**3GPP TSG-SA5 Meeting #157 *S5-245261rev1***

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 | **x** | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | R15 CR 32.423 missing Sec requirements  |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S5 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2024-10-04 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** | Rel-15 |
|  | *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.”However, the stage 3 security requirements are missing in TS32.423. |
|  |  |
| ***Summary of change:*** | Adding the missing stage 3 security requirements  |
|  |  |
| ***Consequences if not approved:*** | Missing security requirements could lead to security risk at implemenations  |
|  |  |
| ***Clauses affected:*** | 2, 4.1, 4.1, 4.13 |
|  |  |
|  | **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 S5-241142 |

\*\*\* 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 32.421: "Telecommunication management; Subscriber and equipment trace: Trace concepts and requirements."

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

[4] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[5] W3C Recommendation "Extensible Markup Language (XML) 1.0" (Second Edition, 6 October 2000) http://www.w3.org/TR/2000/REC-xml-20001006

[6] W3C Recommendation "Namespaces in XML" (14 January 1999)
http://www.w3.org/TR/1999/REC-xml-names-19990114

[7] W3C Recommendation "XML Schema Part 0: Primer" (2 May 2001)
http://www.w3.org/TR/2001/REC-xmlschema-0-20010502

[8] W3C Recommendation "XML Schema Part 1: Structures" (2 May 2001)
http://www.w3.org/TR/2001/REC-xmlschema-1-20010502

[9] W3C Recommendation "XML Schema Part 2: Datatypes" (2 May 2001)
http://www.w3.org/TR/2001/REC-xmlschema-2-20010502

[10] International Standard ISO 8601: 1988 (E) "Representations of dates and times" (1988-06-15)
http://www.iso.ch/markete/8601.pdf

[11] 3GPP TS 32.300: "Telecommunication management; Configuration Management (CM); Name convention for Managed Objects".

[12] 3GPP TS 32.622: "Telecommunication management; Configuration Management (CM); Generic network resources Integration Reference Point (IRP): Network Resource Model (NRM)".

[13] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[14] 3GPP TS 29.212: "Policy and Charging Control (PCC);Reference points".

[15] 3GPP TS 29.273: "Evolved Packet System (EPS); 3GPP EPS AAA interfaces".

[16] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[17] 3GPP TS 36.423 "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 Application Protocol (X2AP)".

[18] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[19] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2"

[20] 3GPP TS 38.300: "NR and NG-RAN Overall Description; Stage 2".

[21] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[22] 3GPP TS 38.401: "NG-RAN; Architecture Description".

[23] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[24] 3GPP TS 38.423: "NG-RAN; Xn Application Protocol (XnAP)".

[25] 3GPP TS 38.463: "NG-RAN; E1 Application Protocol (E1AP)".

[26] 3GPP TS 38.473: "NG-RAN; F1 Application Protocol (F1AP)".

[27] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[28] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[29] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[30] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol specification".

[31] 3GPP TS 36.314: "Evolved Universal Terrestrial Radio Access (E-UTRA); Layer 2 - Measurements".

[32] 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".

[33] 3GPP TS 36.213: "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures".

[34] 3GPP TS 36.133: "Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for support of radio resource management".

[x1] 3GPP TS 33.401: "System Architecture Evolution (SAE); Security architecture".

[x2] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

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

## 4.1 General

The trace reference, trace type and operation system identification are all provided on trace activation.
Each record may contain an MSC Server, MGW, SGSN, GGSN, S-CSCF, P-CSCF, UTRAN, HSS, MME, Serving GW, E-UTRAN, AUSF, AMF, NEF, NRF, NSSF, PCF, SMF, SMSF, UDM, UPF, AF and , ng-eNB, gNB-CU-CP, gNB-CU-UP and gNB-DU event record. A key is included in the table indicating whether or not the field is mandatory.

The following table shows the template for trace record description for minimum and medium trace depth:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Interface name | Protocol name | IE name | Message name(s) | Trace depth | Notes |
| **Min** | **Med** |
|  |  |  |  |  |  |  |

**Interface name**: Contains the name of the interface, where the IE is available.

**Protocol name**: Contains the protocol name on the interface, where the IE is available.

**IE name**: The name of the Information Element, which should be decoded.

**Message name(s):** The name of the message(s), where the IE is included.

**Trace depth**: Shows in which trace depth the IE should be recorded. It also classifies whether the IE is mandatory in the trace record or not (M, O or X: meaning described in the previous table)

|  |  |  |
| --- | --- | --- |
| **M** | Mandatory | This field must be in the trace record if it is available, i.e. if the message appears during the trace recording session and the IE is present in the message. |
| **O** | Optional | This field is optional and its support is a matter for agreement between equipment manufacturer and network operator. |
| **X** | Not applicable | This field is not required in this instance. |
| **CM** | Conditional Mandatory | This field must be in the trace record if it is available and the condition is met. |

NOTE: Any kind of comments related to the IE can be made here. Also this is the placeholder for referencing the relevant 3GPP specifications, which define the IE.

