**3GPP TSG-CT WG4 Meeting #98eC4-20xxxx**

**E-Meeting, 02nd – 12th June 2020 *Revision of C4-203210***

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **29.503** | **CR** | **0439** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  |
| *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:***  | Authentication results for multiple registrations |
|  |  |
| ***Source to WG:*** | Huawei, Samsung |
| ***Source to TSG:*** | CT4 |
|  |  |
| ***Work item code:*** | [TEI16](http://portal.3gpp.org/desktopmodules/WorkItem/WorkItemDetails.aspx?workitemId=840002) |  | ***Date:*** | 2020-06-08 |
|  |  |  |  |  |
| ***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 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:*** | According to the LS from SA3 (C4-203416), SA3 has identified that the UDM stores the authEvents for both serving networks when a user is simultaneously registered in two Serving Networks via different access types (3gpp and non-3gpp):*“It is SA3’s understanding that UDM stores the authEvents for both serving networks in multiple registrations.”*……*“UDM, when deleting the authentication results for the new serving network, keeps the AUSF info in the authEvent.”*Currently, the specification is not clear whether one UE can have individual AuthEvent per serving network.It is proposed the individual AuthEvent is per UE per serving network, and a UE in multiple registrations can have different AuthEvents for different Serving Networks.Similarly, changes done via C4-201167 (CR 0358) uses DELETE Operation to remove AuthEvent resource (which contains AUSF information) from UDM as part of result removal procedure. This may result in UDM losing information on AUSF holding latest Kausf.It is proposed to updated the result deletion procedure to not use DELETE method. |
|  |  |
| ***Summary of change:*** | Update the description of Authentication Confirmation to indicate the individual AuthEvent is per UE per serving network.Removed changes done via C4-201167 (CR 0358), and propose to use the PUT method to remove the authentication result only. |
|  |  |
| ***Consequences if not approved:*** | AuthEvent of the UE will be removed by mistake. Also, SA3 requirement of storing latest Kausf may not be met as with current implementation UDM may remove authEvent data-structure holding latest AUSF information that authenticated the UE. |
|  |  |
| ***Clauses affected:*** | 5.4.2.3.2, 5.4.2.3.3, 6.3.3.1, 6.3.3.6.1, 6.3.3.6.2, 6.3.6.2.7, 6.3.7.3, A.4  |
|  |  |
|  | **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:*** | The CR introduces backward compatible corrections to the OpenAPI file for *Nudm\_UEAU* API. |
|  |  |
| ***This CR's revision history:*** | Rev1: Incorporated changes done for C4-203127, and proposes to use PUT to remove the authentication result. |

\* \* \* \* Begin of Change \* \* \* \*

##### 5.4.2.3.2 Authentication Confirmation

Figure 5.4.2.3.2-1 shows a scenario where the NF service consumer (AUSF) confirms the occurence of a successful or unsuccessful authentication in a serving network to the UDM (see also 3GPP TS 33.501 [6] clause 6.1.4.1a). The request contains the UE's identity (supi), and information about the authentication occurrence (AuthEvent).



Figure 5.4.2.3.2-1: NF service consumer confirms UE authentication

1. The NF service consumer sends a POST request to the resource representing the UE's authentication events. The payload body of the POST request shall contain a representation of the individual AuthEvent resource to be created. There shall be only one individual AuthEvent per UE per Serving Network identified by the supi in URI and servingNetworkName in AuthEvent.

2a. On success, the UDM responds with "201 Created" and the "Location" header shall be present and shall contain the URI of the created resource.

2b. On failure, the appropriate HTTP status code indicating the error shall be returned and appropriate additional error information should be returned.

\* \* \* \* Next Change \* \* \* \*

##### 5.4.2.3.3 Authentication Result Removal

Figure 5.4.2.3.3-1 shows a scenario where the NF service consumer requests the UDM to remove the Authentication Result. The request contains the UE's identity (supi), the authEvent Id, and an indication to remove Authentication result.



Figure 5.4.2.3.3-1: NF service consumer removes the authentication result

1. The NF service consumer shall send a PUT request to the UDM. The payload of the body shall contain the indication to remove authentication result.

