**3GPP TSG-CT WG1 Meeting #134-eC1-221229\_r2**

**E-Meeting, 17th – 25th February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.109** | **CR** | **0071** | **rev** | **-** | **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:*** | GBA-based shared secret with PSK authentication in TLS 1.3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eCryptPr | | | | |  | ***Date:*** | | | 2022-01-31 |
|  |  | | | |  | |  | | |  |
| ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | SA3 specified GBA-based shared secret with Pre-Shared Key (PSK) authentication in TLS 1.3 in TS 33.222.  CT1 needs to specify the corresponding stage 3 details. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clause 5.3.3.1 restructured to include the new PSK-based authentication procedure using TLS 1.3. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The stage 3 requirements for the use of GBA-based shared secret with Pre-Shared Key (PSK) authentication in TLS 1.3 will remain unspecified, leading to differing implementations and interoperability issues. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.3.1, 5.3.3.1.1 (new), 5.3.3.1.2 (new), 5.3.3.1.3 (new), 5.3.3.3, 5.3.3.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* First Change \*\*\*

#### 5.3.3.1 Authentication procedure

##### 5.3.3.1.1 General

The authentication mechanism described in this section for ME-based application is optional to implement in the ME and the NAF.

The authentication mechanism described in this section for UICC-based application is optional to implement in the UICC and the NAF.

The PSK-based authentication for TLS (PSK TLS) may be used with bootstrapped security association as the authentication, confidentiality, and integrity protection method. The profile for TLS and TLS Extensions to be used together with PSK TLS is defined in annex E of 3GPP TS 33.310 [25].

##### 5.3.3.1.2 Authentication procedure using TLS 1.2

The PSK TLS handshake shall be used with bootstrapped security association as follows:

- the ClientHello message shall contain one or more PSK-based ciphersuites;

- the ClientHello message shall contain the server\_name TLS extension and it shall contain the hostname of the NAF;

- the ServerHello message shall contain a PSK-based ciphersuite selected by the NAF;

- the ServerKeyExchange shall be sent by the server and it shall contain the psk\_identity\_hint field and it shall contain the static string "3GPP‑bootstrapping" or "3GPP-bootstrapping-uicc" or "3GPP-bootstrapping-digest". If several authentication methods are supported then the ServerKeyExchange message shall include the PSK-identity hints for all allowed authentication methods, separated by semi-colon ";" (e.g., "3GPP-bootstrapping;3GPP-bootstrapping-uicc").

In the case of GBA\_U, the NAF shall indicate to the UE which NAF specific key can be used by setting the psk\_identity\_hint to "3GPP-bootstrapping" (for the ME-based key i.e. Ks\_ext\_NAF), or to "3GPP-bootstrapping-uicc" (for the UICC-based key i.e. Ks\_int\_NAF). If the NAF allows both types of keys to be used then the psk\_identity\_hint field shall contain both hints separated by semi-colon ";".

In addition, the NAF may include an indication to use a BSF address different from the one specified in 3GPP TS 23.003 [7] in the psk\_identity\_hint field of the ServerKeyExchange message. The indication to use the different BSF address shall contain a prefix "3GPP bootstrapping-BSF-address", a separator character ":" and the FQDN of the BSF. The NAF may only include this indication for an application specified to support this functionality (e.g. Proximity-based Services, see 3GPP TS 33.303 [29]) and if it is included then the static strings "3GPP bootstrapping" shall be included.

The psk\_identity\_hint field may contain a list of psk\_identity\_hints and are separated by a semi-colon character (";") (see NOTE 1);

NOTE 1: Other psk identity name spaces than "3GPP‑bootstrapping" or "3GPP‑bootstrapping-uicc" can be supported, however, they are out of the scope of this specification.

