|  |
| --- |
| 3GPP TS 33.503 V0.2.0 (2021-11) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Security Aspects of Proximity based Services (ProSe) 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 Overview 8

4.1 General 8

4.2 Reference points and functional entities 8

5 Common security procedures 8

5.1 General 8

5.2 Network domain security 8

5.2.1 General 8

5.2.2 Security of Npc2 reference point 9

5.2.2.1 General 9

5.2.2.2 Security requirements 9

5.2.2.3 Security procedures 9

5.2.3 Security of UE-5G DDNMF interface 9

5.2.3.1 General 9

5.2.3.2 Security requirements 9

5.2.3.3 Security procedures for configuration transfer to the UICC 9

5.2.3.4 Security procedures for PC3a using GBA 9

5.2.3.5 Security procedures for PC3a using AKMA 10

5.2.3.6 The privacy issue in PC3a interface 10

5.2.4 Security of service-based interfaces used in 5G Prose 10

5.2.4.1 Security requirements 10

5.2.4.2 Security procedures 10

5.2.5 Security for UE - 5G PKMF interface 10

5.2.5.1 General 10

5.2.5.2 Security requirements 10

5.2.5.3 Security procedures for PC8 using GBA 11

5.2.5.4 Security procedures for PC8 using AKMA 11

6 Security for 5G ProSe features 11

6.1 Security for 5G ProSe Discovery 11

6.1.1 General 11

6.1.2 Security requirements 11

6.1.3 Security procedures 11

6.1.3.1 Open discovery 11

6.1.3.2 Restricted discovery 14

6.1.3.2.1 General 14

6.1.3.2.2 Security flows 14

6.1.3.2.2.1 Model A restricted discovery 14

6.1.3.2.2.2 Model B restricted discovery 17

6.1.3.2.3 Protection of the discovery messages over the PC5 interface 20

6.2 Security for Unicast mode 5G ProSe Direct Communication 20

6.2.1 General 21

6.2.2 Security requirements 21

6.2.3 Security procedures 21

6.3 Security for 5G ProSe UE-to-Network Relay Communication 21

6.3.1 General 21

6.3.2 Security requirements 21

6.3.3 Security for 5G ProSe Communication via 5G ProSe Layer-3 UE-to-Network Relay 22

6.3.3.1 Security requirements 22

6.3.3.2 Security procedure over User Plane 22

6.3.3.2.1 General 22

6.3.3.2.2 Remote UE attaching to a ProSe UE-to-network relay 23

6.3.3.3 Security procedure over Control Plane 25

6.3.3.3.1 General 26

6.3.3.3.2 Connection with UE-to-Network Relay connection with setup of network Prose security context during PC5 link establishment 26

6.3.3.3.3 PC5 Key Hierarchy 28

6.3.4 Security for 5G ProSe Communication via 5G ProSe Layer-2 UE-to-Network Relay 28

Annex <A> (normative): Key derivation functions 29

A.1 KDF interface and input parameter construction 29

A.1.1 General 29

A.1.2 FC value allocations 29

A.2 5GPRUK derivation function 29

A.3 Derivation of 5GPRUK ID 29

A.4 KNR\_ProSe derivation function 30

Annex <B> (informative): <Informative annex for a Technical Specification> 31

Annex <X> (informative): Change history 31

# Foreword

This Technical Specification 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.

# 1 Scope

The present document specifies the security and privacy aspects of the Proximity based Services (ProSe) in the 5G System (5GS). 5G ProSe security features include: 5G ProSe Direct Discovery security, 5G ProSe Direct communication security, and 5G ProSe UE-to-Network Relay security.

# 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 TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

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

[4] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

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

[6] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[7] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

Definition format (Normal)

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

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

## 3.2 Symbols

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

Symbol format (EW)

<symbol> <Explanation>

## 3.3 Abbreviations

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

Abbreviation format (EW)

<ABBREVIATION> <Expansion>

# 4 Overview

Editor’s Notes: This clause contains the overview of 5G ProSe security and links to other specifications, reference points and functional entities, etc.

## 4.1 General

The overall architecture for 5G ProSe is given in TS 23.304 [2]. 5G ProSe includes several features that may be deployed independently of each other. For this reason, no overall security architecture is provided and each feature describes its own architecture.

Security for the 5G ProSe common procedures is described in clause 5, while the overall security of the 5G ProSe features is described in clause 6.

## 4.2 Reference points and functional entities

Architectural reference model is specified in clause 4.2.1, 4.2.2, 4.2.3, and 4.2.7 of TS 23.304 [2].

In addition to the reference points are specified in clause 4.2.5 of TS 23.304 [2], the 5G Prose architectural reference model shall support the following reference points:

**PC8**: The reference point between the UE and the 5G ProSe Key Management Function (5G PKMF). PC8 relies on 5GC user plane for transport (i.e. an "over IP" reference point). It is used to transport security material to UEs for 5G ProSe UE-to-Network Relay Communication.

# 5 Common security procedures

Editor’s Notes: This clause contains security procedures that are used by more than one ProSe feature.

## 5.1 General

This clause describes the security requirements and procedures that are commonly applied to different modes of ProSe communication, including unicast mode ProSe direct communication and unicast mode ProSe indirect network communication via the U2N relay.

## 5.2 Network domain security

### 5.2.1 General

5G Prose uses several interfaces between network entities, e.g. Npc4 between the 5G DDNMF and the UDM, Npc8 between the 5G DDNMF and the PCF (see TS 23.304 [2]). This subclause describes the security for those interfaces.

### 5.2.2 Security of Npc2 reference point

#### 5.2.2.1 General

Npc2 is the reference point between the ProSe Application Server and the 5G DDNMF as specified in clause 4 of TS 23.304 [2]. When the the ProSe Application Server is in a 3rd party’s network, the Npc2 comprises two interfaces, ie. the service-based interface between the 5G DDNMF and the NEF, and the N33 interface between the NEF and the Prose Application Server. When the Prose Application Server is in a MNO’s network, the Npc2 is a purely service-based interface.

