**3GPP TSG-SA3 Meeting #105-e *S3-214133-r1***

**e-meeting, 8 - 19 November 2021 *revision of S3-212842***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.222** | **CR** | **0055** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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:*** | Correction to the GBA TLS 1.3 specification | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eCryptPr | | | | |  | ***Date:*** | | | 2021-07-22 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | UE does not need to derive TLS key the key until it has received the response that GBA will be used. Furthermore the UE canot derive the key until the ciphersuite is chosen at step 2 as ciphersuites determines Ua protocol identifier which is needed for key derivation. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Allow the UE to derive only the needed TLS key when it has the full information available to derive that key. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | UE is expected to derive a key when it can’t as the needed inofmation is not available in the UE. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.0.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\***

5.4.0.2 TLS 1.3

1. When a UE contacts a NAF, it may indicate to the NAF 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 NAF using the server\_name extension to the ClientHello message according to TLS extensions.

The UE shall use a GBA-based shared secret for TLS with PSK authentication. If the UE does not have a valid GBA-based shared secret it shall obtain one by running the bootstrapping procedure with the BSF over the Ub reference point as specified in TS 33.220 [3].

The PSK identities in the ClientHello shall include prefixes indicating the PSK-identity name space (i.e. "3GPP-bootstrapping-uicc", "3GPP-bootstrapping", or "3GPP-bootstrapping-digest"), and the B-TID. The precise format of the PSK identity is specified in TS 24.109 [18]. The prefix "3GPP-bootstrapping" is used in the PSK-identity to indicate that the UE accepts that AKA-based Ks\_(ext)\_NAF is used establish the TLS session keys. The prefix "3GPP-bootstrapping-uicc" is used in the PSK-identity to indicate that the UE accepts that Ks\_int\_NAF is used to establish the TLS sessions keys. The prefix "3GPP-bootstrapping-digest" is used in the PSK-identity to indicate that the UE accepts that GBA\_Digest-based Ks\_NAF is used to establish the TLS sessions keys. One of these prefixes shall be present in the ClientHello message, and it shall indicate the GBA as the required authentication method. The ClientHello message shall include prefixes for the authentication methods the UE supports. Also, other PSK-identity prefixes may be supported, however, they are out of the scope of this specification.

If the HTTPS client resides in the ME, Ks\_(ext)\_NAF shall be used as the GBA shared key. If the HTTPS client resides in the UICC, Ks\_int\_NAF shall be used as the GBA shared key. In the selection of the GBA mode by the UE, AKA-based modes shall take priority over GBA\_Digest.

The UE derives the TLS external PSKs from the NAF specific key (Ks\_(ext)\_NAF if the initiating HTTPS client resides on the ME or Ks\_int\_NAF if the initiating HTTP client resides on the UICC).

NOTE 1: The ability to send the hostname of the NAF is particularly necessary if a NAF can be addressed using different hostnames, and the NAF cannot otherwise discover what is the hostname that the UE used to contact the NAF. The hostname is needed by the BSF during key derivation.

NOTE 2: If the UE supports PSK authentication but not GBA-based authentication, the TLS handshake will fail if the NAF selected PSK authentication and suggested to use GBA (as described in step 2). In this case, the UE should attempt to establish the TLS tunnel with the NAF without including indicating support of PSK authentication in the CientHello message, according to the procedure specified in clause 5.3. This note does not limit the use of PSK authenticated TLS to HTTP-based services.

2. If the NAF is willing to establish a TLS tunnel using PSK authentication, it shall select one of the psk identities and indicate the index of the selected psk identity in the ServerHello message.

If the NAF receives the "3GPP-bootstrapping" prefix and the B-TID in the ClientHello messages it fetches the NAF specific shared secret (Ks\_(ext)\_NAF) from the BSF using the B-TID, else if the NAF receives the "3GPP-bootstrapping-uicc" prefix and the B-TID in the ClientHello message it fetches the NAF specific shared secret (Ks\_int\_NAF) from the BSF using the B-TID. If the NAF receives the "3GPP-bootstrapping-digest" prefix and the B-TID in the ClientHello message it shall indicate to the BSF that GBA\_Digest is acceptable.

If the NAF has requested a USS, and the USS indicates to the NAF that only the Ks\_int\_NAF shall be allowed, then the NAF shall only accept the Ks\_int\_NAF as the NAF specific key. If the Ks\_(ext)\_NAF was used as the NAF specific key, the NAF shall respond with the appropriate error code and terminate the TLS connection with the UE.

The NAF derives the TLS external PSK from the NAF specific key (Ks\_(ext)\_NAF if the initiating HTTPS client resides on the ME or Ks\_int\_NAF if the initiating HTTP client resides on the UICC).

NOTE 3: If the NAF does not wish to establish a TLS tunnel using a PSK-based authentication, it shall select non-PSK-based authentication and continue TLS tunnel establishment based on the procedure described either in clause 5.3 or clause 5.5.

After the UE has sent the Finished message and the NAF has received the Finished message from the UE, they may start to use the application level communication through this tunnel.

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