INTERNATIONAL STANDARD

ISO/IEC 10164-19

First edition
1998-12-15

Information technology — Open Systems Interconnection — Systems Management: Management domain and management policy management function

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Gestion systèmes: Fonction de gestion de police de gestion et de domaine de gestion

Contents

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 10164-19:1998 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 33, *Distributed application services,* in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.749.

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: Usage metering function for accounting purposes*

— *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*

— *Part 20: Time management function*

— *Part 21: Command sequencer*

— *Part 22: Response time monitoring function*

Annexes A to E form an integral part of this part of ISO/IEC 10164.

iTeh STANDARD PREVIEW

(standards.iteh.ai)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SYSTEMS MANAGEMENT: MANAGEMENT DOMAIN AND MANAGEMENT POLICY MANAGEMENT FUNCTION

1 Scope

This Recommendation | International Standard defines the management domain and management policy management function. This Management Function is a System Management function which may be used by an application process in a centralized or decentralized management environment to interact for the purpose of systems management, as defined by the OSI Management Framework, CCITT Rec. X.700 and ISO/IEC 7498-4. This Recommendation | International Standard defines a function which consists of generic definitions and services. This function is positioned in the application layer of the OSI reference model (ITU-T Rec. X.200 | ISO/IEC 7498-1) and is defined according to the model provided by ISO/IEC 9545. The role of systems management functions is described by CCITT Rec. X.701 | ISO/IEC 10040.

This Recommendation | International Standard:

– identifies the set of requirements satisfied by the function;

– provides a model for the behaviour of the management domain management objects;

– provides a model for the behaviour of the management policy management objects;

– specifies the management requirements of the function and how these are realized by specification of managed objects and their behaviour;

– specifies the mapping of these services onto the CMIS services;

– specifies the abstract syntax of the parameters of the MAPDUs that will be used to refer to managed objects and their characteristics;

– provides a model, in accordance with the Management Information Model and the General Relationship Model, for information associated with management domains, policies, and jurisdictions and for the behaviour of managed objects through which that information is accessed and manipulated;

– provides definitions of the information associated with management domains, policies, and jurisdictions, their representation and the operations which may be performed upon them in terms of managed object and management relationship templates.

This Recommendation | International Standard does not:

– define the nature of any implementation intended to provide the management domain and management policy management function;

– specify the manner in which management is to be accomplished by the user of the management domain and management policy management function;

– define the nature of any interactions which result in the use of the management domain and management policy management function;

– specify the services necessary for the establishment, normal and abnormal release of a management association;

– define the interactions which result by the simultaneous use of several management functions;

– define connection establishment or authorization requirements for the use of this function or for any associated activity;

– preclude the definition of further management domain, management policy, or management jurisdiction managed object classes.

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.210 (1993) | ISO/IEC 10731:1994, *Information technology – Open Systems Interconnection – Basic Reference Model - Conventions for the definition of OSI services.*

– CCITT Recommendation X.701 (1992) | ISO/IEC 10040:1992, *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.*

– ITU-T Recommendation X.725 (1995) | ISO/IEC 10165-7:1996, *Information technology – Open Systems Interconnection – Structure of management information: General relationship model.*

– 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 10164-2:1992, *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.735 (1992) | ISO/IEC 10164-6:1993, *Information technology – Open Systems Interconnection – Systems Management: Log control function.*

– ITU-T Recommendation X.743[1] | ISO/IEC 10164-20[1], *Information technology – Open Systems Interconnection – Systems Management: Time management function.*

– ITU-T Recommendation X.746 (1995) | ISO/IEC 10164-15:1995, *Information technology – Open Systems Interconnection – Systems Management: Scheduling function.*

_____

[1] Presently at the stage of draft.

- 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).*

- CCITT Recommendation X.209 (1988), *Specification of basic encoding rules for Abstract Syntax Notation (ASN.1).*

  ISO/IEC 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

- ITU-T Recommendation X.290 (1995), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – General concepts.*

  ISO/IEC 9646-1:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 1: General concepts.*

- ITU-T Recommendation X.291 (1995), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T 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 (1995), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – 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 (OSI) 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.*

3   Definitions

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

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:

- systems management.

3.2   Management framework definitions

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

a) management information;

b) managed object.

2.2   Paired Recommendations | International Standards equivalent in technical content

3.3 Systems management overview definitions

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

- a) agent role;
- b) agent;
- c) generic definitions;
- d) managed system;
- e) management domain;
- f) management jurisdiction;
- g) management operation;
- h) management policy violation;
- i) management policy;
- j) manager role;
- k) manager;
- l) managing system;
- m) membership filter;
- n) Managed Object Conformance Statement (MOCS);
- o) Management Information Conformance Statement (MICS);
- p) MOCS proforma;
- q) MICS proforma;
- r) notification;
- s) systems management functional unit.