2a. On success, "200 OK" shall be returned. The UDM shall remove the Authentication result of the UE by completely replacing the individual AuthEvent resource. The payload body of the PUT response shall contain the representation of the replaced resource.

2b. On failure, the appropriate HTTP status code indicating the error shall be returned and appropriate additional error information should be returned.

\* \* \* \* Next Change \* \* \* \*

#### 6.3.3.1 Overview

Figure 6.3.3.1-1 describes the resources supported by the Nudm\_UEAU API.



Figure 6.3.3.1-1: Resource URI structure of the nudm\_ueau API

Table 6.3.3.1-1 provides an overview of the resources and applicable HTTP methods.

Table 6.3.3.1-1: Resources and methods overview

|  |  |  |  |
| --- | --- | --- | --- |
| Resource name(Archetype) | Resource URI | HTTP method or custom operation | Description |
| SecurityInformation(Custom operation) | /{supiOrSuci}/security-information/generate-auth-data | generate-auth-data (POST) | If the variable {supiOrSuci} takes the value of a SUCI, the UDM calculates the corresponding SUPI. The UDM calculates a fresh authentication vector based on the received information and the stored security information for the SUPI if 5G-AKA or EAP-AKA' is selected. Otherwise, UDM provides corresponding authentication information. |
| SecurityInformationForRg | /{supiOrSuci}/security-information-rg | GET | If the variable {supiOrSuci} takes the value of a SUCI, the UDM calculates the corresponding SUPI. The UDM decides, based on the received information and the stored authentication profile of the SUPI, that authentication by the home network is not required for the FN-RG. |
| AuthEvents(Collection) | /{supi}/auth-events | POST | Create an Authentication Event |
| Individual AuthEvent(Document) | /{supi}/auth-events/{authEventId} | PUT | Update an Authentication Event |
| HssSecurityInformation(Custom operation) | /{supi}/hss-security-information/generate-av | generate-av (POST) | The UDM generates the authentication vector(s) for EPS or IMS domain based on stored security information for the SUPI. |

\* \* \* \* Next Change \* \* \* \*

#### 6.3.3.6 Resource: Individual AuthEvent

##### 6.3.3.6.1 Resource Definition

Resource URI: {apiRoot}/nudm-ueau/v1/{supi}/auth-events/{authEventId}

This resource shall support the resource URI variables defined in table 6.3.3.6.1-1.

Table 6.3.3.6.1-1: Resource URI variables for this resource

|  |  |
| --- | --- |
| Name | Definition |
| apiRoot | See clause 6.3.1 |
| supi | Represents the Subscription Permanent Identifier (see 3GPP TS 23.501 [2] clause 5.9.2) pattern: See pattern of type Supi in 3GPP TS 29.571 [7] |
| authEventId | Represents the authEvent Id per UE per serving network assigned by the UDM during ResultConfirmation service operation. |

##### 6.3.3.6.2 Resource Standard Methods

###### 6.3.3.6.2.1 PUT

This method shall support the URI query parameters specified in table 6.3.3.6.2.1-1.

Table 6.3.3.6.2.1-1: URI query parameters supported by the PUT method on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| n/a |  |  |  |  |

This method shall support the request data structures specified in table 6.3.3.6.2.1-2 and the response data structures and response codes specified in table 6.3.3.6.2.1-3.

Table 6.3.3.6.2.1-2: Data structures supported by the PUT Request Body on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| AuthEvent | M | 1 | The UE Authentication Event |

Table 6.3.3.6.2.1-3: Data structures supported by the PUT Response Body on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Responsecodes | Description |
| AuthEvent | O | 0..1 | 200 OK | Upon success, a response body containing a representation of the replaced Authentication Event may be returned. |
| ProblemDetails | O | 0..1 | 404 Not Found | If the resource corresponding to the authEventId does not exist, a response code of 404 Not Found shall be returned.The "cause" attribute may be set to:- DATA\_NOT\_FOUND |
| NOTE: In addition common data structures as listed in table 6.3.7-1 are supported. |

