**3GPP TSG-SA3 Meeting #105-e *S3-213875***

e-meeting, 8 - 19 November 2021

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.512** | **CR** |  | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  |
| *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:***  | 33.512 – Alignment with TS 33.501 Rel-17 |
|  |  |
| ***Source to WG:*** | Keysight Technologies |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eSCAS\_5G |  | ***Date:*** | 2021-10-27 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *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:*** | Alignment of TS 33.512 to TS 33.501 for Rel-17 |
|  |  |
| ***Summary of change:*** | Updated references to TS 33.501 and changes in related texts. Some minor editorial changes |
|  |  |
| ***Consequences if not approved:*** | Incorrect references to previous releases documents. |
|  |  |
| ***Clauses affected:*** | 2, 4.2.2.1.1, 4.2.2.1.2, 4.2.2.1.3, 4.2.2.3.1, 4.2.2.3.2, 4.2.2.3.3, 4.2.2.4.1, 4.2.2.4.2, 4.2.2.5.1, 4.2.2.9.1 |
|  |  |
|  | **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:*** | Reference [7] is not used in the document right now, then we propose to re-use to Release 17. |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\* START OF CHANGE 1 \*\*\*\*

# 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 33.501 (Release 15): "Security architecture and procedures for 5G system".

[3] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[4] 3GPP TS 23.003: "Numbering, addressing and identification".

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

[6] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[8] 3GPP TS 23.501: "System Architecture for the 5G System".

[9] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

\*\*\*\* END OF CHANGE 1 \*\*\*\*

\*\*\*\* START OF CHANGE 2 \*\*\*\*

##### 4.2.2.1.1 Synchronization failure handling

*Requirement Name*: Synchronization failure handling

*Requirement Reference:* TS 33.501 [7], clause 6.1.3.3.2

*Requirement Description*: "Upon receiving an authentication failure message *with synchronisation failure* (AUTS) from the UE, the SEAF sends an Nausf\_UEAuthentication\_Authenticate Request message with a "*synchronisation failure indication*" to the AUSF and the AUSF sends an Nudm\_UEAuthentication\_Get Request message to the UDM/ARPF, together with the following parameters:

*- RAND* sent to the UE in the preceding Authentication Request, and

*- AUTS* received by the SEAF in the response from the UE to that request, as described in clause 6.1.3.2.0 and 6.1.3.3.1.

An SEAF will not react to unsolicited "synchronisation failure indication" messages from the UE.

The SEAF does not send new authentication requests to the UE before having received the response to its Nausf\_UEAuthentication\_Authenticate Request message with a "*synchronisation failure indication*" from the AUSF (or before it is timed out). "

as specified in TS 33.501[7], clause 6.1.3.3.2.

\*\*\*\* END OF CHANGE 2 \*\*\*\*

\*\*\*\* START OF CHANGE 3 \*\*\*\*

##### 4.2.2.1.2 RES\* verification failure handling

*Requirement Name*: RES\* verification failure handling

*Requirement Reference:* TS 33.501 [7], clause 6.1.3.2.2

*Requirement Description*:

"The SEAF shall proceed with step 10 in Figure 6.1.3.2-1 and after receiving the Nausf\_UEAuthentication\_Authenticate Request message from the AUSF in step 12 in Figure 6.1.3.2-1, proceed as described below:

- If the AUSF has indicated in the Nausf\_UEAuthentication\_Authenticate Response message to the SEAF that the verification of the RES\* was not successful in the AUSF, or

- if the verification of the RES\* was not successful in the SEAF,

then the SEAF shall either reject the authentication by sending an Authentication Reject to the UE if the SUCI was used by the UE in the initial NAS message or the SEAF/AMF shall initiate an Identification procedure with the UE if the 5G-GUTI was used by the UE in the initial NAS message to retrieve the SUCI and an additional authentication attempt may be initiated.

Also, if the SEAF does not receive any Nausf\_UEAuthentication\_Authenticate Request message from the AUSF as expected, then the SEAF shall either reject the authentication to the UE or initiate an Identification procedure with the UE."

As specified in TS 33.501 [7], clause 6.1.3.2.2.

\*\*\*\* END OF CHANGE 3 \*\*\*\*

\*\*\*\* START OF CHANGE 4 \*\*\*\*

##### 4.2.2.1.3 NAS based redirection from 5GS to EPS

*Requirement Name*: NAS based redirection from 5GS to EPS

*Requirement Reference:* TS 33.501 [7], clause 6.16.4, TS 23.501 [8], clause 5.31.3.

*Requirement Description*: "When a UE initiates registration procedure with the AMF, the AMF may redirect the UE from 5GC to EPC by including a EMM cause indicating to the UE that it shall not use 5GC, as described in clause 5.31.3 in TS 23.501 [2]. The following requirements apply to Registration Reject message with an EMM cause which indicates to the UE that the UE shall not use 5GC:

- the AMF shall only send such a Registration Reject message once NAS security has been established between the AMF and the UE; and

- the UE shall only act upon such Registration Reject message if received integrity protected and if UE has verified the integrity of the Registration Reject message successfully.

NOTE: This solution does not apply to unauthenticated emergency calls.

" as specified in TS 33.501 [7], clause 6.16.4.

"In networks that support CIoT features in both EPC and 5GC, the operator may steer UEs from a specific CN type due to operator policy, e.g. due to roaming agreements, Preferred and Supported Network Behaviour, load redistribution, etc. Operator policies in EPC and 5GC are assumed to avoid steering UEs back and forth between EPC and 5GC.