#### 5.2.2.2 Security requirements

When the ProSe Application Server is controlled by a 3rd party, requirements on security aspects of NEF are captured in clause 5.9.2.3 of TS 33.501 [3].

#### 5.2.2.3 Security procedures

When the ProSe Application Server is controlled by a 3rd party, security procedures specified in clause 12 of TS 33.501 [3] is applicable.

When the Prose Application Server is controlled by an MNO, security procedures specified in clause 13 of TS 33.501 [3] is applicable.

As specified in TS 23.304 [2], the 5G System architecture supports the service based Npc2 interface between 5G DDNMF and ProSe Application Server and optionally supports PC2 interface between 5G DDNMF and ProSe Application Server. The security of PC2 reference point specified in TS 33.303 [4] shall be reused.

### 5.2.3 Security of UE-5G DDNMF interface

#### 5.2.3.1 General

PC3a is the reference point between the 5G Prose-enabled UE and the 5G DDNMF as specified in clause 4.2.5 of TS 23.304 [2].

#### 5.2.3.2 Security requirements

3rd parties shall not be allowed to provide configuration data impacting the ProSe-related network operations to the ProSe-enabled UE. The ProSe-enabled UE and the 5G DDNMF shall mutually authenticate each other.

The transmission of the material for 5G Prose discovery between the 5G DDNMF and the ProSe-enabled UE shall be integrity protected.

The transmission of the material for 5G Prose discovery between the 5G DDNMF and the ProSe-enabled UE shall be confidentiality protected.

The transmission of the material for 5G Prose discovery between the 5G DDNMF and the ProSe-enabled UE shall be protected from replays.

#### 5.2.3.3 Security procedures for configuration transfer to the UICC

See clause 5.3.3.1 in TS 33.303 [4].

#### 5.2.3.4 Security procedures for PC3a using GBA

For the security procedures for protecting data transfer between the UE and the 5G DDNMF on the PC3a interface the use of either TLS v1.2 or TLS v. 1.3, as described in clause 5.3.3.2 in TS 33.303 [4] applies with the following modifications:

- The ProSe function is replaced by the 5G DDNMF.

- Confidentiality protection shall be enabled.

#### 5.2.3.5 Security procedures for PC3a using AKMA

Security procedures specified in clause B.1.3.2 of TS 33.535 [5] is applicable with the additional change:

- The 5G DDNMF takes the role of AF.

- Confidentiality protection shall be enabled.

#### 5.2.3.6 The privacy issue in PC3a interface

PC3a interface will be used to transfer the configuration data that is used to perform 5G Direct discovery. According to clause 6.3.1.4 of TS 23.304 [2], the UE Identity is included in the Discovery Request message. Privacy of UE identity is ensured by the confidentiality protection over PC3a interface.

### 5.2.4 Security of service-based interfaces used in 5G Prose

#### 5.2.4.1 Security requirements

The 5G Prose network entities shall be able to authenticate the source of the received data communications.

The transmission of data between 5G Prose network entities shall be integrity protected.

The transmission of data between 5G Prose network entities shall be confidentiality protected.

The transmission of data between 5G Prose network entities shall be protected from replays.

#### 5.2.4.2 Security procedures

Npc4, Npc6, Npc7 and Npc8 specified in clause 4.2.5 of TS 23.304 [2] are realised by corresponding NF service-based interfaces, therefore security procedures specified in clause 13 of TS 33.501 [3].

### 5.2.5 Security for UE - 5G PKMF interface

#### 5.2.5.1 General

The ProSe-enabled UEs have interactions with the 5G PKMF over the PC8 interface in the ProSe features described in TS 23.304 [2].

#### 5.2.5.2 Security requirements

The 5G PKMF for commercial services and for public safety services, provides the security keys and security material impacting the ProSe-related network operations to the ProSe-enabled UE as discovery of a UE-to-network relay and PC5 communication with a UE-to-network relay.

The ProSe-enabled UE and the 5G PKMF shall mutually authenticate each other.

The 5G system shall support that the transmission of the security keys and security material between the 5G PKMF and the ProSe-enabled UE shall be integrity protected.

The 5G system shall support that the transmission of the security keys and security material between the 5G PKMF and the ProSe-enabled UE shall be confidentiality protected.

The 5G system shall support that the transmission of the security keys and security material between the 5G PKMF and the ProSe-enabled UE shall be protected from replays.

The 5G system shall support that the transmission of the UE identity on the PC8 interface.shall be confidentiality protected.

#### 5.2.5.3 Security procedures for PC8 using GBA

For the security procedures for protecting data transfer between the UE and the 5G PKMF on the PC8 interface the use of either TLS v1.2 or TLS v. 1.3, as described in clause 5.3.3.2 in TS 33.303 [4] applies with the following modifications:

- The ProSe function is replaced by the 5G PKMF.

#### 5.2.5.4 Security procedures for PC8 using AKMA

Security procedures specified in clause B.1.3.2 of TS 33.535 [5] is applicable with the additional change:

- The 5G PKMF takes the role of AF.

# 6 Security for 5G ProSe features

Editor’s Notes: This clause contains 5G ProSe features.

## 6.1 Security for 5G ProSe Discovery

Editor’s Notes: This clause contains the description of the security for open 5G ProSe Direct Discovery and restricted 5G ProSe Direct Discovery and 5G ProSe UE-to-Network Relay Discovery.

### 6.1.1 General

### 6.1.2 Security requirements

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

The system shall support confidentiality protection, integrity protection and replay protection of discovery messages in restricted discovery.

The system shall support a method to verify source authenticity of discovery messages.

