**3GPP TSG-SA5 Meeting #139-e *S5-215221***

**e-meeting, 11 - 20 October 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **28.533** | **CR** | **88** | **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:***  | enhance request-response communication paradigm to support access contro |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S5 |
|  |  |
| ***Work item code:*** | MSAC |  | ***Date:*** | 2021-09-29 |
|  |  |  |  |  |
| ***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 conclusion of TR 28.817, the service based management architecture should be updated to support authentication and authorization capabilities for management service access control. |
|  |  |
| ***Summary of change:*** | As proposed in possible solution to support access control on management service in 7.1 of TR 28.817:Enhance Request-response communication paradigm to support authentication and authorization |
|  |  |
| ***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:*** | 5.1.2 |
|  |  |
|  | **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's revision history:*** |  |

|  |
| --- |
| **Start of 1st modification** |

### 5.1.2 Interactions between management service producer and management service consumer

The interactions between the management service producer and management service consumer follows one of the three following paradigms:

- "Request-response": A management service producer is requested by a management service consumer to invoke an operation, which either performs an action or provides information or both. The management service producer provides response based on the request by management service consumer.



Figure 5.1.1.1: Request-response communication paradigm

- "Subscribe-notify": A management service consumer requests a management service producer to establish a subscription to receive network events via notifications, under the filter constraint specified in this operation.

Subscriptions can be created also by other means than by using such operation.



Figure 5.1.1.2: Subscribe-notify communication paradigm

NOTE: Example of a common aspect applicable to all management services is the use of notifications. For a management service to use notifications the management service consumer needs a subscription to notifications it is interested in. The management service consumer requests the creation of a subscription by sending a subscribe operation to the management service producer. To cancel a subscription the consumer sends an unsubscribe operation to the producer.

- "Connect-streaming": A management producer is provided with the address the management service consumer. The management service producer requests to establish a connection with the management service consumer for management data streaming. The management service producer sends the management data, when they are ready, by streaming to the management service consumer over the established connection.



Figure 5.1.1.3: Connect-streaming communication paradigm

- "Request-response with access control": An authentication service producer is requested by a management service consumer for authentication, the authentication service producer authenticates the management service consumer according to information provided by the management service consumer and authentication policies associated to the management service consumer. After successfully authenticated, the management service consumer may send request to an authorization service producer to get access permissions, and sends request to corresponding management service producers to invokes operations . The management service producer provides response based on the request by management service consumer andaccess permissions granted to the management service consumer. Figure 5.1.1.x-1 and Figure 5.1.1.x-2 depicte typical Request-response communication paradigm with access control.

NOTE: A management service consumer may send request to management service producer without permissions from authorization service producer, in this case, the management service producer checks the permissions of the management service consumer with authorization service producer before providing response to the management service consumer. A management service consumer may also send request for authorization without authentication with authetnication service producer. In this case, authorization service producer may interact with authenticaiton service producer to authenticate management serivce consumer. In addition, local authentication and authorziation enforcement may be supported by management service producer for specific deployment options. In other words, the authentication and authorization service producers may be deployed together with a management service producer.



Figure 5.1.1.x-1: Request-response communication paradigm with access control (access token is supported)



Figure 5.1.1.x-2: Request-response communication paradigm with access control (access token is not supported)

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