**3GPP TSG-SA3 Meeting #108-e *draft\_S3-221896-r1***

e-meeting, 22 - 26 August 2022 (revision of S3-yyxxxx)

**Source: ZTE**

**Title: New WID on DTLS Ua\* protocol profile for AKMA**

**Document for: Agreement**

**Agenda Item: 6**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: IETF DTLS Ua\* protocol profile for AKMA

Acronym: AKMA\_DTLS

Unique identifier: TBD

Potential target Release: Rel-18

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X |  | X |  |
| No |  |  | X |  |  |
| Don't know | X |  |  |  | X |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | Feature |
|  | Building Block |
|  | *Work Task* |
|  | Study Item |

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A | N/A | N/A | N/A |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| 890030 | Authentication and key management for applications based on 3GPP credential in 5G | Uses the keys derived by the AKMA procedures to bootstrap the IETF DTLS protocol key material.  |

**Dependency on non-3GPP (draft) specification:** IETF RFC 7252, 6347

# 3 Justification

The AKMA specification (TS 33.535) enables a UE and an Application Function to share a common secret key after an application session establishment procedure. However, no application session protocol (Ua\*) has been standardized yet especially for the IoT types of devices. One choice for an IoT friendly protocol is the IETF DTLS specified in IETF RFC 7252 using the IETF CoAP as an underlying transfer layer. And in SEAL specification TS 33.434, communication security for CoAP is based on DTLS or OSCORE. The security of CoAP is based on DTLS, which is specified in RFC 6347. IETF DTLS is currently specified as one choice for providing security for the OMA Lightweight M2M standard.

# 4 Objective

To provide an IoT friendly Ua\* security protocol profile based on the already specified IETF DTLS. The specification will focus on how to use the common AKMA KAF key to bootstrap the security context of IETF DTLS.

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| TS 33.535 | Specification of the new IoT Ua\* security protocol based on IETF DTLS | SA#98 (December 2022) |  |
| TS 33.220 | Addition of the new Ua security protocol identifier for the new AKMA IETF DTLS Ua\* security protocol  | SA#98 (December 2022) |  |

# 6 Work item Rapporteur(s)

Liu, yuze, ZTE, liu.yuze@zte.com.cn

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

CT1 to provide stage 3 details of the Ua\* protocol.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| ZTE |
| CMCC |
| China Telecom |
| VIVO |
| OPPO |
| China Unicom |
| CATT |