### 6.1.3 Security procedures

#### 6.1.3.1 Open discovery

The open discovery security procedure is described as follows:



Figure 6.1.3.1-1: Open discovery security procedure

1. The announcing UE sends a Discovery Request message containing the ProSe Application ID to the 5G 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 5G DDNMF. The 5G DDNMF in the HPLMN requests authorization from the VPLMN 5G DDNMF by sending Announce Auth.() message.

3. VPLMN 5G 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 5G 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 5G DDNMF stores the Discovery Key with the ProSe App Code. In addition, the 5G DDNMF provides the UE with a CURRENT\_TIME parameter, which contains the current UTC-based time at the 5G DDNMF, a MAX\_OFFSET parameter, and a Validity Timer. The UE sets a clock which is used for ProSe authentication (i.e. ProSe clock) to the value of CURRENT\_TIME and the UE stores the MAX\_OFFSET parameter, overwriting any previous values. The announcing UE obtains a value for a UTC-based counter associated with a discovery slot based on UTC time. The counter is set to a value of UTC time in a granularity of seconds. The UE may obtain UTC time from any sources available, e.g. the RAN via SIB9, 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 to 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.

5. The UE starts announcing, if the difference between UTC-based counter provided by the system associated with the discovery slot and the UE’s ProSe clock is not greater than the MAX\_OFFSET and if the Validity Timer has not expired. For each discovery slot it uses to announce, the announcing UE calculates a 32-bit Message Integrity Check (MIC) to include with the ProSe App Code in the discovery message. Four least significant bits of UTC-based counter are transmitted along with the discovery message. The MIC is calculated as described in clause A.2 of TS 33.303 [4] using the Discovery Key and the UTC-based counter associated with the discovery slot.

6. The Monitoring UE sends a Discovery Request message containing the ProSe Application ID to the 5G DDNMF in its HPLMN in order to get the Discovery Filters that it wants to listen for.

7. The 5G DDNMF in the HPLMN of the monitoring UE sends Monitor Req. message to the 5G DDNMF in the HPLMN of the announcing UE.

8. The 5G DDNMF in the HPLMN of the announcing UE sends Monitor Resp. message to the 5G DDNMF in the HPLMN of the monitoring UE.

9. The 5G DDNMF returns the Discovery Filter containing either the ProSe App Code(s), the ProSe App Mask(s) or both along with the CURRENT\_TIME and the MAX\_OFFSET parameters. The UE sets its ProSe clock to CURRENT\_TIME and stores the MAX\_OFFSET parameter, overwriting any previous values. The monitoring UE obtains a value for a UTC-based counter associated with a discovery slot based on UTC time. The counter is set to a value of UTC time in a granularity of seconds. The UE may obtain UTC time from any sources available, e.g. the RAN via SIB9, NITZ, NTP, GPS (depending on which is available).

10. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter, if the difference between UTC-based counter associated with that discovery slot and UE’s ProSe clock is not greater than the MAX\_OFFSET of the monitoring UE's ProSe clock.

11. On hearing such a discovery message, and if the UE has either not checked the MIC for the discovered ProSe App Code previously or has checked a MIC for the ProSe App Code and the associated Match Report refresh timer (see steps 14 and 15 for details of this timer) has expired, or as required based on the procedure specified in TS 23.304 [2], the Monitoring UE sends a Match Report message to the 5G 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.5G DDNMF If a Match Report is not required, the Monitoring UE shall locally process the discovery message and the rest of the procedure is not performed.

12. The 5G 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 5G DDNMF in the HPLMN of the announcing UE in the Match Report message.

13. The 5G DDNMF in the HPLMN of the announcing UE shall check the MIC is valid. The relevant Discovery Key is found using the ProSe App Code.

14. The 5G DDNMF in the HPLMN of the announcing UE shall acknowledge a successful check of the MIC to the 5G DDNMF in the HPLMN of the monitoring UE in the Match Report Ack message. The 5G DDNMF in the HPLMN of the announcing UE include 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.

15. The 5G DDNMF in the HPLMN of the monitoring UE acknowledges the MIC check result to the monitoring UE. The 5G 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 5G 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.

#### 6.1.3.2 Restricted discovery

##### 6.1.3.2.1 General

The security for both models of restricted discovery is similar to that of open discovery described in subclause 6.1.3.1. Both models also use a UTC-based counter (see step 9 in clause 6.1.3.1) to provide freshness for the protection of the restricted discovery message on the PC5 interface. The parameters CURRENT\_TIME and MAX\_OFFSET are also provided to the UE from the 5G DDNMF in its HPLMN to ensure that the obtained UTC-based counter is sufficiently close to real time to protect against replays.

The major differences are that restricted discovery requires confidentiality protection of the discovery messages (e.g. to ensure a UE is not discovered by unauthorized parties or tracked due to constantly sending the same ProSe Restricted/Response Code in the clear) and that the MIC checking may be performed by the receiving UE (if allowed by the 5G DDNMF).

The security parameters needed by a sending UE to protect a discovery message (i.e., in model A the announcing UE and in model B the Discoverer UE sending the ProSe Query Code and the Discoveree UE sending the ProSe Response Code) are provided in the Code-Sending Security Parameters. Similarly, the security parameters needed by a UE receiving a discovery message (i.e., in model A the monitoring UE and in model B the Discoverer UE receiving a ProSe Response Code and the Discoveree receiving a ProSe Query Code) are provided in the Code-Receiving Security Parameters.

In addition to clause 6.1.3.4.1 in TS 33.303 [4], 5G Prose introduced a new feature:

- During the discovery request procedure, 5G DDNMF may optionally provide the PC5 security policies to the UEs.

##### 6.1.3.2.2 Security flows

###### 6.1.3.2.2.1 Model A restricted discovery

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



Figure 6.1.3.2.2.1-1: Model A restricted discovery security procedure

Steps 1-4 refer to an Announcing UE.

