**3GPP TSG-SA3 Meeting #100e *S3-201947r1***

**e-meeting, 17 - 28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0203** | **rev** | **1** | **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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Assigning FC values for IAB and AKMA TS | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated, China Mobile, Samsung | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16 | | | | |  | ***Date:*** | | | 06-08-2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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 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:*** | | Need to assign FC values to the AKMA TS | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Assign AKMA values to the AKMA TS | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | AKMA key derivations can not be standardised | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, B.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **x** |  | Other core specifications | | | | TS 33.535 CR 0026 | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS 33.501 CR 0937 | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | | This CR should only be approved if the related CRs are approved | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev 1: Merge with S3-201869 and S3-201978 to include FC allocation for IAB | | | | | | | | |

**\*\*\*\* START OF 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 31.102: "Characteristics of the USIM application".

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

[3] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[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] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2 (Release 6)".

[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] IETF RFC 3548: "The Base16, Base32, and Base64 Data Encodings".

[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] IETF RFC 2246: "The TLS Protocol Version 1".

[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] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".

[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] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[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".

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

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

B.2.2 FC value allocations

FC values shall only be assigned to a key derivation function by their allocated specification.

FC values in the range 0x00 – 0x0F are allocated for use in this specification.

FC values in the range 0x10 – 0x1F are allocated for use in TS 33.401 [35].

FC values in the range 0x20 – 0x2F are allocated for use in TS 33.402 [36].

FC values in the range 0x30 – 0x37 are allocated for use in TS 33.102 [2].

FC values in the range 0x38 – 0x3F are allocated for use in TS 43.020 [47].

FC values in the range 0x40 – 0x47 are allocated for use in TS 33.224 [39].

FC values in the range 0x48 – 0x4F are allocated for use in TS 33.303 [49].

FC values in the range 0x50 – 0x57 are allocated for use in TS 33.179 [50].

FC values in the range 0x50 – 0x57 are also allocated for use in TS 33.180 [54].

FC values in the range 0x58 – 0x5F are allocated for use in TS 33.203 [51].

FC values in the range 0x60 – 0x68 are allocated for use in TS 33.163 [52].

FC values in the ranges 0x69 – 0x79, 0x7B – 0x7D and 0x83 are allocated for use in TS 33. 501 [53].

FC value 0x7A is allocated for use in TS 33.122 [55].

FC values in the range 0x7E – 0x7F are allocated for use in TS 33.536 [56].

FC values in the range 0x80 – 0x82 are allocated for use in TS 33.535 [xx].

FC values in range 0x84 – 0xDF are reserved for future use in 3GPP specifications.

FC values in the range 0xE0 – 0xEF are reserved for uses of the KDF by other standardization organisations where the FC value for such use is registered in the present specification.

FC values in the range 0xF0 – 0xFE are reserved for proprietary uses of the KDF where the FC value for the such use is not registered with 3GPP.

FC values of the form 0xFF || FC2 are reserved for future use in 3GPP specifications.

NOTE 1: Registering an FC value with 3GPP for use by other standardization organisations means that only the FC value is recorded in the present specification, but the full specification of the key derivation is done elsewhere. This has the advantage that clashes in FC values in different uses by other standardization organisations can be avoided. On the other hand, not registering an FC value with 3GPP for proprietary use means that 3GPP may have no knowledge of this use at all.

NOTE 2: Ranges of FC values for use by other standardization organisations or for proprietary use could be extended in the future if such a need was indicated to 3GPP.

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