

# ETSI TS 133 303 V13.5.0 (2017-07)



**Universal Mobile Telecommunications System (UMTS);  
LTE;  
Proximity-based Services (ProSe);  
Security aspects  
(3GPP TS 33.303 version 13.5.0 Release 13)**



## Reference

---

RTS/TSGS-0333303vd50

## Keywords

---

LTE,SECURITY,UMTS

**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 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

**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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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/CommiteeSupportStaff.aspx>

**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 2017.  
All rights reserved.

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 protected for the benefit of its Members.  
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

---

## Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 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  |
| Foreword.....  | 2  |
| Modal verbs terminology.....   | 2  |
| Foreword.....  | 7  |
| 1 Scope .....  | 8  |
| 2 References .....   | 8  |
| 3 Definitions and abbreviations.....   | 10 |
| 3.1 Definitions .....  | 10 |
| 3.2 Abbreviations .....  | 10 |
| 4 Overview of ProSe security.....  | 12 |
| 4.1 General .....  | 12 |
| 4.2 Reference points and Functional Entities .....   | 12 |
| 5 Common security procedures .....   | 12 |
| 5.1 General .....  | 12 |
| 5.2 Network domain security .....  | 12 |
| 5.2.1 General.....   | 12 |
| 5.2.2 Security requirements .....  | 12 |
| 5.2.3 Security procedures.....   | 12 |
| 5.3 Security of UE to ProSe Function interface .....   | 13 |
| 5.3.1 General.....   | 13 |
| 5.3.2 Security requirements .....  | 13 |
| 5.3.3 Security procedures.....   | 13 |
| 5.3.3.1 Security procedures for configuration transfer to the UICC .....                     | 13 |
| 5.3.3.2 Security procedures for data transfer to the UE .....                                | 13 |
| 5.4 Security of the PC2 reference point.....   | 14 |
| 5.4.1 Requirements on PC2 reference point .....  | 14 |
| 5.4.2 Security procedures for PC2 reference point .....                                      | 14 |
| 6 Security for ProSe features .....  | 15 |
| 6.1 ProSe direct discovery .....   | 15 |
| 6.1.1 Overview of ProSe direct discovery in network coverage .....                           | 15 |
| 6.1.2 Security requirements .....  | 15 |
| 6.1.3 Security procedures.....   | 16 |
| 6.1.3.1 Interface between the UE and ProSe Function.....                                     | 16 |
| 6.1.3.2 Interfaces between network elements.....   | 16 |
| 6.1.3.3 Integrity protection and validation of the transmitted code for open discovery ..... | 16 |
| 6.1.3.3.1 Open discovery security flows .....  | 16 |
| 6.1.3.4 Restricted discovery .....   | 19 |
| 6.1.3.4.1 General .....  | 19 |
| 6.1.3.4.2 Security flows.....  | 19 |
| 6.1.3.4.2.1 Model A security flows.....  | 19 |
| 6.1.3.4.2.2 Model B security flows.....  | 22 |
| 6.1.3.4.3 Protection of the discovery messages over the PC5 interface .....                  | 25 |
| 6.1.3.4.3.1 General.....   | 25 |
| 6.1.3.4.3.2 Message Processing in the sending UE.....  | 26 |
| 6.1.3.4.3.3 Protected message processing in the receiving UE .....                           | 26 |
| 6.1.3.4.3.4 Integrity protection description .....   | 27 |
| 6.1.3.4.3.5 Scrambling description .....   | 27 |
| 6.1.3.4.3.6 Message-specific confidentiality description.....                                | 27 |
| 6.2 Security for One-to-many ProSe direct communication.....                                 | 28 |
| 6.2.1 Overview of One-to-many ProSe direct communication.....                                | 28 |
| 6.2.2 Security requirements .....  | 28 |
| 6.2.3 Bearer layer security mechanism .....  | 29 |

