**3GPP TSG-CT WG4 Meeting #111-eC4-224**

**E-Meeting, 18th – 26th August 2022 revision of C4-224150**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.509** | **CR** | **0171** | **rev** | **1** | **Current version:** | **17.6.0** |  |
|  | | | | | | | | |
| *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:*** | MSK in EapSession | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | CT4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | NSWO\_5G | | | | |  | ***Date:*** | | | 2022-08-25 |
|  |  | | | |  | |  | | |  |
| ***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 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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | According to 33.501 annex S.3.2 step 16, the AUSF provides MSK to NSWOF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add MSK to EapSession | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Requirment from 33.501 cannot be implemented. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.2.2.3.2, 6.1.6.1, 6.1.6.2.7, 6.1.6.3.2, 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 backwards compatible corrections with impact to the following APIs: TS29509\_UEAuthentication.yaml | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\* \* \* First Change \* \* \* \*

5.2.2.2.3.2 EAP method: EAP-AKA'

EAP-AKA' is the EAP method used in this procedure



Figure 5.2.2.2.3-1: EAP-based authentication with EAP-AKA' method

1. The NF Service Consumer (AMF, NSWOF) shall send a POST request to the AUSF. The payload of the body shall contain at least the UE Id, Serving Network Name. If the consumer is an NSWOF the NSWO Indicator shall be present in the payload of the body.

2a. On success, "201 Created" shall be returned. The payload body shall contain the representation of the resource generated and the "Location" header shall contain the URI of the generated resource (e.g. .../v1/ue\_authentications/{authCtxId}). The AUSF generates a sub-resource "eap-session". There shall be only one sub-resource "eap-session" per UE per Serving Network identified by the supiOrSuci and servingNetworkName in AuthenticationInfo. The AUSF shall provide a hypermedia link towards this sub-resource in the payload to indicate to the AMF or NSWOF where it shall send a POST containing the EAP packet response. The body payload shall also contain the EAP packet EAP-Request/AKA'-Challenge.

2b. On failure or redirection, one of the HTTP status code listed in table 6.1.3.2.3.1-3 shall be returned. For a 4xx/5xx response, the message body may contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.3.2.3.1-3. In particular, if the serving network is not authorized, the AUSF shall use the "Cause" SERVING\_NETWORK\_NOT\_AUTHORIZED.

3. Based on the relation type, the NF Service Consumer (AMF, NSOWF) shall send a POST request including the EAP-Response/AKA' Challenge received from the UE. The POST request is sent to the URI provided by the AUSF or derived by the NF Service Consumer (AMF, NSWOF).

4a. On success, and if the AUSF and the UE have indicated the use of protected successful result indications as in IETF RFC 9048 [17], the AUSF shall reply with a "200 OK" HTTP message containing the EAP Request/AKA' Notification and an hypermedia link towards the sub-resource "eap-session".

4b. On failure or redirection, one of the HTTP status code listed in table 6.1.3.4.3.1-3 shall be returned. For a 4xx/5xx response, the message body may contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.3.4.3.1-3.

NOTE: Steps 4 to 5 are optional.

5. The NF Service Consumer (AMF, NSWOF) shall send a POST request including the EAP Response/AKA' Notification received from the UE. The POST request is sent to the URI provided by the AUSF or derived by the NF Service Consumer (AMF, NSWOF).

6a. If the EAP authentication exchange is successfully completed (with or without the optional Notification Request/Response messages exchange), "200 OK" shall be returned to the NF Service Consumer (AMF, NSWOF). The payload shall contain the result of the authentication, an EAP success/failure and if the authentication is successful the Kseaf if the consumer is an AMF or the MSK if the consumer is a NSWOF (as indicated by the NSWO indicator received in step 1). If the UE is not authenticated, the AUSF shall set the authResult to AUTHENTICATION\_FAILURE.

In SNPN onboarding scenarios, if the UE is authenticated successfully, the AUSF may include in the response the address of an onboarding Provisioning Server (PVS) to the NF Service Consumer (AMF) ; see 3GPP TS 23.501 [2], clause 5.30.2.10.

