**3GPP TSG-SA3 Meeting #107-e *S3-22xxxx***

e-meeting, 16 – 20 May 2022

**Title: [Draft]** **LS on handling of the modification policy in the IPX and receiving SEPP**

**Response to:**

**Release: Rel-15**

**Work Item: 5GS\_Ph1-SEC**

**Source: SA3**

**To: CT4**

**Cc:**

**Contact person: Bo Zhang**

**Zhangbo6@huawei.com**

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

**Attachments:** NONE

# 1 Overall description

SA3 would like to inform that modification policy handing in the IPX and receiving SEPP is not align between SA3 and CT4.

SA3 specified that the modification handling is performed on the clearTextEncapsulationMsg by the IPX, and pSEPP, i.e. TS 33.501, 13.2.4.5.2, IPX side:

*…The first intermediary shall parse the encapsulated request (i.e. the* ***clearTextEncapsulationMsg*** *in the dataToIntegrityProtect block) and determine which changes are required. The first intermediary creates an Operations JSON patch document to describe the differences between received and desired message, using the syntax and semantic from RFC 6902 [64], such that, when applying the JSON patch to the encapsulated request the result will be the desired request. If no patch is required, the operations element is null.*

TS 33.501, 13.2.4.8, pSEPP side:

*- The pSEPP updates the clearTextEncapsulationMessage block in the message by replacing the references to the dataToIntegrityProtectAndCipher block with the referenced decrypted values from the dataToIntegrityProtectAndCipher block.*

*- The pSEPP then verifies IPX provider updates of the attributes in the modificationsArray. It checks whether the modifications performed by the intermediaries were permitted by policy.*

*The pSEPP further verifies that the PLMN-ID contained in the message is equal to the "Remote PLMN-ID" in the related N32-f context.*

*- The pSEPP updates the modified values of the attributes in the* ***clearTextEncapsulationMessage*** *in order.*

However, CT4 specified that the modification handling is performed on the formed original JSON request / response body by the IPX and pSEPP, i.e. TS 29.573, 5.3.21, pSEPP side:

*5. For each entry in the "modificationsBlock" of the received message:*

*- First verify the integity protection of that entry using the keying material applicable for the IPX that inserted that block (using the "identity" IE in the "modificationsBlock");*

*- Identify the modifications policy exchanged during the parameter exchange procedure with the sending SEPP if the IPX that inserted the modificationsBlock is from the sending SEPP side; else identify the modifications policy applicable for the IPX based on local configuration;*

*- Check if the inserted modifications are as per the identified modifications policy;*

*- Apply the modifications as a JSON patch* ***over the formed original JSON request / response body from step 4.***

It is obvious that the relevant IPX should perform the corresponding modification over the formed original JSON request / response body according the handing in the pSEPP side in CT4.

Misalignment between SA3 and CT4 will mislead the reader and guys for implementation. Therefore, SA3 would like know whether the implementation in CT4 is workable or not? Here is our proposal:

- if the modification handling defined in CT4 is workable, please clarify the detailed procedure for the IPX and pSEPP, then SA3 will align with CT4, since no security issue is identified.

- if not workable, then please take the modification handling in SA3 specification into account. CT4 may have to align with SA3.

Furthermore, if further issues are identified on the SA3 mechanism by CT4, please let us know.

# 2 Actions

**To CT4**

**ACTION:** SA3 kindly asks CT4 to take the above information into consideration, and give the feedback.

# 3 Dates of next TSG SA WG 3 meetings

SA3#107-e-Bis 27 June – 01 July 2022 Electronic meeting (TBC)