovery Code broadcast by Announcing UEs; the DF originates in the 5G DDNMF in the 5GC and is carried in the Discovery Request message over the PC3 interface;

NOTE 2: The Discovery Filter is constructed in the same way as has been described for LTE based ProSe (e.g. in clause 4.6.4.2a of TS 23.303 [5]).

NOTE 3: The DF is carried in the response to the Discovery Request message, which is protected according to the solutions for Key Issue #10.

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

#### 6.22.2.2 Solution for Model B

The solution for Model B consists of the following components:

- The use of a Query Code (QC), that is broadcast by the Discoverer UE for announcing its query in search for (one or more) Discoveree UEs; the Query Code represents the ProSe Application to be discovered by the Discoveree UE; the Query Code may also provide information about the Discoverer UE, so that the Discoveree UE can select whether or not to allow the Discoverer UE to discover the Discoveree UE;

- The use of a Query Filter (QF), that can be used by Discoveree UEs for recognizing the query sent by the Discoverer UE;

- The use of a Response Code (RC), that is broadcast by Discoveree UE for announcing its response to the query received from the Discoverer UE; the Response Code represents the application for which the Discoveree UE wants to be discovered;

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

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



Figure 6.22.2.2-1 Direct discovery flows for Discoverer UE

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

1. At the start of direct discovery the Discoverer UE requests and receives from the 5GC a Query Code (QC) and a Response Filter (RF); the Query Code is a representation of the ProSe application the Discoverer UE wants to discover and it may contain information on the Discoverer UE; the Response Filter is a representation of the Response Code broadcast by Discoveree UEs that can be used to check for a match; the QC and RF originate in the 5G DDNMF in the 5GC and are carried in the Discovery Request message over the PC3 interface;

NOTE 1 The Query Code is identical to the ProSe Query Code defined in TS 23.303 [5], which is a representation of a ProSe Application Code or ProSe Restricted Code.

NOTE 2: The Response Filter is constructed in the same way as has been described for LTE based ProSe (e.g. in clause 4.6.4.2a of TS 23.303 [5]).

NOTE 3: The QC and RF are carried in the response to the Discovery Request message, which is protected according to the solutions for Key Issue #10.

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

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



Figure 6.22.2.2-2 Direct discovery flows for Discoveree UE

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

1. At the start of direct discovery the Discoveree UE request and receives from the 5GC a Query Filter (QF) and a Response Code (RC); the Query Filter is a representation of the Query Code broadcast by Discoverer UEs that can be used to check for a match; the Response Code is a representation of the ProSe application for which the Discoveree UE wants to be discovered; the QF and RC originate in the 5G DDNMF in the 5GC and are carried in the Discovery Request message over the PC3 interface;

NOTE 4: The Response Code is identical to the ProSe Response Code defined in TS 23.303 [5], which is the representation of a ProSe Application Code or ProSe Restricted Code.

NOTE 5: The Query Filter is constructed in the same way as has been described for LTE based ProSe (e.g. in clause 4.6.4.2a of TS 23.303 [5]).

NOTE 6: The QF and RC are carried in the response to the Discovery Request message, which is protected according to the solutions for Key Issue #10.

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

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

### 6.22.3 Evaluation

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

Based on the ProSe Direct Discovery procedure defined in TS 23.303 [5], this solution clarifies how different discovery codes (e.g. Query Code, Response Code) are used to represent the ProSe application for which the UEs are discovering each other, and how the discovery filters (e.g. Query Filter, Response Filter) are used to identify the match between the UEs which want to conmmunicate on the same ProSe application. The codes/filters are generated by 5GC and used as the 3GPP layer representation for the identity of ProSe application to be discovered and requested. Hence, the privacy of the ProSe application in discovery is protected.

This solution has limited applicability in the out of coverage scenario due to need to get in coverage after the expiration of timers to invoke the ProSe Direct Discovery procedure.

The solution does not address the requirements in key issue #11, because it doesn't address the privacy of UE identity (e.g. Layer-2 IDs) broadcast during discovery in addition to the privacy of ProSe application.

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

### 6.23.1 Introduction

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

### 6.23.2 Solution details

#### 6.23.2.1 Overview

The solution involves the following steps:

1. A set of matching initial keys is provisioned to a selected set of authenticated and authorised ProSe UEs by the 5GC. Matching initial keys have identical validity times.

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

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

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

NOTE 3: The lifetime of the initial key and security context of a PC5 communication link are synchronised. Upon expiry of the initial key, the corresponding security context will also expire.

3. Upon expiration of the initial key, all keys derived from it will become invalid. In order to continue secure communication, ProSe UEs need to request a new initial key from the 5GC. Until they obtain the new initial key, ProSe UEs cannot perform direct communication with peer ProSe UEs.

#### 6.23.2.2 Procedures

Figure 6.23.2.2-1 shows the procedure of this solution. The initial key is referred to as AD-key at Announcing UE or Discoveree UE. It is referred to as MD-key at Monitoring UE or Discoverer UE. In the case of symmetric encryption, MD-Key is the same as AD-Key. In the case of asymmetric encryption, MD-Key and AD-Key are corresponding to each other. This key is the root of the security of one-to-one communication between ProSe UEs.



Figure 6.23.2.2-1: Procedure for provisioning and update of initial keys.

NOTE: Steps 1-4 refer to actions performed between Announcing UE or Discoveree UE (referred to as UE-1) and the 5GC.

1. UE-1 sends a Discovery request message to 5GDDNMF.

2. If UE-1 is authorised to perform ProSe direct communication, 5GDDNMF sends a key request to the 5G ProSe key management function.

3. 5G ProSe key management function sends a key response message with AD-key with its associated validity period, AD-key ID. It also keeps track of keys issued to various UEs.

4. AD-Key and AD-key ID are forwarded by 5GDDNMF to UE-1. This message also contains the address of the ProSe key management function. It would enable UE-1 to contact the ProSe key management function directly at later stages.

NOTE: Steps 5-8 refer to actions performed between Monitoring UE or Discoverer UE (referred to as UE-2) and the 5GC.

5. UE-2 sends a Discovery request message to 5GDDNMF.

6. If UE-2 is authorised to perform ProSe direct communication, 5GDDNMF sends a key request to 5G ProSe key management function.

7. 5G ProSe key management function sends a key response message with MD-key with its associated validity period, MD-key ID.

8. MD-Key and MD-key ID are forwarded by 5GDDNMF to UE-2. This message also contains the address of ProSe key management function. It would enable UE-2 to contact the ProSe key management function directly at later stages.

9. Establishment of security context over PC5 using the AD-key and MD-key , cf Solution #7, steps 2 to 6 as described in clause 6.7.2 of this document.

NOTE: Steps 10-12 refer to actions performed between Announcing UE or Discoveree UE (referred to as UE-1) and the 5GC.

10. Upon completion of the validity period, AD-key along with keys derived from it shall expire.

11. Address of ProSe key management function obtained in step 4 is used by UE-1 to perform a key request. This request also contains the identifier of the expired key.

12. A new key (AD-key-new) with an associated validity is issued to UE-1 along with its identifier.

NOTE: Steps 13-15 refer to actions performed between Monitoring UE or Discoverer UE (referred to as UE-2) and the 5GC.

13. Upon completion of the validity period, MD-key along with keys derived from it shall expire.

14. Address of the ProSe key management function obtained in step 4 is used by UE-2 to perform a key request. This request also contains the identifier of the expired key.

15. A new key (MD-key-new) with an associated validity is issued to UE-1 along with its identifier.

### 6.23.3 Evaluation

This solution addresses the following security requirement of key issue #12: "The system shall support means for a secure refresh of the UE security context.". It provides means for a secure refresh of the UE security context.

The benefits of this solution are that it prevents unbounded direct communication between ProSe UEs and secure direct communication between ProSe UEs is possible even when the ProSe UEs are out of coverage. By having a validity time to the matching initial keys, 5GC can limit the usage of direct communication even if ProSe UEs are out of coverage.

The drawback of the solution is that once the initial key expires, ProSe UEs cannot have direct communication. They need to contact the 5GC to obtain a new initial key.

## 6.24 Solution #24: NSSAA for Remote UE with L3 UE-to-Network relay

### 6.24.1 Introduction

The contribution proposes a solution to address KI #4: Authorization in the UE-to-Network relay scenario. The solution describes how to support a Network Slice-Specific Authentication and Authorization (NSSAA) procedure for a Remote UE connecting via an L3 UE-to-Network relay.

This solution proposes to use a Network-controlled authorization of Remote UE procedure as described in sol#10 (based on TR 23.752 Solution #47) with enhancements to enable the Remote UE to perform NSSAA for a given S-NSSAI (no dedicated solution is documented in TR 23.752[2] for the support of NSSAA for a Remote UE). The S-NSSAI subject to NSSAA is associated with the connectivity service (RSC) requested by the Remote UE. The RSC that requires Network-controlled authorization is configured in the Remote UE and the UE-to-Network relay which determines the associated S-NSSAI based on RSC requested by Remote UE (as per TR 23.752[2], Sol#35). The authentication messages for NSSAA of Remote UE are exchanged securely during or after the PC5 link establishment. Upon successful completion of the NSSAA procedure by the Remote UE, the relay provides Remote UE access to the slice.

This solution assumes that the AMF serving the relay is always able to serve the Remote UE (same as solution #10, clause 6.10.1). Moreover, the S-NSSAI associated with the connectivity service provided by the Relay is assumed to be the same for the Remote UE and Relay UE or that it can be mapped to the same S-NSSAI in the Relay serving PLMN.

### 6.24.2 Solution details

#### 6.24.2.1 PC5 link establishment with L3 UE-to-Network relay to use an S-NSSAI subject to NSSAA

The procedure for PC5 link establishment with L3 UE-to-Network relay to use an S-NSSAI subject to NSSAA is depicted in Figure 6.24.2-1.



Figure 6.24.2.1-1: Procedure for PC5 link establishment with L3 UE-to-Network relay to use an S-NSSAI subject to NSSAA

0. Remote UE is provisioned with authorization parameters to act as Remote UE. Relay UE is provisioned with authorization parameters to act as a Relay UE. Relay has registered for the S-NSSAI(s) associated with the services that are provided by the relay, including for the S-NSSAIs that are subject to NSSAA.

1. Remote UE and Relay perform a discovery procedure.

2. The Remote UE determines from the configuration provided in step 0 that the relay service code/type discovered in step 1 is associated with an S-NSSAI that is subject to NSSAA (e.g., based on an indication parameter for the S-NSSAI). Based on this determination, the Remote UE sends a DCR message including the RSC, a Remote UE's identity (e.g.,), and NSSAA capabilities.

3. Upon receiving the DCR message, the Relay may determine that a network-controlled authorization based NSSAA for Remote UE is required to provide Remote UE access to the slice. The determination may be based on any of the following conditions:

- Relay has performed NSSAA for the S-NSSAI (e.g., as performed in step 0). For example, during the NSSAA procedure, S-NSSAI is marked with an indication that it is subject to NSSAA.

- Based on configuration from step 0, the service provided (i.e., RSC) is associated with a particular S-NSSAI that is subject to NSSAA (e.g., based on an indication parameter for the S-NSSAI) or an indication that network-controlled authorization is required to use the relay service.

4. Upon receiving the DCR message including a Remote UE identity (e.g., SUCI), the relay decides to trigger a network-controlled authorization of Remote UE. The relay sends a NAS request message that includes the Remote UE id, the S-NSSAI, and Remote UE's NSSAA capabilities.

NOTE 2: If the Remote UE has a 5G native context established with the Relay UE's serving PLMN, it provides its 5G-GUTI (instead of SUCI) and the primary authentication steps below may be skipped as described in solution #10.

5. The AMF checks that the relay is authorized to act as a relay and is authorized to provide access to the S-NSSAI (e.g., S-NSSAI is part of Relay's UE Allowed NSSAI). Upon successful check, the AMF decides to trigger a primary authentication of Remote UE via the relay.

6. The Remote UE performs a primary authentication procedure via the relay. Authentication messages are transported over NAS messages between the AMF and Relay. The NAS messages include an indication (e.g., Remote UE's GPSI, Remote User Id, or any id provided by Remote UE in message 2) that the authentication messages are for the Remote UE. The relay forwards those messages transparently between Remote UE and AMF.

7. Upon successful authentication procedure, the AMF checks with Remote UE's UDM that Remote UE is authorized to use the relay and has S-NSSAI as part of its subscription. If S-NSSAI is subject to NSSAA, AMF verifies that Remote UE supports NSSAA from the capabilities received from the Relay. AMF registers with Remote UE's UDM (including information about serving Relay) to handle further UDM subscription notifications or to handle revocation/re-authentication requests for Remote UE from AAA-S.

Following successful subscription-based authorization checks, AMF generates key material to authorize and enable secure communication between the Relay and Remote UE. The generated key material is derived from the key material generated during the primary authentication with the Remote UE. Upon successful authentication procedure, the Remote UE generates key material for securing communication with relay the same way as AMF.

8. Upon successful completion of the authentication procedure, the AMF sends a NAS response message that includes the Remote UE id (e.g., GPSI), the generated key material, the S-NSSAI, NSSAA status which indicates whether NSSAA is to be performed, ongoing or successful (e.g., if initiated or performed successfully from a previous registration). If primary authentication or subscription-based authorization check fails, the NAS message indicates a failure cause (e.g., S-NSSAI not authorized).

NOTE 3: Remote UE may have performed successfully or initiated NSSAA for the S-NSSAI from a previous Registration with Relay UE's AMF or another AMF. In that case, the Relay UE's AMF may retrieve the current NSSAA status from the Remote UE context (as described in sol#10).

9. The relay establishes the PC5 link security with the Remote UE using the key material generated from step 7. This step is skipped in case of failure indication in message 8.

10. The relay may send an ack message to confirm the PC5 link security establishment to the AMF. AMF may trigger the NSSAA procedure upon receiving this message illustrated in Figure 6.24.2.2-1.

11. The relay sends a DCA message including indication for NSSAA status (e.g., pending, required, successful) and S-NSSAI to Remote UE. In case of failure indication in message 8, the relay sends a reject message to the Remote UE including the failure cause.

12. If NSSAA is required, an NSSAA procedure for Remote UE via Relay may be triggered by Relay as illustrated in Figure 6.24.2.2-1.

13. Upon successful completion of the NSSAA procedure, the relay sends a PC5 message (e.g., a PC5 Link Modification Request) that includes a successful NSSAA indication, the authorized S-NSSAI. If the NSSAA procedure fails, the relay may release the PC5 link indicating the failure cause.

In the above procedure, the NSSAA procedure is triggered after the relay sends the DCA message to the Remote UE. Alternatively, the NSSAA procedure may be triggered during the PC5 link establishment (e.g., NSSAA triggered after successful completion of DSMC procedure and before sending DCA to Remote UE). Upon successful NSSAA procedure, the relay sends a DCA message that includes a successful NSSAA indication and the authorized S-NSSAI. If the NSSAA fails, the relay may send a PC5 reject message indicating the failure cause.

Upon successful NSSAA procedure, the relay may send a NAS message (e.g., PDU Session Modification, Establishment request, or Remote UE Report) to the SMF to provide connectivity to the Remote UE. The message may include the Remote UE User id and Remote UE addressing info (e.g., IP or MAC address) and other PDU Session parameters (e.g., S-NSSAI, DNN). The SMF receives the message from AMF which includes the Remote UE's SUPI, obtained by AMF during primary authentication of Remote UE (see step 6 above). Using Remote UE SUPI, AMF can verify that Remote UE is authorized to access the selected DNN according to existing procedures (see TS 23.502 [10], clause 4.3.2.2.1) before sending the request message to SMF.

#### 6.24.2.2 NSSAA of Remote UE connecting via L3 UE-to-Network relay

The procedure for NSSAA of Remote UE connecting via L3 UE-to-Network relay is depicted in Figure 6.24.2.2-1.



Figure 6.24.2.2-1: Procedure for NSSAA of Remote UE connecting via L3 UE-to-Network relay

1. The relay UE or the AMF may decide to trigger an NSSAA procedure for the Remote UE according to conditions as described in Figure 6.24.2.1-1 (i.e., successful completion of network controlled authorization procedure, confirmation of PC5 link security establishment from Relay). If the procedure is triggered by AMF steps 2 and 3 are skipped. If the procedure is triggered by Relay step 8 is skipped.

2. The Relay sends a NAS request message to the AMF that includes the Remote UE id (e.g., SUPI, GPSI) and S-NSSAI.

3. The AMF checks that the relay is authorized to act as a relay and is authorized to provide access to the S-NSSAI (e.g., S-NSSAI is part of Relay's UE Allowed NSSAI) and that NSSAA is to be performed for Remote UE to use S-NSSAI (e.g., based on NSSAA status associated with S-NSSAI/Remote UE stored in Relay UE context). Upon successful check, the AMF decides to trigger a primary authentication of Remote UE via the relay.

4. The Remote UE performs an NSSAA procedure via the relay. Authentication messages are transported over NAS messages between the AMF and Relay. The NAS messages include an indication (e.g., Remote UE's GPSI) to inform the Relay that authentication messages are for the Remote UE. The relay forwards those messages transparently between Remote UE and AMF. AMF may receive authorization information from AAA-S for the Remote UE to use the S-NSSAI (e.g., a time limit).

5. Upon successful completion of the NSSAA procedure, the AMF updates the S-NSSAI status information associated with Remote UE in Relay UE context (e.g., mark S-NSSAI as Allowed for Remote UE).

6. The AMF sends a NAS message to the relay indicating the result of the NSSAA procedure, including an identity of the Remote UE, S-NSSAI and optionally authorization information associated with S-NSSAI (as provided by the AAA-S).

7. On the condition of successful NSSAA, the relay stores S-NSSAI authorization information for Remote UE.

8. The relay sends a NAS message to acknowledge message 6 from AMF.

The Relay UE proceeds with the rest of the PC5 link setup with relay using S-NSSAI subject to NSSAA as illustrated in Figure 6.24.2.1-1.

#### 6.24.2.3 AAA-S triggered Authorization Revocation to use S-NSSAI for Remote UE

The procedure for AAA-S triggered Authorization Revocation to use S-NSSAI for Remote UE in Figure 6.24.2.3-1.

 Figure 6.24.2.3-1: Procedure for AAA-S triggered Authorization Revocation to use S-NSSAI for Remote UE

0. Remote UE is connected to the Relay UE and authorized to use an S-NSSAI subject to NSSAA.

1. NSSAAF receives an authorization revocation request from AAA-S. The request includes the GPSI of the Remote UE.

NOTE: Existing protection mechanisms for communications between NSSAAF and AAA-S as per TS 33.501 [14] are assumed (e.g., for the privacy of GPSI, S-NSSAI).

2. NSSAAF requests UDM to get the ID of the AMF serving the Remote UE. NSSAAF receives AMF ID and Relay UE GPSI (UDM has obtained info about Relay UE and its AMF prior, see clause 6.24.2.1, step 7).

3. NSSAAF notifies AMF about the S-NSSAI authorization revocation for Remote UE, providing both Remote UE and Relay UE's GPSI.

4. AMF locates the Relay UE context and removes the association of Remote UE with S-NSSAI in the Relay UE context. If no other S-NSSAI is used for Remote UE via the Relay UE, the AMF removes the Remote UE information from the Relay UE context. AMF de-registers from the Remote UE's UDM if Remote UE info is removed from the Relay UE context.

5. AMF sends a NAS command message to the Relay including the Remote UE ID (e.g., GPSI) and S-NSSAI to revoke authorization of Remote UE to use S-NSSAI.

6. The Relay UE discards S-NSSAI authorization information associated with Remote UE including Krelay/Krelay ID.

7. The Relay UE initiates a Link Release procedure and provides Remote UE with the appropriate link release cause.

8. The Relay UE sends a response to the AMF to ack the command.

The re-authentication/authorization procedure is similar to the authorization revocation procedure above. The differences are as follows:

* Upon receiving a re-authentication request from AAA-S via NSSAAF for the Remote UE, the AMF triggers NSSAA of Remote UE via Relay procedure as illustrated in clause 6.24.2.2.
* If NSSAA fails, Figure 6.24.2.3-1 steps 4 – 8 are performed.

#### 6.24.2.4 AAA-S triggered Authorization Revocation to use S-NSSAI for Relay UE

The procedure for AAA-S triggered Authorization Revocation to use S-NSSAI for Relay UE. The messages 1-3, 5 and 8 are the same as TS 33.501[14], Figure 16.5-1 steps 1-4.

 Figure 6.24.2.3-1: Procedure for AAA-S triggered Authorization Revocation to use S-NSSAI for Relay UE

0. Remote UE is connected to the Relay UE and authorized to use an S-NSSAI subject to NSSAA.

1. NSSAAF receives an authorization revocation request from AAA-S. The request includes the GPSI of the Relay UE.

NOTE: Existing protection mechanisms for communications between NSSAAF and AAA-S as per TS 33.501 [14] are assumed (e.g., for the privacy of GPSI, S-NSSAI).2. NSSAAF requests UDM to get the ID of the AMF serving the Relay UE. NSSAAF receives AMF ID.

