INTERNATIONAL STANDARD

ISO/IEC 10164-9

First edition
1995-12-15

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

iTeh STANDARD PREVIEW

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

(standards.iteh.ai)

ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

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

Contents

		Page
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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/6ff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

© 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

		Page
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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

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 integrai part of this part of ISO/IEC 10164. Annexes G and H are for information only.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

This page intentionally left blank

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

This page intentionally left blank

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SYSTEMS MANAGEMENT: OBJECTS AND ATTRIBUTES FOR ACCESS CONTROL

1 Scope

The specifications contained herein are applicable to the provision of access control for applications that use OSI management services and protocols.

This Recommendation | International Standard

- establishes user requirements for the provision of access control for applications that use OSI management services and protocols;
- interprets and applies the general model of access control defined in ITU-T Rec. X.812 | ISO/IEC 10181-3 for use with management applications that use OSI management services and protocols;
- defines procedures for the imposition of access control rules in conjunction with the use of OSI management services and protocols;
- defines managed object classes and attribute types that
  a) represent some of the access control information that may be used in the provision of access control; and
  b) are only for use when the management of the access control information is to be achieved using systems management;
- specifies the protocol that is necessary to exchange the access control information defined in this Recommendation | International Standard, when the exchange is achieved using OSI systems management;
- specifies conformance requirements for open systems that claim to support access control for applications that use OSI management services and protocols;
- specifies conformance requirements for open systems that claim to support the management of the access control information defined in this Recommendation | International Standard.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/b8f4f2b6-6e9d-4475-9b23-ed74e1035e9f/iso-iec-10164-9-1995

The access control information identified by this Recommendation | International Standard may be used in support of access control schemes based on access control lists, capabilities, security labels, and contextual constraints.

This Recommendation | International Standard does not

- define an access control policy for applications that use OSI management services and protocols;
- define security (or management) domains in which an access control policy may be imposed;
- define how the components of an access control function be implemented, nor where those components be located;
- specify the form of any access control information that is temporarily or permanently stored in an open system;
- specify any access control mechanisms, nor mandate the use of any particular access control mechanism;
- mandate that access control information be managed, and if it is to be managed, that management be achieved using OSI systems management;
- describe how communicating management application entities act to make access control decisions on behalf of, or for the benefit of any third party;
- specify any conformance requirement for the access control parameter defined in this Recommendation | International Standard.

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 10040:1992[1], *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.810[2] | ISO/IEC 10181-1...[2], *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security frameworks overview.*
- ITU-T Recommendation X.812[2] | ISO/IEC 10181-3...[2], *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10164-9:1995

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 8649:1988[3], *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 8650:1988[4], *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.296[5], *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.*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bf4f2b6-6c9d-4475-9b25-ed74e11035c9/iso-iec-10164-9-1995

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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:

ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

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

iTeh STANDARD PREVIEW

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

(standards.iteh.ai)

a) action;

b) characteristic.

ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/IEC 10164-9:1995
https://standards.iteh.ai/catalog/standards/sist/ed74e110-35c9-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/bff4f2b6-6c9d-4475-9b23-ed74e11035c9/iso-iec-10164-9-1995

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.