**3GPP TSG-SA3 Meeting #119 S3-245168**

Orlando, USA 11 - 15 October 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **draftCR** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  |
| *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:***  | Living document for MonStra: Draft CR to 33.501 |
|  |  |
| ***Source to WG:*** | Vodafone, Nokia, Nokia Shanghai Bell, Ericsson, Telefonica, Telecom Italia |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | MonStra-Sec |  | ***Date:*** | 2024-11-13 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-19 |
|  | *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:*** | SA3#118 agreed Living Draft CR of MonStra requirements in S3-244490. SA3#119: Includes the updated terminology as per S3-244853 and solution according to S3-245167. |
|  |  |
| ***Summary of change:*** | Updating Draft CR is proposed |
|  |  |
| ***Consequences if not approved:*** | Living document missing |
|  |  |
| ***Clauses affected:*** | 3.1, 5.9.1, 5.9.X (new), 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:*** | S3-244490, S3-244853, S3-245167 |

\*\*\* Start of 1st Change \*\*\*

##

# 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] Void

[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 9113: "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] IETF RFC 9048: "Improved Extensible Authentication Protocol Method for 3GPP Mobile Network 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] IETF RFC 9190: "EAP-TLS 1.3: Using the Extensible Authentication Protocol 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] Void

[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".

[97] 3GPP TS 23.402: "Authentication enhancements for non-3GPP accesses".

[98] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[99] RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[100] RFC 6678: "Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method".

[101] General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>.

[102] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (MBMS)".

[103] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services".

[104] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[105] 3GPP TS 23.288: "Architecture enhancements for 5G System(5GS) to support network data analytics services".

[106] 3GPP TS 23.554 Application architecture for MSGin5G Service; Stage 2.

[107] 3GPP TS 22.262 Message service with the 5G System (5GS); Stage 1.

[108] 3GPP TS 26.502: "5G multicast–broadcast services; User Service architecture".

[109] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[110] NIST Special Publication 800-90A (2015): "Recommendation for Random Number Generation Using Deterministic Random Bit Generators".

[111] IETF RFC 4555 (2006-06): "RFC IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[112] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[113] RFC 9110: "HTTP Semantics".

[114] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[115] IETF RFC 9000: "QUIC: A UDP-Based Multiplexed and Secure Transport".

[116] IETF RFC 9001: "Using TLS to Secure QUIC".

[117] draft-ietf-quic-multipath: "Multipath Extension for QUIC".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[x] 3GPP TS 28.abc: “Management and orchestration; Signalling traffic monitoring management (Stage 1, stage 2, and stage 3)”.

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

## 3.1 Definitions

**Secondary node**: As defined in TS 37.340 [51].

**Signalling Monitor Consumer**: This term is defined in 3GPP TS 28.abc [x]

**Signalling Monitor Producer**: This term is defined in 3GPP TS 28.abc [x]

NOTE: The Signalling Monitor Producer and the Signalling Monitor Consumer are left for implementation, with the consideration of being the end-point of the Signalling monitoring interfaces for which security requirements are specified in 5.9.X.

**subscription credential(s):** The set of values in the USIM and in the home operator's network, consisting of at least the long-term key(s) and the subscription identifier SUPI, used to uniquely identify a subscription and to mutually authenticate the UE and 5G core network.

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

### 5.9.1 Trust boundaries

It is assumed for the set of requirements in this sub-clause that mobile network operators subdivide their networks into trust zones. Subnetworks of different operators are assumed to lie in different trust zones. Messages that traverse trust boundaries shall follow the requirements in sub-clause 5.9.2 to 5.9.x of the present document, if not protected end to end by NDS/IP as specified in TS 33.210 [3].

\*\*\* Start of 4th Change \*\*\*

### 5.9.X Requirements for Monitoring 5GC Signaling Traffic

#### 5.9.X.1 Security requirements for the configuration of signalling monitoring

The 5G shall support mutual authentication between the Signalling Monitor Producer at the 5GC (for configuration/activation of the functionality) and the Signalling Monitor Consumer in charge of the signalling traffic monitoring management.

