**3GPP TSG-CT WG1 Meeting #133e-bisC1-220xxx**

**E-meeting, 17-21 January 2022 (was C1-220052)**

**Source: Qualcomm Incorporated, China Mobile**

**Title: New WID on CT aspects of AKMA TLS protocol profiles**

**Document for: Approval**

**Agenda Item: 17.1.1**

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: CT aspects of AKMA TLS protocol profiles

## Acronym: AKMA\_TLS

## Unique identifier: TBD

Potential target Release: Rel-17

## 1 Impacts

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

## 2 Classification of the Work Item and linked work items

### 2.1 Primary classification

This work item is a …

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

### 2.2 Parent Work Item

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| AKMA\_TLS | SA3 | 920027 | AKMA TLS protocol profiles |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work Items (if any) |
| Unique ID | Title | Nature of relationship |
| 910024 | Enhancements of 3GPP profiles for cryptographic algorithms and security protocols | Defines Stage 2 of TLS 1.3 with GBA keys which is used as the basis for TLS 1.3 using AKMA keys  |
| 940007 | Enhancements of 3GPP profiles for cryptographic algorithms and security protocols | Defines Stage 3 of TLS 1.3 with GBA keys which is used as the basis for TLS 1.3 using AKMA keys |

**Dependency on non-3GPP (draft) specification**:

- Internet draft draft-ietf-tls-dtls13: " The Datagram Transport Layer Security (DTLS) Protocol Version 1.3".

## 3 Justification

The AKMA specification (TS 33.535) enables the derivation of application specific keys based on an authentication of a UE connected to 5GS. SA3 has agreed in S3-212352 a Rel-17 Work Item to create a profile of protocols similar to the ones defined in TS 24.109 for GBA (e.g. TLS protocols) to use the AKMA keys, and the work was completed in November 2021. A corresponding stage 3 work item is needed to update the stage 3 in CT1 specification.

## 4 Objective

The objectives of this Work Item are to:

- provide an AKMA based profile of the TLS similar to GBA profiles that are currently specified in TS 24.109 to enable the use of these protocols with AKMA derived keys.

- once a GBA based profile for TLS 1.3 is added to TS 24.109 as part of the eCryptPr Work Item, add an AKMA based profile for TLS 1.3.

NOTE: The AKMA based profile should be compatible with the GBA one such that it is possible to enable a choice of AKMA or GBA keys.

## 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 |
| 24.109 | Addition of profiles of TLS using AKMA keys to an annex of TS 24.109 | TSG CT#95 (March 2022) |  |

## 6 Work item Rapporteur(s)

Chaponniere, Lena, Qualcomm Incorporated, lguellec@qti.qualcomm.com

## 7 Work item leadership

CT1

## 8 Aspects that involve other WGs

None identified yet

## 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Qualcomm Incorporated |
| China Mobile |
| Nokia |
| Nokia Shanghai Bell |
| Ericsson |
| ZTE |