**3GPP TSG-CT WG4 Meeting #99eC4-204371**

**E-Meeting, 18th – 28th August 2020 was C4-204115**

**Source: ZTE**

**Title: Key Issue - Header Enrichment for HTTPS**

**Spec: 3GPP TR29.820**

**Agenda item: 6.1.3**

**Document for: Approval**

**1. Introduction**

Lots of websites use HTTPS schema to provide various services, including security sensitive service like personal banking. For those security sensitive services, local regulations may require recording which user has invoked the service. On the other hand, some value-added services (e.g. controlled by operators) may also require providing useful user information (e.g. user location) to the server, e.g. for make accurate service decision based on user information. In order to support such kind of requirements, header enrichment shall be supported for HTTPS, i.e. attaching the UE information (e.g. MSISDN, user location) to the service requests sent from the UE.

Currently TS29.244 only supports Header Enrichment for HTTP, and existing mechanism cannot be applied to HTTPS. When using HTTP schema, the HTTP messages are transmitted in clear text, thus the UPF is easy to inspect IP packets from a UE to extract the HTTP content so as to add custom headers to HTTP payload. When using HTTPS schema, the HTTP messages are encrypted in SSL/TLS packets, and normally the UPF is not able to get security parameters of SSL/TLS encryption.

In order to support operator’s requirement to add customized information when HTTPS schema is used, it is strongly proposed to study how to perform Header Enrichment for HTTPS.

**2. Proposal**

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

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

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

## 5.X Key Issue #X: Header Enrichment for HTTPS

### 5.X.1 Description of the use case

Lots of websites use HTTPS schema to provide various services, including security sensitive service like personal banking. For those security sensitive services, local regulations may require recording which user has invoked the service. On the other hand, some value-added services (e.g. controlled by operators) may also require providing useful user information (e.g. user location) to the server, e.g. for make accurate service decision based on user information. In order to support such kind of requirements, header enrichment shall be supported for HTTPS, i.e. attaching the UE information (e.g. MSISDN, user location) to the service requests sent from the UE.

### 5.X.2 Key issue definition

This key issue will study the following aspects:

- How does the SMF instruct the UPF to perform Header Enrichment for HTTPS?

- How does the UPF detect the HTTPS packets and attach header fields and values to the detected HTTPS packets?

- If security sensitive information is potentially transmitted to the server, how to ensure the transmission in a safe way?

Editor's Note: It needs SA3 evaluation on whether security sensitive information is allowed to be transmitted to the server, and if allowed how to ensure the secure transmission.

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