6b. On failure or redirection, one of the HTTP status code listed in table 6.1.3.4.3.1-3 shall be returned. For a 4xx/5xx response, the message body may contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.3.4.3.1-3.

\* \* \* 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 Nausf service based interface protocol.

Table 6.1.6.1-1: Nausf specific Data Types

|  |  |  |
| --- | --- | --- |
| Data type | Clause defined | Description |
| AuthenticationInfo | 6.1.6.2.2 | Contains the UE id (i.e. SUCI or SUPI) and the Serving Network Name. |
| UEAuthenticationCtx | 6.1.6.2.3 | Contains the information related to the resource generated to handle the UE authentication. It contains at least the UE id, Serving Network, the Authentication Method and related EAP information or related 5G-AKA information. |
| 5gAuthData | 6.1.6.2.4 | Contains 5G authentication related information. |
| Av5gAka | 6.1.6.2.5 | Contains Authentication Vector for method 5G AKA. |
| ConfirmationData | 6.1.6.2.6 | Contains the "RES\*" generated by the UE. |
| DeregistrationInfo | 6.1.6.2.11 | Contains the UE id (i.e. SUPI). |
| EapSession | 6.1.6.2.7 | Contains information related to the EAP session. |
| ConfirmationDataResponse | 6.1.6.2.8 | Contains the result of the authentication. |
| RgAuthenticationInfo | 6.1.6.2.9 | Contains the UE id (i.e. SUCI) and the authenticated indication. |
| RgAuthCtx | 6.1.6.2.10 | Contains the UE id (i.e. SUPI) and the authentication indication. |
| ProSeAuthenticationInfo | 6.1.6.2.12 | Contains the UE id (i.e. SUCI or SUPI), Relay Service Code and Nonce\_1. |
| ProSeAuthenticationCtx | 6.1.6.2.13 | Contains the information related to the resource generated to handle the ProSe authentication. |
| ProSeEapSession | 6.1.6.2.14 | Contains information related to the EAP session for the 5G ProSe Remote UE. |
| ProSeAuthData | 6.1.6.2.15 | Contains ProSe authentication related information. |
| EapPayload | 6.1.6.3.2 | Contains the EAP packets. |
| ResStar | 6.1.6.3.2 | Contains the RES\*. |
| Kseaf | 6.1.6.3.2 | Contains the Kseaf. |
| HxresStar | 6.1.6.3.2 | Contains the HXRES\*. |
| Suci | 6.1.6.3.2 | Contains the SUCI. |
| KnrProSe | 6.1.6.3.2 | Contains the KNR\_ProSe. |
| Nonce1 | 6.1.6.3.2 | Contains the Nonce1. |
| Nonce2 | 6.1.6.3.2 | Contains the Nonce2. |
| AuthType | 6.1.6.3.3 | Indicates the authentication method used. |
| AuthResult | 6.1.6.3.4 | Indicates the result of the authentication. |
| Msk | 6.1.6.3.2 | Contains the Master Session Key. |

Table 6.1.6.1-2 specifies data types re-used by the Nausf 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 Nausf service based interface.

Table 6.1.6.1-2: Nausf re-used Data Types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Reference | Comments | |
| ResynchronizationInfo | 3GPP TS 29.503 [12] |  | |
| ServingNetworkName | 3GPP TS 29.503 [12] |  | |
| Autn | 3GPP TS 29.503 [12] |  | |
| Rand | 3GPP TS 29.503 [12] |  | |
| LinksValueSchema | 3GPP TS 29.571 [10] | 3GPP Hypermedia link | |
| ProblemDetails | 3GPP TS 29.571 [10] | Common Data Type used in response bodies | |
| Supi | 3GPP TS 29.571 [10] |  | |
| Uri | 3GPP TS 29.571 [10] |  | |
| SupiOrSuci | 3GPP TS 29.571 [10] |  | |
| Pei | 3GPP TS 29.571 [10] |  | |
| TraceData | 3GPP TS 29.571 [10] |  | |
| NfGroupId | 3GPP TS 29.571 [10] |  | |
| CagId | 3GPP TS 29.571 [10] |  | |
| SupportedFeatures | 3GPP TS 29.571 [10] | Supported Features | |
| ServerAddressingInfo | 3GPP TS 29.571 [10] | |  |
| RelayServiceCode | 3GPP TS 29.571 [10] | |  |

