**TSG-SA5 Meeting #162 *S5-253955d1***

**, , – Revision of S5-253464**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.3* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0010** | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: compr*  *ehensive 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-19 CR TS 28.319 Clarify default behaviour for access control | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | , Huawei | | | | | | | | | |
| ***Source to TSG:*** | SA5 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | MSAC | | | | |  | ***Date:*** | | | 2025-08-28 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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 can be 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-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)  Rel-20 (Release 20)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Clarify system default behaviour for access control. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify system default behaviour for access control. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The default behavior for access control is important for MSAC implementation. Leaving it unspecified may lead to wrong developments, which may risk the security protection of the system resources. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7.3.3.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | No stage 3 | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

|  |
| --- |
| **1st Change** |

## 7.3 Class definitions

### 7.3.1 Identity

#### 7.3.1.1 Definition

This class represents an identity of a MnS consumer. It is used for authentication and authorization.

The MnS consumer can be a human or a machine user. This class enables the creation and storage of an identity of a MnS consumer. The information in this class is the starting point for a MnS consumer to identity who it is. This is validated against an authentication service producer.

For the authentication operation to take place the identity related information has to be provisioned into the system by a network operator who could be an administrator. The administrator adds the identityType attribute and identityName attribute which characterizes a machine user or human user respectively. For example, an operator might have an identity like a tenant mapped to the relevant list of roles.

Attribute credential is used to provide information for the credential used together with identity when requesting authentication. The examples of credential are password, certificate, biometric, etc.

The roleList attribute defines the role names associated to a particular Identity.

The class stores the details of the expected tasks to be performed by an identity. The tasks are what is to be done on the network management system. To ease the administration on the system, the tasks are organised as roles. The user can be associated to one or more roles.

#### 7.3.1.2 Attribute

The Identity class includes the following attributes:

|  |  |
| --- | --- |
| **Attribute Name** | **S** |
| identityType | M |
| identityName | M |
| credential | O |
| **Attributes related to role** |  |
| roleList | M |

#### 7.3.1.3 Attribute constraints

None.

### 7.3.2 Role

#### 7.3.2.1 Definition

The Role class represents a task or collection of tasks in a network management system.

The Role class enables the storage of information as to what resources and actions an identity can work upon. This class maintains the resources that are known to the management system. This contains all the granular level resources and the corresponding actions.

The roleName attribute defines the name of a role.

The accessRulesList attribute contains a list of access rules that contain the list of granular permission sets. This could be the possible order in which the access rules are considered by the MnS producer.

#### 7.3.2.2 Attribute

|  |  |
| --- | --- |
| **Attribute Name** | **S** |
| roleName | M |
| **Attribute related to role** |  |
| accessRulesList | M |

### 7.3.3 AccessRule

#### 7.3.3.1 Definition

The AccessRuleclass represents the granular resource and actions in a network management system on which an action has to be performed.

This class enables the storage of the resource types in the system and the possible actions that are allowed on it. The permutations and combinations of these permissions are assigned to a role.

The roleName attribute binds the instances in the network as well as the permissions and the operations allowed upon it.

The dataNodeSelector attribute defines the resources. The resources are classes(IOC) or instances of classes(MOI) in the network that need to be access controlled. The resources define the root instances or the leaf instances. For example, the Managed Element could be the root object and the attributes could be referred to as the leaf objects. The resources here could be whole classes or specific instances of classes with a known DN value or could be an expression(e.g.: XPATH or JEX) that could be resolved by the producer to get the nodes at runtime.

Examples of the resources attribute value could be as below. Please note this is not an exhaustive set of examples and shown for depiction purpose.

a) Values related to IOC:

- Description: this means that:

- all attributes of an IOC are eligible for the access rule.

- at operation time, all instances of this IOC are eligible for the access rule.

Examples 1:

1) IOC name : "ManagedElement"

2) Expression resolving to IOCs under a subnetwork SN1:

"/SubNetwork[id="SN1"]/ManagedElement"

b) Values related to one or more instances of an IOC:

- Description: this means that:

- all attributes of the IOC are eligible for the access rule.

- at operation time, only the specified instances of this IOC are eligible for the access rule.

Examples 2:

Specific instance of IOC name : "SN1/ME1"

c) Values related to one or more IOC attributes:

- Description: this means that:

- only the specified attributes of the IOC are eligible for the access rule.

- at operation time, all attributes of the instances of this IOC are eligible for the access rule.

Examples 3:

1) Attribute name: "SubNetwork/ManagedElement/vendorName"

2) Expression resolving to specific instance of attribute name "/SubNetwork[id="SN1"]/ManagedElement[id="ME1"]/attributes[vendorName="Company XY"]"

3) Specific attribute instance: "SN1/ME1/vendorName='Company XY'"

d) Any combination between a-c.

The operations attribute defines the list of operations that are permitted on the resources value encompassed under this ruleName.

The actions is an optional attribute which specifies whether the operation allows to permit all or deny all and may be used depending on the solution set.

The componentCData is an optional attribute which specifies notification types and performance metric names. The "dataNodeSelector" shall specify objects when access rights for notifications and performance metrics are specified.

When an MnS consumer requests a MnS producer to perform an operation over a resource, the MnS producer leverages the authorization service producer (TS 28.533 [5]) to authorize such request. If the request cannot be resolved to a valid Role and AccessRule, then the default system behaviour is to deny the MnS consumer request.

#### 7.3.3.2 Attribute

|  |  |
| --- | --- |
| **Attribute Name** | **S** |
| ruleName | M |
| dataNodeSelector | M |
| operations | M |
| actions | O |
| componentCData | O |

#### 7.3.3.3 Attribute constraints

None.

|  |
| --- |
| **End of Changes** |