**3GPP TSG-SA3 Meeting #115 *draft\_S3-240908-r2***

Athens, Greece, 26th February - 1st March 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **1933** | **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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Details of the DNS security mechanism in EDGE computing (non-roaming) | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | EDGE\_Ph2 | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | To provide details of the DNS security mechanism (DNS over TLS, namely DoT) in the context of EDGE computing. DoT has been agreed to be specified as protection mechanism for more secure and private DNS resolution process between UE and EASDF in EDGE architecture as defined by 3GPP. IETF RFCs 7858 and 8310 specify DoT and usage profiles for DoT respectively, including several configuration options. This CR is intended to profile the mechanism by selecting the options of Strict Privacy profile, Authentication Domain Name (ADN) and PKIX certificate verification. More details about the justifiction for that selection can be found in the Discussion Paper S3-240584.  Since the content of Annex P of TS 33.501 does not include relevant information and details about the specified security mechanism (DoT), and the annex itself was added for a particular scenario, the proposal is to revert the Annex P to informative and specify the DNS security mechanisms to be used in EDGE in the corresponding Annex T of TS 33.501. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Providing details for DoT specified security mechanism | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Specification would be incomplete, and may cause interoperability issues. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex T | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\* FIRST CHANGE\*\*\*\*\*\*

Annex P (informative):  
Security Aspects of DNS and ICMP

# P.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.

# P.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 [83] and RFC 8310 [84]. The DNS server(s) that are deployed within the 3GPP network can enforce the use of DNS over (D)TLS. The UE can be pre-configured with the DNS server security information (out-of-band configurations specified in the IETF RFCs like, credentials to authenticate the DNS server, supported security mechanisms, port number, etc.), or the core network can configure the DNS server security information to the UE.

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 document.

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

# P.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 activated either on a per N4 Session basis or on a UPF basis. For ICMPv6, the recommendations in RFC 4890 [85] 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 FIRST CHANGE\*\*\*\*\*\*

\*\*\*\*\* SECOND CHANGE\*\*\*\*\*\*

# T.3 Security of EAS discovery procedure via EASDF in non-roaming Scenario

DNS over TLS and Strict Privacy usage profile as specified in IETF RFC 7858 [83] and RFC 8310 [84] shall be supported by the UE and the EASDF. The DNS connection shall be authenticated and encrypted.

NOTE X: Other DNS protection mechanisms are subject to implementation.

The security information of the EASDF can be preconfigured in the UE or if the core network is used to configure the security information, the SMF is preconfigured with the EASDF security information (authentication information, supported security mechanisms, port number, etc.) and provides the security information to the UE as follows:

The SMF provides the EASDF security information to the UE via PCO.

According to the clause 6.4.1.3 of TS 24.501, upon receiving the DNS server security information, the UE passes it to the upper layer. The UE uses this information to send the DNS over TLS. Additionally, the clause 10.5.6.3 of TS 24.008 provides the configuration of the different options of DNS over TLS specified in the RFC 7858 [83].

\*\*\*\*\* END of SECOND CHANGE\*\*\*\*\*\*