**3GPP TSG-CT WG4 Meeting #99eC4-204099v1**

**E-Meeting, 18th – 28th August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.526** | **CR** | **0005** | **rev** | **-** | **Current version:** | **16.0.0** |  |
|  | | | | | | | | |
| *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:*** | Update References | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | ZTE, Huawei | | | | | | | | | |
| ***Source to TSG:*** | CT4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNS | | | | |  | ***Date:*** | | | 2020-08-11 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The clauses of other specification (e.g. TS33.501) referred by TS29.526 need to be updated, after SA3 generates new TS version. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Update the clause number of referred specifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Specificaiton is not refined. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.1, 5.2.2.2.1, 5.2.2.3.1, 5.2.2.4.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 does not introduce any change to the OpenAPI file TS29526\_Nnssaaf\_NSSAA. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev1:  Further correct the clause references. | | | | | | | | |

*BEGIN OF CHANGES*

## 4.1 Introduction

Within the 5GC, the NSSAAF offers services to the AMF via the Nnssaaf service based interface.

The AMF shall make use of the NSSAAF service when it needs to invoke network slice-specific authentication and authorization for a specific UE and a specific S-NSSAI (see 3GPP TS 23.502 [3] clause 4.2.9.2, and 3GPP TS 33.501 [14] clause 16.2 and 16.3).

The NSSAAF service shall also be used by the AMF to receive slice re-authentication notification or slice authorization revocation notification sent from the AAA-S (see 3GPP TS 23.502 [3] clause 4.2.9.3, 4.2.9.4 and 3GPP TS 33.501 [14] clause 16.3 and 16.4).

Figure 4.1-1 provides the reference model with focus on the NSSAAF.



Figure 4.1-1: Reference model – NSSAAF

*NEXT CHANGE*

##### 5.2.2.2.1 General

The Authenticate service operation permits the NF Service Consumer (i.e. the AMF) to initiate slice-specific authentication and authorization. The NSSAAF may relay the EAP message to an AAA-S and collect the result of slice-specific authentication and authorization from the AAA-S, as specified in clause 4.2.9.2 of 3GPP TS 23.502 [3], and clause 16.3 of 3GPP TS 33.501 [8].

The NF Service Consumer (i.e. the AMF) shall send a POST request to the resource representing slice authentication collection (i.e. …/v1/slice-authentications) to request the NSSAAF to create the corresponding resource context and perform slice-specific authentication and authorization.



Figure 5.2.2.2.1-1: Slice-Specific Authentication and Authorization

1. The NF Service Consumer (AMF) shall send a POST request to the NSSAAF, targeting the resource of slice authentication collection (i.e. …/v1/slice-authentications), to perform slice-specific authentication and authorization.

The payload of the body shall contain the slice authentication information, which includes:

- UE ID (i.e. GPSI)

- S-NSSAI

- EAP ID Response message (which is received from the UE)

- optionally, the AAA-S address

Editor's Note: It is FFS whether the AAA-S address is provided by the AMF in this step and subsequent steps.

- optionally, the callback URI of the AMF to receive re-authentication notification from the NSSAAF;

- optionally, the callback URI of the AMF to receive revocation notification from the NSSAAF.

Based on local policy, the AMF may determine to provide callback URI(s) for receiving re-authentication notification or revocation notification. For example, the callback URIs are provided for an UE identified with low mobility characteristic.

2. The NSSAAF creates slice authentication context for the UE, and starts the slice-specific authentication and authorization procedure. If the AAA-S is involved in slice-specific authentication and authorization procedure, the NSSAAF shall forward the EAP ID Response message to the AAA-S. Depending on the result, either step 3a or step 3b is performed.

3a. On success, "201 Created" shall be returned. The "Location" header shall contain the URI of the created resource (e.g. .../v1/slice-authentications/{authCtxId}). The payload body shall contain the slice authentication context, which includes the EAP message generated by the NSSAAF or from the AAA-S. The NF Service Consumer (i.e. the AMF) shall forward the received EAP message to the UE in NAS message, as specified in clause 4.2.9.2 of 3GPP TS 23.502 [3].

3b. On failure, one of the HTTP status code listed in Table 6.1.7.3-1 shall be returned with the message body containing a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1. If the slice is not authorized, the NSSAAF shall use the "SLICE\_AUTH\_REJECTED" application error code.

4. Once receiving EAP message from the UE, the NF Service Consumer (i.e. the AMF) shall send a PUT request to the NSSAAF, targeting the resource of the slice authentication context (i.e. …/v1/slice-authentications/{authCtxId}).

The payload body shall carry the slice authentication confirmation data which includes:

- UE ID (i.e. GPSI)

- S-NSSAI

- AAA-S address

- EAP Message (which is received from the UE)

5. The NSSAAF checks and confirms the slice-specific authentication and authorization. If the AAA-S is involved, the NSSAAF shall forward the EAP Message to the AAA-S to confirm the slice-specific authentication and authorization. Depending on the result, either step 6a or step 6b is performed.

