

INTERNATIONAL STANDARD

ISO/IEC
10164-9

First edition
1995-12-15

Information technology — Open Systems Interconnection — Systems Management: Objects and attributes for access control

*Technologies de l'information — Interconnexion de systèmes ouverts
(OSI) — Gestion de systèmes: Objets et attributs pour le contrôle d'accès*



Reference number
ISO/IEC 10164-9:1995(E)



Documents

Document Sharing Hub

Contents

	<i>Page</i>
1 Scope	1
2 Normative references	2
2.1 Identical Recommendations International Standards	2
2.2 Paired Recommendations International Standards equivalent in technical content	2
3 Definitions	3
3.1 Basic reference model definitions	4
3.2 Security architecture definitions	4
3.3 Management framework definitions	4
3.4 Security frameworks overview definitions	4
3.5 Access control framework definitions	4
3.6 Systems management overview definitions	5
3.7 Management information model definitions	5
3.8 Implementation conformance statement proforma definitions	5
3.9 Event report management definitions	5
3.10 OSI conformance testing definitions	5
3.11 Additional definitions	6
4 Symbols and abbreviations	6
5 Conventions	6
6 Requirements	6
7 Interpretation of the Access Control Model	7
7.1 Overview	7
7.2 Access control policies	8
7.3 Access control information	8
7.4 Access control procedures	9
7.5 Representation of access control rules	13
8 Generic definitions	14
8.1 Managed objects	14
8.2 Parameters	23
8.3 Name bindings	23
8.4 Attributes	23
8.5 Imported generic definitions	24
8.6 Compliance	24
9 Service definition	24
9.1 Introduction	24
9.2 Access control management service	24
9.3 Targets administration service	25
9.4 Initiators administration service	25
9.5 Operations administration service	25
9.6 Label administration service	26
9.7 Access control notification service	26

© ISO/IEC 1995

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

	<i>Page</i>
10 Functional units	26
11 Protocol	26
11.1 Elements of procedure	26
11.2 Abstract syntax	26
11.3 Negotiation of access control functional unit.....	27
12 Relationship with other functions	27
13 Conformance	29
13.1 Static conformance.....	29
13.2 Dynamic conformance	29
13.3 Management information conformance requirements	30
Annex A – Definition of management information.....	31
Annex B – MCS proforma	49
Annex C – MICS proforma	57
Annex D – MOCS proforma	61
Annex E – MRCS proforma for name binding.....	102
Annex F – MIDS (Parameter) proforma.....	104
Annex G – CMIP Access Control Parameter	105
Annex H – Relationship to ITU-T Rec. X.812 ISO/IEC 10181-3: Security Frameworks in Open Systems – Access Control	106

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 10164-9 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.741.

ISO/IEC 10164 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — Systems Management*:

- *Part 1: Object management function*
- *Part 2: State management function*
- *Part 3: Attributes for representing relationships*
- *Part 4: Alarm reporting function*
- *Part 5: Event report management function*
- *Part 6: Log control function*
- *Part 7: Security alarm reporting function*
- *Part 8: Security audit trail function*
- *Part 9: Objects and attributes for access control*
- *Part 10: Accounting metering function*
- *Part 11: Metric objects and attributes*
- *Part 12: Test management function*
- *Part 13: Summarization function*
- *Part 14: Confidence and diagnostic test categories*
- *Part 15: Scheduling function*
- *Part 16: Management knowledge management function*
- *Part 17: Change over function*
- *Part 18: Software management function*
- *Part 19: Management domain and Management policy management function*

Annexes A to F form an integral part of this part of ISO/IEC 10164. Annexes G and H are for information only.

Introduction

This Recommendation | International Standard specifies an Access Control Security Model and the management information necessary for creating and administering access control associated with OSI Systems Management. Security policy adopted for any instance of use is not specified and is left as an implementation choice. This Specification is of generic application and is applicable to the security management of many types of application. It is expected to be adopted for TMN use.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.
- ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework*.
- CCITT Recommendation X.701 (1992)¹⁾ | ISO/IEC 10040:1992¹⁾, *Information technology – Open Systems Interconnection – Systems management overview*.
- CCITT Recommendation X.720 (1992) | ISO/IEC 10165-1:1993, *Information technology – Open Systems Interconnection – Structure of management information: Management information model*.
- CCITT Recommendation X.721 (1992) | ISO/IEC 10165-2:1992, *Information technology – Open Systems Interconnection – Structure of management information: Definition of management information*.
- CCITT Recommendation X.722 (1992) | ISO/IEC 10165-4:1992, *Information technology – Open Systems Interconnection – Structure of management information: Guidelines for the definition of managed objects*.
- ITU-T Recommendation X.724 (1993) | ISO/IEC 10165-6:1994, *Information technology – Open Systems Interconnection – Structure of management information: Requirements and guidelines for implementation conformance statement proformas associated with OSI management*.
- CCITT Recommendation X.730 (1992) | ISO/IEC 10164-1:1993, *Information technology – Open Systems Interconnection – Systems management: Object management function*.
- CCITT Recommendation X.731 (1992) | ISO/IEC 10164-2:1993, *Information technology – Open Systems Interconnection – Systems management: State management function*.
- CCITT Recommendation X.732 (1992) | ISO/IEC 10164-3:1993, *Information technology – Open Systems Interconnection – Systems management: Attributes for representing relationships*.
- CCITT Recommendation X.734 (1992) | ISO/IEC 10164-5:1993, *Information technology – Open Systems Interconnection – Systems management: Event report management function*.
- CCITT Recommendation X.736 (1992) | ISO/IEC 10164-7:1992, *Information technology – Open Systems Interconnection – Systems management: Security alarm reporting function*.
- CCITT Recommendation X.740 (1992) | ISO/IEC 10164-8:1993, *Information technology – Open Systems Interconnection – Systems management: Security audit trail function*.
- ITU-T Recommendation X.810²⁾ | ISO/IEC 10181-1...²⁾, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security frameworks overview*.
- ITU-T Recommendation X.812²⁾ | ISO/IEC 10181-3...²⁾, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.208 (1988), *Specification of Abstract Syntax Notation One (ASN.1)*.
ISO/IEC 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)*.

¹⁾ As amended by ITU-T Rec. X.701/Cor.2 | ISO/IEC 10040/Cor.2.

²⁾ Presently at the stage of draft.

- CCITT Recommendation X.209 (1988), *Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.
ISO/IEC 8825:1990, *Information technology – Open systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.
- CCITT Recommendation X.217 (1992), *Service definition for the Association Control Service Element*.
ISO 8649:1988³⁾, *Information processing systems – Open Systems Interconnection – Service definition for the Association Control Service Element*.
- CCITT Recommendation X.227 (1992), *Connection-oriented protocol specification for the Association Control Service Element*.
ISO 8650:1988⁴⁾, *Information processing systems – Open Systems Interconnection – Protocol specification for the Association Control Service Element*.
- CCITT Recommendation X.290 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – General concepts*.
ISO/IEC 9646-1:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 1: General concepts*.
- CCITT Recommendation X.291 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – Abstract test suite specification*.
- ISO/IEC 9646-2:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract Test Suite specification*.
- ITU-T Recommendation X.296⁵⁾, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Implementation conformance statements*.
ISO/IEC 9646-7:1995, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 7: Implementation conformance statements*.
- CCITT Recommendation X.700 (1992), *Management framework for Open Systems Interconnection for CCITT applications*.
ISO/IEC 7498-4:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework*.
- CCITT Recommendation X.710 (1991), *Common management information service definition for CCITT applications*.
ISO/IEC 9595:1991, *Information technology – Open Systems Interconnection – Common management information service definition*.
- CCITT Recommendation X.711 (1991), *Common management information protocol specification for CCITT applications*.
ISO/IEC 9596-1:1991, *Information technology – Open Systems Interconnection – Common management information protocol – Part 1: Specification*.
- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security architecture*.

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

³⁾ As amended by ISO/IEC 8649:1988/Amd.1:1990.

⁴⁾ As amended by ISO/IEC 8650:1988/Amd.1:1990.

⁵⁾ Presently at the stage of draft

3.1 Basic reference model definitions

This Recommendation | International Standard makes use of the following term defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

- open system.

3.2 Security architecture definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.800 | ISO 7498-2:

- a) access control;
- b) access control list;
- c) authentication;
- d) capability;
- e) security label;
- f) security policy.

3.3 Management framework definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.700 | ISO/IEC 7498-4:

- a) managed object;
- b) systems management application entity.

3.4 Security frameworks overview definitions

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.810 | ISO/IEC 10181-1:

- a) security certificate;
- b) security domain;
- c) security token.

