**3GPP TSG-SA3 Meeting #103e *S3-211785-r1***

**e-meeting, 17 - 28 May 2021** *revision of S3-2111785*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.535** | **CR** | **0066** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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:*** | Profiling the GBA TLS protocols for use with AKMA | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA\_TLS | | | | |  | ***Date:*** | | | 2021-01-07 |
|  |  | | | |  | |  | | |  |
| ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | AKMA provides a new way to derive keys for a UE’s subscription but there are currently no security protocols to use that key with. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add a profile of the TLS protocols that are used with GBA so that these protocols can be used with AKMA | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, Annex X (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 \*\*\*\***

2 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".

[xx] 3GPP TS 33.222: " Generic Authentication Architecture (GAA); Access to network application functions using HypertextTransfer Protocol over Transport Layer Security (HTTPS)".

[yy] IETF RFC 2616 (1999): "Hypertext Transfer Protocol (HTTP) – HTTP/1.1".

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

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

# X.1 TLS based protocols

## X.1.1 General

Annex X.1 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 [xx].

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

### X.1.2.1 General

The following subclause of clause X.1.2 provides the changes needed to adapt the Ua protocol given in clause 5.3 of TS 33.222 [xx] to work with a KAF derived using the AKMA procedures.

### X.1.2.2 Procedures

The procedures follow those given in clause 5.3.0 of TS 33.222 [xx] 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 clients 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 2616 [yy].

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 [xx]).

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.

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

### X.1.3.1 General

The following subclause of clause X.1.3 provides the changes needed to adapt the Ua protocol given in clause 5.4 of TS 33.222 [xx] to work with a KAF derived using the AKMA procedures.

### X.1.3.2 Procedures

The procedures follow those given in clause 5.4.0 of TS 33.222 [xx] 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).

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