

ETSI TS 133 503 V17.0.1 (2022-07)



**5G ;
Security Aspects of Proximity based Services (ProSe)
in the 5G System (5GS)
(3GPP TS 33.503 version 17.0.1 Release 17)**



Reference

DTS/TSGS-0333503vh01

Keywords

5G, SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	6
1 Scope	8
2 References	8
3 Definitions of terms, symbols and abbreviations	8
3.1 Terms.....	8
3.2 Symbols.....	9
3.3 Abbreviations	9
4 Overview	10
4.1 General	10
4.2 Reference points and functional entities.....	10
4.2.1 Functional entities.....	10
4.2.1.1 General	10
4.2.1.2 5G ProSe Key Management Function.....	10
4.2.2 Reference points	10
5 Common security procedures	11
5.1 General	11
5.2 Network domain security	11
5.2.1 General.....	11
5.2.2 Security of Npc2 reference point	11
5.2.2.1 General	11
5.2.2.2 Security requirements.....	11
5.2.2.3 Security procedures	11
5.2.3 Security of UE - 5G DDNMF interface	11
5.2.3.1 General	11
5.2.3.2 Security requirements.....	12
5.2.3.3 Security procedures for configuration transfer to UICC	12
5.2.3.4 Security procedures for PC3a using GBA.....	12
5.2.3.5 Security procedures for PC3a using AKMA.....	12
5.2.3.6 Privacy issue in PC3a interface.....	12
5.2.4 Security of service-based interfaces used in 5G ProSe.....	12
5.2.4.1 Security requirements.....	12
5.2.4.2 Security procedures	12
5.2.5 Security for UE - 5G PKMF interface	13
5.2.5.1 General	13
5.2.5.2 Security requirements.....	13
5.2.5.3 Security procedures for PC8 using GBA	13
5.2.5.4 Security procedures for PC8 using AKMA.....	13
6 Security for 5G ProSe features	13
6.1 Security for 5G ProSe Discovery	13
6.1.1 General.....	13
6.1.2 Security requirements	13
6.1.3 Security procedures.....	14
6.1.3.1 Open 5G ProSe Direct Discovery	14
6.1.3.2 Restricted 5G ProSe Direct Discovery.....	16
6.1.3.2.1 General	16
6.1.3.2.2 Security flows.....	16
6.1.3.2.3 Protection of discovery messages over PC5 interface	24
6.2 Security for unicast mode 5G ProSe Direct Communication	25
6.2.1 General.....	25

6.2.2	Security requirements	25
6.2.3	Security procedures.....	25
6.3	Security for 5G ProSe UE-to-Network Relay Communication.....	25
6.3.1	General.....	25
6.3.2	Security requirements	26
6.3.3	Security for 5G ProSe Communication via 5G ProSe Layer-3 UE-to-Network Relay.....	26
6.3.3.1	Security requirements.....	26
6.3.3.2	Security procedure over User Plane	27
6.3.3.2.1	General	27
6.3.3.2.2	5G ProSe Remote UE attaching to a 5G ProSe UE-to-Network Relay	27
6.3.3.2.3	PC5 Key Hierarchy over User Plane	31
6.3.3.3	Security procedure over Control Plane	31
6.3.3.3.1	General	31
6.3.3.3.2	Connection with 5G ProSe UE-to-Network Relay connection with setup of network Prose security context during PC5 link establishment	31
6.3.3.3.3	PC5 Key Hierarchy over Control Plane.....	35
6.3.3.3.4	5G ProSe Remote UE Secondary Authentication via a 5G ProSe Layer-3 UE-to-Network Relay without N3IWF	35
6.3.3.4	Security for 5G ProSe Communication via Layer-3 UE-to-Network Relay with N3IWF support	41
6.3.4	Security for 5G ProSe Communication via 5G ProSe Layer-2 UE-to-Network Relay.....	41
6.3.5	Direct Communication Request in 5G ProSe UE-to-Network Relay Communication.....	42
6.3.5.1	General	42
6.3.5.2	Privacy protection of PRUK ID and RSC in DCR.....	42
6.3.5.3	Integrity protection of DCR	43
7	5G ProSe services.....	43
7.1	General	43
7.2	5G PKMF Services.....	43
7.2.1	General.....	43
7.2.2	Npkmf_PKMFKeyRequest service	43
7.2.2.1	Npkmf_PKMFKeyRequest_ProseKey service operation	43
7.3	AUSF Services	44
7.3.1	General.....	44
7.3.2	Nausf_UEAuthentication Service.....	44
7.3.2.1	Nausf_UEAuthentication_ProseAuthenticate service operation.....	44
7.3.2.2	Nausf_UEAuthentication_ProseGet service operation	44
7.4	UDM Services	45
7.4.1	General.....	45
7.4.2	Nudm_UEAuthentication Service	45
7.4.2.1	Nudm_UEAuthentication_GetProseAv service operation	45
7.4.3	Nudm_UEIdentifier Service	45
7.4.3.1	Nudm_UEIdentifier_Deconceal service operation.....	45
7.5	Prose Anchor Function Services	45
7.5.1	General.....	45
7.5.2	Npanf_ProseKey service.....	46
7.5.2.1	Npanf_ProseKey_Register service operation.....	46
7.5.2.2	Npanf_ProseKey_Get service operation	46
7.5.3	Npanf_get service	46
7.5.3.1	Npanf_Get service operation.....	46
Annex A (normative):	Key derivation functions	47
A.1	KDF interface and input parameter construction	47
A.1.1	General	47
A.1.2	FC value allocations	47
A.2	5GPRUK derivation function.....	47
A.3	Derivation of 5GPRUK ID*.....	47
A.4	K_{NR_ProSe} derivation function.....	48
A.5	Calculation of DCR confidentiality keystream	48

A.6	Calculation of MIC value for discovery message	48
A.7	Message-specific confidentiality mechanisms for discovery	49
A.8	Calculation of K_{NRP} for UE-to-Network relays	49
A.9	Calculation of MIC value for Direct Communication Request.....	49
Annex B (informative):	Source authenticity of discovery messages	51
Annex C (informative):	Change history	52
History		53

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)".
- [9] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".
- [10] 3GPP TS 23.502: "Procedures for the 5G System".
- [11] 3GPP TS 33.102: "3G security; Security architecture".
- [12] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".
- [13] 3GPP TS 23.502: "Procedures for the 5G System".
- [14] IETF RFC 7542: "The Network Access Identifier".

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].

For the purposes of the present document, the following terms given in 3GPP TS 23.304 [2] apply:

5G ProSe Direct Communication
 5G ProSe Direct Discover
 5G ProSe-enabled UE
 5G ProSe Remote UE
 5G ProSe UE-to-Network Relay
 Direct Network Communication
 Discovery Filter
 Discovery Query Filter
 Discovery Response Filter
 Indirect Network Communication
 Mode of communication
 Model A
 Model B
 Open ProSe Discovery
 ProSe Application Code
 ProSe Application ID
 ProSe Application Mask
 ProSe Query Code
 ProSe Response Code
 ProSe Restricted Code
 Restricted ProSe Application User ID
 Restricted ProSe Discovery

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

5G DDNMF	5G Direct Discovery Name Management Function
5G PKMF	5G ProSe Key Management Function
5GPRUK	5G ProSe Remote User Key
AF	Application Function
AKMA	Authentication and Key Management for Applications
AV	Authentication Vector
BSF	Bootstrapping Server Function
CP	Control Plane
DCR	Direct Communication Request
DUCK	Discovery User Confidentiality Key
DUIK	Discovery User Integrity Key
DUSK	Discovery User Scrambling Key
GBA	Generic Bootstrapping Architecture
GPI	GBA Push Info
GPS	Global Positioning System
MIC	Message Integrity Check
NAI	Network Access Identifier
NITZ	Network Identity and Time Zone
NRPEK	NR PC5 Encryption Key
NRPIK	NR PC5 Integrity Key
NTP	Network Time Protocol
ProSe	Proximity-based Services
PRUK	Prose Remote User Key
RPAUID	Restricted ProSe Application User ID
RSC	Relay Service Code
SBI	Service Based Interface
UP	User Plane

UTC Universal Time Coordinated

4 Overview

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

4.2.1 Functional entities

4.2.1.1 General

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].

4.2.1.2 5G ProSe Key Management Function

In addition to the architectural reference model specified in TS 23.304 [2], the architectural reference model shall support the functional entity 5G ProSe Key Management Function (5G PKMF) which is the logical function handling network related actions required for the key management and the security material for discovery of a 5G ProSe UE-to-Network Relay by a 5G ProSe Remote UE, and for establishing a secure PC5 communication link between a 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay.

The 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay know from which 5G ProSe Key Management Function(s) to get the needed discovery security materials for protecting discovery messages and PRUK(s) for establishing a secure PC5 link between the 5G ProSe Remote UE and the UE-to-Network Relay as the address of the 5G PKMF(s) is either pre-provisioned or provided by the 5G DDNMF (or the PCF) in the HPLMN of the 5G ProSe Remote UE to the 5G ProSe Remote UE, and by the 5G DDNMF (or the PCF) in the HPLMN of the 5G ProSe UE-to-Network Relay to the 5G ProSe UE-to-Network Relay.

The 5G PKMF interacts with the 5G ProSe-enabled UE using procedures over PC8 reference point defined in clause 4.2.2. The protection for the key request/response messages are described in clause 5.2.5.

The 5G PKMF of the 5G ProSe Remote UE shall request the discovery security materials from the 5G PKMFs of the potential 5G ProSe UE-to-Network Relays from which the 5G ProSe Remote UE gets the relay services.

The 5G PKMF of the 5G ProSe UE-to-Network Relay shall request the security materials (e.g. Knrp and Knrp freshness parameter) from the 5G PKMF of the 5G ProSe Remote UE for PC5 communication.

4.2.2 Reference points

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.
- Npc9:** The reference point between the 5G PKMF of the 5G ProSe Remote UE and the 5G PKMF of the 5G ProSe UE-to-Network Relay. It is used to transport security material between two 5G PKMFs.

Npc10: The reference point between the UDM and 5G PKMF. It is used to de-conceal SUCI to gain SUPI, obtain a GBA Authentication Vector (AV) for a UE, or request relay service authorization information from the UDM.

5 Common security procedures

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 Network Communication and unicast mode ProSe Indirect Network Communication via the 5G ProSe UE-to-Network 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 clause 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 ProSe Application Server is in a 3rd party's network, the Npc2 comprises two interfaces, i.e. 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 a 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 the 5G DDNMF and the 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 5G ProSe-related network operations to the 5G ProSe-enabled UE. The 5G 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 5G ProSe-enabled UE shall be integrity protected.

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

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

5.2.3.3 Security procedures for configuration transfer to 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 changes:

- The 5G DDNMF takes the role of AF.
- Confidentiality protection shall be enabled.

5.2.3.6 Privacy issue in PC3a interface

PC3a interface will be used to transfer the configuration data that is used to perform 5G ProSe 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 realized by corresponding NF service-based interfaces, therefore security procedures specified in clause 13 of TS 33.501 [3] apply to these interfaces.

5.2.5 Security for UE - 5G PKMF interface

5.2.5.1 General

The 5G ProSe-enabled UEs have interactions with the 5G PKMF over the PC8 interface in the ProSe features described in clause 4.2.2.

5.2.5.2 Security requirements

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

The 5G 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 5G 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 5G 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 5G 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 of TS 33.303 [4] applies with the following modifications:

- The ProSe function is replaced by the 5G PKMF.
- Confidentiality protection shall be enabled.

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.
- Confidentiality protection shall be enabled.

6 Security for 5G ProSe features

6.1 Security for 5G ProSe Discovery

6.1.1 General

6.1.2 Security requirements

The 5G System shall support integrity protection and replay protection of discovery messages in open 5G ProSe Direct Discovery.

The 5G System shall support confidentiality protection, integrity protection and replay protection of discovery messages in restricted 5G ProSe Direct Discovery.

The 5G System shall support a method to verify source authenticity of discovery messages.

6.1.3 Security procedures

6.1.3.1 Open 5G ProSe Direct Discovery

The open 5G ProSe Direct Discovery security procedure is described as follows.

