**3GPP TSG-SA3 Meeting #104-e *S3-213680***

**e-meeting, 27 - 30 September 2021** Revision of S3-21abcd

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **DraftCR** | **rev** |  | **Current version:** | **17.2.1** |  |
|  |
| *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:***  | Living CR for UC3S in TS 33.501 |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | UC3S\_SEC |  | ***Date:*** | 2021-09-27 |
|  |  |  |  |  |
| ***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 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:*** | Adding the security requirements for the user consent handling in 3GPP services. |
|  |  |
| ***Summary of change:*** | The changes include:* Generic security requirements, services and guidance for user consent check and revocation.

(To be removed when the document is converted to a CR) Change history of the living document:SA3#104-e: * S3-212706 (Draft skeleton for UC3S WID)
 |
|  |  |
| ***Consequences if not approved:*** | No security requirements for the user consent handling in 3GPP services |
|  |  |
| ***Clauses affected:*** | 5.8.X (new), 5.9.2.X (new), 14.2.X (new), 14.2.Y (new), Annex X (new) |
|  |  |
|  | **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's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 5.8 Requirements on the UDM

5.8.1 Generic requirements

The long-term key(s) used for authentication and security association setup purposes shall be protected from physical attacks and shall never leave the secure environment of the UDM/ARPF unprotected.

NOTE 1: Security mechanisms for protection of subscription credentials in ARPF are left to implementation.

NOTE 2: Security mechanisms for storage of subscription credentials in the UDR and for the transfer of authentication subscription data (as specified in 3GPP TS 29.505 [70]) between UDR and ARPF are left to implementation.

5.8.2 Subscriber privacy related requirements to UDM and SIDF

The SIDF is responsible for de-concealment of the SUCI and shall fulfil the following requirements:

- The SIDF shall be a service offered by UDM.

- The SIDF shall resolve the SUPI from the SUCI based on the protection scheme used to generate the SUCI.

The Home Network Private Key used for subscriber privacy shall be protected from physical attacks in the UDM.

The UDM shall hold the Home Network Public Key Identifier(s) for the private/public key pair(s) used for subscriber privacy.

The algorithm used for subscriber privacy shall be executed in the secure environment of the UDM.

5.8.X User consent related requirements

NOTE: The user consent related requirements in the present document are applicable only when it is required by regional regulations or operator’s local policy, not otherwise.

The UDM shall provide the following services related to the user consent.

- retrieval of user consent parameters.

The user consent parameters shall be stored in the UDM as subscription data.

The user consent parameters shall be effective only after the point in time that user consent was given, and they shall be effective until they are revoked.

UDM does not provide revocation service, it only provides notification.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.9 Core network security

5.9.1 Trust boundaries

It is assumed for the set of requirements in this sub-clause that mobile network operators subdivide their networks into trust zones. Subnetworks of different operators are assumed to lie in different trust zones. Messages that traverse trust boundaries shall follow the requirements in sub-clause 5.9.2 of the present document, if not protected end to end by NDS/IP as specified in TS 33.210 [3].

5.9.2 Requirements on service-based architecture

5.9.2.1 Security Requirements for service registration, discovery and authorization

NF Service based discovery and registration shall support confidentiality, integrity, and replay protection.

NRF shall be able to ensure that NF Discovery and registration requests are authorized.

NF Service based discovery and registration shall be able to hide the topology of the available / supported NF's in one administrative/trust domain from entities in different trust/administrative domains (e.g. between NFs in the visited and the home networks.)

NF Service Request and Response procedure shall support mutual authentication between NF Service Consumer and NF Service Producer.

Each NF shall validate all incoming messages. Messages that are not valid according to the protocol specification and network state shall be either rejected or discarded by the NF.

5.9.2.2 NRF security requirements

The Network Repository Function (NRF) receives NF Discovery Request from an NF instance, provides the information of the discovered NF instances to the NF instance, and maintains NF profiles.

The following NRF service-based architecture security requirements shall apply:

NRF and NFs that are requesting service shall be mutually authenticated.

NRF may provide authentication and authorization to NFs for establishing secure communication between each other

5.9.2.3 NEF security requirements

The Network Exposure Function (NEF) supports external exposure of capabilities of Network Functions to Application Functions, which interact with the relevant Network Functions via the NEF.

