**3GPP TSG-SA3 Meeting #108e *draft\_S3-221860-r1***

**e-meeting, 22 - 26 August 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI5 conclusion on e2e integrity prot of HTTP msg**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***Conclusion proposal for key issue 5.***

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

*From a security point of view the end-to-end protection of HTTP messages for indirect communication would be useful. But since discouraged from stage 3 perspective and because feedback is missing which headers are not subject to modification, mediation, or alteration by the SCP (i.e. can be delivered as is to the other far end of the indirect communication), it is proposed to not follow up normatively and thus, postpone the topic.*

# 4 Detailed proposal

*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE*

7.5 KI #5: End-to-end integrity protection of HTTP messages

7.5.1 Analysis

The KI #5 is about end-to-end protection of HTTP message for indirect communication. The key issue seek for solutions on how an NF Service Producer can verify that a service request of the NF Service Consumer received via SCP has not been modified tampered with.

Parameters in the request messages may be modified by the intermediate node according to the reply LS S3-212418 from CT WG4, and end-to-end protection of HTTP headers and bodies is discouraged, i.e. CT4 discourages end-to-end protection of HTTP headers and bodies and segregating the parameters based on SCP (or SEPP) modification criteria. There can be multiple SCPs and/or SEPPs involved in the service request/response path where SCP can modify the HTTP headers, and SEPP (or IPX) can modify the HTTP headers and/or HTTP body attributes. In addition, CT4 also raises potential compatibility issues with end-to-end protection of HTTP headers and bodies.

7.5.2 Conclusion

Since 3GPP CT4 WG indicated that one of the fundamental functionalities of SCP is message mediation which may require SCP to modify certain headers and/or content of the HTTP message, typical end-to-end message integrity protection between the far end NFs seems not feasible.

For this reason, 3GPP SA3 so far relies on hop-by-hop security.

Editor's note: Normative work is FFS.

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