**3GPP TSG-CT WG4 Meeting #99eC4-204372v1**

**E-Meeting, 18th – 28th August 2020 was C4-204116**

**Source: ZTE**

**Title: Solution for Header Enrichment for HTTPS**

**Spec: 3GPP TR29.820**

**Agenda item: 6.1.3**

**Document for: Approval**

**1. Introduction**

This contribution provides a solution for Header Enrichment for HTTPS.

**2. Proposal**

It is proposed to agree the following changes to 3GPP TR29.820 v0.1.0.

**\*\*\*\*\*\*\***

\* \* \* First Change \* \* \* \*

## 6.X Solution #X: Header Enrichment for HTTPS

### 6.X.1 Description

When HTTPS schema is used, HTTP messages are transmitted in encrypted SSL/TLS packets. Before sending HTTP message to the remote server, the client shall first perform SSL/TLS handshake procedure to set up SSL/TLS connection with the remote server. In this solution, the SSL/TLS protocol refers to TLS version 1.2 and onwards.

The initial SSL/TLS handshake messages are exchanged in clear text, which provides possibility to the UP Function to insert some customized information in the initial SSL/TLS handshake messages. A simple way is, when detecting an initial SSL/TLS handshake message (i.e. ClientHello message) from an UE, the UP Function can append additional SSL/TLS extension to the SSL/TLS handshake message to carry customized field names and values. If security sensitive information is required to be carried, such customized information should be secured by certain application layer encrypt methods which are known to the operator’s UP Function and the remote HTTPS server, e.g. by pre-configuration.

Editor's Note: It needs SA3 evaluation on whether security sensitive information is allowed to be transmitted to the application server, e.g. encapsulated by application layer encryption method.

In order to support Header Enrichment for HTTPS, both the CP Function (e.g. SMF) and UP Function (e.g. UPF) shall be enhanced to support corresponding functionalities.

To instruct the UP Function to detect SSL/TLS packets and perform Header Enrichment for HTTPS, the CP Function shall:

- Create UL PDR for detecting uplink SSL/TLS packets towards the remote server;

- Create FAR and associate it to the UL PDR. In the FAR, provide header field names and values which are required to be inserted into SSL/TLS handshake messages. And set the Header Type of Header Enrichment IE to “SSL/TLS” (or set to “HTTPS”).

Upon instruction from the SMF, the UP Function shall:

- Install the UL PDR and FAR, and keep monitoring uplink IP packets from the UE and check whether it is SSL/TLS packets;

- Once SSL/TLS packets from the UE is detected, further inspect whether the SSL/TLS packets carries initial SSL/TLS handshake message from the UE (i.e. ClientHello message);

- Once the initial SSL/TLS handshake message from the UE is detected, insert additional SSL/TLS extension and carry the required field names and the values in the additional SSL/TLS extension, and finally forward the altered SSL/TLS packets onwards.

### 6.X.2 Impacts on services, entities and interfaces

CP Function:

- Indicate to UP Function that detection of SSL/TLS handshake message is required and indicated header field names and values are to be inserted to SSL/TLS handshake message;

UP Function:

- Detect SSL/TLS handshake message from UE;

- Insert the required header field names and values to the detected SSL/TLS handshake messages from UE.

### 6.X.3 Pros

### 6.X.4 Cons

\* \* \* End of Changes \* \* \* \*