##### " as specified in TS 23.501 [8], clause 5.31.3.

\*\*\*\* END OF CHANGE 4 \*\*\*\*

\*\*\*\* START OF CHANGE 5 \*\*\*\*

##### 4.2.2.3.1 Replay protection of NAS signalling messages

*Requirement Name:* Replay protection of NAS signalling messages

*Requirement Reference:* TS 33.501 [7], clause 5.5.2.

*Requirement Description:* " The AMF shall support integrity protection and replay protection of NAS-signalling." as specified in TS 33.501 [2], clause 5.5.2.

\*\*\*\* END OF CHANGE 5 \*\*\*\*

\*\*\*\* START OF CHANGE 6 \*\*\*\*

##### 4.2.2.3.2 NAS NULL integrity protection

*Requirement Name*: NAS NULL integrity protection

*Requirement Reference:* TS 33.501 [7], clause 5.5.2

*Requirement Description*: "NIA0 shall be disabled in AMF in the deployments where support of unauthenticated emergency session is not a regulatory requirement." as specified in TS 33.501 [7], clause 5.5.2

\*\*\*\* END OF CHANGE 6 \*\*\*\*

\*\*\*\* START OF CHANGE 7 \*\*\*\*

##### 4.2.2.3.3 NAS integrity algorithm selection and use

*Requirement Name*: NAS integrity algorithm selection and use

*Requirement Reference:* TS 33.501 [7], clause 6.7.1

*Requirement Description*: "The AMF shall then initiate a NAS security mode command procedure, and include the chosen algorithm and UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE (see sub-clause 6.7.2 of the present document). The AMF shall select the NAS algorithm which have the highest priority according to the ordered lists." as specified in TS 33.501 [7], clause 5.5.2.

\*\*\*\* END OF CHANGE 7 \*\*\*\*

\*\*\*\* START OF CHANGE 8 \*\*\*\*

##### 4.2.2.4.1 Bidding down prevention in Xn-handover

*Requirement Name*: Bidding down prevention in Xn-handovers

*Requirement Reference:* TS 33.501 [7], clause 6.7.3.1

*Requirement Description*: "In the Path-Switch message, the target gNB/ng-eNB shall send the UE's 5G security capabilities received from the source gNB/ng-eNB to the AMF. The AMF shall verify that the UE's 5G security capabilities received from the target gNB/ng-eNB are the same as the UE's 5G security capabilities that the AMF has locally stored. If there is a mismatch, the AMF shall send its locally stored 5G security capabilities of the UE to the target gNB/ng-eNB in the Path-Switch Acknowledge message. The AMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm."

as specified in TS 33.501 [7], clause 6.7.3.1.

\*\*\*\* END OF CHANGE 8 \*\*\*\*

\*\*\*\* START OF CHANGE 9 \*\*\*\*

##### 4.2.2.4.2 NAS protection algorithm selection in AMF change

*Requirement Name*: NAS protection algorithm selection in AMF change

*Requirement Reference:* TS 33.501 [7], clause 6.7.1.2

*Requirement Description*: "If the change of the AMF at N2-Handover or mobility registration update results in the change of algorithm to be used for establishing NAS security, the target AMF shall indicate the selected algorithm to the UE as defined in Clause 6.9.2.3.3 for N2-Handover (i.e., using NAS Container) and Clause 6.9.3 for mobility registration update (i.e., using NAS SMC). The AMF shall select the NAS algorithm which has the highest priority according to the ordered lists (see sub-clause 6.7.1.1 of the present document)."

as specified in TS 33.501 [7], clause 6.7.1.2.

\*\*\*\* END OF CHANGE 9 \*\*\*\*

\*\*\*\* START OF CHANGE 10 \*\*\*\*

##### 4.2.2.5.1 5G-GUTI allocation

*Requirement Name*: 5G-GUTI allocation

*Requirement Reference:* TS 33.501 [7], clause 6.12.3

*Requirement Description*: "A new 5G-GUTI shall be sent to a UE only after a successful activation of NAS security. The 5G-GUTI is defined in TS 23.003 [19].

Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE, the AMF shall send a new 5G-GUTI to the UE during the registration procedure.

Upon receiving Registration Request message of type "periodic registration update" from a UE, the AMF should send a new 5G-GUTI to the UE during the registration procedure.

Upon receiving Service Request message sent by the UE in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the N1 NAS signalling connection is suspended.

Upon receiving an indication from the lower layers that the RRC connection has been resumed for a UE in 5GMM-IDLE mode with suspend indication in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the suspension of the N1 NAS signalling connection.NOTE 1: It is left to implementation to re-assign 5G-GUTI more frequently than in cases mentioned above, for example after a Service Request message from the UE not triggered by the network.

NOTE 2: It is left to implementation to generate 5G-GUTI containing 5G-TMSI that uniquely identifies the UE within the AMF."

as specified in TS 33.501 [7], clause 6.12.3.

\*\*\*\* END OF CHANGE 10 \*\*\*\*

\*\*\*\* START OF CHANGE 11 \*\*\*\*

##### 4.2.2.9.1 NSSAA revocation

*Requirement Name*: NSSAA revocation

*Requirement Reference:* TS 33.501 [7], clause 16.5

*Requirement Description*: " If no S-NSSAI is left in Allowed NSSAI for an access after the revocation, and no Default NSSAI can be provided to the UE in the Allowed NSSAI or a previous NSSAA failed for the Default NSSAI over this access, then the AMF shall execute the Network-initiated Deregistration procedure for the access as described in subclause 4.2.2.3.3 in TS 23.502 [8], and it shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value. "

as specified in TS 33.501[7], clause 16.5

\*\*\*\* END OF CHANGE 11 \*\*\*\*