ETSI TS 128 319 V18.2.0 (2025-03)

5G;
Management and orchestration;
Access Control for Management services
(3GPP TS 28.319 version 18.2.0 Release 18)

Reference
RTS/TSGS-0528319vi20

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 4
1 Scope 6
2 References 6
3 Definitions of terms, symbols and abbreviations 6
3.1 Terms 6
3.2 Symbols 6
3.3 Abbreviations 6
4 Concepts and overview 6
5 Requirements 10
6 High level solution description 10
7 Model 11
7.0 Introduction 11
7.1 Imported information entities and local labels 11
7.2 Class diagrams 11
7.3 Class definitions 12
7.3.1 Identity 12
7.3.1.1 Definition 12
7.3.1.2 Attribute 13
7.3.1.3 Attribute constraints 13
7.3.2 Role 13
7.3.2.1 Definition 13
7.3.2.2 Attribute 13
7.3.2.3 Attribute constraints 13
7.3.3 AccessRule 13
7.3.3.1 Definition 13
7.3.3.2 Attribute 15
7.3.3.3 Attribute constraints 15
7.4 Attribute definitions 15
7.4.1 Attribute properties 15
Annex A (normative): Solution sets 17
A.1 RESTful HTTP-based solution set 17
A.2 NETCONF/YANG solution set 17
Annex B (informative): Change history 18
History 19

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies access control for management services.

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".

[2] 3GPP TS 32.161: "Management and orchestration; JSON expressions (Jex)".

[3] Void.

[4] IETF RFC 8341: " Network Configuration Access Control Model".

[5] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[6] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[7] 3GPP TS 28.623: "Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Solution Set (SS) definitions".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

4 Concepts and overview

Identity and Access Control

Network Management systems are becoming a challenge to manage in terms of the users of the system as well as the access control that needs to be applied continuously on a need-to-know basis.

Flexibility and agility to adapt to these growing needs is the key for a sustainable identity and access control implementation.

The service based architecture needs to factor seamless integration to any system for authentication and authorization of Management Service (MnS) consumers.

The need to make continuous access control related changes should be supported with ease and simplicity.

Today there are various human users, machine users and various resources that are continuously growing with complexities below:

- Human users seem to require various levels of access control.
- Machine type of communication in the direction towards automated systems require another type of access and may not necessarily be user name password based.
- Resources and modules themselves require various level of clearance depending on the sensitivity of the data being accessed.

The identity and access control system should be designed for role based access control. Also the authorization rules may support the fine grained permissions i.e. based on MnS component A, B and C.

Role based access control

This is based upon the concept of assigning the appropriate permissions and privileges to authorized users. The combinations of the permissions and privileges make up a role. The users who belong to a role should be assigned to resources based on a least privilege principle and access rules associated to the resource. The principle of least privileges states that the users should be granted access only to the data and the operations that are required to perform the job. This minimizes the possibility of a security breach.

The management system should be setup for access control by a system administrator who will have the know-how of creating the required users and roles. Roles will use the various access rules. Additionally, the system administrator will also need to setup the access rules for a MnS producer.

Roles could be in various categories like full access and restricted access.

Figure 4-1: Role based access control

The Figure 4-1 shows how a user is assigned to a role. The roles in turn are able to act upon a resource with the required operation on a MnS Producer. The operations that can be performed are defined by the access rules.

The Figure 4-2 shows an example of how role based access control is adapted to service based management architecture. In the service based management architecture, the user is regarded as MnS consumer, and the combination of resource and operation is represented by management services. Different MnS consumers can be assigned to one role or different roles. The access rules for roles will be configured according to the MnS consumer access right of management service instances which are composed by different MnS component A and component B or component C.