3. NSSAAF notifies AMF about the S-NSSAI authorization revocation for Relay UE, providing Relay UE's GPSI and S-NSSAI.

4. AMF locates the Relay UE context and for each Remote UE associated with the revoked S-NSSAI in the Relay UE context the AMF removes the association of Remote UE with S-NSSAI (e.g., NSSAA status) from the Relay UE context. If no other S-NSSAI is used for Remote UE, the AMF removes the Remote UE information from the Relay UE context. AMF de-registers from the Remote UE's UDM if Remote UE info is removed from the Relay UE context.

5. AMF initiates a UCU procedure with the Relay to revoke the authorization for the relay to use the S-NSSAI.

6. For each Remote UE associated with the revoked S-NSSAI, the Relay UE discards S-NSSAI authorization information associated with Remote UE including Krelay/Krelay ID.

7. For each Remote UE connected to the relay and associated with the revoked S-NSSAI, the relay initiates a link release procedure.

8. The Relay completes the UCU procedure. If the Relay is left with no Allowed NSSAI and no default S-NSSAI can be provided to the Relay UE. The Relay is de-registered by the AMF, and the Relay UE releases any active link with Remote UE(s).

### 6.24.3 Evaluation

This solution proposes a mechanism to authorize a Remote UE to access a specific slice that requires NSSAA via an L3 UE-to-Network Relay using a network-controlled authorization procedure. This solution fully addresses the requirements in KI#4 in the case of slice access that requires NSSAA.

Impacts on 5GC and Remote UE/Relay UE to support the network-controlled authorization procedure are documented in sol#10 evaluation. Other KIs covered in sol#10 (e.g., KI#3, KI#5 etc) are not in scope of this solution.

This solution requires a new relayed NSSAA procedure that needs to be supported by the AMF and the Relay UE. For impact of NSSAA support, the following capabilities are required:

* Remote UE has to support EAP authentication procedure via Relay UE
* Relay UE has to support relay of EAP authentication procedure towards the Remote UE
* AMF has to be able to trigger Remote UE NSSAA based on Remote UE subscription and perform NSSAA for the Remote UE via Relay UE

In this solution, AMF is required to support triggering NSSAA for the Remote UE as part of a new network-controlled authorization procedure instead of the Registration procedure.

The solution supports Remote UE operating in or out of coverage.

The solution supports the roaming scenario while complying with LI requirements, i.e., allowing LI to take place in VPLMN using Remote UE's SUPI.

Editor's Note: the impact on 5GC and the existing procedures needs to be evaluated in consultation with SA2.

Editor's Note: Further evaluation is FFS.

## 6.25 Solution #25: Secondary authentication of Remote UE with L3 UE-to-Network relay

### 6.25.1 Introduction

The contribution proposes a solution to address KI #4: Authorization in the UE-to-Network relay scenario. The solution describes how to support a secondary authentication of a Remote UE via an L3 UE-to-Network relay.

During a PC5 link establishment procedure, the UE-to-Network relay enables a Remote UE to perform a PDU Session establishment with secondary A&A following a network-controlled authorization of Remote UE, where the UE-to-Network Relay reports Remote UE's SUCI to network, as described in sol#10. The EAP authentication messages for secondary A&A of Remote UE are exchanged over a secure d PC5 link during or after the PC5 link establishment. Upon successful completion of PDU Session with secondary A&A for Remote UE, the relay provides Remote UE access to the PDU Session. The PDU Session may be shared among multiple Remote UEs.

To maintain compliance with the pre-requisites specified for the existing PDU Session with secondary A&A (see TS 23.501 [15], clause 5.6.6), the PDU Session with secondary A&A for a Remote UE via Relay UE takes place in addition to the Remote UE primary authentication by Relay UE's AMF and PDU Session authorization enforced by Relay UE's SMF with regard to subscription data retrieved from Remote UE's UDM. Remote UE's primary authentication and access to subscription data are enabled via the network-controlled authorization procedure.

### 6.25.2 Solution details

#### 6.25.2.1 PC5 link establishment with L3 UE-to-Network relay to use a PDU Session subject to secondary A&A

The procedure for PC5 link establishment with L3 UE-to-Network relay to use a PDU Session subject to secondary A&A is depicted in Figure 6.25.2.1-1.



Figure 6.25.2.1-1: Procedure for PC5 link establishment with L3 UE-to-Network relay to use a PDU Session subject to secondary A&A

0. Remote UE is provisioned with authorization parameters to act as Remote UE. Relay UE is provisioned with authorization parameters to act as a Relay UE.

1. The Relay may perform a PDU Session with secondary A&A by DN-AAA. It is assumed that the Relay is provisioned with credentials used during this procedure.

2. The Remote UE and Relay UE perform a discovery procedure whereby the Remote UE may discover the connectivity service provided by the Relay (e.g., based on a broadcasted service code).

3. The Remote UE may determine from the configuration in step 0 that the service code is associated with a DN that requires secondary A&A. Based on this determination, the Remote UE sends a DCR message including its identity (e.g., SUCI).

4. Upon receiving the DCR message, the Relay may determine that a network controlled authorization is needed before trying to fulfil the Remote UE PC5 connection request. The determination may be based on any of the following conditions:

- an existing PDU session that can satisfy the Remote UE connectivity requirements (e.g., as established in step 1) is marked with an indication that secondary A&A is required

- from the configuration in step 0, the service code is associated with a DN that is marked with a parameter indicating that it requires network controlled authorization.

If the network controlled authorization is not required the Relay may proceed according to the procedure described in 23.752 [2], clause 6.6.

5. On the condition that the DCR message includes a SUCI, the relay triggers a network-controlled authorization of Remote UE, as described in sol#10. Alternatively, the relay may send an identity request message to the Remote UE to obtain the Remote UE identity (e.g., SUCI) before triggering the network-controlled authorization procedure of Remote UE if the procedure is required as per step 4. If the Remote UE fails to provide its identity required for network-controlled authorization, the relay rejects the connection request and provides in the rejection message a cause indicating that a required identity parameter (e.g., SUCI) is missing.

6. Upon successful network-controlled authorization of Remote UE procedure the Relay initiates a Direct Security Mode Command procedure with Remote UE to establish the security of the PC5 link. The security of the PC5 link may be established as described in sol#10.

7. Upon successful security establishment, the relay sends a DCA message that may include an indication that a PDU Session with secondary A&A is pending. The relay may allocate an IP address or IPv6 prefix to the Remote UE. The relay may configure a traffic filter (e.g., as a default filter for IP or non-IP traffic) for the PC5 link to prevent any data traffic until successful completion of subsequent PDU Session secondary A&A (next step). Based on the indication in the DCA message, the Remote UE may refrain from sending any data traffic over the PC5 link until successful completion of subsequent PDU Session secondary A&A.

8. The relay triggers a PDU Session secondary A&A over relay procedure (e.g., as described in Figure 6.25.2.2-1).

9. Upon successful PDU Session with secondary A&A over relay procedure, the relay sends a PC5 message (e.g., a PC5 Link Modification Request) that includes a successful indication, that may include an EAP success message (received from SMF in step 8). The relay may configure the link to allow data traffic between the Remote UE and the network/DN (e.g., remove the filter configured in step 7). If the PDU Session with secondary A&A fails, the relay may release the PC5 link indicating the failure cause. The reject message may include the EAP failure message (received from SMF in step 8).

In the above procedure, the PDU Session secondary A&A procedure is triggered after the relay sends the DCA message to the Remote UE. Alternatively, the relay may trigger the PDU Session secondary A&A during the link establishment procedure (e.g., trigger PDU Session secondary A&A after successful completion of DSMC procedure and before sending DCA to Remote UE). In this case, secure PC5-S messages may be used to carry EAP authentication messages for the PDU Session secondary A&A to/from the Remote UE. Upon successful PDU Session with secondary A&A of Remote UE, the relay sends a DCA message that includes a successful secondary A&A indication. The message may include an EAP success message (received from SMF in step 8). If the PDU Session with secondary A&A fails, the relay sends a PC5 reject message indicating the failure cause. The reject message may include the EAP failure message (received from SMF).

#### 6.25.2.2 PDU Session secondary A&A of Remote UE via L3 UE-to-Network relay

The procedure for PDU Session secondary A&A of Remote UE via L3 UE-to-Network relay is depicted in Figure 6.25.2.2-1.



Figure 6.25.2.2-1: Procedure for PDU Session secondary A&A of Remote UE via L3 UE-to-Network relay

1. The relay UE decides to trigger a PDU Session secondary A&A for the Remote UE according to conditions, as described in Figure 6.25.2.1-1.

2. The Relay sends a NAS message (e.g., PDU Session Modification or Establishment request or Remote UE Report) to the SMF. The message may include the Remote UE User id and Remote UE addressing info (e.g., IP or MAC address) and other PDU Session parameters (e.g., S-NSSAI, DNN). The SMF receives the message from AMF which includes the Remote UE's SUPI, obtained by AMF during a controlled authorization of Remote UE procedure as described in sol#10.

NOTE 1: In the case of Home Routed roaming, the SMF in the call flow is the H-SMF (and the V-SMF is not shown for simplicity). SMF selection by AMF is performed as per TS 23.502 [10], clause 4.3.2.2.3 (e.g., using PLMN ID of the SUPI, S-NSSAI, etc.).

3. The SMF determines based on Remote UE's subscription information (i.e., Secondary authentication indication as per TS 23.502 [10], Table 5.2.3.3.1) that the requested DN is subject to secondary A&A and triggers a PDU Session secondary A&A of Remote UE via Relay.

4. The Remote UE performs a PDU Session secondary A&A via the Relay. Authentication messages are transported over NAS messages between the SMF and Relay. The NAS messages include an identity of the Remote UE (e.g., GPSI, Remote User Id) to indicate to the Relay that authentication messages are for the Remote UE. The relay forwards those messages transparently and securely between Remote UE and SMF. The SMF maintains an N4 session with DN-AAA for all UEs sharing the PDU Session as long as the PDU Session is not released. DN-AAA may allocate and assign an IP address/IPv6 prefix for the Remote UE during the procedure. The DN-AAA may authorize QoS parameter (e.g., session AMBR) for the Remote UE using the shared PDU Session.

NOTE 2: Details on support for DN-AAA allocation of address/IPv6 prefix and DN-AAA authorized QoS parameters for a shared PDU Session will be determined during the normative phase. The architectural aspects will be coordinated with SA WG2.

5. Upon successful PDU Session secondary A&A via the Relay procedure, the SMF stores the Remote UE information in the Relay Session Management context including Remote UE identity (e.g., SUPI or GPSI), individual authorization information (e.g., assigned IP, QoS parameters) received from DN-AAA.

6. The SMF sends a NAS message (e.g., PDU Session Modification or Establishment response or Remote UE Report ack) to the relay indicating the result of the PDU Session secondary A&A, including an identity of the Remote UE (e.g., GPSI, Remote User Id), an EAP success or failure message. In the case of successful secondary A&A, the message may include addressing and QoS authorization info for the relay to respectively apply and enforce.

7. In the case of successful secondary A&A, the relay stores any received authorization info associated with the Remote UE. The Relay UE proceeds with the rest of the PC5 link setup with Remote UE as described in Figure 6.25.2.1-1.

#### 6.25.2.3 DN-AAA triggered PDU Session Authorization Revocation for Remote UE

The procedure for DN-AAA triggered PDU Session Authorization Revocation for Remote UE is depicted in Figure 6.25.2.3-1.



Figure 6.25.2.3-1: procedure for DN-AAA triggered PDU Session Authorization Revocation for Remote UE

0. The Remote UE is connected to the Relay UE and authorized to use PDU Session subject to secondary A&A.

1. The SMF receives an authorization revocation request from DN-AAA via UPF. The request includes the GPSI of the Remote UE and addressing info (e.g., IP/MAC address).

2. The SMF identifies the PDU Session/Relay UE SM context and removes Remote UE information from Relay UE SM context and may release any address allocated for the Remote UE. SMF configures the UPF to drop any remaining packets associated with the Remote UE. The SMF retains the N4 session with the DN-AAA to continue serving other UEs (including Relay UE) that are still sharing the PDU Session.

3. The SMF sends a NAS command message to release the connection with the Remote UE whose authorization has been revoked. The message includes the Remote UE identity (e.g., Remote User Id, GPSI), Remote UE addressing info, and an indication of the reason for the release.

4. The Relay UE initiates a PC5 link release procedure with the Remote UE.

5. The Relay acknowledges the NAS command message.

NOTE: if DN-AAA revokes Relay UE authorization for the PDU Session the SMF may release the PDU Session as specified in sub-clause 4.3.4 of TS 23.502[10] and the Relay UE initiates a Link Release procedure with all Remote UE(s) sharing the released PDU Session.

#### 6.25.2.4 DN-AAA triggered PDU Session Re-Authentication/Authorization for Remote UE

The procedure for DN-AAA triggered PDU Session Re-Authentication/Authorization for Remote UE is depicted in Figure 6.25.2.4-1.



Figure 6.25.2.4-1: Procedure for DN-AAA triggered PDU Session Re-Authentication/Authorization for Remote UE

0. The Remote UE is connected to the Relay UE and authorized to use a PDU Session subject to secondary A&A.

1. The SMF receives a re-authentication/authorization request from DN-AAA via UPF. The request includes the GPSI of the Remote UE and addressing info (e.g., IP/MAC address).

2. The SMF identifies the PDU Session/Relay UE SM context and retrieves the Remote UE information from Relay UE SM context based on the provided information.

3. The SMF initiates a procedure of PDU Session secondary A&A of Remote UE via Relay procedure as described in clause 6.25.2.2, step 4.

4. If new authorization information is provided by DN-AAA the SMF updates the Remote UE info in the Relay UE SM context accordingly.

5. The SMF sends a NAS message (e.g., PDU Session Modification Command) to the relay indicating the result of the PDU Session secondary re-authentication/re-authorization, including Remote UE Id (e.g., GPSI, Remote User Id), an EAP success or failure message. In the case of successful secondary re-A&A, the message may include new authorization information associated with the Remote UE connection.

6. In case of successful secondary re-A&A of Remote UE, the Relay UE updates any authorization info associated with the Remote UE with new info received from SMF. The relay sends a PC5 message (e.g., a PC5 Link Modification Request) that includes an EAP success message. In case of a failed re-A&A procedure, the relay initiates a PC5 link release procedure with Remote UE.

7. The Relay acknowledges the NAS command message from SMF.

### 6.25.3 Evaluation

This solution proposes a mechanism to authorize a Remote UE to access a DN that requires a secondary A&A via L3 UE-to-Network relay using a network-controlled authorization procedure. This solution fully addresses the requirements in KI#4.

Impacts on 5GC and Remote UE/Relay UE to support the network-controlled authorization procedure are documented in sol#10 evaluation. Other KIs covered in sol#10 (e.g., KI#3, KI#5 etc) are not in scope of this solution.

For impact of secondary authentication support, the following capabilities are required:

* Remote UE has to support the EAP authentication procedure via Relay UE
* Relay UE has to support the relaying of EAP authentication procedure towards the Remote UE.
* SMF has to be able to trigger Remote UE secondary authentication based on Remote UE subscription and perform secondary authentication for the Remote UE via Relay UE

The solution supports both Home Routed and Local breakout scenarios while reusing existing SMF selection mechanisms.

The solution supports Remote UE operating in or out of coverage.

The solution supports the roaming scenario while complying with LI requirements, i.e., allowing LI to take place in VPLMN using Remote UE's SUPI.

Editor's Note: the impact on 5GC and the existing procedures needs to be evaluated in consultation with SA2.

Editor's Note: Further evaluation is FFS.

## 6.26 Solution #26: Protecting PDU session-related parameters for L2 relay with existing mechanism

### 6.26.1 Introduction

This solution addresses Key Issue #16: Privacy protection of PDU session-related parameter for relaying. In the L2 UE-to-network relay scenario, the PDU session-related parameters in the communications after initial registration between remote UE and core network transparently pass the relay with protected AS and NAS security. Hence only privacy sensitive PDU session-related parameters during initial registration are needed to be protected, specifically speaking, the NSSAI information in the initial registration messages.

This solution proposes to reuse the existing mechanism in order to protect the PDU session-related parameters that may be exposed to the UE-to-network relay in clear during initial registration.

### 6.26.2 Solution details

Based on the threat mentioned in Key Issue #16, exposing slice and DNN information may violate privacy about a UE’s special subscription group belongings. During the UE-to-Network relay discovery and PC5 connection setup, DNN and slice information are not included in the UE-to-Network Relay Discovery messages (both Model A and Model B) and PC5 connection setup as specified in solution #7 and clause 8.2 of TR 23.752 [2], respectively. The only privacy sensitive PDU session-related parameter that may expose to the L2 UE-to-network relay is the NSSAI information in the initial registration message as the subsequent parameters are covered by the protected AS and NAS information. This solution proposes to reuse the existing mechanism to protect PDU session-related parameters for L2 relay:

If the operator decides to protect the privacy of PDU session-related parameter(s) (i.e. slice information) for L2 relay, AMF shall provide the remote UE an ‘Access Stratum Connection Establishment NSSAI Inclusion Mode’ parameter in the Registration Accept message during the registration procedure. This parameter indicates the Remote UE to not include any NSSAI in the Access Stratum (AS), as specified in the mode (d) in 23.501 [15] clause 5.15.9. The remote UE shall by default not provide NSSAI in the AS under UE-to-network relay scenario unless it has been provided with an indication to operate in other modes as specified in 23.501[15] clause 5.15.9.

The subsequent communications between remote UE and the core network are sent with AS and NAS security, thus the PDU session-related parameters (e.g. requested NSSAI, requested DNN) are prevented to be read by the UE-to-network relay.

### 6.26.3 Evaluation

The L2 UE-to-network relay doesn’t introduce any new security vulnerabilities related to Key Issue #16 and the existing mechanism in TS 23.501 [15] is capable to fulfil the security requirements of KI#16 to prevent tracing and tracking privacy attacks on the remote UE caused by exposing PDU session-related parameters.

## 6.27 Solution #27: Mitigating the conflict between security policies using match report procedures

### 6.27.1 Introduction

This solution addresses Key Issue #1 and Key Issue #12, including how to get the security materials to protect discovery and avoids one-to-one communication failure in advance. Two UEs should finish the discovery procedure and the direct one-to-one communication establishment before actually starting direct one-to-one communication (i.e. the discovery request procedures are prerequisite steps of direct one-to-one communication).

Security flexibility is provided by introducing on-demand PC5 one-to-one communication policies. The security policies for ProSe UEs may be provisioned by different PCFs and they might issue different values. PC5 security policies are provisioned according to different services and geographical area(s) based on the referenced technology in TS 33.536 [8] and TS 23.287 [9]. The referenced technology, eV2X unicast in 33.536 [8], still has a mechanism to abort the PC5 unicast establishment upon policy mismatch (e.g. NOT NEED and REQUIRED) if the peer UE replies to the annunciation of the same v2x service from the initiating UE. This shows the security policies on each UE may not the same for the same service/ProSe Code. Moreover, UEs still need to negotiate final security activation status according to the real-time conditions and the network has no such real-time information. For the above reasons, the conflict between security policies may cause one-to-one communication establishment failure and make the previous discovery request procedures in vain. To avoid connection failure caused by the conflict between policies, this contribution proposes to check the policy match in advance with the help of the match report procedures specified in TS 33.303 [6] for 5G ProSe open discovery and restricted discovery.

NOTE: This solution does not work with the V2X based direct discovery (e.g. clause 6.2 in TR 23.752 [2]).

### 6.27.2 Solution details

NOTE: This solution assumes all the security policies are provisioned/configured to UE with the existing ways as specified in clause 5.1 of TS 23.304 (i.e. provisioned in ME, configured in the UICC, from ProSe application server via PCF/PC1 reference point, and/or from PCF). The security policies for ProSe Services are not provisioned or configured to UE from 5G DDNMF. 5G DDNMF may get security policies from PCF.

NOTE: This solution requires network coverage to work.