- the ClientKeyExchange shall contain the psk\_identity field and it shall contain a prefix "3GPP‑bootstrapping" or "3GPP‑bootstrapping-uicc" or "3GPP-bootstrapping-digest" indicating the selected psk identity name space, a separator character ";" and the B-TID. In the selection of the GBA mode by the UE, AKA-based modes shall take priority over GBA\_Digest.;

- if the PSK TLS client resides in the ME, the UE shall derive the TLS premaster secret from the NAF specific key material i.e. Ks\_NAF in the case of GBA\_ME. For GBA\_U the UE shall derive the TLS premaster secret from the ME-based key material i.e. Ks\_ext\_NAF;

- if the PSK TLS client resides in the UICC, the UE shall derive the TLS premaster secret from the NAF specific UICC-based key material i.e. Ks\_int\_NAF;

- if the indication to use a different BSF address was included in the psk\_identity\_hint field of the ServerKeyExchange message, the ME shall derive the TLS premaster secret from a Ks\_NAF resulting from a GBA\_ME bootstrapping with the indicated BSF and shall use the prefix "3GPP bootstrapping" in the psk\_identity field of the ClientKeyExchange message.

NOTE 2: A GBA\_U capable NAF indicates to the UE the type of the authorized NAF specific key (i.e. (Ks\_ext\_NAF or Ks\_int\_NAF or both). The details of the key decision mechanism in the NAF are specified in 3GPP TS 29.109 [3].

In the case of GBA\_U, if the HTTPS client application resides in the ME then the application shall use only the ME-based key i.e. Ks\_ext\_NAF (the UICC-based key Ks\_int\_NAF is not available in the ME). If a NAF indicates to a ME-based HTTPS client application that the UICC-based key shall be used then the application must terminate the communication with this NAF. If a HTTPS client application resides in the UICC, then the application shall only use the UICC-based key. If the NAF indicates to the UICC-based application that only the ME-based key can be used then the application must terminate the communication with the NAF.

In the case of GBA\_U, the operator may indicate the type of the key to be used in the Ua reference point in the NAF specific USS as specified in 3GPP TS 29.109 [3]. If the NAF has requested an application specific USS, and the indication is present in the USS, the NAF shall use the indicated key type. If the type of the negotiated key is different from the type indicated in the USS, the NAF shall terminate the communication with the UE.

An example flow of the PSK TLS procedure can be found in clause F.3.

\*\*\* Next Change \*\*\*

##### 5.3.3.1.3 Authentication procedure using TLS 1.3

The PSK TLS handshake shall be used with bootstrapped security association as follows:

1) The UE shall include in the ClientHello message:

a) an indication that it supports the TLS with PSK authentication using the "psk\_key\_exchange\_modes" extension;

b) the hostname of the NAF using the "server\_name" TLS extension;

c) authentication methods other than PSK the UE supports;

d) PSK identities within the psk\_identities field. Each included psk\_identity parameter within the psk\_identities field shall contain a prefix indicating the PSK identity name space, a separator character ";" and the B-TID. The psk\_identity parameters within the psk\_identities field are separated by a comma character (","); and

e) an additional psk\_identity parameter in the psk\_identities field for each of psk\_identity parameter included in step 1)d) to allow the NAF to signal that a bootstrapping is required for that bootstrapping method. The format of this additional psk\_identity parameter is the original one without the semi-colon character and B-TID but with "\_bootstrappingrequired" appended, e.g. "3GPP-bootstrapping-uicc-bootstrappingrequired" parameter is included if the psk\_identity parameter with the "3GPP-bootstrapping-uicc" PSK identity name space is included in the psk\_identities field and similarly for the other methods.

The prefix "3GPP-bootstrapping" is used in the psk\_identity parameter 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 parameter 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 parameter to indicate that the UE accepts that GBA\_Digest-based Ks\_NAF is used to establish the TLS sessions keys.

NOTE: Other PSK identity name spaces can be supported, however, they are out of the scope of the present document.

If the UE has a choice in the selection of the GBA mode, AKA-based modes shall take priority over GBA\_Digest.

