

ETSI TS 133 503 V17.10.0 (2025-01)



5G;
Security Aspects of Proximity based Services (ProSe)
in the 5G System (5GS)
(3GPP TS 33.503 version 17.10.0 Release 17)

[ETSI TS 133 503 V17.10.0 \(2025-01\)](https://standards.iteh.ai/catalog/standards/etsi/351940f3-fe50-47fc-9a68-9745a40fd2c7/etsi-ts-133-503-v17-10-0-2025-01)

<https://standards.iteh.ai/catalog/standards/etsi/351940f3-fe50-47fc-9a68-9745a40fd2c7/etsi-ts-133-503-v17-10-0-2025-01>



Reference

RTS/TSGS-0333503vha0

Keywords

5G

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 the
[ETSI Search & Browse Standards application](#).

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 on [ETSI deliver repository](#).

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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 2025.
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 IPR online database](#).

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™**, **LTE™** and **5G™** logo 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. (2025-01)

The cross reference between 3GPP and ETSI identities can be found at [3GPP to ETSI numbering cross-referencing](#).

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	9
3.1 Terms.....	9
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
4.2.1.3 ProSe Anchor Function.....	11
4.2.2 Reference points	11
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	12
5.2.2.1 General	12
5.2.2.2 Security requirements.....	12
5.2.2.3 Security procedures	12
5.2.3 Security of UE - 5G DDNMF interface	12
5.2.3.1 General.....	12
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.....	13
5.2.3.6 Privacy issue in PC3a interface.....	13
5.2.4 Security of service-based interfaces used in 5G ProSe.....	13
5.2.4.1 Security requirements.....	13
5.2.4.2 Security procedures	13
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	14
5.2.5.4 Security procedures for PC8 using AKMA.....	14
6 Security for 5G ProSe features	14
6.1 Security for 5G ProSe Discovery	14
6.1.1 General.....	14
6.1.2 Security requirements	14
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.....	17
6.1.3.2.1 General	17
6.1.3.2.2 Security flows.....	17
6.1.3.2.2.1 Restricted 5G ProSe Direct Discovery Model A	17
6.1.3.2.2.2 Restricted 5G ProSe Direct Discovery Model B.....	21

6.1.3.2.3	Protection of discovery messages over PC5 interface	26
6.2	Security for unicast mode 5G ProSe Direct Communication	27
6.2.1	General.....	27
6.2.2	Security requirements	27
6.2.3	Security procedures.....	27
6.2.4	Identity privacy for the PC5 unicast link	27
6.3	Security for 5G ProSe UE-to-Network Relay Communication.....	28
6.3.1	General.....	28
6.3.2	Security requirements	28
6.3.3	Security for 5G ProSe Communication via 5G ProSe Layer-3 UE-to-Network Relay.....	28
6.3.3.1	Security requirements.....	28
6.3.3.2	Security procedure over User Plane	29
6.3.3.2.1	General	29
6.3.3.2.2	PC5 security establishment for 5G ProSe UE-to-Network relay communication over User Plane	30
6.3.3.2.3	PC5 Key Hierarchy over User Plane	35
6.3.3.3	Security procedure over Control Plane	35
6.3.3.3.1	General	35
6.3.3.3.2	PC5 security establishment for 5G ProSe UE-to-Network relay communication over Control Plane	35
6.3.3.3.3	PC5 Key Hierarchy over Control Plane.....	40
6.3.3.3.4	Void.....	41
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.....	41
6.3.5.1	General.....	41
6.3.5.2	Privacy protection of UP-PRUK ID and RSC	41
6.3.5.3	Integrity protection of DCR	42
6.4	Security for broadcast mode 5G ProSe Direct Communication	43
6.4.1	General.....	43
6.4.2	Security requirements	43
6.4.3	Security procedures.....	43
6.5	Security for groupcast mode 5G ProSe Direct Communication.....	43
6.5.1	General.....	43
6.5.2	Security requirements	43
6.5.3	Security procedures.....	43
7	5G ProSe services.....	43
7.1	General	43
7.2	5G PKMF services	44
7.2.1	General.....	44
7.2.2	Npkmf_PKMFKeyRequest service	44
7.2.2.1	Npkmf_PKMFKeyRequest_ProseKey service operation	44
7.2.3	Npkmf_ResolveRemoteUserId service.....	44
7.2.3.1	Npkmf_ResolveRemoteUserId_Get service operation	44
7.2.4	Npkmf_Discovery service	45
7.2.4.1	Npkmf_Discovery_AnnounceAuthorize service operation.....	45
7.2.4.2	Npkmf_Discovery_MonitorKey service operation	45
7.2.4.3	Npkmf_Discovery_DiscoveryKey service operation.....	45
7.3	AUSF services.....	45
7.3.1	General.....	45
7.3.2	Nausf_UEAuthentication service.....	46
7.3.2.1	Nausf_UEAuthentication_ProseAuthenticate service operation.....	46
7.3.2.2	Void.....	46
7.4	UDM Services	46
7.4.1	General.....	46
7.4.2	Nudm_UEAuthentication Service	46
7.4.2.1	Nudm_UEAuthentication_GetProseAv service operation	46
7.4.3	Nudm_UEIdentifier Service	47
7.4.3.1	Nudm_UEIdentifier_Deconceal service operation.....	47
7.5	Prose Anchor Function Services	47
7.5.1	General.....	47