Receiving nodes may be outside an operator’s secure domain.  For any IEs or parts of IEs containing security keys as specified in subclause 6.2 of 3GPP TS 33.401 [x1] and subclause 6.2.2.1 of TS 33.501 [x2] (e.g. KeNB) the value 0 shall be written in the trace file.

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

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

## 4.13 E-UTRAN Trace Record Content

For eNB, the Maximum level of detail shall be supported. The trace record is the same for management based activation and for signalling based activation.

Table 4.13.1 : E-UTRAN Trace Record Content

|  |  |  |  |
| --- | --- | --- | --- |
| **Interface (specific messages)** | **Format** | **Level of details** | **Description** |
| **Min** | **Med** | **Max** |
| RRC (without rrc dedicated measurements) | Decoded | **M** | **M** | **O** | Message name  |
| **O** | **O** | **O** | Record extensions |
| **M** | **M** | **X** | Global eNBID of traced eNB |
| **M** | **M** | **X** | Dedicated IE extracted from RRC messages between the traced eNB and the UE. A subset of IEs as given in the table 4.13.2. is provided. |
| ASN.1 | **X** | **X** | **M** | Raw Uu Messages: RRC messages between the traced eNB and the UE. The encoded content of the message is provided |
| S1 | Decoded | **M** | **M** | **O** | Message name  |
| **O** | **O** | **O** | Record extensions |
| **M** | **M** | **X** | Global eNBID of traced eNBMME ID of the connected MME |
| **M** | **M** | **X** | E-RabId + Dedicated IE extracted from S1AP messages between the traced eNB and Core Network. A subset of IEs as given in the table 4.13.2. is provided. |
| ASN.1 | **X** | **X** | **M** | Raw S1 Messages S1AP: messages between the traced eNB and Core Network The encoded content of the message is provided |
| X2 | Decoded | **M** | **M** | **O** | Message name  |
| **O** | **O** | **O** | Record extensions |
| **M** | **M** | **X** | Global eNBID of traced eNBGlobal eNBID of neighbouring eNBGlobal gNBID of connected gNB-CU-CP node over X2 (for NSA) |
| **M** | **M** | **X** | Dedicated IE extracted from X2AP messages between the traced eNB and the neighbouring eNB/connected gNB-CU-CP. A subset of IEs as given in the table 4.13.2.is provided |
| ASN.1 | **X** | **X** | **M** | Raw X2 Messages:X2AP messages between the traced eNB and the neighbouring eNB/connected gNB-CU-CP. The encoded content of the message is provided |
| RRC (only dedicated measurements) | Decoded | **X** | **M** | **X** | Uu IEs from RRC measurement reports messages |
| ASN.1 | **X** | **X** | **M** | RRC measurement reports messages |

**Definitions:**

Global eNBID of traced eNB: The id of the eNB traced, e.g. the eNB which handles the connection of the traced MS, during the Trace Recording Session. The id corresponds to the “Global eNB ID”, as defined in [16] and [17].

Global eNBID of neighbouring eNB: The ids of all Neighbouring eNB involved in the X2 procedures during the Trace Recording Session. The id corresponds to the “Global eNB ID”, as defined in [16] and [17].

Global gNBID of connected gNB-CU-CP node over X2 (for NSA): The ids of all connected NSA nodes involved during the Trace Recording Session. The id corresponds to the “Global gNB ID”, as defined in [16] and [17].

cell Id: The cell Ids of the cells involved in the X2 procedures during the Trace Recording Session. The cell Ids is provided with each X2AP messages for which the cId is relevant.

E-RABId: Specific recorded IE that contains the E-RAB identifier.

Message name: Name of the protocol message

Record extensions: A set of manufacturer specific extensions to the record

Decoded: Some IEs shall be decoded (cf. detailed list in table 4.6.2. depending on trace depth)

