**3GPP TSG-CT WG4 Meeting #98eC4-203**

**E-Meeting, 02nd – 12th June 2020 was C4-203180**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.505** | **CR** | **0280** | **rev** | **1** | **Current version:** | **16.2.0** |  |
|  | | | | | | | | |
| *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:*** | N5GC device Authentication | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, CableLabs, Charter Communications | | | | | | | | | |
| ***Source to TSG:*** | CT4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5WWC | | | | |  | ***Date:*** | | | 2020-06-03 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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 Authentication Method that shall be used when the user uses a Non-5G-Capable device needs to be part of the Authentication Subscription Data; see TS 33.501 Annex O. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add n5gcAuthMethod attribute to type AuthenticationSubscription,  add rgAuthenticationInd attribute to type AuthenticationSubscription | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misalignment with stage 2 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.2.2, 5.4.3.3, 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 new features to the  Nudr\_DR API. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

#### 5.4.2.2 Type: AuthenticationSubscription

Table 5.4.2.2-1: Definition of type AuthenticationSubscription

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| authenticationMethod | AuthMethod | M | 1 | String containing the Authentication Method ( "5G\_AKA" , "EAP\_AKA\_PRIME, "EAP\_TLS"...) that shall be used when the UE's device is 5G capable." |
| encPermanentKey | string | C | 0..1 | The encrypted value (hexstring) of the permanent authentication key (K) (see 3GPP TS 33.501 [9]).  It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME" unless vector generation is to be done in the HSS. |
| protectionParameterId | string | C | 0..1 | Identifies a parameter set securely stored in the UDM(ARPF) that can be used to decrypt the encPermanentKey (and encOpcKey or encTopcKey if present). Values and their meaning are HPLMN-operator specific.  It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME" unless vector generation is to be done in the HSS. |
| sequenceNumber | SequenceNumber | C | 0..1 | String containing the SQN as defined in 3GPP TS 33.102 [10].  It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME" unless vector generation is to be done in the HSS. |
| authenticationManagementField | string | C | 0..1 | Hexstring containing the Authentication management field as defined in 3GPP TS 33.501 [9].  It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME" unless vector generation is to be done in the HSS.  Pattern: '^[A-Fa-f0-9]{4}$' |
| algorithmId | string | C | 0..1 | Identifies a parameter set securely stored in the UDM(ARPF) that provides details on the algorithm and parameters used to generate authentication vectors. Values and their meaning are HPLMN-operator specific.  It shall be present if the authentication method is "5G\_AKA" or "EAP\_AKA\_PRIME" unless vector generation is to be done in the HSS. |
| encOpcKey | string | O | 0..1 | Hexstring of the encrypted OPC Key.  Presence indicates that the provided value (decrypted) shall be used instead of the value derived from OP and K. |
| encTopcKey | string | O | 0..1 | Hexstring of the encrypted TOPC Key.  Presence indicates that the provided value (decrypted) shall be used instead of the value derived from TOP and K. |
| vectorGenerationInHss | boolean | O | 0..1 | True indicates that the UDM needs to retrieve an Authentication Vector from the HSS;  False and absence indicates that vector generation shall be performed in the UDM. |
| n5gcDeviceAuthMethod | AuthMethod | O | 0..1 | String containing the Authentication Method that shall be used when the UE's device is Non-5G-Capable behind Cable RGs in private networks or in isolated deployment scenarios with wireline access.  See NOTE |
| rgAuthenticationInd | boolean | O | 0..1 | true: indicates that authentication by the home network is not required if authentication has been completed by the W-5GAN. See 3GPP TS 33.501 [9] clause 7b. false (default): otherwise. |
| NOTE: The attribute n5gcDeviceAuthMethod is used for EAP-TLS, which is described in the informative annex O of 3GPP TS 33.501 [9] and is not mandatory to support. | | | | |

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

#### 5.4.3.3 Enumeration: AuthMethod

Table 5.4.3.3-1: Enumeration AuthMethod

|  |  |
| --- | --- |
| Enumeration value | Description |
| "5G\_AKA" | 5G AKA |
| "EAP\_AKA\_PRIME" | EAP AKA' |
| "EAP-TLS" | EAP TLS |

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

## A.2 Nudr\_DataRepository API for Subscription Data

For the purpose of referencing entities in the Open API file defined in this Annex, it shall be assumed that this Open API file is contained in a physical file named "TS29505\_Subscription\_Data.yaml".

openapi: 3.0.0

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

AuthenticationSubscription:

type: object

required:

- authenticationMethod

properties:

authenticationMethod:

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

encPermanentKey:

type: string

protectionParameterId:

type: string

sequenceNumber:

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

authenticationManagementField:

type: string

pattern: '^[A-Fa-f0-9]{4}$'

algorithmId:

type: string

encOpcKey:

type: string

encTopcKey:

type: string

vectorGenerationInHss:

type: boolean

default: false

n5gcAuthMethod:

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

rgAuthenticationInd:

type: boolean

default: false

\* \* \* \* End Of Change \* \* \* \*