**3GPP TSG-SA3 Meeting #101-e *S3-203313-r1***

**e-meeting, 9th - 20th November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0052** | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Aligning TLS in 33.222 with the current 3GPP TLS profile | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | CryptPr | | | | |  | ***Date:*** | | | 2020-10-30 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | |  |
|  | *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:*** | | TLS 1.3 is mandatory to support in 3GPP TLS profile, but 33.222 does not give enough details when TLS 1.3 is used.  - TLS 1.3 deprecates Session ID and deprecates the 24 hour lifetime recommendation. The server may prolong the lifetime as long as it wants.  - In TLS 1.3, ServerHelloDone, ServerKeyExchange, and ClientKeyExchange messages are deprecated.  - In TLS 1.3 PSK authentication is not negotiated as part of the cipher suite and there are no PSK hints, the client instead sends a list of PSK identities in the ClientHello and the server choses one of them.  - TLS 1.3 specified its own exporter function.  - NULL ciphers are forbidden in the general 3GPP TLS profile. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | - Reference to TLS 1.3 introduced.  - New paragraph on resumption for TLS 1.3  - Authentication mechanism for TLS 1.2 and TLS 1.3 separated into two different subclauses.  - TLS 1.3 exporter is used for TLS 1.3 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Risk for non-compatible implementations when the mandatory to support TLS 1.3 is used in 33.222 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 5.3.1.1, 5.3.1.5, 5.4.0, 5.4.1.4, Annex D.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:*** | |  | | | | | | | | |

\*\*\* BEGIN 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 TS 23.002: "Network architecture".

[2] 3GPP TS 22.250: "IP Multimedia Subsystem (IMS) group management"; Stage 1".

[3] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[4] 3GPP TR 33.919: "Generic Authentication Architecture (GAA); System description".

[5] 3GPP TS 33.141: "Presence Service; Security".

[6] Void.

[7] Void.

[8] Void.

[9] IETF RFC 2818 (2000): "HTTP Over TLS".

[10] IETF RFC 2617 (1999): "HTTP Authentication: Basic and Digest Access Authentication".

[11] IETF RFC 3310 (2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

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

[13] 3GPP TS 33.210: "3G Security; Network Domain Security; IP network layer security".

[14] Void.

[15] Void.

[16] 3GPP TS 33.221: "Generic Authentication Architecture (GAA); Support for subscriber certificates".

[17] Void.

[18] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[19] 3GPP TS 29.109: "Generic Authentication Architecture (GAA), Zh and Zn Interface based on the Diameter protocol; Stage 3".

[20] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[21] V oid.

[22] Void.

[23] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[24] W3C Working Draft (Jan 22, 2013): "HTML5.1 Nightly – A vocabulary and associated APIs for HTML and XHTML", work in progress, <http://dev.w3.org/html5/spec/>.

[25] IETF RFC 5929 (2010): "Channel Bindings for TLS".

[26] W3C Working Draft (Oct 20, 2011): "File API", work in progress, <http://www.w3.org/TR/FileAPI/>.

[27] W3C Candidate Recommendation (Dec 8, 2011): "Web Storage", work in progress, http://www.w3.org/TR/webstorage/

[28] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[29] IETF RFC 5705 (2010): "Keying Material Exporters for Transport Layer Security (TLS)".

[XX] IETF RFC 8446 (2018): "The Transport Layer Security (TLS) Protocol Version 1.3".

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

#### 5.3.1.1 Protection mechanisms

The rules on allowed and mandatory ciphersuites are given in TS 33.310 [20], Annex E .

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

#### 5.3.1.5 Set-up of Security parameters

In TLS 1.2, the TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The Client and the AP/AS shall allow for resuming a session. This facilitates that a Client and Server may resume a previous session or duplicate an existing session. The lifetime of a Session ID is maximum 24 hours. The Session ID shall only be used under its lifetime and shall be considered by both the Client and the Server as obsolete when the Lifetime has expired.

In TLS 1.3, the Client can only intiate resumption if the Sever has sent a NewSessionTicket Post-Handshake message. Each received ticket has a lifetime, and the client may attempt resumption as long as it has a valid ticket.

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

### 5.4.0 Procedures

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

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

The HTTP client and server may authenticate each other based on the shared key generated during the bootstrapping procedure. The shared key shall be used as a master key to generate TLS session keys, and also be used as the proof of secret key possession as part of the TLS authentication function. The usage of Pre-Shared Key authentication in Transport Layer Security (TLS) is specified in the TLS profile given in TS 33.310 [20], Annex E.

This section explains how a GBA-based shared secret that is established between the UE and the BSF as specified in TS 33.220 [3] is used with Pre-Shared Key (PSK) authentication in TLS according to the TLS profile given in TS 33.310 [20], Annex E. The HTTPS client may reside in the ME or in the UICC. In former case, Ks\_(ext)\_NAF shall be used to establish the TLS session keys. In latter case, Ks\_int\_NAF shall be used to establish the TLS session keys.

NOTE 0: It should be noted that the term "GBA mode" does not refer to used bootstrapping mechanism, but it refers to NAF keys in the following way:   
- "3GPP-bootstrapping" and "3gpp-gba" refer to Ks\_NAF from GBA\_ME, Ks\_ext\_NAF from GBA\_U or Ks\_NAF from 2G GBA;  
- "3GPP-bootstrapping-uicc" and "3gpp-gba-uicc" refer to Ks\_int\_NAF from GBA\_U;  
- "3GPP-bootstrapping-digest" and "3gpp-gba-digest" refer to Ks\_NAF from GBA\_Digest.

