**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *draft\_S3-232128-r1***

**Electronic meeting, Online, 17 - 21 April 2023** (revision of S3-23xxxx)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.220** | **CR** | **draftCR** | **rev** | **<->** | **Current version:** | **17.4.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Living document for GBA DTLS to TS 33.220 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | ZTE,THALES,Qualcomm | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA\_GBA\_DTLS | | | | |  | ***Date:*** | | | 2023-2-6 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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:*** | | In order to complete the work on the DTLS for GBA Ua protocol, it is required to add a dedicated annex in 3GPP TS 33.220 including description about Shared key-based UE authentication with certificate-based AF authentication and Shared key-based mutual authentication between UE and AF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Addition of a new annex including the skeleton of DTLS for GBA Ua protocol | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete work for the DTLS for GBA Ua protocol | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, Annex H.3, Annex X (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 draft CR's revision history:*** | | SA3#110: S3-231476  SA3#110Adhoc-e: S3-232135 | | | | | | | | |

\*\*\*\* Start of Change1\*\*\*\*

Annex X (normative):   
GBA Ua protocol based on DTLS

## X.1 General

This Annex covers the aspects specific to the GBA Ua protocol based on DTLS. This feature is optional to be supported for the UE and NAF. If the feature is supported, the following clauses apply.

#### X.1.1 Requirement on the UE

UE hosts the DTLS client. The DTLS client may reside in the ME or in the UICC or both might host an DTLS client independently of each other.

The UE should be able to indicate to the NAF which key (Ks\_(ext)\_NAF or Ks\_int\_NAF) the UE intends to or can use to secure the Ua reference point based on DTLS.

#### X.1.2 Requirement on the NAF

DTLS should be supported by the NAF for the UE-NAF reference point (Ua).

The NAF should be able to require that a certain key (i.e., Ks\_(ext)\_NAF or Ks\_int\_NAF) used to secure the Ua reference point based on DTLS.

## X.2 Shared key-based mutual authentication between UE and NAF

#### X.2.1 General

The TLS profile specified in TS 33.210 [13] clause 6.2 apply to DTLS 1.3[x].

#### X.2.2 Procedures for DTLS 1.3

The procedures and PSK identities given in clause 5.4.0.2 of TS 33.222[25] for TLS 1.3 are also applicable for DTLS 1.3, with the following changes.

At step 1, If the DTLS client resides in the ME, Ks\_(ext)\_NAF shall be used as the GBA shared key. If the DTLS client resides in the UICC, Ks\_int\_NAF shall be used as the GBA shared key.

The UE derives the DTLS premaster secret from the NAF specific key (Ks\_(ext)\_NAF if the initiating DTLS client resides on the ME or Ks\_int\_NAF if the initiating DTLS client resides on the UICC).

PSK identities should be delivered via DTLS message.

This section explains how a GBA-based shared secret that is established between the UE and the NAF is used with Pre-Shared Key (PSK) authentication in DTLS. It does not have any dependency on the application layer protocol.

\*\*\*\* End of Change 1\*\*\*\*

\*\*\*\* Start of Change 2\*\*\*\*

H.3 Ua security protocol identifiers for 3GPP specified protocols

The following Ua security protocol identifiers are specified by 3GPP:

( 0x01,0x00,0x00,0x00,0x00 ) Ua security protocol according to TS 33.221 [5].

( 0x01,0x00,0x00,0x00,0x01 ) Ua security protocols according to TS 33.246 [26].

NOTE 1: TS 33.246 [26] provides key separation between the keys that are used within HTTP digest and MIKEY protocols.

( 0x01,0x00,0x00,0x00,0x02) Ua security protocol HTTP digest authentication according to TS 24.109 [29], unless HTTP digest authentication is used in the context of another Ua security protocol, which is already covered elsewhere in this Annex.

( 0x01,0x00,0x00,0x00,0x03 ) Ua security protocols used with HTTP-based security procedures for MBMS user services according to TS 26.237 [38].

( 0x01,0x00,0x00,0x00,0x04 ) Ua security protocols used with SIP-based security procedures for MBMS user services according to TS 26.237 [38].

( 0x01,0x00,0x00,0x00,0x05 ) Ua security protocols used with Generic Push Layer according to TS 33.224 [39], unless Generic Push Layer is used in the context of another Ua security protocol, which is already covered elsewhere in this Annex.

( 0x01,0x00,0x00,0x00,0x06 ) Ua security protocol for IMS UE to KMS http based message exchanges according to "IMS media plane security", TS 33.328 [40]

( 0x01,0x00,0x00,0x00,0x07 ) Ua security protocol for shared key TLS 1.3 given in clause 5.4.0.2 of TS 33.222 [25].

( 0x01,0x00,0x00,0x00,0x09 ) Ua security protocol for DTLS according to Annex X.

