**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *draft\_S3-231841-r1***

**Electronic meeting, Online, 17 - 21 April 2023** (revision of S3-yyxxxx)

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.535** | **CR** | **draftCR** | **rev** | **<->** | **Current version:** | **17.8.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)*** *on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Living document for AKMA DTLS to TS 33.535 |
|  |  |
| ***Source to WG:*** | ZTE |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | AKMA\_GBA\_DTLS |  | ***Date:*** | 2023-4-6 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | In order to complete the work on the DTLS for AKMA Ua\* protocol, it is required to add a dedicated annex in 3GPP TS 33.535 including description about Shared key-based mutual authentication between UE and AF.  |
|  |  |
| ***Summary of change:*** | Addition of a new annex including the skeleton of DTLS for AKMA Ua\* protocol |
|  |  |
| ***Consequences if not approved:*** | Incomplete work for the DTLS for AKMA Ua\* protocol |
|  |  |
| ***Clauses affected:*** | 2, Annex X (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This draft CR's revision history:*** | SA3#110 Adhoc: |

\*\*\*\* Start of Change1\*\*\*\*

Annex X (normative):
AKMA Ua\* protocol based on DTLS

## X.1 General

This Annex covers the aspects specific to the AKMA Ua\* protocol based on DTLS. This feature is optional to be supported for the UE and AF. If the feature is supported, the following clauses apply.

#### X.1.1 Requirement on the UE

UE hosts the DTLS client. The UE should be able to indicate to the AF which key (KAF) the UE intends to use to secure the Ua\* reference point based on DTLS.

#### X.1.2 Requirement on the AF

DTLS should be supported by the AF for the UE-AF reference point (Ua\*).

The AF should be able to require that a certain key (i.e., KAF) used to secure the Ua reference point based on DTLS.

## X.2 Shared key-based mutual authentication between UE and AF

#### X.2.1 General

The TLS profile specified in TS 33.210 [y] clause 6.2 apply to DTLS 1.3[x].

#### X.1.3.3 Procedures for DTLS 1.3

The procedures given in B.1.3.2.2for TLS 1.3 is also applicable for DTLS 1.3.

AKMA PSK identity should be delivered via DTLS message.

The UE derives the DTLS premaster secret from the KAF.

\*\*\*\* End of Change 1\*\*\*\*

\*\*\*\* Start of Change 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)".

[5] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[6] IETF RFC 7542: "The Network Access Identifier".

[7] 3GPP TS 33.222: " Generic Authentication Architecture (GAA); Access to network application functions using HypertextTransfer Protocol over Transport Layer Security (HTTPS)".

[8] Void

[9] 3GPP TS 23.003: "Numbering, addressing and identification".

[10] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[11] 3GPP TS 29.503: "5G System; Unified Data Management Services ".

[x] IETF RFC 9146: "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3"

[y] 3GPP TS 33.210: "3G Security; Network Domain Security; IP network layer security".

\*\*\*\* End of Changes\*\*\*\*