#### 5.4.0.1 TLS 1.2

1. When an UE contacts a NAF, it may indicate to the NAF that it supports PSK-based TLS by adding one or more PSK-based ciphersuites to the ClientHello message. The UE shall include ciphersuites other than PSK-based ciphersuites 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.

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: When the UE adds one or more PSK-based ciphersuites to the ClientHello message, this can be seen as an indication that the UE supports PSK-based TLS. If the UE supports PSK-based ciphersuites but not GBA-based authentication, the TLS handshake will fail if the NAF selected the PSK-based ciphersuite 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 PSK-based ciphersuites to the CientHello message, according to the procedure specified in clause 5.3. This note does not limit the use of PSK TLS to HTTP-based services.

2. If the NAF is willing to establish a TLS tunnel using a PSK-based ciphersuite, it shall select one of the PSK-based ciphersuites offered by the UE, and send the selected ciphersuite to the UE in the ServerHello message.

The NAF shall send the ServerKeyExchange message with a list of PSK-identity hints. A constant string "3GPP-bootstrapping" is used as PSK-identity hint to indicate the local configuration in the NAF i.e. that the NAF accepts that AKA-based Ks\_(ext)\_NAF is used establish the TLS session keys. A constant string "3GPP-bootstrapping-uicc" is used as PSK-identity hint to indicate that the local configuration in the NAF accepts that Ks\_int\_NAF is used to establish the TLS sessions keys. A constant string "3GPP-bootstrapping-digest" is used as PSK-identity hint to indicate that the local configuration in the NAF accepts that GBA\_Digest-based Ks\_NAF is used to establish the TLS sessions keys. One of these PSK-identity hints shall be present in the ServerKeyExchange message, and it shall indicate the GBA as the required authentication method. If the local configuration in the NAF allows several authentication methods to be used to access its service then the ServerKeyExchange message shall include the PSK-identity hints for all allowed authentication methods. Also other PSK-identity hints may be supported, however, they are out of the scope of this specification. The NAF finishes the reply to the UE by sending a ServerHelloDone message.

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

3. The UE shall use a GBA-based shared secret for PSK TLS, if the NAF has sent a ServerHello message containing a PSK-based ciphersuite, and a ServerKeyExchange message containing at least one of the constant strings "3GPP-bootstrapping", "3GPP-bootstrapping-uicc", or "3GPP-bootstrapping-digest" as the PSK identity hint. 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].

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 premaster secret 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).

The UE shall send a ClientKeyExchange message. The PSK identity in the ClientKeyExchange message shall include a prefix indicating the PSK-identity name space that was selected (i.e. "3GPP-bootstrapping-uicc", "3GPP-bootstrapping", or "3GPP-bootstrapping-digest"), and the B-TID. The prefix shall match one of the PSK-identity hints that NAF offered in ServerKeyExchange message. The precise format of the PSK identity is specified in TS 24.109 [18]. The UE concludes the TLS handshake by sending the ChangeCipherSuite and Finished messages to the NAF.

4. If the NAF receives the "3GPP-bootstrapping" prefix and the B-TID in the ClientKeyExchange 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 ClientKeyExchange messages 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 ClientKeyExchange messages 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 premaster secret from the NAF specific key (Ks\_(ext)\_NAF or Ks\_int\_NAF).

The NAF concludes the TLS handshake by sending the ChangeCipherSuite and Finished messages to the UE.

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

#### 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 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 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 or Ks\_int\_NAF).

NOTE 3: If the NAF does not wish to establish a TLS tunnel using a PSK-based authentication, it selects 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.

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

#### 5.4.1.4 Set-up of Security parameters

In TLS 1.2, the TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The Client and the AP/AS shall allow for resuming a session. This facilitates that a Client and Server may resume a previous session or duplicate an existing session. The lifetime of a Session ID is the lifetime of the GAA shared secret or maximum of 24 hours. The Session ID shall only be used under its lifetime and shall be considered by both the Client and the Server as obsolete when the Lifetime has expired.

In TLS 1.3, the Client can only intiate resumption if the Sever has sent a NewSessionTicket Post-Handshake message. Each received ticket has a lifetime, and the client may attempt resumption as long as it has a valid ticket.

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

### D.1.3.2 Channel binding using RFC 5705 and RFC 5929

After receiving the Ks\_(ext)\_NAF key from the GBA Function the GBA API obtains the TLS\_MK\_Extr, which is extracted from the TLS master key using the exporter function . For TLS 1.2, the exporter specified in RFC 5705 [29] shall be used. For TLS 1.3, the exporter described in section 7.5 of RFC 8446 [XX] shall be used. The label for the exporter function shall be "TLS\_MK\_Extr". The GBA API obtains the tls-server-endpoint as specified in RFC 5929 [25]. The Ks\_js\_NAF shall be derived from Ks\_(ext)\_NAF as follows:

Ks\_js\_NAF = KDF (Ks\_(ext)\_NAF, TLS\_MK\_Extr, tls-server-endpoint)

A sequence flow is in clause D.2.1.

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