**3GPP TSG-CT WG1 Meeting #135-eC1-22xxxx**

**E-Meeting, 6th – 12th April 2022 (was C1-222712)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Adding AKMA based profile for TLS 1.3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA\_TLS | | | | |  | ***Date:*** | | | 2022-04-06 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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 can be 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:*** | | SA3 has specified the use of TLS 1.3 with AKMA keys (see S3-214132). Hence to complete the work on AKMA TLS protocol profiles, an AKMA based profile for TLS 1.3 needs to be added to Annex K of TS 24.109. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | An AKMA based profile for TLS 1.3 was added to Annex K of TS 24.109. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | It will not be possible to use TLS 1.3 with AKMA derived keys. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | K.3.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 CR's revision history:*** | |  | | | | | | | | |

\* \* \* First Change \* \* \* \*

## K.3.3 TLS 1.3

The PSK TLS handshake shall be used with bootstrapped security association as follows:

1) The UE shall include in the ClientHello message:

a) an indication that it supports the TLS with PSK authentication using the "psk\_key\_exchange\_modes" extension;

b) the hostname of the AF using the "server\_name" TLS extension;

c) authentication methods other than PSK which the UE supports; and

d) PSK identities within the psk\_identities field. The psk\_identity parameter within the psk\_identities field shall contain a prefix indicating the PSK identity name space, i.e. "3GPP-AKMA", a separator character ";" and the A-KID;

The UE shall derive the TLS external PSK from the AF specific key KAF.

2) If the AF is willing to establish a TLS tunnel using PSK authentication with AKMA keys, the AF shall reply with the ServerHello message and indicate the index of the AKMA psk\_identity parameter. The AF concludes the TLS handshake by sending Finished message to the UE.

NOTE 1: The choice between AKMA and AKA-based GBA at the UE and the AF, if both are supported, is application dependent.

The AF shall derive the TLS external PSK from the AF specific key KAF.

3) The UE concludes the TLS handshake by sending Finished message to the AF.

Once the UE and the AF have established a TLS tunnel using AKMA-based shared secret, they may start to use the application level communication through this tunnel.

The authentication failures are supported as described in clause 5.3.3.2.

Clauses 5.3.3.3 and 5.3.3.4 are not supported as AKMA does not support deriving a fresh key in the same way as GBA.

NOTE 2: How a fresh key is derived for AKMA is up to Ua\* protocol implementation.

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