( 0x01,0x00,0x00, 0x01,0x00 ) Generation of TMPI according to Annex B.4.

NOTE 2: This protocol identifier is not strictly a Ua protocol identifier, but its use in key derivation function is exactly equal.to a Ua protocol identifier.

( 0x01,0x00,0x01,yy,zz ) Ua security protocol for "Shared key-based UE authentication with certificate-based NAF authentication", according to TS 33.222 [25] section 5.3, or "Shared key-based mutual authentication between UE and NAF" for TLS 1.2 (see above for Ua security protocol identifier for TLS 1.3 with shared keys), according to TS 33.222 [25] section 5.4.0.1. Here, "yy,zz" is the protection mechanism CipherSuite code according to the defined values for TLS CipherSuites in the IANA TLS Cipher Suite Registry which is referenced in RFC 8446 [59].

NOTE 3: The "Certificate based mutual authentication between UE and NAF” according to TS 33.222 [25] section 5.5 does not require a Ua protocol identifier.

NOTE 4: As an example: The TLS 1.2 CipherSuite TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 has code = { 0xC0,0x2B }, thus the according protocol identifier shall be ( 0x01,0x00,0x01, 0xC0,0x2B  ).

( 0x01,0x00,0x02,yy,zz ) Ua security protocol for "Shared key-based UE authentication with certificate-based NAF authentication", according to TS 33.222 [25] Annex D. Here, "yy,zz" is the protection mechanism CipherSuite code according to the defined values for TLS CipherSuites in the IANA TLS Cipher Suite Registry which is referenced in RFC 8446 [59]. This Ua security protocol identifier is used for the case outlined in TS 33.222 [5] Annex D, where e.g. HTML FORM based authentication is used within a TLS tunnel.

NOTE 4: The third octet (0x02) distinguish this case from other protocols tunneled inside the TLS tunnel.

\*\*\*\* End of Change 2\*\*\*\*

\*\*\*\* Start of Change 3\*\*\*\*

# 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 31.102: "Characteristics of the USIM application".

[2] 3GPP TS 33.102: "3G Security; Security architecture".

[3] Void

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

[5] 3GPP TS 33.221: "Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[6] Void

[7] Void

[8] Void

[9] Void.

[10] 3GPP TS 31.103: "Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[11] 3GPP TS 23.003: "Numbering, addressing and identification".

[12] Void

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

[14] Void.

[15] 3GPP TS 31.101: "UICC-terminal interface; Physical and logical characteristics".

[16] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services".

[17] Void.

[18] IETF RFC 2818: "HTTP over TLS".

[19] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[20] Void.

[21] Void.

[22] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[23] ISO/IEC 10118-3:2004: "Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions".

[24] IETF RFC 3629: "UTF-8, a transformation format of ISO 10646".

[25] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[26] 3GPP TS 33.246: "3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)".

[27] Void.

[28] Void

[29] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[30] (void)

[31] (void)

[32] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[33] Void

[34] 3GPP TS 23.002: “Network architecture “.

[35] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".

[36] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[37] "Unicode Standard Annex #15; Unicode Normalization Forms", Unicode 5.1.0, March 2008. <http://www.unicode.org>

[38] 3GPP TS 26.237: "IP Multimedia Subsystem (IMS) based Packet Switch Streaming (PSS) and Multimedia Broadcast/Multicast Service (MBMS) User Service; Protocols".

[39] 3GPP TS 33.224: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push Layer".

[40] 3GPP TS 33.328: "IMS Media plane security".

[41] Void

[42] (void)

[43] Void.

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

[45] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[46] 3GPP TS 44.006 "Technical Specification Group GSM/EDGE Radio Access Network; Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification".

[47] 3GPP TS 43.020 "Technical Specification Group Services and system Aspects; Security related network functions".

[48] IETF RFC 5929 "Channel Bindings for TLS".

[49] 3GPP TS 33.303: "Proximity-based Services; Security Aspects".

[50] 3GPP TS 33.179: "Security of Mission Critical Push-To-Talk (MCPTT)".

[51] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[52] 3GPP TS 33.163: " Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST)".

[53] 3GPP TS 33.501: " Security architecture and procedures for 5G system".

[54] 3GPP TS 33.180: "Technical Specification Group Services and System Aspects; Security of the mission critical service".

[55] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[56] 3GPP TS 33.536: "Security Aspect of 3GPP Support for Advanced V2X Services".

[57] Void

[58] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

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

[60] IETF RFC 4648: "The Base16, Base32, and Base64 Data Encodings".

[61] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[62] IETF RFC 7616: "HTTP Digest Access Authentication".

[63] IETF RFC 7230: " Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[64] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[65] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[66] 3GPP TS 23.501: " System architecture for the 5G System (5GS)".

[67] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[x] IETF RFC 9146: "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3"\*\*\*\* End of Changes\*\*\*\*