|  |
| --- |
| 3GPP TS 33.535 V0.3.0 (2020-03) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Authentication and key management for applications; based on 3GPP credential in 5G （AKMA）(Release 16) |
|   |
| *5G-logo_175px* | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2019, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Architecture for Authentication and Key Management for Applications (AKMA) 7

4.1 Reference model 7

4.2 Network elements 7

4.2.1 AAnF 7

4.2.2 AF 7

4.2.3 NEF 7

4.3 Interface description 8

4.3.1 Reference point Ua\* 8

4.4 Security requirements and principles for AKMA 8

4.3.1 Requirenments on Ua\* Reference point 8

5 Key Management 9

5.1 AKMA key hierarchy 9

5.2 AKMA key lifetimes 9

6 AKMA Procedures 9

6.1 Deriving AKMA key during UE registration 9

6.2 Deriving AKMA Application key for a specific AF 11

Annex A (normative): Key derivation functions 12

A.1 KDF interface and input parameter construction 12

A.1.1 General 12

A.1.2 FC value allocations 12

A.2 KAKMA derivation function 12

Annex <X> (informative): Change history 12

# 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.

# Introduction

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

The present document specifies the security features and mechanisms to support authentication and key management aspects for applications based on subscription credential(s) in 5G system as defined in 33.501[2].

# 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 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP TS 23.501: "System Architecture for the 5G System".

[4] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

Definition format (Normal)

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

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

## 3.2 Symbols

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

Symbol format (EW)

<symbol> <Explanation>

## 3.3 Abbreviations

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

AAnF AKMA Anchor Function

AF Application Function

AMFAccess and Mobility Management Function

AUSFAUthentication Server Function

NEFNetwork Exposure Function

UDM Unified Data Management

# 4 Architecture for Authentication and Key Management for Applications (AKMA)

Editor’s Note: Titles and Numberings of sub clauses could be adjusted according to the content.

## 4.1 Reference model

Figure 4.1-1 shows a fundamental network model of AKMA, as well as the interfaces between them.



Figure 4.1-1: Fundamental Network Model for AKMA

NOTE: Figure 4.1-1 shows the case where AAnF is deployed as a standalone function. Deployments can choose to collocate AAnF with AUSF or with NEF according to operators’ deployment scenarios.

The AKMA service requires a new logical entity: AKMA Anchor Function (AAnF).

AAnF is the anchor function in the HPLMN that generates the key material to be used between the UE and the AF and maintains UE AKMA contexts to be used for subsequent bootstrapping requests.

## 4.2 Network elements

Editor’s Note: This clause will describe the functionalities and requirements of each entities in the reference model.

### 4.2.1 AAnF

AAnF enables the AKMA anchor key (KAKMA) derivation for AKMA service. Before invoking AKMA service, UE shall have successfully registered to the 5G core, which results in KAUSF being stored at the AUSF and the UE after a successful 5G primary authentication.

### 4.2.2 AF

AF is defined in TS 23.501 [3] with the additional functions:

- AF with the AKMA service enabling requests for KAF from the AAnF using AKMA key Identifier.

### 4.2.3 NEF

NEF is defined in TS 23.501[3] with the additional functions:

- NEF finds the AAnF.

## 4.3 Interface description

The following interfaces are involved in AKMA network architecture:

* **Nnef:** Service-based interface exhibited by NEF.
* **Nausf:** Service-based interface exhibited by AUSF.
* **Nudm:** Service-based interface exhibited by UDM.
* **Naanf:** Service-based interface exhibited by AAnF.
* **Naf:** Service-based interface exhibited by AF.

The AAnF interacts with the AUSF and the AF using Service-Based Interfaces. When the AF is located in the operator’s network, the AAnF shall use Service-Based Interface to communicate with the AF directly. When the AF is located outside the operator’s network, the NEF shall be used to exchange the messages between the AF and the AAnF.

### 4.3.1 Reference point Ua\*

The reference point Ua\* carries the application protocol, which is secured using the key material agreed between UE and AAnF as a result of successful AKMA procedures.

Editor’s Note: It is expected that the existing GBA based Ua protocols are reused with necessary adaptations as the Ua\* for AKMA. The changes required for Ua\* are FFS.

## 4.4 Security requirements and principles for AKMA

The following security requirements are applicable to AKMA:

- AKMA shall reuse the same UE subscription and the same credentials used for 5G access.

-    AKMA shall reuse the 5G primary authentication procedure and methods (both 5G AKA and EAP AKA’ shall be supported) for the sake of implicit authentication for AKMA services.

 -    AAnF’s SBI interface to AUSF shall be confidentiality, integrity and replay protected.

-    The interface between AAnF and AF shall be confidentiality, integrity and replay protected.

-    The application key shall be provided with a maximum lifetime. When the application key lifetime is expired, it shall be renegotiated.

Editor’s Note: Further security requirements regarding roaming and other aspects will be added.

### 4.3.1 Requirenments on Ua\* Reference point

The Ua\* reference point is application specific. The generic requirements for Ua\* are:

* Ua\* protocol shall be able to carry AKMA Key Identifier (A-KID);
* the UE and the AKMA AF shall be able to secure the reference point Ua\* using the AMKA AF specific shared key derived from AKMA key;

NOTE: The exact method of securing the reference point Ua\* depends on the application protocol used over reference point Ua\*.

* the AKMA AF shall be able to indicate to the UE that the current shared secret has expired, and the UE should use newer shared secret with the AKMA AF;

Editor’s Note: Further requirements (including the need to specify Ua\* protocol identifier) are FFS.

# 5 Key Management

Editor’s Note: Sub clauses will be added according to the conclusions made in TR 33.835.

## 5.1 AKMA key hierarchy

Editor’s Note: This clause needs further details.