The UE shall derive 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).

2) If the NAF wants the UE to perform a new bootstrapping for a particular method:

a) the NAF shall indicate the index of the bootstrapping required of the selected psk\_identity parameter in the ServerHello message;

b) the UE shall treat the ServerHello message the NAF sent in step 2)a) as a HelloRetryRequest message and shall perform a new bootstrapping run for the indicated bootstrapping method; and

c) once the bootstrapping is completed, the UE shall send a new ClientHello message with the psk\_identities field including only the psk\_identity parameter containing the psk\_identity\_namespace of the chosen bootstrapping method and the new B-TID.

3) If the NAF is willing to establish a TLS tunnel using PSK authentication the NAF shall select one of the psk\_identity parameters from the psk\_identities field received within the ClientHello message.

4) The NAF shall reply with the ServerHello message and indicate the index of the psk\_identity parameter. The NAF concludes the TLS handshake by sending Finished message to the UE.

If the NAF received within the ClientHello messages the psk\_identities field with the psk\_identity parameter containing:

a) "3GPP-bootstrapping" prefix and the B-TID the NAF shall fetch the NAF specific shared secret (Ks(\_ext)\_NAF) from the BSF using the B-TID;

b) "3GPP-bootstrapping-uicc" prefix and the B-TID the NAF shall fetch the NAF specific shared secret (Ks\_int\_NAF) from the BSF using the B-TID; or

c) "3GPP-bootstrapping-digest" prefix and the B-TID the NAF shall indicate to the BSF that GBA\_Digest is acceptable.

If the NAF has requested an application specific USS, and the indication is present in the USS, the NAF shall use the indicated key type. If the type of the negotiated key is different from the type indicated in the USS, the NAF shall terminate the communication with the UE.

The NAF shall derive the TLS external PSK from the NAF specific key (Ks(\_ext)\_NAF or Ks\_int\_NAF).

5) The UE concludes the TLS handshake by sending Finished message to the NAF.

The UE and the NAF have established a TLS tunnel using GBA-based shared secret, and they may start to use the application level communication through this tunnel.

\*\*\* Next Change \*\*\*

#### 5.3.3.3 Bootstrapping required indication

In TLS 1.2, during TLS handshake, the NAF shall indicate to the UE that bootstrapped security association is required by sending a ServerHello message containing a PSK-based ciphersuite, and a ServerKeyExchange message containing the psk\_identity\_hint field, which contains a static string "3GPP-bootstrapping" or "3GPP-bootstrapping-uicc" or "3GPP-bootstrapping-digest". This shall trigger the UE to run the bootstrapping procedure over Ub interface.

NOTE: The NAF shall select a PSK-based ciphersuite only if the UE has offered one or more PSK-based ciphersuites in the corresponding ClientHello message.

In TLS 1.3, during TLS handshake, the UE shall include the psk\_identities field in the ClientHello message to enable the request of a fresh bootstrapping. If the NAF wants the UE to perform a new bootstrapping for a particular method, the NAF shall indicate the index of the bootstrapping required of the selected psk\_identity parameter in the ServerHello message. This shall trigger the UE to run the new bootstrapping procedure over Ub interface.

\*\*\* Next Change \*\*\*

#### 5.3.3.4 Bootstrapping renegotiation indication

During usage of TLS session, the NAF shall indicate to the UE that bootstrapped security association has expired by sending close\_notify alert message to the UE.

In TLS 1.2, the UE may attempt resume the old TLS session by sending a ClientHello message containing the old session ID. The NAF shall refuse to use the old session ID by sending a ServerHello message with a new session ID. This will indicate to the UE that the bootstrapped security association it used has expired.

During TLS handshake, the NAF shall indicate to the UE that the bootstrapped security association has expired by sending handshake\_failure message as a response to the Finished message sent by the UE. This will indicate to the UE that the bootstrapped security association it used has expired.

\*\*\* End of Changes \*\*\*