The 5G shall support authorization to the Signalling Monitor Consumer in charge of the signalling traffic monitoring management.

NOTE 1: Local policy-based authorization should be supported by the Signalling Monitor Producer, according to 3GPP TS 28.533 [54].

The 5G shall support integrity protection, replay protection and confidentiality protection for communication between the Signalling Monitor Producer at the 5GC and the Signalling Monitor Consumer in charge of the signalling traffic monitoring management.

NOTE 2: If interface between the Signalling Monitor Producer and the Signalling Monitor Consumer in charge of the signalling traffic monitoring management is trusted (e.g. physically protected), it is for the PLMN-operator to decide whether to apply integrity protection, replay protection and confidentiality protection for communication.

#### 5.9.X.2 Security requirements for the streaming of signalling monitoring data

The 5G shall support mutual authentication between the Signalling Monitor Producer at the 5GC and the Monitoring system.

NOTE: The Monitoring system is outside the scope of this specification.

The 5G shall provide confidentiality protection, integrity protection and replay protection of the interface between the Signalling Monitor Producer at the 5GC and the Monitoring system.

\*\*\* Start of 5th Change \*\*\*

# X Protection of 5GC Signalling Traffic Monitoring

## X.1 General

The protection of the Signalling Monitoring functionality aims to provide the security mechanisms on the interfaces between the 5GC trust zones and the trust zone where the Management/Monitoring Systems reside. The architecture of the Signalling Monitoring for configuration, authorisation controls, enablement and disablement requests as well as for the transfer of the signalling monitoring data can be found in clause xxx of TS 28.abc [x].

Figure X.1-1 provides an example of trust zones in the overall architecture of Signalling Traffic Monitoring.



Figure X.1-1 Signalling Traffic Monitor trust zones example

NOTE: The final definition of the trust zones is to be established by the PLMN-operator.

## X.2 Protection for the configuration and enabling/disabling of signalling monitoring

TLS shall be supported and shall be used to provide mutual authentication, integrity protection, replay protection and confidentiality protection for the interface between the Signalling Monitor Producer and the Signalling Monitor Management Consumer handling the configuration and the enabling/disabling requests.

NOTE 1: If interface between the Signalling Monitor Producer and the Signalling Monitor Management Consumer is trusted (e.g. physically protected), it is for the PLMN-operator to decide whether to apply integrity protection, replay protection and confidentiality protection for communication.

Security profiles for TLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

NOTE 2: A PLMN-operator policy may determine to use dedicated certificates for this secure communication, separated from those used in SBI interfaces.

## X.3 Protection for the streaming of signalling monitoring data

The protection mechanism to provide mutual authentication, integrity protection, replay protection and confidentiality protection is to be implemented at transport layer.

NOTE 1: If interface between the Signalling Monitor Producer and the Signalling Monitor Management Consumer is trusted (e.g. physically protected), it is for the PLMN-operator to decide whether to apply integrity protection, replay protection and confidentiality protection for communication.

When UDP is used as transport protocol for the streaming of monitoring data, DTLS shall be supported and shall be used to provide mutual authentication, integrity protection, replay protection and confidentiality protection between the Signalling Monitor Producer at the 5GC and at the Signalling Monitor Consumer.

When TCP is used as transport protocol for the streaming of signalling monitoring data, TLS shall be supported and shall be used to provide mutual authentication, integrity protection, replay protection and confidentiality protection between the Signalling Monitor Producer at the 5GC and at the Signalling Monitor Consumer.

Security profiles for DTLS and TLS implementations and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

NOTE 2: A PLMN-operator policy may determine to use dedicated certificates for this secure communication, separated from those used in SBI interfaces.

\*\*\* End of Changes \*\*\*