6a. On success, "200 OK" shall be returned. The payload body shall contain the slice authentication confirmation response, which includes the EAP message (e.g. EAP success/failure message) generated by the NSSAAF or from the AAA-S. The NF Service Consumer (i.e. the AMF) shall forward the EAP message to the UE in NAS message.

If the UE is authenticated, the NSSAAF shall set the "authResult" attribute to "EAP\_SUCCESS". If failed to authenticate the UE, the "authResult" attribute shall be set to "EAP\_FAILURE".

If subsequent EAP message exchange is needed between the UE and the NSSAAF(AAA-S), the NSSAAF shall not include SliceAuthResult in the response message.

6b. On failure, one of the HTTP status codes listed in Table 6.1.7.3-1 shall be returned with the message body containing a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1.

7-9. If subsequent EAP message exchange is needed between the UE and the NSSAAF to finish the EAP based authentication, step 7-9 are performed.

In above steps, if the AAA-S is involved in the slice-specific authentication and authorization procedure while there is no expected response from the AAA-S in the case of time out, the NSSAAF shall return HTTP status code "504 Gateway Timeout", with the message body containing a ProblemDetails structure with the "cause" attribute set to "TIMED\_OUT\_REQUEST".

After the completion of slice-specific authentication and authorization procedure, it is up to implementation whether the NSSAAF stores the slice authentication context and related resources for a configured period, or deletes the context and resource immediately, e.g. depending on the potential need for AAA-S initiated slice-specific re-authentication/revocation notification.

*NEXT CHANGES*

##### 5.2.2.3.1 General

The Re-Authentication Notification service operation shall be used by the NSSAAF to notify the AMF to re-initiate slice-specific authentication and authorization for a given UE, as specified in clause 4.2.9.3 of 3GPP TS 23.502 [3], and clause 16.4 of 3GPP TS 33.501 [8].

The NSSAAF shall notify the NF Service Consumer (i.e. the AMF) by using the HTTP POST method as shown in Figure 5.2.2.3.1-1.



Figure 5.2.2.3.1-1: Re-authentication Notification

1. The NSSAAF shall send a POST request to the callback URI used to receiving re-authentication notification, which is either provided by the NF Service Consumer (i.e. the AMF), or retrieved from the AMF profile stored in the NRF.

The HTTP payload body of the POST request shall contain the SliceAuthReauthNotification data structure, within which:

- the notificationType set to the SliceAuthNotificationType of "SLICE\_RE\_AUTH";

- the gpsi set to the GPSI of the given UE required to be re-authenticated;

- the snssai set to the S-NSSAI required to be re-authenticated;

2a. On success, "204 No Content" shall be returned and the payload body of the POST response shall be empty.

After responding the request, the NF Service Consumer (i.e. the AMF) shall send NAS message to the UE to trigger re-authentication and re-authorization for the given slice.

2b. On failure, one of the HTTP status code listed in Table 6.1.7.3-1 shall be returned. For a 4xx/5xx response, the message body shall contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1.

*NEXT CHANGES*

##### 5.2.2.4.1 General

The Revocation Notification service operation shall be used by the NSSAAF to notify the AMF to revoke slice-specific authentication and authorization result, as specified in clause 4.2.9.4 of 3GPP TS 23.502 [3], and clause 16.5 of 3GPP TS 33.501 [8], and may trigger the AMF to release the corresponding PDU sessions associated to the indicated slice.

The NSSAAF shall notify the NF Service Consumer (i.e. the AMF) by using the HTTP POST method as shown in Figure 5.2.2.4.1-1.



Figure 5.2.2.4.1-1: Revocation Notification

1. The NSSAAF shall send a POST request to the revocation notification callback URI, which is either provided by the NF Service Consumer (i.e. the AMF), or retrieved from the AMF profile stored in the NRF.

The HTTP payload body of the POST request shall contain the SliceAuthRevocNotification data structure, within which:

- the notificationType set to the SliceAuthNotificationType of "SLICE\_REVOCATION";

- the gpsi set to the GPSI of the given UE for whom the slice-specific authorization revocation is required;

- the snssai set to the S-NSSAI for which the slice-specific authorization revocation is required;

2a. On success, "204 No Content" shall be returned and the payload body of the POST response shall be empty.

On receiving the request, the NF Service Consumer (i.e. the AMF) shall revoke the slice-specific authentication and authorization result for the given UE. If there is PDU session associated to the given slice, the AMF shall trigger the PDU session release to the SMF, with appropriate cause value.

2b. On failure, one of the HTTP status code listed in Table 6.1.7.3-1 shall be returned. For a 4xx/5xx response, the message body shall contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1.

*END OF CHANGES*