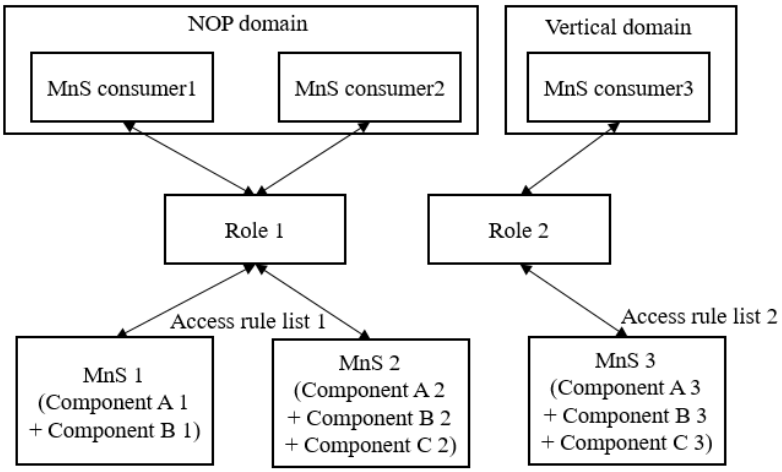

Figure 4-2: Example of role based access control of management services

MnS consumers belonging to different domains (e.g. NOP domain and Vertical domain) are assigned to different roles respectively. For each role, there is an associated access rule list which shows the allowed accessing scope of MnSs. MnS 1, MnS 2 and MnS 3 are different with each other in at least one of the component A, component B and component C.

Entities in access control

In a distributed system the responsibilities of authentication and authorization is split between several entities (Figure 4-3):

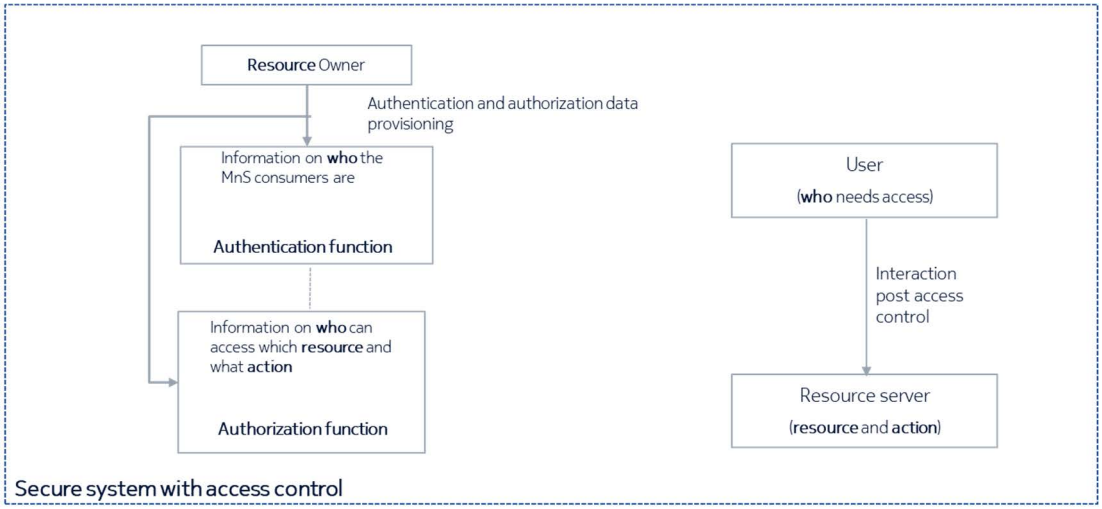

Figure 4-3: Entities in access control

The figure 4-3 shows the various entities that need to be involved in setting up and using access control. Irrespective of any implementation and functional split, the concept of access control is based on the following steps:

- The resource server needs to relate to the request coming from the user to a known identity
- The resource server needs to relate to the request coming from the user to resource, which in case of SBMA means a combination of MnS components as defined in TS 28.533 [5], i.e. MnS operations (component A), object instances or classes from the NRMs (component B), and alarm information or performance data (component C).
- The resource server needs to check whether the requesting identity is allowed to perform the requested operation on the requested resources. These checks can be assigned to a functional block for authentication and a block for authorization, no matter whether these functional blocks are internal parts of a management function (e.g. as part

of a Netconf server) or whether these blocks are visible as standalone services (e.g. like a dedicated OAuth authorization server).

- As precondition for any access control and irrespective of any implementation or deployment, the owner of the resources needs to configure these functional blocks in order to define which identity is allowed to access which resources.

Access control is highly specific to the solution set, the protocol and the CRUD operations defined by the solution underlying the solution set. For example, oAUTH offers the possibility of the authentication and authorization function integrated and Netconf has the possibility of authentication taking place separately on the transport layer and the authorization separately on the Netconf server. Netconf will use standardized RFC 8341 Network Configuration Access Control Model (NACM). REST solutions with OpenAPI will use OAUTH2.0.