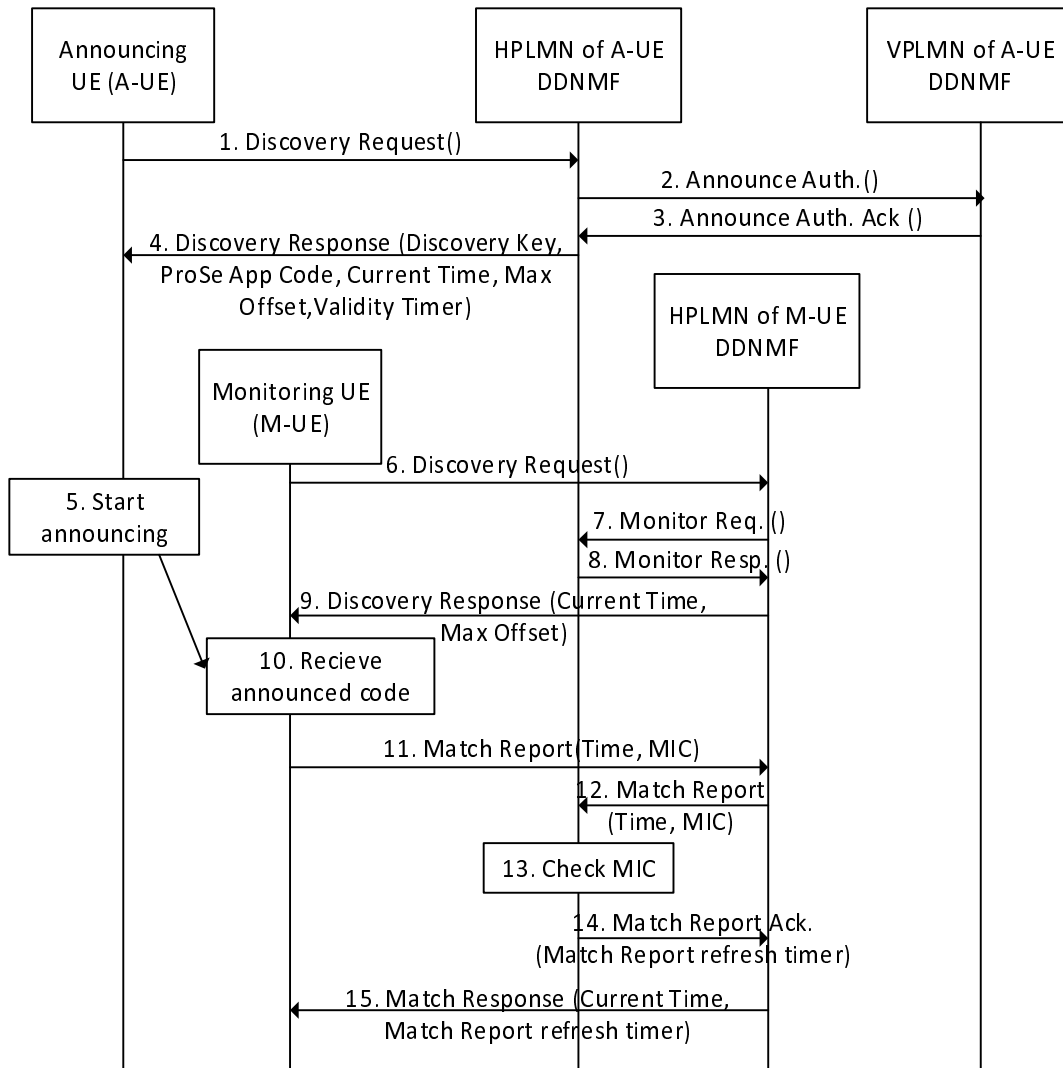


Figure 6.1.3.1-1: Open 5G ProSe Direct Discovery security procedure

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 authorized 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 5G ProSe Direct 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 Application Code that the Announcing UE can announce and a Discovery Key associated with it. The 5G DDNMF stores the Discovery Key with the ProSe Application 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 Application 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 Application Code(s), the ProSe Application 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 via Match Report previously or has checked a MIC for the ProSe App Code via Match Report 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. 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 Application 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 Application 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 Application 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 5G ProSe Direct Discovery

6.1.3.2.1 General

The security for both models of restricted 5G ProSe Direct Discovery is similar to that of open 5G ProSe Direct Discovery described in clause 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 5G ProSe Direct 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 5G ProSe Direct Discovery requires confidentiality protection of the discovery messages (e.g. to ensure a UE's privacy is not disclosed to 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.
- A ciphering algorithm for message-specific confidentiality is configured at the UE during the Discovery Request procedure.

5G ProSe UE-to-Network Relay discovery is different from 5G ProSe Restricted Direct Discovery. In 5G ProSe UE-to-Network Relay discovery, the discovery security materials are provided by the PKMF in case of user-plane based security procedure (as specified in clause 6.3.3.2), and by the DDNMF or the PCF in case of control-plane based security procedure. The 5G ProSe UE-to-Network Relay discovery procedures described in clause 6.1.3.2.2.1 and clause 6.1.3.2.2.2 apply with adjustment when 5G DDNMF or 5G PKMF is used for 5G ProSe UE-to-Network Relay discovery.

6.1.3.2.2 Security flows

6.1.3.2.2.1 Restricted 5G ProSe Direct Discovery Model A

The security procedure for restricted 5G ProSe Direct Discovery Model A is described as follows.

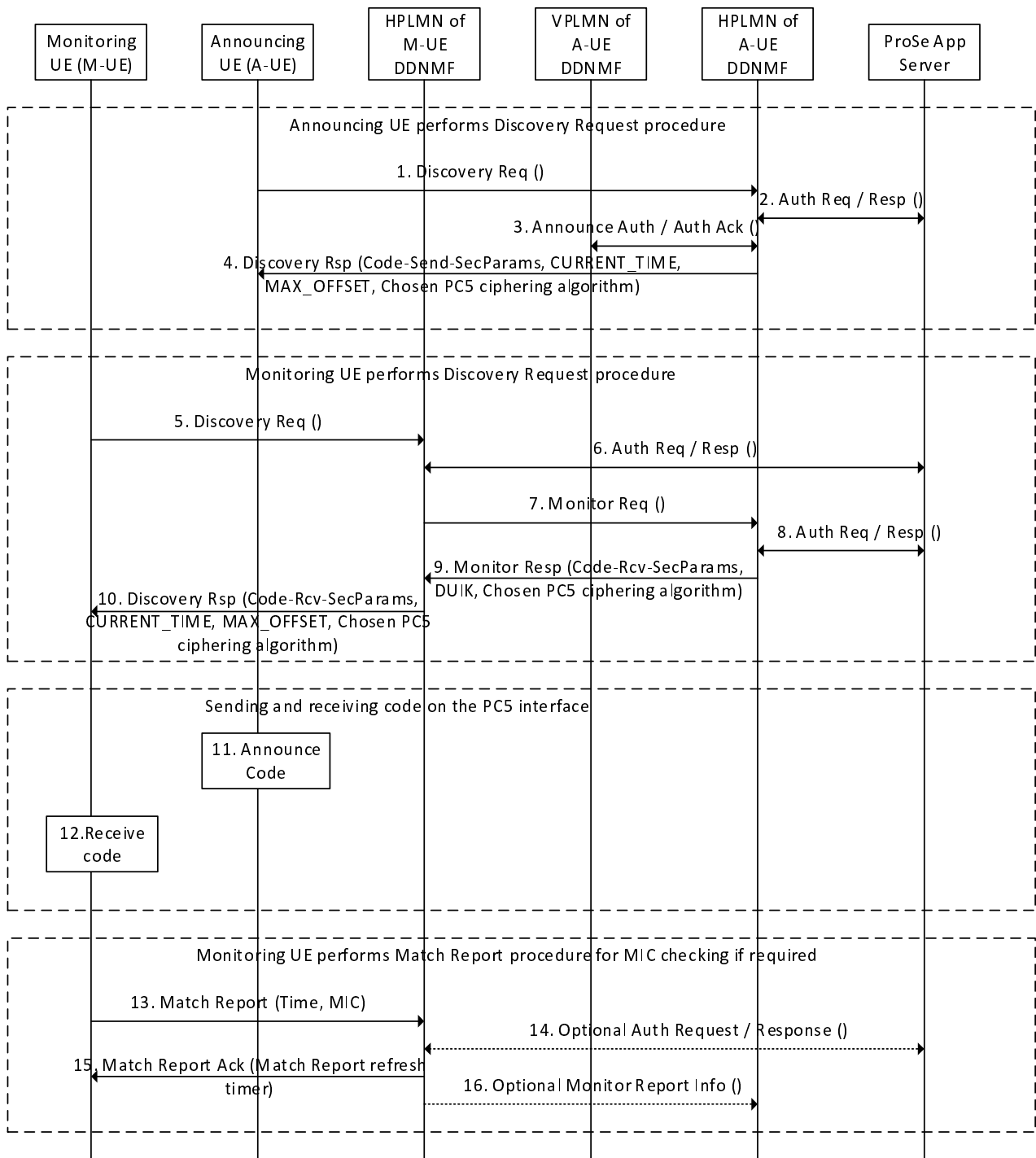


Figure 6.1.3.2.2.1-1: Security procedure for restricted 5G ProSe Direct Discovery Model A

NOTE 1: When the user-plane based security procedure for the UE-to-Network Relay is used, the 5G PKMF takes the role of the 5G DDNMF as described in 6.3.3.2 of the present document.

Steps 1-4 refer to an Announcing UE:

1. Announcing UE sends a Discovery Request message containing the Restricted ProSe Application User ID (RPAUID) to the 5G DDNMF in its HPLMN in order to get the ProSe Code to announce and to get the associated security material. In addition, the Announcing UE shall include its PC5 UE security capability that contains the list of supported ciphering algorithms by the UE in the Discovery Request message.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe UE-to-Network Relay plays the role as the Announcing UE and sends a Relay Discovery Key Request instead of a Discovery Request. The Relay Discovery Key Request message includes the Relay Service Code (RSC) and the 5G ProSe UE-to-Network Relay's PC5 security capability.

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

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.

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 Restricted 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 Restricted Code and are stored with the ProSe Restricted Code. The Announcing UE takes the same actions with CURRENT_TIME and MAX_OFFSET as described for the Announcing UE in step 4 of clause 6.1.3.1 of the present document. The 5G DDNMF in the HPLMN of the Announcing UE shall include the chosen PC5 ciphering algorithm in the Discovery Response message. The 5G DDNMF determines the chosen PC5 ciphering algorithm based on the ProSe Restricted Code and the received PC5 UE security capability in step 1. The UE stores the chosen PC5 ciphering algorithm together with the ProSe Restricted Code.

In addition, the 5G DDNMF in the HPLMN of the Announcing UE may associate the ProSe Restricted Code with the PC5 security policies and include the PC5 security policies in the Discovery Response message.

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Discovery Response, and the RSC is used instead of the ProSe Restricted Code. The response message contains the discovery security materials.

NOTE 2: 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 and its PC5 UE security capability to the 5G DDNMF in its HPLMN in order to be allowed to monitor for one or more Restricted ProSe Application User IDs.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe Remote UE plays the role of the Monitoring UE and sends a Relay Discovery Key Request instead of the Discovery Request. The Relay Discovery Key Request message includes the RSC and the 5G ProSe Remote UE's PC5 security capability.

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.

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.

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 including the PC5 UE security capability received in step 5.

For 5G ProSe UE-to-Network Relay Discovery, Relay Discovery Key Request and RSC are used instead of Discovery Request and RPAUID.

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

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.

9. If the PC5 UE security capability in step 5 includes the chosen PC5 ciphering algorithm, 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 Restricted Code, the corresponding Code-Receiving Security Parameters, an optional Discovery User Integrity Key (DUIK), and the chosen PC5 ciphering algorithm (based on the information/keys stored in step 4). 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 Restricted Code and the Discovery User Integrity Key (if it received one outside of the Code-Receiving Security Parameters).

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Discovery Response, and the RSC is used instead of the ProSe Restricted Code. The response message contains the discovery security materials.

The 5G DDNMF in the HPLMN of the Announcing UE may send the PC5 security policies associated with the ProSe Restricted Code to the 5G DDNMF in the HPLMN of the Monitoring UE.

NOTE 3: There are two possible configurations for integrity checking, namely, MIC checked by the 5G DDNMF of the Monitoring UE, and MIC checked at the Monitoring UE side. Which configuration to use is decided by the 5G DDNMF, which assigns the monitored ProSe Restricted Code and signals the Monitoring UE in the Code-Receiving Security Parameters.

NOTE 4: The chosen PC5 ciphering algorithm is associated with the ProSe Restricted Code.

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 and the chosen PC5 ciphering algorithm. The Monitoring UE takes the same actions with CURRENT_TIME and MAX_OFFSET as described for the Monitoring UE in step 9 of clause 6.1.3.1 of the present document. The UE stores the Discovery Filter, Code-Receiving Security Parameters, and the chosen PC5 ciphering algorithm together with the ProSe Restricted Code.

If the 5G DDNMF in the HPLMN of the Monitoring UE receives the PC5 security policies associated with the ProSe Restricted Code 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 5: 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 Restricted Code previously or the 5G DDNMF has checked a MIC for the ProSe Restricted 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 Restricted 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 Application Server to ensure that Monitoring UE is authorized to discover the Announcing UE.

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.

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 included 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 Restricted 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 Restricted 5G ProSe Direct Discovery Model B

The security procedure for restricted 5G ProSe Direct Discovery Model B is described as follows.

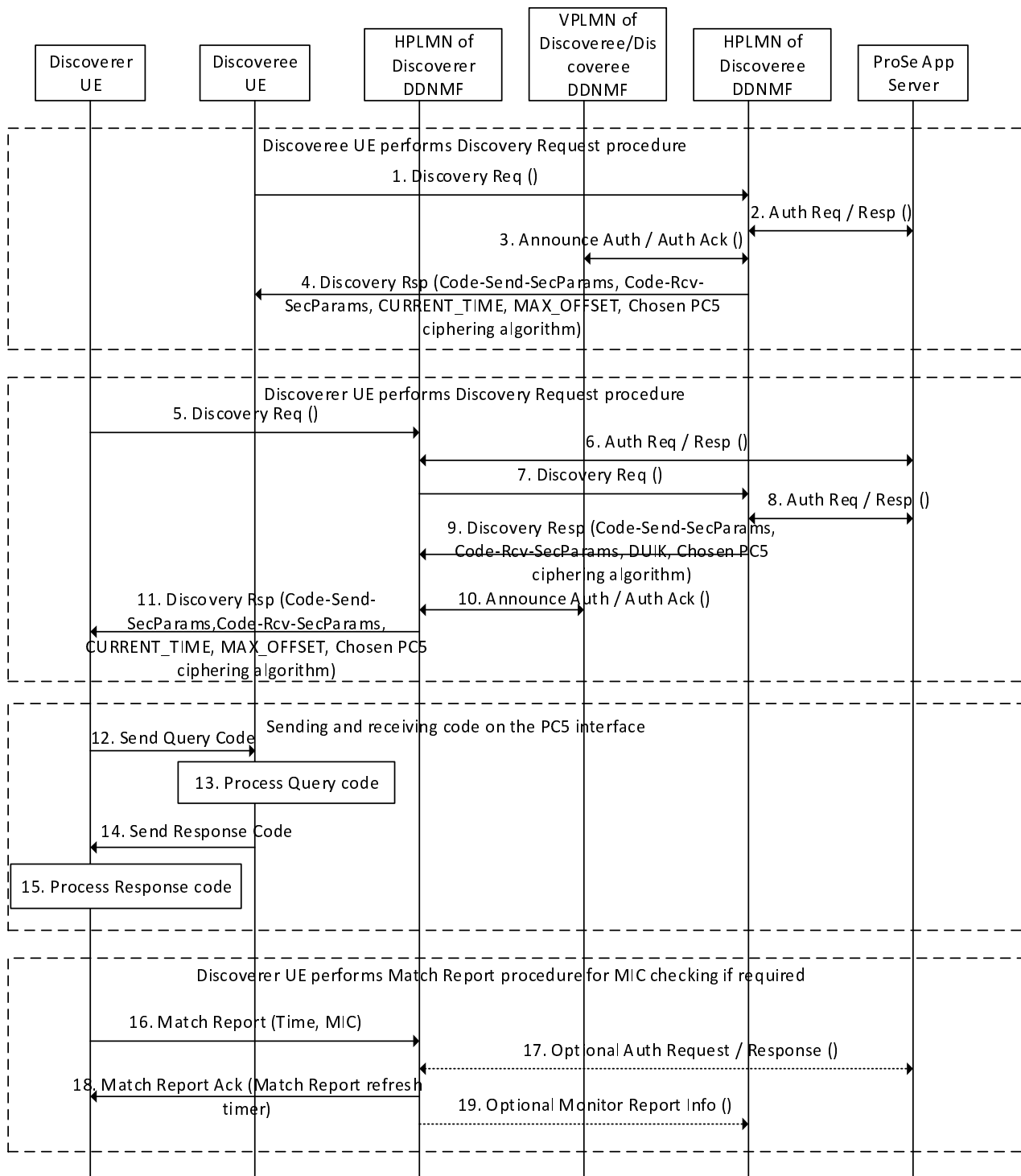


Figure 6.1.3.2.2-1: Security procedure for restricted 5G ProSe Direct Discovery Model B

NOTE 1: When the user-plane based security procedure for the UE-to-Network Relay is used, the 5G PKMF takes the role of the 5G DDNMF as described in 6.3.3.2 of the present document.