1. Announcing UE sends a Discovery Request message containing the RPAUID to the 5G DDNMF in its HPLMN in order to get the ProSe Code to announce and to get the associated security material.

2. The 5G DDNMF may check for the announce authorization with the ProSe Application Server.

3. If the Announcing UE is roaming, the 5G DDNMFs in the HPLMN and VPLMN of the Announcing UE exchange Announce Auth.

4. The 5G 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 6.1.3.1 of the current specification.

 The 5G DDNMF in the HPLMN of the Announcing UE may include the PC5 security policies in the Discovery Response message.

NOTE 1: 5G DDNMF may get the PC5 security policies in different ways (e.g., from PCF, from ProSe Application server, or based on local configuration).

Steps 5-10 refer to a Monitoring UE.

5. The Monitoring UE sends a Discovery Request message containing the RPAUID to the 5G DDNMF in its HPLMN in order to be allowed to monitor for one or more Restricted ProSe Application User IDs.

6. The 5G 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.

7. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates a different PLMN, the 5G DDNMF in the HPLMN of the Monitoring UE contacts the indicated PLMN’s 5G DDNMF i.e. the 5G DDNMF in the HPLMN of the Announcing UE, by sending a Monitor Request message.

8. The 5G DDNMF in the HPLMN of the Monitoring UE may exchange authorization messages with the ProSe Application Server.

9. The 5G DDNMF in the HPLMN of the Announcing UE responds to the 5G 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 shall be included as a separate parameter if the Code-Receiving Security Parameters indicate that the Monitoring UE use Match Reports for MIC checking. The 5G 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).

 The 5G DDNMF in the HPLMN of the Announcing UE may send the PC5 security policies to the 5G DDNMF in the HPLMN of the Monitoring UE.

NOTE 2: There are two configurations possible for integrity checking, namely, MIC checked by the 5G DDNMF, and MIC checked at the UE side. Which of the configuration is used is decided by the 5G DDNMF that assigned the ProSe Code being monitored, and signalled to the Monitoring UE in the Code-Receiving Security Parameters.

10. The 5G 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 6.1.3.1 of the current specification. The UE stores the Discovery Filter and Code-Receiving Security Parameters.

 If the 5G DDNMF in the HPLMN of the Monitoring UE receives the PC5 security policies in step 9, the Monitoring UE’s 5G DDNMF forwards the PC5 security policies to the Monitoring UE.

Steps 11 and 12 occur over PC5.

11. 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 UTC-based counter are transmitted along with the protected discovery message.

12. 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 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 23.304 [2]. 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.

13. If the UE has either not had the 5G DDNMF check the MIC for the discovered ProSe Code previously or the 5G 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, or as required based on the procedure specified in TS 23.304 [2], then the Monitoring UE sends a Match Report message to the 5G 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 5G DDNMF checks the MIC.

14. The 5G 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.

15. The 5G DDNMF in the HPLMN of the monitoring UE returns to the Monitoring 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 5G DDNMF in the HPLMN of the Monitoring UE include 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.

16. The 5G DDNMF in the HPLMN of the Monitoring UE may send a Match Report Info message to the 5G DDNMF in the HPLMN of the Announcing UE.

###### 6.1.3.2.2.2 Model B restricted discovery

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



Figure 6.1.3.2.2.2-1: Model B restricted discovery security procedure

Steps 1-4 refer to a Discoveree UE.

1. Discoveree UE sends a Discovery Request message containing the RPAUID to the 5G 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 5G DDNMF may check for the announce authorization with the ProSe Application Server depending on 5G DDNMF configuration.

3. The 5G 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 5G 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 6.1.3.1 of the current specification.

 The 5G DDNMF in the HPLMN of the Discoveree UE may include the PC5 security policies in the Discovery Response message.

NOTE 1: 5G DDNMF may get the PC5 security policies in different ways (e.g., from PCF, from ProSe Application server, or based on local configuration).

Steps 5-10 refer to a Discoverer UE.

5. The Discoverer UE sends a Discovery Request message containing the RPAUID to the 5G DDNMF in its HPLMN in order to be allowed to discover one or more Restricted ProSe Application User IDs.

6. The 5G 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.

7. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates a different PLMN, the 5G DDNMF in the HPLMN of the Discoverer UE contacts the indicated PLMN’s 5G DDNMF i.e. the 5G DDNMF in the HPLMN of the Discoveree UE, by sending a Discovery Request message.

8. The 5G DDNMF in the HPLMN of the Discoveree UE may exchange authorization messages with the ProSe Application Server.

9. The 5G DDNMF in the HPLMN of the Discoveree UE responds to the 5G 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 shall be included as a separate parameter if the Code-Receiving Security Parameters indicate that the Discoverer UE use Match Reports for MIC checking. The 5G 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.

 The 5G DDNMF in the HPLMN of the Discoveree UE may send the PC5 security policies to the 5G DDNMF in the HPLMN of the Discoverer UE.

NOTE 2: There are two configurations possible for integrity checking, namely, MIC checked by the 5G DDNMF, and MIC checked at the UE side; this is decided by the 5G DDNMF that assigned the ProSe Code being monitored, and signalled to the Monitoring UE in the Code-Receiving Security Parameters.

10. The 5G 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.

11. The 5G 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 6.1.3.1 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.

 If the 5G DDNMF in the HPLMN of the Discoverer UE receives the PC5 security policies in step 9, the Discoverer UE’s 5G DDNMF forwards the PC5 security policies to the Discoverer UE.

Steps 12 to 15 occur over PC5.

12. 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.

13. 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 3: Match Reports are not used for the MIC checking of ProSe Query Codes.

14. 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.

15. 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 4: 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 23.304 [2]. If such a Match Report is sent, then there is no security functionality involved.

