**3GPP TSG-SA5 Meeting #139-e *S5-215222***

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **28.622** | **CR** | DraftCR | **rev** | - | **Current version:** | **16.10.0** |  |
|  |
| *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 | **X** | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Rel-17 DraftCR 28.622 for MSAC |
|  |  |
| ***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 discussion paper and requirements related to access control. |
|  |  |
| ***Summary of change:*** | Add NRM fragment 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:*** | 4.2, 4.3.x (new), 4.3.y (new), 4.3.z (new), 4.3.xx (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:*** | Information model to access ASP is similar to information to access other MnSP, which could be part of discovery WI. |
|  |  |
| ***This CR's revision history:*** |  |

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

## 4.2 Class diagrams

### 4.2.1 Relationships

This clause depicts the set of classes (e.g. IOCs) that encapsulates the information relevant for this IRP. This clause provides the overview of the relationships of relevant classes in UML. Subsequent clauses provide more detailed specification of various aspects of these classes.

The following figure shows the containment/naming hierarchy and the associations of the classes defined in the present document. See Annex A of a class diagram that combines this figure with Figure 1 of [2], the class diagram of UIM.



NOTE 1: ManagedElement may be contained either

- in a SubNetwork (since *SubNetwork* inherits from *Domain*\_ and *ManagedElement* inherits from *ManagedElement*\_ and *Domain*\_ name-contained *ManagedElement\_* as observed in the figure of Annex A) or

- in a MeContext instance as observed by the above figure or in the figure of Annex A.

This either-or relation cannot be shown by using an {xor} constraint in the above figure.

ManagedElement may also have no parent instance at all.

NOTE 2: Void

NOTE 3: If the configuration contains several instances of SubNetwork, exactly one SubNetwork instance shall directly or indirectly contain all the other SubNetwork instances.

NOTE 4: The SubNetwork instance not contained in any other instance of SubNetwork is referred to as "the root SubNetwork instance".

NOTE 5: ManagementNode shall be contained in the root SubNetwork instance.

NOTE 6: If contained in a SubNetwork instance, MnsAgent shall be contained in the root SubNetwork instance.

NOTE 7: For a clarification on the choice of containment of the IRPAgent (since it has three possible parents), see the definition of MnsAgent.

NOTE 8: The MnsAgent shall be replaced by the IRPAgent in deployments using the IRP framework as defined in TS 32.102 [2].

Figure 4.2.1-1: NRM fragment

Each Managed Object is identified with a Distinguished Name (DN) according to 3GPP TS 32.300 [13] that expresses its containment hierarchy. As an example, the DN of a ManagedElement instance could have a format like:

 SubNetwork=Sweden,MeContext=MEC-Gbg-1,ManagedElement=RNC-Gbg-1.



NOTE 8: Void

NOTE 9: Void

Figure 4.2.1-2: Vendor specific data container NRM fragment



Figure 4.2.1-3: PM control NRM fragment



Figure 4.2.1-4: Threshold monitoring control NRM fragment



Figure 4.2.1-5: Notification subscription and heartbeat notification control NRM fragment



Figure 4.2.1-6: FM control NRM fragment



Figure 4.2.1-7: Trace control NRM fragment



Figure 4.2.1-x: Access control NRM fragment

Figure 4.2.1-y: Access control NRM fragment for authorization

### 4.2.2 Inheritance

This clause depicts the inheritance relationships.





Figure 4.2.2-1: NRM fragment



Figure 4.2.2-2: PM control NRM fragment



Figure 4.2.2-3: Threshold monitoring control NRM fragment



Figure 4.2.2-4: Notification subscription and heartbeat notification control NRM fragment



Figure 4.2.2-5: FM control NRM fragment



Figure 4.2.2-6: Trace control NRM fragment



Figure 4.2.2-x: Access control NRM fragment

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

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

### 4.3.x Identity4AC

#### 4.3.x.1 Definition

A Identity4AC is an identity used for authentication and authorization. It represents a management service consumer or producer.

#### 4.3.x.2 Attributes

The Identity4AC IOC includes attributes inherited from Top IOC (defined in clause 4.3.29) and the following attributes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| administrativeState | M | T | T | F | T |
| identifier | M | T | T | F | T |
| identifierType | O | T | T | F | T |
| identityType | M | T | F | T | F |
| identityStatus | O | T | T | F | T |
| identityOwner | O | T | T | F | T |
| identityDomain | O | T | T | F | T |
| authSessionList | O | T | F | F | T |
| credential | M | T | T | F | T |
| **Attribute related to role** |  |  |  |  |  |
| groupRef | M | T | T | F | T |
| roleRef | O | T | T | F | T |

#### 4.3.x.3 Attribute constraints

None.

#### 4.3.x.4 Notifications

The common notifications defined in clause 4.5 are valid for this IOC, without exceptions or additions

### 4.3.y GroupOfIdentity

#### 4.3.y.1 Definition

A GroupOfIdentity represents a group of management service consumers or producers.

#### 4.3.y.2 Attributes

The GroupOfIdentity IOC includes attributes inherited from Top IOC (defined in clause 4.3.29) and the following attributes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| administrativeState | M | T | T | F | T |
| groupType | M | T | F | T | F |
| groupOwner | O | T | T | F | T |
| groupDomain | O | T | T | F | T |
| noOfMembers | O | T | F | F | T |
| **Attribute related to role** |  |  |  |  |  |
| authPolicyRef | CM | T | T | F | T |
| identityRef | M | T | F | F | T |
| roleRef | O | T | T | F | T |
| permRef | O | T | T | F | T |

#### 4.3.y.3 Attribute constraints

Attribute constraint for authPolicyRef: The attribute authPolicyRef should be supported by a GroupOfIdentity MOI if the MOI is designed to represent a group of management service consumers.

