

# ETSI TS 133 535 V18.8.0 (2025-07)



TECHNICAL SPECIFICATION

**5G;**  
**Authentication and Key Management for Applications (AKMA)**  
**based on 3GPP credentials in the 5G System (5GS)**  
**(3GPP TS 33.535 version 18.8.0 Release 18)**

[ETSI TS 133 535 V18.8.0 \(2025-07\)](https://standards.iteh.ai/catalog/standards/etsi/c92650e8-5753-486c-a16c-95860b5c03a6/etsi-ts-133-535-v18-8-0-2025-07)

<https://standards.iteh.ai/catalog/standards/etsi/c92650e8-5753-486c-a16c-95860b5c03a6/etsi-ts-133-535-v18-8-0-2025-07>



---

**Reference**RTS/TSGS-0333535vi80

---

**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. [2025-07](#)

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 Architecture for AKMA .....	9
4.1 Reference model.....	9
4.2 Network elements.....	10
4.2.1 AAnF .....	10
4.2.2 AF .....	11
4.2.3 NEF.....	11
4.2.4 AUSF .....	11
4.2.5 UDM.....	11
4.3 AKMA Service Based Interfaces(SBIs).....	11
4.3.0 General.....	11
4.3.1 Void .....	11
4.4 Security requirements and principles for AKMA.....	12
4.4.0 General .....	12
4.4.1 Requirements on Ua* reference point.....	12
4.4.2 Requirements on AKMA Key Identifier (A-KID).....	12
4.4.3 Requirements on the UE.....	12
4.5 AKMA reference points .....	13
4.6 Roaming .....	13
4.6.1 AKMA roaming requirements .....	13
4.7 Use of Authentication Proxy (AP) .....	13
4.7.1 Architecture of using AP .....	13
4.7.2 AP-AS reference point.....	14
4.7.3 Example of using AP for TLS tunnels.....	15
5 Key management.....	15
5.1 AKMA key hierarchy.....	15
5.2 AKMA key lifetimes.....	16
6 AKMA Procedures .....	16
6.1 Deriving AKMA key after primary authentication .....	16
6.2 Deriving AKMA Application Key for a specific AF .....	18
6.2.1 AAnF response with UE Identity.....	18
6.2.2 AAnF response without UE Identity.....	19
6.3 AKMA Application Key request via NEF .....	20
6.4 AKMA key change.....	21
6.4.1 $K_{AKMA}$ re-keying .....	21
6.4.2 $K_{AF}$ re-keying.....	21
6.4.3 $K_{AF}$ refresh .....	21
6.4.4 $K_{AKMA}$ refresh .....	21
6.5 Initiation of AKMA.....	21
6.6 AAnF AKMA context removal.....	22
6.6.1 General.....	22
6.7 AAnF Discovery and Selection.....	23
6.8 Notification about AKMA service disabling.....	23

6.8.1	Notification to internal AF about AKMA service disabling .....	23
6.8.2	Notification to external AF about AKMA service disabling .....	25
7	Security related services .....	26
7.1	Services provided by AAnF .....	26
7.1.1	General.....	26
7.1.2	Naanf_AKMA_AnchorKey_Register service operation .....	26
7.1.3	Naanf_AKMA_ApplicationKey_Get service operation .....	26
7.1.4	Naanf_AKMA_Context_Remove operation.....	26
7.1.5	Naanf_AKMA_ApplicationKey_AnonUser_Getservice operation .....	27
7.1.6	Naanf_AKMA_ServiceDisableNotification service operation .....	27
7.2	Void.....	27
7.3	Services provided by NEF.....	27
7.3.1	General.....	27
7.3.2	Nnef_AKMA_ApplicationKey_Get service operation .....	27
7.3.3	Nnef_AKMA_ServiceDisableNotification service operation.....	28
7.4	Services provided by UDM .....	28
<b>Annex A (normative): Key derivation functions.....</b>		<b>29</b>
A.1	KDF interface and input parameter construction .....	29
A.1.1	General .....	29
A.1.2	FC value allocations .....	29
A.2	$K_{AKMA}$ derivation function.....	29
A.3	A-TID derivation function.....	29
A.4	$K_{AF}$ derivation function .....	30
B.1	TLS based protocols.....	31
B.1.1	General .....	31
B.1.2	Shared key-based UE authentication with certificate-based AF authentication .....	31
B.1.2.1	General.....	31
B.1.2.2	Procedures.....	31
B.1.3	Shared key-based mutual authentication between UE and AF.....	31
B.1.3.1	General.....	31
B.1.3.2	Procedures.....	32
B.1.3.2.1	Procedures for TLS 1.2 .....	32
B.1.3.2.2	Procedures for TLS 1.3 .....	32
<b>Annex C (normative): AKMA Ua* protocol based on DTLS.....</b>		<b>33</b>
C.1	General .....	33
C.1.1	Requirement on the UE .....	33
C.1.2	Requirement on the AF .....	33
C.2	Shared key-based mutual authentication between UE and AF.....	33
C.2.1	General .....	33
C.2.2	Procedures for DTLS 1.3.....	33
<b>Annex D (normative): Ua* security protocol: Object Security for Constrained RESTful Environments (OSCORE).....</b>		<b>34</b>
D.1	General .....	34
D.2	Requirements.....	34
D.2.1	General .....	34
D.2.2	Requirements on the UE.....	34
D.2.3	Requirements on the AF.....	34
D.2.4	Requirements on the OSCORE .....	34
D.3	IETF OSCORE as an AKMA Ua* protocol.....	34
D.3.1	General .....	34
D.3.2	Procedures .....	34
D.3.3	OSCORE Security context .....	35

D.3.4 Refresh of OSCORE key material.....35  
D.3.5 OSCORE Ua\* protocol payload encoding .....36  
**Annex E (informative): Change history .....37**  
History .....40

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

[ETSI TS 133 535 V18.8.0 \(2025-07\)](#)

<https://standards.iteh.ai/catalog/standards/etsi/c92650e8-5753-486c-a16c-95860b5c03a6/etsi-ts-133-535-v18-8-0-2025-07>