NOTE 5: 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.

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

16. If the Discoverer UE has either not had the 5G DDNMF check the MIC for the discovered ProSe Response Code previously or the 5G 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, or as required based on the procedure specified in TS 23.304 [2], then the Discoverer UE sends a Match Report message to the 5G 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 5G DDNMF checks the MIC.

17. The 5G 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.

18. The 5G 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 5G DDNMF in the HPLMN of the Discoverer UE include 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.

19. The 5G DDNMF in the HPLMN of the Discoverer UE may send a Match Report Info message to the 5G DDNMF in the HPLMN of the Discoveree UE.

##### 6.1.3.2.3 Protection of the discovery messages over the PC5 interface

There are three types of security that are used to protect the restricted discovery messages over the PC5 interface: integrity protection, scrambling protection, and message-specific confidentiality which are defined in clause 6.1.3.4.3 in TS 33.303 [4].

Editor’s Note: it is for ffs whether security algorithms and/or process in clause 6.1.3.4.3 TS 33.303 [4] can be applied without modification given the potentially different size of the discovery message in 5G ProSe.

## 6.2 Security for Unicast mode 5G ProSe Direct Communication

Editor’s Notes: This clause contains the description of the security for Unicast mode (one-to-one) 5G ProSe Direct Communication.

### 6.2.1 General

The unicast mode 5G ProSe Direct communication procedures are described in TS 23.304 [2]. Unicast ProSe Direct Communication is used by two UEs that directly exchange traffic for the ProSe applications running between the peer UEs.

PC5 direct communication security for relay services is specified in clause 6.3. PC5 security policy provisioning and negotiation during 5G ProSe Restricted Discovery with 5G DDNMF scenario for unicast mode Prose direct communication is specified in clause 6.1.

### 6.2.2 Security requirements

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

The mutual authentication between two ProSe-enabled UEs during PC5 unicast shall be supported.

The PC5 unicast signalling shall support confidentiality protection, integrity protection and anti-replay protection.

The PC5 unicast user plane shall support confidentiality protection, integrity protection and anti-replay protection.

The PCF shall be able to provision the PC5 security policies to the UE per ProSe application, during service authorization and information provisioning procedure as defined in TS 23.304 [2].

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.)

### 6.2.3 Security procedures

The unicast mode security mechanism defined in clause 5.3 of TS 33.536 [6] is reused in 5G ProSe to provide unicast mode 5G ProSe Direct communication security.

## 6.3 Security for 5G ProSe UE-to-Network Relay Communication

Editor’s Notes: This clause contains the description of the security for 5G ProSe UE-to-Network Relay Communication.

### 6.3.1 General

This clause describes the security requirements and the procedures that are specifically applied to 5G ProSe UE-to-Network relay communication defined in TS 23.304 [2]. The security requirements for Layer-3 UE-to-Network relay and Layer-2 UE-to-Network relay are different and are defined in 6.3.3 and 6.3.4 respectively.

The functionality in this clause is supported by both ProSe-enabled UEs for commercial services and public safety.

### 6.3.2 Security requirements

The following security requirements apply to both Layer-3 UE-to-Network relay and Layer-2 UE-to-Network relay:

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

- The 5G system shall support the authorisation of the UE as a Remote UE in the UE-to-Network relay scenario.

- For the discovery, the security requirements in subclause 6.1.2 apply.

- The 5G system shall support a secure means to establish a PC5 link between the remote UE and the UE-to-Network relay.

- The 5G system shall support confidentiality protection, integrity protection and replay protection for secure communication between the remote UE and the 3GPP network via UE-to-Network relays.

### 6.3.3 Security for 5G ProSe Communication via 5G ProSe Layer-3 UE-to-Network Relay

#### 6.3.3.1 Security requirements

Both user-plane (UP) based and control-plane (CP) based the procedure can be used for 5G ProSe Layer-3 UE-to-Network Relay authorization and security establishment. The UP based procedure uses a UP connection to the 5G PKMF, while the CP based procedure uses the primary authentication for PC5 key establishment.

The following are the security requirements for 5G ProSe L3 U2N relay communication:

- For L3 relay security established over control plane, the PCF shall be able to provision the PC5 security policies to the UE per ProSe relay service, during service authorization and information provisioning procedure as defined in TS 23.304 [2].

- For L3 relay security established over user plane, the 5G PKMF shall be able to provision the PC5 security policies to the UE per ProSe relay service, during security materials provisioning procedure defined in clause 6.3.3.2.

- The PC5 UP security policies for protecting 5G ProSe relay communication shall be configured per ProSe relay service based on the security requirements of the specific relay service.

- The activation of PC5 signalling security is based on PC5 CP security policies of the specific ProSe relay service. PC5 signalling integrity security policy is set to “REQUIRED” for 5G ProSe Layer-3 UE-to-Network Relay.

- The activation of PC5 user plane security is based on PC5 UP security policies of the specific ProSe relay service.

- The remote UE shall establish a different PC5 security context with each different relay UE and for each different Relay Service Code. It shall also be possible to establish a security context when the remote UE is out of coverage.

#### 6.3.3.2 Security procedure over User Plane

##### 6.3.3.2.1 General

This clause describes a mechanism to setup a PC5 link between a remote UE and UE-to-network relay. The mechanism includes how a Remote UE and UE-to-network relay get authorized by the ProSe Key Management Function (PKMF) and verify each other’s role.

Editor’s Note: Co-existence with CP based solution is FFS

##### 6.3.3.2.2 Remote UE attaching to a ProSe UE-to-network relay



Figure 6.3.3.2.2-1: Authorization and secure PC5 link establishment procedure for UE-to-network relay

The remote UE is provisioned with the discovery security materials (see clause 6.1.3.2) and Prose Remote User Key (PRUK) when it is in coverage. These security materials are associated with an expiration time, after which they become invalid. If the UE does not have valid discovery security materials, the Remote UE needs to connect to the PKMF and obtain fresh ones to use the UE-to-Network relay services.

