**3GPP TSG-SA3 Meeting #101-e *S3-203313-r2***

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

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.222** | **CR** | **0052** | **rev** | **-** | **Current version:** | **16.0.0** |  |
|  |
| *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 |  | 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:*** | Rel-16 |
|  | *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 canbe 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, 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 \*\*\*

### 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 \*\*\*