|               |   |    |
|---------------|---|----|
| 6.2.3.1       | Security keys and their lifetimes .....                                     | 29 |
| 6.2.3.2       | Identities.....   | 29 |
| 6.2.3.3       | Security flows .....  | 31 |
| 6.2.3.3.1     | Overview .....  | 31 |
| 6.2.3.3.2     | Messages between UE and ProSe Key Management Function .....                 | 33 |
| 6.2.3.3.2.1   | General.....  | 33 |
| 6.2.3.3.2.2   | Key Request and Key Response messages .....                                 | 33 |
| 6.2.3.3.2.3   | MIKEY messages .....  | 35 |
| 6.2.3.3.2.3.1 | General .....   | 35 |
| 6.2.3.3.2.3.2 | Creation of the MIKEY key delivery message.....                             | 35 |
| 6.2.3.3.2.3.3 | Processing the MIKEY key delivery message .....                             | 35 |
| 6.2.3.3.2.3.4 | MIKEY Verification message.....   | 36 |
| 6.2.3.4       | Protection of traffic between UE and ProSe Function .....                   | 36 |
| 6.2.3.5       | Protection of traffic between UE and ProSe Key Management Function .....    | 36 |
| 6.2.3.6       | Protection of traffic between UEs .....                                     | 36 |
| 6.2.3.6.1     | Protection of data.....   | 36 |
| 6.2.3.6.2     | Key derivation data in PDCP header.....                                     | 37 |
| 6.2.4         | Solution description for media security of one-to-many communications ..... | 38 |
| 6.3           | EPC-level discovery of ProSe-enabled UEs.....                               | 39 |
| 6.3.1         | Security for proximity request authentication and authorization .....       | 39 |
| 6.3.1.1       | General .....   | 39 |
| 6.3.1.2       | Application Server-signed proximity request.....                            | 39 |
| 6.3.1.3       | Proximity request digital signature algorithms and key strength .....       | 40 |
| 6.3.1.4       | Proximity request hash input format .....                                   | 42 |
| 6.3.1.5       | Verification key format.....  | 42 |
| 6.3.1.6       | Profile for Application Server certificate .....                            | 42 |
| 6.3.2         | Protection of traffic between UE and ProSe Function .....                   | 42 |
| 6.4           | Security for EPC support WLAN direct discovery and communication.....       | 43 |
| 6.5           | Security for One-to-one ProSe Direct communication.....                     | 43 |
| 6.5.1         | General.....  | 43 |
| 6.5.2         | Security Requirements.....  | 43 |
| 6.5.3         | Overview of One-to-one ProSe Direct communication.....                      | 43 |
| 6.5.3.1       | Description of different layers of keys and their identities .....          | 43 |
| 6.5.3.2       | Security states .....   | 44 |
| 6.5.3.3       | High level overview of security establishment .....                         | 44 |
| 6.5.4         | Direct Authentication and Key Establishment.....                            | 45 |
| 6.5.4.1       | General.....  | 45 |
| 6.5.5         | Security Establishment procedures.....                                      | 45 |
| 6.5.5.1       | General .....   | 45 |
| 6.5.5.2       | Security establishment during connection set-up.....                        | 45 |
| 6.5.5.3       | Rekeying security.....  | 46 |
| 6.5.6         | Protection of the one-to-one traffic.....                                   | 47 |
| 6.5.6.1       | General .....   | 47 |
| 6.5.6.2       | Integrity protection.....   | 48 |
| 6.5.6.3       | Confidentiality protection .....  | 48 |
| 6.5.6.4       | Security contents in the PDCP header.....                                   | 48 |
| 6.5.7         | ProSe one-to-one communication security using ECCSI and SAKKE .....         | 49 |
| 6.5.7.1       | General .....   | 49 |
| 6.5.7.2       | Key and their identities .....  | 49 |
| 6.5.7.3       | Security flows .....  | 49 |
| 6.5.7.3.1     | Direct Connection Request .....   | 49 |
| 6.5.7.3.2     | Direct Rekeying Request .....   | 50 |
| 6.6           | Security for ProSe Public Safety Discovery.....                             | 51 |
| 6.6.1         | General.....  | 51 |
| 6.6.2         | Security Requirements.....  | 51 |
| 6.6.3         | Overview of ProSe Public Safety Discovery .....                             | 51 |
| 6.6.3.1       | General .....   | 51 |
| 6.6.3.2       | Key and their identities .....  | 52 |
| 6.6.4         | Security flows .....  | 52 |
| 6.6.4.1       | Overview.....   | 52 |
| 6.6.4.2       | Messages between UE and ProSe Key Management Function.....                  | 54 |
| 6.6.4.2.1     | General .....   | 54 |