NOTE 1: The procedure is described for the scenario that the PKMF of the remote UE is different from the PKMF of the UE-to-network relay. If both the remote UE and the UE-to-network relay are served by a single PKMF, the PKMF takes the role of the PKMF of the remote UE and the PKMF of the UE-to-network relay and the inter-PKMF message exchanges are not needed.

NOTE 2: Steps 0a, 0b, 1a, 1b are performed when the remote UE is in coverage.

0a. The Remote UE gets the ProSe Key management function (PKMF) address from the 5G DDNMF of its HPLMN. Alternatively, the Remote UE may be provisioned with the PKMF address by PCF. If the Remote UE is provisioned with the PKMF address, the Remote UE may access the PKMF directly without requesting it to the 5G DDNMF. In case that the UE cannot access the PKMF using the provisioned PKMF address, the UE may request the PMKF address to the 5G DDNMF.

0b. The remote UE shall establish a secure connection with the PKMF via PC8 reference point. Security for PC8 interface relies on Ua security if GBA [8] is used (see clause 5.2.3.4) or Ua\* security if AKMA [5] is used (see clause 5.2.3.5). The PKMF shall check whether the Remote UE is authorized to receive UE-to-network relay service and if the UE is authorized, the PKMF provides the discovery security materials to the Remote UE. The PKMF of the remote UE shall request the discovery security materials to the PKMFs of the potential relay UEs from which the remote UE gets the relay services, if the Remote UE provided the list of the visited networks.

NOTE 3: The PKMF may be locally configured with the UE’s authorization information. Otherwise, the PKMF interacts with the UDM to retrieve the UE’s authorization information.

NOTE 4: The remote UE is provisioned by PCF with the list of the potential visited networks for the UE-to-network relay service (which is identified by RSC).

0c. The UE-to-network relay gets the ProSe Key management function (PKMF) address from its HPLMN in the same way as described in step 0a.

0d. The UE-to-network relay shall establish a secure connection with the PKMF via PC8 reference point as in step 0b. The PKMF shall check whether the UE-to-network relay is authorized to act as a relay and if authorized, the PKMF provides the discovery security materials to the UE-to-network relay.

1a. The Remote UE sends a PRUK Request message to its PKMF. The message indicates that the Remote UE is requesting a PRUK from the PKMF. If the Remote UE already has a PRUK from this PKMF, the message shall also contain the PRUK ID of the PRUK.

1b. The PKMF checks that the Remote UE is authorised to receive UE-to-network Relay service. This is done by using the Remote UE’s identity associated with the key used to establish 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. If a PRUK and PRUK ID are included, the Remote UE shall store these and delete any previously stored ones for this PKMF.

2. The discovery procedure is performed between the Remote UE and the UE-to-network Relay using the discovery parameters and discovery security material as described in clause 6.1.3.2.

3. The Remote UE sends a Direct Communication Request (DCR) that contains the PRUK ID, Relay Service Code (RSC) of the UE-to-network relay service and KNRP freshness parameter 1 to the UE-to-network relay. If PRUK ID does not contain the HPLMN ID of the Remote UE or the routing information to the PKMF of the Remote UE (e.g., realm part when the NAI format of PRUK ID is used), the DCR message shall include the HPLMN ID of the Remote UE. The PC5 security establishment procedure between the Remote UE and the UE-to-network relay including security parameters and security policy negotiation and protection of messages hereafter shall follow the one-to-one security establishment described in clause 6.2.3 of the present document. Only additional parameters required for the Layer-3 UE-to-network relay scenario are described in this subclause.

Editor’s Note: privacy of PRUK ID is FFS.

4a. The UE-to-network relay sends a Key Request message that contains PRUK ID, RSC and KNRP freshness parameter 1 to its PKMF. The Key Request message shall also include the HPLMN ID of the Remote UE if it is included in the DCR.

4b. On receiving the Key Request message, the PKMF of the UE-to-network relay shall check if the UE-to-network relay is authorized to act as a relay to the Remote UE based on the UE-to-network relay’s identity associated with the key used to establish the secure PC8 connection. If the UE-to-network relay’s authorization information is not locally available, the PKMF shall request the authorization information to the UDM of the UE-to-network relay (not shown in the figure). If the UE-to-network relay is authorized to provide the relay service, the PKMF of the UE-to-network relay sends the Key Request with the PRUK to the PKMF of the remote UE. The PKMF identifies the PKMF address of the Remote UE based on the PRUK ID or HPLMN ID of the Remote UE if it is included in the Key Request message.

Editor’s Note: PKMF’s authorization check of the UE with UDM requires alignment with SA2.

4c. On receiving the Key Request message from the PKMF of the UE-to-network relay, the PKMF of the Remote UE shall check if the Remote UE is authorized to use the relay service based on the PRUK ID and RSC included in the Key Request message. If the Remote UE’s authorization information is not locally available, the PKMF shall request the authorization information to the UDM of the Remote UE (not shown in the figure).

If the PKMF determines a PRUK to be refreshed, the PKMF shall perform the one of the following procedures:

- If the PKMF of the Remote UE supports the Zpn interface to the BSF of the Remote UE, the PKMF of the Remote UE may request a GBA Push Info (GPI – see TS 33.223[xx]) for the Remote UE from the BSF. When requesting the GPI, the PKMF shall include a PRUK ID in the P-TID field. On receiving the GPI, the 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

- If the PKMF supports the SBI interface to the BSF of the Remote UE, the PKMF may request the GPI via SBI interface as described in TS 33.223[xx]. On receiving the GPI, the 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

- If the PKMF of the Remote UE supports the PC4a interface to the HSS of the UE, then the PKMF of Remote UE may request a GBA Authentication Vector (AV) for the Remote UE from the HSS. On receiving the AV, the PKMF locally forms the GPI including a PRUK ID in the P-TID field. The PKMF shall use Ks(\_ext)\_NAF as the PRUK.