#### 6.27.2.1 Open discovery scenario

Mitigating security conflict between policies using open discovery match report procedures is described as follows:

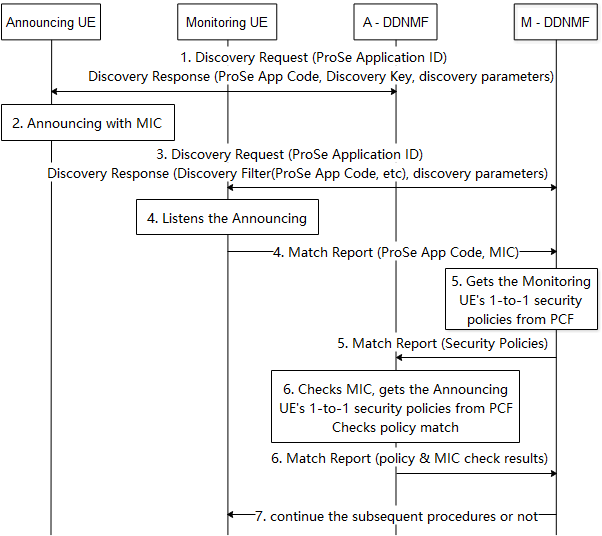


Figure 6.27.2.1-1: Check the conflict between policies using open discovery match report

1. The Announcing UE sends a Discovery Request message containing the ProSe Application ID to the DDNMF in its HPLMN (A-DDNMF) to get permission to announce on its serving PLMN. The A-DDNMF returns the ProSe App Code, Discovery Key and other discovery parameters in the Discovery Response message. This step reuses the procedures as specified in TS 33.303 [6].
2. The Announcing UE starts announcing with a Message Integrity Check (MIC) calculated by using the Discovery Key as described in TS 33.303 [6].
3. The Monitoring UE sends a Discovery Request message containing the ProSe Application ID to the DDNMF in its HPLMN (M-DDNMF) to get the parameters for monitoring. The DDNMF returns the Discovery Filter containing the ProSe App Code(s) and/or the ProSe App Mask(s) with other discovery parameters in the Discovery Response message. The M-DDNMF and A-DDNMF exchange Monitor Req/Resp messages if the ProSe Application ID indicates a different PLMN. This step reuses the procedures as specified in TS 33.303 [6].
4. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter. On hearing the 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 M-DDNMF. The Match Report includes the ProSe App Code and MIC.
5. The M-DDNMF gets the Monitoring UE’s ProSe one-to-one communication security policies of the service related to the ProSe App Code from PCF and passes the policies to the A-DDNMF in the Match Report message. The one-to-one communication security policies are used to establish security during one-to-one communication establishment.
6. The A-DDNMF shall check the MIC is valid. The A-DDNMF also gets the security policies of the Announcing UE for direct one-to-one communication service related to the ProSe App Code from PCF and checks if the security policies of the Monitoring UE and the policies of the Announcing UE are not in conflict. If the MIC check passes and the security policies are not in conflict with each other, the A-DDNMF shall acknowledge a successful check of the MIC to the M-DDNMF in the Match Report Ack message, otherwise, it shall acknowledge the check failure.
7. The M-DDNMF acknowledges the Monitoring UE to continue the subsequent procedures if passing the checks in step 6. Otherwise, the M-DDNMF indicates the Monitoring UE to stop the procedure.

#### 6.27.2.2 Restricted discovery scenario

Mitigating security conflict between policies using restricted discovery match report procedures is described as follows:

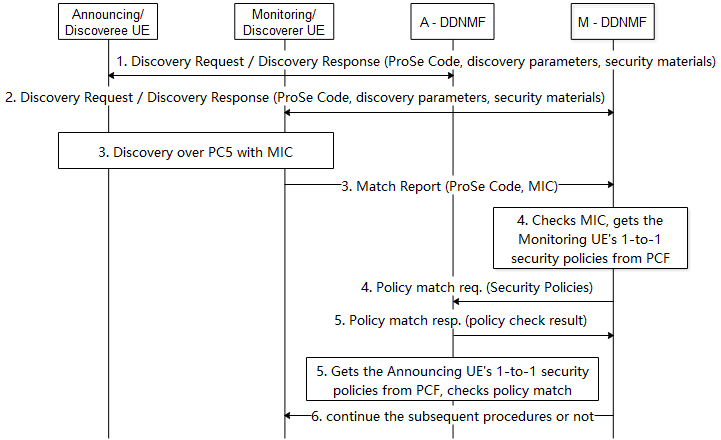


Figure 6.27.2.2-1: Check the conflict between policies using open discovery match report

1. The Announcing/Discoveree UE sends a Discovery Request message to the DDNMF in its HPLMN (A-DDNMF) to get the ProSe Code, the discovery parameters and the associated security material for announcing. The DDNMF may check for the announced authorization with the ProSe Application Server. The A-DDNMF returns the ProSe Code, the discovery parameters and the associated security materials to the Announcing/Discoveree UE.
2. The Monitoring/Discoverer UE sends a Discovery Request message to the DDNMF in its HPLMN (M-DDNMF) to get the ProSe Code, the discovery parameters and security materials for monitoring. The M-DDNMF sends an authorisation request to the ProSe Application Server and gets an authorisation response. If the Discovery Request is authorised, the M-DDNMF sends a Monitor Request to the A-DDNMF to get the discovery parameters and the associated security materials if they are not in the same PLMN. The M-DDNMF returns the discovery parameters and the associated security materials to the Monitoring/Discoverer UE.
3. The Monitoring/Discoverer UE and the Announcing/Doscoveree UE continue the discovery procedure over PC5 including the MIC, i.e. Model A or Model B discovery. The Monitoring/Discoverer UE sends a Match Report to M-DDNMF including the MIC and ProSe Code if required.
4. The M-DDNMF checks the MIC is valid. The M-DDNMF gets the Monitoring/Discoverer UE’s ProSe one-to-one communication security policies of the service related to the ProSe Code from PCF and passes the policies to the A-DDNMF. The one-to-one communication security policies are used to establish security during one-to-one communication establishment.
5. The A-DDNMF gets the security policies of the Announcing UE for direct one-to-one communication service related to the ProSe Code from PCF, and checks if the security policies of the Monitoring/Discoverer UE and the policies of the Announcing/Discoveree UE are not in conflict with each other. The A-DDNMF returns the check result to the M-DDNMF.
6. The M-DDNMF shall only indicate the acknowledge Monitoring/Discoverer UE to continue subsequent procedures if both MIC and the policies are not in conflict with each other.

### 6.27.3 Evaluation

This solution involves the ProSe discovery procedure related to Key Issue #1 and the one-to-one communication establishment procedure related to Key Issue #12. Security flexibility is provided by introducing on-demand PC5 one-to-one communication policies and the policy mismatch during one-to-one communication establishment makes the discovery signalling pointless. To avoid connection failure caused by policy conflict during one-to-one communication establishment, this contribution checks the policy match in advance with the help of the match report procedures.

The solution may require that the 5G ProSe Direct Discover procedure defined in TS 23.304 [16] to be updated.

The solution may require a new procedure to be supported on Npd between the 5G DDNMF and PCF for obtaining PC5 security policies.

The solution requires policy match request/response to be supported on N65/N66 between the 5G DDNMFs for checking the PC5 security policy match. Whether a new procedure is needed or the existing procedure can be used is up to SA2.

The solution requires that the 5G DDNMF has the logic to understand and check the match of PC5 security policies.

## 6.28 Solution #28: Mitigating the conflict between security policies using restricted discovery procedures on network side

### 6.28.1 Introduction

This solution addresses Key Issue #1 and Key Issue #12, including how to get the security materials to protect discovery and avoids one-to-one communication failure in advance. Two UEs should finish the discovery authorisation and the direct one-to-one communication establishment before actually starting direct one-to-one communication (i.e. the discovery request procedures are prerequisite steps of direct one-to-one communication).

Security flexibility is provided by introducing on-demand PC5 one-to-one communication policies. The security policies for ProSe UEs may be provisioned by different PCFs and they might issue different values. PC5 security policies are provisioned according to different services and geographical area(s) based on the referenced technology in TS 33.536 [8] and TS 23.287 [9]. The referenced technology, eV2X unicast in 33.536 [8], still has a mechanism to abort the PC5 unicast establishment upon policy mismatch (e.g. NOT NEED and REQUIRED) if the peer UE replies to the annunciation of the same v2x service from the initiating UE. This shows the security policies on each UE may not the same for the same service/ProSe Code. Moreover, UEs still need to negotiate final security activation status according to the real-time conditions and the network has no such real-time information. For the above reasons. For the above reasons, the conflict between security policies may cause one-to-one communication establishment failure and make the previous discovery request procedures in vain. To avoid connection failure caused by the conflict between policies, this contribution proposes to check the conflict between policies in advance with the help of the discovery request procedures specified in TS 33.303 [6] for 5G ProSe restricted discovery.

NOTE: This solution assumes all the security policies are provisioned/configured to UE with the existing ways as specified in clause 5.1 of TS 23.304 (i.e. provisioned in ME, configured in the UICC, from ProSe application server via PCF/PC1 reference point, and/or from PCF). The security policies for ProSe Services are not provisioned or configured to UE from 5G DDNMF. 5G DDNMF may get security policies from PCF.

NOTE: This solution does not work with the V2X based direct discovery (e.g. clause 6.2 in TR 23.752 [2]).

### 6.28.2 Solution details

The security procedure for restricted discovery is described as follows:

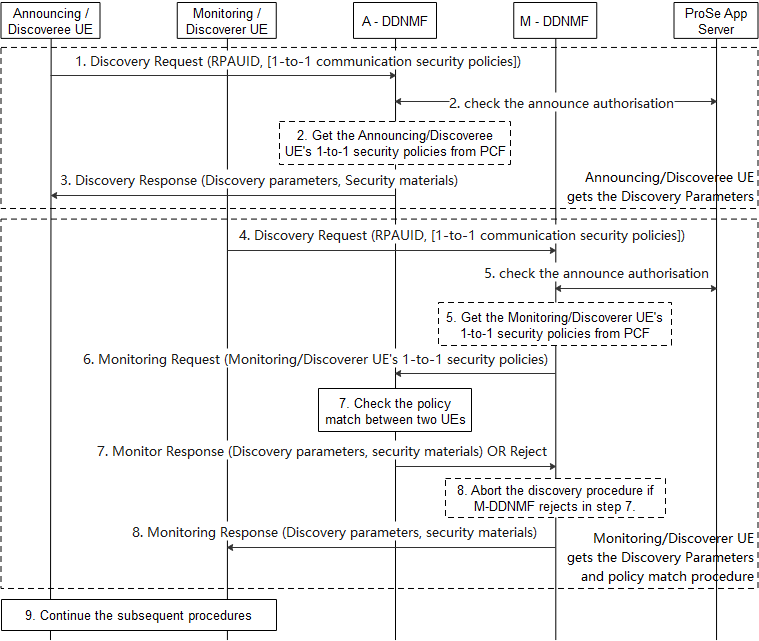


Figure 6.28.2-1: Check the conflict between policies using restricted discovery procedure

Steps 1-3 show the discovery request procedures of Announcing/Discoveree UE:

1. The Announcing/Discoveree UE sends a Discovery Request message including its PRAUID to the DDNMF in its HPLMN (A-DDNMF) to get the discovery parameters and the associated security material for announcing. The Announcing/Doscoveree UE may include its ProSe one-to-one communication security policies of the service related to the RPAUID. The one-to-one communication security policies are used to establish security during one-to-one communication establishment.
2. The DDNMF may check for the announced authorization with the ProSe Application Server. The A-DDNMF further exchanges the announced authorisation with the DDNMF of VPLMN if the Announcing/Doscoveree UE is roaming. The A-DDNMF obtains the Announcing/Doscoveree UE’s ProSe one-to-one communication security policies of the service related to the RPAUID from PCF if not received in step 1.
3. The A-DDNMF returns the discovery parameters and the associated security materials.

Steps 4-8 show the discovery request procedures of Monitoring/Discoverer UE:

1. The Monitoring/Discoverer UE sends a Discovery Request message including its RPAUID to the DDNMF in its HPLMN (M-DDNMF) to get the discovery parameters and security materials for monitoring. The Monitoring/Discoverer UE may include its ProSe one-to-one communication security policies of the service related to its RPAUID.
2. The M-DDNMF sends an authorisation request to the ProSe Application Server and gets an authorisation response if the RPAUID is allowed to discover at least one of the Target RPAUID(s). The authorisation response includes the above Target RPAUID(s). The M-DDNMF obtains the Monitoring/Doscoverer UE’s ProSe one-to-one communication security policies of the service related to the RPAUID from PCF if not received in step 4.
3. If the Discovery Request is authorised, and the PLMN ID in the Target RPAUID indicates a different PLMN, the M-DDNMF sends a Monitor Request to the indicated PLMN’s DDNMF i.e. the A-DDNMF. The Monitor Request includes the security policies got from either step 4 or 5. The A-DDNMF may exchange authorisation messages with the ProSe Application Server.
4. The A-DDNMF shall first check if the security policies provided by the DDNMF of the Monitoring/Discoverer UE and the security policies of the Announcing/Doscoveree UE are not in conflict, the A-DDNMF responds to the M-DDNMF with a Monitor Response message including the discovery parameters and the associated security materials if the Monitoring/Discoverer UE’s security policies and the Announcing/Doscoveree UE’s security policies are not in conflict with each other. The A-DDNMF shall reject the monitor request if the security policies between the Announcing/Doscoveree UE are in conflict with the security policies of the Monitoring/Discoverer UE. If the Discovery Request is authorised, and the PLMN ID in the Target RPAUID indicates the same PLMN, then the M-DDNMF does the confliction check locally.

For Model B scenario, the DDNMFs in the HPLMN and VPLMN of the Discoverer UE exchange Announce Authorisation messages if the Discoverer UE is roaming.

1. The M-DDNMF returns the discovery parameters and the associated security materials to the Monitoring/Discoverer UE. If the A-DDNMF rejects the Monitor Request, the M-DDNMF shall abort the discovery procedure and inform the Monitoring/Discoverer UE.
2. The Monitoring/Discoverer UE and the Announcing/Discoveree UE continue the subsequent procedures if M-DDNMF informs to continue the discovery procedures, i.e. Model A or Model B discovery, the match report procedures (if applicable) and establishment of ProSe one-to-one communication.

NOTE: This solution requires network coverage to work.

### 6.28.3 Evaluation

This solution involves the ProSe discovery procedure related to Key Issue #1 and one-to-one communication establishment procedure related to Key Issue #12. Security flexibility is provided by introducing on-demand PC5 one-to-one communication policies and the policy mismatch during one-to-one communication establishment makes the discovery signalling in vain. To avoid connection failure caused by policy conflict during one-to-one communication establishment, this contribution checks the policy match in advance with the help of the ProSe discovery procedures.

The solution may require that the 5G ProSe Direct Discover procedure defined in TS 23.304 [16] to be updated.

The solution may require that 5G ProSe UE is able to send its PC5 security policy to the 5G DDNMF.

The solution may require a new procedure to be supported on Npd between the 5G DDNMF and PCF for obtaining PC5 security policies.

The solution requires monitoring request/response to be supported on N65/N66 between the 5G DDNMFs for checking PC5 security policy match. Whether a new procedure is needed or the existing procedure can be used is up to SA2.

The solution requires that the 5G DDNMF has the logic to understand and check the match of PC5 security policies.

## 6.29 Solution #29: Security flow for Layer-3 UE-to-Network Relay

### 6.29.1 Introduction

This solution addresses Key Issue #3, Key Issue #4, and Key Issue #9. It is an L3 relay solution.

This solution uses the UE-to-network relay security flows specified in TS 33.303 [6] as the baseline, with some necessary modifications to suit 5GS.

The solution reuses the PC5 unicast communication security procedure defined in TS 33.536 [8] for the PC5 communication security.

NOTE: The PC5 unicast communication security procedure may be modified according to the conclusion of KI#12. This modification will be dealt with in the normative phase.

The main differences between this solution and the LTE procedure defined in TS 33.303 [6] are as follows:

- In this solution, 5GPRUK is generated based on an AV of the Remote UE, but in LTE, PRUK is generated by the GBA system or based on an AV of the Remote UE.

- In LTE, the Remote UE may provide IMSI in a Direct Communication Request, but in this solution, the Remote UE may provide SUCI in a Direct Communication Request.

### 6.29.2 Solution details

The UE-to-network relay security flow is described as follows:

NOTE: The Remote UE needs to be in coverage to obtain 5GPRUK from 5GPKMF through steps 1-4, otherwise the 5GPRUK is derived during link establishment with the Relay UE.

0. The Remote UE and the Relay UE get the discovery parameters, security materials, relay service codes and address of the 5GPKMF of the relay service from the 5GDDNMF in the HPLMN respectively. The security policies may also be provisioned for the PC5 unicast link of the relay service. 5GPKMF is set by the relay service.

1. The Remote UE establishes a secure connection with the 5GPKMF of the relay service.

2. The Remote UE sends a Relay Key Request to the 5GPKMF of relay service. The message includes Relay Service Code, and an optional 5GPRUK ID if the Remote UE already has a 5GPRUK.

NOTE: 5GPRUK and 5GPRUK ID are equivalent to PRUK and PRUK ID in TS 33.303 [6], respectively.

3. The 5GPKMF of the relay service checks whether the Remote UE is authorized to be a Remote UE according to the Relay Service Code.

4. The 5GPKMF of the relay service generates a relay key (i.e. 5GPRUK) and a corresponding key ID (i.e. 5GPRUK ID) for the Remote UE, and sends them to the Remote UE in a Relay Key Response.

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

6. The Remote UE generates a freshness parameter Nonce\_1 for the one-to-one communication and sends a Direct Communication Request to the Relay UE. In addition to the one-to-one communication parameters and Relay Service Code, the message includes 5GPRUK ID if the Remote UE already has a 5GPRUK, otherwise, it needs to include a SUCI.

7. The Relay UE sends a Relay Key Request to the 5GPKMF of relay service. The message includes 5GPRUK ID or a SUCI of the Remote UE, Relay Service Code and Nonce\_1.

8. The 5GPKMF of the relay service checks whether the Relay UE is authorized as a Relay UE according to the Relay Service Code. If the message includes the 5GPRUK ID of the Remote UE, the 5GPKMF checks whether the Remote UE is authorized as a Remote UE according to the Relay Service Code and the 5GPRUK ID, and then performs step 14.

9. The 5GPKMF of the relay service sends a Get AV Request to the UDM of the Remote UE through NEF. The message includes SUCI of the Remote UE and Relay Service Code.

10. The UDM of the Remote UE decrypts the SUCI, generates an Authentication Vector (AV), and sends the AV and the SUPI of the Remote UE to the 5GPKMF of the relay service.

11. The 5GPKMF of the relay service checks whether the Remote UE is authorized as a Remote UE according to the Relay Service Code and the SUPI of the Remote UE.

12. The 5GPKMF of the relay service derives a 5GPRUK based on the AV and some other parameters, generates a corresponding 5GPRUK ID. The 5GPKMF of the relay service also needs to generate a 5GPRUK\_Info from which the Remote UE can derive 5GPRUK and obtain 5GPRUK ID.

NOTE: The detailed structure of 5GPRUK\_Info will be defined in the normative phase, e.g. using a method similar to GPI used in LTE.

13. The 5GPKMF of the relay service generates a new random number as the 5GKd Freshness Parameter and then generates a new 5GKd using 5GPRUK, 5GKd Freshness Parameter, Nonce\_1, Relay Service Code, etc.

14. The 5GPKMF of the relay service sends 5GKd, 5GKd Freshness, and 5GPRUK\_Info to the Relay UE.

15. The Relay UE sends a Direct Security Mode Command to the Remote UE. In addition to the one-to-one communication parameters, the message includes the 5GKd Freshness Parameter and 5GPRUK\_Info if it exists.

16. The Remote UE derives the 5GPRUK and obtains the 5GPRUK ID using the information in 5GPRUK\_Info if 5GPRUK\_Info is provided. The Remote UE stores the 5GPRUK and 5GPRUK ID. The Remote UE further derives the 5GKd and performs other procedures.

17. The Remote UE sends Direct Security Mode Complete message to Relay UE.



Figure 6.29.2-1: UE-to-network relay security flow

### 6.29.3 Evaluation

Editor’s note: Further evaluation is FFS.

This solution introduces a method to establish a secure connection between the Remote UE and the UE-to-Network Relay UE. This solution does not address a requirement in KI#3, that is, Confidentiality protection, Integrity protection, and replay-protection shall be supported between the remote UE and the 3GPP network.

## 6.30 Solution #30: UE-to-Network Relay security based on primary authentication

### 6.30.1 Introduction

This solution addresses Key Issue #3, Key Issue #4, and Key Issue #9. It is applicable to both L2 and L3 UE-to-Network Relay architectures.

The solution reuses the PC5 unicast communication security procedure defined in TS 33.536 [8] for the PC5 communication security.

NOTE: The PC5 unicast communication security procedure may be modified according to the conclusion of KI#12. This modification will be dealt with in the normative phase.

The main differences between this solution and the LTE procedure defined in TS 33.303 [6] are as follows:

- In this solution, the PKMF in LTE is replaced by the AUSF of the Relay UE.

- In this solution, 5GPRUK is derived from Kausf, but in LTE, PRUK is generated by the GBA system.

- In LTE, the UE-to-network relay is only used for public safety services, but in this solution, it is mainly used for commercial services.

- In LTE, the Remote UE provides PRUK ID or IMSI in a Direct Communication Request, but in this solution, the Remote UE provides 5G PRUK ID and/or 5G-GUTI/SUCI in a Direct Communication Request.

### 6.30.2 Solution details

The UE-to-network relay security flow based on primary authentication is described as follows:

1. The Remote UE generates a freshness parameter Nonce\_1 for the one-to-one communication and sends a Direct Communication Request to the Relay UE. In addition to the one-to-one communication parameters, the message may contain the following parameters:

- a Relay Service Code that the Remote UE would like to access.

- a 5GPRUK ID (if the Remote UE has a 5GPRUK for this relay connection)

- a 5G-GUTI (if the Remote UE has a 5G security context) or a SUCI (if the Remote UE does not have a 5G security context). In the case of 5G-GUTI, 5GPRUK ID, GUTI, Relay Service Code and Nonce\_1 should be integrity protected with KNASint.