|                               |  |           |
|-------------------------------|--|-----------|
| 6.6.4.2.2                     | Key Request and Key Response messages .....  | 54        |
| 6.6.4.2.3                     | MIKEY messages .....   | 55        |
| 6.6.4.2.3.1                   | General .....  | 55        |
| 6.6.5                         | Protection of traffic between UE and ProSe Function .....                                | 55        |
| 6.6.6                         | Protection of traffic between UE and ProSe Key Management Function .....                 | 55        |
| 6.6.7                         | Protection of discovery messages between the UEs .....                                   | 56        |
| 6.7                           | Security for ProSe UE-to-network relays .....  | 56        |
| 6.7.1                         | General .....  | 56        |
| 6.7.2                         | Security Requirements .....  | 56        |
| 6.7.3                         | Overview of ProSe UE-to-network relay security .....                                     | 57        |
| 6.7.3.1                       | General .....  | 57        |
| 6.7.3.2                       | Security flows .....   | 57        |
| 6.7.3.2.1                     | Overview .....   | 57        |
| 6.7.3.2.1.1                   | Remote UE attaching to a ProSe UE-to-network relay .....                                 | 57        |
| 6.7.3.2.1.2                   | Re-synchronisation in GBA Push authentication .....                                      | 59        |
| 6.7.3.2.1.3                   | Rekeying procedures .....  | 60        |
| 6.7.3.2.2                     | Messages between the Remote UE and ProSe Key Management Function .....                   | 61        |
| 6.7.3.2.2.1                   | General .....  | 61        |
| 6.7.3.2.2.2                   | Key Request and Key Response messages .....  | 61        |
| 6.7.3.2.3                     | Messages between the Relay and ProSe Key Management Function .....                       | 62        |
| 6.7.3.2.3.1                   | General .....  | 62        |
| 6.7.3.2.3.2                   | Key Request and Key Response messages .....  | 62        |
| 6.7.3.3                       | Protection of traffic between Remote UE or Relay and ProSe Function .....                | 63        |
| 6.7.3.4                       | Protection of traffic between Remote UE or Relay and ProSe Key Management Function ..... | 63        |
| 6.7.3.5                       | Protection of traffic between Remote UE and Relay .....                                  | 64        |
| <b>Annex A (normative):</b>   | <b>Key derivation functions .....</b>  | <b>65</b> |
| A.1                           | KDF interface and input parameter construction .....                                     | 65        |
| A.1.1                         | General .....  | 65        |
| A.1.2                         | FC value allocations .....   | 65        |
| A.2                           | Calculation of the MIC value .....   | 65        |
| A.3                           | Calculation of PTK .....   | 65        |
| A.4                           | Calculation of keys from PTK and $K_{D-secs}$ .....                                      | 66        |
| A.5                           | Calculation of scrambling bits for discovery .....                                       | 66        |
| A.6                           | Calculation of message-specific confidentiality keystream for discovery .....            | 66        |
| A.7                           | Calculation of $K_D$ for UE-to-network relays .....                                      | 67        |
| A.8                           | Calculation of discovery keys from PSDK .....  | 67        |
| <b>Annex B (informative):</b> | <b>Void .....</b>  | <b>69</b> |
| <b>Annex C (informative):</b> | <b>Void .....</b>  | <b>70</b> |
| <b>Annex D (informative):</b> | <b>Void .....</b>  | <b>71</b> |
| <b>Annex E (Normative):</b>   | <b>Key Request and Response messages .....</b>   | <b>72</b> |
| E.1                           | Introduction .....   | 72        |
| E.2                           | Transport protocol for messages between UE and ProSe Key Management Function .....       | 72        |
| E.3                           | XML Schema .....   | 72        |
| E.4                           | Semantics .....  | 75        |
| E.4.1                         | General .....  | 75        |
| E.4.2                         | Semantics of <KEY_REQUEST> .....   | 76        |
| E.4.3                         | Semantics of <KEY_RESPONSE> .....  | 77        |
| E.5                           | General message format and information elements coding .....                             | 79        |
| E.5.2.2                       | Parameters in ProSe key management messages .....  | 79        |

