**3GPP TSG-SA3 Meeting #102e *S3-21xxxx***

**e-meeting, 18 - 29 January 2021**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1019** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  |
| *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:***  | Resolving editor's note on encryption policy mismatch between SEPPs |
|  |  |
| ***Source to WG:*** | NTT Docomo, Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5GS\_Ph1-SEC  |  | ***Date:*** | 2021-01-29 |
|  |  |  |  |  |
| ***Category:*** | **A** |  | ***Release:*** | Rel-17 |
|  | *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:*** | There is an unresolved editor's note that depended on CT4 error message definitionIn Rel-16 TS 29.573 table has been updated recently as follows:Table 6.1.4.3.2-2: Data structures supported by the POST Response Body on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Responsecodes | Description |
| SecParamExchRspData | M | 1 | 200 OK | This represents the successful processing of the requested parameters. The SEPP shall provide the selected parameters (i.e selected cipher suite and/or selected protection policy) depending on what was requested by the requesting SEPP and what is supported by the responding SEPP, or the SEPP shall provide the security information lists of the connected IPXs. |
| ProblemDetails | O | 0..1 | 409 Conflict | The "cause" attribute may be used to indicate one of the following application errors:- REQUESTED\_PARAM\_MISMATCH |
| NOTE: The mandatory HTTP error status codes for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] other than those specified in the table above also apply, with a ProblemDetails data type (see clause 5.2.7 of 3GPP TS 29.500 [4]). |

 |
|  |  |
| ***Summary of change:*** | Adding CT 4 reference on error code and deleting ed. note. Removing duplicated reference to TS 29.500, adding reference to TS 29.573. |
|  |  |
| ***Consequences if not approved:*** | Unsolved editor's note. |
|  |  |
| ***Clauses affected:*** | 2, 13.2.3.6  |
|  |  |
|  | **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:*** | S3-210075-r3 |

\*\*\*\*\*\*\*\*\*\*\*\* 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 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')".

Editor’s note: This reference will be removed and references to it updated when the IETF updates the RFC and publishes a new RFC that supercedes this RFC.

[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] IETF RFC 4279 "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

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

[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".

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

#### 13.1.1.1 TLS protection based on telescopic FQDN and wildcard certificate

A telescopic FQDN is an FQDN with a single label as the first element and the SEPP’s domain as the trailer component. The label uniquely represents the original FQDN.

NOTE 3: The structure of telescopic FQDN is defined in 3GPP TS 23.003 [19], clause 28.5.2.

The SEPP shall generate a telescopic FQDN for the following messages received over N32-f:

a. Nnrf\_NFDiscovery\_Get response HTTP message with FQDNs of a set of the discovered NF or NF service instance(s) (cf. TS 29.510). The cSEPP generates a telescopic FQDN for each target Network Function FQDN in the Discovery response, rewrites the original FQDN with the telescopic FQDN and forwards the modified Discovery response to the NRF.

b. Subscription message with the Callback URI in the payload of the message (cf. TS 29.501). The pSEPP generates a telescopic FQDN from the Callback URI in the Subscription message, rewrites the original FQDN in the callback URI, and forwards the modified Subscription message to the producer Network Function.

c. Nsmf\_PDUSession\_POST HTTP message from a V-SMF with PduSessionCreateData containing the URI representing the PDU session in the V-SMF (cf. TS 29.502). The pSEPP generates a telescopic FQDN from the Callback URI in the message, rewrites the original FQDN in the callback URI, and forwards the modified message to the target H-SMF.

The following procedure illustrates how SEPPs use telescopic FQDN and wildcard certificate to establish a TLS connection between a Network Function or a SCP and the SEPP:

1. When the SEPP receives one of the messages identified in a-c above, it shall rewrite the FQDN from the received message with a telescopic FQDN and it forwards the modified HTTP message to the target Network Function or SCP inside the PLMN.

2. When the Network Function or SCP that received the telescopic FQDN in step 1 is ready to communicate with the target Network Function or SCP in another PLMN, it uses the telescopic FQDN in the Request URI of the HTTP Request. When communication between the Network Function or SCP and the SEPP that generated the telescopic FQDN is based on using the 3gpp-Sbi-Target-apiRoot custom HTTP header as specified in TS 29.500 [74], clause 5.2.3.2.4, the Network Function or SCP uses the telescopic FQDN in the 3gpp-Sbi-Target-apiRoot custom HTTP header of the HTTP Request. During TLS setup between the Network Function and the SEPP, the SEPP shall authenticate towards the Network Function or SCP using the wildcard certificate.

3. When the SEPP receives a HTTP request from the Network Function or SCP, the SEPP shall rewrite the telescopic FQDN with the original FQDN by replacing the unique delimiter in the label with the period character and removing its own suffix part.

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

13.2.3.6 Precedence of policies in the SEPP

This clause specifies the order of precedence of data-type encryption policies and modification policies available in a SEPP.

In increasing order of precedence, the following policies apply for a message to be sent on N32:

1. The set of default rules specified in the present specification:

- For the data-type encryption policy, the rules on data-types that are mandatory to be encrypted according to clause 5.9.3.3.

- For the modification policy, the basic validation rules defined in clause 13.2.3.4.

2. Manually configured policies:

 - For the data-type encryption policy: rules according to clause 13.2.3.2, on a per roaming partner basis.

 - For the modification policy: rules according to clause 13.2.3.4, per roaming partner and per IPX provider that is used for the specific roaming partner.

NOTE 1: It is assumed that operators agree both data-type encryption and modification policy in advance, for example as part of their bilateral roaming agreement. The protection policies exchanged via N32-c during the initial connection establishment only serve the purpose of detecting possible misconfigurations.

NOTE 2: It is assumed that the default rules and manually configured policies do not overlap or contradict each other. The manually configured policies are used to extend the protection by the default rules in the present document and are applied on top of them.

When a SEPP receives a data-type encryption or modification policy on N32-c as specified in clause 13.2.2.2, it shall compare it to the one that has been manually configured for this specific roaming partner and IPX provider. If a mismatch occurs for one of the two policies, the SEPP shall perform one of the following actions, according to operator policy:

- Send the error message as specified in TS 29.573 [73], clause 6.1.4.3.2, to the peer SEPP.

- Create a local warning.

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