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

##### 6.1.6.2.7 Type: EapSession

Table 6.1.6.2.7-1: Definition of type EapSession

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| eapPayload | EapPayload | M | 1 | Contains the EAP packet (see IETF RFC 3748 [18]).  If no EAP packet has been provided by the UE the null value is conveyed to the AUSF. |
| kSeaf | Kseaf | C | 0..1 | Shall be absent for N5GC device authentication; otherwise:  If the authentication is successful and the consumer is an AMF, the Kseaf shall be included |
| \_links | map(LinksValueSchema) | C | 1..N | If the EAP session requires another exchange e.g. for EAP-AKA' notification, this IE shall contain a member whose name is "eap-session" and the URI to continue the EAP session.  See NOTE. |
| authResult | AuthResult | C | 0..1 | Indicates the result of the authentication. |
| supi | Supi | C | 0..1 | If the authentication is successful and if the AMF had provided a SUCI, this IE shall contain the SUPI of the UE. |
| supportedFeatures | SupportedFeatures | C | 0..1 | This IE shall be present if at least one optional feature defined in clause 6.1.9 is supported. |
| pvsInfo | array(ServerAddressingInfo) | O | 1..N | Addressing information of the SNPN UE onboarding Provisioning Servers (PVS). |
| msk | Msk | C | 0..1 | If the authentication is successful and the consumer is an NSWOF as indicated by the NSWO indicator received within the AuthenticationInfo, the MSK shall be included (see 3GPP TS 33.501 [8] annex S) |
| NOTE: In the current version of this API, only 0 or 1 hypermedia link is provided. | | | | |

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

##### 6.1.6.3.2 Simple data types

Table 6.1.6.3.2-1: Simple data types

|  |  |  |
| --- | --- | --- |
| Type Name | Type Definition | Description |
| EapPayload | string | The EAP packet is encoded using base64 (see IETF RFC 4648 [19]) and represented as a String.  Format: byte |
| ResStar | string | pattern: "^[A-Fa-f0-9]{32}$"; nullable |
| Kseaf | string | pattern: "^[A-Fa-f0-9]{64}$" |
| HxresStar | string | pattern: "^[A-Fa-f0-9]{32}$" |
| Suci | string | String containing a SUCI.  Pattern: "^(suci-(0-[0-9]{3}-[0-9]{2,3}|[1-7]-.+)-[0-9]{1,4}-(0-0-.+|[a-fA-F1-9]-([1-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])-[a-fA-F0-9]+)|.+)$" |
| KnrProSe | string | String contain the KNR\_ProSe  pattern: "^[A-Fa-f0-9]{64}$" |
| Nonce1 | string | The Nonce1 is encoded using base64 (see IETF RFC 4648 [19]) and represented as a String.  Format: byte |
| Nonce2 | string | The Nonce2 is encoded using base64 (see IETF RFC 4648 [19]) and represented as a String.  Format: byte |
| Msk | string | pattern: "^[A-Fa-f0-9]{128}$" |

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

## A.2 Nausf\_UEAuthentication API

openapi: 3.0.0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*text not shown for clarity\*\*\*\*\*\*\*\*\*\*\*\*\*

EapSession:

description: Contains information related to the EAP session.

type: object

properties:

eapPayload:

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

kSeaf:

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

\_links:

type: object

description: A map(list of key-value pairs) where member serves as key

additionalProperties:

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

authResult:

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

supi:

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

supportedFeatures:

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

pvsInfo:

type: array

items:

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

minItems: 1

msk:

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

required:

- eapPayload

\*\*\*\*\*\*\*\*\*\*\*\*\*\*text not shown for clarity\*\*\*\*\*\*\*\*\*\*\*\*\*

Kseaf:

description: Contains the Kseaf.

type: string

pattern: '[A-Fa-f0-9]{64}'

Msk:

description: Contains the Master Session Key.

type: string

pattern: '[A-Fa-f0-9]{128}'

\*\*\*\*\*\*\*\*\*\*\*\*\*\*text not shown for clarity\*\*\*\*\*\*\*\*\*\*\*\*\*

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