3.4 CMIS definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.710 and ISO/IEC 9595:

- a) attribute;
- b) Common Management Information Service.

3.5 OSI conformance testing definitions

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

- – system conformance statement.

3.6 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) MCS proforma;
- d) MRCS proforma.

3.7 Additional definitions

The following terms are defined in this Recommendation | International Standard:

3.7.1 domain managed object: A managed object that represents a domain for the purposes of managing the membership of that management domain.

3.7.2 **(systems management) policy managed object**: A managed object that represents a (systems management) policy for the purpose of managing the policy.

3.7.3 **violation detection**: The activity which detects policy violations.

3.7.4 **domain (membership specifier)**: A specification that, through explicit reference or predicates, serves to identify a set of managed objects for the purposes of management.

3.7.5 **jurisdiction managed object**: A managed object that represents the relationship between a policy and a domain to which it is to be applied.

3.7.6 **administrative aspect managed object**: A managed object used to represent non-procedural information relevant to the administration of domains, jurisdictions, and policies.

4 Symbols and abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

ASN.1	Abstract Syntax Notation One
AVA	Attribute Value Assertion
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMISE	Common Management Information Service Element
Cnf	Confirm
GDMO	Guidelines for the Definition of Managed Objects
GRM	General Relationship Model
ICS	Implementation Conformance Statement
Id	Identifier
Ind	Indication
MAPDU	Management Application Protocol Data Unit
MCS	Management Conformance Summary
MICS	Management Information Conformance Statement
MIS-user	Management Information Service user
MOCS	Managed Object Conformance Statement
MRCS	Managed Relationship Conformance Statement
PICS	Protocol Implementation Conformance Statement
Req	request
Rsp	response
SMAPM	Systems Management Application Protocol Machine

5 Conventions

This Recommendation | International Standard defines services for the Management domain management function following the descriptive conventions defined in ITU-T Rec. X.210 | ISO/IEC 10731.

The following notation is used in the service parameter tables:

M the parameter is mandatory;

C the parameter is conditional;

(=) the value of the parameter is identical to the corresponding parameter in the interaction described by the preceding related service primitive;

U the use of the parameter is a service-user option;

– the parameter is not present in the interaction described by the primitive concerned;

P the parameter is subject to the constraints imposed by CCITT Rec. X.710 and ISO/IEC 9595.

NOTE – The parameters which are marked "P" in service tables of this Recommendation | International Standard are mapped directly onto the corresponding parameters of the CMIS service primitive, without changing the semantics or syntax of the parameters. The remaining parameters are used to construct an MAPDU.

Throughout this Specification, GDMO and ASN.1 productions are printed using **Times New Roman** font.

6   Requirements

For logistic or other management reasons, there is a requirement to modularize management activities and groups of managed objects. The need to define groups of managed objects is associated with the concept of domains.

It may occur that there is a need to describe these activities so that they can be accessed by means of management operations. The definition of such management activities is associated with the concept of policies. A policy defines a set of management activities which apply to domains.

In the course of normal operations it may happen that the required operations or constraints on managed objects no longer match the operational requirements associated with the group (perhaps for reasons of failure or lack of integrity) however caused. It is therefore an essential management requirement that systems shall be able to recognize occasions when there are violations and to take steps to resolve them.

In response to such situations, management policies and the rules associated with them may be modified and new rules affirmed so that they might apply to new goals and to different managed objects. A minimal requirement of management is the action to be taken in the event of violation detection, this action is known as violation resolution and is for further study.

The requirements for management domain and management policy management are identified in the Systems Management Overview (see CCITT Rec. X.701 | ISO/IEC 10040). Additional functional requirements are identified below.

For management domains there are the requirements that:

– A mechanism shall be provided for managing the membership of a domain.

– There shall be mechanisms to generate a membership list for a given management domain (membership enumeration).

– It shall be possible to discover whether a given managed object is a member of a particular management domain (membership verification).

– It shall be possible to determine which management domain(s) a given managed object is a member of.

    NOTE 1 – Actually performing this discovery may require considerable time and resources.

– It shall be possible to determine which management policies apply to a management domain.

– It shall be possible to access a representation of management domains for the purpose of managing the domain.

– A member of one management domain may be a member of another management domain.

For management policies there are the requirements that:

– A mechanism shall be provided for managing the change of policies.

– It shall be possible to specify management policy violation detection and violation resolution.

    NOTE 2 – Violation resolution mechanisms to accomplish this are for further study.

7   Model

An MIS-user in the manager role (manager) interacts with a managed object via an MIS-user in the agent role (agent) over an interoperable interface.

A managed object may be subject to any number of policies; any number of policies may be of relevance to a given object.

A domain managed object is a support object which allows the specification of a set of objects of interest.

A policy managed object is a support object which represents a system management policy, encapsulating any rules and rule combination semantics used to construct that policy.

