**3GPP TSG-SA3 Meeting #115 *S3-240587***

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

**Title: Reply LS on DNS over TLS (DoT)**

**Response to: LS (S2-2313793) on Reply LS on DNS over TLS (DoT) and DNS over HTTPS (DoH)**

**Release: Rel-18**

**Work Item: TEI18**

**Source:** **3GPP SA3 meeting #115**

**To:** **SA2**

**Cc:**

**Contact person: German Peinado**

 **german.peinado@nokia.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** Agreed CRs S3-240588, S3-240589, S3-240590

# 1 Overall description

SA3 thanks SA2 for the reply LS on DNS over TLS (DoT) and DNS over HTTPS (DoH).

The feedback to the questions provided in the LS is the following:

*1) SA2 kindly asks SA3 to specify now the security information in the PCO should be used by the UE.*

Response:

In clauses T.3 and T.4 of TS 33.501, it is specified that the EASDF security information (credentials to authenticate the EASDF, supported security mechanisms, port number, etc.) is provided 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 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.

SA3 has discussed the options provided in RFC 7858 and RFC 8310 for the configuration of the DNS over (D)TLS mechanism, and reached to the following recommendations which are implemented in the CRs S3-240588 for Rel-17, and S3-240589 and S3-240590 for Rel-18:

The security information provided in the PCO should be the Authentication Domain Name (ADN) for the DNS server (EASDF). The authentication is based on PKIX certificate verification mechanism (clause 8.1 of RFC 8310), thus the PKIX certificate of the DNS server (EASDF) and the entire certification path for validation needs to be verified by the DNS client.

*2) SA2 ask if SA3 have any concerns to allow the security information to be provided by the EASDF to the SMF.*

Response:

EASDF security information may either be locally configured in the SMF or retrieved by the SMF from the network (EASDF). If the EASDF and SMF belong to the same security domain there is no need to specify any standard security mechanism for such communication. If they belong to different security domains, NDS/IP as defined in TS 33.210 applies.

# 2 Actions

**To SA2**

**ACTION:**

SA3 kindly asks SA2 to take the provided information into consideration.

# 3 Dates of next TSG SA WG 3 meetings

SA3#115AdHoc-e 15 - 19 April 2024 Electronic meeting

SA3#116 20 - 24 May 2024 Jeju (South Korea)

SA3#117 19 - 23 August 2024 Maastricht (Netherlands)