NOTE 1: 5GPRUK and 5GPRUK ID are equivalent to PRUK and PRUK ID in TS 33.303 [6], respectively.

2. The Relay UE sends a NAS Relay Key Request to its serving AMF. The message includes the parameters received from the Remote UE, i.e. 5GPRUK ID and/or SUCI/GUTI, Relay Service Code and Nonce\_1. In case a 5G-GUTI is included, these parameters are integrity protected with KNASint by the Remote UE.

3. The AMF of the Relay UE checks whether the Relay UE is authorized to be a Relay UE according to the Relay Service Code. The relay service authorization information is stored in the UDM of the Relay UE.

In the case that the Direct Communication Request message of the Remote UE contains a 5G-GUTI and the AMF of the Remote UE and the AMF of the Relay UE are the same, the AMF should retrieve the SUPI and current 5G security context of the Remote UE, and then check the integrity protection of the parameters of Direct Communication Request message as received in the NAS Relay Key Request message.

In the case that the Direct Communication Request message of the Remote UE contains a 5G-GUTI and the AMF of the Remote UE and the AMF of the Relay UE are not the same, the AMF should send the Direct Communication Request message of the Remote UE to the AMF of the Remote UE according to the 5G-GUTI. The AMF of the Remote UE should check the integrity protection of the message, and then check if the Remote UE is authorized to be a Remote UE. If these checks are passed, the AMF of the Remote UE should transfer the current security context of the Remote UE to the AMF of the Relay UE as defined in clause 6.9.3 of TS 33.501[14].

Editor’s note: When there is a K\_AMF change during UE security context transfer, how to deal with desynchronization of K\_AMF is FFS.

Editor’s note: How 5G-GUTI reallocation and Registration Update is performed when Remote UE is transferred to Relay's AMF is FFS.

4. The AMF of the Relay UE sends a Relay Key Request to the AUSF of the Remote UE. The message includes Remote UE's SUCI or SUPI, Relay Service Code, Nonce\_1 and the 5GPRUK ID (if it exists).

5-7. In the case of a SUCI in the Relay Key Request, the AUSF performs a primary authentication procedure defined in TS 33.501 [14] to the remote UE through the Relay UE.

8. The AUSF of the Remote UE checks whether the Remote UE is authorized to be a Remote UE according to Remote UE’s SUPI and Relay Service Code. The relay service authorization information is stored in the UDM of the Remote UE.

9-10. In the case of a 5GPRUK ID in the Relay Key Request, the AUSF of the Remote UE retrieves the 5GPRUK from the UDM using the Remote UE's SUPI and the 5GPRUK ID.

11. If there is no 5GPRUK ID in the Relay Key Request or the 5GPRUK ID needs refreshing, a new 5GPRUK will be generated. The AUSF of the Remote UE derives 5GPRUK using Kausf and some other parameters, generates a corresponding 5GPRUK ID. The AUSF of the Remote UE should generate a 5GPRUK\_Info from which the Remote UE can derive 5GPRUK and obtain 5GPRUK ID.

NOTE 2: The detailed structure of 5GPRUK\_Info will be defined in the normative phase.

12. In the case that a new 5GPRUK is generated, the AUSF of the Remote UE stores the newly generated 5GPRUK and 5GPRUK ID in the UDM.

13. The AUSF of the Remote UE generates a new random number as the 5GKD Freshness Parameter, and then generates a new 5GKD using 5GPRUK, 5GKD Freshness Parameter, Nonce\_1, Relay Service Code, etc.

NOTE 3: 5GKD is equivalent to KD in TS 33.303 [6].

14-15. The AUSF of the Remote UE sends 5GKD, 5GKD Freshness and 5GPRUK\_Info to the AMF of the Relay UE, and then further passes them to the Relay UE.

16. The Relay UE sends a Direct Security Mode Command to the Remote UE. In addition to one-to-one communication parameters, the message includes 5GKD Freshness Parameter and 5GPRUK\_Info (if it exists).

NOTE 4: In Remote UE and Relay UE, 5GKD is equivalent to KNRP.

17. In the case that there is a 5GPRUK\_Info in the message, the Remote UE derives the 5GPRUK and obtains the 5GPRUK ID using the information in 5GPRUK\_Info. The Remote UE stores the 5GPRUK and 5GPRUK ID. The Remote UE further derives the 5GKD and performs other procedures.

18. The Remote UE sends Direct Security Mode Complete message to Relay UE.



Figure 6.30.2-1: UE-to-Network Relay security flow based on primary authentication

### 6.30.3 Evaluation

Editor’s note: Further evaluation is FFS.

This solution introduces a method to establish a secure connection between the Remote UE and the UE-to-Network Relay UE. This solution does not address a requirement in KI#3, that is, Confidentiality protection, Integrity protection and replay-protection shall be supported between the remote UE and the 3GPP network.

This solution requires a new relayed primary authentication procedure to enable Remote UE to perform primary authentication with the AUSF of Remote UE via the AMF of Relay UE, which further requires new core network procedures in managing the remote UE context.

The Remote UE needs to perform a primary authentication whenever it establishes a connection with a relay UE if the Remote UE is not registered to the 5GS.

This solution requires AUSF to support ProSE key management functionality. It also requires the AMF and the UE (including the Remote UE and Relay UE) to support new NAS procedures.

In this solution, the PC5 link root key 5GKD is sent over the air interface to the Relay UE. It requires that the NAS message carrying 5GKD is both integrity and confidentiality protected. Otherwise, there is the risk that the root key 5GKD is exposed in clear text if confidentiality protection of the NAS signaling is not activated.

## 6.31 Solution #31: Use of authorization tokens in UE-to-UE relay

### 6.31.1 Introduction

This solution addresses key issue #7 (Authorization in the UE-to-UE relay scenario).

In the UE-to-UE relay use case, authorization of the UE that requests to be a source UE or a target UE discovering a UE-to-UE Relay, needs to be provided. The 5GS shall also support authorization of the UE requesting to act as a UE-to-UE relay. The 3GPP system shall provide means to authorize a source UE to communicate with another target UE via a UE-to-UE Relay.

In the UE-to-UE relay use case, the source UE and the UE-to-UE relay may be out of 3GPP coverage. In this case, they cannot ask the 3GPP network to perform the authorization.

This solution proposes to use authorization tokens as in OAuth 2.0 to indicate that the source UE or the UE-to-UE relay are authorized to use a specific relaying service or to serve a specific relaying service.

This solution also applies for authorization between the UE-to-UE relay and the target UE even though the solution description below does not explicitly mention the target UE.

### 6.31.2 Solution details

When the source UE or the UE-to-UE relay registers in the 3GPP network and is authorized to use a specific service, then the core network provides a token stating what kind of relaying service it can use or serve. The token has an expiration time and is signed with a private key of the core network. The core network also provides the public key to the source UE or the UE-to-UE relay used for verifying the token from other parties.

Editor note: How the core network provides the public key to the source UE and the UE-to-UE relay is FFS.

Figure 6.31.2-1 illustrates the high-level procedure of the proposed solution.

**Figure 6.31.2-1: High-level procedure of mutual verification between Source UE and UE-to-UE relay**

Step 0: The source UE and the UE-to-UE relay register and are authorized in the 3GPP network. The network provides one authorization token to the source UE and a second token to the UE-to-UE relay stating what kind of relaying service it can use/provide and other policies (e.g. to what kinds of remote UE the relay will provide service, what kinds of relay the UE can use, etc. ). The authorization token has an expiration time and is signed with the private key of the CN. The CN also provides the public key to the source UE and the UE-to-UE relay used for verifying the token from other parties. The authorization token could be generated by a CN NF or by the Application Server.

NOTE: The information included in the token (e.g. UE ID, indication if the UE can act as relay UE or remote UE, expiration time, etc.) is left for the normative work

Editor note: It’s FFS which NF generates the authorization token (e.g. UDM, PCF or ProSe Application Server).

Editor note: How the authorization token is provided to the source UE and the UE-to-UE relay is FFS.

Step1: The source UE and the UE-to-UE relay do the relay discovery and selection, e.g. using Discovery procedures using either Model A or Model B as defined in TS 33.303 and TS 23.303 or similar.

Step 2: The source UE sends a Direct Communication Request message to the UE-to-UE relay.

Step 3: Authentication and key agreement may be performed.

Editor note: The authentication and key agreement is FFS.

Step 4: The UE-to-UE relay sends Direct Security Mode Command message to the source UE.

Step 5: The source UE sends Direct Security Mode Complete message to the UE-to-UE relay.

The source UE can include its authorization token-1 in the Direct Security Mode Complete message, but the source UE could also include the authorization token-1 in a new signaling procedure as shown in step 7/7a. When the UE-to-UE relay receives the authorization token-1 from the source UE, it can verify the authorization token-1. For the verification of the authorization token, the receiving side can use the public key to verify the authorization token and check the policies/claims in the authorization token and decide if it should continue the procedure.

Step 5a: As an option, if the UE-to-UE relay is in 3GPP coverage then the 3GPP network could verify the authorization token on behalf of the UE-to-UE relay.

Step 6: If the verification of the authorization token-1 received from the source UE is successful in the UE-to-UE relay, then the UE-to-UE relay includes its authorization token-2 in the Direct Security Mode Response message to the source UE. For the verification of the authorization token-2, the receiving side can use the public key to verify the token and check the policies/claims in the token and decide if it should continue the procedure.

Step 7 and 7a: The source UE could also include the authorization token-1 in separate signaling procedures as shown in step 7/7a to the UE-to-UE relay. When the UE-to-UE relay receives the authorization token-1 from the source UE, it can verify the authorization token-1. For the verification of the authorization token, the receiving side can use the public key to verify the authorization token and check the policies/claims in the authorization token and decide if it should continue the procedure. If the verification of the authorization token-1 received from the source UE is successful in the UE-to-UE relay, then the UE-to-UE relay includes its authorization token-2 in a new signaling procedure to the source UE. For the verification of the authorization token-2, the receiving side can use the public key to verify the token and check the policies/claims in the token and decide if it should continue the procedure.

As an option, if the UE-to-UE relay is in 3GPP coverage then the 3GPP network could verify the authorization token on behalf of the UE-to-UE relay.

Step 8: If the mutual verification of the tokens fails either the UE-to-UE relay or the source UE may release the PC5 link.

**Authorization token is generated by the ProSe Application Server:**

The ProSe Application Server can be a candidate for generating the authorization token. In that case, the UE accesses the application server via the user plane for application level authorization. The application server generates (maybe with collaboration with PCF, UDM via NEF) and signs the token and gives it to the UE as well as the key for verifying tokens from other UEs. In this case, the application server will maintain the public/private key by itself.

Editor note: How the authorization token is provided to the source UE and the UE-to-UE relay is FFS.

Figure 6.31.2-2 illustrates the high-level procedure of the proposed solution.



Figure **6.31.2-2**: Authorization token generated by ProSe application server

In the Authorization Token Request message, the Source UE or UE-to-UE Relay could add an indication that the authorization token is required, so that the ProSe Application Server will generate the token for the UE. In the response, the ProSe Application Server can provide the public key for verifying token, if the ProSe Application Server has the public key for token verification.

When the ProSe Application Server generates the authorization token, it shall digitally sign the token, so that the token cannot be modified or forged by the attacker. The token generator can use a private key to sign the token and the token can be verified by the corresponding public key.

The public/private keys could be provided by the ProSe application server, or from a centralized entity like a CA.

### 6.31.3 Evaluation

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

## 6.32 Solution #32: Mitigating privacy issues of relay service codes and PDU parameters for L3 UE-to-NW relays

### 6.32.1 Introduction

This solution addresses key issues #5 (Privacy protection over the UE-to-Network Relay), #11 (UE identity protection during ProSe discovery) and #16 (Privacy protection of PDU session-related parameters for relaying) for Layer-3 UE-to-Network Relay connections, in particular, it addresses the privacy issues related the use of relay service codes and their associated PDU session parameters during discovery and connection setup.

This solution builds on top of solutions for key issues #4 and #9 (such as solution #1, #6, #10, #15, …) by adding a mechanism for updating the values of the relay service codes for Remote UEs and UE-to-Network Relays to mitigate privacy issues. These values can be seen as a kind of aliases, that can be used instead of the original value of the Relay Service Code, but they may be, e.g. still associated with the same PDU session parameters and authorization policies.

NOTE 1: how exactly this mechanism is to be integrated with solutions for key issues #4 and #9 depends on which solution is selected as the baseline for normative work, and details can be defined during the normative phase.

It further builds on solution #35 of TR 23.752, whereby in the solution description below we identify two different solution alternatives with different levels of protection and different levels of alignment:

*ALTERNATIVE 1*: As in solution #35, each UE-to-Network relay gets provisioned by the PCF with PDU session parameters associated with the supported Relay Service Codes during the initial authorization and provisioning step.

*ALTERNATIVE 2*: As solution #35, but with the difference that UE to Network relay does not get provisioned by the PCF with PDU session parameters associated with the supported Relay Service Codes during the initial authorization and provisioning step. Instead, the PDU session parameters are provided by the network only to the single UE-to-Network relay that is selected by the Remote UE and only after the network has verified the Remote UE and the selected Relay UE are authorized to set up a relay connection for the given Relay Service Code, and not to other UE-to-Network relays in the vicinity for additional privacy protection. This alternative therefore would require alignment with SA2.

In both alternatives, in line with solution #35 of TR 23.752, it is assumed that the Relay Service Codes are provisioned to the Remote UE and UE-to-Network Relay by the PCF. It is further assumed that the allocation of new values (i.e. aliases) for the Relay Service Codes is done by the PCF (or may be done in cooperation with the DDNMF).

NOTE 2: The details on how the PCF of the Remote UE and the UE-to-Network relay cooperate in the assignment and provisioning of the relay service codes, e.g. in a roaming scenario, are left for SA2 to decide. Also, the details on whether the DDNMF needs to be involved in the allocation of new values (i.e. aliases) for the Relay Service Codes or if this is the sole responsibility of the PCF are left for SA2 to decide and are not further elaborated in this solution. Alignment with SA2 on these aspects can be done during the SA3 normative phase.

For simplicity, the steps related to AUSF, UDM and PKMF are not described separately (the details depend on the respective solutions for key issues #4 and #9).

This solution assumes that the AMF of the UE-to-Network relay can directly or indirectly interface with the AMF (not shown) and the PCF serving the Remote UE. Depending on the solution for key issue #4 and #9 it may also interface with the AUSF, UDM and/or PKMF serving the Remote UE.

### 6.32.2 Solution Details

The procedure for updating relay service codes to mitigate privacy issues is depicted in Figure 6.32.2-1.



Figure 6.32.2-1: Procedural call flow for updating relay service codes to mitigate privacy issues

**Step 0:** Remote UE gets authorized by its PCF for relay discovery and connection setup, and is provisioned with a set of Relay Service Codes each associated with a set of PDU session parameters (S-NSSAI, DNN, etc.). Furthermore, the Remote UE gets provisioned with long term security material for ProSe discovery (e.g. root discovery key such as PSDK as defined in TS 33.303) and for relay connections (e.g. root relay connection key, such as PRUK as defined in TS 33.303), possibly with security material to allow direct communication over PC5 (e.g. the long term credentials in TS 33.536 that form the root of the security of the PC5 unicast link to derive KNRP).

Similarly, UE-to-Network Relay gets authorized by its PCF for relay discovery and connection setup and is provisioned with its supported Relay Service Codes, and security material for discovery (e.g. discovery key). In *ALTERNATIVE 1* of this solution, **t**he UE-to-Network relay does get provisioned with a set of PDU session parameters (S-NSSAI, DNN, etc.) for each Relay Service Code. In *ALTERNATIVE 2* of this solution, **t**he UE-to-Network relay does not get provisioned with a set of PDU session parameters (S-NSSAI, DNN, etc.) for each Relay Service Code. In both alternatives of this solution, the UE-to-Network relay should further be provisioned with a set of spare Relay Service Code values.

NOTE 3: For step 0 the Remote UE and the UE-to-Network relay are assumed to be in coverage. For subsequent steps 1 through 10, the Remote UE can be out of coverage, and the UE-to-Network relay is assumed to be in coverage.

**Step 1:** Remote UE discovers the UE-to-Network Relay through model A or B UE-to-Network relay discovery procedure by using one (or more) of the Relay Service Codes provisioned to the Remote UE. In this solution, the UE-to-Network relay should provide its SUCI or 5G-GUTI (i.e. ID\_Relay) and a fresh nonce N\_Relay to the Remote UE during discovery.

For this solution, it is assumed that for security protection of the discovery messages a solution that meets the requirements for restricted discovery in KI#1 is used. This implies that only UE-to-Network relays that have the respective key to decrypt the discovery message from the Remote UE can decrypt the Relay Service Code. For further privacy protection in line with KI#11, the Remote UE must frequently change its layer-2 identifier used for model B solicitation messages, preferably using a different layer-2 identifier for each subsequent solicitation message. The Remote UE should also randomly pause between sending two subsequent messages and frequently change the keys to protect the messages, and if possible also interchange with soliciting other Relay Service Codes.

**Step 2:** Remote UE sends a Direct Communication Request to the selected relay to establish a secure PC5 unicast link for relaying. The Remote UE shall select a different layer-2 ID for the Direct Communication Request from the layer-2 ID that was used in previous model B solicitation messages. In this solution, the Direct Communication Request message includes at least:

* an identifier to identify the Remote UE (i.e. ID\_Remote) such as SUCI or 5G GUTI,
* an encrypted value representing the Relay Service Code (RSC) concatenated together with the SUCI or 5G-GUTI of the selected UE-to-Network relay (i.e. ID\_Relay),
* the nonce N\_Relay received from the UE-to-Network relay,
* a fresh nonce N\_Remote generated by the Remote UE,
* a Message Authentication Code for integrity protection of each of these parameters.

The Relay Service Code and the identity of the selected UE-to-Network relay are encrypted (together) to prevent an eavesdropper to link these identities to the Remote UE, and to ensure that only the UE-to-Network relay that is selected by the Remote UE will receive:

* in case of *ALTERNATIVE 1:* the decrypted Relay Service Code in order to retrieve the PDU session parameters
* in case of *ALTERNATIVE 2*: the PDU session parameters from the network.

The keys K\_enc and K\_int are used to ensure the confidentiality and integrity of the message. These keys can be derived from the latest KAUSF of the Remote UE by using the key derivation function in TS 33.220 and a unique distinguishing FC identifier. These keys could also be derived from the long term security material for relay connection as received in step 0a (e.g. PRUK). To ensure replay protection, other inputs to the key derivation function can include nonces N\_Relay and N\_Remote. Another input can be a counter so that the receiving party, i.e., the AUSF, can check that a malicious node is not replaying messages from the remote UE.

NOTE 4: the selection of which key to use, and further details on the key derivation are left for the normative phase, as they depend on which solution(s) are chosen for key issues #4 and #9. See also NOTE 1.

NOTE 5: in case PRUK is used to derive K\_enc and K\_int, the PRUK ID needs to be included as part of the Direct Communication Request message, and assuming PRUK ID is unique for each Remote UE the PRUK ID may be used as ID\_Remote, instead of using the SUCI/5G-GUTI of the Remote UE.

The Message Authentication Code may be calculated as follows:

MAC (K\_int, ID\_Remote | N\_Relay | N\_Remote | ENCRYPT(K\_enc, RSC | ID\_Relay) )

where “|” indicates concatenation.

**Step 3a:** Upon receiving the Direct Communication request, the UE-to-Network relay verifies the presence of its nonce N\_Relay, and verifies its freshness.

**Step 3b:** If the nonce is valid, fresh and not repeated in a short timeframe, the UE-to-Network relay issues a NAS Relay Authorization Request/Key Request to its AMF. In this solution, the UE-to-Network relay includes ID\_Remote, the encrypted value of the Relay Service Code concatenated together with SUCI/5G-GUTI of the selected UE-to-Network relay (i.e. ENCRYPT(RSC | ID\_Relay)), the nonces and the Message Authentication Code received in step 2 in the NAS Relay Authorization Request/Key Request.

**Step 4a:** The UE-to-Network relay’s AMF selects the AUSF/UDM/PKMF based on ID\_Remote (e.g. SUCI/5G-GUTI of the Remote UE) and then together with the AUSF/UDM/PKMF derive K\_enc and K\_int based on ID\_Remote and the received nonces, and then decrypt and verify the integrity of the message fields. To this end, the AMF may need to send the information received in the NAS Relay Authorization Request/Key Request to the respective AUSF, which after verifying the integrity and decrypting the value, returns the decrypted RSC and ID\_Relay to the AMF. Subsequently, the AMF can verify if the ID\_Relay matches the identity of the UE-to-Network Relay from which the message was received. Otherwise, the AMF breaks off the procedure if these do not match.

**Step 4b:** The UE-to-Network relay’s AMF together with the selected AUSF/UDM/PKMF authenticate the Remote UE and verify if the Remote UE and the selected Relay UE are authorized to set up a relay connection for the given Relay Service Code (RSC) and generate the respective key material for the remote UE and selected UE-to-Network relay. Details of this procedure can be found in the respective solution for key issues #4 and #9.