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. In addition, the Discoveree UE shall include its PC5 UE security capability that contains the list of supported ciphering algorithms by the UE in the Discovery Request message.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe UE-to-Network Relay plays the role of the Discoveree UE and sends a Relay Discovery Key Request instead of a Discovery Request. The Relay Discovery Key Request message includes the Relay Service Code (RSC) and the 5G ProSe UE-to-Network Relay's PC5 security capabilities.

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

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.

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), Code-Receiving Security Parameters corresponding to each discovery filter along with the CURRENT_TIME and MAX_OFFSET parameters and the chosen PC5 ciphering algorithm. 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 clause 6.1.3.1 of the present document. The 5G DDNMF in the HPLMN of the Discoveree UE shall include the chosen PC5 ciphering algorithm in the Discovery Response message. The 5G DDNMF determines the chosen PC5 ciphering algorithm based on the ProSe Response Code and the received PC5 UE security capability in step 1. The UE stores the chosen PC5 ciphering algorithm together with the ProSe Response Code.

In addition, the 5G DDNMF in the HPLMN of the Discoveree UE may associate the ProSe Response Code with the PC5 security policies and include the PC5 security policies in the Discovery Response message.

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Discovery Response, and the RSC is used instead of ProSe Query Code and ProSe Response Code. The response message contains the discovery security materials.

NOTE 2: 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 and its PC5 UE security capability to the 5G DDNMF in its HPLMN in order to be allowed to discover one or more Restricted ProSe Application User IDs.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe Remote UE plays the role of the Discoverer UE and sends a Relay Discovery Key Request instead of the Discovery Request. The Relay Discovery Key Request message includes the RSC and the 5G ProSe Remote UE's PC5 security capabilities.

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.

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.

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 including the PC5 UE security capability in step 5.

For 5G ProSe UE-to-Network Relay Discovery, Relay Discovery Key Request and RSC are used instead of Discovery Request and RPAUID.

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

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.

9. If the PC5 UE security capability in step 5 includes the chosen PC5 ciphering algorithm, 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, an optional Discovery User Integrity Key (DUIK) for the ProSe Response Code, and a chosen PC5 ciphering algorithm. 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 associated with the ProSe Response Code to the 5G DDNMF in the HPLMN of the Discoverer UE.

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Discovery Response, and the RSC is used instead of ProSe Query Code and ProSe Response Code. The response message contains the discovery security materials.

NOTE 3: There are two possible configurations for integrity checking, namely, MIC checked by the 5G DDNMF of the Discoverer UE, and MIC checked at the Discoverer UE side; this is decided by the 5G DDNMF that assigns the ProSe Restricted Code, and signals the Discoverer UE in the Code-Receiving Security Parameters.

NOTE 4: The chosen PC5 ciphering algorithm is associated with the ProSe Response Code.

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, the Code-Sending Security Parameters along with the CURRENT_TIME and MAX_OFFSET parameters and the chosen PC5 ciphering algorithm. The Discoverer UE takes the same actions with CURRENT_TIME and MAX_OFFSET as described for the Monitoring UE in step 9 of clause 6.1.3.1 of the present document. The UE stores the Discovery Response Filter and its Code-Receiving Security Parameters and the ProSe Query Code and its Code-Sending Security Parameters, and the chosen PC5 ciphering algorithm together with the ProSe Response Code.

If the 5G DDNMF in the HPLMN of the Discoverer UE receives the PC5 security policies associated with the ProSe Response Code in step 9, the Discoverer UE's 5G DDNMF forwards the PC5 security policies to the Discoverer UE.

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Discovery Response, and the RSC is used instead of the ProSe Restricted Code. The response message contains the discovery security materials.

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 5: 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 6: 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 7: 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 Application Server to ensure that Discoverer UE is authorized to discover the Discoveree UE.

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.
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 discovery messages over PC5 interface

There are three types of security that are used to protect the restricted 5G ProSe Direct 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]. The protection mechanisms specified in TS 33.303 [4] are reused with the following changes:

- Input parameters to integrity protection algorithm as specified in clause A.6 in the present document.
- Message-specific confidentiality mechanisms as specified in clause A.7 in the present document.
- In A.5 of TS 33.303 [4], the time-hash-bitsequence keystream is set to L least significant bits of the output of the KDF, where L is the bit length of the discovery message to be scrambled and set to Min (the length of discovery message - 16, 256).
- Step 3 of clause 6.1.3.4.3.5 of TS 33.303 [4] becomes:

XOR (0xFFFF || time-hash-bitsequence) with the most significant (L + 16) bits of discovery message.

NOTE 1: 16 is the size of Message Type and UTC-based counter LSB in bit length.

NOTE 2: The maximum length of the discovery message to be scrambled is limited to 256 bits.

- Step 2 of clause 6.1.3.4.3.2 of TS 33.303 [4] becomes:
 - Calculate MIC if a DUIK was provided, otherwise set MIC to a 32-bit random string. Then, set the MIC IE to the MIC.
- Step 4 of clause 6.1.3.4.3.2 of TS 33.303 [4] is not processed.

6.2 Security for unicast mode 5G ProSe Direct Communication

6.2.1 General

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

PC5 security policy provisioning by 5G DDNMF for unicast mode 5G ProSe Direct Communication during the restricted 5G ProSe Discovery procedure is specified in clause 6.1.3.2.

PC5 direct communication security for relay services is specified in clause 6.3.

If the UE receives PC5 security policies from 5G DDNMF as specified in clause 6.1.3.2.2, the UE uses the PC5 security policies from 5G DDNMF to establish PC5 unicast communication security instead of the PC5 security policies provisioned by PCF or pre-configured in UE as defined in TS 23.304 [2].

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 5G ProSe-enabled UEs are out of coverage.

The mutual authentication between two 5G 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

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 5G ProSe Layer-3 UE-to-Network Relay and 5G ProSe Layer-2 UE-to-Network Relay are different and are defined in clause 6.3.3 and clause 6.3.4 respectively.

Editor's note: There are two security options for 5G ProSe Layer-3 UE-to-Network Relay: security procedure over User Plane as defined in clause 6.3.3.2 and security procedure over Control Plane as defined in clause 6.3.3.3. The choice of authentication mechanism will be defined in SA2's specification, and SA3's specification can refer to it later.

The functionality in this clause is supported by both 5G ProSe-enabled UEs for commercial services and public safety.

6.3.2 Security requirements

The following security requirements apply to both 5G ProSe Layer-3 UE-to-Network Relay and 5G ProSe Layer-2 UE-to-Network Relay:

- The 5G System shall support the authorization of the UE as a 5G ProSe UE-to-Network Relay in the 5G ProSe UE-to-Network Relay scenario.
- The 5G System shall support the authorization of the UE as a 5G ProSe Remote UE in the 5G ProSe UE-to-Network Relay scenario.
- For UE-to-Network Relay discovery, the security requirements in clause 6.1.2 apply.
- The 5G System shall support a secure means to establish a PC5 link between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.
- The 5G System shall support confidentiality protection, integrity protection and replay protection for secure communication between the 5G ProSe Remote UE and the network via 5G ProSe UE-to-Network Relays.
- PC5 signalling integrity security policy is set to "REQUIRED" for the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.
- The 5G ProSe Remote UE shall establish a different PC5 security context with each different 5G ProSe UE-to-Network Relay and for each different Relay Service Code. It shall also be possible to establish a PC5 security context when the 5G ProSe Remote UE is out of coverage.

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 procedures can be used for 5G ProSe 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 ProSe authentication for PC5 key establishment.

The following are the security requirements for 5G ProSe Layer-3 UE-to-Network Relay communication:

- For 5G ProSe Layer-3 UE-to-Network Relay security established over control plane, the PCF shall be able to provision the PC5 security policies to the 5G ProSe Remote UE and the UE-to-Network Relay respectively per 5G ProSe UE-to-Network Relay service, during service authorization and information provisioning procedure as defined in TS 23.304 [2].
- For 5G ProSe Layer-3 UE-to-Network Relay security established over user plane, the 5G PKMF shall be able to provision the PC5 security policies to the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay respectively per 5G ProSe UE-to-Network Relay service, during security materials provisioning procedure defined in clause 6.3.3.2.
- The PC5 UP security policies for protecting 5G ProSe UE-to-Network Relay communication shall be configured per 5G ProSe UE-to-Network Relay service based on the security requirements of the specific relay service.
- The activation of PC5 signalling security shall be based on PC5 CP security policies of the specific 5G ProSe UE-to-Network Relay service.
- The activation of PC5 user plane security shall be based on PC5 UP security policies of the specific 5G ProSe UE-to-Network Relay service.

- 5G PKMF shall be configured with the PC5 security policies associated with each 5G ProSe Layer-3 UE-to-Network Relay service.

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 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay. The mechanism includes how a 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay get authorized by the 5G ProSe Key Management Function (5G PKMF) and verify each other's roles.

6.3.3.2.2 5G ProSe Remote UE attaching to a 5G ProSe UE-to-Network Relay

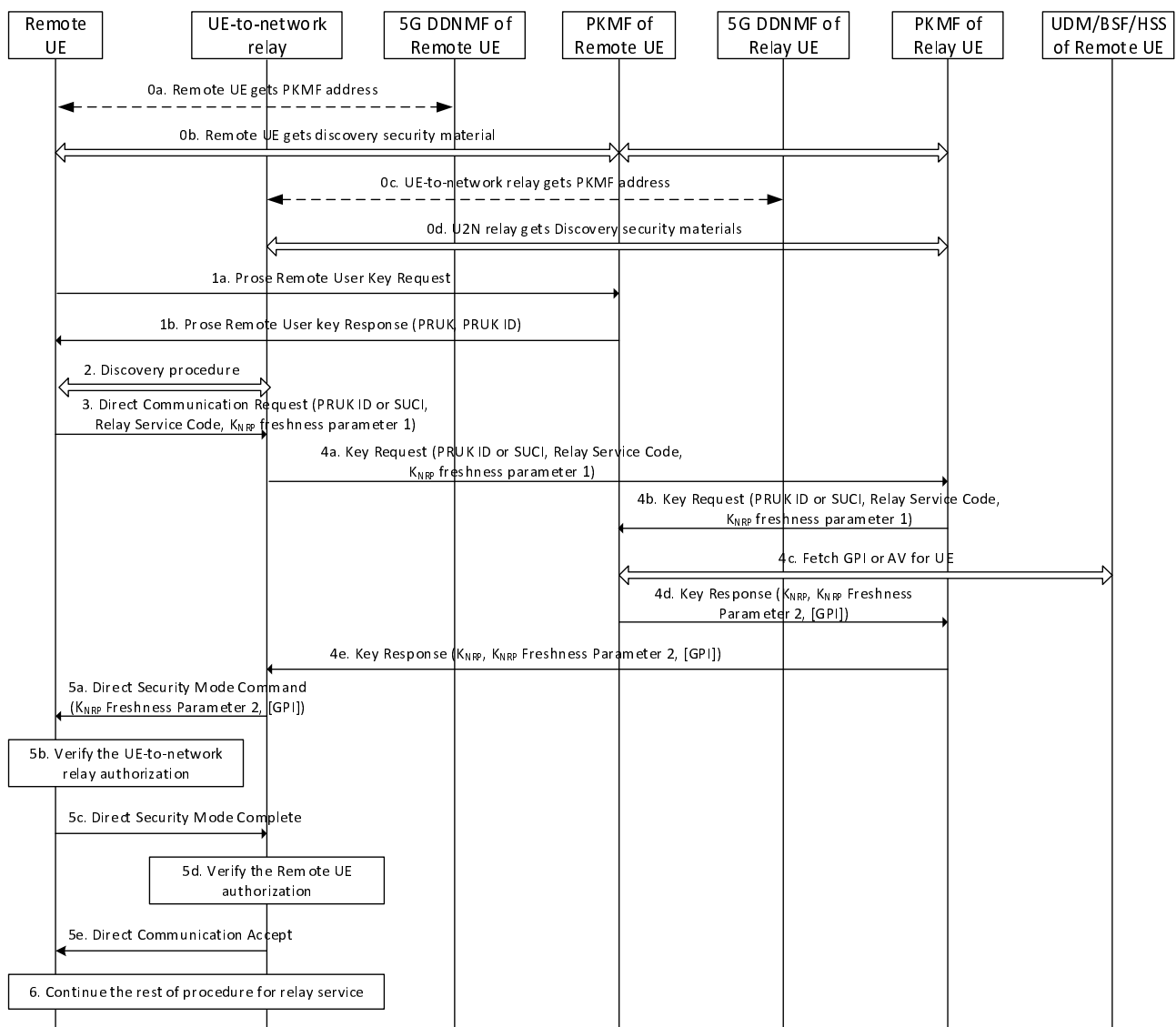


Figure 6.3.3.2.2-1: Authorization and secure PC5 link establishment procedure for 5G ProSe UE-to-Network Relay

The 5G ProSe 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 5G ProSe Remote UE needs to connect to the 5G PKMF and obtain fresh ones to use the 5G ProSe UE-to-Network Relay services.

