**3GPP TSG SA WG3 Meeting #100-e S3-201849-r5**

**e-meeting, 17 – 28 August 2020**

**Title:** Reply LS on N32-f Protection Policy IE Data-Type Mapping

**Response to:** S3-202055 / 5GIS Doc 11\_01

**Release:** Rel-15

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

**Source:** SA3

**To:** GSMA FASG 5GIS, CT4

**Cc:**

**Contact Person:**

#### Name: Bo Zhang

**Tel. Number:** +86 13410752800

E-mail Address: 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 thank GSMA FASG 5GIS for their LS on N32-f Protection Policy IE Data-Type Mapping. SA3 has evaluated these IEs and provide the following feedback.

**5GIS question 1:**

*Are these guidelines correct, or are there alternative guidelines which can be given?*

**SA3 Answer:**

SA3 would consider it sound practice to start by considering that all IEs are potentially sensitive. However, SA3 also understands that operators will rely on certain services by IPX providers that can only be provided if the IPX provider has access to the IE.

The specific encryption policy between operators can take into consideration the services that the involved IPX providers are supplying and differ from the default policy.

SA3 is not in the position to evaluate IPX services, and would therefore rely on GSMA to make prudent default assumptions that can be overridden by operator specific policies.

However, SA3 considers keys, authentication vector, and authorization tokens always as sensitive.

Following this general principle, the following concrete answers for default encryption policies are given:

|  |  |
| --- | --- |
| UEID | As SUPI, charging ID and GPSI are personally identifying information, they are seen potentially sensitive, i.e. they should be encrypted unless they need to be available to the IPX providers in order to provide the subscriber with services. |
| LOCATION | With the same reasoning as above, cell-id, physical cell id and TAI are potentially sensitive, unless they need to be available to the IPX providers in order to provide necessary services. |
| KEY\_MATERIAL | Please consider KSEAF as sensitive, and UPU related information as potentially sensitive. SA3 is not aware of IEs with the names encryptionKey and encryptionAlgorithm that are sent over the N32 interface. From a general point of view, though, please consider keys as sensitive and cryptographic algorithms as potentially sensitive. |
| AUTHENTICATION\_MATERIAL | Please consider authentication vectors as sensitive. Please consider EAP payload as potentially sensitive. |
| AUTHORIZATION\_TOKEN: | Please consider Authorization Tokens as sensitive. |
| OTHER | No comments |
| NON-SENSITIVE | No comments. |

**5GIS question 2:**

*Is it an objective for 3GPP to define the correct Data-Type for IEs?*

**SA3 Answer:**

SA3 considers it is an objective for SA3 to provide guidelines on which IEs need to be protected, and to assist with listing concrete IEs. SA3 currently does not plan to update TS 33.501 with concrete IEs.

**2. Actions:**

**To CT4 group.**

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

**To GSMA FASG 5GIS group.**

**ACTION:** SA3 kindly asks GSMA FASG 5GIS group to take above information into account.

**3. Date of Next TSG-SA WG3 Meetings:**

SA3#100Bis-e 12-16 Oct. 2020 eMeeting

SA3#101-e 9-20 Nov. 2020 eMeeting