**Step 5:** In this solution, after it has been verified that the relay connection is authorized for the respective relay service code in step 4, the UE-to-Network relay’s AMF performs the following additional steps:

1. AMF selects the PCF based on ID\_Remote and requests the PCF to provide a different value serving as an alias for the original Relay Service Code [See NOTE 2] for the Remote UE to be used instead of the Relay Service Code value that was used during discovery and connection setup. We distinguish two options here:

* Option 1: the alias value is chosen to be one of the values in the set of spare Relay Service Code values that are already provisioned to UE-to-Network relays in step 0b. In this case, all UE-to-Network relays that are already provisioned with this spare Relay Service Code value can be discovered and used by the Remote UE without any update procedures of the UE-to-Network relays involved, and without affecting the discovery and connection setup of other Remote UEs that are still using the original Relay Service Code.
* Option 2: the alias value is chosen to be a new value for the respective Relay Service Code. In this case, all involved UE-to-Network relays using the respective Relay Service Code need to be provided with the new alias for the respective Relay Service Code. The provisioning procedure as described in step 0b (in this case initiated by the network, e.g. through UE configuration update procedure) can be used for providing the alias to the UE-to-Network relays, which can add the provided alias to a list of aliases for the respective Relay Service Code.

The PCF should encrypt this Relay Service Code alias for the Remote UE in a manner that it cannot be decrypted by the UE-to-Network relay (e.g. using a key derived from the latest KAUSF of the Remote UE as in Step 2). [Not shown in figure] Assuming the security context of the Remote UE has not been transferred to the UE-to-Network Relay’s AMF, the UE-to-Network relay’s AMF may contact the Remote UE’s AMF, which should prepare a fresh 5G-GUTI for the Remote UE to use for subsequent discovery and connection setup over PC5 for further privacy protection. The Remote UE’s AMF may encrypt the fresh 5G-GUTI using the latest Kamf for the Remote UE..

The following step only gets executed in case of *ALTERNATIVE 2*:

1. AMF retrieves from the PCF the PDU session parameters associated with the requested Relay Service Code (to be returned to the UE-to-Network relay).

**Step 6:** In case of *ALTERNATIVE 1:*TheUE-to-Network relay’sAMF adds the decrypted Relay Service Code and the encrypted and integrity protected new Relay Service Code alias received from the PCF for the Remote UE (as received in step 5a) and, if received from the Remote UE’s AMF, a fresh 5G-GUTI to the NAS Relay Authorization Response/Key Response message to be sent back to the UE-to-Network Relay

In case of *ALTERNATIVE 2*: TheUE-to-Network relay’s AMF adds the PDU session parameters for the requested Relay Service Code (as received in step 5b) and the encrypted and integrity protected new Relay Service Code alias received from the PCF for the Remote UE (as received in step 5a) and, if received from the Remote UE’s AMF, a fresh 5G-GUTI to the NAS Relay Authorization Response/Key Response message to be sent back to the UE-to-Network Relay.

**Step 7a/b:** UE-to-Network relay uses the information received in step 6 to complete the secure link setup between the Remote UE andthe UE-to-Network relay. In this solution, the UE-to-Network relay adds the encrypted Relay Service Code alias received for the Remote UE ) to the Direct Security Mode Command as an additional parameter.

**Step 8:** In this solution, the Remote UE updates its list of relay service codes and the aliases based on theencrypted Relay Service Code alias it received in the Direct Security Mode command. The Remote UE will use the received alias for the Relay Service Code in subsequent discovery and/or Direct Connection setup requests.

**Step 9:** During or after secure connection setup over PC5 is completed, the UE-to-Network relay configures/initiates the PDU session used for relaying with the PDU session parameters (received in step 6) related to the Relay Service Code.

**Step 10:** The UE-to-Network relay can now start relaying data from the Remote UE to the network via the selected UE-to-Network relay. During the time the Remote UE is connected to the UE-to-Network relay, the Remote UE and UE-to-Network relay need to regularly run the Link Identifier Update procedure as defined in TS 33.536 to change the L2 identifiers of the UEs involved in the PC5 unicast link

NOTE 6:At some point in time, the UE-to-Network relays and other Remote UEs may need to be updated as well (e.g. to renew the authorization policies for relay service codes or after all spare relay service code values have been used). This can be done independently using the authorization and provisioning procedure as described in steps 0a and 0b.

### 6.32.3 Evaluation

This solution mitigates the privacy issues in key issue #16 in the following ways:

In case of discovery: the privacy issues in key issue #16 are mitigated by mandating a frequent change in layer-2 identifiers used during discovery, e.g. for each subsequent Model B solicitation request, the Remote UE cannot easily be traced using a requested Relay Service Code, in particular, if it is not the only Relay Service Code it solicits for and randomly pauses between sending subsequent solicitation messages to avoid any pattern detection. Furthermore, since the layer-2 identifiers are also changed before sending a subsequent Direct Connection Request, whereby the requested Relay Service Code is encrypted (using a different key than used during discovery), the discovery process cannot be linked to the connection setup process.

* In the case of ALTERNATIVE 1, during discovery a UE-to-Network relay can associate a solicited Relay Service Code with the pre-provisioned PDU session parameters, and hence has access to some privacy specific information of the Remote UE if the UE-to-Network relay supports the respective Relay Service Code. This implies that for the UE-to-Network relays in the vicinity of the Remote UE that support the respective Relay Service Code and can decrypt the respective discovery solicitation message the security requirements of key issue#16 can temporarily not be met. However, given the frequent change in layer-2 identifiers and the change to the Relay Service Code to a new alias after subsequent connection setup, this may be an acceptable risk.
* In the case of ALTERNATIVE 2, during discovery, a UE-to-Network relay cannot associate a solicited Relay Service Code with pre-provisioned PDU session parameters. Hence, the security requirements of key issue #16 are met during discovery. Furthermore, the selected UE-to-Network relay that is given the PDU session parameters during the subsequent connection setup process cannot trace the Remote UE with the solicited Relay Service Code since the Relay Service Code is changed to a new alias (using a message that cannot be decrypted by that selected UE-to-Network relay) and the Remote UE will use the new alias in subsequent discovery messages.

In case of connection setup: the privacy issues in key issue #16 are mitigated by enabling only the UE-to-Network relay that is selected by the Remote UE and for which the Remote UE has issued a Direct Connection Request to link the requested Relay Service Code to a set of PDU session parameters.

* In the case of ALTERNATIVE 1, this is achieved by only exposing the requested Relay Service Code to the selected UE-to-Network relay after it has been decrypted/integrity verified by the home network and the request to set up a relayed connection via the selected UE-to-Network for the respective Remote UE and requested Relay Service Code has been authorized/approved by the home and serving networks.
* In the case of ALTERNATIVE 2, this is achieved by only providing the PDU session parameters to the selected UE-to-Network relay after it has been decrypted/integrity verified by the home network and the request to set up a relayed connection via the selected UE-to-Network for the respective Remote UE and requested Relay Service Code has been authorized/approved by the home and serving networks.

The Relay Service Code and the identifiers of both the Remote UE and the selected UE-to-Network relay are encrypted/integrity protected in such a manner that only the home network of the remote UE can decrypt/verify these values, so neither eavesdroppers nor any of the other UE-to-Network relays nor other Remote UEs can make the link between the respective Relay Service Code and its associated PDU session parameters. This is so even if in ALTERNATIVE 1 each UE-to-Network Relay and each Remote UE is provisioned with associations between Relay Service Codes and PDU session parameters beforehand. Replaying this encrypted value (i.e. ENCRYPT(K\_enc, RSC | ID\_Relay)) by another UE-to-Network relay will fail because the core network will verify that the ID\_Relay in the encrypted value corresponds to the identifier of the UE-to-Network Relay that sent this encrypted value to the core network along with the NAS Authorization request.

The privacy risk when the Remote UE’s PDU session-related parameters are exposed to the UE-to-Network relay serving the Remote UE is not addressed in this solution. However, this privacy risk is only temporary for the duration of the communication session, since the Remote UE will use a different Relay Service Code in subsequent discovery and connection setup messages and this different Relay Service Code was provided to the Remote UE using a message that cannot be decrypted by a UE-to-Network Relay, only by the Remote UE.

In both ALTERNATIVE 1 and ALTERNATIVE 2, this solution requires the AMF to support new procedures to retrieve from the PCF a new RSC that is encrypted. In the case of ALTERNATIVE 2, the AMF also needs to support new procedures to retrieve from the PCF the PDU session parameters associated with the requested RSC. This second alternative is not aligned with the procedures in TS 23.304 [16] where the PDU Session parameters to be used for the relayed traffic for each associated Relay Service Code (RSC) are provisioned to both a Remote UE and UE-to-network relay before PC5 link setup when Layer-3 UE-to-Network relay is used. Hence, if ALTERNATIVE 2 is adopted given its stronger privacy guarantees, then alignment with SA2 will be required.

This solution mitigates the privacy issues in key issue #5 in the following ways:

Encryption of the requested Relay Service Code and ID\_relay during connection setup ensures that an eavesdropper cannot trace a Remote UE based on a Relay Service Code that may be used during discovery and connection setup. Although an identifier of the Remote UE is sent along with the Direct Communication Request (i.e. one single time), this cannot be linked to what was sent/received by the Remote UE during discovery given that the layer-2 identifier used in a Direct Communication Request differs from the layer-2 identifier(s) used during discovery. The identifier of the Remote UE can also not be traced after the initial connection setup, since once connection between the Remote UE and UE-to-Network relay has been established, the Remote UE and UE-to-Network relay will regularly update the layer-2 identifiers by running the Link Identifier Update procedure as defined in TS 33.536. Solution #32 also facilitates updating the 5G-GUTI of the out-of-coverage Remote UE for subsequent discovery and connection setup.

This solution mitigates the privacy issues in key issue #11 in the following ways:

During discovery the layer-2 identifiers and the Relay Service Code can be seen as identifiers of the UE that may be used to trace a Remote UE. In order to protect the Relay Service Code against eavesdropping this solution assumes that restricted discovery is used. During discovery phase, the layer-2 identifiers are also regularly updated to prevent tracing based on the layer-2 identifiers being used within a series of discovery solicitation messages. Furthermore, the Relay Service Codes are updated after each connection setup request to prevent tracing of the Remote UE and UE-to-Network Relay during subsequent discovery phase. Although an identifier of the Remote UE is sent along with the Direct Communication Request (i.e. one single time), this cannot be linked to what was sent/received by the Remote UE during discovery given that the layer-2 identifier used in a Direct Communication Request differs from the layer-2 identifier(s) used during discovery. Solution #32 also facilitates updating the 5G-GUTI of the out-of-coverage Remote UE for subsequent discovery and connection setup.

Editor’s Note: Further evaluation is FFS.

## 6.33 Solution #33: Security establishment of one-to-one PC5 communication rekeying

### 6.33.1 Introduction

This solution addresses the following security requirement in Key Issue #12: Security of one-to-one communication over PC5:

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

The initiating UE starts a Direct Rekeying Request to the receiving UE to trigger the refresh of security context between UEs, similar to the rekeying procedures as specified in clause 6.5.5.3 of TS 33.303 [6]. After receiving the Direct Rekeying Request, the new root key shared only between two UEs is generated securely by running Direct authentication and key establishment. The new security context is derived after the Direct Security Mode Command message based on the new root key.

### 6.33.2 Solution Details

Figure 6.33.2-1 Procedures for one-to-one communication rekeying over PC5

0. ProSe security-related parameter (for one-to-one secure communication over PC5) pre-configuration and provisioning.

Initiating UEInitiating UE

Receiving UEReceiving UE

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

3. Direct Auth and Key Establishment3. Direct Auth and Key Establishment

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

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

1. existing One-to-One Communication1. Discovery Procedures, or One-to-Many Communication

6. Direct Rekeying Accept ( )6. Direct Communication Accept ( User plane security indication )

0. ProSe Parameter pre-configuration and previsioning

1. The initiating UE and receiving UE already have established ProSe one-to-one communication.

2. The initiating UE starts a Direct Rekeying Request message containing 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. The message may also include a Re-auth Flag if UE\_1 wants to rekey the root key between the initiating UE and the receiving UE. The nonce for new session key derivation from the initiating UE, and the most significant bits of the new session key identifier are included in this message.

3. The receiving UE may initiate the Direct authentication and key establishment procedures with the initiating UE. This is mandatory if the Re-auth Flag appears in the Direct Rekeying Request message. The new root key shared only between two UEs is generated securely after Direct authentication and key establishment procedures.

4. The receiving UE uses the Chosen\_algs to indicate the selected confidentiality and integrity protection algorithms of this link and includes the Chosen\_algs in the Direct Security Mode Command message. The initiating UE’s security capabilities are sent back to the initiating UE. The new security context is derived by using the new root key if it is generated in step 3, otherwise, only the session key is refreshed. The receiving UE integrity protects the Direct Security Mode Command message with the new security context before sending it to the initiating UE. The nonce for new session key derivation from the receiving UE and the least significant bits of the new session key identifier are included in this message.

The session key is generated using the root key (either refreshed in step 3 or previously used) and the nonces from the initiating UE and receiving UE.

NOTE: The security activation status of both signalling and user plane remains the same for the lifetime of this PC5 link. The signalling and user plane use the same security algorithm if they have the same security activation status.

5. The initiating UE derives the new security context using the new root key if it is generated in step 3, otherwise, only the session key is refreshed. After the Direct Security Mode Command message passes integrity check, the initiating UE is then ready to both send and receive both signalling and user plane traffic protected with the new security context. The initiating UE sends the Direct Security Mode Complete message protected with new security context to the receiving UE.

6. The receiving UE replies with the Direct Rekeying Accept message to accept the Direct Rekeying Request.

### 6.33.3 Evaluation

Solution #33 addresses the security requirement for a secure refresh of UE security context in key issue #12. The secure refresh of the UE security context is based on the root key that is securely established only between two UEs using the Direct authentication and key establishment procedure.

## 6.34 Solution #34: Authorization of the remote UE in L3 U2N relay

### 6.34.1 Introduction

This solution addresses KI #4. This solution provides a mechanism to authorize a remote UE’s access to (1) a specific network slice(s) that requires slice-specific authentication and (2) a DN that requires a secondary authentication.

### 6.34.2 Solution details

This solution reuses the existing slice-specific authentication and secondary authentication procedures specified in TS 33.501 [14].

To access a DN that requires a secondary authentication, the remote UE establishes an IPsec connection with the N3IWF via a L3 U2N relay if it has not been established yet, and then requests a PDU session to the network via the N3IWF. The secondary authentication procedure for the PDU session is performed via the N3IWF as specified in TS 33.501 [14].

To access a network slice that requires a slice-specific authentication, the remote UE establishes an IPsec connection with the N3IWF via a L3 U2N relay if it has not been established yet, and then sends a Registration Request to access the slice to the AMF via the N3IWF. The slice-specific authentication procedure is performed via the N3IWF as specified in TS 33.501 [14].

The Relay Service Code (RSC) used for discovery and PC5 link setup is associated with the PDU session for the Remote UE to access the N3IWF. The Remote UE determines the N3IWF address and accesses the N3IWF over the PDU session established by the U2N relay UE based on the procedure in TS 23.304 [16].

NOTE: The policies for the relay UE’s PDU session established for the remote UE’s N3IWF access (e.g., whether and how the relay UE’s PDU session is limited to the N3IWF access) is specified in TS 23.304 [16].

### 6.34.3 Evaluation

This solution fulfils the second security requirement of KI#4 for the remote UE that accesses (1) a specific network slice(s) that requires slice-specific authentication or (2) a DN that requires a secondary authentication:

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

Editor’s Note: Further evaluation is FFS.

In this solution, the N3IWF is always required to support the secondary authentication and the slice-specific authentication.

## 6.35 Solution #35: Discovery procedures for UE-to-network relays

### 6.35.1 Introduction

This solution describes how the Remote UE and the UE-to-network relay retrieve the discovery keys for the corresponding Relay Service Code. This solution addresses key issues #2 and #10.

NOTE 1: This solution requires Remote UE to be in coverage to obtain the discovery keys.

Editor’s Note: The architecture of this solution needs to be aligned with SA2.

### 6.35.2 Solution details

#### 6.35.2.1 Commercial applications are dependent on the VPLMNs

When the commercial applications are dependent on the VPLMNs (Visiting PLMNs), i.e. the Remote UE only connects to the relays (i.e. UE-to-network relays) that are being served by some specific PLMNs, the Remote UE sends key request to the 5GDDNMF of its HPLMN and provides a list of VPLMN ID’s, then its 5GDDMNF (5GDDNMF of the Remote UE) will contact the 5GDDMNFs of the VPLMNs identified by the VPLMN ID’s to get the discovery keys. The UE-to-network relay gets the discovery key in the same way as the Remote UE.

A 5G PKMF is an NF located in a UE-to-network relay’s HPLMN which can handle the management of discovery keys for discovering a UE-to-network relay.

The procedures are shown below:

Figure 6.35.2.1-1: Discovery key provisioning (Commercial applications are dependent on the VPLMNs)

Step 0: The Remote UE connects to the network and gets authorized to be a Remote UE. The Remote UE also gets the address of the 5GDDNMF of its HPLMN.

NOTE 1: Whether the Remote UE ID consists of one or more of the following parameters: ProSe application id, ProSe application user id and/or GPSI of the Remote UE is for SA2 to decide.

NOTE 2: The Remote UE will be provisioned with a list of VPLMN IDs by the PCF, from which the Remote UE can obtain discovery keys.

Step 1: The Remote UE establishes a secure connection with its 5GDDNMF of the Remote UE of its HPLMN. The Remote UE ID is authenticated and authorized by the 5GDDNMF of the Remote UE. As this connection is established in the user plane, the same mechanism as used to protect the PC3 interface can be re-used. Either solution #5 or solution #11 can be used for securing the connection.

NOTE 3: The VPLMN 5G DDNMF needs to trust that the HPLMN 5G DDNMF has performed the authorization of the Remote UE to use this relay service.

Step 2: The Remote UE sends the key request to its 5GDDNMF of its HPLMN to get the discovery key. The key request includes at least the following information: the list of VPLMN IDs that the Remote UE will potentially visit (note that the list of VPLMN IDs can also include its HPLMN ID), the Remote UE ID, ProSe application ID and Relay service code(s).

Step 3: The 5GDDNMF of the HPLMN of the Remote UE checks if the Remote UE can consume or provide relay service in those VPLMNs.

Step 4: If the check in step 3 is successful, then the 5GDDNMF in the HPLMN of the Remote UE sends the key request to the 5GDDNMF of every VPLMN in the list.

Step 5: For every VPLMN in the VPLMN list, its 5GDDNMF receives the key request sent by the 5GDDNMF of the HPLMN of the Remote UE. The 5GDDNMF checks if the Remote UE can consume or provide relay service in the VPLMN. If the check is successful, the 5GDDNMF will generate the discovery key corresponding to the relay service code and its PLMN ID. If the key management is done by another NF (network function) or a PKMF, the 5GDDNMF will contact that NF or PKMF to get the discovery key.

NOTE 4: When and how often the discovery keys need to be generated is left for normative work.

Step 6: For every VPLMN in the VPLMN list, its 5GDDNMF sends the key response to the 5GDDNMF of the HPLMN of the Remote UE. The key response message includes at least the following information: PLMN ID, Remote UE ID, ProSe application ID, Relay service code, Discovery key.

Step 7: After receiving the key response from other 5GDDNMF, the 5GDDNMF of the HPLMN of the Remote UE sends the key response to the Remote UE. The key response message includes at least the following information: VPLMN IDs, Remote UE ID, ProSe application ID, Relay service code(s), Discovery keys.

#### 6.35.2.2 Commercial applications are dependent on the HPLMNs of the relays

In this scenario, the procedure for the Remote UE is the same as section 6.35.2.1. The PLMN list sent in step 1 in section 6.35.2.1 indicates HPLMNs of the UE-to-network relays that the Remote UE wants to discover. When a 5GDDNMF receives the key request, it checks if the Remote UE can discover the relay belonging to the corresponding PLMN.

In this scenario, the procedure for the UE-to-network relay is simpler than section 6.35.2.1. The 5GDDNMF of the UE-to-network relay does not need to contact 5GDDNMFs in other PLMNs. The 5G PKMF is an NF located in UE-to-network relay’s HPLMN. The procedure is shown below.



Figure 6.35.2.2-1: Discovery key provisioning (Commercial applications are dependent on the HPLMN of the Relays)

Step 0: The UE-to-network relay connects to the network and gets authorized to be a relay. The UE-to-network relay also gets the address of the 5GDNNMF of its HPLMN and the Relay Service Code.

NOTE 1: Whether the Remote UE ID consists of one or more of the following parameters: ProSe application id, ProSe application user id and/or GPSI of the UE-to-network relay is for SA2 to decide.

