**3GPP TSG-SA3 Meeting #116 *draft\_S3-242433-r1***

Jeju, South Korea, 20th - 24th May 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  **1989** | **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:***  | Retrieval of the EASDF security information from EASDF |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2024-05-13 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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 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:*** | Alignment with updated SA2 specifications on Security for EAS discovery procedure via (V-)EASDF : TS 23.501, TS 23.548 and TS 23.502. The CR is intended to capture in annex T of TS 33.501 the possibility for the (V-)SMF to obtain the (V-)EASDF security information in interaction with the (V-) EASDF.  |
|  |  |
| ***Summary of change:*** | (V-) SMF can retrieve (V-) EASDF DNS security information from EASDF  |
|  |  |
| ***Consequences if not approved:*** | Disalignment between SA2 and SA3 specifications |
|  |  |
| ***Clauses affected:*** | T.3, T.4 |
|  |  |
|  | **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:*** | The feature was agreed in SA2 in S2-2405584 and S2-2405586. |
|  |  |
| ***This CR's revision history:*** |  |

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

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

DNS over TLS 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 1: Other DNS protection mechanisms are subject to implementation.

The security information of the EASDF can be preconfigured in the UE by using out of band mechanisms; or if the core network is used to configure the security information, the SMF either is preconfigured with the EASDF security information (authenticat ion information, supported security mechanisms, port number, etc.), or the SMF retrieves the EASDF security information from the EASDF, 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 [35], 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 [112] provides the configuration of the different options of DNS over TLS specified in the RFC 7858 [83].

 \*\*\*\*\*\*\*\*\*\*END OF FIRST CHANGE\*\*\*\*\*\*

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

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

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

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

The security information of the V-EASDF can be preconfigured in the UE by using out of band mechanisms; or if the core network is used to configure the security information, the V-SMF either is preconfigured with the V-EASDF security information (authentication information, supported security mechanisms, port number, etc.), or the V-SMF retrieves the V-EASDF security information from the V-EASDF, 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 [35], 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 [112] provides the configuration of the different options of DNS over TLS specified in the RFC 7858 [83].

 \*\*\*\*\*\*\*\*\*\*END OF SECOND CHANGE\*\*\*\*\*\*