**3GPP TSG-SA3 Meeting #115 *S3-240590***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1934** | **rev** |  | **Current version:** | **18.4.0** |  |
|  | | | | | | | | |
| *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:*** | Details of the DNS security mechanism in EDGE computing (roaming) | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | EDGE\_Ph2 | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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 V-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. | | | | | | | | |
|  | |  | | | | | | | | |
| ***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\*\*\*\*\*\*

# T.4 Security of EAS discovery procedure via V-EASDF in roaming Scenario

DNS over (D)TLS as specified in IETF RFC 7858 [83] and RFC 8310 [84], shall be used to protect the discovery messages between the UE and the V-EASDF which is used as the DNS server for EAS discovery in the roaming case.

If the core network is used to configure the security information, the V-SMF is preconfigured with the V-EASDF security information (credentials to authenticate the V-EASDF, supported security mechanisms, port number, etc.) and provides the security information to the UE as follows:

- In the case of LBO roaming, the V-SMF provides the V-EASDF security information to the UE via PCO.

- In the case of HR with Session Breakout (HR-SBO) roaming scenarios, during the PDU session establishment or modification procedure, the V-SMF provides the V-EASDF security information via Nsmf\_PDUSession\_Create/ Nsmf\_PDUSession\_Update to H-SMF when the V-SMF determines to use a V-EASDF for EAS discovery, and the H-SMF provides the V-EASDF security information to UE via PCO if HR SBO is authorized.

NOTE: The security information of V-EASDF provided to the UE is only related with the VPLMN parameter.

According to the clause 6.4.1.3 of TS 24.501, upon receiving the DNS server security information, the UE shall pass it to the upper layer. The UE shall use this information to send the DNS over (D)TLS. Additionally, the clause 10.5.6.3 of TS 24.008 provides the configuration of the different options of DNS over (D)TLS specified in the RFC 7858.

DNS over TLS and Strict Privacy usage profile as specified in [84] should be selected by the UE and supported by the EASDF, thus the connection needs to be authenticated and encrypted. The UE requires to securely obtain the authentication information it can use to authenticate the EASDF. The authentication information should include the Authentication Domain Name (a DNS-ID), obtained for the EASDF, that later the UE can validate by comparing it with the provided EASDF PKIX certificate (inspecting the subjectAltName extension), as described in [84]. The PKIX certificate of the EASDF and the entire certification path for validation needs to be verified by the UE.

NOTE X: Other DNS over (D)TLS configuration options described in [83] and [84] are allowed and subject to the implementation.

\*\*\*\*\* END of FIRST CHANGE\*\*\*\*\*\*