#### 4.3.y.4 Notifications

The common notifications defined in clause 4.5 are valid for this IOC, without exceptions or additions

### 4.3.z Policy4Authn

#### 4.3.z.1 Definition

A Policy4Authn represents authentication policy which can be assigned to a group of management service consumers.

#### 4.3.z.2 Attributes

The Policy4Authn IOC includes attributes inherited from Top IOC (defined in clause 4.3.29) and the following attributes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| policies | M | T | T | F | T |

#### 4.3.z.3 Attribute constraints

None.

#### 4.3.z.4 Notifications

The common notifications defined in clause 4.5 are valid for this IOC, without exceptions or additions

### 4.3.xx AuthSession <<dataType>>

#### 4.3.xx.1 Definition

This dataType defines state, condition and other context of an authentication session of a management service consumer.

#### 4.3.xx.2 Attributes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| sessionId | M | T | F | F | T |
| authState | M | T | F | F | T |
| context | O | T | F | F | T |
| assocClient | O | T | F | F | T |
| assertion | O | T | F | F | T |

|  |
| --- |
| **End of 2nd modification** |

|  |
| --- |
| **Start of 3rd modification** |

### 4.3.a AccessRight

#### 4.3.a.1 Definition

An AccessRight represents access right on a managed object instance (MOI) on which the access right is applied, e.g. read, update or delete the MOI, read or update attribute of the MOI, read MIB tree (naming containment tree) of the MOI, create/delete child MOI (contained MOI) of the MOI, etc.

#### 4.3.a.2 Attributes

The AccessRight IOC includes attributes inherited from Top IOC (defined in clause 4.3.29) and the following attributes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| operation | M | T | T | F | T |
| attribute | M | T | T | F | T |
| childObjectClass | O | T | T | F | T |
| childObjectInstance | O | T | T | F | T |

#### 4.3.a.3 Attribute constraints

None.

#### 4.3.a.4 Notifications

The common notifications defined in clause 4.5 are valid for this IOC, without exceptions or additions.

### 4.3.b ResourceGroup

#### 4.3.b.1 Definition

A ResourceGroup represents group of managed object instance. Resource could be grouped for a PLMN, a tenant, a domain, a network slice or a service, etc.

#### 4.3.b.2 Attributes

The ResourceGroup IOC includes attributes inherited from Top IOC (defined in clause 4.3.29) and the following attributes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| administrativeState | M | T | T | F | T |
| name | M | T | F | T | F |
| profile | M | T | T | F | T |
| **Attribute related to role** |  |  |  |  |  |
| resource | M | T | T | F | T |

#### 4.3.b.3 Attribute constraints

None.

#### 4.3.b.4 Notifications

The common notifications defined in clause 4.5 are valid for this IOC, without exceptions or additions.

### 4.3.c ResourceGroupProfile <<dataType>>

#### 4.3.c.1 Definition

This dataType defines the profile of the group includes properties of the resource group.

#### 4.3.c.2 Attributes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| owner | O | T | F | F | T |
| domain | O | T | F | F | T |
| plmnId | O | T | F | F | T |
| sNSSAI | O | T | F | F | T |
| region | O | T | F | F | T |

### 4.3.d RoleInfo

#### 4.3.d.1 Definition

A RoleInfo IOC represents the role to be created/read/updated/deleted.

#### 4.3.d.2 Attributes

The RoleInfo IOC includes attributes inherited from Top IOC (defined in clause 4.3.29) and the following attributes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| administrativeState | M | T | T | F | T |
| name | CM | T | F | T | F |
| **Attribute related to role** |  |  |  |  |  |
| permRef | CM | T | T | F | T |

#### 4.3.d.3 Attribute constraints

None.

#### 4.3.d.4 Notifications

The common notifications defined in clause 4.5 are valid for this IOC, without exceptions or additions.

### 4.3.e PermInfo

#### 4.3.e.1 Definition

A PermInfo IOC represents a permission assigned to a role or group.

#### 4.3.e.2 Attributes

The PermInfo IOC includes attributes inherited from Top IOC (defined in clause 4.3.29) and the following attributes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| condition | M | T | T | F | T |
| **Attribute related to role** |  |  |  |  |  |
| accessRight | M | T | T | F | T |
| subjectRef | M | T | T | F | T |

#### 4.3.e.3 Attribute constraints

None.

#### 4.3.e.4 Notifications

The common notifications defined in clause 4.5 are valid for this IOC, without exceptions or additions

### 4.3.f AccessToken

#### 4.3.f.1 Definition

An AccessToken IOC represents a list of permissions granted the authorization service producer to an authenticated MnS consumer by in specific context .

#### 4.3.f.2 Attributes

The AccessToken IOC includes attributes inherited from Top IOC (defined in clause 4.3.29) and the following attributes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | S | isReadable  | isWritable | isInvariant | isNotifyable |
| issuer | M | T | F | F | T |
| context | M | T | F | F | T |
| Type | M | T | F | F | T |
| **Attribute related to role** |  |  |  |  |  |
| consumer | M | T | F | F | T |
| permRef | M | T | F | F | T |

#### 4.3.f.3 Attribute constraints

None.

#### 4.3.f.4 Notifications

The common notifications defined in clause 4.5 are valid for this IOC, without exceptions or additions

|  |
| --- |
| **End of 3rd modification** |