UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.741

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(04/95)

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – GESTIÓN DE SISTEMAS: OBJETOS Y ATRIBUTOS PARA EL CONTROL DE ACCESO

Recomendación UIT-T X.741

(Anteriormente «Recomendación del CCITT»)

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. En el UIT-T, que es la entidad que establece normas mundiales (Recomendaciones) sobre las telecomunicaciones, participan unos 179 países miembros, 84 empresas de explotación de telecomunicaciones, 145 organizaciones científicas e industriales y 38 organizaciones internacionales.

Las Recomendaciones las aprueban los Miembros del UIT-T de acuerdo con el procedimiento establecido en la Resolución N.° 1 de la CMNT (Helsinki, 1993). Adicionalmente, la Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, aprueba las Recomendaciones que para ello se le sometan y establece el programa de estudios para el periodo siguiente.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI. El texto de la Recomendación UIT-T X.741 se aprobó el 10 de abril de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10164-9.

NOTA

En esta Recomendación, la expresión «Administración» se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

(Febrero de 1994)

ORGANIZACIÓN DE LAS RECOMENDACIONES DE LA SERIE X

Dominio	Recomendaciones
REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1-X.19
Interfaces	X.20-X.49
Transmisión, señalización y conmutación	X.50-X.89
Aspectos de redes	X.90-X.149
Mantenimiento	X.150-X.179
Disposiciones administrativas	X.180-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200-X.209
Definiciones de los servicios	X.210-X.219
Especificaciones de los protocolos en modo conexión	X.220-X.229
Especificaciones de los protocolos en modo sin conexión	X.230-X.239
Formularios para enunciados de conformidad de implementación de protocolo	X.240-X.259
Identificación de protocolos	X.260-X.269
Protocolos de seguridad	X.270-X.279
Objetos gestionados de capa	X.280-X.289
Pruebas de conformidad	X.290-X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300-X.349
Sistemas móviles de transmisión de datos	X.350-X.369
Gestión	X.370-X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400-X.499
DIRECTORIO	X.500-X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta uno	X.680-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Cometimiento, concurrencia y recuperación	X.850-X.859
Tratamiento de transacciones	X.860-X.879
Operaciones a distancia	X.880-X.899
TRATAMIENTO ABIERTO DISTRIBUIDO	X.900-X.999

ÍNDICE

Página

Resumen

En esta Recomendación | Norma Internacional se especifica un modelo de seguridad de control de acceso y la información de gestión necesaria para crear y administrar el control de acceso asociado con la gestión de sistemas de OSI. La política de seguridad adoptada para cualquier caso de utilización no se especifica y se deja como una opción de la realización. Esta especificación es de aplicación genérica y se puede emplear para la gestión de seguridad de muchos tipos de aplicación. Se cree que se adoptará para su utilización en la red de gestión de las telecomunicaciones.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – GESTIÓN DE SISTEMAS: OBJETOS Y ATRIBUTOS PARA EL CONTROL DE ACCESO

1 Alcance

Las especificaciones contenidas en esta Recomendación | Norma Internacional son aplicables a la provisión del control de acceso para aplicaciones que utilizan servicios y protocolos de gestión de interconexión de sistemas abiertos (OSI, *open systems interconnection*).

Esta Recomendación | Norma Internacional

- establece los requisitos de usuario relacionados con la provisión de control de acceso para aplicaciones que utilizan servicios y protocolos de gestión de OSI;
- interpreta y aplica el modelo general de control de acceso definido en la Rec. UIT-T X.812 | ISO/CEI 10181-3 para uso con aplicaciones de gestión que emplean servicios y protocolos de gestión de OSI;
- define los procedimientos para la imposición de reglas de control de acceso junto con la utilización de servicios y protocolos de gestión de OSI;
- define clases de objetos gestionados y tipos de atributos que
  a) representan alguna información de control de acceso que se puede utilizar en la provisión de control de acceso, y
  b) se aplican sólo cuando la gestión de la información del control de acceso se ha de efectuar mediante la gestión de sistemas;
- especifica el protocolo necesario para intercambiar la información de control de acceso definida en esta Recomendación | Norma Internacional, cuando el intercambio se efectúa mediante la gestión de sistemas de OSI;
- especifica los requisitos de conformidad para sistemas abiertos que alegan sustentar el control de acceso para aplicaciones que utilizan servicios y protocolos de gestión de OSI;
- especifica los requisitos de conformidad para sistemas abiertos que alegan sustentar la gestión de la información de control de acceso definida en esta Recomendación | Norma Internacional.

La información de control de acceso identificada por esta Recomendación | Norma Internacional se puede utilizar para sustentar esquemas de control de acceso basados en listas de control de acceso, capacidades, etiquetas de seguridad y constricciones contextuales.

La presente Recomendación | Norma Internacional

- no define una política de control de acceso para aplicaciones que utilizan servicios y protocolos de gestión de OSI;
- no define dominios de seguridad (o de gestión) en los cuales se puede imponer una política de control de acceso;
- no define cómo se realizan los componentes de una función de control de acceso, ni dónde estarán situados estos componentes;
- no especifica la forma de cualquier información de control de acceso que está almacenada temporal o permanentemente en un sistema abierto;
- no especifica ningún mecanismo de control de acceso, ni impone la utilización de un mecanismo de control de acceso determinado;
- no impone que la información de control de acceso sea gestionada, y si se ha de gestionar, que esa gestión se efectúe utilizando la gestión de sistemas de OSI;

- no describe cómo actúan las entidades de aplicación de gestión comunicantes para adoptar decisiones de control de acceso en nombre o en beneficio de terceros;
- no especifica ningún requisito de conformidad para el parámetro de control de acceso definido en la presente Recomendación | Norma Internacional.

