**3GPP TSG-SA3 Meeting #104-e ad-hoc *S3-214430***

e-meeting, 27 - 30 September 2021 revision of S3-214108

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **draft-CR** | **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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Living Document: Security aspects of MSGin5G |
|  |  |
| ***Source to WG:*** | China Mobile |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  930005 |  | ***Date:*** | 2021-09-30 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***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 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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Security aspects for MSGin5G need to be specified. |
|  |  |
| ***Summary of change:*** | Enhancements to 5GS on the security aspects for MSGin5G. Specifically:- Authentication and authorization between the MSGin5G client and the MSGin5G server- Transport security protection for MSGin5G interfaces |
|  |  |
| ***Consequences if not approved:*** | Enhanced support of MSGin5G will not have necessary security aspects specified. |
|  |  |
| ***Clauses affected:*** | 2, 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 CR's revision history:*** |  |

\*\*\* START of 1st 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

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

[4] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[7] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[8] 3GPP TS 23.502: "Procedures for the 5G System".

[9] 3GPP TS 33.102: "3G security; Security architecture".

[10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[12] IETF RFC 5448: " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[13] 3GPP TS 24.301: " Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[14] 3GPP TS 35.215: " Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".

[15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197)".

[16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[18] 3GPP TS 35.221: " Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[19] 3GPP TS 23.003: "Numbering, addressing and identification".

[20] 3GPP TS 22.101: "Service aspects; Service principles".

[21] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[22] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[23] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[24] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[25] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)"

[26] Void

[27] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[28] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[29] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available <http://www.secg.org/sec1-v2.pdf>

[30] SECG SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>

[31] 3GPP TS 38.470: "NG-RAN; F1 General aspects and principles".

[32] 3GPP TS 38.472: "NG-RAN; F1 signalling transport".

[33] 3GPP TS 38.474: "NG-RAN; F1 data transport".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)"

[35] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[36] 3GPP TS 35.217: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data".

[37] 3GPP TS 35.223: "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data".

[38] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[39] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

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

[41] 3GPP TS 38.460: "NG-RAN; E1 general aspects and principles".

[42] Void.

[43] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[44] IETF RFC 7519: "JSON Web Token (JWT)".

[45] IETF RFC 7515: "JSON Web Signature (JWS)".

[46] IETF RFC 7748: "Elliptic Curves for Security".

[47] IETF RFC 7540: " Hypertext Transfer Protocol Version 2 (HTTP/2)".

[48] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[49] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[50] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[51] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[52] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[53] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[54] 3GPP TS28.533: " Management and orchestration; Architecture framework".

[55] 3GPP TS28.531: "Management and orchestration of networks and network slicing; Provisioning".

[56] Void

[57] IETF RFC 7542: "The Network Access Identifier".

[58] IETF RFC 6083: " Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[59] IETF RFC 7516: "JSON Web Encryption (JWE)".

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

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

[62] IETF RFC 5869 "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".

[63] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois Counter Mode (GCM) and GMAC".

[64] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

[65] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications.

[66] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[67] Internet draft draft-ietf-emu-rfc5448bis: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[68] 3GPP TS 29.510: "5G System; Network function repository services".

[69] 3GPP TS 36.331: "Radio Resource Control (RRC); Protocol specification".

[70] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3".

[71] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[72] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

[73] 3GPP TS 29.573: " Public Land Mobile Network (PLMN) Interconnection; Stage 3".

[74] 3GP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[75] IEEE TSN network aspects: see 3GPP TS 23.501 [2] references [95], [96], [97], [98], [104], and [107].

[76] Internet draft draft-ietf-emu-eap-tls13: "Using EAP-TLS with TLS 1.3"

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

[78] 3GPP TS 38.401: "NG-RAN; Architecture description".

[79] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)"

[80] IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[81] IETF RFC 2410 "The NULL Encryption Algorithm and Its Use With IPsec".

[82] Void

[83] RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[84] RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

[85] RFC 4890: "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[86] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[87] 3GPP TS 38.305: "Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[88] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[89] IANA: "Transport Layer Security (TLS) Parameters".

[90] RFC 2818: "HTTP Over TLS".

[91] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

[92] 3GP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection".

[93] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[94] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition".

[95] 3GPP TS 29.502: "5G System; Session Management Services".

[96] 3GPP TS 29.526: "5G System; Network Slice-Specific Authentication and Authorization (NSSAA) services".

[X] 3GPP TS 23.554 Application architecture for MSGin5G Service; Stage 2

[Y] 3GPP TS 22.262 Message service with the 5G System (5GS); Stage 1

\*\*\* END of 1st CHANGES \*\*\*

\*\*\* START of 2nd CHANGES \*\*\*

Annex X (normative):

Security aspects of the Message Service for MIoT over the 5G System (MSGin5G)

X.1 General

This Annex specifies the security aspects of Message Service for MIoT over the 5G System (MSGin5G). The general features of MSGin5G are described in 23.554 [X], 22.262 [Y].

X.2 Authentication and authorization between MSGin5G client and MSGin5G Server

The Authentication and authorization between MSGin5G Client and MSGin5G Server shall be based on AKMA, which is specified in TS 33.535 [91]. Before initiating communication with MSGin5G Server, the UE needs to have performed primary authentication and registered with the 5GC, resulting in the successful generation of KAKMA and A-KID at both MSGin5G Client and the 5GC as specified in clause 6.1, TS 33.535 [91].

Once the UE is registered in 5GC, the MSGin5G Client in the UE and the MSGin5G Server may use TLS for authentication as specified in Annex B of TS 33.535 [91] with the MSGin5G Server taking the role of AKMA AF.

Editor's Note: Further clarification on usage of GPSI or SUPI for authorization in MSGin5G services is FFS.

Methods other than TLS with AKMA may be used for authentication between the MSGin5G Client and MSGin5G Server, depending on the Ua\* protocols.

X.3 Transport security protection for MSGin5G interfaces

The MSGin5G-1 interface may be protected by TLS based on KAF established by AKMA as specified in TS 33.535 [91]. The MSGin5G Client and the MSGin5G Server establish the TLS session following the procedures defined in Annex B of TS 33.535 [91].

The MSGin5G-1 interface may be protected using mechanisms other than TLS with AKMA, depending on the Ua\* protocols.

For the data protection over MSGin5G-3 interface between MSGin5G Server and Application Server, the transport security protection on SBI interface shall be reused as specified in clause 13. If the Application Server supports CAPIF capability, the existing interface security protection mechanisms for CAPIF shall be reused. TLS can be used for confidentiality, integrity and replay protection.

For MSGin5G-2 and MSGin5G-4 interfaces, TLS shall be used for transport protection unless network security is provided by other means.

X.4 Authentication and Authorization between Application Server and MSGin5G Server

The authentication and authorization between Application Server and MSGin5G is based on the transport security protection. TLS should be used as specified in TS 33.210 [3].

X.5 Authentication and Authorization between message Gateway and MSGin5G Server

The authentication and authorization between Message Gateway and the MSGin5G Server can reuse the authentication and authorization between network functions in 13.3.2 in this document.

In direct communication, authentication between message gateway and MSGin5GServer shall use one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for authentication between message gateway and MSGin5GServer.

- If the PLMN does not use protection at the transport layer, authentication between message gateway and MSGin5GServer may be implicit by NDS/IP or physical security.

If the PLMN uses token-based authorization, the network shall use protection at the transport layer as described in clause 13.1.

In indirect communication scenarios, 13.3.2 in this document also applies.

\*\*\* END of CHANGES \*\*\*