NOTE 1: The procedure is described for the scenario that the 5G PKMF of the 5G ProSe Remote UE is different from the 5G PKMF of the 5G ProSe UE-to-Network Relay. If both the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay are served by a single 5G PKMF, the 5G PKMF takes the role of the 5G PKMF of the 5G ProSe Remote UE and the 5G PKMF of the 5G ProSe UE-to-Network Relay and the inter-5G PKMF message exchanges are not needed.

NOTE 2: Steps 0a, 0b, 1a, 1b are performed when the 5G ProSe Remote UE is in coverage.

- 0a. The 5G ProSe Remote UE gets the 5G PKMF address from the 5G DDNMF of its HPLMN. Alternatively, the 5G ProSe Remote UE may be provisioned with the 5G PKMF address by PCF. If the 5G ProSe Remote UE is provisioned with the 5G PKMF address, the 5G ProSe Remote UE may access the 5G PKMF directly without requesting it from the 5G DDNMF. In case that the 5G ProSe Remote UE cannot access the 5G PKMF using the provisioned 5G PKMF address, the 5G ProSe Remote UE may request the 5G PKMF address to the 5G DDNMF.
- 0b. The 5G ProSe Remote UE shall establish a secure connection with the 5G PKMF via PC8 reference point. Security for PC8 interface relies on Ua security if GBA specified in TS 33.220 [8] is used (see clause 5.2.3.4) or Ua* security if AKMA specified in TS 33.535 [5] is used (see clause 5.2.5.4). The 5G PKMF of the 5G ProSe Remote UE shall check whether the 5G ProSe Remote UE is authorized to receive UE-to-Network Relay service, and if the UE is authorized, the 5G PKMF of the 5G ProSe Remote UE provides the discovery security materials to the 5G ProSe Remote UE. If the 5G ProSe Remote UE provides a list of visited networks, the 5G PKMF of the 5G ProSe Remote UE shall request the discovery security materials from the 5G PKMFs of the potential 5G ProSe UE-to-Network Relays from which the 5G ProSe Remote UE gets the relay services. The 5G PKMF of the 5G ProSe UE-to-Network Relay may include the PC5 security policies to the 5G ProSe Remote UE.

NOTE 3: The 5G PKMF may be locally configured with the UE's authorization information. Otherwise, the 5G PKMF interacts with the UDM of the UE to retrieve the UE's authorization information.

NOTE 4: The 5G ProSe Remote UE is provisioned by PCF with a list of the potential visited networks for the 5G ProSe UE-to-Network Relay service (which is identified by RSC).

- 0c. The 5G ProSe UE-to-Network Relay gets the 5G PKMF address from its HPLMN in the same way as described in step 0a.
- 0d. The 5G ProSe UE-to-Network Relay shall establish a secure connection with the 5G PKMF via PC8 reference point as in step 0b. The 5G PKMF of the 5G ProSe UE-to-Network Relay shall check whether the 5G ProSe UE-to-Network Relay is authorized to provide 5G ProSe UE-to-Network Relay service, and if the UE is authorized, the 5G PKMF of the 5G ProSe UE-to-Network Relay provides the discovery security materials to the 5G ProSe UE-to-Network Relay. The 5G PKMF of the 5G ProSe UE-to-Network Relay may include the PC5 security policies to the 5G ProSe UE-to-Network Relay.
- 1a. The 5G ProSe Remote UE sends a PRUK Request message to its 5G PKMF. The message indicates that the 5G ProSe Remote UE is requesting a PRUK from the 5G PKMF. If the 5G ProSe Remote UE already has a PRUK from this 5G PKMF, the message shall also contain the PRUK ID of the PRUK.
- PRUK ID shall take the form of either the NAI format or the 64-bit string. If the PRUK ID is in NAI format, i.e. username@realm, the realm part shall include Home Network Identifier (i.e. HPLMN ID).
- 1b. The 5G PKMF checks whether the 5G ProSe Remote UE is authorized to receive UE-to-Network Relay services. This is done by using the 5G ProSe Remote UE's identity associated with the key used to establish the secure connection between the 5G ProSe Remote UE and 5G PKMF in step 0b. If the 5G ProSe Remote UE is authorized to receive the service, the 5G PKMF sends a PRUK and PRUK ID to the 5G ProSe Remote UE. If a PRUK and PRUK ID are included, the 5G ProSe Remote UE shall store these and delete any previously stored ones for this 5G PKMF.
2. The discovery procedure is performed between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay using the discovery parameters and discovery security material as described in clause 6.1.3.2.

3. The 5G ProSe Remote UE sends a Direct Communication Request (DCR) that contains the PRUK ID or a SUCI if the Remote UE does not have a valid PRUK, Relay Service Code (RSC) of the 5G ProSe UE-to-Network Relay service and K_{NRP} freshness parameter 1 to the 5G ProSe UE-to-Network Relay. If the PRUK ID is not in NAI format, the DCR message shall include the HPLMN ID of the 5G ProSe Remote UE. The PC5 security establishment procedure between the 5G ProSe Remote UE and the 5G ProSe 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 5G ProSe Layer-3 UE-to-Network Relay scenario are described in this clause. The privacy and integrity protection of DCR are described in clause 6.3.5.
- 4a. The 5G ProSe UE-to-Network Relay sends a Key Request message that contains PRUK ID or SUCI, RSC and K_{NRP} freshness parameter 1 to its 5G PKMF. The Key Request message shall also include the HPLMN ID of the 5G ProSe Remote UE if it is included in the DCR.
- 4b. On receiving the Key Request message, the 5G PKMF of the 5G ProSe UE-to-Network Relay shall check if the 5G ProSe UE-to-Network Relay is authorized to provide relay service to the 5G ProSe Remote UE based on the 5G ProSe UE-to-Network Relay's identity associated with the key used to establish the secure PC8 connection and the received RSC. If the 5G ProSe UE-to-Network Relay's authorization information is not locally available, the 5G PKMF shall request the authorization information from the UDM of the 5G ProSe UE-to-Network Relay (not shown in the figure) using Nudm_SDM_Get service as described in TS 23.502 [13]. If the 5G ProSe UE-to-Network Relay is authorized to provide the relay service based on ProSe Subscription data as specified in TS 23.502 [10], the 5G PKMF of the 5G ProSe UE-to-Network Relay sends the Key Request with the PRUK ID or the SUCI to the 5G PKMF of the 5G ProSe Remote UE. The 5G PKMF of the 5G ProSe UE-to-Network Relay identifies the 5G PKMF address of the 5G ProSe Remote UE based on the PRUK ID or HPLMN ID or SUCI of the 5G ProSe Remote UE if it is included in the Key Request message.
- 4c. On receiving the Key Request message from the 5G PKMF of the 5G ProSe UE-to-Network Relay, the 5G PKMF of the 5G ProSe Remote UE shall check if the 5G ProSe Remote UE is authorized to use the relay service. The relay service authorization check shall be based on the PRUK ID and RSC included in the Key Request message or the SUPI of the Remote UE and the RSC included in the Key Request message. If a SUCI is included in the Key Request message, the 5G PKMF of the 5G ProSe Remote UE shall request the UDM of the 5G ProSe Remote UE to de-conceal the SUCI to gain the SUPI using Nudm_UEIdentifier_Deconceal service, and the UDM invokes SIDF to de-conceal SUCI to gain SUPI. If the 5G ProSe Remote UE's authorization information is not locally available, the 5G PKMF shall request the authorization information from the UDM of the 5G ProSe Remote UE (not shown in figure 6.3.3.2.2-1).

NOTE 5: Privacy issues need to be considered while determining whether the SUPI is to be sent to the PKMF. For a privacy control, the UDM can authorize the PKMF based on its NF type or the service provider domain.

If a new PRUK is required, the 5G PKMF shall perform the one of the following procedures (as shown in the step 4c in figure 6.3.3.2.2-1):

- If the 5G PKMF of the 5G ProSe Remote UE supports the Zpn interface to the BSF of the 5G ProSe Remote UE, the 5G PKMF of the 5G ProSe Remote UE may request a GBA Push Info (GPI - see TS 33.223 [9]) for the 5G ProSe Remote UE from the BSF. When requesting the GPI, the 5G PKMF shall include a PRUK ID in the P-TID field. On receiving the GPI, the 5G PKMF shall use $Ks_(\text{ext})_NAF$ as the PRUK.
- If the 5G PKMF of the 5G ProSe Remote UE supports the SBI interface to the BSF of the 5G ProSe Remote UE, the 5G PKMF may request the GPI via SBI interface as described in TS 33.223 [9]. On receiving the GPI, the 5G PKMF shall use $Ks_(\text{ext})_NAF$ as the PRUK.
- If the 5G PKMF of the 5G ProSe Remote UE supports the PC4a interface to the HSS of the UE, then the 5G PKMF of 5G ProSe Remote UE may request a GBA Authentication Vector (AV) for the 5G ProSe Remote UE from the HSS. On receiving the AV, the 5G PKMF locally forms the GPI including a PRUK ID in the P-TID field. The 5G PKMF shall use $Ks_(\text{ext})_NAF$ as the PRUK.
- If the 5G PKMF of the 5G ProSe Remote UE is co-located or integrated with BSF functionality and supports the SBI interface to the UDM/HSS of the 5G ProSe Remote UE, the 5G PKMF may request the GBA AV via SBI interface as described in TS 33.220 [8]. On receiving the AV, the 5G PKMF locally forms the GPI including a PRUK ID in the P-TID field. The 5G PKMF shall use $Ks_(\text{ext})_NAF$ as the PRUK.

NOTE 6: GPI is supported only when GBA is used.

- 4d. The 5G PKMF of the 5G ProSe Remote UE shall generate K_{NRP} freshness parameter 2 and derive K_{NRP} using the PRUK identified by PRUK ID, RSC, K_{NRP} freshness parameter 1 and K_{NRP} freshness parameter 2 as specified in A.8. Then, the 5G PKMF of the 5G ProSe Remote UE sends a Key Response message that contains K_{NRP} and K_{NRP} freshness parameter 2 to the 5G PKMF of the 5G ProSe UE-to-Network Relay. This message shall include GPI if generated. The 5G PKMF of the 5G ProSe Remote UE shall also include the Remote User ID of the 5G ProSe Remote UE in the Key Response message to the 5G ProSe UE-to-Network Relay. PRUK ID is used as a 5G ProSe Remote UE ID in the present document.
- 4e. The 5G PKMF of the 5G ProSe UE-to-Network Relay sends the Key Response message to the 5G ProSe UE-to-Network Relay, which includes Remote User ID, K_{NRP} , K_{NRP} freshness parameter 2, the PC5 security policies of the relay service, the GPI if used to calculate a fresh PRUK to the UE-to-Network Relay.
- 5a. The 5G ProSe UE-to-Network Relay shall derive the session key ($K_{\text{NRP-SESS}}$) from K_{NRP} and then derive the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies as specified in TS 33.536 [6]. The 5G ProSe UE-to-Network Relay shall store the Remote User ID received in step 4d. The 5G ProSe UE-to-Network Relay sends a Direct Security Mode Command message to the 5G ProSe Remote UE. This message shall also include the K_{NRP} Freshness Parameter 2 in addition to the parameters specified in TS 33.536 [6] and shall be protected as specified in TS 33.536 [6].
- 5b. If the 5G ProSe Remote UE receives the message containing the GPI, it processes the GPI as described in TS 33.223 [9]. The 5G ProSe Remote UE shall derive the PRUK and obtain the PRUK ID from the GPI.

The 5G ProSe Remote UE shall derive K_{NRP} from its PRUK, RSC, K_{NRP} Freshness Parameter 1 and the received K_{NRP} Freshness Parameter 2 as specified in A.8. It shall then derive the session key ($K_{\text{NRP-SESS}}$) and the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies in the same manner as the 5G ProSe UE-to-Network Relay and process the Direct Security Mode Command. Successful verification of the Direct Security Mode Command assures the 5G ProSe Remote UE that the 5G ProSe UE-to-Network Relay is authorized to provide the relay service.

Handling of synchronization failure (for details of synchronization failures - see TS 33.102 [11]) when UE processes the authentication challenge in the GPI is performed similarly to clause 6.7.3.2.1.2 in TS 33.303 [4]. The 5G ProSe Remote UE shall send Direct Security Mode Failure message and include RAND and AUTS in the message. The 5G ProSe UE-to-Network Relay shall send the key request message to the 5G PKMF of the 5G ProSe Remote UE via the 5G PKMF of the 5G ProSe UE-to-Network Relay upon receiving the Direct Security Mode Failure message from the 5G ProSe Remote UE. The key request message shall include the HPLMN ID of the 5G ProSe Remote UE, Relay Service Code and K_{NRP} freshness parameter 1 together with the RAND and the AUTS received from the 5G ProSe Remote UE. If the 5G PKMF of the 5G ProSe Remote UE decides to retry GBA Push procedure, the 5G PKMF of the 5G ProSe Remote UE shall request GPI as described in step 4c.

