**3GPP TSG-SA5 Meeting #154 *S5-242210***

Changsha, China, 15 - 19 April 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **28.319** | **CR** | **0002** | **rev** | **1** | **Current version:** | **0.0** |  |
|  | | | | | | | | |
| *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-18 CR TS 28.319 Add mnsType in accessRule | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei | | | | | | | | | |
| ***Source to TSG:*** | S5 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | MSAC | | | | |  | ***Date:*** | | | 2024-4-5 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Unclear on how authentication and/or authorization process is done. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add brief description for authentication and/or authorization process with reference to TS 28.533. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear description of authentication and/or authorization process | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | clause 2, 7.3.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[x] 3GPP TS 28.622: " Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)".

[y] 3GPP TS 28.533: " Management and orchestration; Architecture framework".

|  |
| --- |
| **Next Change** |

### 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 maybe 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.

Based on the creation of *role* and *accessRule* and the association between *identity* and *accessRule*, access control MnS producer obtains the information of the permissions on management service and management data for MnS consumer (e.g. tenant). When an MnS consumer requests a management service with corresponding input parameters, the access control (i.e. authentication and/or authorization) could be done explicitly as described in TS 28.533 Annex D [y]. Only with successful permission verification, the MnS consumer can consume the management service to which the input parameters indicate.

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

|  |
| --- |
| **Next Change** |

## 7.4 Attribute definitions

### 7.4.1 Attribute properties

The following table defines the properties of attributes specified in the present document.

| Attribute Name | Documentation and Allowed Values | Properties |
| --- | --- | --- |
| identityType | This indicates a type of identifier  AllowedValues: username, email address, phone number, IP address, machineuser | type: ENUM  multiplicity: 1  isOrdered: NA  isUnique: NA  defaultValue: None  isNullable: False |
| identityName | This defines a readable string to uniquely represent an identity  AllowedValues: NA | type: String  multiplicity: 1  isOrdered: NA  isUnique: NA  defaultValue: None  isNullable: False |
| credential | The credential of an MnS consumer or producer used for authentication with authentication service producer. It could be password, certificate, key, pass phrase, etc., based on authentication protocol and factor.  AllowedValues: NA | type: String  multiplicity: 1  isOrdered: N/A  isUnique: N/A  defaultValue: No value  isNullable: False |
| roleList | This defines the list of roles associated with an identity  AllowedValues: NA | type: DN  multiplicity: \*  isOrdered: False  isUnique: True  defaultValue: None  isNullable: False |
| roleName | This string defines a unique representation of the name of a role  AllowedValues: NA | type: String  multiplicity: 1  isOrdered: NA  isUnique: NA  defaultValue: None  isNullable: False |
| accessRuleList | This defines the list of access rules associated with a role  AllowedValues: NA | type: DN  multiplicity: \*  isOrdered: False  isUnique: True  defaultValue: None  isNullable: False |
| ruleName | This string defines a unique representation of the name of an access rule.  The name of the access rule could also contain the name of the management service  AllowedValues: NA | type: String  multiplicity: 1  isOrdered: NA  isUnique: NA  defaultValue: None  isNullable: False |
| dataNodeSelector | This attribute contains an expression allowing to select data nodes (Component type B). The expression semantic and syntax is SS specific.  AllowedValues: NA | type: String  multiplicity: 1  isOrdered: False  isUnique: True  defaultValue: None  isNullable: False |
| operations | This defines the Component A related operations.  The operations related to attributes are also contained in this set.  The operations are of the MnS as defined in 28.532.  AllowedValues: NA | type: String  multiplicity: \*  isOrdered: False  isUnique: True  defaultValue: None  isNullable: False |
| actions | This defines whether the operation is allowed or denied on the operation  AllowedValues: allow, deny | type: ENUM  multiplicity: 1  isOrdered: NA  isUnique: NA  defaultValue: None  isNullable: False |
| componentCData | This attribute defines alarm types and performance metrics.  AllowedValues: NA | type: String  multiplicity: \*  isOrdered: False  isUnique: True  defaultValue: None  isNullable: False |
|  |  |  |

|  |
| --- |
| **Next Change** |

\*\*\* OpenAPI/TS28319\_MsacNrm.yaml \*\*\*

<CODE BEGINS>

openapi: 3.0.1

info:

title: MSAC NRM

version: 18.0.0

description: >-

OAS 3.0.1 definition of the MSAC NRM

© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

externalDocs:

description: 3GPP TS 28.319; MSAC NRM

url: http://www.3gpp.org/ftp/Specs/archive/28\_series/28.319/

paths: {}

components:

schemas:

#-------- Definition of types-----------------------------------------------------

#-------- Definition of concrete IOCs --------------------------------------------

Identity-Single:

allOf:

- $ref: 'TS28623\_GenericNrm.yaml#/components/schemas/Top'

- type: object

properties:

attributes:

type: object

properties:

identityType:

type: string

enum:

- USERNAME

- EMAIL\_ADDRESS

- PHONE\_NUMBER

- IP\_ADDRESS

- MACHINEUSER

identityName:

type: string

credential:

type: string

roleRefList:

$ref: 'TS28623\_ComDefs.yaml#/components/schemas/DnList'

Role-Single:

allOf:

- $ref: 'TS28623\_GenericNrm.yaml#/components/schemas/Top'

- type: object

properties:

attributes:

type: object

properties:

roleName:

type: string

accessRulesList:

$ref: 'TS28623\_ComDefs.yaml#/components/schemas/DnList'

AccessRule-Single:

allOf:

- $ref: 'TS28623\_GenericNrm.yaml#/components/schemas/Top'

- type: object

properties:

attributes:

type: object

properties:

ruleName:

type: string

resources:

type: string

operations:

type: array

items:

type: string

actions:

type: string

enum:

- ALLOW

- DENY

componentCData:

type: array

items:

type: string

resources-msacNrm:

oneOf:

- $ref: '#/components/schemas/Identity-Single'

- $ref: '#/components/schemas/Role-Single'

- $ref: '#/components/schemas/AccessRule-Single'

<CODE ENDS>

|  |
| --- |
| **End of changes** |