- If the PKMF is co-located or integrated with BSF functionality and supports the SBI interface to the UDM/HSS of the Remote UE, the PKMF may request the GBA AV via SBI interface as described in TS 33.220 [8]. On receiving the AV, the PKMF locally forms the GPI including a PRUK ID in the P-TID field. The PKMF shall use Ks(\_ext)\_NAF as the PRUK.

Editor’s Note: GBA push info (GPI) aspects are still under discussion in TR 33.847 [x] therefore additional details for GPI handling are FFS.

 The PKMF of the remote UE shall generate KNRP freshness parameter 2 and derive KNRP using the PRUK identified by PRUK ID, RSC, KNRP freshness parameter 1 and KNRP freshness parameter 2. Then, the PKMF of the remote UE sends a Key Response message that contains KNRP and KNRP freshness parameter 2 to the PKMF of the UE-to-network relay. This message shall include GPI if generated.

4d. The PKMF of the UE-to-network relay sends the Key Response message to the UE-to-network relay.

5a. The UE-to-network relay shall derive the session key (KNRP-SESS) from KNRP and then derive the confidentiality key (NRPEK) and integrity key (NRPIK) as specified in TS 33.536 [6]. The UE-to-network relay sends a Direct Security Mode Command message to the Remote UE. This message shall include the KNRP Freshness Parameter 2 and be protected as specified in TS 33.536 [6].

5b. If the Remote UE receives the message containing the GPI, it processes the GPI as described in TS 33.223[xx]. The Remote UE shall derive the PRUK and obtain the PRUK ID from the GPI.

The Remote UE shall derive KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2. It shall then derive the session key (KNRP-SESS) in the same manner as the UE-to-network relay and process the Direct Security Mode Command. Successful verification of the Direct Security Mode Command assures the Remote UE 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.

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

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

#### 6.3.3.3 Security procedure over Control Plane

Editor’s Notes: This clause describes the security procedure that relies on primary authentication procedure to authenticate/authorize UE during 5G ProSe UE-to-Network Relay Communication.

##### 6.3.3.3.1 General

This subclause describes the security mechanisms for the L3 U2N Relay authentication, authorization and key management using the primary authentication for PC5 keys establishment. Network entities AMF, AUSF and UDM are involved for key derivation and distribution of keys used for UE-to-network relay communication. The UE shall be provisioned with necessary policies and parameters to use 5G ProSe services, as part of the UE ProSe Policy information as defined in TS 23.503 [7] clause 4.2.2. PCF shall provision the authorization policy and parameters for 5G UE-to-Network Relay Discovery and Communication as specified in 5.1.4 in TS 23.304 [2].

##### 6.3.3.3.2 Connection with UE-to-Network Relay connection with setup of network Prose security context during PC5 link establishment

This subclause describes a procedure for a Remote UE to establish a PC5 link between a Remote UE and a UE-to-Network relay. The procedure includes how the Remote UE is authenticated by AUSF via Relay UE and Relay UE's AMF during 5G ProSe PC5 establishment. The mechanism can be used by a Remote UE while out of coverage.



Figure 6.3.3.3.2-1: UE-to-Network Relay security procedure with setup of network Prose security context during PC5 link establishment

0. The Remote UE and relay UE shall be registered with the network. The UE-to-Network relay shall be authenticated and authorized by the network to support as a relay UE. Remote UE shall be authenticated and authorized by the network to act as a Remote UE.

1. The remote UE shall initiate discovery procedure using any of Model A or Model B method as specified in clause 6.3.1.2 or 6.3.1.3 of TS 23.304 [2] respectively.

2-5. After the discovery of the UE-to-Network relay, the Remote UE shall send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE shall include its security capabilities and security policy in the DCR message as specified in TS 33.536 [6]. The message shall also include SUCI, Relay Service Code, Nonce\_1. Upon receiving the DCR message, the Relay UE shall send the relay key request to the relay AMF, including the parameters received in the DCR message. The Relay AMF shall verify whether the relay UE is authorized to act as U2N relay. The relay AMF shall select AUSF based on SUCI and forward the key request to the AUSF in Nausf\_UEAuthentication\_Authenticate Request message.

6-7. The AUSF shall retrieve the Authentication Vectors from the UDM and trigger primary authentication of the remote UE using existing procedure as specified in TS 33.501 [3]. This authentication is performed between the AUSF and the remote UE via the relay AMF and relay UE. AUSF shall not make the newly derived KAUSF as the latest KAUSF. At the remote UE, the newly derived KAUSF shall not be taken as latest KAUSF as NAS SMC procedure is not performed between remote UE and relay AMF.

Editor's note: Further details on authentication message handling in UE, Relay UE's AMF and AUSF are FFS.

Editor's note: There are essentially two different KAUSF keys. Different key names should be used to avoid confusion and misleading. This is FFS.

Editor's note: A new service operations should be used for Prose authentication to distinguish it from primary authentication defined in 33.501, to separate the different function and service logic. This is FFS.

8. On successful primary authentication, the AUSF and Remote UE shall generate 5GPRUK (as specified in Annex A.2) and 5GPRUK ID as specified in Annex A.3 using the newly derived KAUSF.