3.5 Access control framework definitions

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.812 | ISO/IEC 10181-3:

- a) access control certificate;
- b) Access Control Decision Information (ADI);
- c) Access Control Decision Function (ADF);
- d) Access Control Enforcement Function (AEF);
- e) Access Control Information (ACI);
- f) access control policy;
- g) contextual information;
- h) initiator;
- i) Initiator Access Control Decision Information (initiator ADI);
- j) Initiator Access Control Information (initiator ACI);
- k) Initiator-bound Access Control Information (initiator-bound ACI);
- l) Operand Access Control Decision Information (operand ACI);
- m) Operand-bound Access Control Information (operand-bound ACI);

- n) retained ADI;
- o) target;
- p) Target Access Control Decision Information (target ADI);
- q) Target Access Control Information (target ACI);
- r) Target-Bound Access Control Information (target-bound ACI).

3.6 Systems management overview definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.701 | ISO/IEC 10040:

- a) generic definitions;
- b) managed object class;
- c) Managed Object Conformance Statement (MOCS);
- d) Management Information Conformance Statement (MICS);
- e) management operation;
- f) MICS proforma;
- g) MOCS proforma;
- h) notification.

3.7 Management information model definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.720 | ISO/IEC 10165-1:

- a) action;
- b) characteristic.

3.8 Implementation conformance statement proforma definitions

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.724 | ISO/IEC 10165-6:

- a) Managed Relationship Conformance Statement (MRCS);
- b) Management Conformance Summary (MCS);
- c) Management Information Definition Statement (MIDS) proforma;
- d) MCS proforma;
- e) MRCS proforma.

3.9 Event report management definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.734 | ISO/IEC 10164-5:

- event forwarding discriminator.

3.10 OSI conformance testing definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.290 | ISO/IEC 9646-1:

- a) PICS proforma;
- b) protocol implementation conformance statement;
- c) system conformance statement.

3.11 Additional definitions

3.11.1 security domain authority: An entity responsible for the implementation of a security policy.

3.11.2 operation type: The effective action on a managed object as a result of a management request.

4 Symbols and abbreviations

ACC	Access Control Certificate
ADI	Access Control Decision Information
ACI	Access Control Information
ACL	Access Control List
ADF	Access Control Decision Function
AEF	Access Control Enforcement Function
CMIS	Common Management Information Service
CMIP	Common Management Information Protocol
ICS	Implementation Conformance Statement
MAPDU	Management Application Protocol Data Unit
MCS	Management Information Conformance Statement
MICS	Management Information Conformance Statement
MIDS	Management Information Definition Statement
MOCS	Managed Object Conformance Statement
MRCS	Managed Relationship Conformance Statement
PAC	Privilege Attribute Certificate
PICS	Protocol Implementation Conformance Statement
SMAE	Systems Management Application Entity

5 Conventions

This Recommendation | International Standard makes use of the notational techniques for defining managed objects and attributes specified in CCITT Rec. X.722 | ISO/IEC 10165-4.

6 Requirements

An OSI Management user requires that unauthorized access to management applications and management information be prevented by the use of one or more access control mechanisms.

Control of access to management information is required in each of the following cases:

- a) to protect management information from unauthorized creation, deletion, modification or disclosure by means of OSI Management operations;
- b) to ensure that initiators are only able to use the management operations for which access rights were granted during application association establishment; and
- c) to prevent management information from being transmitted to unauthorized recipients by means of confirmed or non-confirmed event reports.

NOTE – For completeness there is also a requirement for the control of access to associations. This subject is for further study.

Various levels of access control may be required. For example, some users may be given read and write access to specific attributes, whilst others may have only read access or no access. Some users may be granted rights to access only specific managed objects whilst other users may have access to a different set of managed objects. For management operations, access restrictions need to cater for managed objects, individual attributes of managed objects, values of individual attributes, context of the access and actions associated with the managed object.

There is a requirement for the provision of an access control parameter that may be used in management exchanges which use CMIS.

There is a requirement for open systems which support access control for management applications which use OSI management services and protocols to be observed to exhibit the same access control behaviour when imposing the same set of access control rules.

It is required that the use of access control mechanisms not identified in this Recommendation | International Standard shall not be prevented by the provisions contained herein.

In order that the management of access control information be achieved using OSI systems management, it is required that:

- the information be modelled as managed objects so that it may be created, deleted, modified and read;
- it be possible to determine which targets may be accessed by an initiator; and
- it be possible to determine which initiators may have access to a target.

It is required that the discovery of which managed objects are contained within a management information sub-tree by use of a scoped get may be prevented.

It is required that the general application of a scoped management operation (such as delete) may be prevented.

It is required that unique security labels may be assigned to specific targets.

7 Interpretation of the Access Control Model

7.1 Overview

Access control for OSI management is based on the model for access control defined in ITU-T Rec. X.812 | ISO/IEC 10181-3. In the base model, the access control decision and enforcement functions are interposed between the initiator and the target. This Recommendation | International Standard illustrates how that model applies to the provision of access control for applications that use OSI Management services and protocols.

The access control decision function requires information, generically termed Access Control Information (ACI), for use in the decision making process. Access control information may be modelled as management information and documented using the notational techniques specified in CCITT Rec. X.722 | ISO/IEC 10165-4. This Recommendation | International Standard defines some access control information as attributes of managed object classes, so that OSI systems management may be used to exchange that information between open systems.

NOTE – This Recommendation | International Standard does not specify the actual form or structure of any access control information that is temporarily or permanently stored in an open system. It does specify the abstract syntax of those elements of access control information that may be exchanged between open systems using OSI systems management.

All access control schemes identified in ITU-T Rec. X.812 | ISO/IEC 10181-3 – ACL schemes, capability schemes, context based schemes and label based schemes – are applicable to the provision of access control for applications that use OSI Management services and protocols. Access control schemes may be used singly or in combination in order that access control may be supported in accordance with an access control policy appropriate to the security domain.

Access control is controlled by an access control policy. Where a specific access control policy is imposed on a group of elements, the combination of elements plus access control policy are encompassed by a specific security domain. Within a security domain a single access control policy is enforced at any instant of time.

Authentication of the OSI Management user and the peer authentication of SMAEs are outside the scope of this Recommendation | International Standard. However, the access control procedures defined herein require the use of authentication procedures at the appropriate time. Possible authentication procedures are described in CCITT Rec. X.217 | ISO 8649, CCITT Rec. X.227 | ISO 8650 and ITU-T Rec. X.509 | ISO/IEC 9594-8.

Access control for OSI Management is specified as a collection of denials and permissions to perform management operations. The user of the management application that invokes the management operation is the initiator, and the elements of management information, for example managed objects and attributes, identified by the parameters of the management operation combine to form the target(s).

Access control of event reports is effected by applying access control to management operations upon event forwarding discriminators.

7.2 Access control policies

An access control policy incorporates one or more sets of rules. It is the responsibility of the access control policy implementor to ensure that the access control rules accurately represent an instantiation of the access control policy.

An access control policy is a specific management policy that may be the subject of management policy administration.

NOTE – This Recommendation | International Standard does not specify the management of management policies and in particular does not specify any means to check the integrity of access control information.

An access control policy is enforced by the use of one or more access control schemes. Access control schemes include:

- ACL schemes;
- Capability schemes;
- Context based schemes; and
- Label based schemes.

If some characteristics of a managed object (for instance attributes) are under the jurisdiction of different security policies, then the managed object may be in multiple security domains. When multiple access control policies apply to a managed object, the enforced access control policy is one that is associated with both the initiator and the target.

7.3 Access control information

Access control information includes:

- access control rules;
- the identity of the initiator of the access request (Initiator ACI);
- capabilities and security clearances associated with the initiator (Initiator ACI);
- information pertaining to the authentication of the initiator (Retained ADI);
- the management information identities (targets) to which access has been requested (Target ACI);
- capabilities and security clearances associated with the target (Target ACI);
- the permitted operations that may be performed on the management information (Initiator ACI, Target ACI);
- information retained by the access control decision function for subsequent use (Retained ADI); and
- contextual information.

7.3.1 access control rules: The access control information that represents the permitted operations and the conditions upon their execution in a security domain. There are five classifications of access, control rule which are to be applied by the access decision function:

- **Global deny rules:** Access control rules that deny access to all targets. If a global rule denies access, then no other rule shall apply. If a global rule does not deny access, then the item deny rules are imposed.
- **Item deny rules:** Access control rules that deny access to particular targets. If an item deny rule denies access, then no other rule shall apply. If an item deny rule does not deny access, then the global grant rules are applied.
- **Global grant rules:** Access control rules that grant access to all targets. If a global rule grants access, then no other rule shall apply. If a global rule does not grant access, then the item grant rules are imposed.
- **Item grant rules:** Access control rules that grant access to particular targets. If an item grant rule grants access, then no other rule shall apply. If an item grant rule does not grant access, then the default rules are applied.
- **Default rules:** The access control rules to be applied when no other rule has specifically granted or denied access. The default rules shall grant or deny access.