A jurisdiction managed object is a support object which represents the relationship between a policy and a domain.

An administrative aspect is a support object which represents non-procedural aspects and descriptive information for domains, policies, and jurisdictions.

7.1   Domain

A domain allows the specification of a set of objects of interest. A domain permits the management of the specification of its membership. The set of members specified by a domain is the union of its set of direct members with its set of indirect members. Membership may change as objects are created or deleted.

The intersection of the set of objects described by a domain member selection list with the set of objects described by its member selection filter is its set of direct members. The member selection list is a set whose elements name managed object instances, which may or may not actually exist. If the member selection list is the empty set, it implies that all objects are identified. The member selection filter is a single valued attribute representing a logical predicate. If its value is empty, it evaluates to true for all objects.

A domain also allows reference by name to other domains. The union of the sets of members specified by the objects identified in this manner is a domain's set of indirect members. The ability to specify membership both directly and indirectly permits convenient grouping and representation of hierarchies of domains.

The management operations supported by a membership specifier include:

–   list direct membership;

–   list membership;

–   verify membership of a given managed object instance.

Figure 1 illustrates how domain D1 describes a set which contains objects A, B, and C through direct membership. Domain D2 describes a set containing D, E, and F through direct membership. Domain D3 describes a set containing F and G through direct membership. Domain D4 has no direct members, but has A, B, C, D, E, and F as indirect members.

T0730490-97/d01
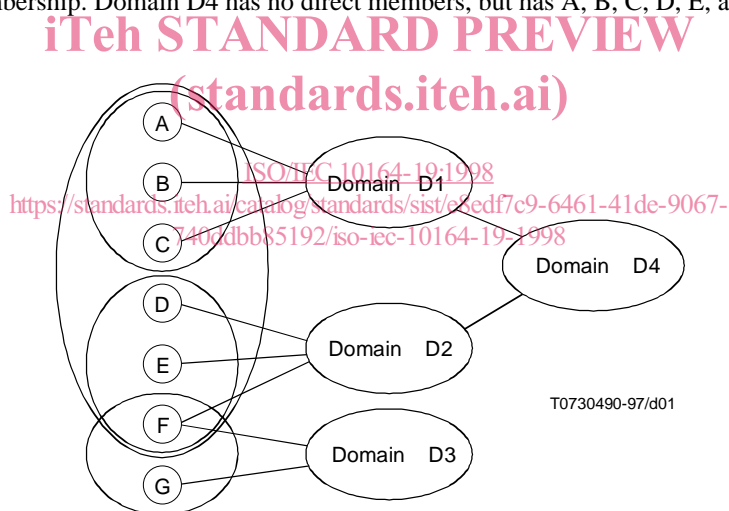
Figure 1 – Example of domain membership

7.2   Policy

A policy encapsulates a representation of system management goals. Policies reflect obligations, authorizations, and aspirations. Their representation may be transparent or opaque. A transparent policy does provide management access to the representation of its semantics. An opaque policy does not provide management access to the representation of its semantics.

This Recommendation | International Standard provides class definitions to support management of opaque policies.

Subclasses of policy may be defined to support capabilities such as scheduling, and the representation of policy semantics. This Recommendation | International Standard provides class definitions for a scheduled opaque policy.

This Recommendation | International Standard describes one means of representing policy semantics in support of a transparent policy class. The development of more powerful representations is for further study.
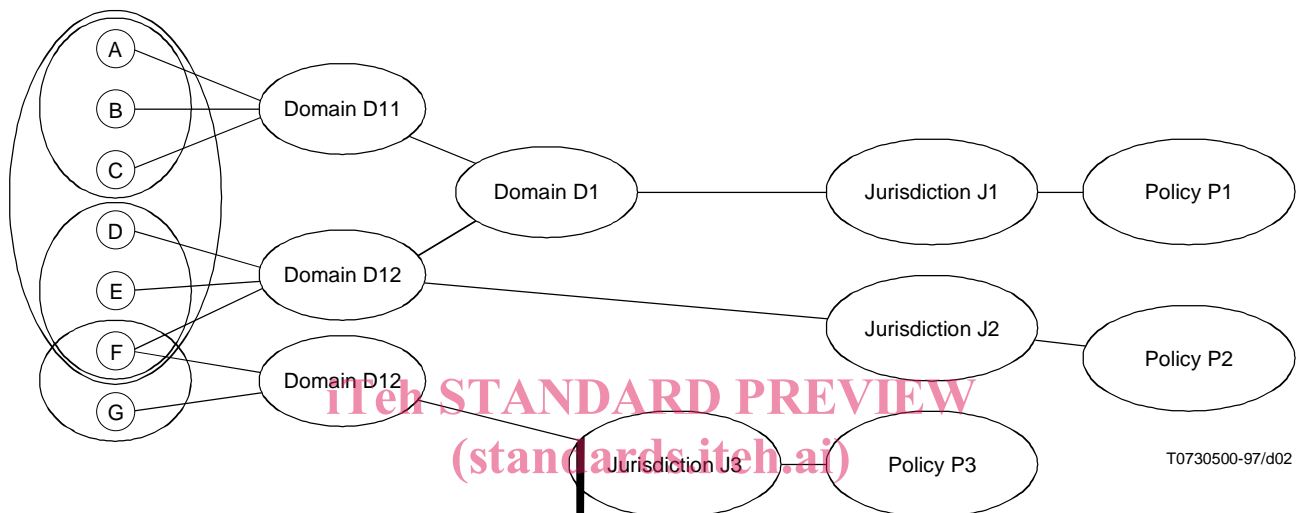
7.3   Jurisdiction