The different entities need to have a common notion of the security-related parameters. E.g. Authentication and authorization function and potential user need to use the same notion of identity, as well as authentication and authorization function and potential resource server need to use the same notion of resource. Therefore the involved entities need to be based on an overarching security-related information model (explained in next clause related to Information Model), which is the basis for the concrete data models of the security-related interfaces that are needed to fulfil the security-related use cases of access control

Use case: authentication and authorization

Authorization function and resource server need to have a common understanding of resources and refer to the same resources and corresponding actions. The access control information needs to be provisioned in the authentication and authorization function.

To carry out authentication and authorization based on role-based access the following tasks needs to be in place.

Pre-deployment task – This relates to the identification of the resources represented by the MnS component B and C and it associated operations represented by MnS component A. This is typically done by a Network Equipment Provider (NEP) during the design phase.

Post deployment task – this relates to the set of administrative tasks which are requires to enable role-based access control typically caried out by a network operator (NOP). This is done once the system is up and running and access control needs to be administered.

Post the above tasks there is the possibility to have role-based access in operation with every service call being authenticated and authorized.

When an MnS is invoked, the MnS consumer authenticates towards an authentication service producer. This is then followed by checking the access rights with respect to the role-based access. This takes place in the authorization service producer which is invoked from the MnS producer to check if its resources can be accessed with respect to the related operation.

Use case: identity to roles association

The identity or user of the system needs to be assigned the permissions to carry out the management operations. A set of permissions is defined as a role. An efficient and flexible means is to define various roles by a network operator. In a second step, association of the roles to an identity (entity or human user) is carried out.

Roles associated to resources (consisting of IOCs, MOIs and corresponding operations)

Role-based access control defines roles. Roles are associated to access rules which are combinations of resources and operations (e.g., CRUD operations). The resources can be represented by IOCs(static) and/or MOIs (dynamic). Hence the resources in context are typically Component B and the operations are Component A.

Component C which represents that management data is also a possible resource to be access control protected.

The present TS specifies the information model allowing to configure access control rules into the system. Access control for CRUD operations, notifications and performance metrics is covered.

5 Requirements

REQ-MSAC-01 3GPPP management system shall support role-based access control for the resources represented by the MnS components A, B and C.

REQ-MSAC-01.01 3GPP management system shall support authentication and authorisation for management services.

REQ-MSAC-01.02 3GPP management system shall support identity to role assignment.

REQ-MSAC-01.03 3GPP management system shall support roles which are associated to resources (IOCs and/or MOIs) and the corresponding operations.

REQ-MSAC-02: The security information model should support identity information.

REQ-MSAC-03: The security information model should support authorization at MOI level.

REQ-MSAC-04: The security information model should support authorization at MOI attribute level.

REQ-MSAC-05: The security information model should support authorization of operations.

REQ-MSAC-06: The security information model should support authorization of notifications.

6 High level solution description

This clause elaborates the information architecture of the classes necessary to enable the role based access control explained in the clause above. This clause elaborates the concept into further logical classes that need to interact to enable the design.

The classes, attributes specified here shall be seen as concepts that might not have a direct mapping in some solution sets.

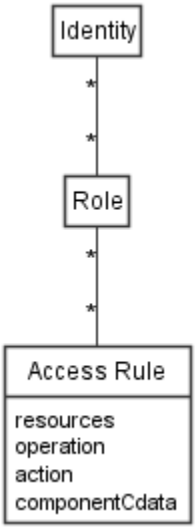

Figure 6-1: Information model for role based access control relationship

The information model above depicts the following to realise a role based access control relationship:

- One Identity could be associated to one or more Roles.
- One Role might be associated to one or more Access Rules. One Role might be associated to one or more Identities.

- The Access rule class allows protecting resources, by specifying which permissions are eligible for each resource. A resource is identified by the class name or class instance. The permission specifies which operation (identified by a CRUD) is applicable and possibly which action (allow or deny) is applicable".

The classes represent the information architecture that is necessary to implement an access control system. They are and not meant to be provisioned and managed like the NRM classes.

This clause provides an overview of the relationships between relevant classes in UML format.

As mentioned in the use cases the classes are provisioned during the integration time by a network operator. The data is sent to an authentication and authorization service producer.

Post this during integration time when a MnS consumer invokes an operation on the MnS producer, the authentication and authorization service producer validates the action on the resource to enable the decision for the MnS producer. The decision could be that the MnS producer allows or disallows the action on the resource.