7.3.2 action-bound ACI: The access control information (such as a security label) that is associated with the management information carried in management operations and event reports. Action-bound ACI may also be used to create and/or modify access control information associated with a target.

7.3.3 initiator-bound ACI: The access control information provided by, or otherwise associated with, the initiator of a management request. This information may be:

- the identity of the initiator of the management operation;
- information conveyed in the access control parameter of management operations (e.g. CMIS access control parameter, CMIP user information access control parameter);
- information assigned by a security domain authority; or
- a combination of the above.

The access control parameter conveyed by CMIS may take the form of security certificate or a security token.

NOTE – The identity of the initiator may be passed from authentication mechanisms using local procedures outside the scope of this Recommendation | International Standard.

7.3.4 target-bound ACI: The access control information that identifies the management information on which operations are to be performed.

7.3.5 contextual information: The access control information associated with context (for example, time of day, authentication level, location, resource limitation, participation in a relationship).

7.3.6 ADI: Action ADI, Initiator ADI, and Target ADI are derived from Action-bound ACI, Initiator-bound ACI and Target-bound ACI respectively, for the decision purpose.

7.3.7 retained ADI: The access control information that is retained by the access control decision function. According to the access control policy, some of this information may be retained for periods of time longer than that of the life of an association. Retained ADI may be used by the ADF to evaluate access privileges.

7.4 Access control procedures

Access control rules specify the security criteria that have to be met in order to allow management information to be accessed. The rules may mandate that some or all of the following procedures be performed:

- validation of initiator-bound ACI;
- identification of the target;
- determination of the access decision;
- modification of retained ADI;
- modification of target-bound ACI; and
- enforcement of the decision.

Prior to the establishment of an association, access control information that represents access control rules for that access control domain may be generated and distributed by a security domain authority using mechanisms outside the scope of this Recommendation | International Standard.

The procedures which follow specify which access decisions have to be made, not where they are to be made. This Recommendation | International Standard does not specify whether the decisions are to be made in the managing system, managed system, both systems or elsewhere.

It is the responsibility of the initiator to provide access control information that is compatible with the access control mechanisms specified by the security policy.

The use of some or all of these procedures does not exclude the use of other procedures and other access control mechanisms, not specified by this Recommendation | International Standard.

7.4.1 Validation of initiator-bound ACI

Initiator-bound ACI may be supplied in the access control parameter of the CMIS service request for the management operation. The information may take the form of a security certificate, for example an Access Control Certificate (ACC), or a security token.

The security policy specifies which of the following shall be performed:

- the integrity of the information shall be validated using procedures outside the scope of this Recommendation | International Standard;
- the validity of the information shall be verified by checking that the origin of the information was a recognized security domain authority;

- the content of the information shall be verified by checking that the value of the information was within a permitted range.

7.4.2 Identification of the target

A target is an element of information that is to be protected by an access control scheme. Management information is contained in the management information tree. A sub-tree may be selected using the CMIS scope parameter. Where this is the case, then the entire selected sub-tree is considered a target. The selection may be further refined by use of the CMIS scope and filter parameters which select individual managed objects and their characteristics from the management information tree. In this case all the selected managed objects and their characteristics are the target. At the finest granularity it is possible to select individual managed objects from the management information tree. In this case, only the selected managed object and its characteristics are the target.

Any given management operation request identifies one or more targets. These targets are identified as follows:

- a) When the scope parameter is present in the request, the entire management sub-tree encompassed by the request is a target. That is, the combination of base managed object class, base managed object instance, scope, synchronization, operation type, attribute id, action id, attributeInfoArg value, actionInfoArg value parameters forms a target;
- b) When the scope and filter parameters are present in the request, the selected managed objects and characteristics of those managed objects is a target. That is, each distinct base managed object class, base managed object instance, attributeValue, operation type, attribute id, action id, attributeInfoArg value, actionInfoArg value) combination formed from
 - the managed objects selected by the base managed object class, base managed object instance and scope parameters; and
 - the filter item elements of the filter parameter
 forms a target; or
- c) Each distinct managed object and its characteristics selected by the operation form a target. That is, base managed object class, managed object class, base managed object instance, managed object instance, superior managed object instance, reference managed object instance, initial value managed object instance, operation type, attribute id, action id, attributeInfoArg value, actionInfoArg value combination for each managed object selected by the managed object selection parameters is a target.

NOTE – A target includes the operation(s) that is (are) requested for the managed object.

7.4.3 Determination of the access decision

The access control decision function shall perform all of the procedures specified by the security policy. Initiator ADI, Retained ADI, Target ADI, Operand ADI, and contextual information may be used during the procedures. The security policy may include some, or all, of the procedures in 7.4.3.1.

7.4.3.1 Access decision procedures

The procedure identified in 7.4.3.1.1 shall be applied first.

7.4.3.1.1 Identify the management information access rules that apply to the security domain of the initiator and the target.

7.4.3.1.2 For all global rules that deny access by initiators, perform the applicable tests in 7.4.3.2. If any test returns success, indicate to the access control enforcement function that the management operation request shall be denied and apply the procedures in 7.4.6, otherwise apply procedure in 7.4.3.1.3.

7.4.3.1.3 For all item rules that deny access to targets, perform the applicable tests in 7.4.3.2. If any test returns success, indicate to the access control enforcement function that the management operation request shall be denied and apply the procedures in 7.4.6, otherwise apply procedure in 7.4.3.1.4.

7.4.3.1.4 For all global rules that grant access by initiators, perform the applicable tests in 7.4.3.2. If any test returns success, indicate to the access control enforcement function that the management operation request shall be granted and apply the procedures in 7.4.4, 7.4.5 and 7.4.6, otherwise apply procedure in 7.4.3.1.5.

7.4.3.1.5 For all item rules that grant access to targets, perform the applicable tests in 7.4.3.2. If any test returns success, indicate to the access control enforcement function that the management operation request shall be granted and apply the procedures in 7.4.4, 7.4.5 and 7.4.6, otherwise apply procedure in 7.4.3.1.6.

7.4.3.1.6 If the policy has not specified any rule that specifically grants or denies access to the target, indicate to the access control enforcement function that the management operation request shall be granted or denied according to the default rule for that operation, and the default denial response shall apply. If the management operation request is to be denied, only the procedures in 7.4.6 apply otherwise apply the procedures in 7.4.4, 7.4.5 and 7.4.6.

7.4.3.2 Access decision tests

The following tests are available to the access decision function, in accordance with the security policy. Each test receives information associated with the initiator and a rule identifying operations on targets. Each test returns a boolean, the value of which is the truth or falsehood of the proposition that “the initiator satisfies the rule”.

Evaluating a requested operation on a specific target managed object may require information about a superior, reference or initial values managed object class or instance that will be disclosed to the initiator. If the initiator does not have access (GET permission) to the required information about the superior, reference or initial values managed object class or instance as determined appropriately by a) to e) below, then the rule shall evaluate to FALSE:

- a) When required by an ACL scheme, the identity, group or role of the initiator shall be compared with the identities of initiators that are associated with the rule. If an identical match is found and if the operation and target associated with the request are compatible with the operations and targets specified by the rule, then the rule shall evaluate to TRUE. If an identical match is not found or either the operation or target associated with the request is incompatible with the operations and targets specified by the rule, then the rule shall evaluate to FALSE.
- b) When required by a capability scheme, the identity associated with the initiator shall be compared with a list of initiator identities associated with the rule. If an identical match is found that allows the capability to be used and the operation and target identified in the request are compatible with those specified in the capability, then the rule shall evaluate to TRUE. If an identical match is not found or either the operation or target identified in the request is incompatible with those specified in the capability, then the rule shall evaluate to FALSE.
- c) When required by a context based scheme, the contextual conditions associated with the rule shall be checked. If all of the contextual conditions are satisfied, then the rule shall evaluate to TRUE, otherwise the rule shall evaluate to FALSE.
- d) When required by a label based scheme, the label associated with the initiator shall be validated against the label associated with the target. If the label associated with the initiator is determined by the label algorithm to be compatible with the label associated with the target, then the rule shall evaluate to TRUE, otherwise the rule shall evaluate to FALSE.
- e) When required by the security policy, perform any other test associated with the rule.

