**3GPP TSG-CT WG4 Meeting #99eC4-204xxx**

**E-Meeting, 18th – 28th August 2020**

Title: LS on Misalignments on HTTP message format over N32-f

Release: Rel-15 onwards

Work Item: 5GS Phase 1

Source: CT4

To: SA3

Cc:

**Contact Person:**

Name: Caixia Qi

Tel. Number:

E-mail Address: caixia.qi@huawei.com

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

Attachments: C4-204150 (DISC paper)

**1. Overall Description:**

CT4 has noted that misalignments exist between TS 33.501 and TS 29.573 on the JSON representation of a reformatted HTTP message, i.e. how to reformat the encrypted data:

- TS 33.501 Clause 13.2.4.2 specifies that the value part of encrypted data in DataToIntegrityProtect is null and there are additional paths to indicate the index of each encrypted data in dataToIntProtectAndCipher object.

- TS 29.573 A.3 OpenAPI of JOSE Protected Message Forwarding API on N32-f specifies that the value part of encrypted data in DataToIntegrityProtect indicates the index of the element in dataToIntProtectAndCipher object.

See details and quotes from the respective specifications in the attached DISC paper (C4-204150).

To align with the definition in TS 33.501, CT4 would need to define the new encodings in JOSE Protected Message Forwarding API on N32-f, which would be non-backward compatible changes to existing frozen stage 3 specification (Rel-15 and Rel-16).

CT4 kindly asks SA3 to indicate whether the current stage 3 protocol presents major security or robustness issues, and if not, to consider aligning TS 33.501 on TS 29.573 on the JSON representation of a reformatted HTTP message.

**2. Actions:**

**To SA3 group.**

**ACTION:** CT4 kindly asks SA3 group to indicate whether the current stage 3 protocol presents major security or robustness issues, and if not, to consider aligning TS 33.501 on TS 29.573 on JSON representation of a reformatted HTTP message.

**3. Date of Next CT4 Meetings:**

3GPP TSG CT4#101e 11/2020 E-Meeting