**3GPP TSG-SA3 Meeting #115 *S3-240857***

**Athens, Greece, 26th Feb 2024 - 1st Mar 2024**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1900** | **rev** | **1** | **Current version:** | **18.4.0** |  |
|  |
| *For* ***HE******LP*** *on using this form: comprehensive instructions can be found at http://www.3gpp.org/Change-Requests.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Correction of UDM service naming |
|  |  |
| ***Source to WG:*** | BSI (DE) |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5GS\_Ph1-SEC |  | ***Date:*** | 2024-02-16 |
|  |  |  |  |  |
| ***Category:*** | **A** |  | ***Release:*** | Rel-18 |
|  | *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. | *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:*** | The name of a UDM service does not match the one given by the service definition in TS 29.503. |
|  |  |
| ***Summary of change:*** | Fixed 2 occurrences of Nudm\_UEAuthentication\_Get |
|  |  |
| ***Consequences if not approved:*** | UDM service naming does not adhere to the standard. |
|  |  |
| ***Clauses affected:*** | 3.1, 6.1.3.2.0 |
|  |  |
|  | **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 is a copy of a CR from Gothenburg S3-234191, which was already agreed but did not get fully implemented. The 2nd change was missing in the implementation. No discussion needed. It should automatically be agreed. |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**5G security context:** The state that is established locally at the UE and a serving network domain and represented by the "5G security context data" stored at the UE and a serving network.

NOTE 1: The "5G security context data" consists of the 5G NAS security context, and the 5G AS security context for 3GPP access and/or the 5G AS security context for non-3GPP access.

NOTE 2: A 5G security context has type "mapped", "full native" or "partial native". Its state can either be "current" or "non-current". A context can be of one type only and be in one state at a time. The state of a particular context type can change over time. A partial native context can be transformed into a full native. No other type transformations are possible.

**5G AS security context for 3GPP access:** The cryptographic keys at AS level with their identifiers, the Next Hop parameter (NH), the Next Hop Chaining Counter parameter (NCC) used for next hop access key derivation, the identifiers of the selected AS level cryptographic algorithms, the UE security capabilities, and the UP Security Policy at the network side, UP security activation status and the counters used for replay protection.

NOTE 3: NH and NCC need to be stored also at the AMF during connected mode.

NOTE 4: UP security activation status is sent from gNB/ng-eNB in step 1b in clause 6.6.2 corresponding to the active PDU session(s).

**5G AS security context for non-3GPP access:** The key KN3IWF, the cryptographic keys, cryptographic algorithms and tunnel security association parameters used at IPsec layer for the protection of IPsec SA.

**5G AS Secondary Cell security context**: The cryptographic keys at AS level for secondary cell with their identifiers, the identifier of the selected AS level cryptographic algorithms for secondary cell, the UP Security Policy at the network side, and counters used for replay protection.

**5G** **Home Environment Authentication Vector:** authentication data consisting of RAND, AUTN, XRES\*, and KAUSF for the purpose of authenticating the UE using 5G AKA.

NOTE 3a: This vector is received by the AUSF from the UDM/ARPF in the Nudm\_UEAuthentication\_Get Response.

\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*

##### 6.1.3.2.0 5G AKA

5G AKA enhances EPS AKA [10] by providing the home network with proof of successful authentication of the UE from the visited network. The proof is sent by the visited network in an Authentication Confirmation message.

The selection of using 5G AKA is described in sub-clause 6.1.2 of the present document.

NOTE 1: 5G AKA does not support requesting multiple 5G AVs, neither the SEAF pre-fetching 5G AVs from the home network for future use.



Figure 6.1.3.2-1: Authentication procedure for 5G AKA

The authentication procedure for 5G AKA works as follows, cf. also Figure 6.1.3.2-1:

1. For each Nudm\_UEAuthentication\_Get Request, the UDM/ARPF shall create a 5G HE AV. The UDM/ARPF does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1" as defined in TS 33.102 [9]. The UDM/ARPF shall then derive KAUSF (as per Annex A.2) and calculate XRES\* (as per Annex A.4). Finally, the UDM/ARPF shall create a 5G HE AV from RAND, AUTN, XRES\*, and KAUSF

\*\*\*\*\*\*\*\*\*\* END OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*