When evaluating the access control rules in a security domain which uses a combination of access control mechanisms, a single rule shall satisfy all the mechanisms associated with that rule.

NOTE – Some security policies may apply combinations of the access control schemes to the rule. In this case, the access control policy shall identify the precedence of the schemes.

7.4.4 Modification of retained ADI

If specified by the security policy, the ADI retained by the access control decision function may be modified using the initiator ACI that was supplied with the management operation request. Relevant information includes:

- ACI that is permanently associated with the initiator;
- ADI retained from previous associations;
- ACI supplied by the initiator;
- ACI obtained as a result of the authentication procedure; and
- contextual information.

NOTE – Mechanisms for managing, obtaining, storing, and retrieving retained ADI are outside the scope of this Recommendation | International Standard.

7.4.5 Modification of target ADI

If specified by the security policy, the ADI associated with the target may be modified using the Action ADI that was supplied with the management operation request according to the following procedures.

7.4.5.1 For the create operation, Action ADI may be used to create Target ADI specific to the newly created managed object. ADI associated with other targets may not be modified.

7.4.5.2 For the delete operation, Action ADI may be used to modify or remove Target ADI specific to the deleted managed object(s). ADI associated with other targets may not be modified.

7.4.5.3 For the replace attribute value, replace with default value, add member, and remove member operations, Action ADI may be used to modify Target ADI specific to the target attribute(s) being modified by the operation. ADI associated with other targets need not be modified.

NOTE – Independent of the management operations identified above, target ADI may be modified. ADI associated with targets may be created, deleted and modified by means outside the scope of this Recommendation | International Standard. For example, the creation of a managed object which represents a resource may also create target ADI as a direct consequence of the creation of the managed object. If management of ACI using OSI Systems Management is permitted, then target ADI may be modified according to clause 8.

7.4.6 Enforcement of the decision

The access control enforcement function shall be responsible for enforcing the policy decision indicated by the access control decision function.

The following subclauses describe:

- a) the meanings of the possible access denial responses that may be returned to the initiator as a result of action by the access control enforcement function;
- b) the procedure to be taken by the access control enforcement function as a result of a management operation request being received with invalid initiator-bound ACI;
- c) the procedure to be taken by the access control enforcement function as a result of a management operation being denied as a result of a global rule denying access;
- d) the procedure to be taken by the access control enforcement function as a result of a management operation being denied as a result of an item rule denying access or as a result of the default rule denying access; and
- e) the requirements for the recording and reporting of events significant to the support of an access control scheme.

7.4.6.1 Enforcement of access denial

Enforcement of access denied requires specification of the appropriate denial response to return to the initiator, and the specification of the specific targets to which access is denied.

One of the following denial response actions shall be specified:

- a denial response is given, the access control enforcement function shall ensure that the access denied error response is returned to the initiator if the management operation service was requested in the confirmed mode;
- no response is given, the access control enforcement function shall ensure that no response is returned to the initiator;
- the association is aborted, the access control enforcement function shall ensure that the ACSE A-ABORT procedure is invoked; or
- a false response is given, the access control enforcement function shall ensure that incorrect management information is returned to the initiator if the management operation service was requested in the confirmed mode.

If no denial response action is specified, the default denial response action is a matter of local policy.

The denial response shall have an associated denial granularity. The possible denial granularities include:

- A single denial at the level of the total management request. Denial of access to any element of management information will result in the total request being denied. No management operations on targets associated with the request shall be performed.
- A denial at the level of each managed object referenced in the request. Denial of access to any operations and attributes of that managed object will result in denial of access to that managed object, but not to other managed objects associated with the request. No management operations on targets associated with the managed object to which access is denied shall be performed.
- A denial at the level of each attribute within individual managed objects referenced by the request. A denial of access to a specific attribute within a managed object will result in access to that attribute being denied, but not to other attributes within the containing managed object, or attributes within other managed objects. No management operations on the specific attributes for which access is denied shall be performed.

If no denial granularity is specified, the default denial granularity is a matter of local policy.

NOTES

- 1 A default denial granularity at the level of the total request is recommended to satisfy the principle of least privilege.
- 2 A default enforcement action of no response or abort association is recommended to satisfy the principle of least privilege.

7.4.6.2 Denial as a result of invalid initiator-bound ACI

If the decision is to deny the request as a result of invalid initiator-bound ACI, then:

- no operation shall be performed on any of the targets specified in the request;
- the specified or default denial enforcement action shall be invoked, with the exception that a specified denial enforcement action of a false response be changed to abort the association;
- the specified granularity of the denial response, if any, shall be ignored, and the response given at the granularity of the total request.

7.4.6.3 Denial as a result of a global rule being satisfied

If the decision is to deny the management operation as a result of global rule, then:

- no operation shall be performed on any of the targets specified in the request;
- the specified or default denial enforcement action shall be invoked;
- the specified granularity of the denial response, if any, shall be ignored, and the response given at the granularity of the total request.

7.4.6.4 Denial as a result of an item rule or a default rule being satisfied

If the decision is to deny the management operation upon the identified target as a result of an item or default rule, then:

- if the target encompasses a sub-tree of the management information tree, i.e. the target was selected by a) of 7.4.2, then no operation shall be performed on any managed objects held within the selected sub-tree;
- if the target is a selection of managed objects [from b) of 7.4.2], then no operation shall be performed on those managed objects identified by the target;
- if the target is one of those identified in accordance with c) of 7.4.2, then no operation shall be performed on that target;
- the specified or default denial enforcement action shall be invoked;
- the granularity of the response shall be at the specified denial granularity, if is specified, or at the default denial granularity.

NOTES

- 1 In the case of multiple object selection, CMIS does not define a response suitable for use at the managed object level of denial. That is, a denial response shall be given for each attribute selected.
- 2 In the case of denial due to access being denied to an attribute in the filter, CMIS provides no means to indicate that the filter attribute is the cause. Therefore, if the target is one of those defined by b) of 7.4.2, and a denial response is called for at the managed object level, then the response need not provide an indication of the attribute that caused the denial.

7.4.6.5 Requirements for recording events significant to access control

If the security policy mandates that requests for management operations be recorded, the access control enforcement function shall ensure that the appropriate notification is generated as follows:

- if the access request is denied, the notification shall be a security alarm report; or
- if the access request is granted, the notification shall be a security audit trail report.

7.5 Representation of access control rules

An access control rule is a mapping from the combination of (initiator, target) pairs to the access permission (grant or deny).

The space of initiators comprises every possible user of managing applications. This space is divisible according to security policy (e.g. ACL schemes, capability schemes, label based schemes). There may be as many ways of dividing this space as there are security policies.

Groups of initiators may be represented by managed objects. The identification of initiators is dependent on the security policy.

The space of targets comprises every conceivable (management operation, argument) value pair. There are many ways of dividing this space:

- by operation;
- by managed object;
- by managed object class;
- by attribute;
- by action;
- by attribute/argument value;
- by scope parameter; and
- by synchronization parameter.

The finest granularity that may be achieved is managed object class, managed object instance, operation, action id, action value, attribute id, attribute value. Where multiple object selection is permitted, access control may be imposed on the managed object class, managed object instance, scope and synchronization combinations. Where scoping and filtering is permitted, access control may be imposed on the managed object class, managed object instance, attribute identifier and attribute value combination for each managed object within the scope.

Groups of targets may be represented by managed objects.

Access control is enforced within the context of a security domain. There are five hierarchies of access control rules within each domain:

- rules which deny specific initiators access to any of the targets in the domain;
- rules which deny specific initiators access to specific targets in the domain;
- rules which grant specific initiators access to all of the targets in the domain;
- rules which grant specific initiators access to specific targets in the domain; and
- rules which grant or deny access in the absence of any other rule which grants or denies access.

8 Generic definitions

The access control information and procedures described in clause 7 may be modelled as managed objects. Figure 1 depicts the inheritance hierarchy for the managed object classes defined in this Recommendation | International Standard.

Figure 2 shows the relationships between some of the managed objects identified in Figure 1.

NOTE – Not all the managed objects shown in Figure 1 are shown in Figure 2. The managed objects not included in Figure 2 (the access control managed object class and the assigned labels and derived managed object classes) are omitted for clarity.

8.1 Managed objects

8.1.1 Access control

This managed object class comprises the management information elements and behaviour which are common to all managed objects representing access control information. It is specified only to provide a single point of specialization for other managed object classes representing access control information.

8.1.1.1 Attributes of access control

The following mandatory attribute is defined for the access control managed object class.

8.1.1.1.1 Access control object name

This attribute is used to identify instantiations of specializations of the access control managed object class.