A jurisdiction managed object serves to relate a policy and a domain.

The relationship defined by a jurisdiction managed object indicates to which managed objects, identified by the domain, the policy shall apply.

Figure 2 illustrates the following concepts:

– hierarchical domains for administrative convenience (domains D11 and D12 may be administered-separately);

– re-use of a domain for multiple jurisdictions (domain D12 is used for both jurisdiction J1 and jurisdiction J2);

– application of multiple policies to a single object (Object F is subject to policies P1, P2, and P3).

T0730500-97/d02

This example shows the following:

– jurisdiction J1 associates policy P1 with domain D1;

– this means that policy P1 applies to objects A, B, C, D, E, F, the members specified directly or indirectly by D1;

– jurisdiction J2 associates policy P2 with domain D12;

– this means that policy P2 applies to objects D, E, and F, the members specified directly or indirectly by D12;

– both policy P1 and P2 are applicable to Objects D, E, and F;

– a change to domain D12 can affect the applicability of both policy P1 and P2;

– jurisdiction J3 associates policy P3 with domain D13;

– objects F and G are subject to policy P3;

– object F is also subject to policy P1 and to P2.

An enhanced jurisdiction managed object provides the ability to request the application of an operation to the members of its domain.

7.4   Administrative aspects

The administrative aspects include identification of the authority responsible for setting the domain, the authority for setting the policy and the application of policy to the domain members. An authority may be a composite entity; such an entity must be identifiable. An authority may delegate some, or all, of its responsibilities to another authority.

Administrative aspects include non-procedural aspects for recording relevant descriptive information for objects.

The following subclauses demonstrate that this function's requirements are satisfied by this model.

7.5.1   Managing membership

A jurisdiction's membership is defined to be the membership of the domain referenced by that jurisdiction.

Membership is managed by means of domains. A domain's membership may be changed in two ways:

  a)   a managed object's membership status may change, through its creation, deletion, or a change in a value of one or more of its attributes;

  b)   attributes of the domain (or a domain to which it refers, at any level of indirection) may be modified.

7.5.2   Listing membership

The listing of a jurisdiction's membership is requested by directing a list membership request to the jurisdiction. The result obtained is effectively the same as would be obtained by directing a list membership request to that jurisdiction's domain.

7.5.3   Verifying membership

The verification of jurisdiction membership for an object is requested by directing a membership verification request to the jurisdiction. The result obtained is effectively the same as would be obtained by directing a membership verification request to that jurisdiction's domain.

7.5.4   Determining which jurisdictions a managed object is a member of

Determining which jurisdictions a managed object is a member of requires performing a membership verification operation (or list membership operation) for all known jurisdictions. The discovery of jurisdictions can be performed by directing an all-levels scoped get for objects of class jurisdiction to all relevant systems.

A similar procedure may be applied against domains to determine which domains a given managed object is a member of.

7.5.5   Determining which policy applies to the members of a jurisdiction

Determining which policies apply to the membership of a domain requires retrieving the attribute which names its policy from all jurisdictions that reference the domain in question.

7.5.6   Determining whether a given object violates a policy

Determining whether a given object violates a policy is accomplished by sending a determine violation status operation to the appropriate jurisdiction or policy managed object, supplying the name of the object instance in question as a parameter. The response will be the determination of whether the policy was applicable (always true when query directed to a policy object), and, if it was, the object's violation status.

7.5.7   Applying an operation to the membership of a domain

Applying an operation to membership of a domain can be accomplished by issuing an apply operation to membership request to the appropriate jurisdiction object.

7.5.8   Determining which policies apply to a given object

In order to determine the policies applying to a managed object, it is necessary to determine the jurisdictions of which it is a member. The object in question is not required by this model to have any knowledge of the set of applied policies. The set of relevant jurisdictions can be retrieved using the procedure outlined above in 7.5.4. For each jurisdiction of which the object in question is a member, the identity of the relevant policy may be retrieved using the procedures of 7.5.5.

7.5   Procedural aspects of the model