|  |  |           |
|--|--|-----------|
| E.5.2.2.1  | Transaction ID.....                                | 79        |
| E.5.2.2.2  | Supported Algorithm.....                           | 79        |
| E.5.2.2.3  | Group ID .....                                     | 80        |
| E.5.2.2.4  | PGK ID .....                                       | 80        |
| E.5.2.2.5  | Error Code.....                                    | 80        |
| E.5.2.2.6  | Group Member ID.....                               | 81        |
| E.5.2.2.7  | Algorithm Info .....                               | 81        |
| E.5.2.2.8  | PMK ID.....  | 81        |
| E.5.2.2.9  | PMK.....   | 81        |
| E.5.2.2.10   | PRUK ID.....                                       | 81        |
| E.5.2.2.11   | PRUK.....  | 81        |
| E.5.2.2.12   | IMSI .....   | 81        |
| E.5.2.2.13   | Relay Service Code.....                            | 81        |
| E.5.2.2.14   | MSISDN .....                                       | 82        |
| E.5.2.2.15   | Nonce 1 .....                                      | 82        |
| E.5.2.2.16   | RAND .....   | 82        |
| E.5.2.2.17   | AUTS .....   | 82        |
| E.5.2.2.18   | Key $K_D$ .....                                    | 82        |
| E.5.2.2.19   | $K_D$ Freshness parameter .....                    | 82        |
| E.5.2.2.20   | GPI.....   | 82        |
| E.5.2.2.21   | Remote UE other identity.....                      | 82        |
| E.5.2.2.22   | Public Safety Discovery Security Capabilities..... | 82        |
| E.5.2.2.23   | Relay Service Code .....                           | 82        |
| E.5.2.2.24   | PSDK ID .....                                      | 83        |
| E.5.2.2.25   | Discovery Group ID.....                            | 83        |
| E.5.2.2.26   | Protection Profile .....                           | 83        |
| E.5.2.2.27   | Encrypted bit mask.....                            | 83        |
| E.5.2.2.28   | Key Type ID.....                                   | 83        |
| E.5.2.2.29   | Current time .....                                 | 83        |
| E.5.2.2.30   | Max Offset .....                                   | 83        |
| <b>Annex F (Informative): Network options for PC3 security .....</b>                                       |  | <b>84</b> |
| F.1  | General .....                                      | 84        |
| F.2  | Prose Function using standalone BSF.....           | 84        |
| F.3  | BSF - Prose Function/NAF colocation.....           | 84        |
| F.4  | Prose Function with bootstrapping entity.....      | 85        |
| <b>Annex G (Informative): Protection of Restricted Discovery and Public Safety Discovery messages.....</b> |  | <b>87</b> |
| G.1  | General .....                                      | 87        |
| G.2  | Different combinations of security mechanisms..... | 87        |
| <b>Annex H (informative): Change history .....</b>   |  | <b>89</b> |
| History .....  |  | 92        |

---

# Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> 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.