The interface between the NEF and the Application Function shall fulfil the following requirements:

- Integrity protection, replay protection and confidentiality protection for communication between the NEF and Application Function shall be supported.

- Mutual authentication between the NEF and Application Function shall be supported.

- Internal 5G Core information such as DNN, S-NSSAI etc., shall not be sent outside the 3GPP operator domain.

- SUPI shall not be sent outside the 3GPP operator domain by NEF.

The NEF shall be able to determine whether the Application Function is authorized to interact with the relevant Network Functions.

5.9.2.4 Requirements on the Service Communication Proxy (SCP)

The SCP has interfaces with Network Functions (NF) and peer SCPs within the PLMN. The interface between the SCP and the NFs and between the two SCPs shall fulfil the following requirements:

- Mutual authentication shall be performed between the SCP and NFs, and between the two SCPs within the PLMN.

- All communication between the SCP and NFs and between SCPs shall be confidentiality, integrity and replay protected.

If SCP endpoints are co-located with the NFs, the above two requirements may be satisfied by colocation.

The SCP shall provide confidentiality, integrity and replay protection for its internal communication over SCP internal network interfaces.

5.9.2.X Requirements on User Consent

Editor's Note: This clause will describe the NF requirement on check and revocation of user consent, etc.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

14.2 Services provided by UDM

14.2.1 General

UDM provides within Nudm\_UEAuthentication service all authentication-related service operations, which are Nudm\_UEAuthentication\_Get (clause 14.2.2) and Nudm\_UEAuthentication\_ResultConfirmation (clause 14.2.3).

The complete list of UDM services is defined in TS 23.501 [2], clause 7.2.5, and further refined in TS 23.502 [8], clause 5.2.3.1.

14.2.2 Nudm\_UEAuthentication\_Get service operation

**Service operation name:** Nudm\_UEAuthentication\_Get

**Description:** Requester NF gets the authentication data from UDM. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. If SUCI is included, this service operation returns the SUPI.

**Inputs, Required:** SUPI or SUCI, serving network name.

**Inputs, Optional:** Synchronization Failure indication and related information (i.e. RAND/AUTS).

**Outputs, Required:** Authentication method and corresponding authentication data for a certain UE as identified by SUPI or SUCI input.

Outputs, Optional**:** SUPI if SUCI was used as input. AKMA Indication, if the subscriber has an AKMA subscription (see TS 33.535 [91])

14.2.3 Nudm\_UEAuthentication\_ResultConfirmation service operation

**Service operation name:** UEAuthentication\_ResultConfirmation

**Description:** Requester NF informs UDM about the result of an authentication procedure with a UE.

**Inputs, Required:** SUPI, timestamp of the authentication, the authentication type (e.g. EAP method or 5G-AKA), and the serving network name.

**Inputs, Optional:** None.

**Outputs, Required:** None.

**Outputs, Optional:** None.

14.2.X Nudm\_SDM\_Get service operation used for user consent check

Editor's Note: This clause will describe the inputs and outputs relevant to check of user consent service reusing Nudm\_SDM\_Get services.

14.2.Y Nudm\_SDM\_Notification service operation used for notification of user consent change

Editor's Note: This clause will describe the inputs and outputs relevant to revocation of user consent service reusing Nudm\_SDM\_Notification services.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Annex X (normative): Generic Requirements for adapting procedures related to user consent

X.1 General

### X.1.1 Scope

User consent can be required for 3GPP features depending on local regulations. Therefore, this annex describes the generic security requirements and procedures to support user consent enforcement in 3GPP services. While the use cases can differ, the annex focuses on the common and generic aspects related to the storage, checking and revocation of the user consent.

### X.1.2 Relationship between end-users and subscriber

It is assumed that the user consent is obtained from the end-users. The end-user(s) is the subscriber itself or authorize the subscriber to provide consent on behalf of the end-users. Alternatively, the end-users are authorized by the subscriber to provide the consent. That means user consent is always tied to the subscription information. How authorization is provided between the subscriber and the end-users is out-of-scope of this specification.

NOTE: The term end-user is defined in TR 21.905 [1].

X.2 User consent check

Editor's Note: This clause will describe how to check of user consent in order to provide guideline that if a new use case needs to check of user consent.

X.3 User consent revocation

Editor's Note: This clause will describe how to check of user consent in order to provide guideline that if a new use case needs to check of user consent.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*