**3GPP TSG-CT1 Meeting #126-e *C1-20xxxx***

**Electronic meeting, 15-23 October 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **2780** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  |
| *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:***  | AMF behavior in case of NSSAA failure due to “504 gateway timeout” |
|  |  |
| ***Source to WG:*** | LG Electronics , Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** |  5GProtoc17 |  | ***Date:*** | 2020-10-08 |
|  |  |  |  |  |
| ***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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | In the previous CT meeting, C1-203894 was agreed as follows.***If the AMF receives the HTTP code set to "4xx" or "5xx" as specified in 3GPP TS 29.500 [x] or the AMF detects that the NSSAAF failure as specified in 3GPP TS 29.526 [y] during the NSSAA procedure for an S-NSSAI, then the AMF considers the NSSAA procedure has failed for this S-NSSAI.***In this case, the AMF stores failed S-NSSAI into the rejected NSSAI.In case of HTTP code set “504 gateway timeout”, the Authentication message does not reach to AAA-S. In this case, in AAA-S perspective, the authentication procedure is not performed. So, re-authentification procedure can not be performed. Also, NSSAA initianted procedure is triggered by requested NSSAI (incluing pending NSSAI). But this S-NSSAI is rejected NSSAI. So, the UE and AMF will not trigger NSSAA procedure.Also, in case of “504 gateway timeout” due to temporary NW problem, if another NSSAA procedure is triggered later, the NSSAA procedure can be success.Therefore, considering HTTP code set “5xx”, the specification should provide the AMF trigger initiating NSSAA procedure for rejected NSSAI. Also, the specification should give The AMF freedom to initiate NSSAA depending on HTTP code set. |
|  |  |
| ***Summary of change:*** | In case of NSSAA failure, the AMF can trigger NSSAA initiating procedure for rejected NSSAI. |
|  |  |
| ***Consequences if not approved:*** | Due to temporary NW problem, the AMF receives HTTP code set “504 gateway timeout”, the NSSAA procedure can not be triggered by NW. |
|  |  |
| ***Clauses affected:*** | 4.6.1 |
|  |  |
|  | **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:*** |  |
|  |  |
| ***This CR's revision history:*** | Rev.1 1. The reason for re-initiating re-NSSAA procedure by AMF is changed from “HTTP code set 504 gateway timeout” to “UE local policy”, because the AMF does not store NSSAA failure status with different cause according to the TS29.571.
2. ME box is unchecked and CN box is checked.
3. Changed NOTE2 to NOTE3
 |

#### \*\*\*\*\* First change \*\*\*\*\*

### 4.6.1 General

The 5GS supports network slicing as described in 3GPP TS 23.501 [8]. Within a PLMN or SNPN, a network slice is identified by an S-NSSAI, which is comprised of a slice/service type (SST) and a slice differentiator (SD). Inclusion of an SD in an S-NSSAI is optional. A set of one or more S-NSSAIs is called the NSSAI. The following NSSAIs are defined in 3GPP TS 23.501 [8]:

a) configured NSSAI;

b) requested NSSAI;

c) allowed NSSAI;

d) subscribed S-NSSAIs; and

e) pending NSSAI.

The following NSSAIs are defined in the present document:

a) rejected NSSAI for the current PLMN or SNPN;

b) rejected NSSAI for the current registration area; and

c) rejected NSSAI for the failed or revoked NSSAA.

In roaming scenarios, rejected NSSAI for the current PLMN or SNPN, or rejected NSSAI for the current registration area also contains a set of mapped HPLMN S-NSSAI(s) if available and the S-NSSAI(s) included in the rejected NSSAI for the failed or revoked NSSAA is HPLMN S-NSSAI(s).

In case of a PLMN, a serving PLMN may configure a UE with the configured NSSAI per PLMN. In addition, the HPLMN may configure a UE with a single default configured NSSAI and consider the default configured NSSAI as valid in a PLMN for which the UE has neither a configured NSSAI nor an allowed NSSAI. In case of an SNPN, the SNPN may configure a UE with a configured NSSAI applicable to the SNPN.

The allowed NSSAI and the rejected NSSAI for the current registration area are managed per access type independently, i.e. 3GPP access or non-3GPP access, and is applicable for the registration area. If the UE does not have a valid registration area, the rejected NSSAI for the current registration area is applicable to the tracking area on which it was received. If the registration area contains TAIs belonging to different PLMNs, which are equivalent PLMNs, the allowed NSSAI and the rejected NSSAI for the current registration area are applicable to these PLMNs in this registration area.

The allowed NSSAI that is associated with a registration area containing TAIs belonging to different PLMNs, which are equivalent PLMNs, can be used to form the requested NSSAI for any of the equivalent PLMNs when the UE is outside of the registration area where the allowed NSSAI was received.

When the network slice-specific authentication and authorization procedure is to be initiated for one or more S-NSSAIs in the requested NSSAI, these S-NSSAI(s) will be included in the pending NSSAI. When the network slice-specific authentication and authorization procedure is completed for an S-NSSAI that has been in the pending NSSAI, the S-NSSAI will be moved to the allowed NSSAI or rejected NSSAI depending on the outcome of the procedure and communicated to the UE. The pending NSSAI is managed regardless of access type i.e. the pending NSSAI is applicable to both 3GPP access and non-3GPP access for the current PLMN even if sent over only one of the accesses. If the registration area contains TAIs belonging to different PLMNs, which are equivalent PLMNs, the pending NSSAI is applicable to these PLMNs in this registration area.

The rejected NSSAI for the current PLMN or SNPN is applicable for the whole registered PLMN or SNPN. The AMF shall only send a rejected NSSAI for the current PLMN when the registration area consists of TAIs that only belong to the registered PLMN. If the UE receives a rejected NSSAI for the current PLMN, and the registration area also contains TAIs belonging to different PLMNs, the UE shall treat the received rejected NSSAI for the current PLMN as applicable to the whole registered PLMN.

The rejected NSSAI for the failed or revoked NSSAA includes one or more S-NSSAIs that have failed the network slice-specific authentication and authorization or for which the authorization have been revoked, and are applicable for the whole registered PLMN or SNPN.

NOTE 1: Based on local policies, the UE can remove an S-NSSAI from the rejected NSSAI for the failed or revoked NSSAA when the UE wants to register to the slice identified by this S-NSSAI.

NOTE  2: Network slice-specific authentication and authorization procedure can be initiated by the AMF for S-NSSAIs in rejected NSSAI for failed NSSAA when the S-NSSAI(s) are requested by the UE based on its local policy.

NOTE 3: At least one S-NSSAI in the default configured NSSAI or in the subscribed S-NSSAIs marked as default S-NSSAI is recommended as not subject to network slice-specific authentication and authorization, in order to ensure that at least one PDU session can be established to access service, even when Network Slice-specific Authentication and Authorization fails.\*\*\*\*\* End of Changes \*\*\*\*\*