ASN.1: Messages in encoded format

Table 4.13.2 : trace record description for minimum and medium trace depth

| **Interface name** | **Prot.****name** | **IE name** | **Message name(s)** | **Trace depth** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| **Min** | **Med** |
| Uu | RRC | Cs fallback indicator | MOBILITY FROM EUTRA COMMAND | **M** | **M** | TS 36.331 |
| CN domain | PAGING | **O** | **O** | TS 36.331 |
| S-TMSI | PAGING | **O** | **O** | TS 36.331 |
| ReestablishmentCause | RRC CONNECTION REESTABLISHMENT REQUEST | **M** | **M** | TS 36.331 |
| Wait time | RRC CONNECTION REJECT | **CM** | **M** | TS 36.331 |
| Release Cause | RRC CONNECTION RELEASE | **M** | **M** | TS 36.331 |
| Redirection Information | RRC CONNECTION RELEASE | **M** | **M** | TS 36.331 |
| Establishment Cause | RRC CONNECTION REQUEST | **CM** | **CM** | TS 36.331 |
| Selected PLMN-Identity | RRC CONNECTION SETUP COMPLETE | **CM** | **CM** | TS 36.331 |
| RegisteredMME | RRC CONNECTION SETUP COMPLETE | **CM** | **CM** | TS 36.331 |
| Rat-Type | UE CAPABILITY INFORMATION | **M** | **M** | TS 36.331 |
| Measured Results | MEASUREMENT REPORT | **X** | **M** | TS 36.331 |
| CDMA2000-Type | HANDOVER FROM EUTRA PREPARATION REQUESTUL HANDOVER PREPARATION TRANSFERUL INFORMATION TRANSFER | **M** | **M** | TS 36.331 |
| Target RAT Type | MOBILITY FROM EUTRA COMMAND | **M** | **M** | TS 36.331 |
| ConnEstFailReport-r11 | UE INFORMATION RESPONSE | **X** | **M** | TS 36.331 |
| RLF-Report-r9 | UE INFORMATION RESPONSE | **X** | **M** | TS 36.331 |
| S1 | S1AP | E-RAB ID | All messages where it is present | **M** | **M** | TS 36.413 |
| E-RAB Level QoS Parameters | E-RAB SETUP REQUESTE-RAB MODIFY REQUESTINITIAL CONTEXT SETUP REQUEST | **M** | **M** | TS 36.413 |
| Cause | INITIAL CONTEXT SETUP FAILUREUE CONTEXT RELEASE REQUESTUE CONTEXT RELEASE COMMANDUE CONTEXT MODIFICATION FAILUREHANDOVER REQUIREDHANDOVER PREPARATION FAILUREHANDOVER REQUESTHANDOVER FAILUREHANDOVER CANCELPATH SWITCH REQUEST FAILURENAS NON DELIVERY INDICATION | **M** | **M** | TS 36.413 |
| Handover Type | HANDOVER REQUIREDHANDOVER COMMANDHANDOVER REQUEST | **M** | **M** | TS 36.413 |
| E-UTRAN CGI | HANDOVER NOTIFYPATH SWITCH REQUESTINITIAL UE MESSAGEUPLINK NAS TRANSPORT | **CM** | **CM** | TS 36.413 |
| TAI | HANDOVER NOTIFYPATH SWITCH REQUESTUPLINK NAS TRANSPORT | **M** | **M** | TS 36.413 |
| Target ID | HANDOVER REQUIRED | **M** | **M** | TS 36.413 |
| CDMA2000 HO Status | DOWNLINK S1 CDMA2000 TUNNELING | **M** | **M** | TS 36.413 |
| CDMA2000 RAT Type | DOWNLINK S1 CDMA2000 TUNNELINGUPLINK S1 CDMA2000 TUNNELING | **M** | **M** | TS 36.413 |
| CDMA2000 Sector ID | UPLINK S1 CDMA2000 TUNNELING | **M** | **M** | TS 36.413 |
| CDMA2000 HO Required Indication | UPLINK S1 CDMA2000 TUNNELING | **M** | **M** | TS 36.413 |
| X2 | X2AP | E-RAB id | All messages where it is present | **M** | **M** | TS 36.423 |
| E-RAB Level QoS | HANDOVER REQUESTSGNB ADDITION REQUESTSGNB ADDITION REQUEST ACKNOWLEDGESGNB MODIFICATION REQUESTSGNB MODIFICATION REQUEST ACKNOWLEDGESGNB MODIFICATION REQUIRED | **M** | **M** | TS 36.423 |
| Cause | HANDOVER REQUESTHANDOVER PREPARATION FAILUREHANDOVER CANCELSGNB ADDITION REQUEST REJECTSGNB RECONFIGURATION COMPLETESGNB MODIFICATION REQUESTSGNB MODIFICATION REQUEST REJECTSGNB MODIFICATION REQUIREDSGNB MODIFICATION REFUSESGNB RELEASE REQUESTSGNB RELEASE REQUEST REJECTSGNB RELEASE REQUIREDSGNB CHANGE REQUIREDSGNB CHANGE REFUSE | **M** | **M** | TS 36.423 |
| Target Cell ID | HANDOVER REQUEST | **M** | **M** | TS 36.423 |
| GUMMEI | HANDOVER REQUEST | **M** | **M** | TS 36.423 |
| UE History Information | HANDOVER REQUEST | **M** | **M** | TS 36.423 |
| UE RLF Report Container | RLF INDICATION | **X** | **M** | TS 36.423 |

 **Constraints:**

The condition for capturing the following Information Element is that Cell Traffic Trace is used:

- Wait time from RRC protocol.

- Establishment Cause from RRC protocol.

- Selected PLMN-Identity from RRC protocol.

- RegisteredMME from RRC protocol.

- E-UTRAN CGI from S1 interface from the following messages: Initial UE message, Handover Notify.