- 5c. The 5G ProSe Remote UE responds with a Direct Security Mode Complete message to the 5G ProSe UE-to-Network Relay as specified in TS 33.536 [6].
- 5d. On receiving the Direct Security Mode Complete message, the 5G ProSe UE-to-Network Relay shall verify the Direct Security Mode Complete message. Successful verification of the Direct Security Mode Complete message assures the 5G ProSe UE-to-Network Relay that the 5G ProSe Remote UE is authorized to get the relay service.
- 5e. After successful verification, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to complete the PC5 connection establishment procedure.
6. The 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay continues the rest of procedure for the relay service over the secure PC5 link such as establishing a new PDU session or modifying an existing PDU session for relaying, if needed etc.

When the 5G ProSe Layer-3 UE-to-Network Relay sends a Remote UE Report to the SMF as specified in TS 23.304 [2], the 5G ProSe Layer-3 UE-to-Network Relay shall include Remote User ID received in step 4d.

6.3.3.2.3 PC5 Key Hierarchy over User Plane

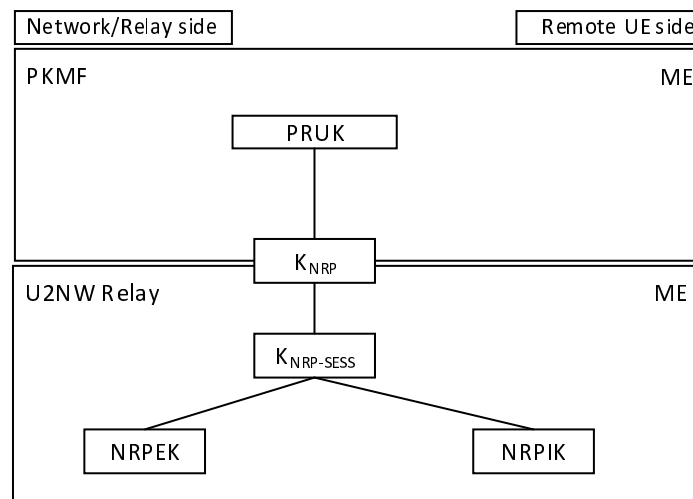


Figure 6.3.3.2.3-1: PC5 Key Hierarchy for 5G ProSe UE-to-Network Relay security over User Plane

The different layers of keys (see figure 6.3.3.2.3-1) are the following:

- PRUK: The root key of the PC5 unicast link.
- K_{NRP} : The key is equivalent to K_{NRP} as specified in TS 33.536 [6]. This key is derived as specified in clause A.8.
- $K_{NRP-SESS}$: This key is derived as specified in TS 33.536 [6].
- NRPEK, NRPIK: These keys are derived as specified in TS 33.536 [6].

6.3.3.3 Security procedure over Control Plane

6.3.3.3.1 General

This clause describes the security mechanisms for the 5G ProSe Layer-3 UE-to-Network Relay authentication, authorization and key management using the 5G ProSe Remote UE specific authentication for PC5 keys establishment. Network entities AMF, AUSF and UDM are involved for key derivation and distribution of keys used for 5G ProSe 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 clause 4.2.2 of TS 23.503 [7]. PCF shall provision the authorization policy and parameters for 5G ProSe UE-to-Network Relay discovery and communication as specified in clause 5.1.4 of TS 23.304 [2].

6.3.3.3.2 Connection with 5G ProSe UE-to-Network Relay connection with setup of network Prose security context during PC5 link establishment

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

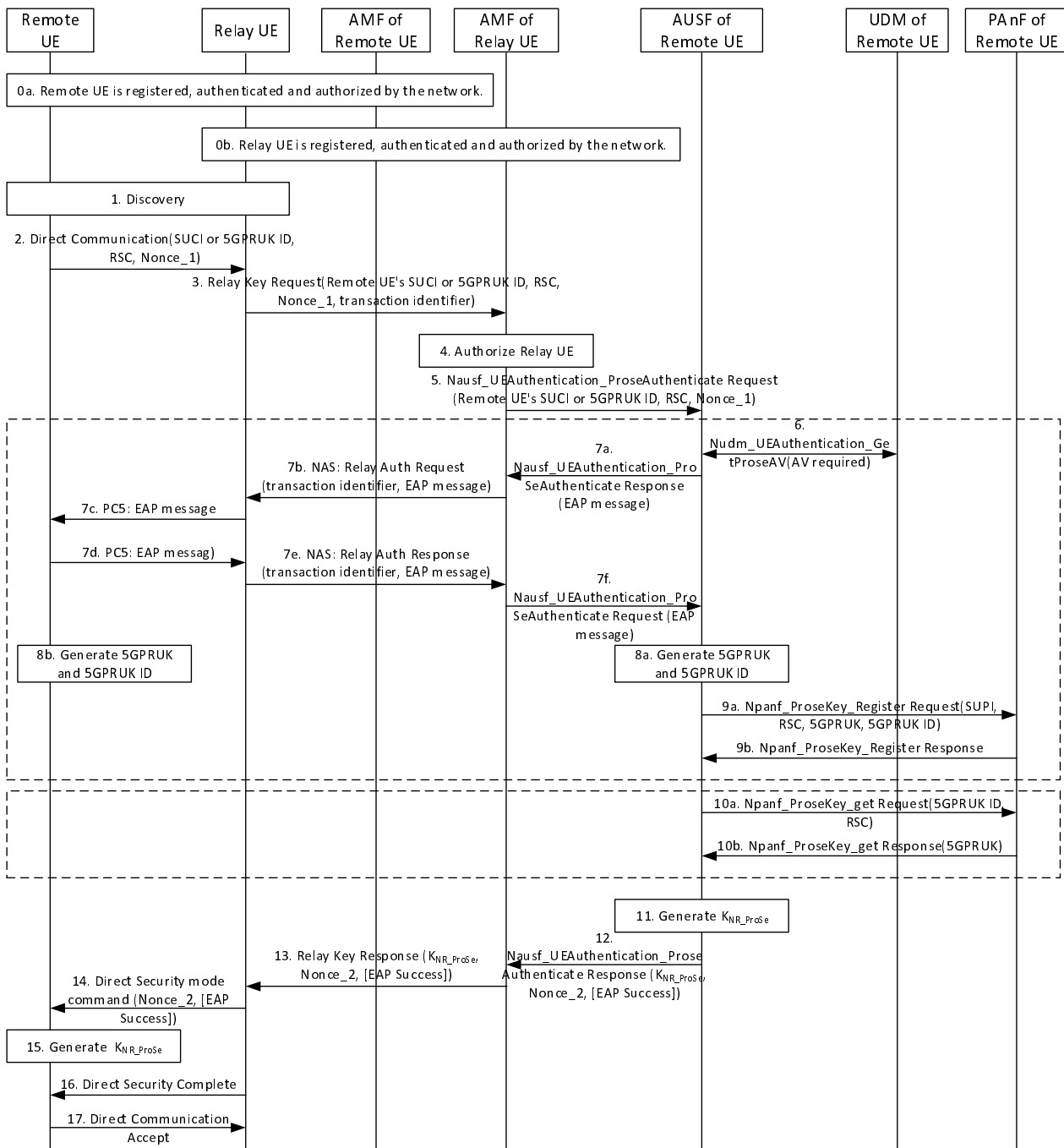


Figure 6.3.3.2-1: 5G ProSe UE-to-Network Relay security procedure with setup of network Prose security context during PC5 link establishment

0. The 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay shall be registered with the network. The 5G ProSe UE-to-Network Relay shall be authenticated and authorized by the network to provide UE-to-Network Relay service. The 5G ProSe Remote UE shall be authenticated and authorized by the network to receive UE-to-Network Relay service. PC5 security policies are provisioned to the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay respectively during this authorization and information provisioning procedure.
1. The 5G ProSe 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. After the discovery of the 5G ProSe UE-to-Network Relay, the 5G ProSe Remote UE shall send a Direct Communication Request to the 5G ProSe UE-to-Network Relay for establishing secure PC5 unicast link. The 5G ProSe Remote UE shall include its security capabilities and PC5 signalling security policy in the DCR message as specified in TS 33.536 [6]. The message shall also include Relay Service Code, Nonce_1.

If the 5G ProSe Remote UE does not have a valid 5G ProSe Remote User Key (5GPRUK), the 5G ProSe Remote UE shall include SUCI in the DCR to trigger 5G ProSe Remote UE specific authentication and establish a 5GPRUK.

If the 5G ProSe Remote UE already has a valid 5GPRUK, the 5G ProSe Remote UE shall include the 5GPRUK ID in the DCR to indicate that the 5G ProSe Remote UE wants to get relay connectivity using the 5GPRUK.

3. Upon receiving the DCR message, the 5G ProSe UE-to-Network Relay shall send the Relay Key Request to the AMF of the 5G ProSe UE-to-Network Relay, including SUCI or 5GPRUK ID, RSC and Nonce_1 received in the DCR message. The 5G ProSe UE-to-Network Relay shall also include in the message a transaction identifier that identifies the 5G ProSe Remote UE for the subsequent messages over 5G ProSe UE-to-Network Relay's NAS messages.
4. The AMF of the 5G ProSe UE-to-Network Relay shall verify whether the 5G ProSe UE-to-Network Relay is authorized to provide the UE-to-Network Relay service.
5. The AMF of the 5G ProSe UE-to-Network Relay shall select an AUSF based on SUCI or 5GPRUK ID and forward the parameters received in Relay Key Request to the AUSF in Nausf_UEAuthentication_ProseAuthenticate Request message. The Nausf_UEAuthentication_ProseAuthenticate Request message shall contain the 5G ProSe Remote UE's SUCI or 5GPRUK ID, Relay Service Code, Nonce_1. If 5GPRUK ID is received from AMF of the 5G ProSe UE-to-Network Relay, the AUSF of the 5G ProSe Remote UE skips steps 6-9. If the 5G ProSe Remote UE's SUCI is received from AMF of the 5G ProSe UE-to-Network Relay, the AUSF of the 5G ProSe Remote UE skips step 10.
6. The AUSF shall initiate a 5G ProSe Remote UE specific authentication using the ProSe specific parameters received (i.e. RSC, etc.). The serving network name handling is the same as defined in TS 33.501 [3].

The AUSF of the 5G ProSe Remote UE shall retrieve the Authentication Vectors and the Routing Indicator of the 5G ProSe Remote UE from the UDM via Nudm_UEAuthentication_GetProseAv Request message. Upon reception of the Nudm_UEAuthentication_GetProseAv Request, the UDM shall invoke SIDF de-conceal SUCI to gain SUPI before UDM can process the request. The UDM checks whether the UE is authorized to use a ProSe UE-to-Network Relay service based on authorization information in UE's Subscription data. If the UE is authorized, the UDM shall choose the authentication method based on SUPI.

- 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE shall trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message defined in clause 6.1.3.1 of TS 33.501 [3] and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProseAuthenticate Response message.
- 7b. The AMF of the 5G ProSe UE-to-Network Relay shall forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.
- 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay shall forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102 [11].

For EAP-AKA', the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. The ME shall derive CK' and IK' according to clause A.3 in TS 33.501 [3].

- 7d. The 5G ProSe Remote UE shall return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.
- 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.
- 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProseAuthenticate Request.

The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information as described in TS 33.501 [3].

For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response/AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay and the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE shall derive the K_{AUSF_P} in the same way as K_{AUSF} is derived in TS 33.501 [3].

8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE shall generate 5GPRUK as specified in clause A.2 and 5GPRUK ID.

The 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542 [14], i.e. username@realm. The username part includes the Routing Indicator from step 6 and the 5GPRUK ID*, and the realm part includes Home Network Identifier. The 5GPRUK ID* is specified in clause A.3.

- 9a. The AUSF of the 5G ProSe Remote UE shall select the PAnF (Prose Anchor Function) based on 5GPRUK ID and send the SUPI, RSC, 5GPRUK and 5GPRUK ID in Npanf_ProseKey_Register Request message to the PAnF.
- 9b. The PAnF shall store the Prose context info (i.e. SUPI, RSC, 5GPRUK, 5GPRUK ID) for the 5G ProSe Remote UE and send Npanf_ProseKey_Register Response message to the AUSF.
- 10a. The AUSF of the 5G ProSe Remote UE shall select the PAnF based on 5GPRUK ID and send received 5GPRUK ID and RSC in Npanf_ProseKey_get Request message.
- 10b. The PAnF retrieves 5GPRUK based on the 5GPRUK ID and checks whether the 5G ProSe Remote UE is authorized to use the UE-to-Network Relay service based on received RSC. If the 5G ProSe Remote UE is authorized and the retrieved 5GPRUK is valid, the PAnF sends Npanf_ProseKey_get Response message with 5GPRUK to the AUSF.
11. The AUSF of the 5G ProSe Remote UE shall generate Nonce_2 and derive the K_{NR_ProSe} key using 5GPRUK, Nonce_1 and Nonce_2 as defined in clause A.4.
12. The AUSF of the 5G ProSe Remote UE shall send the K_{NR_ProSe} , Nonce_2 in Nausf_UEAuthentication_ProseAuthenticate Response message to the 5G ProSe UE-to-Network Relay via the AMF of the 5G ProSe UE-to-Network Relay. EAP Success message shall be included if step 7 is performed successfully. The AUSF of the 5G ProSe Remote UE shall also include the 5GPRUK ID in the message if generated in step 8.
13. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE via the AMF of the 5G ProSe UE-to-Network Relay, the 5G ProSe UE-to-Network Relay derives PC5 session key K_{relay_sess} and confidentiality key K_{relay_enc} (if applicable) and integrity key K_{relay_int} from K_{NR_ProSe} , as defined in clause 6.3.3.3.3 of the present document. K_{NR_ProSe} ID and K_{relay_sess} ID are established in the same way as K_{NRP} ID and K_{NRP_sess} ID in TS 33.536 [6]. The EAP Success message and 5GPRUK ID are also sent from the AMF of the 5G ProSe UE-to-Network Relay to UE-to-Network Relay if received from AUSF.
14. The 5G ProSe UE-to-Network Relay shall send the received Nonce_2 and 5G ProSe Remote UE's PC5 signalling security policy to the 5G ProSe Remote UE in Direct Security mode command message, which is integrity protected using K_{relay_int} . EAP Success message shall be included if received from the AMF of the 5G ProSe UE-to-Network Relay.
15. The 5G ProSe Remote UE shall generate the K_{NR_ProSe} key to be used for remote access via the 5G ProSe UE-to-Network Relay in the same way as defined in step 11. The 5G ProSe Remote UE shall derive PC5 session key K_{relay_sess} and confidentiality and integrity keys from K_{NR_ProSe} in the same way as defined in step 13.
16. The 5G ProSe Remote UE shall send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by K_{relay_int} or/and K_{relay_enc} derived from K_{relay_sess} according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

17. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures and store the 5GPRUK ID in the security context associated to the PC5 link with the 5G ProSe Remote UE.