Step 1: The UE-to-network relay establishes a secure connection with its 5GDDNMF of the UE-to-network relay of its HPLMN. The UE-to-network relay ID is authenticated and authorized by the 5GDDNMF of the UE-to-network relay. As this connection is established in the user plane, the same mechanism as used to protect the PC3 interface can be re-used. Either solution #5 or solution #11 can be used for securing the connection.

Step 2: The UE-to-network relay sends the key request to its 5GDDNMF of its HPLMN to get the discovery key. The key request includes at least the following information: optionally its own HPLMN ID, UE-to-network relay ID, ProSe application ID and Relay service code.

Step 3: The 5GDDNMF of the HPLMN of the UE-to-network relay checks if the UE-to-network relay can consume or provide relay service in this PLMN.

Step 4: If the check in step 3 is successful, then the 5GDDNMF will generate the discovery key corresponding to the relay service code and its PLMN ID. If the key management is done by another NF (network function) i.e. 5G PKMF, the 5GDDNMF will contact that NF to get the discovery key.

NOTE 2: When and how often the discovery keys need to be generated is left for normative work.

Step 5: The 5GDDNMF sends the key response to the UE-to-network relay. The key response message includes at least the following information: optionally the PLMN ID, UE ID, ProSe application ID, Relay service code, Discovery key.

NOTE 3: The PLMN ID in step 2 and step 5 is optional since the 5GDDNMF knows its own PLMN ID.

### 6.35.3 Evaluation

This solution addresses key issues #2 and #10.

This solution describes how the Remote UE and the UE-to-network relay retrieve the discovery keys for the corresponding Relay Service Code. This solution is intended for commercial services.

Editor’s Note: It’s FFS whether this solution can be used for public safety

The Remote UE will be provisioned with a list of VPLMN IDs by the PCF, from which the Remote UE can obtain discovery keys.

This solution has no impact on network nodes, RAN, AMF and AUSF.

This solution has an impact on network nodes, 5GDDNMF and potentially the UDM.

In this solution, the 5G DDNMF or an NF (network function) - 5G PKMF, located in a UE-to-network relay’s HPLMN, handles the management of discovery keys for discovering a UE-to-network relay.

SA2 has not defined the 5G DDNMF in the architecture for the UE-to-network relay scenario as proposed in this solution.

SA2 has not defined the NF (network function) - 5G PKMF, which manages discovery keys, in the architecture for the UE-to-network relay scenario as proposed in this solution, as SA2 does not define PKMF in LTE. The 5G PKMF could interact with the 5G DDNMF via SBI.

In LTE, the PKMF is only used for Public Safety.  However, in 5G we need also to support the commercial use case. It is very hard to have a single PKMF for all the applications that are independent of PLMNs. It’s unclear which authority should be responsible for maintaining the function for commercial use cases. This solution is proposing to reuse the logic of the 5G DDNMF (or the ProSe Function in LTE) or the 5G PKMF which is bound with the PLMN.

## 6.36 Solution #36: UE-to-Network Relay security based on AKMA

### 6.36.1 Introduction

This solution describes how the Remote UE and the UE-to-network relay be able to communicate over the PC5 interface. This solution addresses key issue#4.

This solution is based on AKMA service. The DDNMF acts as an AKAM AF and can derive the KDIRECT, which is a key shared between two entities (Remote UE and Relay UE).

### 6.36.2 Solution details

Figure 6.36.2-1 shows the solution steps:



Figure 6.36.2-1 Procedure for Authorization and security with UE-to-Network relay

1. The Remote UE derives the KDDNMF. This step happens before the Remote UE tries to access the UE-to Network relay service.

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

3. The Remote UE sends a Direct Communication Request on PC5 interface. The Direct Communication Request message includes the A-KID, a freshness parameter Nonce\_1, relay service code and the Remote DDNMF ID. The derivation of A-KID is specified in TS 33.535[7]. The Remote DDNMF ID can be used to find the specific DDNMF.

**Option 1: (The Relay UE cannot directly connect to the Remote DDNMF)**

4. The Relay UE receives the Direct Communication Request and sends a Direct key request to the Relay DDNMF.The Direct Key Request message includes the A-KID, a freshness parameter Nonce\_1, relay service code and the Remote DDNMF ID.

5. The Relay DDNMF uses the received the Remote DDNMF ID to find the Remote DDNMF and sends a Nddnmf\_key\_request message to the Remote DDNMF. Nddnmf\_key\_request message includes the A-KID and the Nonce\_1 and relay service code.

6~8. If the Remote DDNMF does not have the KDDNMF which is identity by the A-KID. The Remote DDNMF gets the KDDNMF from AAnF. The procedure is specified in TS 33.535[7].

9. After received the KDDNMF, and if the remote UE is authorized to access this service, the Remote DDNMF stores the key and derives a KDIRECT using KDDNMF and Nonce\_1 as input. Remote DDNMF also generates the KDIRECT ID.

10~11. Remote DDNMF sends the KDIRECT and the KDIRECT ID to Relay DDNMF and Relay DDNMF forwards the KDIRECT and KDIRECT ID to the Relay UE.

**Option 2: (The Relay UE can directly connect to the Remote DDNMF)**

4. The Relay UE uses the received the Remote DDNMF ID to find the Remote DDNMF and sends a Direct key request to the Remote DDNMF. The Direct Key Request message includes the A-KID, a freshness parameter Nonce\_1 and relay service code.

5~8. These steps are the analogous to steps 6~9.

10, The Remote DDNMF sends a Direct key response to the Relay UE to include the KDIRECT and KDIRECT ID.

**Option 1 and Option 2**

12. The Relay UE sends a Direct Security Mode Command message to the Remote UE that includes KDIRECT ID.The message is integrity protected using the security key derived based on KDIRECT.

13. The Remote UE derives the KDIRECT and KDIRECT ID. This derivation is the same as in step 9 in the option 1.

14. If the security verification is successful, the Remote UE sends a Direct Security Mode Complete message to the Relay UE with security protection (integrity, confidentiality) using security keys derived based on KDIRECT. The Relay UE verifies the Direct Security Mode Complete message security using security derived based on KDIRECT. A successful security verification indicates to the Relay UE that the Remote UE is authorized to use the relay service provided by Relay UE.

15. The Remote UE receives a DCA message completing the successful PC5 link establishment.

### 6.36.3 Evaluation

This solution uses AKMA to address key issue #4. This solution assumes the DDNMF performs the authorization function,

## 6.37 Solution #37: Keying procedures for Group Member and Relay discovery: public safety case

### 6.37.1 Introduction

This solution describes how the UE obtains the necessary security parameters to support group members and relay discovery, in coverage and out of coverage, for public safety scenarios. This solution addresses key issues #1, #2, and #4.

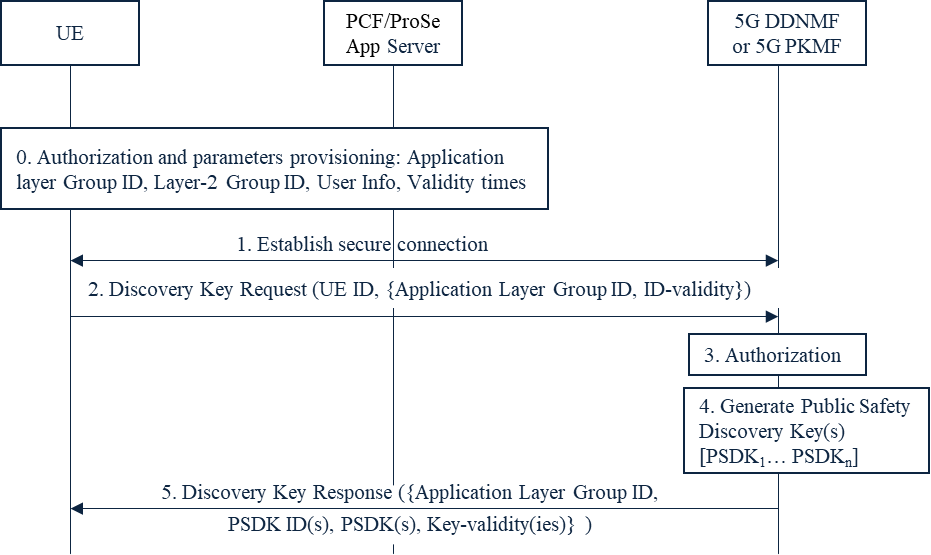
### 6.37.2 Solution details

#### 6.37.2.1 Group member discovery case

Group member discovery is a type of restricted discovery and is expected to be supported in coverage and out of coverage. Group member discovery uses provisioned keys to support integrity, confidentiality and non-trackability of the discovery messages. A discovery root key from which other keys can be derived is used to secure over the air discovery and communications. This root key can be provisioned by the 5G DDNMF and/or by the 5G PKMF – this clarification is left for the normative stage.

The solution follows that of TS 33.303 [2], where for both public safety discovery scenarios – group member discovery and relay discovery – the same solution is provided: a Public Safety Discovery Key (PSDK) is provisioned as the root key that is used for the protection of the Public Safety Discovery messages, and is associated with one or more Application Layer Group IDs or respectively Relay Service Codes (RSCs). Both of these identifiers are defined in TS 23.303 [5].

The procedures are shown below for Group Member Discovery.



**Figure 6.37.2.1-1: Discovery key provisioning for group member discovery, public safety case**

Step 0: The UE connects to the network and obtains authorization from the PCF/ProSe App Server to perform Group Member discovery. The UE also gets the address of the 5GDDNMF of its HPLMN and/or of the 5G PKMF. Besides the security policy, the following additional parameters are sent to the UE: a set of one or more (ProSe) Layer-2 Group ID, User Info, Application Layer Group ID and their validity times.

NOTE 1: This step is briefly described in TS 23.304 [3].

Step 1: The UE establishes a secure connection with the 5GDDNMF or the 5G PKMF of its HPLMN. The UE ID is authenticated and authorized by the 5GDDNMF or the 5G PKMF.

NOTE 2: As this connection is established on the user plane, the same mechanism as used to protect the PC3 interface can be re-used. Either solution #5 or solution #11 can be used for securing the connection.

Step 2: The UE sends a discovery key request to the 5GDDNMF or the 5G PKMF of its HPLMN. In the key request includes at least the following information: UE ID, set of one or more Application Layer Group IDs and their validity times.

Step 3: The 5GDDNMF or the 5G PKMF checks whether the UE is authorized for group member discovery.

Step 4: If the check in step 3 is successful, then the 5GDDNMF or the 5G PKMF generates one or more Public Safety Discovery Keys (PSDK1… PSDKn) corresponding to the Application Layer Group ID and its PLMN ID. More than one PSDK may be generated, but the overall validity time should match the validity times of the corresponding set of Application Layer Group IDs of Step 2. The Expiry Time of the PSDK needs to be set such that the keys for later periods have a longer expiration period. PSDKs that have not expired can be used for discovery in out of coverage cases.

NOTE 3: When and how often the discovery keys need to be generated is left for normative work.

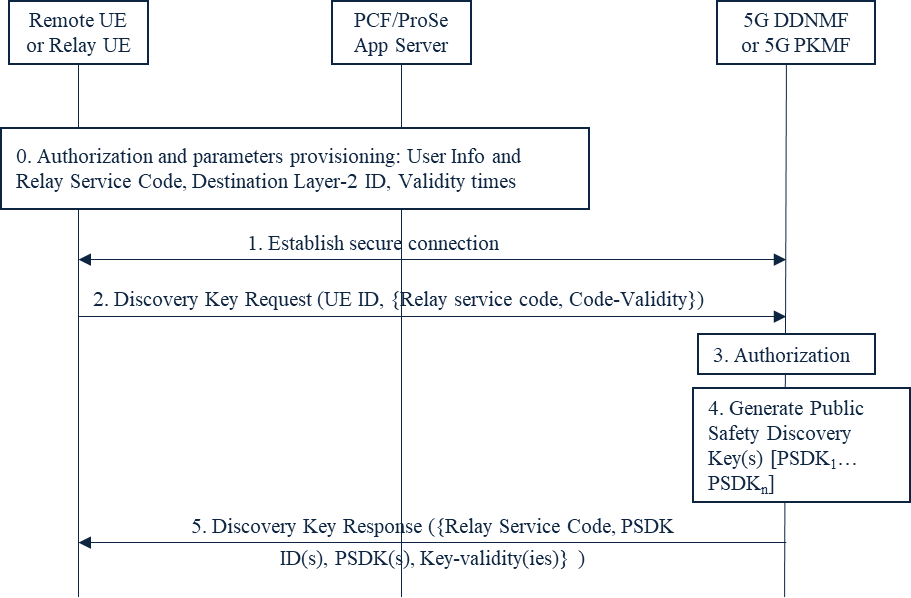
NOTE 4: The security keys in the Code-Sending Security Parameters of discoverer UE and the security keys in the Code-Sending Security Parameters of discoveree UE must be generated from two different PSDKs to avoid impersonation attacks in certain discovery configurations.

Step 5: The 5GDDNMF or the 5G PKMF sends the key response to the UE. The key response message includes at least the following information: UE ID, PDSK identifier(s), PDSK(s), validity time(s).

#### 6.37.2.2 Relay discovery case

The procedures are similar to the ones for Group Member Discovery. For Relay discovery, the procedures for the relay discovery are identical, with the following exceptions:

* The UE is now the Remote UE or the UE-to-network Relay
* Instead of the parameter Application Layer Group ID, the Relay Service Code is used.
* Instead of Layer-2 Group ID, the Destination Layer-2 ID is used



**Figure 6.37.2.2-1: Discovery key provisioning for relay discovery, public safety case**

6.37.3 Evaluation

The solution addresses key issues #1, and partially key issues #2, and #4 in the following way. Authorization for the UE to act as a group member, or UE-to-network relay, or Remote UE is provided by the PCF/ProSe App Server. The PCF/ProSe App Server provisions both policy as well as a group member and relay discovery parameters, along with their validity times. In addition, this solution describes how the UE obtains discovery keying material to support Group Member Discovery, in coverage and out of coverage. Lastly, the solution describes how the Remote UE and the UE-to-network Relay retrieve the discovery keying material for the corresponding Relay Service Code(s). This solution is intended for Public Safety services.

The following observations are made:

The UE is provisioned by the PCF/ProSe App Server with the address of the 5G DDNMF and/or the 5G PKMF.

This solution has no impact on the RAN or the network nodes AMF, AUSF.

In this solution, the 5G DDNMF, or another NF – the 5G PKMF (located in the UE’s HPLMN or external to it), handles the management of discovery keys for discovering a group member UE or a UE-to-network Relay.

SA2 has defined the 5G DDNMF in TS 23.304 [16] in the architecture, with reference points and services provided.

SA2 has not defined the NF - 5G PKMF, which manages discovery keys, in the architecture for the Group member discovery and UE-to-network relay scenarios as proposed in this solution, but SA2 did not define the PKMF in LTE either.

In LTE, the PKMF is only used for Public Safety.  This solution proposes to reuse the logic of the 5G DDNMF (or the ProSe Function in LTE) or the 5G PKMF which is part of the PLMN.

SA2 should make note that the security material for relay discovery is not provisioned by the PCF/ProSe App Server, but by the 5G DDNMF or 5G PKMF.

## 6.38 Solution #38: Mitigating the conflict between security policies using restricted discovery procedures on network side

### 6.38.1 Introduction

This solution addresses Key Issue #1 and Key Issue #12, the mechanism in this solution relies on the discovery procedures to avoid one-to-one communication failure caused by policy mismatch. Two UEs should finish the discovery authorisation and the direct one-to-one communication establishment before actually starting direct one-to-one communication (i.e. the discovery request procedures are prerequisite steps of direct one-to-one communication, except for the scenario in which UEs can start one-to-one communication directly).

In the referenced technology, eV2X unicast in 33.536 [8], security flexibility is provided by introducing on-demand PC5 one-to-one communication policies. The security policies for eV2X UEs may be provisioned by different PCFs and they might with different values (e.g. eV2X allows different security policies at different geographic locations). eV2X still has a mechanism to abort the PC5 unicast establishment upon policy mismatch (e.g. NOT NEED and REQUIRED) if the peer UE replies to the annunciation of the same v2x service from the initiating UE. This shows the security policies on each UE may not the same for the same service/ProSe Code. For the above reasons, UEs still need to negotiate final security activation status according to the real-time conditions and the network has no such real-time information.

The conflict between security policies may cause one-to-one communication establishment failure and make the previous discovery request procedures in vain. To avoid resource waste caused by the conflict between policies, this contribution proposes to distribute the same security policy with the help of the discovery procedures specified in TS 33.303 [6] for 5G ProSe restricted discovery.

NOTE: This solution does not work with the V2X based direct discovery.

NOTE: This solution requires network coverage to work.

### 6.38.2 Solution details

The UEs use the following discovery procedures to get the one-to-one communication security policy:

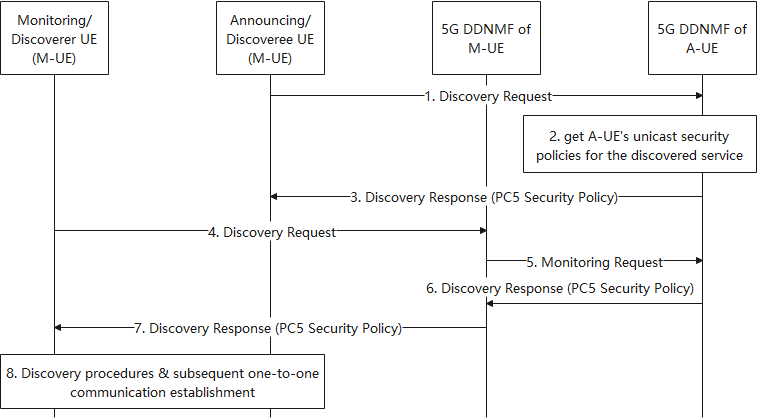


Figure 6.38.2-1: UEs get the security policy during the discovery procedures

Step 1-3 show the discovery request procedures of Announcing UE or Discoveree UE (hereinafter called A-UE):

1. The A-UE sends a Discovery Request message to the 5G DDNMF in its HPLMN (A-DDNMF) to get the discovery parameters and the associated security material for discovering the peer under a specific ProSe service.
2. The A-DDNMF may check for the authorization of A-UE to use the ProSe service. The A-DDNMF further gets one-to-one communication security policy of the ProSe service related to the Discovery Request in step 1. The security status of the one-to-one communication of the ProSe service is decided based on the security policy.

NOTE: A-DDNMF gets the security policy from PCF, or other selected methods during the normative phase.

1. The A-DDNMF returns the discovery parameters, the associated security materials and the security policy to the A-UE.

The Step 4-8 shows the discovery request procedures of Monitoring or Discoverer UE (M-UE):

1. The M-UE sends a Discovery Request message to the 5G DDNMF in its HPLMN (M-DDNMF) to get the discovery parameters and security materials for discovering the peer under the same ProSe service in step 1-3.
2. The M-DDNMF may check for the authorisation of M-UE to use the ProSe service. If the Discovery Request is authorised, The M-DDNMF sends a Monitor Request to the A-DDNMF to request the one-to-one communication security policy of the ProSe service which was got by A-DDNMF in step 2.
3. The A-DDNMF responds to the M-DDNMF with a Monitor Response message including the discovery parameters, the associated security materials and the security policy.
4. The M-DDNMF returns the discovery parameters, the associated security materials and the security policy to the M-UE.
5. The A-UE and M-UE process to discovery each other and continue the subsequent one-to-one communication establishment procedures using the one-to-one communication security policy from A-DDNMF and M-DDNMF, respectively.

### 6.38.3 Evaluation

This solution involves the ProSe discovery procedure related to Key Issue #1 and one-to-one communication establishment procedure related to Key Issue #12. Security flexibility is provided by introducing on-demand PC5 one-to-one communication policies and the policy mismatch during one-to-one communication establishment makes the discovery signalling in vain, as well as network resource waste. To avoid resource waste caused by policy confliction during one-to-one communication establishment, this contribution to distribute the same security policy with the help of the discovery procedures.

Editor's Note: Further evaluation is FFS

Editor's Note: It is FFS which specific requirements are addressed by this solution.