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/121d08a5-3ff7-4d5b-b63e-3859fdac697a/etsi-ts-133-303-v13.5.0-2017-07>

---

# 1 Scope

The present document specifies the security aspects of the Proximity Services (ProSe) features in EPS. Based on the common security procedures (clause 5) for

- interfaces between network entities (using NDS),
- configuration of ProSe-enabled UEs, and
- data transfer between the ProSe Function and a ProSe enabled UE (PC3 interface)

security for the following ProSe features is covered:

- Open ProSe Direct Discovery in network coverage (clause 6.1);
- One-to-many ProSe direct communication for ProSe-enabled Public Safety UEs (clause 6.2);
- EPC-level Discovery of ProSe-enabled UEs (clause 6.3);
- EPC support for WLAN Direct Discovery and Communication (clause 6.4) ;
- One-to-one ProSe direct communication for ProSe-enabled Public Safety UEs (clause 6.5);
- Prose Public Safety Discovery (clause 6.6);
- Prose UE-to-network relays (clause 6.7);

---

# 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 23.303: "Proximity-based services (ProSe); Stage 2".
- [3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".
- [4] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".
- [5] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".
- [6] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".
- [7] ETSI TS 102 226: "Smart cards; Remote APDU structure for UICC based applications".
- [8] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".
- [9] 3GPP TS 31.116: "Remote APDU Structure for (U)SIM Toolkit applications ".
- [10] Void.
- [11] Void.

- [12] IETF RFC 6509: "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)".
- [13] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".
- [14] IETF RFC 6507: "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)".
- [15] NIST FIPS 186-4: "Digital Signature Standard (DSS)".
- [16] BSI TR-03111: "Technical Guideline TR-03111; Elliptic Curve Cryptography".
- [17] IETF RFC 5639: "Elliptic Curve Cryptography (ECC) Brainpool Standard; Curves and Curve Generation".
- [18] IETF RFC 3339: "Date and Time on the Internet: Timestamps".
- [19] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [20] NIST FIPS 180-4: "Secure Hash Standard (SHS)".
- [21] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".
- [22] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".
- [23] Void.
- [24] IETF RFC 6508: "Sakai-Kasahara Key Encryption (SAKKE)".
- [25] Void.
- [26] Void.
- [27] Void.
- [28] Void.
- [29] Void.
- [30] Void.
- [31] IETF RFC 5116: "An Interface and Algorithms for Authenticated Encryption".
- [32] Void.
- [33] Void.
- [34] Void.
- [35] IETF RFC 4563: "The Key ID Information Type for the General Extension Payload in Multimedia Internet KEYing (MIKEY)".
- [36] W3C REC-xmlschema-2-20041028: "XML Schema Part 2: Datatypes".
- [37] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".
- [38] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".
- [39] 3GPP TS 23.003: "Numbering, addressing and identification".
- [40] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".
- [41] 3GPP TS 29.368: "Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS)".

- [42] 3GPP TS 33.102: "3G Security; Security architecture".
- [43] 3GPP TS 33.179: "Security of Mission Critical Push-To-Talk (MCPTT)".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 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 TR 21.905 [1].

**Application Level Container:** See 3GPP TS 23.303 [2]

**Discovery Filter:** See [2]

**Discovery Group ID:** See [2]

**ProSe Application ID:** See [2]

**ProSe Application Code:** See [2]

**ProSe Application Mask:** See [2]

**ProSe Direct Communication:** See [2]

**ProSe Direct Discovery:** See [2]

**ProSe-enabled non-Public Safety UE:** See [2]

**ProSe-enabled Public Safety UE:** See [2]

**ProSe-enabled UE:** See [2]

**ProSe Query Code:** See [2]

**ProSe Response Code:** See [2]

**ProSe Restricted Code:** See [2]

**Relay Service Code:** See [2]

**Restricted ProSe Application User ID:** See [2]

**Validity Timer:** See [2]

### 3.2 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].

|       |   |
|-------|---|
| ADF   | Accounting Data Forwarding  |
| ALUID | Application Layer User ID   |
| AS    | Application Server  |
| BSF   | Bootstrapping Server Function   |
| CA    | Certificate Authority   |
| CTF   | Charging Trigger Function   |
| DSA   | Digital Signature Algorithm   |
| ECCSI | Elliptic Curve-based Certificateless Signatures for Identity-based Encryption |