Further communication between the 5G ProSe Remote UE and the Network takes place securely via the 5G ProSe UE-to-Network Relay.

6.3.3.3.3 PC5 Key Hierarchy over Control Plane

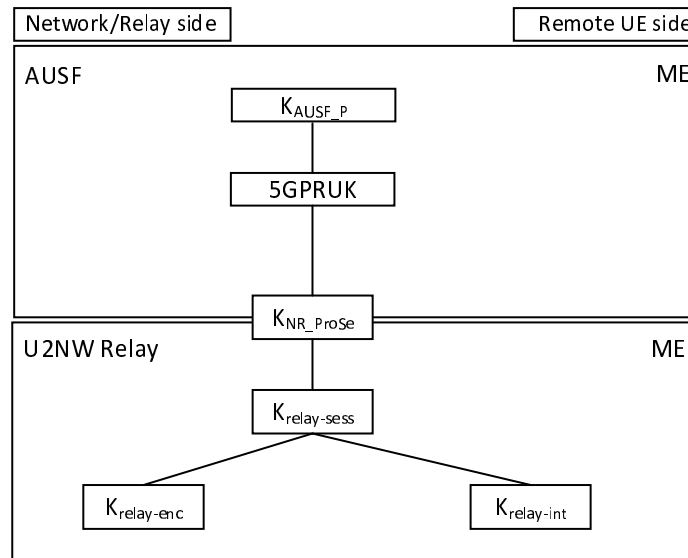


Figure 6.3.3.3.3-1: PC5 Key Hierarchy for 5G ProSe UE-to-Network Relay security over Control Plane

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

- K_{AUSF_P} : A key derived based on 5G ProSe Remote UE specific authentication, only used to derive 5GPRUK.
- 5GPRUK: The root credential derived from K_{AUSF_P} that is the root of security of the PC5 unicast link used for 5G ProSe UE-to-Network Relay service.
- K_{NR_ProSe} : This is a 256-bit root key that is established between the two entities that communicating using NR PC5 unicast link.
- $K_{relay-sess}$: This is the 256-bit key that is derived by UE from K_{NR_ProSe} and is used derive keys that to protect the transfer of data between the UEs. The $K_{relay-sess}$ is derived per unicast link same as $K_{NRP-sess}$ specified in TS 33.536 [6]. During activated unicast communication session between the UEs, the $K_{relay-sess}$ may be refreshed by running the rekeying procedure. The keys for confidentiality and integrity algorithms are derived directly from $K_{relay-sess}$. The 16-bit $K_{relay-sess}$ ID identifies the $K_{relay-sess}$.
- $K_{relay-int}$, $K_{relay-enc}$: The $K_{relay-int}$ and $K_{relay-enc}$ 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 $K_{relay-sess}$ and are refreshed automatically every time $K_{relay-sess}$ is changed.

6.3.3.3.4 5G ProSe Remote UE Secondary Authentication via a 5G ProSe Layer-3 UE-to-Network Relay without N3IWF

6.3.3.3.4.1 General

This clause specifies the 5G ProSe Remote UE specific secondary authentication between a 5G ProSe Remote UE, which is different from the secondary authentication defined in TS 33.501 [3], via a 5G ProSe Layer-3 UE-to-Network Relay without N3IWF and an external Data Network (DN) based on network-controlled authorization (i.e. using 5G ProSe Remote UE specific authentication) as described in clause 6.3.3.3.2. This procedure is optional to support.

The SMF of the 5G ProSe UE-to-Network Relay triggers the secondary authentication of the 5G ProSe Remote UE based on the subscription information and the local configuration of the SMF when it receives a NAS message (e.g. Remote UE Report) from the 5G ProSe UE-to-Network Relay.

The EAP framework specified in IETF RFC 3748 [12] shall be used for authentication between the 5G ProSe Remote UE and a DN-AAA server in the external data network.

Following clause describes the procedures for initial secondary authentication of the 5G ProSe Remote UE with the external DN-AAA server.

6.3.3.3.4.2 PDU Session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay

The PDU session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay follows the steps described in figure 6.3.3.3.4.2-1.

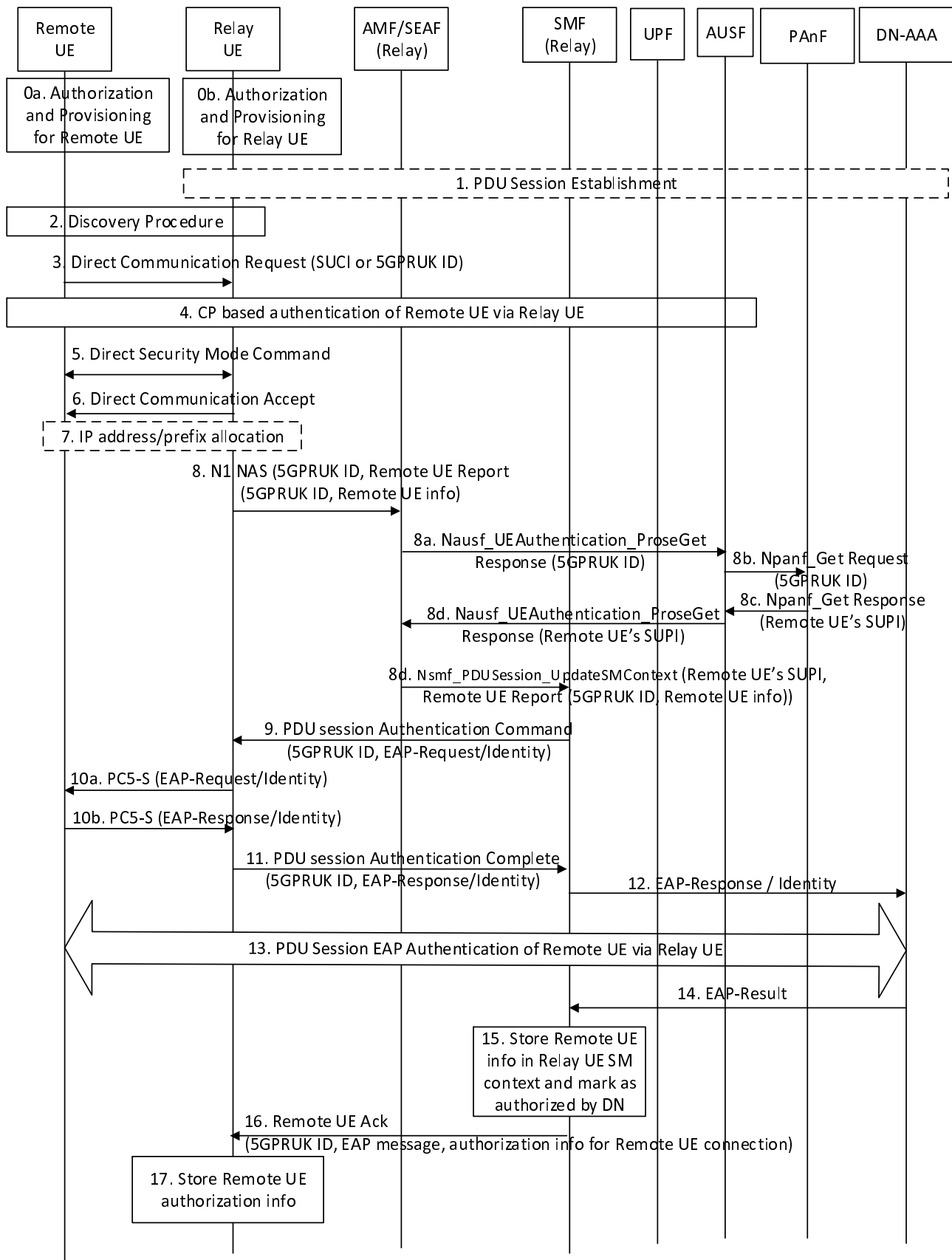


Figure 6.3.3.4.2-1: Procedure for PDU session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay

- 0. During the Registration procedure, authorization and provisioning are performed for 5G ProSe Remote UE(0a) and 5G ProSe Layer-3 UE-to-Network Relay(0b) as described in clause 5.1.4 of TS 23.304 [2].

1. The 5G ProSe Layer-3 UE-to-Network Relay may establish a PDU session for relaying with default PDU session parameters as described in clause 6.5.1.1 in TS 23.304 [2].
2. Based on the authorization and provisioning in step 0, the 5G ProSe Remote UE performs the discovery of a 5G ProSe Layer-3 UE-to-Network Relay. As part of the discovery procedure, the 5G ProSe Remote UE learns about the connectivity service the 5G ProSe Layer-3 UE-to-Network Relay provides (e.g. based on a broadcasted service code) as described in clause 6.3.1.2 or 6.3.1.3 of TS 23.304 [2].
3. The 5G ProSe Remote UE selects a 5G ProSe Layer-3 UE-to-Network Relay sends a DCR (Direct Communication Request) message including its SUCI or a 5GPRUK ID as described in clause 6.3.3.3.2.
4. The Remote UE runs CP based authentication as described in 6.3.3.3.2. In addition, the following procedure may happen in this step as described in clause 6.5.1.1 in TS 23.304 [2].

If there is no PDU session satisfying the requirements of the PC5 connection with the 5G ProSe Remote UE, e.g. S-NSSAI, DNN, QoS, UP security activation status, the 5G ProSe Layer-3 UE-to-Network Relay initiates a new PDU session establishment or modification procedure for relaying.

5. Upon successful network-controlled authentication of 5G ProSe Remote UE procedure, the 5G ProSe Layer-3 UE-to-Network Relay initiates a Direct Security Mode Command procedure with the 5G ProSe Remote UE as described in clause 6.2.3.
6. Upon successful security establishment, the 5G ProSe Layer-3 UE-to-Network Relay stores the 5GPRUK ID as described in clause 6.3.3.3.2 and sends a DCA (Direct Communication Accept) message to the Remote UE. The DCA may include an indication that a PDU Session with secondary authentication is pending if the L3 UE-to-Network Relay determines the DN that is associated with the relay service code requires secondary authentication for the 5G ProSe Remote UE based on the fact that the L3 UE-to-Network Relay performed secondary authentication with the same DN either in step 1 or step 4, and there is no stored authentication information associated with the Remote UE. Based on the indication in the DCA message, the 5G ProSe Remote UE may refrain from sending any data traffic over the PC5 link until successful completion of subsequent PDU Session secondary authentication.
7. For IP PDU Session Type and IP traffic over the PC5 reference point, the IPv6 prefix or IPv4 address is allocated for the 5G ProSe Remote UE as defined in clause 5.5.1.3 in TS 23.304 [2]. In addition, the 5G ProSe Layer-3 UE-to-Network 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 authentication.
8. The 5G ProSe Layer-3 UE-to-Network Relay sends a Remote UE Report message to the SMF for the PDU session associated with the 5G ProSe Layer-3 UE-to-Network Relay. The 5G ProSe Layer-3 UE-to-Network Relay shall include the 5GPRUK ID as the Remote User ID and 5G ProSe Remote UE addressing info (e.g. IP or MAC address). The Remote UE Report message includes the 5G ProSe Remote UE info (Remote User ID, addressing info) and excludes other 5G ProSe Remote UEs info. The Relay shall additionally include the 5GPRUK ID in the subsequent NAS messages. The AMF shall select AUSF based on 5GPRUK ID and forwards the 5GPRUK ID to the AUSF in Nausf_UEAuthentication_ProseGet Request message. The AUSF shall select PAnF based on 5GPRUK ID and forwards the 5GPRUK ID to the PAnF in Npanf_Get Request message. The PAnF shall retrieve the Remote UE's SUPI from the Prose context based on 5GPRUK ID and send the Remote UE's SUPI to the AUSF in the PAnF in Npanf_Get Response message. The AUSF shall forward Remote UE's SUPI to the AMF in Nausf_UEAuthentication_ProseGet Response message. The Relay AMF shall forward the received SUPI and the Remote UE Report message to the SMF in Nsmf_PDUSession_UpdateSMContext message.

Editor's Notes: How to support multiple Remote User IDs in Remote UE Report is FFS.

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 [13], clause 4.3.2.2.3 (e.g. using PLMN ID of the SUPI, S-NSSAI, etc.).

9. When the SMF receives Remote UE Report the SMF retrieves Remote UE's SM subscription data from the UDM by triggering Nudm_SDM_Get service operation. The SMF may include DNN, S-NSSAI of the PDU Session for relaying in addition to the Remote UE's SUPI as input parameters. The SMF determines based on the subscription data of the 5G ProSe Remote UE (i.e. Secondary authentication indication as per TS 23.502 [13], Table 5.2.3.3.1). The SMF may also check whether the 5G ProSe Remote UE has been authenticated by the same DN as indicated in the subscription data and, if secondary authentication is required, the SMF triggers a PDU Session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay by sending PDU Session Authentication Command message to the 5G ProSe Layer-3 UE-to-Network Relay including the 5GPRUK ID of the Remote UE and an EAP-Request/Identity.