## 6.39 Solution #39: Key management in UE-to-Network Relay based on shared key generated during primary authentication

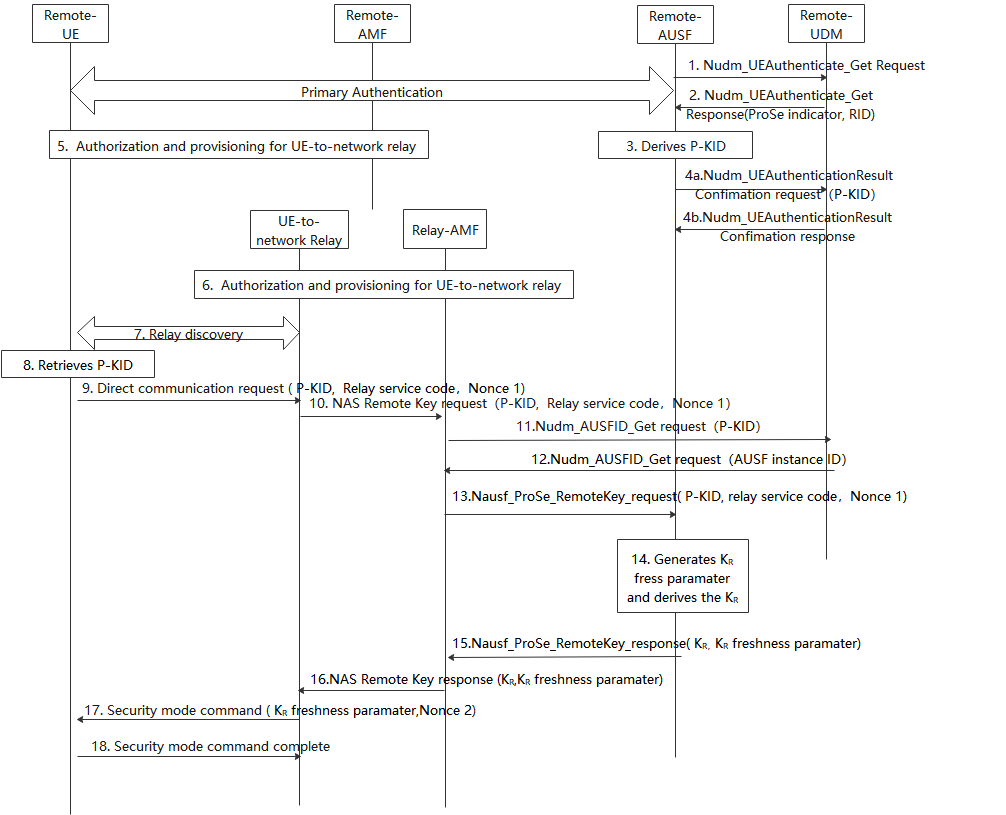
### 6.39.1 Introduction

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

### 6.39.2 Solution details

#### 6.39.2.1 Procedure

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



1. During the primary authentication procedure, the AUSF interacts with the UDM in order to fetch authentication information such as subscription credentials (e.g. AKA Authentication vectors) and the authentication method using the Nudm\_UEAuthentication\_Get Request service operation.

2. In the response, the UDM may also indicate to the AUSF whether ProSe Key Identifier (P-KID) needs to be generated for the UE. If the ProSe Indicator is included, the UDM shall also include the RID of the UE.

3. If the AUSF receives the ProSe indication from the UDM, the AUSF shall store the KAUSF and generate the P-KID from KAUSF after the primary authentication procedure is successfully completed.

P-KID is in NAI format as specified in clause 2.2 of IETF RFC 7542 [6], i.e. username@realm. The username part includes the Routing Identifier and the P-TID (ProSe Temporary UE Identifier), and the realm part includes Home Network Identifier.

The P-TID is derived from KAUSF as specified in 6.39.2.2.

4. AUSF sends the P-KID via Nudm\_UEAuthenticationResultConfirmation request to UDM, the UDM stores the P-KID with AUSF instance ID and sends Nudm\_UEAuthenticationResultConfirmation response to the AUSF.

5. Authorization and provisioning are performed for the Remote UE.

6. During the Registration procedure, authorization and provisioning are performed for the ProSe UE-to-NW relay.

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

8. The Remote UE derives P-KID using the same method as the remote AUSF.

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

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

11. The relay AMF that serves the relay UE first check whether the relay UE is authorized to be a relay. If authorized, The AMF discovers the UDM based on the P-KID, the relay AMF sends Nudm\_AUSFID\_Get request with P-KID to the UDM.

12. UDM response to relay AMF via Nudm\_AUSFID\_Get with AUSF instance ID of the AUSF serving remote UE.

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

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

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

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

NOTE: This solution requires integrity and confidentiality protected NAS messages.

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

18. The Remote UE derives the KR key in the same way as the remote AUSF in step 14. The DSMC message is integrity and confidentiality protected as in TS 33.536[8].

NOTE: The key lifetime issue will further align with the other normative work to address key lifetime

Editor’s Note: How to protect privacy of P-TID is FFS.

Editor’s Note: Kausf desync should be further studied.

Editor’s Note: How to determine the key lifetime is FFS.

#### 6.39.2.2 Derivation of P-TID

When deriving the P-TID from KAUSF, the following parameters are used to form the input S to the KDF:

- FC = xxxx (to be allocated by 3GPP);

- P0 = SUPI;

- L0 = length of SUPI.

- P1 = “P-TID”;

- L1 = length of “P-TID”.

The input key KEY is KAUSF.

SUPI has the same value as parameter P0 in Annex A.7.0 of TS 33.501 [2].

### 6.39.3 Evaluation

This solution requires AUSF to derive the P-KID when receives the ProSe indicator from the UDM and stores the P-KID in the UDM.

The AUSF is responsible for the ProSe key management function in this solution.

Editor’s Note: Further evaluation is FFS.

## 6.40 Solution #40: Protection with Security Policies for PC5 Direct Communication

### 6.40.1 Introduction

This solution addresses key issue #17: Supporting security policy handling for PC5 connection of 5G ProSe services. It aims to meet all the potential requirements in key issue #17 by achieving the following:

- Configuration of PC5 security policies for protecting ProSe services between the UEs.

- Secure provisioning of the configured PC5 security policies from the network to the UE.

- Negotiation between the UEs on the PC5 security policies provisioned separately to them for correct enforcement of ProSe service protection.

This solution largely reuses the security policy configuration and negotiation defined for V2X security in TS 33.536 [8].

### 6.40.2 Solution details

#### 6.40.2.1 Security policy configuration and provisioning

As per TS 23.304 [16], the following privacy related parameters are provisioned by the PCF to the UE for 5G ProSe Direct Communications over the PC5 reference point:

- The list of ProSe services (i.e. ProSe Application IDs) with Geographical Area(s) that require privacy support

This solution proposes that PC5 security policies are also provisioned by the PCF in a similar way, i.e. the following additional parameters need to be configured by the PCF and provisioned from the PCF to the UE:

- The list of ProSe services (i.e. ProSe Application IDs) with Geographical Area(s) that require security protection, and the PC5 security policies for each of the ProSe services in the list.

The provisioning of the security policy related parameters from the PCF to the UE can be protected with the existing NAS security established after the UE’s registration.

The configuration of security policies for V2X services defined in TS 33.536 [8] could be resued for PC5 security policies of ProSe services.

Editor’s Note: It is FFS whether the existing security policy configuration defined in TS 33.536 [8] needs to be adapted for 5G ProSe services.

#### 6.40.2.2 Security policy negotiation and enforcement

The negotiation and enforcement of PC5 security policies for ProSe direct communication can reuse the mechanisms in TS 33.536 [8] defined for protecting V2X communication.

Editor’s Note: It is FFS whether the existing security policy negotiation defined in TS 33.536 [8] needs to be adapted for 5G ProSe services.

### 6.40.3 Evaluation

This solution addresses all the three potential requirements in key issue #17 by largely reusing the mechanisms defined for V2X service protection in TS 33.536 [8].

The proposal of using PCF to configure and provision PC5 security policies for different ProSe services is aligned with the requriements of policy provisioning for 5G ProSe Direct Communication defined in TS 23.304 [16].

Editor’s Note: Further evaluation is FFS.

## 6.41 Solution #41: Security protection for 5G ProSe indirect network communication

### 6.41.1 Introduction

This solution addresses one of the requirements in key issue #3 for security of UE-to-Network Relay, which is:

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

To be more exact, this solution addresses the security protection requirement for both control plane traffic and user plane traffic between the Remote UE and the 3GPP network.

As per TS 23.304 [16], the figure below shows the high level reference architecture for the 5G ProSe L3 U2N relay.

****

**Figure 6.41.1-1: Reference Architecture for 5G ProSe Layer-3 UE-to-Network Relay**

As indirect network communication between the remote UE and the NG-RAN via L3 U2N relay goes through the PC5 link and the Uu link, hop-by-hop security is required to be supported over PC5 link and Uu link, including both signalling security and user plane security over PC5 and Uu links.

Regarding the UP security policies configured by the network for the remote UE requested service, as no AS security can be established between the remote UE and the NG-RAN in case of an L3 U2N relay in between, how the UP security activation indication can be securely provisioned to the remote UE and how the UP security policy can be consistently enforced between the remote UE and 3GPP network are addressed in the solution.

### 6.41.2 Solution details

#### 6.41.2.1 Framework of security protection for 5G ProSe indirect network communication

For a 5G ProSe remote UE accessing network via a trusted L3 U2N relay, the security protection of the service’s traffic between the remote UE and the network still relies on the UP security policies set and provided by the network, which needs to be supported by the security protection on PC5-U link between the remote UE and the U2N relay and the security protection for the PDU session established between the U2N relay and the network. Therefore, as shown in Figure 6.41.2.1-1, the end-to-end security protection of the service requested by the remote UE can only be met when the security policies for the two links (PC5 and Uu) are consistently configured and enforced.



**Figure 6.41.2.1-1: Security Protection for 5G ProSe Indirect Network Communication**

As the security protection of the service requested by the remote UE should follow the UP security policies set by the core network, there are two aspects to consider for achieving the E2E security protection:

1. Alignment of PC5 signalling security to Uu signalling security, which is required to support the secure provisioning of the UP security activation indication from the NG-RAN to the remote UE via the U2N relay.

2. Alignment of PC5 UP security to Uu UP security, which is required to support the security requirements based on the UP security policies set for the service requested by the remote UE.

#### 6.41.2.2 Secure provisioning of UP security policies for 5G ProSe indirect network communication

To securely provision the UP security activation indication from the NG-RAN to the remote UE, both Uu signaling and PC5 signaling need to be protected. Uu signaling security can be ensured by the AS signaling security established between the U2N relay and the NG-RAN.

According to TS 33.303 [6] for LTE ProSe, the PC5 signaling between the remote UE and U2N relay are protected based on the security requirements defined for protection of LTE ProSe direct communication, which require that:

- Direct link signaling integrity protection and replay protection shall be supported and used;

- Direct link signaling ciphering shall be supported and may be used. Direct link signaling ciphering is a configuration option

As the above security requirements on PC5 signaling are aligned with AS signalling security requirements, it means that PC5 signaling security for 5G ProSe indirect network communication can reuse PC5 signaling security defined for LTE ProSe indirect relay communication in TS 33.303 [6], which entails the following requirements on PC5 signalling for 5G ProSe indirect network communication:

- Integrity and anti-replay protection for PC5 signaling between the remote and relay UEs shall be supported and used;

- Ciphering for PC5 signaling between the remote and relay UEs shall be supported, and its activation is a configuration option.

#### 6.41.2.3 Enforcement of UP security policies for 5G ProSe indirect network communication

The assumption is that the 5G ProSe remote UE and U2N relay have already been authorized by the network to act as remote UE and U2N relay respectively during their registration, and have discovered each other.



**Figure 6.41.2.3-1: Protection of 5G ProSe Indirect Network Communication via L3 U2N Relay**

1. The Remote UE selects the L3 U2N Relay to establish a connection for indirect network communication. The Remote UE sends a Direct Communication Request message to initiate the PC5 link establishment procedure.

2. The U2N Relay sends a Relay Key Request (including the Relay Service Code) to the network for the authorization of the U2N relay and remote UE according to the RSC, as well as the generation of the PC5 link root key (e.g. 5G\_KNRP) and its relevant parameters (e.g. 5GPRUK ID, 5G\_KNRP Freshness, 5GPRUK\_Info, etc.).

3. The U2N Relay sends a Direct Security Mode Command to the Remote UE, including the relevant parameters for deriving the PC5 link root key, and derives the session keys for PC5 signaling protection, i.e. the Direct Security Mode Command is protected.

4. The Remote UE derives the PC5 link root key based on the parameters received from the U2N relay, and then derives the session keys for PC5 signaling protection.

5. The Remote UE sends Direct Security Mode Complete message to U2N Relay, which is protected by the session keys. By this step, the signaling security of the PC5 link is established.

6. As per TS 23.304 [16], if there is no PDU Session associated with the RSC or a new PDU Session for relaying is needed, the U2N Relay initiates a new PDU session establishment procedure for relaying before completing the PC5 connection establishment.

7. As per TS 33.501 [14] and TS 23.502 [10], the SMF sets the UP security policies for the PDU session for relaying requested by the U2N Relay, and provides the UP security policies to the NG-RAN.

8. The NG-RAN activates Uu UP security protection based on the UP security policies received from the core network.

9. The NG-RAN indicates the Uu UP security activation status to the relay UE using RRC Connection Reconfiguration procedure, according to TS 33.501 [14]. Meanwhile, the NG-RAN sends N2 PDU Session Response to the AMF.

10. The U2N relay activates its Uu UP security based on the security activation indication received from the NG-RAN. From this step on, the Uu UP security in Figure 6.Y.2.1-1 is protected based on the UP security policies set for the relayed service.

11. The U2N relay further activates its PC5 UP security based on its Uu UP security activation status for alignment.

12. The U2N relay sends the Direct Communication Accept message to the Remote UE to accept the PC5 connection establishment, which includes the PC5 UP security activation indication. The whole message is protected with PC5 signaling security, hence the PC5 UP security activation indication sent from the relay is protected. Meanwhile, the U2N relay sends the Remote UE Report to its SMF.

13. The Remote UE activates its PC5 UP security according to the PC5 UP security activation indication received from the U2N relay. From this step on, the PC5 UP security in Figure 6.41.2.1-1 is protected based on the UP security policies set for the relayed service.

14. The service data relayed between the Remote UE and network over the PC5 link and Uu link are now sent with protection based on the UP security policies set by the core network.

With the above procedure, the integrity, confidentiality and anti-replay protection between the Remote UE and the 3GPP network can be supported through consistent enforcement of UP security policies between the Remote UE and the network for the relayed service, as well as the aligned security protection for Uu signalling and PC5 signaling.

### 6.41.3 Evaluation

This solution addresses the requirement of integrity, confidentiality and anti-replay protection between the Remote UE and the 3GPP network in key issue #3 for the security of UE-to-Network Relay.

The protection on signalling relies on the alignment of Uu signalling security and PC5 signaling security, which reuses the AS security in TS 33.501 [14] and PC5 signaling protection for LTE ProSe indirect relay communication in TS 33.303 [6] respectively.

The protection on user plane relies on the UP security policies set by the network for the relayed service, which need to be consistently enforced by the Remote UE and the NG-RAN. This largely reuses the existing mechanisms for configuration and enforcement of UP security policies defined in TS 33.501 [14] and TS 23.502 [10]. The only difference and impact are that the relay UE needs to internally map its Uu UP security activation status to its PC5 UP security activation status, which is then indicated to the Remote UE, for alignment between Uu UP security and PC5 UP security.

Editor’s Note: Further evaluation is FFS.

## 6.42 Solution #42: Privacy enhancements during PC5 link setup for UE-to-Network relay

### 6.42.1 Introduction

This solution addresses KI #5. This solution provides a mechanism for protecting RSC (and PRUK ID) during PC5 link setup for UE-to-Network (U2N) relay when RSC is protected in restricted discovery. In restricted discovery, RSC is protected (i.e., scrambled and/or ciphered) in both discovery model A and B based on the provisioned discovery security parameters (i.e., DUSKs and/or DUCKs). However, the RSC is not protected in subsequent link setup procedure even when it can be protected in a similar way as in the discovery. To ensure this privacy protection in the subsequent link setup procedures, this solution can be optionally enabled by applying the same protection mechanisms to the Remote UE’s RSC (and PRUK ID) if they are transmitted between the Remote UE and the U2N relay. Note that this protection mechanism only applies when the RSC is privacy protected during restricted discovery procedure.

### 6.42.2 Solution details

#### 6.42.2.1 General

This solution provides a mechanism to optionally privacy protect the RSC and PRUK ID in Direct Communication Request (DCR) message based on the provisioned discovery security materials in case a restricted discovery is used to protect the discovery message during a PC5 link setup procedure for U2N relay service. In particular, the RSC and PRUK ID in DCR message are protected using the code-receiving security parameters as described in clause 6.42.2.2. The U2N relay, on receiving the DCR message, retrieves the RSC and PRUK ID from DCR message using the code-sending security parameters as described in clause 6.42.2.2 and checks if the RSC matches with the one that it sent in the discovery message. The reason that the code-receiving security parameters are used for privacy protection is to have consistency between discovery Model A and Model B, and reuse the already provisioned security parameters. The rest of the PC5 setup procedure remains the same as described in the U2N relay solution selected for the normative work.

#### 6.42.2.2 Protection of PRUK ID and RSC over the PC5 interface

The Remote UE does the following:

- If the Remote UE is provisioned with DUCK:

1. Form Message = RSC || PRUK ID

2. Calculate *Keystream* = KDF (DUCK, UTC-based counter, RSC) – see subclause 6.42.2.3.3. Ciphertext = Message XOR *Keystream*

- If the Remote UE is provisioned with DUSK:

1. Set the 4 LSBs of the UTC-based counter equal zero, for the purpose of this scrambling calculation only.

2. Compute the time-hash-bitsequence from Discovery User Scrambling Key (DUSK) and the UTC-based counter (modified as in step 1), passed through a keyed hash function as described in 6.42.2.4.

3. XOR the time-hash-bitsequence with the RSC and PRUK ID being processed.

The UE-to-network relay does the following to retrieve the RSC and PRUK ID from the received DCR:

- If the U2N relay UE is provisioned with DUCK:

1. Form Ciphertext = a part of protected (RSC || PRUK ID) in the received DCR message.

2. Calculate *Keystream* = KDF (DUCK, UTC-based counter, RSC) – see subclause 6.42.2.3.

3. Message = Ciphertext XOR *Keystream*

- If the U2N relay is provisioned with DUSK:

1. Set the 4 LSBs of the UTC-based counter equal zero, for the purpose of this scrambling calculation only.

2. Compute the time-hash-bitsequence from Discovery User Scrambling Key (DUSK) and the UTC-based counter (modified as in step 1), passed through a keyed hash function as described in 6.42.2.4.

3. XOR the time-hash-bitsequence with the scrambled part of RSC and PRUK ID in the received DCR.

Editor’s Note: the FC values used in the confidentiality/scrambling routines for the DCR message protection must be different than the FC values used for the discovery message protection.

Editor’s Note: The parameters to be used as input in the KDF need to be further analysed.

Editor’s Note: the process for integrity verification, e.g., by computing a MIC, and the key used to compute such a MIC is FFS.

#### 6.42.2.3 Calculation of message-specific confidentiality keystream

When calculating the message-specific confidentiality keystream, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [12]:

- FC = 0xXX

- P0 = UTC-based counter

- L0 = length of above (i.e., 0x00 0x04).

- P1 = RSC

- L1 = length of above.

The input key shall be the 256-bit DUCK.

The message-specific confidentiality keystream is set to the L least significant bits of the output of the KDF, where L is the length of the RSC and PRUK ID.

#### 6.42.2.4 Calculation of time-hash-bitsequence

When calculating the time-hash-bitsequence, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [12]:

- FC = 0xZZ

- P0 = UTC-based counter (modified as in subclause 6.42.2.2)

- L0 = length of above (i.e., 0x00 0x04).

The input key shall be the 256-bit DUSK.

The time-hash-bitsequence keystream is set to the L least significant bits of the output of the KDF, where L is the length of the RSC and PRUK ID.

### 6.42.3 Evaluation

The solution fulfils the requirements of KI#5 by protecting Remote UE’s RSC and PRUK ID in case 1) a restricted discovery is performed as a relay discovery and 2) RSC is protected based on either a DUCK or DUSK during restricted discovery.

This solution does not introduce additional network impacts.

Editor’s Note: Further evaluation is FFS.

## 6.43 Solution #43: Improved LTE security mechanism for 5G ProSe restricted discovery to ensure source authentication in out of coverage use cases

### 6.43.1 Introduction

This solution focuses on Key Issue #1(Discovery message protection). This solution proposes to reuse the discovery security mechanism specified in TS 33.303[w] for 5G ProSe restricted discovery, as Solution #4 does, but enhanced to:

* Ensure source authenticity in out of coverage use cases,
* Remove the need of the core network having to verify the integrity of the announcing messages, and
* Improve the resilience against message modification and replay attacks,

The proposed enhancements are motivated by the fact that in TS 33.303/Solution #4 the integrity protection of the discovery messages over the PC5 interface requires a Discovery User Integrity Key (DUIK). This key is used to compute a Message Integrity Code (MIC). For instance, in model A, the MIC can be verified:

(1) at the receiving UE, e.g., the monitoring UE in Model A restricted discovery, if the UE has been supplied with the DUIK, or

(2) at the HPLMN of M-UE DDNMF (Step 13, Figure 6.4.2.1-1) if this NF has been provided with the DUIK and match reports are used.

In the first case, if the DUIK is supplied to a monitoring UE, the monitoring UE can verify the MIC itself. However, if multiple monitoring UEs receive the same DUIK, it is not feasible to guarantee integrity protection, replay protection and most importantly, source authenticity as required in KI#1, since any of those UEs might be malicious. If the ProSe Function has to check the MIC, the solution as described in TS 33.303/Solution#4 does not work when the remote UE is out of coverage.