8.1.1.2 Notifications of access control

The following notifications are defined for the access control managed object class:

- attribute value change;
- object creation; and
- object deletion.

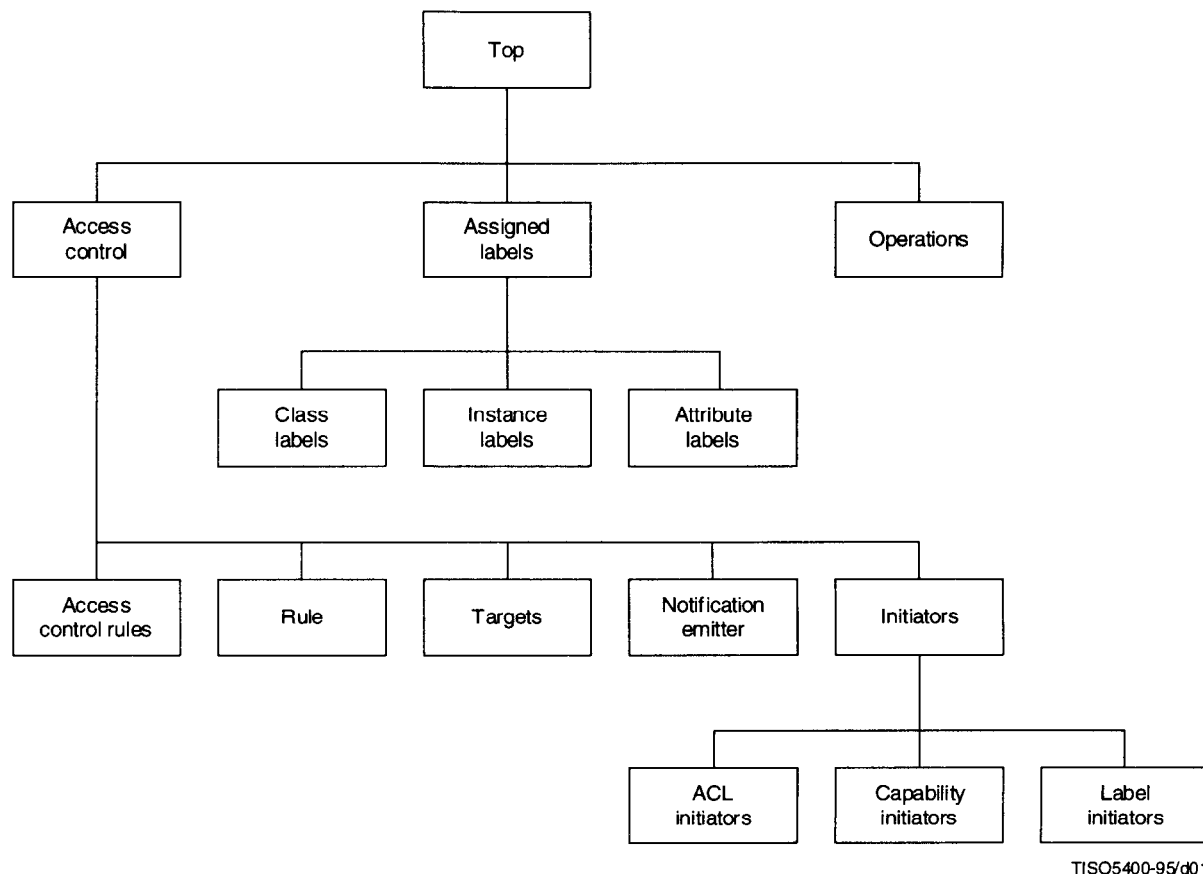


Figure 1 – Managed object class inheritance hierarchy

8.1.2 Access control rules

Access control rules managed objects represent the access control decision function for a security domain. Their attributes and contained rules managed objects identify the access control rules for the security domain. The access control rules managed object class is a sub-class of the access control managed object class.

The access control rules managed object contains the other managed objects that represent access control rules for the access control decision function.

8.1.2.1 Attributes of access control rules

The following mandatory attributes are defined for the access control rules managed object class.

8.1.2.1.1 Default access

The default access attribute identifies, in accordance with 7.4.3.1.6, the default access rights for each operation type.

8.1.2.1.2 Default denial response

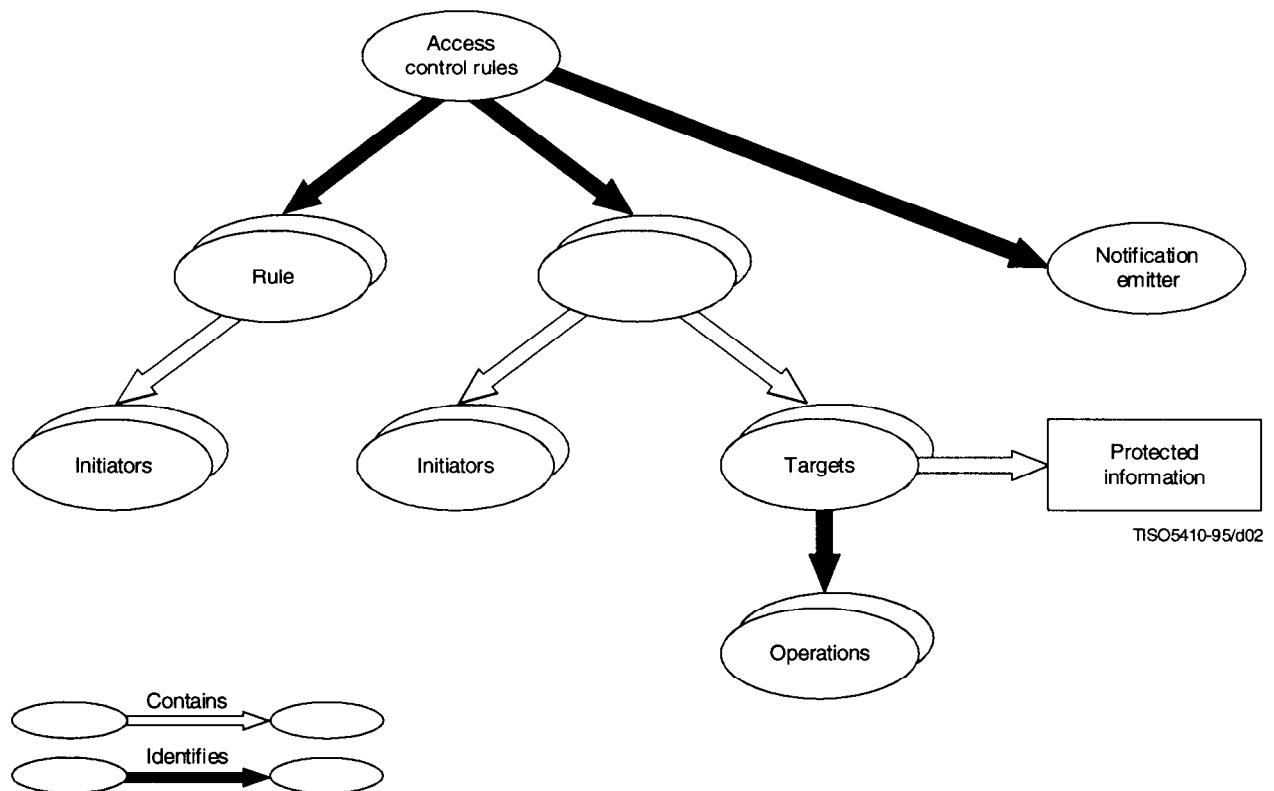
The default denial response attribute identifies the default response returned to the initiator in the event that the ADF has denied access to the target on the basis of the default rule.

8.1.2.1.3 Domain identity

This attribute identifies the access control domain governing these access control rules.

8.1.2.1.4 Denial granularity

This attribute identifies the level at which denial of access shall be exhibited, if at all.



TISO5410-95/d02

Figure 2 – Relationship between managed objects

8.1.3 Rule

The rule managed object class represents global and item rules. The rule managed object class is a sub-class of the access control managed object class.

8.1.3.1 Attributes of rule

The following mandatory attributes are defined for the rule managed object class.

8.1.3.1.1 Enforcement action

This attribute identifies the action to be taken by the access control enforcement function if the rule is satisfied.

8.1.3.1.2 Initiators list

This set-valued attribute identifies the sub-classes of initiators managed objects which specify the initiators to which the rule pertains.

8.1.3.1.3 Targets list

This set-valued attribute identifies the targets managed objects which themselves specify the targets to which the item rule pertains.

8.1.3.2 Scheduling packages

To accommodate various levels of complexity in scheduling rule activity periods, conditional packages that are related to scheduling are defined for the rule.