|        |                                      |
|--------|--------------------------------------|
| ECDSA  | Elliptic Curve DSA                   |
| EPUID  | EPC Level User ID                    |
| GBA    | Generic Bootstrapping Architecture   |
| GMK    | Group Master Key                     |
| GPS    | Global Positioning System            |
| GSK    | Group Session Key                    |
| ID     | Identity                             |
| KMS    | Key Management System                |
| LCID   | Logical Channel Identifier           |
| MIC    | Message Integrity Code               |
| MIKEY  | Multimedia Internet Keying           |
| NAF    | Network Application Function         |
| NITZ   | Network Identity and Time Zone       |
| NTP    | Network Time Protocol                |
| OTA    | Over The Air                         |
| PEK    | ProSe Encryption Key                 |
| PIK    | ProSe Integrity Key                  |
| PFID   | ProSe Function ID                    |
| PGK    | ProSe Group Key                      |
| ProSe  | Proximity-based Services             |
| PSDK   | Public Safety Discovery Key          |
| PTK    | ProSe Traffic Key                    |
| RPAUID | Restricted ProSe Application User ID |
| RSC    | Relay Service Code                   |
| RTP    | Real-Time Transport Protocol         |
| RTCP   | RTP Control Protocol                 |
| SAKKE  | Sakai-Kasahara Key Encryption        |
| SDP    | Session Description Protocol         |
| SEG    | Security Gateway                     |
| SRTP   | Secure Real-Time Transport Protocol  |
| UID    | User ID                              |
| UTC    | Universal Time Coordinated           |

INTERNET STANDARD PREVIEW  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/121d08a5-3ff7-4d5b-b63e-3859fdac697a/etsi-ts-133-303-v13.5.0-2017-07>

---

## 4 Overview of ProSe security

### 4.1 General

The overall architecture for ProSe is given in TS 23.303 [2]. 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.

Although made of several different features, those features share many procedures, for example, both ProSe Direct Discovery and ProSe Direct Communication utilize the same procedure for service authorization (see TS 23.303 [2]). Security for this common procedures are described in clause 5 of the present document, while the overall security of the ProSe features is described in clause 6 of the present document (which refers back to clause 5 as necessary).

### 4.2 Reference points and Functional Entities

- PC8:** The reference point between the UE and the ProSe Key Management Function. PC8 relies on EPC user plane for transport (i.e. an "over IP" reference point). It is used to transport security material to UEs for ProSe one-to-many communications.

---

## 5 Common security procedures

### 5.1 General

This clause contains a description of the security procedures that are used by more than one ProSe feature.

### 5.2 Network domain security

#### 5.2.1 General

ProSe uses several interfaces between network entities, e.g. PC4a between the ProSe Function and the HSS (see TS 23.303 [2]). This subclause describes the security for those interfaces.

#### 5.2.2 Security requirements

The ProSe network entities shall be able to authenticate the source of the received data communications.

The transmission of data between ProSe network entities shall be integrity protected.

The transmission of data between ProSe network entities shall be confidentiality protected.

The transmission of data between ProSe network entities shall be protected from replays.

#### 5.2.3 Security procedures

For all interfaces between network elements,

TS 33.210 [3] shall be applied to secure signalling messages on the reference points unless specified otherwise, and

TS 33.310 [4] may be applied regarding the use of certificates with the security mechanisms of TS 33.210 [3] unless specified otherwise in the present document.

**NOTE:** For the case of an interface between two entities in the same security domain, TS 33.210 [3] does not mandate the protection of the interface by means of IPsec.