Editor's Notes: how SMF is notified with the 5G ProSe remote UE's subscription update is FFS.

NOTE 2: The information on a successful authentication between a 5G ProSe Remote UE and an SMF may be saved in SMF and/or UDM.

10. Based on the 5GPRUK ID, the 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP-Request/Identity to the 5G ProSe Remote UE via PC5 signalling(10a). The 5G ProSe Remote UE returns the EAP-Response/Identity to the 5G ProSe Layer-3 UE-to-Network Relay via PC5 signalling(10b).
11. The 5G ProSe Layer-3 UE-to-Network Relay sends PDU Session Authentication Complete message to the SMF including the 5GPRUK ID of the Remote UE and an EAP-Response/Identity received from the 5G ProSe Remote UE.
12. The SMF sends an EAP-Response/Identity to the DN-AAA.
13. The DN AAA server and the UE should exchange EAP messages, as required by the EAP method. The SMF and Relay shall include the 5GPRUK ID in the NAS messages transporting the EAP messages.
14. The DN-AAA sends EAP-Success or EAP-Failure to the SMF.
15. Upon successful PDU Session secondary authentication via the Relay procedure, the SMF stores the 5G ProSe Remote UE information in the 5G ProSe Layer-3 UE-to-Network Relay's SM context including 5G ProSe Remote UE identity (e.g. GPSI, SUPI), individual authentication information received from DN-AAA.
16. The SMF sends Remote UE Report Ack message to the 5G ProSe Layer-3 UE-to-Network Relay indicating the result of the PDU Session secondary authentication, including the 5GPRUK ID of the remote UE and an EAP success or failure message. In the case of successful secondary authentication, the message may include QoS authorization info for the 5G ProSe Layer-3 UE-to-Network Relay to enforce. In case the secondary authentication is failed, the NAS message may indicate that 5G ProSe Layer-3 UE-to-Network Relay should release the PC5 link with the 5G ProSe Remote UE.
17. In the case of successful secondary authentication for the 5G ProSe Remote UE, the 5G ProSe Layer-3 UE-to-Network Relay stores any received authentication info associated with the 5G ProSe Remote UE. In case the secondary authentication is failed, the 5G ProSe UE-to-Network Relay releases the PC5 link with the 5G ProSe Remote UE and may keep the PDU session as the default PDU session or release it if there is no more 5G ProSe Remote UE using the same PDU session.

6.3.3.3.4.3 Re-Authentication of Remote UE via L3 UE-to-Network Relay without N3IWF

The Re-Authentication of Remote UE via L3 UE-to-Network Relay follows the steps described in Figure 6.3.3.3.4.3-1. The call flow is based on the call flow in TS 33.501 [3], Figure 11.1.3-1 with the main difference that the EAP messages for Re-authentication are exchanged between the Remote UE and DN-AAA using PC5 transport provided via the PC5 link with the UE-to-Network Relay.

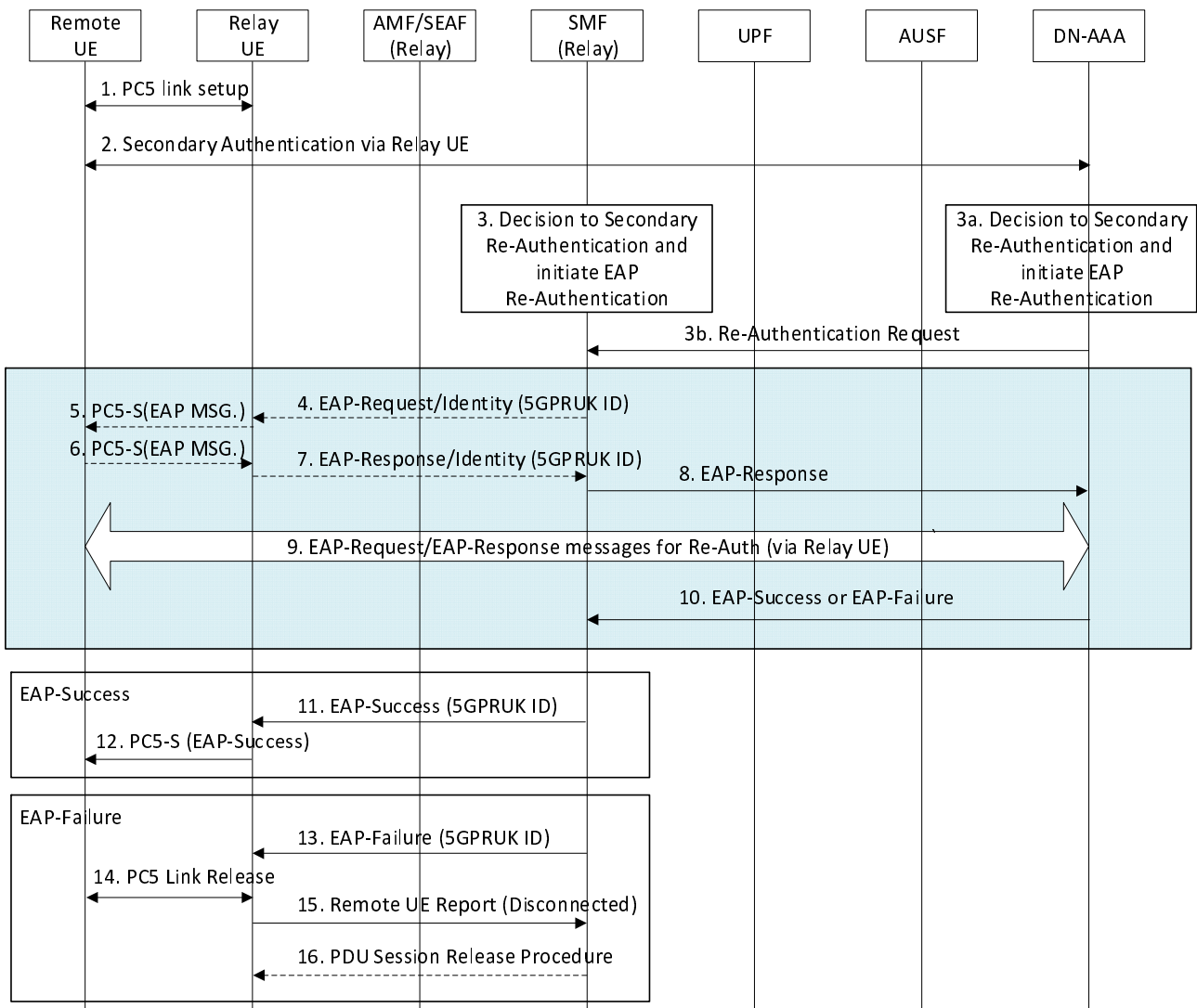


Figure 6.3.3.3.4.3-1: EAP Re-Authentication of Remote UE via L3 UE-to-Network Relay with an external AAA server

1-2. Secondary Authentication for the 5G ProSe Remote UE via the 5G ProSe Layer-3 UE-to-Network Relay has been established according to the procedures specified in clause 6.3.3.3.4, PDU Session secondary authentication of the 5G ProSe Remote UE via the 5G ProSe Layer-3 UE-to-Network Relay.

Secondary Re-authentication may either be initiated by the SMF or the external DN-AAA server. If Re-authentication is initiated by the SMF, the procedure proceeds with step 4 (skipping steps 3a and 3b). If Re-authentication is initiated by the external DN/AAA server, the procedure proceeds with the alternative steps 3a and 3b.

- 3. The SMF decides to initiate Secondary Re-Authentication for the 5G ProSe Remote UE.
- 3a. The DN AAA server decides to initiate Secondary Re-Authentication for the 5G ProSe Remote UE.
- 3b. The DN AAA shall send a Secondary Re-Authentication request to UPF, and the UPF forwards it to the SMF. The Secondary Re-authentication request contains the GPSI, and the IP/MAC address of the UE allocated to the PDU Session and the MAC address if the PDU session is of Ethernet PDU type for the 5G ProSe Remote UE. The SMF retrieves the corresponding 5GPRUK ID from the 5G ProSe Layer-3 UE-to-Network Relay's SM context using the GPSI.

Editor's Notes: How the GPSI of the remote UE is obtained by SMF is FFS.

- 4. The SMF may send an EAP Request/Identity message to the 5G ProSe Layer-3 UE-to-Network Relay including 5GPRUK ID of the 5G ProSe Remote UE. In case the procedure is initiated by the DN AAA, the SMF retrieves the 5GPRUK ID that is mapped with the received GPSI.

5. The 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP message to the 5G ProSe Remote UE via PC5 signalling.
6. The 5G ProSe Remote UE may respond with an EAP Response/Identity message to the 5G ProSe Layer-3 UE-to-Network Relay via PC5 signalling.
7. The 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP Response/Identity to SMF.
8. SMF forwards the EAP Response/Identity to the UPF, selected during initial authentication, over N4 interface. Then, the UPF shall forward the EAP Response/Identity message to the DN AAA Server. This establishes an end-to-end connection between the SMF and the external DN-AAA server for EAP exchange.
9. The DN AAA server and the 5G ProSe Remote UE shall exchange EAP messages as required by the EAP method.
10. After the completion of the authentication procedure, DN AAA server either sends EAP Success or EAP Failure message to the SMF. This completes the Re-authentication procedure at the SMF.
11. If the authentication is successful, EAP-Success and 5GPRUK ID shall be sent to the 5G ProSe Layer-3 UE-to-Network Relay.
12. The 5G ProSe Layer-3 UE-to-Network Relay shall forward the EAP-Success to the corresponding 5G ProSe Remote UE via PC5 signalling.
13. If authentication is not successful, EAP-Failure and 5GPRUK ID shall be sent to the 5G ProSe Layer-3 UE-to-Network Relay.
14. The 5G ProSe Layer-3 UE-to-Network Relay shall forward EAP-Failure to the corresponding 5G ProSe Remote UE via PC5 signalling and shall release the PC5 link with the 5G ProSe Remote UE.
15. The 5G ProSe Layer-3 UE-to-Network Relay shall send a Remote UE Report message indicating the 5G ProSe Remote UE is disconnected to the SMF.
16. The SMF may release the PDU session that was used for the relay service.

Editor's Notes: It is FFS whether this procedure is needed, depending on the outcome of secondary Authentication and authorization procedure.

6.3.3.3.4.4 Secondary Authentication Revocation of Remote UE via L3 UE-to-Network Relay without N3IWF

At any time, a DN-AAA may revoke the authentication and authorization for a PDU Session and according to the request from the DN-AAA server, the SMF may request the 5G ProSe Layer-3 UE-to-Network Relay to release the PC5 link with the revoked 5G ProSe Remote UE, or release the PDU Session of the 5G ProSe Layer-3 UE-to-Network Relay as specified in clause 4.3.4 of TS 23.502 [10] when it is not used by other 5G ProSe Remote UE(s).

6.3.3.4 Security for 5G ProSe Communication via Layer-3 UE-to-Network Relay with N3IWF support

The 5G ProSe Layer-3 Remote UE selects N3IWF as specified in TS 23.304 [2].

The 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay shall establish security for PC5 connection using either User Plane based solution as specified in clause 6.3.3.2 or Control Plane based solution as specified in clause 6.3.3.3. Then, the 5G ProSe Layer-3 Remote UE performs the security procedures as specified in clause 7.2.1 of TS 33.501 [3].

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 5G ProSe Remote UE and NG-RAN node shall establish AS security as specified in TS 33.501 [3].

The 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay shall establish security for PC5 connection using either User Plane based solution as specified in clause 6.3.3.2 or Control Plane based solution as specified in clause 6.3.3.3.2. The requirements on security policies for PC5 connection between the 5G ProSe Remote UE and the Layer-2 UE-to-Network Relay are as follows:

- The PCF shall be able to provision the PC5 security policies to the 5G ProSe Remote UE and Layer-2 UE-to-Network Relay respectively per ProSe relay service during their service authorization and information provisioning procedures as defined in TS 23.304 [2].

NOTE: If PC5 UP security policies are included in the PC5 security policies, they are negotiated but not enforced by the 5G ProSe Layer-2 UE-to-Network Relay.

6.3.5 Direct Communication Request in 5G ProSe UE-to-Network Relay Communication

6.3.5.1 General

This clause describes the mechanism to protect the privacy of the PRUK ID and RSC in Direct Communication Request (DCR) message when restricted discovery is used for the UE-to-Network Relay service. This clause also describes a mechanism to integrity protect the DCR message when DUK is provisioned for discovery.

6.3.5.2 Privacy protection of PRUK ID and RSC in DCR

The 5G ProSe Remote UE encrypts the PRUK ID and RSC using the code-receiving security parameters used for discovery. The 5G ProSe UE-to-Network Relay, on receiving the DCR message, decrypts the encrypted PRUK ID and RSC using the code-sending security parameters used for discovery and verifies if the RSC matches with the one that it sent in the discovery message. If the RSC does not match, the 5G ProSe UE-to-Network Relay shall abort the PC5 direct link establishment procedure.

The 5G ProSe UE-to-Network Relay shall decrypt the encrypted PRUK ID and RSC as follows:

- 1) If the UE is configured with Discovery User Confidentiality Key (DUCK), the DCR ciphering key K_{DCR} is set to DUCK. If the UE is configured with Discovery User Scrambling Key (DUSK) but not DUCK, K_{DCR} is set to DUSK. If the UE is neither configured with DUCK nor DUSK, the DCR message is not protected, and Steps 2-3 are skipped.
- 2) Set Keystream to DCR confidentiality keystream calculated using K_{DCR} , UTC-based counter and RSC as described in clause A.5.
- 3) XOR the first L bits of the Keystream with the RSC where L is the length of the RSC, and XOR the remaining bits of the Keystream with the PRUK ID.

