**3GPP TSG-SA3 Meeting #105-e *S3-214075-r2***

e-meeting, 8 - 19 November 2021

**Title: Reply LS on Header Enrichment for HTTPS in PFCP**

**Response to: LS CT4-214531 on Reply LS on Header Enrichment for HTTPS in PFCP from CT4**

**Release: Rel17**

**Work Item: BEst Practice of PFCP (BEPoP)**

**Source:** **Huawei<To be SA3>**

**To: CT4**

**Cc:**

**Contact person: Bo Zhang**

 **Zhangbo6@huawei.com**

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

**Attachments:** None

# 1 Overall description

SA3 thanks CT4 for their reply LS on Header Enrichment for HTTPS in PFCP (CT4-214531) and provides the following feedback.

Thanks for the explanation of the endpoint. SA3 would like to clarify that if the endpoints are in the 3GPP network domain, then all the sensitive information could be sent to the endpoints. If the endpoints is outside the 3GPP network domain, IMSI/SUPI, IMEI and MSISDN are internal identifiers that are not supposed to be sent outside the 3GPP network domain.

 Depending on regulations, sending other parameters related to subscribers and users could require user consent: *UE IP address, User location, etc*.

SA3 would also like to provide answers to the questions asked by CT4 in the previous LS (C4-211662/S3-211380) as below.

Q1: When encapsulating header fields and values in TLS packets during initial TLS handshake procedure, whether security sensitive information is allowed or forbidden to be included?

A1: Initial TLS packets are not a suitable way to transport the information. Since a man-in-the-middle inserts information to be consumed by the server, without consent from the client, it could be considered a privacy breach. Also, TLS will often be terminated in a frontend, which may not the intended receiver of the information. SA3 encourages CT4 to focus on solutions that use IETF protocols in the way they are intended to be used.

 Regarding encryption of the sensitive information, it could be more suitable to protect the whole channel between PSA UPF and the application server. This would allow the use of existing protocols and implementations.

Q2: If security sensitive information is potentially encapsulated in initial TLS packets, whethere.g. application layer encryption method is sufficient? If not, does SA3 intent to define corresponding security mechanism for this scenario, or does SA3 have suggestion of candidate security mechanism?Does SA3 agree that operator can select security mechanisms?

A2: SA3 recommends using an existing mechanism for protecting the channel between PSA UPF and the application server. SA3 has currently no plans to specify which mechanism should be used. Potentially, SA3 could specify it in the future, since it is in SA3's scope.

# 2 Actions

**To CT4 group.**

**ACTION:** SA3 kindly asks CT4 group to take the above feedback into account.

# 3 Dates of next TSG SA WG 3 meetings

SA3#106 7-11 February 2022 TBD

SA3#106-Bis 4 - 8 April 2022 TBD