**3GPP TSG-CT WG4 Meeting #102-eC4-211xyz**

**E-Meeting, 24th Feb – 5th Mar 2021 (was C4-211468)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.505** | **CR** | **0330** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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:*** | AKMA Subscription Data | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | CT4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA-CT | | | | |  | ***Date:*** | | | 2021-02-15 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Based on 33.535 Figure 6.1-1 step 2, UDM is required to indicate to AUSF whether AKMA anchor key should be generated during primary authentication procedure.  UDM shall base on AKMA subscription data to set the above indication, but the AKMA subscription data is not supported by UDR yet. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is proposed to extend the authentication subscription data with a new attribute akmaAllowed to indicate whether AKMA is allowed for the subscriber:   * true: AKMA is allowed for the subscriber * false: AKMA is not allowed for the subscriber | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Without AKMA subscription data, UDM can’t indicate to AUSF whether AKMA anchor key should be generated after a successful primary authentication procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.2.2, 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 new features, with impacts to the following APIs:  - TS29504\_Nudr\_DataRepository.yaml | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\* \* \* First 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.  If AV generation for HSS is required in UDM, this attribute shall take any 5G AKA-based value (i.e. "5G\_AKA" or "EAP\_AKA\_PRIME"). |
| 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. |
| supi | Supi | C | 0..1 | If present, this IE shall contain the UE's SUPI which shall contain an IMSI.  It shall be present if the subscription is allowed to be identified by a pseudonym of the SUPI e.g. by a GCI or GLI that is not the SUPI. |
| akmaAllowed | boolean | O | 0..1 | This IE indicates whether or not the subscriber is allowed to use AKMA:  - true: subscriber is allowed to use AKMA  - absent or false: subscriber is not allowed to use AKMA |
| 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 \* \* \* \*

## 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

info:

version: '-'

title: 'Unified Data Repository Service API file for subscription data'

description: |

Unified Data Repository Service (subscription data).

The API version is defined in 3GPP TS 29.504.

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

All rights reserved.

externalDocs:

description: 3GPP TS 29.505 V17.1.0; 5G System; Usage of the Unified Data Repository Service for subscription data; Stage 3

url: 'http://www.3gpp.org/ftp/Specs/archive/29\_series/29.505/'

*(... text not shown for clarity ...)*

components:

schemas:

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

supi:

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

akmaAllowed:

type: boolean

default: false

SequenceNumber:

type: object

properties:

sqnScheme:

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

sqn:

type: string

pattern: '^[A-Fa-f0-9]{12}$'

lastIndexes:

type: object

additionalProperties:

type: integer

minimum: 0

indLength:

type: integer

minimum: 0

difSign:

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

*(... text not shown for clarity ...)*

\* \* \* End of Changes \* \* \* \*