Scheduling packages enable rules managed objects to transit automatically between “in force” and “not in force” conditions, signalled by the availability status attribute taking the value {} and {offDuty} respectively.

8.1.3.2.1 Availability status package

This package shall be present if any of the other scheduling related packages are present. If this package is not present, then the rule managed object shall always be available.

8.1.3.2.2 Duration package

The duration package provides the ability to control automatically the times at which a managed object starts and stops functioning. This package shall be present if such functionality is required. If this package and one of the other scheduling packages are co-resident then the availability status shall take the value {offDuty} unless both packages signal activity, in which case the availability status shall be {}.

8.1.3.2.3 Daily scheduling package

The daily scheduling package provides the ability to schedule operation with a period of 24 hours. It shall be present if such functionality is required. It shall not be co-resident with either the weekly or external scheduler scheduling package.

8.1.3.2.4 Weekly scheduling package

The weekly scheduling package provides the ability to schedule operation with a period of one week. It shall be present if such functionality is required. It shall not be co-resident with either the daily or external scheduler scheduling package.

8.1.3.2.5 External scheduler scheduling package

The external scheduler scheduling package provides the capability of scheduling operation using a schedule defined in another managed object. It shall be present if such functionality is required. It shall not be co-resident with either the daily or weekly scheduling package.

8.1.3.3 State conditions package

The state conditions package enables a rule to operate within the context of the state of identified managed objects. It shall be present if such functionality is required.

8.1.3.3.1 Attributes of the state conditions package

The following mandatory attribute is defined for the state conditions package.

8.1.3.3.1.1 State conditions

This set-valued attribute identifies managed objects and associated filters upon the attributes of those managed objects.

8.1.3.4 Authentication context package

When present in a rule managed object the authentication context package specifies the authentication policy identity and authentication requirements that an initiator is required to satisfy.

8.1.3.4.1 Attributes of the authentication context package

The following mandatory attribute is defined for the authentication context package.

8.1.3.4.1.1 Authentication context

The authentication context attribute is a sequence of authentication policy identifier and the requirements identified thereby.

8.1.4 Notification emitter

This managed object class is used to enable notifications to be emitted that are applicable to the provision of access control for OSI management. The types of notification that are applicable include certain security alarms as defined in CCITT Rec. X.736 | ISO/IEC 10164-7, and certain security audit trail notifications as defined in CCITT Rec. X.740 | ISO/IEC 10164-8.

A single notification emitter managed object may be contained within an access control rules managed object.

8.1.4.1 Packages of notification emitter

This managed object class supports the following conditional packages to provide a flexible ability to transmit access control related notifications:

- security violation alarm package;
- time violation alarm package;
- operational violation alarm package;
- access control usage package; and
- access control service report package.

8.1.4.1.1 Security violation alarm package

This package enables a security alarm notification of type 'Security service or mechanism violation' and cause 'unauthorized access attempt' to be emitted if access control checks should fail.

8.1.4.1.2 Time violation alarm package

This package enables a security alarm notification of type 'Time domain violation' and causes 'Key expired' and 'out of hours activity' to be emitted if access control checks should fail. The cause 'key expired' shall be used when the key identified by the access control certificate seal is out of date. The 'out of hours activity' cause shall be used when contextual time checks fail.

8.1.4.1.3 Operational violation alarm package

This package enables a security alarm notification of type 'operational violation' and causes 'out of service' and 'unspecified reason' to be emitted if access control checks should fail. The cause 'out of service' shall be used when the access control mechanism identified is not available. The 'unspecified reason' cause shall be used in other cases.

8.1.4.1.4 Access control usage package

This package is used to count the number of valid and invalid access attempts and to enable usage reports containing this information to be sent to a security audit trail log. The usage report is sent at a time interval defined by the security policy. The additional information field is used to convey the counter values.

8.1.4.1.4.1 Attributes of the access control usage package

The following attributes are defined for the access control usage package.

8.1.4.1.4.1.1 Valid access attempts

This attribute is used to count the number of occasions that an access control decision function has authorized an access.

8.1.4.1.4.1.2 Invalid access attempts

This attribute is used to count the number of occasions that an access control decision function has not authorized an access.

8.1.4.1.5 Access control service report package

This package allows security audit trail notifications of type 'service report' to be emitted for possible inclusion in a security audit trail log.

8.1.5 Targets

A targets managed object identifies a collection of management information that is to be subject to access control. The targets managed object class is a sub-class of the access control managed object class.

8.1.5.1 Attributes of targets

The following mandatory attributes are defined for targets managed objects.

8.1.5.1.1 Managed object classes

This set-valued attribute identifies protected managed object classes and optional associated name bindings.

8.1.5.1.2 Managed object instances

This set-valued attribute identifies protected managed objects.

8.1.5.1.3 Scope

The scope attribute identifies a scope for the selection of protected managed objects.

8.1.5.1.4 Filter

This attribute identifies a filter to be applied to managed objects identified by the other attributes of the targets managed object to determine their inclusion as a protected managed object.

8.1.5.2 Operations list package

This package provides support for the operations type attribute as an alternative to the operations managed object. It may only be included in the targets managed object if it contains no instantiation of the operations managed object.

8.1.5.2.1 Attributes of the operations list package

The following mandatory attribute is defined for the operations type package.

8.1.5.2.1.1 Operations list

This set-valued attribute identifies the operation types that are subject to the rules identifying the targets managed object containing these operations.

8.1.6 Operations

The operations managed object identifies constraints on operation types for managed objects identified by the containing targets managed object.

Operation types are the operations defined in CCITT Rec. X.720 | ISO/IEC 10165-1, including:

- action;
- create;
- delete;
- get;
- replace;
- add member;
- remove member;
- replace with default;
- filter, and;
- multiple object selection.

There shall be only one operations managed object for a specific operations type contained within a targets managed object.

The operation type is used as the value of the naming attribute for the operations managed object class.

Conditional packages provide attributes to specify constraints upon the attributes and actions associated with the operation type. In addition, attributes are provided in conditional packages for the purpose of placing constraints on the value of the scope and synchronization parameter values that are allowed in an access request involving multiple object selection.

NOTE – It may be required to apply different constraints on the same operation type, or sub-operations for the same operation type, for the same managed object(s). For example, this requirement may exist when different constraints shall be applied to different specific actions for the same managed object(s). In such cases, a new targets managed object shall be created that contains the managed object to which the constraint applies, and which contains an operations managed object that specifies the new constraints to be applied for the operation type.

8.1.6.1 Attributes of operations

The following mandatory attribute is defined for the operations managed object class.

8.1.6.1.1 Operation type

This attribute identifies the operation type to which constraints apply, and is used for naming operations managed objects.

8.1.6.2 Notifications of operations

The following mandatory notifications are defined for the operations managed object class:

- a) object creation;
- b) object deletion;
- c) attribute value change.

8.1.6.3 Packages of operations

This managed object class supports the following conditional packages:

- attribute ids package;
- attribute modification package;
- actions package; and
- scope package.

8.1.6.3.1 Attribute ids package

The attribute ids package identifies attributes to which access is to be controlled. It shall be present if the operation type is get, replace, add value, remove value, replace with default, or filter and not present if the operation is any other type.

8.1.6.3.1.1 Attributes of the attribute ids package

The attribute identifier list attribute as specified in CCITT Rec. X.721 | ISO/IEC 10165-2 is included in this package.

8.1.6.3.2 Attribute modification package

The attribute modification package identifies constraints upon the modification of attribute values. It shall be present if the operation type is replace, add value, remove value, or create and not present if the operation is any other type.

8.1.6.3.2.1 Attributes of the attribute modification package

The attribute filter list attribute is included in this package.

8.1.6.3.2.1.1 Attribute filter list

This set-valued attribute identifies constraints upon the value of attributes in an operation request by means of a set of CMIS filters (one CMIS filter for each attribute for which constraints are specified).

8.1.6.3.3 Actions package

The actions package identifies constraints upon the values of action information. It shall be present if the operation type is action and not present if the operation is any other type.

8.1.6.3.3.1 Attributes of the actions package

The action filter list attribute is included in this package.

8.1.6.3.3.1.1 Action filter list

This set-valued attribute identifies actions and, optionally, constraints upon their argument values by means of a CMIS filter.

8.1.6.3.4 Scope package

The scope package identifies constraints upon the scope and synchronization parameters of management operations involving multiple object selection. It shall be present if the operation type is multiple object selection and not present if the operation is any other type.

