**3GPP TSG-SA3 Meeting #99e *S3-201274r2***

**e-meeting, 11 -15 May 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **0841** | **rev** | - | **Current version:** | **16.2.0** |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Security Aspects of DNS and ICMP |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | UPIP\_SEC |  | ***Date:*** | 2020-04-28 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***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 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:*** | UP IP is optional to use based on the network policy and the UE capability. When UP IP is not used, an attacker may be able to modify the user plane data over the air undetected, leading to a security vulnerability that may be exploited by an attacker when DNS or ICMP messages are carried over the user plane. |
|  |  |
| ***Summary of change:*** | Addition of new Annex to specify the security aspects of DNS and ICMP. Update of references and an addition of a note. |
|  |  |
| ***Consequences if not approved:*** | DNS and ICMP messages remain vulnerable when the use of UP IP is not activated. |
|  |  |
| ***Clauses affected:*** | 2, 5.2.3, 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 CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 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 29.500: "Technical Realization of Service Based Architecture".

[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".

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

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

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.2.3 User data and signalling data integrity

The UE shall support integrity protection and replay protection of user data between the UE and the gNB.

The UE shall activate integrity protection of user data based on the indication sent by the gNB.

The UE shall support integrity protection and replay protection of RRC and NAS-signalling.

The UE shall implement the following integrity protection algorithms:

NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The UE may implement the following integrity protection algorithm:

128-NIA3 as defined in Annex D of the present document.

The UE shall implement the integrity algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Integrity protection of the user data between the UE and the gNB is optional to use.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected.

All RRC signalling messages except those explicitly listed in TS 38.331 [22] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

The UE shall implement NIA0 for integrity protection of NAS and RRC signalling. NIA0 is only allowed for unauthenticated emergency session as specified in clause 10.2.2.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Annex X (Informative):
Security Aspects of DNS and ICMP

# X.1 General

This annex specifies security measures to protect DNS and ICMP messages. These security measures are intended when integrity protection over the user plane can not be used.

# X.2 Security aspects of DNS

It is recommended that the UE and DNS server(s) support DNS over (D)TLS as specified in RFC 7858 [xx] and RFC 8310 [yy]. The DNS server(s) that are deployed within the 3GPP network can enforce the use of DNS over (D)TLS.

NOTE: The use of DNS over (D)TLS with DNS server(s) that are deployed outside the 3GPP network is outside the scope of this specification.

When DNS over (D)TLS is used, a TLS cipher suite that supports integrity protection needs to be negotiated.

# X.3 Security aspects of ICMP

ICMP (Internet Control Message Protocol) is part of the internet protocol (IP) suite. The lack of security in ICMP may be exploited to launch further attacks on the 3GPP system. To mitigate such attacks, it is recommended that the use of ICMP is restricted in the UE and the UPF (e.g., by default, use of ICMP is not allowed). In scenarios where the use of ICMP is required, it is recommended that one or more of following mitigations be enforced:

Disable the UE from responding to ICMP requests received over 3GPP network interface(s).

Install IP filter(s) at the UPF in order to block ICMP messages. This filter can be configured either on a per UE basis or on a UPF basis. For ICMPv6, the recommendations in RFC 4890 [zz] can be used for filtering ICMPv6 messages.

Limit the maximum size of ICMP messages (e.g., to 64 bytes). Any ICMP messages that are greater than this limit needs to be dropped by the UE as well as by the UPF.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*