**3GPP TSG-SA3 Meeting #104-e *S3-212840r1***

**e-meeting, 16 - 27 August 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.535** | **CR** | **0098** | **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:***  | Corrections to the TLS with AKMA specification |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | AKMA\_TLS |  | ***Date:*** | 2021-07-21 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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 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| ***Reason for change:*** | The HTTP reference is outdated compared to the one used in TS 33.222 and come text is not clear.The UE should prefer AKMA over GBA\_Digest. |
|  |  |
| ***Summary of change:*** | Update the HTTP text and clarify some of the text.It is clarified that the UE should prefer AKMA over GBA\_Digest. |
|  |  |
| ***Consequences if not approved:*** | Old references are used which could affect implementations |
|  |  |
| ***Clauses affected:*** | 3, Annex B, B.1.2.2, B.1.3.2 |
|  |  |
|  | **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 \*\*\*\***

3 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)".

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

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

**\*\*\*\* NEXT CHANGE \*\*\*\***

Annex B (normative):
AKMA profiles for Ua\* protocols

# B.1 TLS based protocols

## B.1.1 General

This annex contains profiles of the share key-based UE authentication with certificate-based AF authentication and the shared key-based mutual authentication between UE and AF that are similar to the ones defined in 3GPP TS 33.222 [7].

## B.1.2 Shared key-based UE authentication with certificate-based AF authentication

### B.1.2.1 General

The following clause provides the changes needed to adapt the Ua protocol given in clause 5.3 of TS 33.222 [7] to work with a KAF derived using the AKMA procedures.

### B.1.2.2 Procedures

The procedures follow those given in clause 5.3.0 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, if the client supports AKMA with this protocol then the client shall add the constant string "3gpp-akma" to the "User-Agent" HTTP header as product tokens as specified in IETF RFC 7231 [xx].

At step 3, if the AF selects AKMA for deriving the key, then the AF shall include the "3GPP-bootstrapping-akma" within the WWW-Authenticate header field. In the selection of the key method, AKMA shall take priority over GBA\_Digest (see TS 33.222 [7]).

At step 5 given AKMA has been selected for keying, the client shall send a response with an Authorization header field where Digest is inserted using the A-KID as username. KAF shall be used as password in the Digest calculation.

At step 6 given AKMA has been selected for keying, the AF shall verify the value of the password attribute using KAF retrieved from AAnF using the A-KID received as username attribute in the query. If the AF is not able to obtain the AF-specific key when using AKMA mode, the AF shall respond with an appropriate error message not containing the realm attributes from step 3.

## B.1.3 Shared key-based mutual authentication between UE and AF

### B.1.3.1 General

The following clause provides the changes needed to adapt the Ua protocol given in clause 5.4 of TS 33.222 [7] to work with a KAF derived using the AKMA procedures.

### B.1.3.2 Procedures

The procedures follow those given in clause 5.4.0 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 keys were also indicated as supported by the AF). To use AKMA generated key, the UE shall derive the TLS premaster secret from KAF and shall send a ClientKeyExchange message including a PSK identity consisting of "3GPP-AKMA" and the A-KID. In the selection of the key method, AKMA shall take priority over GBA\_Digest (see TS 33.222 [7]).

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).

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