7.5.2 Npanf_ProseKey service.....47

7.5.2.1 Npanf_ProseKey_Register service operation.....47

7.5.2.2 Npanf_ProseKey_Get service operation47

7.5.3 Void48

7.5.4 Npanf_ResolveRemoteUserId service48

7.5.4.1 Npanf_ResolveRemoteUserId_Get service operation.....48

Annex A (normative): Key derivation functions49

A.1 KDF interface and input parameter construction49

A.1.1 General49

A.1.2 FC value allocations49

A.2 CP-PRUK derivation function.....49

A.3 Derivation of CP-PRUK ID*49

A.4 K_{NR_ProSe} derivation function.....50

A.5 Calculation of DCR confidentiality keystream50

A.6 Calculation of MIC value for discovery message50

A.7 Message-specific confidentiality mechanisms for discovery51

A.8 Calculation of K_{NRP} for UE-to-Network relays51

A.9 Calculation of MIC value for Direct Communication Request.....51

Annex B (informative): Source authenticity of discovery messages53

Annex C (informative): Change history54

History56

iTech Standards
 (https://standards.itih.ai)
 Document Preview

[ETSI TS 133 503 V17.10.0 \(2025-01\)](https://standards.itih.ai/catalog/standards/etsi/351940f3-fe50-47fc-9a68-9745a40fd2c7/etsi-ts-133-503-v17-10-0-2025-01)

<https://standards.itih.ai/catalog/standards/etsi/351940f3-fe50-47fc-9a68-9745a40fd2c7/etsi-ts-133-503-v17-10-0-2025-01>

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.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 133 503 V17.10.0 \(2025-01\)](https://standards.iteh.ai/catalog/standards/etsi/351940f3-fe50-47fc-9a68-9745a40fd2c7/etsi-ts-133-503-v17-10-0-2025-01)

<https://standards.iteh.ai/catalog/standards/etsi/351940f3-fe50-47fc-9a68-9745a40fd2c7/etsi-ts-133-503-v17-10-0-2025-01>

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] Void
- [13] Void
- [14] IETF RFC 7542: "The Network Access Identifier".
- [15] IETF RFC 9048: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

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

iTech Standards
 (https://standards.itih.ai)
 Document Preview

3.2 Symbols ETSI TS 133 503 V17.10.0 (2025-01)

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
CP-PRUK	Control Plane 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
PAnF	Prose Anchor Function
ProSe	Proximity-based Services
RPAUID	Restricted ProSe Application User ID
RSC	Relay Service Code
SBI	Service Based Interface
UP	User Plane
UP-PRUK	User Plane Prose Remote User Key
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 UP-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.

4.2.1.3 Prose Anchor Function

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

The PAnF shall store the Prose context info (i.e. SUPI, RSC, CP-PRUK, CP-PRUK ID) for a 5G ProSe Remote UE.

The PAnF interacts with AUSF using procedures over Npc11 reference point defined in clause 4.2.2. The PAnF interacts with UDM using procedures over Npc12 reference point defined in clause 4.2.2.

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 discovery and 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 the 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.

Npc11: The reference point between the AUSF and Prose Anchor Function (PAnF). It is used to store the Prose context info for a 5G ProSe Remote UE.

Npc12: The reference point between the PAnF and UDM. It is used to check with the UDM whether the Remote UE is authorized to use the UE-to-Network Relay service.

Npc13: The reference point between the SMF and PKMF. It is used to obtain the SUPI of Remote UE from PKMF.

Npc14: The reference point between the SMF and PAnF. It is used to obtain the SUPI of Remote UE from PAnF.

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, Npc8, Npc9 and Npc10 specified in clause 4.2.5 of TS 23.304 [2], Npc11 and Npc12 specified in clause 4.2.2 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.