**3GPP TSG-SA3 Meeting #104-e *S3-212841r1***

**e-meeting, 16 - 27 August 2021 *merger of S3-212841 and S3-212536***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.535** | **CR** | **0099** | **rev** | **1-** | **Current version:** | **17.2.1** |  |
|  | | | | | | | | |
| *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 TLS 1.3 with AKMA keys | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA\_TLS | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | |  |
|  | *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:*** | | TLS 1.3 with AKMA is not supported. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add TLS 1.3 with AKMA support. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | B.1.3.2.1 (new), B.1.3.2.2 (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 CR's revision history:*** | |  | | | | | | | | |

**\*\*\*\* START OF CHANGES \*\*\*\***

B.1.3.2 Procedures

#### B.1.3.2.1 Procedures for TLS 1.2

The procedures follow those given in clause 5.4.0.1 of TS 33.222 [7] with the AKMA AF taking the role of the NAF from GBA (see TS 33.220 [4]), with the following changes.

At step 2, the AF shall include a constant string "3GPP-AKMA" is used as PSK-identity hint to indicate that AKMA based keying is supported.At step 3, the UE may use an AKMA generated key if support was indicated by the AF (even if GBA-based were also indicated as supported by the AF). To use as AKMA generated key, the UE shall TLS premaster secret from KAF and shall send a ClientKeyExchange message including a PSK identity consisting of "3GPP-AKMA" and the A-KID.

At step 4, if the AF receives the "3GPP-AKMA" prefix and the A-KID in the ClientKeyExchange messages it fetches the AF specific shared secret (KAF) from the AAnF using the A-KID. The AF shall derive the TLS premaster secret from the AF specific key (KAF).

#### B.1.3.2.2 Procedures for TLS 1.3

The procedures follow those given in clause 5.4.0.2 of TS 33.222 [7] with the AKMA AF taking the role of the NAF from GBA (see TS 33.220 [4]), with the following changes.At step 1, when a UE contacts an AF, it may indicate to the AF that it supports TLS with PSK authentication in the ClientHello message. The UE shall indicate support of authentication methods other than PSK in the ClientHello message. The UE shall send the hostname of the AF using the server\_name extension to the ClientHello message according to TLS extensions. The AF shall include a constant string "3GPP-AKMA" is used as PSK-identity name space to indicate that AKMA based keying is supported, and the A-KID.In step 2 if the AF is willing to establish a TLS tunnel using PSK authentication with AKMA keys, then the AF shall indicate the index of the AKMA psk identity in the ServerHello message.

The AF uses the "3GPP-AKMA" prefix and the A-KID in the ClientHello messages to fetch the AF specific shared secret (KAF) from the AAnF.

The UE and NAF shall derive the TLS external PSK from KAF.

**\*\*\*\* END OF CHANGES \*\*\*\***