**3GPP TSG-SA5 Meeting #157 *S5-246204d1***

Hyderabad, India, 14 - 18 October 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **3** | **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 |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | R18 CR 32.421 missing Sec requirements  |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S5 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2024-10-04 |
|  |  |  |  |  |
| ***Category:*** | **A** |  | ***Release:*** | Rel-18 |
|  | *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 canbe 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 specified in the incoming LS (S3-243696), “To mitigate security risks related to inadvertent leakage of security key(s) from the core network nodes, 3GPP SA WG3 proposes to include security requirements for masking security keys specified in clause 6.2 of TS 33.401 and in clause 6.2.2.1 of TS 33.501 in UE trace file.”In TS32.421, the security requirements are defined for eNB and NG-RAN. However, the security requirements on core network are missing. |
|  |  |
| ***Summary of change:*** | Adding the missing security requirements on EPC and 5GC |
|  |  |
| ***Consequences if not approved:*** | Misligned security requirements could lead to security risk at implemenations  |
|  |  |
| ***Clauses affected:*** | 2, 5.6 |
|  |  |
|  | **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:*** | Revision of S5-241141 |

\*\*\* START OF NEXT CHANGE \*\*\*

# 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 TS 32.101: "Telecommunication management; Principles and high level requirements".

[2] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace: Trace control and configuration management".

[3] 3GPP TS 32.423: "Telecommunication management; Subscriber and equipment trace: Trace data definition and management".

[4] 3GPP TS 23.002: "Network architecture".

[6] Void

[7] 3GPP TS 52.008: "Telecommunication management; GSM subscriber and equipment trace".

[8] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[9] OMA Service Provider Environment Requirements, OMA-RD-OSPE-V1\_0-20050614-C, The Open Mobile Alliance™ (URL:http://www.openmobilealliance.org/).

[10] 3GPP TS 33.401: "System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 37.320 : "Universal Terrestrial Radio Access (UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRA); Radio measurement collection for Minimization of Drive Tests (MDT); Overall description, Stage 2".

[12] 3GPP TS 32.450: "Key Performance Indicators (KPI) for Evolved Universal Terrestrial Radio Access Network (E-UTRAN): Definitions".

[13] 3GPP TS 32.130: "Network sharing; Concepts and requirements".

[14]3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[15] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[16] 3GPP TS 38.300: "NR and NG-RAN Overall Description; Stage 2".

[17] 3GPP TS 38.401: "NG-RAN; Architecture Description".

[18] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol Specification".

[19] 3GPP TS 25.331: "Radio Resource Control (RRC); protocol specification".

[20] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)"

[21] 3GPP TS 38.423: "NG-RAN; Xn Application Protocol (XnAP)"

[22] 3GPP TS 28.533: "Management and orchestration; Architecture framework"

[x] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

NOTE: Void.

\*\*\* START OF NEXT CHANGE \*\*\*

## 5.6 Requirements for Privacy and Security

The high-level requirements for privacy and security, specific for Service Level Tracing for IMS are as follows:

The following high-level OMA Service Level Tracing requirements apply [9].

[SLT-PRV-1] with the following clarification:

- Privacy shall be applied across the appropriate Trace Itf-N.

[SLT-SEC-1]

[SLT-SEC-2]

[SLT-SEC-3] with the following clarification:

- It may not be possible to retrieve Trace information from IMS NEs from outside the PLMN where the IMS NEs reside.

[SLT-IOP-1] with the following clarification:

- The propagation of the Trace Parameter Configuration and the Start Trigger event shall be prohibited by the PLMN when e.g. the SIP AS is hosted outside a PLMN.

As the radio access nodes in E-UTRAN are outside an operator’s secure domain, the following requirement applies for E-UTRAN as described in 3GPP TS 33.401 [10]:

[SET-SEC-1] Keys stored inside eNBs shall never leave a secure environment within the eNB. When security key(s) transported on control signalling messages are included in the trace file, the key value(s) shall be removed and replaced with the value “Unavailable”.

As the radio access nodes in NG-RAN are outside an operator’s secure domain, the following requirement applies for NG-RAN as described in 3GPP TS 38.401 [17]:

[SET-SEC-2] Keys stored inside NG-RAN node shall never leave a secure environment within the NG-RAN node. When security key(s) transported on control signalling messages are included in the trace file, the key value(s) shall be removed and replaced with the value "Unavailable".

As the receiving entities may be outside an operator’s EPC secure domain, the following requirement applies for EPC as described in 3GPP TS 33.401 [10]:

[SET-SEC-3] Security Keys, as described in subclause 6.2 of 3GPP TS 33.401 [10], stored inside EPC entity shall never leave a secure environment within the EPC node for UE trace purpose. When control signalling messages containing security key(s) are included in the trace output the security key value(s) shall be replaced with a value to indicate they are unavailable.

As the receiving entities may be outside an operator’s 5GC secure domain, the following requirement applies for 5GC as described in 3GPP TS 33.501 [x]:

[SET-SEC-4] Security Keys, described in subclause 6.2.2.1 of TS 33.501 [x], stored inside 5GC entity shall never leave a secure environment within the 5GC node for UE trace purpose. When control signalling messages containing security key(s) are included in the trace output the security key value(s) shall be replaced with a value to indicate they are unavailable.

The high-level requirements for privacy and security in case of streaming trace reporting are as follows:

- The connection between data producer and data consumer shall provide the data privacy.

- The connection between data producer and data consumer shall provide the data integrity.

\*\*\* END OF CHANGE \*\*\*