**3GPP TSG-SA3 Meeting #102-e S3-210378**

**e-meeting, 18 – 29 January 2021, Online**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.517** | **CR** | 0007 | **rev** |  | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification on confidential IEs replacement handling in original N32-f message | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G | | | | |  | ***Date:*** | | | 2020-12-29 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | In SA3 #101e meeting, it was agreed to align the JSON format on encryption IE with CT4. Hence, the test case on the confidential IEs replacement handling in original N32-f message should be updated accordingly. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Change the “NULL” to “encBlockIdx” as defined in TS 29.573. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Not align with the procedure defined in TS 29.573. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.5, 2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | | **X** |  | Test specifications | | | | TR 33.926 CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\* BEGIN CHANGES \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.117: "Catalogue of General Security Assurance Requirements".

[3] 3GPP TS 33.501 (Release 15): "Security architecture and procedures for 5G system".

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[5] Void.

[X] 3GPP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection"

\*\* NEXT CHANGES \*\*\*

#### 4.2.2.5 Confidential IEs replacement handling in original N32-f message

*Requirement Name:* Confidential IEs replacement handling in original N32-f message

*Requirement Reference:* TS 29.573 [X], clause 5.3.2.3

*Requirement Description:*

" 1. Based on the protection policy exchanged between the SEPPs, the sending SEPP prepares an input for the JWE ciphering and integrity protection as an array of free form JSON objects in the "DataToIntegrityProtectAndCipher" block with each entry containing either a HTTP header value or the value of a JSON payload IE of the API message being reformatted. The index value "encBlockIdx" in the payload part of DataToIntegrityProtectBlock shall point to the index of a header value or IE value in this input array. ."

*Threat References:* TR 33.926 [4], clause G.2.4.2, Exposure of confidential IEs in N32-f message

*Test Case:*

**Purpose:**

Verify that the SEPP under test correctly replaces information elements requiring encryption with the value " encBlockIdx " and creates JSON patches containing the respective encrypted values in the dataToIntegrityProtectAndCipher object.

**Procedure and execution steps:**

**Pre-Conditions:**

- System documentation of the SEPP under test, which details how raw public keys/certificates of peer SEPPs are to be configured and how internal log files can be accessed.

- A second SEPP instance for N32 communication with the SEPP under test, which allows for the creation of custom N32-f messages. This system may be simulated.

- Both SEPPs are to be configured with a raw public key/certificate of their communication peer to be able to establish a N32-c connection.

- An arbitrary Data-type encryption policy which includes at least one information element requiring encryption on N32-f. The SEPP under test is to be configured with this policy.

**Execution Steps**

1. Both SEPPs establish a mutual N32-c connection.

2. Via the PLMN-internal interface, the tester provides the SEPP under test with a message to be forwarded to the peer SEPP on N32. This message needs to contain at least one information element that requires encryption according to the locally configured Data-type encryption policy.

3. The tester captures the related N32-f message after transformation by the SEPP under test.

**Expected Results:**

Information elements in the original message that require encryption according to the Data-type encryption policy are replaced with the value "encBlockIdx ".

**Expected format of evidence:**

Evidence suitable for the interface, e.g. text representation of the captured N32-f message.

\*\* END OF CHANGES \*\*\*