The key hierarchy (see Figure 5.1-1) includes the following keys: KAUSF, KAKMA, KAF. KAUSF is generated by AUSF as specified in clause 6 of TS 33.501 [2].

Keys for AAnF:

 KAKMA is a key derived by ME and AUSF from KAUSF.

Keys for AF:

 KAF is a key derived by ME and AAnF from KAKMA.

KAKMA and KAF are derived according to the procedures of clause 6.1 and 6.2.



Figure 5.1-1: AKMA Key Hierarchy

## 5.2 AKMA key lifetimes

The KAKMA is valid until the next primary authentication is performed (implicit lifetime), in which case the KAKMA might be replaced after a successful new authentication or removed after an unsuccessful one.

Application keys KAF shall use explicit lifetimes based on operator’s policy. The lifetime of KAF shall be sent by the AAnF as described in clause 6.2. In case that a new anchor key KAKMA is established, the application key KAF can continue to be used until its lifetime expires. When the KAF lifetime expires, a new application key is established based on the current anchor key KAKMA.

# 6 AKMA Procedures

## 6.1 Deriving AKMA key during UE registration

There is no separate authentication of the UE to support AKMA functionality. Instead, it reuses the 5G primary authentication procedure executed during the UE Registration to authenticate the UE. A successful 5G primary authentication results in KAUSF being stored at the AUSF and the UE.



Figure 6.1-1 Deriving AKMA root key during UE registration

The AUSF shall generate the AKMA Anchor Key (KAKMA) and the associated key Identifier from KAUSF as part of the UE Registration procedure.

The UE shall generate the AKMA Anchor Key (KAKMA) and the associated key Identifier from the KAUSF before initiating communication with an AKMA Application Function.

The KAKMA key identifier identifies the KAKMA key of the UE from which other AKMA keys are derived.

The KAKMA key identifier shall be NAI.

The key derivation of KAKMA shall be performed using the key derivation function (KDF) specified in TS 33.220 [4]. KAKMA is computed (as per Annex A.2) as KAKMA=KDF (KAUSF, "AKMA", SUPI), where the key derivation parameters consist of a static string "AKMA", and SUPI.

Editor’s Note: Format and derivation of KAKMA key identifier and its association with UE identifier is FFS.

Editor’s Note: Whether the AUSF generates the KAKMA key identifier and the associated AKMA Anchor Key (KAKMA) during the primary authentication or as needed (i.e., on-demand), is FFS.

Since AKMA keys are based on KAUSF from primary authentication run, the AKMA keys can only be refreshed by running a fresh primary authentication.

## 6.2 Deriving AKMA Application key for a specific AF



Figure 6.2-1 AF Key generation from KAKMA

Before communication between the UE and the AKMA AF can start, the UE and the AKMA AF needs to know whether to use AKMA. This knowledge is implicit to the specific application on the UE and the AKMA AF.

Editor’s Note: It is FFS whether the capability to negotiate the use of AKMA between the UE application and the AKMA AF also needs to be supported.

When the UE initiates communication with the AKMA AF, it shall include the derived AKMA key identifier (KAKMA ID) in the message (cf. clause 6.1).

If the AF does not have an active context associated with the key identifier, then the AF sends a request to AAnF with the key identifier to request application function specific AKMA keys for the UE. The AF also includes its identity (AF Id) in the request. The AAnF shall check whether the AAnF can provide the service to the AF by checking the AF Id. If succeeds, the following procedures is excuted. Otherwise, the AAnF shall reject the procedure.

Editor’s Note: It is FFS how the AAnF knows whether it can provide the service to a specific AF

If the AAnF is in possession of the AF specific key (KAF), it responds to the AF with the KAF key. If not, the AAnF shall check if it has the UE specific KAKMA key identified by the AKMA key identifier.

If KAKMA is available in AAnF, it shall derive the AF specific AKMA key (KAF) from KAKMA and respond to the AF with KAF and lifetime.

If KAKMA is not available, the AAnF shall send a request to the AUSF to obtain the KAKMA key specific to the UE. It includes the AKMA key identifier in the request. The AUSF shall respond with the KAKMA key identified by the key identifier. The AAnF derives the AF specific key (KAF) from KAKMA and responds to the AF with KAF and lifetime.

Editor’s Note: Derivation of the AF specific KAF is FFS.

Annex A (normative): Key derivation functions

# A.1 KDF interface and input parameter construction

## A.1.1 General

All key derivations for AKMA shall be performed using the key derivation function (KDF) specified in Annex B.2.0 of TS 33.220 [4].

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 [4].

## A.1.2 FC value allocations

The FC number space used is controlled by TS 33.220 [4], FC values allocated for the present document are in range of 0x7A – 0x7F.

# A.2 KAKMA derivation function

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

- FC = 0x7A;

- P0 = "AKMA";

- L0 = length of "AKMA"; (i.e. 0x00 0x04)

- P1 = SUPI;

- L1 = length of SUPI.

The input key KEY shall be KAUSF.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-10 | SA3 #96adhoc | S3-193817 |  |  |  | TS skeleton based on S3-193769; Scope is based on S3-193770; Other content including S3-193841, S3-193772 | 0.1.0 |
| 2019-11 | SA3 #97 | S3-194640 |  |  |  | Updates based on S3-194340, S3-194160, S3-194641, S3-194642, S3-194643, S3-194341, S3-194644, S3-194645, S3-194229, S3-194156 | 0.2.0 |
| 2020-03 | SA3 #98e | S3-200511 |  |  |  | Updates based on S3-200511, S3-200512, S3-200499, S3-200249, S3-200460, S3-200461, S3-200463, S3-200447, S3-200486, S3-200364, S3-200366, S3-200513 | 0.3.0 |