9. The AUSF shall generate the KNR\_ProSe key as defined in Annex A.4.

10-11. The AUSF shall send the 5GPRUK ID, KNR\_ProSe, Nonce\_2 in Nausf\_UEAuthentication\_Authenticate Response message to the UE-to-Network relay via relay AMF. When receiving a KNR\_ProSe from AUSF, the AMF shall not attempt to trigger NAS SMC procedure with Remote UE. Relay UE derives PC5 session key Krelay-sess and confidentiality and integrity keys from KNR\_ProSe, using the KDF defined in clause 6.3.3.3.4 of this document. KNR\_ProSe ID and Krelay-sess ID are established in the same way as KNRP ID and KNRP-sess ID in TS 33.536 [6].

12. The UE-to-Network relay shall send the received 5GPRUK ID, Nonce\_2 to the Remote UE in Direct Security mode command message.

13-14. The remote UE shall use the 5GPRUK ID to locate the KAUSF/5GPRUK to be used for the PC5 link security. Remote UE shall generate the KNR\_ProSe key to be used for Remote access via the Relay UE in the same way as defined in step 9. The Remote UE shall derive PC5 session key Krelay-sess and confidentiality and integrity keys from KNR\_ProSe the same way as defined in step 11. Remote UE shall send 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: Further details on the needs and usage of 5GPRUK ID are FFS.

##### 6.3.3.3.3 PC5 Key Hierarchy



Figure 6.3.3.3.3-1: PC5 Key Hierarchy for UE-to-Network Relay security

The different layers of keys (see Figure 6.3.3.3.3-1) are the following:

- 5GPRUK: The root credential derived from KAUSF that is the root of security of the PC5 unicast link.

- KNR\_ProSe: This is a 256-bit root key that is established between the two entities that communicating using NR PC5 unicast link. It may be refreshed by re-running the authentication to derive a fresh 5GPRUK.

- Krelay-sess: This is the 256-bit key that is derived by UE from KNR\_ProSe and is used derive keys that to protect the transfer of data between the UEs. The Krelay-sess is derived per unicast link same as KNRP-sessspecified in TS 33.536 [6]. During activated unicast communication session between the UEs, the Krelay-sess may be refreshed by running the rekeying procedure. The keys for confidentiality and integrity algorithms are derived directly from Krelay-sess. The 16-bit Krelay-sess ID identifies the Krelay-sess.

- Krelay-int, Krelay-enc: The Krelay-int and Krelay-enc are used in the chosen confidentiality and integrity algorithms respectively for protecting PC5-S signalling, PC5 RRC signalling, and PC5 user plane data. These keys are equivalent to NRPIK and NRPEK as specified in TS 33.536 [6]. They are derived from Krelay-sess and are refreshed automatically every time Krelay-sess is changed.

### 6.3.4 Security for 5G ProSe Communication via 5G ProSe Layer-2 UE-to-Network Relay

Connection establishment for 5G ProSe Communication via 5G ProSe Layer-2 UE-to-Network Relay is specified in clause 6.5.2.2 of TS 23.304 [2]. During the connection establishment, the Remote UE and NG-RAN node shall establish AS security as specified in TS 33.501 [3].

The remote UE and the relay UE shall establish security for PC5 connection as specified in clause 6.2.

Annex <A> (normative):
Key derivation functions

# A.1 KDF interface and input parameter construction

## A.1.1 General

All key derivations for 5G ProSe shall be performed using the key derivation function (KDF) specified in Annex B.2.2 of TS 33.220 [8].

This clause specifies how to construct the input string, S, and the input key, KEY, for each distinct use of the KDF. Note that "KEY" is denoted "Key" in TS 33.220 [8].

## A.1.2 FC value allocations

The FC number space used is controlled by TS 33.220 [8], FC values allocated for the present document are : 0xXX, , 0xAA , 0xZZ.

# A.2 5GPRUK derivation function

When deriving a 5GPRUK from KAUSF, the following parameters shall be used to form the input S to the KDF:

- FC = 0xXX;

- P0 = SUPI;

- L0 = length of SUPI.

- P1 = relay service code;

- L1 = length of relay service code.

The input key KEY is KAUSF.

SUPI shall behave the same value as parameter P0 in Annex A.7.0 of TS 33.501 [3].

# A.3 Derivation of 5GPRUK ID

When deriving the 5GPRUK ID from KAUSF, the following parameters are used to form the input S to the KDF:

- FC = 0xAA (to be allocated by 3GPP);

- P0 = "PRUK-ID";

- L0 = length of "PRUK-ID".

- P1 = relay service code;

- L1 = length of relay service code.

- P2 = SUPI;

- L2 = length of SUPI.

The input key KEY is KAUSF.

# A.4 KNR\_ProSe derivation function

When deriving the KNR\_ProSe from 5GPRUK key, the following parameters shall be used to form the input S to the KDF:

- FC = 0xZZ;

- P0 = Nonce\_2;

- L0 = length of Nonce\_2;

- P1 = Nonce\_1;

- L1 = length of Nonce\_1

The input key KEY shall be 5GPRUK key.

SUPI shall be have the same value as parameter P0 in Annex A.7.0 of TS 33.501 [3].

Annex <B> (informative):
<Informative annex for a Technical Specification>

Informative annexes may appear in both Technical Specifications and Technical Reports. Use style "Heading 8" for use in TSs.

Informative annexes shall not contain requirements for the implementation of the Technical Specification.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-10 | SA3#104e Ad-hoc | S3-213638 |  |  |  | Skeleton for this TS (approved in S3-213638 at SA3#104e Ad-hoc) | 0.0.0 |
| 2021-10 | SA3#104e Ad-hoc | S3-213639 |  |  |  | Inclusion of documents approved at SA3#104e Ad-hoc: S3-213636, S3-213637. | 0.1.0 |
| 2021-11 | SA3#105e | S3-214511 |  |  |  | Inclusion of documents approved at SA3#105e: S3-214470, S3-214471, S3-214472, S3-214473, S3-214105, S3-214110, S3-214438, S3-214441, S3-214444, S3-214488, S3-214495. | 0.2.0 |
|  |  |  |  |  |  |  |  |