**3GPP TSG-CT WG4 Meeting #99eC4-204100v1**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.526** | **CR** | **0006** | **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:*** | AAA Server Address | | | | | | | | | |
|  |  | | | | | | | | | |
| ***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:*** | | As per described in TS23.502 clause 4.2.9.2, the AAA Server address needs to be sent to the NSSAAF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Following changes are made:  - Delete editor’s note in clause 5.2.2.2.1;  - Include the AAA Server address in SliceAuthInfo, SliceAuthConfirmationData structure;  - Update the OpenAPI accordingly. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The NSSAAF is not able to find the correct AAA Server to trigger slice-specific authentication and authorization. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.2.2.1, 6.1.6.1, 6.1.6.2.2, 6.1.6.2.4, A.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 introduces backward compatible changes to the OpenAPI file TS29526\_Nnssaaf\_NSSAA. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev1:  Error fixed in clause 6.1.6.2.4, and coversheet. | | | | | | | | |

*BEGIN OF CHANGES*

##### 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 x.x.x 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

- 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 CHANGE*

#### 6.1.6.1 General

This clause specifies the application data model supported by the API.

Table 6.1.6.1-1 specifies the data types defined for the Nnssaaf service based interface protocol.

Table 6.1.6.1-1: Nnssaaf specific Data Types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Clause defined | Description | Applicability |
| SliceAuthInfo | 6.1.6.2.2 | Contains the GPSI, S-NSSAI, EAP ID Response, etc. |  |
| SliceAuthContext | 6.1.6.2.3 | Contains the information of the resource created for slice-specific authentication and authorization. |  |
| SliceAuthConfirmationData | 6.1.6.2.4 | Contains the EAP message from the UE for EAP process. |  |
| SliceAuthConfirmationResponse | 6.1.6.2.5 | Contains the slice-specific authentication and authorization result from the NSSAAF to the UE. |  |
| SliceAuthReauthNotification | 6.1.6.2.6 | Contains the re-authentication notification for slice-specific authentication and authorization. |  |
| SliceAuthRevocNotification | 6.1.6.2.7 | Contains the revocation notification for slice-specific authentication and authorization. |  |
| SliceAuthCxtId | 6.1.6.3.2 | Contains the resource ID of slice authentication context. |  |
| EapMessage | 6.1.6.3.2 | Contains the string formatted EAP message. |  |
| SliceNotificationType | 6.1.6.3.3 | Notification type of slice-specification authentication and authorization. |  |

Table 6.1.6.1-2 specifies data types re-used by the Nnssaaf service based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Nnssaaf service based interface.

Table 6.1.6.1-2: Nnssaaf re-used Data Types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Reference | Comments | Applicability |
| ProblemDetails | 3GPP TS 29.571 [10] | Common Data Type used in response bodies |  |
| Gpsi | 3GPP TS 29.571 [10] | GPSI |  |
| Snssai | 3GPP TS 29.571 [10] | S-NSSAI |  |
| AuthStatus | 3GPP TS 29.571 [10] | Slice Authentication Status |  |
| IpAddress | 3GPP TS 29.503 [15] | IP Address |  |

*NEXT CHANGES*

##### 6.1.6.2.2 Type: SliceAuthInfo

Table 6.1.6.2.2-1: Definition of type SliceAuthInfo

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| gpsi | Gpsi | M | 1 | Contains the GPSI of the UE. |  |
| snssai | Snssai | M | 1 | Contains the S-NSSAI for authentication. |  |
| eapIdRsp | EapMessage | M | 1 | Contains the EAP ID Responses message from the UE. |  |
| serverAddress | IpAddress | O | 0..1 | When present, it shall contain the address of AAA Server |  |
| amfInstanceId | NfInstanceId | O | 0..1 | This IE may be present, if the AMF determines to provide the re-authentication/revocation notification URI to the NSSAAF.  When present, it shall contain the NF Instance Id of the AMF. |  |
| reauthNotifUri | Uri | O | 0..1 | This IE may be present, e.g. if the AMF determines the UE with low mobility characteristic.  When present, it shall contain the re-authentication notification URI. |  |
| revocNotifUri | Uri | O | 0..1 | This IE may be present, e.g. if the AMF determines the UE with low mobility characteristic.  When present, it shall contain the revocation notification URI. |  |

*NEXT CHANGES*

##### 6.1.6.2.4 Type: SliceAuthConfirmationData

Table 6.1.6.2.4-1: Definition of type SliceAuthConfirmationData

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| gpsi | Gpsi | M | 1 | Contains the GPSI of the UE. |  |
| snssai | Snssai | M | 1 | Contains the S-NSSAI for authentication. |  |
| eapMessage | EapMessage | M | 1 | Contains the EAP message received from the UE. |  |
| serverAddress | IpAddress | O | 0..1 | When present, it shall contain the address of AAA Server. |  |

*NEXT CHANGES*

## A.2 Nnssaaf\_NSSAA API

\*\*\*\*\*\*\*\*TEXT SKIPPED\*\*\*\*\*\*\*\*

# COMPLEX TYPES:

SliceAuthInfo:

type: object

properties:

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

eapIdRsp:

$ref: '#/components/schemas/EapMessage'

serverAddr:

$ref: 'TS29503\_Nudm\_SDM.yaml#/components/schemas/IpAddress'

amfInstanceId:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/NfInstanceId'

reauthNotifUri:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Uri'

revocNotifUri:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Uri'

required:

- gpsi

- snssai

- eapIdRsp

SliceAuthContext:

type: object

properties:

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

authCtxId:

$ref: '#/components/schemas/SliceAuthCtxId'

eapMessage:

$ref: '#/components/schemas/EapMessage'

required:

- gpsi

- snssai

- authCtxId

- eapMessage

SliceAuthConfirmationData:

type: object

properties:

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

eapMessage:

$ref: '#/components/schemas/EapMessage'

serverAddr:

$ref: 'TS29503\_Nudm\_SDM.yaml#/components/schemas/IpAddress'

required:

- gpsi

- snssai

- eapMessage

SliceAuthConfirmationResponse:

type: object

properties:

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

eapMessage:

$ref: '#/components/schemas/EapMessage'

authResult:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/AuthStatus'

required:

- gpsi

- snssai

- eapMessage

SliceAuthReauthNotification:

type: object

properties:

notifType:

$ref: '#/components/schemas/SliceAuthNotificationType'

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

required:

- notifType

- gpsi

- snssai

SliceAuthRevocNotification:

type: object

properties:

notifType:

$ref: '#/components/schemas/SliceAuthNotificationType'

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

required:

- notifType

- gpsi

- snssai

# SIMPLE TYPES:

SliceAuthCtxId:

type: string

description: contains the resource ID of slice authentication context

nullable: false

SliceAuthNotificationType:

type: string

enum:

- SLICE\_RE\_AUTH

- SLICE\_REVOCATION

EapMessage:

type: string

format: base64

description: contains an EAP packet

nullable: true

\*\*\*\*\*\*\*\*TEXT SKIPPED\*\*\*\*\*\*\*\*

*NEXT CHANGES*

*END OF CHANGES*