NOTE – The scope package may be used, for example:

- to prevent discovery of, or access to, managed objects during a scoped get of an entire sub-tree – such as may be used to explore a system in an unauthorized manner;
- to protect given managed objects from deletion as part of a sub-tree, such that the managed object may be deleted by a certain initiator only if directly addressed, never as part of a scoped delete.

8.1.6.3.4.1 Attributes of the scope package

The following attributes are defined for the scope package.

8.1.6.3.4.1.1 Scope filter

For requests that select multiple managed objects the scope filter specifies constraints on the scope parameter of the request, and the scope attribute (see 8.1.5.1.3) identifier is used for all the filter items in the filter.

If the scope filter contains no filter items, then all possible values of the scope parameter shall be regarded as targets.

8.1.6.3.4.1.2 Synchronization filter

For requests that select multiple managed objects the synchronization filter specifies constraints on the synchronization parameter of the request and the synchronization attribute (see 8.4.2) identifier is used for all the filter items in the filter. If the synchronization filter contains no filter items, then all possible values of the synchronization parameter shall be regarded as targets.

8.1.7 Initiators

The Initiators managed object class identifies the permissible initiators of management operations.

8.1.7.1 Attributes of initiators

The following mandatory attribute is defined for the initiators managed object class.

8.1.7.1.1 Initiator ACI mandated

The attribute is used to indicate whether, to satisfy the access control scheme in use, initiator ACI is required with each individual management operation request.

8.1.8 ACL initiators

The ACL initiators managed object class contains a list of names or other identities that together form an access control list.

Multiple ACL initiators managed objects may be instantiated within a rule managed object.

8.1.8.1 Attributes of ACL initiators

The following mandatory attribute is defined for the ACL initiators managed object class.

8.1.8.1.1 Access control list

The access control list attribute is used to contain identities of initiators that are either specifically granted access to management information or specifically denied access to management information.

8.1.9 Capability initiators

The capability initiators managed object class contains a list of identities.

Multiple capability initiators managed objects may be instantiated within a rule managed object.

8.1.9.1 Attributes of capability initiators

The following mandatory attribute is defined for the capability initiators managed object class.

8.1.9.1.1 Capability identities list

The capability identities list attribute contains a set of identities.

The identities may be an individual name, group name, role name, or application name, each of which may be associated with an optional set of security domain authority name and operation type pairs; or, the identity may be of a form not specified within this Recommendation | International Standard.

8.1.10 Label initiators

The label initiators managed object may be used to specify constraints on management operations that are in addition to the constraints of requiring a compatibility match between the security label associated with the initiator and the security label associated with the target.

If a label initiators managed object is present within a rule managed object, the constraints defined by the rule managed object and by the targets managed objects contained within the same rule shall be in addition to the security label compatibility matching requirements of the label access control scheme.

If a label initiators managed object is not present within a rules managed object, then no additional constraints are imposed on the access beyond the security label compatibility matching requirements of the label access control scheme.

Multiple label initiators managed objects may be instantiated within a rule managed object.

8.1.10.1 Attributes of label initiators

The following mandatory attribute is defined for the label initiators managed object class.

8.1.10.1.1 Security label

The security label attribute contains a security label.

8.1.11 Assigned labels

This managed object is the root of the sub-tree that contains the label type managed objects which, in combination with precedence relationships, assign a single security label to targets. In addition to providing a container managed object for the different label type managed objects, this managed object provides a default security label to be assigned to management elements that are not specifically assigned a security label.

8.1.11.1 Attributes of assigned labels

The following mandatory attributes are defined for the assigned labels managed object class.

8.1.11.1.1 Label name

This attribute is used to identify instantiations and specializations of the assigned labels managed object class.

8.1.11.1.2 Security label

This attribute contains the security label to be assigned to the target.

8.1.12 Attribute label

This managed object is used to associate a single security label to targets that are specific attributes within a managed object.

8.1.12.1 Attributes of attribute label

The following mandatory attributes are defined for the attribute label managed object class.

8.1.12.1.1 Managed object instance

This attribute is used to identify a specific managed object.

8.1.12.1.2 Attribute identifier list

This attribute is used to identify specific attributes of the managed object identified by the managed object instance attribute.

8.1.13 Instance label

This managed object is used to associate a single security label to targets that are individual managed objects.

8.1.13.1 Attributes of instance label

The following mandatory attribute is defined for the instance label managed object class.

8.1.13.1.1 Managed object instances

This attribute is used to identify a list of specific targets by their managed object identifier.

8.1.14 Class label

This managed object is used to associate a single security label to targets that are managed object classes.

8.1.14.1 Attributes of class label

The following mandatory attribute is defined for the class label managed object class.

8.1.14.1.1 Managed object classes

This attribute is used to identify a list of specific managed object classes.

8.2 Parameters

8.2.1 Invalid access control filter

This specific error reports an error in a proposed access control filter element. Its value shall be a sequence of an error id, taking one of the values `duplicateId`, `heterogeneousId`, or `invalidId`, and an optional CMIS Filter containing the filter in error.

8.3 Name bindings

8.3.1 Rule – Access control rule

This name binding provides for rules and specializations to be contained within access control rules and specializations. The access control object name attribute shall be used for naming the rules. Rules managed objects may be created by management operation, with automatic instance naming and with reference object. Rules managed objects may be deleted by management operation.

8.3.2 Operations – Targets

This name binding provides for operations managed objects to be contained within targets managed objects. The operation type attribute shall be used for naming the operations. Operations managed objects may be created by management operation and with reference object. Operations managed objects may be deleted by management operation.

8.3.3 Notification emitter – Access control rule

This name binding provides for a single notification emitter managed object to be contained within an access control rules managed object. The notification emitter may be created, created with reference object and deleted by management operation. It may be named automatically.

8.3.4 Attribute label – Assigned labels

This name binding provides for attribute label managed objects to be contained within assigned label managed objects. Attribute label managed objects may be created and deleted by management operation.

8.3.5 Instance label – Assigned labels

This name binding provides for instance label managed objects to be contained within assigned label managed objects. Instance label managed objects may be created and deleted by management operation.

8.3.6 Class label – Assigned labels

This name binding provides for class label managed objects to be contained within assigned label managed objects. Class label managed objects may be created and deleted by management operation.

8.4 Attributes

The following attributes are not defined for any package or managed object class but are used for specifying other attributes and for filtering.

8.4.1 Access control filter

This set-valued attribute identifies constraints upon the value of parameters of management operations. Each element is a CMIS filter, addressed to a single element of management information. Each element of management information is addressed in at most one element of this attribute. An empty set indicates that all possible values are targeted.

8.4.2 Synchronization

This attribute value represents the synchronization parameter of management operations. It is used to represent filters upon this parameter.

8.5 Imported generic definitions

This Recommendation | International Standard makes use of the following generic definitions in CCITT Rec. X.730 | ISO/IEC 10164-1, CCITT Rec. X.731 | ISO/IEC 10164-2, CCITT Rec. X.732 | ISO/IEC 10164-3, CCITT Rec. X.734 | ISO/IEC 10164-5, CCITT Rec. X.736 | ISO/IEC 10164-7, and CCITT Rec. X.740 | ISO/IEC 10164-8:

- attribute identifier list;
- attribute value change notification;
- availability status package;
- counter;
- daily scheduling package;
- discriminator construct;
- duration package;
- external scheduler scheduling package;
- member;
- managed object instance;
- object creation notification;
- object deletion notification;
- operational violation;
- security service or mechanism violation;
- service report;
- time domain violation;
- usage report; and
- weekly scheduling package.

8.6 Compliance

Managed object class definitions support the functions defined in this Recommendation | International Standard by incorporating the specification of managed objects, attributes and notifications defined in this Recommendation | International Standard, in CCITT Rec. X.721 | ISO/IEC 10165-2, in CCITT Rec. X.736 | ISO/IEC 10164-7 and in CCITT Rec. X.740 | ISO/IEC 10164-8. The reference mechanism is defined in CCITT Rec. X.722 | ISO/IEC 10165-4.

9 Service definition

9.1 Introduction

Access control may be applied to management information. The access control applied may change with time or with changes to the access control policy. It is therefore necessary to provide a mechanism for administering the access control service.

9.2 Access control management service

This service provides for the administration of the access control rules utilized by a system.

The service enables managed objects from the following classes to be administered:

- access control rules; and
- rules.

9.2.1 Initiating access control rules

The PT-CREATE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system create instances of the managed object classes listed in 9.2.

9.2.2 Modifying access control rules

The PT-SET service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system change the attribute values of attributes of the managed object classes listed in 9.2.

9.2.3 Terminating access control rules

The PT-DELETE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system delete instances of the managed object classes listed in 9.2.

