**3GPP TSG-SA5 Meeting #141-e *S5-217xxx***

**e-meeting, 17 - 20 January 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **28.532** | **CR** | DraftCR | **rev** | - | **Current version:** |  |  |
|  |
| *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 | **X** | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Rel-17 DraftCR 28.532 for MSAC |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S5 |
|  |  |
| ***Work item code:*** | MSAC |  | ***Date:*** | 2022-01-02 |
|  |  |  |  |  |
| ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | According to discussion paper and requirements related to access control. |
|  |  |
| ***Summary of change:*** | Add new operation to support authentication and authorization capability. |
|  |  |
| ***Consequences if not approved:*** | No standardized way for access control on management service of 3GPP management system, that may cause interoperability issue once security feature is enabled. |
|  |  |
| ***Clauses affected:*** | 11.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 modification** |

## 11.x Access control service

### 11.x.1 Operations and notifications

#### 11.x.1.1 authentication operation (M)

##### 11.x.1.1.1 Definition

The operation used to authenticate a management service (MnS) consumer to the authentication service producer.

Note: The authenticaiton service could be accessed by MnS Consumer directly or by MnS producer. In Explicit Authentication case, Mns Consumer interacts directly with authentication service producer, to acquire authentication assertion or access token to interact with MnS Producer. In Implicit Authentication case, MnS Consumer interacts indirectly with authentication via MnS Producer, to establish a secure session.

##### 11.x.1.1.2 Input parameters

| Parameter Name | S | Information type | Comment |
| --- | --- | --- | --- |
| identifier | M | Identity4AC.identifier | See attribute definition in generic NRM ( see [11] ) |
| credential | M | Identity4AC.credential | See attribute definition in generic NRM ( see [11] ). The credential in the authentication request may not be same as the credential stored in authentication service producer, but it is derived from the credential stored in authentication service producer according to corresponding protocol. |
| assocClient | O | Identity4AC.AuthSes.assocClient | See attribute definition in generic NRM ( see [11] ). It identifies (e.g. FQDN) an associated (machine) client/application which acting on behalf of a human MnS consumer during authentication. e.g. it could be address or hostname of digital portal, user agent, or mediated management function, etc. |

##### 11.x.1.1.3 Output parameters

| Parameter Name | S | Information / Information Type  | Comment |
| --- | --- | --- | --- |
| identifier | M | Identity4AC.identifier | same to the identifier in the request. |
| status | M | ENUM (Success, Failure) | Represent authentication result. |
| sessionId | O | Identity4AC.AuthSes.sessionId | See attribute definition in generic NRM ( see [11] ). Session id of a successful authentication.  |
| context | O | Identity4AC.AuthSes.context | See attribute definition in generic NRM ( see [11] ). It could be, e.g. term of validity of a successful authentication session |
| assertion | O | Identity4AC.AuthSes.assertion | See attribute definition in generic NRM ( see [11] ). It is included in a successful authentication session if the protocol support assertion. |
|  |  |  |  |

|  |
| --- |
| **End of 1st modification** |

|  |
| --- |
| **Start of 2nd modification** |

#### 11.x.1.2 authorization operation (M)

##### 11.x.1.2.1 Definition

The operation is used to authorize a management service (MnS) consumer to the authorization service producer.

##### 11.x.1.1.2 Input parameters

| Parameter Name | S | Information type | Comment |
| --- | --- | --- | --- |
| identifier | M | Identity4AC.identifier | See attribute definition in generic NRM ( see [11] ) |
| credential | M | Identity4AC.credential | See attribute definition in generic NRM ( see [11] ). It could be password, certificate, assertion, etc. |
| assessRight | O | List of DNs of access rights | It identifies the required management services asked by the consumer |

##### 11.x.1.1.3 Output parameters

| Parameter Name | S | Information / Information Type  | Comment |
| --- | --- | --- | --- |
| identifier | M | Identity4AC.identifier | same to the identifier in the request input. |
| result | M | ENUM (Success, Failure) | Represent authorization result. |
| permission | O | List of DNs of permissions | See attribute definition in generic NRM ( see [11] )Permission assigned to an authenticated MnS consumer based on the role/group of the consumer. |
| accessToken | O | AccessToken | See attribute definition in generic NRM ( see [11] )Access token assigned to an authenticated MnS consumer if the protocol supported token. |

Note: Alternatively, may consider to use readMOIAttribute operation to get permissions of a MnS Consumer in a specific sessoin.

|  |
| --- |
| **End of modification** |