**3GPP TSG-SA3 Meeting #104-e *draft\_S3-212535-r1***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.535** | **CR** | **0090** | **rev** | **-** | **Current version:** | **17.2.1** |  |
|  | | | | | | | | |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)*** *on using this form: comprehensive instructions can be found at  <http://www.3gpp.org/Change-Requests>.* | | | | | | | | |
|  | | | | | | | | |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Add step 4 in annex B.1.2.2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | ZTE | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA\_TLS | | | | |  | ***Date:*** | | | 2021-07-30 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | According to TS 33.222, the failure case is described in step 4. In AKMA scenario there is no Ub interface, the client cannot perform a run of the Ub protocol with the AAnF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | To add description about the how to deal with failure case in step 4 to the annex B.1.2.2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The description about the how to deal with failure case is unclear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex B.1.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* 1st CHANGE\*\*\*

### 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 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 [8].

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 4, on receiving the response from the AF, the client shall verify that the FQDN in the realm attribute corresponds to the FQDN of the AF it established the TLS connection with. If failure the client shall terminate the TLS connection with the AF.

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.

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