### 6.43.2 Solution details

#### 6.43.2.1 Basic idea

This solution complements the usage of the integrity key, the DUIK, with a Discovery User Integrity Hash Chain (DUIHC) for source authentication similar to TESLA [x]. The choice of using a solution based on hash chains for source authentication and not on digital signatures is motivated by: (1) bandwidth overhead, (2) CPU overhead, (3) interoperability with the existing LTE solution.

In the following,

* H1(input) = TRUNCb(Hash(Identifier | 1 | input)).
* Hj(input) denotes TRUNCb(Hash(Identifier | j | Hj-1(input)))

Where,

* “|” denotes concatenation,
* Hash(input) refers to the computation of hash function on a given input,
* “Identifiers” include fixed provisioned parameters related to the announcing message, e.g., the relay service code of the announcing UE. Identifiers also include a cryptographic salt.
* TRUNCb(A) is a function that returns b bits of input A, e.g., the b least significant bits of A.

Including “j” and “Identifiers” in the computation of Hj(input) makes the solution more resilient against pre-computation attacks.

The usage of TRUNCb(A) aims at being able to reduce the communication overhead.

With this, a DUIHC is obtained from a randomly generated seed S as:

S 🡪 H1(S) 🡪 H2(S) 🡪 H3(S)🡪 …🡪 HN-2(S) 🡪 HN-1(S) 🡪 HN(S)

Here, the arrow “🡪” indicates the direction when generating the hash chain links H1(S), H2(S),… of the hash chain. The last element, HN(S), is the anchor of this DUIHC. For instance, H1(S) = TRUNCb(Hash(Identifier | 1 | input = S)), H2(S) = TRUNCb(Hash(Identifier | 1 | input = H1(S))),...

An announcing UE is given the seed S of its DUIHC. All monitoring UEs are given the anchor of the DUIHC of the announcing UE. All the UEs, announcing and monitoring, are also given:

* a reference time t0: the time when the announcing UE is supposed to start using the hash chain link, and
* a timeslot duration tDelta: how long a link is valid.
* N: the number of links of the DUIHC.

The number of slots and the timeslot duration determine how long the DUIHC remains valid and how long a UE can perform discovery (supporting source authentication) while being out of coverage. For instance, a hash chain with N=3600 and tDelta=1 second is valid for 1 hour so that UEs configured with it can perform discovery (supporting source authentication) while in out of coverage and without requiring access to the core network

When an announcing UE wants to send an announcing message m at UTC time t, the announcing UE first computes the current timeslot j as (t – t0)/tDelta implying that the announcing UE has to use DUIHC link HN-j(S). Note that this requires that N-j > 0.

The announcing UE uses HN-j(S) together with the DUIK to compute the final key (DHCUIK) used in the creation of the MIC of the message m.

This key is denoted as Discovery Hash Chain User Integrity Key (DHCUIK) and is computed as:

DHCUIK = KDF(DUIK | HN-j(S))

The reason for including the DUIK in the derivation of the DUIKHCL is to: (1) provide interoperability with the existing TS 33.303 solution and (2) show that this solution is as secure as the existing one since the existing DUIK is used in the generation of the key that will be used in the MIC computation.

The MIC of message m is denoted MICm and is computed as:

MICm = MIC(m, DHCUIK)

When the announcing UE broadcasts message m towards the monitoring UEs, the announcing UE includes the previous DUIHC link, namely HN-j+1(S) and MICm:

Announcing UE 🡪 Monitoring UE: m, HN-j+1(S), MICm  (1)

When a monitoring UE receives the above announcing message at time t, the monitoring UE first computes the timeslot j by taking as input the reference time t0 and the timeslot duration tDelta. Then, the monitoring device caches the received message till the next time slot j+1 to receive HN-j(S) in the following announcing message. With HN-j(S), the monitoring UE can check:

1. the validity of the MIC received in the previous message, and thus, the integrity of the message itself. This is done by recomputing DHCUIK and checking that the received MICm matches the computed MIC.
2. the freshness and source authenticity of the message by checking that the received value of HN-j(S)) is correct. To this end, the monitoring UE uses as input the received anchor.

Editor’s note: Process for anchor verification is FFS.

Editor’s note: Scalability in case of many announcing UE is FFS.

Editor’s note: computational overhead at the monitoring UE is FFS.

Editor’s note: replay attack is FFS.

#### 6.43.2.2 Message flows for restricted discovery model A

Referring to Section 6.4.2.1 and Figure 6.4.2.1-1 (Solution #4 restricted discovery model A), the following changes are required to support use cases that require discovery of out of coverage UEs while ensuring source authenticatication.

* Step 4: in addition to the received parameters, the announcing UE also needs to be provided in a secure way with the seed S of the DUIHC, reference time, number of links in the DUIHC, and timeslot duration.
* Step 10: in addition to the received parameters, the monitoring UE also needs to be provided in a secure way with the anchor of the DUIHC, reference time, number of links in the DUIHC, and timeslot duration.
* Step 11 (Announce code): is modified to use links in the DUIHC when computing the broadcasted MIC as described in Section 6.4.2.1. The broadcasted message is as in (1) above.
* Step 12 (Receive code): is modified to use the received anchor of the DUIHC to verify the source authenticity of the received message m. The received broadcast message is as in (1) above.
* Steps 13 – 16 are not required to ensure source authenticity independently whether the monitoring UE is in coverage or out of coverage.

Additionally:

* If a monitoring UE detects a discovery message with a wrong MIC or DUIHC link, the monitoring UE can inform the HPLMN or M-UE DDNMF about the event.
* If an announcing UE is revoked, then the HPLMN oor M-U DDNMF should inform the monitoring UEs that had expressed interest in being able to discover that announcing UE.
* The DUIHC anchor that a monitoring UE receives in Step 10 corresponds to the latest link or a recently disclosed link of the announcing UE DUIHC.

#### 6.43.2.3 Applicability to restricted discovery mode B

The approach described in Sections 6.43.2.1 and 6.43.2.2 can be applied to restricted discovery Mode B with minor modifications as follows: the discoveree UE in Section 6.4.2.2 should own a DUIHC (including the seed) so that it can generate a MIC in a similar way as described above. The discoverer UE in Section 6.4.2.2 should be configured in a secure way with the anchor of the DUIHC so that it can verify the integrity and source authenticity of the Response Code messages without requiring match reports.

### 6.43.3 Evaluation

Editor’s Note: It is FFS whether and how time-limited out of coverage discovery supports out of coverage service requirement (e.g., possible need to standardise the number of hash chain anchors provisioned while in coverage, the starting time t0 and duration N\*tDelta associated to each of those hash chain anchors).

## 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.

## 7.1 Key Issue #1: Discovery message protection

For Key Issue #1, the following is taken as interim conclusions:

* For the open ProSe direct discovery scenario, Solution #3 is used as a basis for normative work.
* For the restricted ProSe direct discovery scenario, Solution #4 is used as a basis for normative work.

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

The conclusions for direct discovery are as follows:

The discovery keys include a cipher key, an integrity key and a scrambling key.

For open discovery, only the integrity key will be assigned by the 5G DDNMF and will be used to provide integrity protection of the announce message.

For restricted discovery, 5G DDNMF will assign the discovery key(s) based on the requirement of the Prose Service.

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

Editor’s Note: Further conclusions is FFS

The solutions for U2N Relay authorization and security can be classified as user-plane (UP) or controlled-plane (CP) based solutions. The UP based solutions use a UP connection to an AF (PKMF) while CP based solutions use the primary authentication for PC5 keys establishment.

It is concluded that both control plane and user plane solutions are supported for L3 U2N relay.

Editor’s Note: Further choices on the co-existence and use cases will be decided further in consultation with SA2.

The following text is taken as conclusions for UE-to-Network Relay solution:

* For the control plane solution, the following conclusion is made:
  + For PC5 link security, PC5 keys are derived using keys derived from the primary authentication (e.g., sol#1, #10, #15, #30). The security of the communication between UE-to-Network relay and remote UE is established based on a shared key which is derived and distributed with the assistance of the network. A root credential is configured in the remote UE and the network. The shared key is individually derived from the root credential by the remote UE and the network. The shared key is distributed by the AMF to the UE-to-Network relay.
  + AUSF derives the PC5 anchor key (e.g., sol#1, sol#15, sol#30, sol#39) used for PC5 keys derivation.

NOTE: The detailed procedure to enable the PC5 link security and the details of the PC5 key hierarchy will be determined accordingly during the normative phase.

* For the user-plane solution, the following is concluded for security in U2N relay:
  + the approach of using the user plane for key management of security keys used for PC5 communication, between the Remote UE and the UE-to-network relay, is adopted as the basis for normative work.
  + a new 5G PKMF function, for commercial services, internal to PLMN, is supporting the key management of security keys used for PC5 communication (between the Remote UE and the UE-to-network relay), which is accessed in the user plane, is adopted as the basis for normative work.
  + the user-plane solutions including Solution #18 and Solution #29 are selected as the basis of normative work.

The following text is taken as the conclusion for the L3 UE-to-Network Relay solution:

* In addition to PC5 link security above, support of end-to-end security requirements when required by Remote UE services using N3IWF as described in solution #19 is taken as a baseline for normative work.

The following text is taken as the conclusion for the L2 UE-to-Network Relay solution:

* It is concluded that the high-level procedure defined in the Solution #14 is taken as the baseline for the normative work. The details of AS security establishment between the Remote UE and the NG-RAN is to be discussed and defined in the normative phase.
* For end-to-end security, the existing NAS/AS security and UP security mechanisms defined in 33.501 [14] are to be reused.

For user-plane solutions, the followings are concluded for both commercial and public safety use cases:

* All security materials for ProSe U2N relay are provided to the UE by PKMF.
  + The discovery keys are managed by PKMF.
  + PC5 keys are managed by PKMF.
  + PCF and/or 5G DDNMF provides the PKMF address to the UE.

NOTE: if PKMF address is configured by both PCF and DDNMF, which one takes precedence will be determined in normative phase in coordination with SA2.

* + For commercial use cases, PKMF can be collocated with 5G DDNMF.
  + For commercial use cases, the PC3 connection between UE and DDNMF (or Ua) can be reused to deliver both the discovery security materials and the PC5 keys (i.e., PRUK and PRUK ID).
  + Both remote UE and relay UE are only required to communicate with the PKMF of their own HPLMN for commercial use cases.
  + For the public safety use case, PKMF may be managed by a public safety operator and located outside of the 3GPP network.
* Authorization information is stored at UDM (and is made available to 5G DDNMF and PKMF) for commercial use cases and at the PKMF for the Public Safety use case.
* When the remote UE has been provided with the PC5 security materials by the PKMF, the PRUK ID (or PC5 key ID) is included in the DCR as a UE ID and other UE IDs and/or UE Info are not sent in clear over the air.

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

The solutions for U2N Relay authorization and security can be classified as user-plane (UP) or controlled-plane (CP) based solutions. The UP based solutions use a UP connection to a PKMF while CP based solutions use the primary authentication for PC5 keys establishment.

The following text is taken as conclusions for the UE-to-Network Relay solution:

* For the control plane solution:
  + Baseline solution for Authorization for Remote UE/Relay is based on primary authentication (CP based approach, e.g., sol#1, #10, #15, #30) and using PCF based service authorization and provisioning as defined in [16] TS 23.304 clause 5.1.4.
  + Performing primary authentication during PC5 link establishment is supported (e.g. Sol#1, Sol#10, Sol#30).

NOTE: The detailed procedure to enable authorization for Remote UE/Relay will be determined accordingly during normative phase. Additional support for Remote UE using its 5G-GUTI in DCR will be determined during normative phase.

* For the user-plane solution, based on the conclusions in KI #3, it is concluded that the user-plane solutions including Solution #18, Solution #21 and Solution #29 are selected as the basis of normative work.

Editor's note: Final conclusion for secondary A&A/NSSAA is FFS.

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

The following text is taken as a conclusion for the UE-to-Network Relay solution (L2, L3 with/without N3IWF):

Path switch is not included in this release, no normative work is needed to address any privacy issue for the path switch scenario.

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

UE-to-UE relay scenario is not included in this release. So there is no need to conclude anything for this key issue.

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

UE-to-UE relay scenario is not included in this release. So there is no need to conclude anything for this key issue.

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

UE-to-UE relay scenario is not included in this release. So there is no need to conclude anything for this key issue.

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

The following text is taken as a conclusion for the UE-to-Network Relay solution (L2, L3 with/without N3IWF):

* For the control-plane solution:
  + Existing network entities (AMF, AUSF, UDM) are used for key derivation and distribution of keys used for UE-to-network relay communication. The security of the communication between UE-to-Network relay and remote UE is established based on a shared key which is derived and distributed with the assistance of the network. A root credential is configured in the remote UE and the network. The shared key is individually derived from the root credential by the remote UE and the network. The shared key is distributed by the AMF to the UE-to-Network relay. The details to realise the above procedures and the details of the PC5 key hierarchy will be determined during the normative phase.
  + AUSF derives the PC5 anchor key (e.g., sol#1, sol#15, sol#30, sol#39) used for PC5 keys derivation.
* For the user-plane solution, based on the conclusions in KI #3, it is concluded that the user-plane solutions including Solution #18, Solution #21 and Solution #29 are selected as the basis of normative work.

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

For Key Issue #10, both Solution #5 and Solution #11 are adopted as the basis for the normative work.

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

Key Issue #11 is about privacy protection of UE identity information that may be broadcasted during discovery.According to TS 23.304 [16] clause 6.3.2.1, one of the UE identities that is broadcasted during discovery is the source Layer-2 ID of the UE broadcasting announcement messages (for Model A) or solicitation messages (for Model B). Also according to TS 23.304 [16], source Layer-2 IDs are always self-assigned and self-selected by the UE originating the corresponding layer-2 frames. Additionaly, a privacy timer value indicating the duration after which the UE shall change each source Layer-2 ID is provisioned to the UE when privacy is required.Therefore, it is concluded that the existing mechanisms in TS 23.304 [16] already support the requirements of Key Issue #11 with respect to the Layer-2 IDs and that apart from potential clarifications on how/when to use these existing mechanisms no additional normative work is needed.

According to TS 23.304 [16], clause 6.3.2.1, also a ProSe Restricted Code is broadcasted during discovery. Although as per section 4.6.4.6 of TS 23.303, a ProSe Restricted Code contains some identity related information in the form of a temporary identifier that corresponds to one or more RPAUIDs, by design of the restricted discovery mechanism (as described in more detail in solutions #4 and #22 for 5G ProSe) the privacy issues of broadcasting a ProSe Restricted Code during discovery are sufficiently addressed. Hence, the resulting normative work for Key Issue #1 is sufficient to address the potential privacy issues for Key Issue #11 with respect to the ProSe Restricted Code.

The privacy of Group Member Discovery of TS 23.304, clause 6.3.2.2, is addressed by Key Issue #13.

According to TS 23.304 [16], clause 6.3.2.3, for ProSe UE-to-Network Relay discovery, next to the Layer-2 IDs, the UEs broadcast Announcer/Discover Info information and Relay Service Code. For the broadcasting of the Layer-2 IDs during discovery similar mitigation as mentioned above can be applied based on the existing mechanisms in TS 23.304. For the Announcer/Discover Info information and Relay Service Code, these can be protected using DUCK/DUSK during discovery to avoid revealing this information to potential eavesdroppers to mitigate tracking of UEs based on this information. This can be handled during the resulting normative work for Key Issue #1.

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

For Key Issue #12, the following textis taken as conclusions:

- It is concluded that the security mechanism defined in TS 33.536 [8] is taken as the baseline for normative work.

Further enhancements can be discussed and added during the normative phase.

Editor's note: Whether other solutions in this TR can be used to enhance one-to-one communication security functionality is FFS.

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

For Key Issue #13, the following text is taken as conclusions:

- For the protection of one-to-many communications between ProSe-enabled UEs, it is concluded that the principle security mechanisms defined in clause 6.2 of TS 33.303 [2] are reused for 5G ProSe public safety case scenarios. Further enhancements or adjustments can be discussed and added during the normative phase.

Editor’s Note: the conclusion on privacy protection of group IDs and L2 IDs is FFS.

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

No solution for Non-IP traffic scenario is available in this release. Hence, no conclusion can be made during this release for this key issue.

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

No solution for Non-IP traffic scenario is available in this release. Hence, no conclusion can be made during this release for this key issue.

## 7.16 Key Issue #16: Privacy protection of PDU session-related parameters for relaying

With an L2 UE-to-Network relay between the Remote UE and the network, no new security vulnerabilities related to KI #16 is identified, hence no new solution is needed. The existing mechanism in TS 23.501 [15] and TS 33.501 [14] are capable to meet the security requirements of KI #16.

Editor’s Note: the conclusion for the case of an L3 U2N relay between the Remote UE and the network is FFS.

## 7.17 Key Issue #17: Supporting security policy handling for PC5 connection of 5G ProSe services

TBD

Annex <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-08 | SA3#100e | S3-201804 |  |  |  | Skeleton | 0.0.0 |
| 2020-08 | SA3#100e | S3-202145 |  |  |  | S3-201804, S3-202144, S3-201826, S3-201756, S3-202129, S3-201757, S3-202130, S3-202147, S3-201616, S3-202157, S3-202146, S3-201618, S3-202064, S3-202066, S3-202065, S3-202067 implemented | 0.1.0 |
| 2020-09 |  |  |  |  |  | Wrong version of the specification was uploaded to the 3GU Portal | 0.1.1 |
| 2020-10 | SA3#100bis-e | S3-202775 |  |  |  | S3-202381, S3-202472, S3-202666, S3-202754, S3-202755, S3-202705, S3-202706, S3-202763, S3-202673, S3-202773, S3-202774, S3-202708, S3-202713, S3-202689, S3-202780, S3-202769, S3-202700, S3-202701, S3-202683, S3-202684, S3-202714 implemented | 0.2.0 |
| 2020-11 | SA3#101-e | S3-203459 |  |  |  | S3-203358, S3-203362, S3-203369, S3-203351, S3-203425, S3-203426, S3-203430, S3-203431, S3-203448, S3-203015, S3-203016, S3-203440, S3-203019, S3-203432, S3-203442, S3-203462, S3-203416, S3-203417, S3-203418, S3-203373, S3-203341, S3-203391, S3-203307, S3-203340, S3-203396, S3-203334 implemented | 0.3.0 |
| 2021-01 | SA3#102-e | S3-210676 |  |  |  | S3-210636, S3-210637, S3-210555, S3-210557, S3-210598, S3-210601, S3-210600, S3-210125, S3-210174, S3-210175, S3-210618, S3-210619, S3-210208, S3-210659, S3-210660, S3-210247, S3-210662, S3-210663, S3-210664, S3-210665, S3-210680, S3-210674, S3-210675, S3-210299, S3-210652, S3-210585, S3-210586, S3-210587, S3-210577, S3-210608, S3-210484, S3-210609, S3-210607, S3-210597 implemented | 0.4.0 |
| 2021-03 | SA3#102bis-e | S3-211274 |  |  |  | S3-211240, S3-211242, S3-210827, S3-211179, S3-211185, S3-210850, S3-211174, S3-211175, S3-211202, S3-211203, S3-211295, S3-211296, S3-211297, S3-210894, S3-210895, S3-211298, S3-211309,, S3-211310, S3-211311, S3-211312, S3-211272, S3-211273, S3-211034, S3-211291, S3-211065, S3-211292, S3-211289, S3-211290, S3-211328, S3-211229, S3-211230, S3-211104, S3-211198, S3-211199, S3-211258 implemented | 0.5.0 |
| 2021-05 | SA3#103-e | S3-212154 |  |  |  | S3-211443, S3-212132, S3-211483, S3-212129, S3-212130, S3-212131, S3-212176, S3-212175, S3-212177, S3-212231, S3-212127, S3-212188, S3-211622, S3-212189, S3-212203, S3-212169, S3-211799, S3-212170, S3-212171, S3-212172, S3-212213, S3-211809, S3-211811, S3-212152, S3-212153, S3-212143, S3-212144, S3-212145, S3-211960, S3-212146, S3-211997, S3-212135, S3-212147 implemented | 0.6.0 |
| 2021-08 | SA3#104-e | S3-213129 |  |  |  | S3-213175, S3-213176, S3-212470, S3-213087, S3-212473, S3-213059, S3-213060, S3-213062, S3-213063, S3-213088, S3-213081, S3-212551, S3-213105, S3-213157, S3-213107, S3-213108, S3-213109, S3-213110, S3-213111, S3-213092, S3-212745, S3-213093, S3-212766, S3-213074, S3-213076, S3-212856, S3-213137, S3-213138, S3-212935, S3-212953, S3-213158, S3-213159, S3-213160, S3-213161, S3-213162, S3-212961, S3-213163, S3-213164, S3-213165 implemented | 0.7.0 |
| 2021-08 | SA3#104e Ad-hoc | S3-213635 |  |  |  | S3-213303, S3-213715, S3-213691, S3-213692, S3-213693, S3-213326, S3-213694, S3-213677, S3-213634, S3-213593, S3-213696, S3-213524, S3-213630, draft\_S3-213554-r8, S3-213560, 3-213619, S3-213620, S3-213621, S3-213622, S3-213588, S3-213613 implemented | 0.8.0 |