**3GPP TSG-SA3 Meeting #124 S3-253684-r9**

**Wuhan, China, 13 – 17 October 2025 merges 3270, 3271**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **-** | **Current version:** |  |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Information protection during command procedure - corrections | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Philips International B.V. | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AmbientIoT-SEC | | | | |  | ***Date:*** | | | 2025-10-06 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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:*** | | As per the current specification, the AIoT device always derives both Kcommand\_enc and Kcommand\_int  regardless of whether the received AIOT NAS Command Request is ciphered or not. As integrity protection is mandatory, the AIoT device is expected to always derive Kcommand\_int, however, ciphering is optional, and as such, the AIoT device should only derive Kcommand\_enc if integrity verification is succesfull and the ciphering indication in the AIOT NAS Command Request message indicates that ciphering is activated. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Changes cover:   * Editorials and corrections * Derivation of Kcommand\_enc being conditional on successful integrity verification and ciphering indication indicating that ciphering is activated. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Ambiguous specification text and unnecessary key derivation performed by the device even when ciphering is de-activated or integrity verification fails. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.2, 5.3.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **x** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

|  |
| --- |
| \*\*\* START OF CHANGES \*\*\* |

### 5.3.2 Security procedure on information protection during command procedure



Figure 5.3.2-1: Security procedure on the information protection during command procedure

1. The command procedure is initiated as specified in step 1-6 of clause 6.2.3 of TS 23.369 [2].

2. The procedure as described in clause 5.2.2 shall be performed. AIOTF acquire the KAIOTF key to be used for command protection. The derivation of KAIOTF key is specified in Annex A.3.

3. The AIOTF shall construct a AIOT NAS Command Request and protect the message based on the KCommand\_enc, KCommand\_int, and the confidentiality and integrity algorithms for the AIoT device. The AIOTF shall send the protected Command Request containing an indication on whether ciphering is activated to NG-RAN. The derivation of KCommand\_enc and KCommand\_int is specified in Annex A.4.

NOTE 1: The whole AIOT NAS Command Request message is integrity protected. If ciphering is activated (i.e., the ciphering algorithm is 128-NEA2), the AIOT NAS Command Request message is partly ciphered with the exception that the indication on whether ciphering is activated is in clear text.

4. The NG-RAN shall send a R2D message containing the protected AIOT NAS Command Request as specified in TS 38.300 [3] and TS 38.391 [6].

NOTE 2: It is left to implementation when KAIOTF is derived on the device.

5. The device shall derive the KCommand\_enc, KCommand\_int, and process the protected AIOT NAS Command Request. If the verification of integrity is successful, the AIoT device shall decipher the protected AIOT NAS Command Request if ciphering is activated. The AIoT device shall construct an AIOT NAS Command Response and protect it based on the derived key(s).

6. The AIoT device shall send a D2R message containing the protected AIOT NAS Command Response to the NG-RAN as specified in TS 38.300 [3] and TS 38.391 [6].

7. The NG-RAN shall forward the protected AIOT NAS Command Response to the AIOTF.

8-9. The AIOTF shall process the protected AIOT NAS Command Response. If the verification of integrity is successful, the AIOTF shall decipher the protected AIOT NAS Command Reponse if ciphering is activated. Then, the AIOTF shall continue the procedure as specified in clause 6.2.3 of TS 23.369 [2].

NOTE 2: It is assumed that there is only one round of command procedure per device following an inventory procedure. Since the KAIOTF key is fresh, there is no need for additional freshness parameters for replay protection.

NOTE 3: It is assumed that in the present document no new algorithms will ever be introduced for information protection during command procedure.

|  |
| --- |
| \*\*\* NEXT CHANGE \*\*\* |

### 5.3.3 Input and output parameters to integrity algorithm

The input parameters to the integrity algorithm as described in Annex D.3 in TS 33.501[5] shall be set as follows.

The KEY input is equal to the K Command\_int key.

The MESSAGE is set to the content of AIOT NAS Command Request or AIOT NAS Command Response.

The DIRECTION bit is set to 0 for uplink and 1 for downlink.

The BEARER is set to all zeros.

The COUNT is set to all zeros.

The output is a 32-bit message authentication codeused for integrity verification.

|  |
| --- |
| \*\*\* END OF CHANGES \*\*\* |