The information architecture translates to the design which considers the below:

- The authentication function mainly contains the 'who' of the MnS consumers. The authorization function contains the information of the resource and the action of the MnS producer associated to the 'who' of the MnS consumers. These functions could be collocated or distributed.

- The MnS consumer is associated to 'who' is carrying out the operation and has to be known to the resource owner who will provide this information. The MnS consumer interacts with an authentication function to identify itself.

- The MnS consumer interacts with the authorization function whether it can carry out the action on the resource. The resource owner also provisions the information associating various resources and corresponding actions to valid MnS consumers as a pre-step.

- The MnS consumer interacts with the MnS producer after getting responses from the authentication and authorization functions. The MnS producer further does a validation if the action on its resource can be allowed or not.

The above interactions can be realized in any implementation.

7 Model

7.0 Introduction

This clause specifies the information model used to configure access control rules into the system.

The following rules for specifying NRMs are relaxed in this (stage 2) information model:

- No name-containment is specified.

- The object definitions do not have a naming attribute.

7.1 Imported information entities and local labels

None.

7.2 Class diagrams

This clause specifies the class diagram.

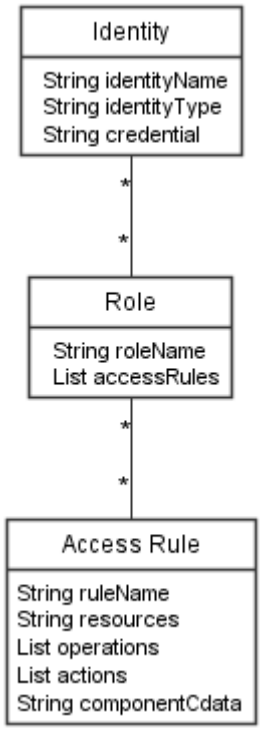

Figure 7.2-1: Classes for role based access control

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

7.3.2.3 Attribute constraints

None.

7.3.3 AccessRule

7.3.3.1 Definition

The AccessRule class 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.

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.

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, machine user	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 TS 28.532 [6]. 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

Annex A (normative): Solution sets

A.1 RESTful HTTP-based solution set

The value of the "dataNodeSelector" is specified using Jex (TS 32.161 [2]).

The naming attribute is used (cf. clause 7.1). This allows to construct Distinguished Names for object instances. Attributes related to roles (pointer attributes) use Distinguished Names as values.

The OpenAPI definitions of the NRM allowing to configure the access control rules into the system are specified in 3GPP Forge, refer to clause 4.3 of TS 28.623 [7] for the Forge location. An example of Forge location is: "https://forge.3gpp.org/rep/sa5/MnS/-/tree/Tag_Rel18_SA104/".

Directory: OpenAPI

Files:

TS28319_MsacNrm.yaml

A.2 NETCONF/YANG solution set

The NETCONF/YANG solution is based on IETF RFC 8341 [4].

The YANG module "ietf-netconf-acm" specifies the datastore for configuring the access control rules into the NETCONF server. Table A.2-1 specifies the mapping of the stage 2 class names to the YANG node names.

Table A.2-1: Mapping stage 2 class names to YANG node names

Stage 2 class name	YANG node name
Identity	user-name
Role	group
AccessRule	rule

The NETCONF server enforces the access control rules.

User authentication is not handled by NACM, but by other processes depending on how the user connects, for example over TLS.

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2023--10	SA5#151	S5-236671	-	-	-	Initial skeleton	0.0.0
2024-02	SA5#153	S5-240861 S5-240862 S5-240863				1. Draft TS 28.319 on Access control of Management services 2. Rel-18 pCR TS28.319 OpenAPI for REST Solution for Access control for management service 3. Rel-18 pCR TS28.319 on concept of NETCONF Solution for Access control for management service	0.1.0
2024-03	SA#103	SP-240265				Draft after editHelp's review and presented for information and approval	1.0.0
2024-03	SA#103					Upgrade to change control version	18.0.0
2024-06	SA#104	SP-240808	0003	-	F	TS28.319 Rel18 Moving normative stage 3 to Forge	18.1.0
2025-03	SA#107	SP-250175	0005	1	F	Rel-18 CR TS 28.319 Move MSAC requirements from TS 28.540	18.2.0

History

Document history		
V18.0.0	May 2024	Publication
V18.1.0	July 2024	Publication
V18.2.0	March 2025	Publication