NOTE 1: If PRUK ID is in NAI format, encryption of the PRUK ID is performed on the username part of the PRUK ID.

The UE-to-network relay shall decrypt the encrypted PRUK ID and RSC as follows:

- 1) If the UE is configured with DUCK, the DCR ciphering key K_{DCR} is set to DUCK. If the UE is configured with DUSK but not DUCK, K_{DCR} is set to DUSK. If the UE is neither configured with DUCK nor DUSK, the DCR message is not protected, and steps 2-3 are skipped.
- 2) Set Keystream to DCR confidentiality keystream calculated using K_{DCR} , UTC-based counter and RSC as described in clause A.5.
- 3) XOR the first L bits of Keystream with the encrypted RSC where L is the length of the encrypted RSC, and XOR the remaining bits of Keystream with the encrypted PRUK ID.

NOTE 2: If PRUK ID is in NAI format, decryption of the PRUK ID is performed on the username part of the PRUK ID.

6.3.5.3 Integrity protection of DCR

The 5G ProSe Remote UE integrity protects the DCR message using the code-receiving security parameters used for discovery. The integrity protection of the DCR message is performed after the privacy protection of PRUK ID and RSC.

The 5G ProSe UE-to-Network Relay, on receiving the DCR message, verifies the integrity of the received DCR message using the code-sending security parameters used for discovery. If the integrity verification of the DCR fails, the 5G ProSe UE-to-Network Relay shall abort the PC5 direct link establishment procedure.

The 5G ProSe Remote UE shall integrity protect the DCR as follows:

1. If the UE is configured with DUIK, the DCR integrity key K_{INT} is set to DUIK. Otherwise, the DCR message is not integrity protected, and steps 2-3 are skipped.
2. Calculate Message Integrity Check (MIC) using K_{INT} , UTC-based counter and the DCR message as described in clause A.9.
3. Set the MIC IE to the calculated MIC.

The 5G ProSe UE-to-Network Relay shall verify the integrity of the received DCR message as follows:

1. If the UE is configured with DUIK, the DCR integrity key K_{INT} is set to DUIK. Otherwise, the DCR message is not integrity protected, and step 2 is skipped.
2. Calculate a MIC using K_{INT} , UTC-based counter and the received DCR message as described in clause A.9 and compare the calculated MIC with the MIC included in the DCR message. If they mismatch, the integrity check fails.

7 5G ProSe services

7.1 General

This clause provides the present document of the SBA services defined for 5G ProSe.

7.2 5G PKMF Services

7.2.1 General

The 5G PKMF supports the key request from another 5G PKMF in another PLMN via the new service operation `Npkmf_PKMFKeyRequest_ProseKey`.

Table 7.2.1-1 shows the services exposed by 5G PKMF supporting 5G ProSe.

Table 7.2.1-1: 5G ProSe Services provided by 5G PKMF

Service	Service Operations	Operation Semantics	Example Consumer(s)
<code>Npkmf_PKMFKeyRequest</code>	<code>ProseKey</code>	Request/Response	5G PKMF

7.2.2 Npkmf_PKMFKeyRequest service

7.2.2.1 Npkmf_PKMFKeyRequest_ProseKey service operation

Service operation name: `Npkmf_PKMFKeyRequest_ProseKey`.

Description: Provides ProSe related keying material.

Input, Required: Relay Service Code, K_{NRP} freshness parameter 1:

- 1) In the initial Key Request: SUCI of the 5G ProSe Remote UE or PRUK ID.
- 2) In the subsequent Key Requests for Synchronization Failure handling: RAND, AUTS.

Input, Optional: None.

Output, Required: K_{NRP} , K_{NRP} freshness parameter 2.

Output, Optional: GPI.

7.3 AUSF Services

7.3.1 General

The AUSF of the 5G ProSe Remote UE supports the 5G ProSe Remote UE specific authentication of a 5G ProSe Remote UE via the AMF of the 5G ProSe UE-to-Network Relay and 5G ProSe UE-to-Network Relay via the new service operation Nausf_UEAuthentication_ProseAuthenticate for the existing Nausf_UEAuthentication service.

Table 7.3.1-1 shows the services exposed by AUSF supporting 5G ProSe.

Table 7.3.1-1: 5G ProSe Services provided by AUSF

Service	Service Operations	Operation Semantics	Example Consumer(s)
Nausf_UEAuthentication	ProseAuthenticate	Request/Response	(Relay) AMF

7.3.2 Nausf_UEAuthentication Service

7.3.2.1 Nausf_UEAuthentication_ProseAuthenticate service operation

Service operation name: Nausf_UEAuthentication_ProseAuthenticate.

Description: Authenticate the 5G ProSe Remote UE and provides Prose related keying material.

Input, Required: One of the options below:

- 1) In the initial authentication request: SUCI or 5GPRUK ID of the 5G ProSe Remote UE, Relay Service Code, Nonce_1.
- 2) In the subsequent authentication requests: EAP message.

Input, Optional: None.

Output, Required: EAP message, Authentication result and if success K_{NR_ProSe} , Nonce_2 and 5GPRUK ID.

Output, Optional: None.

7.3.2.2 Nausf_UEAuthentication_ProseGet service operation

Service operation name: Nausf_UEAuthentication_ProseGet.

Description: Provides the 5G ProSe Remote UE's SUPI.

Input, Required: 5GPRUK ID.

Input, Optional: None.

Output, Required: 5G ProSe Remote UE's SUPI.

Output, Optional: None.

7.4 UDM Services

7.4.1 General

A UDM supports providing the authentication vector for 5G ProSe Remote UE specific authentication via the new service operation Nudm_UEAuthentication_GetProseAv service operation of the existing Nudm_UEAuthentication service.

Table 7.4.1-1 shows the services exposed by UDM supporting 5G ProSe.

Table 7.4.1-1: 5G ProSe Services provided by UDM

Service	Service Operations	Operation Semantics	Example Consumer(s)
Nudm_UEAuthentication	GetProseAv	Request/Response	AUSF
Nudm_UEIdentifier	Deconceal	Request/Response	PKMF

7.4.2 Nudm_UEAuthentication Service

7.4.2.1 Nudm_UEAuthentication_GetProseAv service operation

Service operation name: Nudm_UEAuthentication_GetProseAv.

Description: Requester NF gets the authentication data for Prose and the Routing Indicator from UDM. If SUCI is included, this service operation returns the SUPI.

Inputs, Required: SUPI or SUCI, Relay Service Code, Serving network name.

Inputs, Optional: Synchronization Failure indication and related information (i.e. RAND/AUTS).

Outputs, Required: Authentication Vector for Prose, Routing Indicator.

Outputs, Optional: SUPI if SUCI was used as input.

7.4.3 Nudm_UEIdentifier Service

7.4.3.1 Nudm_UEIdentifier_Deconceal service operation

Service operation name: Nudm_UEIdentifier_Deconceal.

Description: Requester NF gets the SUPI from the UDM.

Inputs, Required: SUCI.

Inputs, Optional: None.

Outputs, Required: SUPI.

Outputs, Optional: None.

7.5 Prose Anchor Function Services

7.5.1 General

The Prose Anchor Function (PANF) supports providing storage for the Prose context info (i.e. SUPI, 5GPRUK, 5GPRUK ID, RSC) for a 5G ProSe Remote UE.

Table 7.5.1-1 shows the PANF Service and the PANF Service Operations.

Table 7.5.1-1: List of PAnF Services

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Npanf_ProseKey	Npanf_ProseKey_Register	Request/Response	AUSF
	Npanf_ProseKey_Get	Request/Response	AUSF

7.5.2 Npanf_ProseKey service

7.5.2.1 Npanf_ProseKey_Register service operation

Service operation name: Npanf_ProseKey_Register.

Description: The NF consumer requests the PAnF to store the Prose context info (i.e. SUPI, 5GPRUK, 5GPRUK ID, RSC).

Input, Required: SUPI, 5G PRUK ID, 5GPRUK, Relay Service Code.

Input, Optional: None.

Output, Required: None.

Output, Optional: None.

7.5.2.2 Npanf_ProseKey_Get service operation

Service operation name: Npanf_ProseKey_Get.

Description: The NF consumer requests 5GPRUK from the PAnF.

Input, Required: 5GPRUK ID, Relay Service Code.

Input, Optional: None.

Output, Required: 5GPRUK.

Output, Optional: None.

7.5.3 Npanf_get service

7.5.3.1 Npanf_Get service operation

Service operation name: Npanf_Get.

Description: The NF consumer requests Remote UE's SUPI from the PAnF.

Input, Required: 5GPRUK ID.

Input, Optional: None.

Output, Required: Remote UE's SUPI.

Output, Optional: None.

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 clause 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, 0xYY.

A.2 5GPRUK derivation function

When deriving a 5GPRUK from $K_{\text{AUSF,P}}$, 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 $K_{\text{AUSF,P}}$.

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

A.3 Derivation of 5GPRUK ID*

When deriving the 5GPRUK ID from $K_{\text{AUSF,P}}$, 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 $K_{\text{AUSF,P}}$.

A.4 K_{NR_ProSe} derivation function

When deriving the K_{NR_ProSe} from 5GPRUK key, the following parameters shall be used to form the input S to the KDF:

- $FC = 0xZZ$;
- $P0 = \text{Nonce_2}$;
- $L0 = \text{length of Nonce_2}$;
- $P1 = \text{Nonce_1}$;
- $L1 = \text{length of Nonce_1}$.

The input key KEY shall be 5GPRUK key.

A.5 Calculation of DCR 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 [8]:

- $FC = 0xBB$
- $P0 = \text{UTC-based counter}$
- $L0 = \text{length of UTC-based counter (i.e. } 0x00\ 0x04)$
- $P1 = \text{RSC}$
- $L1 = \text{length of RSC (i.e. } 0x00\ 0x03)$.

The input key shall be the 256-bit selected key in Step 1 of clause 6.3.5.2.

The DCR confidentiality keystream is set to L least significant bits of the output of the KDF, where $L = \text{the length of the RSC} + \text{the length of the PRUK ID}$.

NOTE: If PRUK ID is in NAI format, the length of the PRUK ID is determined by the username part of the PRUK ID.

A.6 Calculation of MIC value for discovery message

When calculating a MIC using the Discovery Key for open discovery or the DUIK for restricted discovery, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [8]:

- $FC = 0xYY$.
- $P0 = \text{UTC-based counter associated with the discovery slot}$.
- $L0 = \text{length of above (i.e. } 0x00\ 0x04)$.
- $P1 = \text{discovery message with the MIC value field set to all zeros}$.
- $L1 = \text{length of above}$.

The MIC is set to the 32 least significant bits of the output of the KDF.

The Discovery Key, DUIK, Time parameter and discovery message follow the encoding also specified in Annex B of TS 33.220 [8].

A.7 Message-specific confidentiality mechanisms for discovery

Message-specific confidentiality protection is provided by ProSe layer between ProSe UEs.

The use and mode of operation of the ciphering algorithms are specified in Annex D in TS 33.501 [3].

The input parameters to the ciphering algorithms as described in Annex D in TS 33.501 [3] are:

- KEY: 128 least significant bits of the output of the KDF (DUCK, UTC-based counter, MIC)
- COUNT: UTC-based counter
- BEARER: 0x00
- DIRECTION: 0x00
- LENGTH: $\text{LEN}(\text{discovery message}) - (\text{LEN}(\text{Message Type}) + \text{LEN}(\text{UTC-based counter LSB}) + \text{LEN}(\text{MIC}))$, where $\text{LEN}(x)$ is the length of x in number of bits

KEY is set to as such to generate message-specific keystream as in TS 33.303 [4].

The output keystream of the ciphering algorithm (output_keystream) is then masked with the $\text{Encrypted_bits_mask}$ to produce the final keystream for the message-specific confidentiality protection (KEYSTREAM):

$\text{KEYSTREAM} = \text{output_keystream} \text{ AND } (\text{Encrypted_bits_mask} \parallel 0\text{xFF..FF})$

The KEYSTREAM is XORed with the discovery message for message-specific confidentiality protection.

A.8 Calculation of K_{NRP} for UE-to-Network relays

When calculating K_{NRP} from PRUK, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [5]:

- FC = 0xYY
- P0 = Relay Service Code
- L0 = length of Relay Service Code (i.e. 0x00 0x03)
- P1 = K_{NRP} freshness parameter 1
- L1 = length of K_{NRP} freshness parameter 1 (i.e. 0x00 0x10)
- P2 = K_{NRP} freshness parameter 2
- L2 = length of K_{NRP} freshness parameter 2 (i.e. 0x00 0x10)

The input key shall be the 256-bit PRUK.

A.9 Calculation of MIC value for Direct Communication Request

When calculating a MIC using the DUIK to integrity protect Direct Communication Request (DCR) message, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [8]:

- FC = 0xCC.
- P0 = UTC-based counter.

- L0 = length of above (i.e. 0x00 0x04).
- P1 = DCR message with the MIC value field set to all zeros.
- L1 = length of above.

The MIC is set to the 32 least significant bits of the output of the KDF.

The DUIK, UTC-based counter and DCR message follow the encoding also specified in Annex B of TS 33.220 [8].

Annex B (informative): Source authenticity of discovery messages

To achieve source authenticity of discovery messages, the third security requirement in clause 6.1.2, a UE receiving a discovery message can verify the source authenticity of the received discovery message by using the provisioned DUIK under the assumption that the UEs provisioned with the same DUIK are trusted.

Alternatively, if receiving UEs are not provisioned with the DUIK, the network can verify the source authenticity of discovery messages via match report procedure.

Annex C (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2022-06	SA#96	SP-220541				Presented for information and approval	1.0.0
2022-06	SA#96					Upgrade to change control version	17.0.0
2022-06	SA#96					EditHelp review	17.0.1

History

Document history		
V17.0.1	July 2022	Publication