\* \* \* \* Next Change \* \* \* \*

##### 6.3.6.2.7 Type: AuthEvent

Table 6.3.6.2.7-1: Definition of type AuthEvent

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| nfInstanceId | NfInstanceId | M | 1 | Identifier of the NF instance where the authentication occurred |
| success | Success | M | 1 | true indicates success; false indicates no success.Set to false in case of authentication result removal. |
| timeStamp | DateTime | M | 1 | time stamp of the authentication |
| authType | AuthType | M | 1 | stringAuthentication Type ("EAP\_AKA\_PRIME" or "5G\_AKA") |
| servingNetworkName | ServingNetworkName | M | 1 | See 3GPP TS 33.501 [6] clause 6.1.1.4 |
| authRemovalInd | Boolean | O | 0..1 | When present, it shall indicate the authentication result in the UDM shall be removed.This IE shall be set as follows:- true: authentication result in the UDM shall be removed;- false (default): authentication result in the UDM shall not be removed. |

\* \* \* \* Next Change \* \* \* \*

#### 6.3.7.3 Application Errors

The common application errors defined in the Table 5.2.7.2-1 in 3GPP TS 29.500 [4] may also be used for the Nudm\_UEAuthentication service. The following application errors listed in Table 6.3.7.3-1 are specific for the Nudm\_UEAuthentication service.

Table 6.3.7.3-1: Application errors

|  |  |  |
| --- | --- | --- |
| Application Error | HTTP status code | Description |
| AUTHENTICATION\_REJECTED | 403 Forbidden | The user is cannot be authenticated with this authentication method e.g. only SIM data available |
| SERVING\_NETWORK\_NOT\_AUTHORIZED | 403 Forbidden | The requesting network is not authorized to request UE authentication information. |
| USER\_NOT\_FOUND | 404 Not Found | The user does not exist in the HPLMN |
| UNSUPPORTED\_PROTECTION\_SCHEME | 501 Not implemented | The received protection scheme is not supported by HPLMN |
| UNSUPPORTED\_AUTHENTICATION\_METHOD | 501 Not implemented | The requested authenti-cation method is not supported |
| INVALID\_HN\_PUBLIC\_KEY\_IDENTIFIER | 403 Forbidden | Invalid HN public key identifier received |
| INVALID\_SCHEME\_OUTPUT | 403 Forbidden | SUCI cannot be decrypted with received data |
| DATA\_NOT\_FOUND | 404 Not Found | Resource corresponding to the authEventId does not exist |

\* \* \* \* Next Change \* \* \* \*

## A.4 Nudm\_UEAU API

openapi: 3.0.0

info:

 version: '1.1.0.alpha-2'

 title: 'NudmUEAU'

 description: |

 UDM UE Authentication Service.

 © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

 All rights reserved.

externalDocs:

 description: 3GPP TS 29.503 Unified Data Management Services, version 16.3.0

 url: 'http://www.3gpp.org/ftp/Specs/archive/29\_series/29.503/'

servers:

 - url: '{apiRoot}/nudm-ueau/v1'

 variables:

 apiRoot:

 default: https://example.com

 description: apiRoot as defined in clause clause 4.4 of 3GPP TS 29.501.

[…]

 /{supi}/auth-events/{authEventId}:

 put:

 summary: Deletes the authentication result in the UDM

 operationId: DeleteAuth

 tags:

 - Delete Auth

 parameters:

 - name: supi

 in: path

 description: SUPI of the user

 required: true

 schema:

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

 - name: authEventId

 in: path

 description: authEvent Id

 required: true

 schema:

 type: string

 requestBody:

 content:

 application/json:

 schema:

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

 required: true

 responses:

 '200':

 description: Expected response to a successful authentication result removal

 content:

 application/json:

 schema:

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

 '400':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/400'

 '404':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/404'

 '500':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/500'

 '503':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/503'

 default:

 $ref: 'TS29571\_CommonData.yaml#/components/responses/default'

[…]

 AuthEvent:

 type: object

 required:

 - nfInstanceId

 - success

 - timeStamp

 - authType

 - servingNetworkName

 properties:

 nfInstanceId:

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

 success:

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

 timeStamp:

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

 authType:

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

 servingNetworkName:

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

 authRemovalInd:

 type: boolean

 default: false

\* \* \* \* End of Change \* \* \* \*