9.3 Targets administration service

This service is used to administer the targets managed objects that identify the management information protected by access control.

9.3.1 Initiating access control targets

The PT-CREATE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system create instances of the targets managed object class.

9.3.2 Modifying access control targets

The PT-SET service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system change the attribute values of attributes of the targets managed object class.

9.3.3 Terminating access control targets

The PT-DELETE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system delete instances of the targets managed object class.

9.4 Initiators administration service

This service is used to administer sub-classes of the initiators managed objects.

9.4.1 Initiating access control initiators

The PT-CREATE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system create instances of sub-classes of the initiators managed object class.

9.4.2 Modifying access control initiators

The PT-SET service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system change the attribute values of attributes of sub-classes of the initiators managed object class.

9.4.3 Terminating access control initiators

The PT-DELETE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system delete sub-classes of instances of the initiators managed object class.

9.5 Operations administration service

This service is used to administer the operations managed objects.

9.5.1 Initiating access control operations

The PT-CREATE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system create instances of the operations managed object class.

9.5.2 Modifying access control operations

The PT-SET service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system change the attribute values of attributes of the operations managed object class.

9.5.3 Terminating access control operations

The PT-DELETE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system delete instances of the operations managed object class.

9.6 Label administration service

This service is used to administer assigned labels, attribute label, instance label and class label managed objects.

9.6.1 Initiating label control operations

The PT-CREATE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system create instances of the assigned labels, attribute label, instance label and class label managed object classes.

9.6.2 Modifying access control operations

The PT-SET service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system change the attribute values of attributes of the assigned labels, attribute label, instance label and class label managed object classes.

9.6.3 Terminating access control operations

The PT-DELETE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to enable one open system to request that another system delete instances of the assigned labels, attribute label, instance label and object label managed object classes.

9.7 Access control notification service

This service enables reports of events relevant to the monitoring and administration of an access control service to be transmitted from one open system to another. The security alarm reporting function specified in CCITT Rec. X.736 | ISO/IEC 10164-7 is used to forward alarm reports and security audit trail records related to attempts to access management information illegally, whilst the security audit trail function specified in CCITT Rec. X.740 | ISO/IEC 10164-8 is used to forward reports related to the general use of the access control service.

10 Functional units

The objects and attributes for access control function constitutes a single systems management functional unit.

11 Protocol

11.1 Elements of procedure

This Recommendation | International Standard makes use of the elements of procedure defined in CCITT Rec. X.730 | ISO/IEC 10164-1, CCITT Rec. X.736 | ISO/IEC 10164-7, and CCITT Rec. X.740 | ISO/IEC 10164-8 for the services described in clause 9. There are no elements of procedure specific to this Recommendation | International Standard.

11.2 Abstract syntax

11.2.1 Managed objects

Table 1 identifies the relationship between access control managed objects and managed objects, whose abstract syntax is specified in Annex A.

11.2.2 Attributes

Table 2 identifies the relationship between access control attributes and management attributes whose abstract syntax is specified in Annex A.

11.2.3 Attribute groups

There are no attribute groups defined by this systems management function.

11.2.4 Actions

There are no actions defined by this systems management function.

11.2.5 Notifications

There are no notifications defined by this systems management function.

Table 1 – Managed objects

Managed object	Managed object class
Access control	accessControl
Access control rules	accessControlRules
ACL initiators	aclInitiators
Assigned labels	assignedLabels
Attribute label	attributeLabel
Capability initiators	capabilityInitiators
Class label	classLabel
Instance label	instanceLabel
Label initiators	labelInitiators
Notification emitter	notificationEmitter
Operations	operations
Rule	rule
Targets	targets

11.2.6 Parameters

Table 3 identifies the relationship between access control parameters and management parameters whose abstract syntax is specified in Annex A.

11.3 Negotiation of access control functional unit

This Specification assigns the object identifier

{ joint-iso-ccitt ms(9) function(2) part(9) functionalUnitPackage(1) }

as a value of the ASN.1 type **FunctionalUnitPackageId** defined in CCITT Rec. X.701 | ISO/IEC 10040 to use for negotiating the following functional unit:

0 access control functional unit

where the number identifies the bit position assigned to the functional unit, and the name references the functional unit as defined in clause 10.

Within the systems management application context, the mechanism for negotiating the access control functional unit is described by CCITT Rec. X.701 | ISO/IEC 10040.

NOTE – The requirement to negotiate functional units is specified by the application context.

12 Relationship with other functions

The object creation and object deletion notifications defined in CCITT Rec. X.730 | ISO/IEC 10164-1 are used to report the creation and deletion respectively, of instances of the managed object classes defined in this Recommendation | International Standard.

Table 2 – Management attributes

Access control attribute	Attribute name
Access control filter	accessControlFilter
Access control object name	accessControlObjectName
Action filter list	actionFilterList
Attribute filter list	attributeFilterList
Authentication context	authenticationContext
Capability identities list	capabilityIdentitiesList
Default access	defaultAccess
Default denial response	defaultDenialResponse
Denial granularity	denialGranularity
Domain identity	domainIdentity
Enforcement action	enforcementAction
Filter	filter
Initiator ACI mandated	initiatorACImandated
Initiators list	initiatorsList
Invalid access attempts	invalidAccessAttempts
Label name	labelName
Managed object classes	managedObjectClasses
Managed object instances	managedObjectInstances
Operation type	operationType
Operations list	operationsList
Scope	scope
Scope filter	scopeFilter
Security label	securityLabel
State conditions	stateConditions
Synchronization	synchronization
Synchronization filter	synchronizationFilter
Targets list	targetsList
Valid access attempts	validAccessAttempts

Table 3 – Management Parameters

Access Control Parameter	Parameter Name
Invalid access control filter	invalidAccessControlFilter

The attribute value change notification defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to report changes in attribute values in instances of the managed objects defined in this Recommendation | International Standard.

The operational violation, security service or mechanism violation, and time domain violation notifications defined in CCITT Rec. X.736 | ISO/IEC 10164-7 are used to report security alarms associated with the operation of the access control mechanisms.

The service report and service usage notifications defined in CCITT Rec. X.740 | ISO/IEC 10164-8 are used to convey security audit trail reports associated with the use of access control services and mechanisms.

The management of access control information may make use of the following systems management services defined in CCITT Rec. X.730 | ISO/IEC 10164-1:

- PT-CREATE;
- PT-DELETE;
- PT-SET; and
- PT-GET.

The security policy may stipulate that these services be used over a secure association so that the ACI is protected from unwanted disclosure or modification.

13 Conformance

Implementations claiming to conform to this Recommendation | International Standard shall comply with the conformance requirements as defined in the following subclauses.

13.1 Static conformance

The implementation shall conform to the requirements of this Recommendation | International Standard in the manager role, the agent role, or both roles. A claim of conformance to at least one role shall be made in Table B.1.

If a claim of conformance is made for support in the manager role, the implementation shall support at least one management operation or notification of at least one of the managed objects specified by this Recommendation | International Standard. The conformance requirements in the manager role for those management operations are identified in Table B.3 and further tables referenced by Annex B.

If a claim of conformance is made for support in the agent role, the implementation shall support one or more instances of the access control rules managed object class identified in Table B.4.

The system shall support the transfer syntax derived from the encoding rules specified in CCITT Rec. X.209 | ISO/IEC 8825 named {joint-iso-ccitt asn1(1) basic encoding(1)} for the abstract data types referenced by the definitions for which support is claimed.

13.2 Dynamic conformance

Implementations claiming to conform to this Recommendation | International Standard shall support the elements of procedure and definitions of semantics corresponding to the definitions for which support is claimed.

13.3 Management information conformance requirements

Any MCS proforma, MICS proforma, MOCS proforma, MRCS proforma and MIDS proforma which conforms to this Recommendation | International Standard shall be technically identical to the proformas specified in Annexes B, C, D, E and F preserving table numbering and the index number of items, and differing only in pagination and page headers.

The supplier of an implementation which is claimed to conform to this Recommendation | International Standard shall complete a copy of the Management Conformance Summary (MCS) provided in Annex B as part of the conformance requirements, together with any other ICS proformas referenced as applicable from that MCS. An ICS which conforms to this Recommendation | International Standard shall:

- describe an implementation which conforms to this Recommendation | International Standard;
- have been completed in accordance with the instructions for completion given in ITU-T Rec. X.724 | ISO/IEC 10165-6;
- include the information necessary to uniquely identify both the supplier and the implementation.

Claims of conformance to the management information defined in this Recommendation | International Standard in managed object classes defined elsewhere shall include the requirements of the MIDS proforma in the MOCS proforma for the managed object class.