2 Referencias normativas

Las siguientes Recomendaciones | Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas Internacionales son objeto de revisiones, por lo que se preconiza que las partes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y Normas enumeradas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente válidas. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

- Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico*.
- Recomendación UIT-T X.509 (1993) | ISO/CEI 9594-8:1995, *Tecnología de la información – Interconexión de sistemas abiertos – El Directorio: Marco de autenticación*.
- Recomendación X.701 del CCITT (1992)[1)] | ISO/CEI 10040:1992[1)], *Tecnología de la información – Interconexión de sistemas abiertos – Visión general de la gestión de sistemas*.
- Recomendación X.720 del CCITT (1992) | ISO/CEI 10165-1:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Estructura de la información de gestión: Modelo de información de gestión*.
- Recomendación X.721 del CCITT (1992) | ISO/CEI 10165-2:1992, *Tecnología de la información – Interconexión de sistemas abiertos – Estructura de la información de gestión: Definición de la información de gestión*.
- Recomendación X.722 del CCITT (1992) | ISO/CEI 10165-4:1992, *Tecnología de la información – Interconexión de sistemas abiertos – Estructura de la información de gestión: Directrices para la definición de objetos gestionados*.
- Recomendación UIT-T X.724 (1993) | ISO/CEI 10165-6:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Estructura de la información de gestión: Requisitos y directrices para los formularios de declaración de conformidad de realizaciones asociados con la gestión de interconexión de sistemas abiertos*.
- Recomendación X.730 del CCITT (1992) | ISO/CEI 10164-1:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de objetos*.
- Recomendación X.731 del CCITT (1992) | ISO/CEI 10164-2:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de estados*.
- Recomendación X.732 del CCITT (1992) | ISO/CEI 10164-3:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Atributos para la representación de relaciones*.
- Recomendación X.734 del CCITT (1992) | ISO/CEI 10164-5:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de informes de eventos*.
- Recomendación X.736 del CCITT (1992) | ISO/CEI 10164-7:1992, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función señaladora de alarmas de seguridad*.
- Recomendación X.740 del CCITT (1992) | ISO/CEI 10164-8:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de pista de auditoría de seguridad*.

---

1) Modificada en la Rec. UIT-T X.701/Corr.2 | ISO/CEI 10040/Corr.2.

– Recomendación UIT-T X.810[2] | ISO/CEI 10181-1 ...[2], *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión de conjunto*.

– Recomendación UIT-T X.812[2] | ISO/CEI 10181-3 ...[2], *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de control de acceso*.

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

– Recomendación X.208 del CCITT (1988), *Especificación de la notación de sintaxis abstracta uno*.

ISO/CEI 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)*.

– Recomendación X.209 del CCITT (1988), *Especificación de las reglas de codificación básica para la notación de sintaxis abstracta uno*.

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

– Recomendación X.217 del CCITT (1992), *Definición de servicio para el elemento de servicio de control de asociación*.

ISO 8649:1988[3], *Information processing systems – Open Systems Interconnection – Service definition for the Association Control Service Element*.

– Recomendación X.227 del CCITT (1992), *Especificación de protocolo con conexión para el elemento de servicio de control de asociación*.

ISO 8650:1988[4], *Information processing systems – Open Systems Interconnection – Protocol specification for the Association Control Service Element*.

– Recomendación X.290 del CCITT (1992), *Metodología y marco de las pruebas de conformidad de interconexión de sistemas abiertos de las Recomendaciones sobre los protocolos para aplicaciones del UIT-T – Conceptos generales*.

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

– Recomendación X.291 del CCITT (1992), *Metodología y marco de las pruebas de conformidad de interconexión de sistemas abiertos de las Recomendaciones sobre los protocolos para aplicaciones del CCITT – Especificación de sucesiones de pruebas abstractas*.

ISO/CEI 9646-2:1994, *Information Technology – Open Systems Interconnection – OSI Conformance testing methodology and framework – Part 2: Abstract Test Suite specification*.

– Recomendación UIT-T X.296[2], *Metodología y marco de pruebas de conformidad de interconexión de sistemas abiertos de las Recomendaciones sobre los protocolos para aplicaciones del UIT-T – Declaraciones de conformidad de realización.*

ISO/IEC 9646-7:...[2], *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 7: Implementation conformance statements*.

– Recomendación X.700 del CCITT (1992), *Marco de gestión para interconexión de sistemas abiertos para aplicaciones del CCITT*.

ISO/CEI 7498-4:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework*.

– Recomendación X.710 del CCITT (1991), *Definición del servicio común de información de gestión para aplicaciones del CCITT*.

ISO/CEI 9595:1991, *Information technology – Open Systems Interconnection – Common management information service definition*.

– Recomendación X.711 del CCITT (1991), *Especificación del protocolo común de información de gestión para aplicaciones del CCITT*.

---

[2] Actualmente en estado de proyecto.

[3] Modificada en ISO/CEI 8649:1988/Enm.1:1990.

[4] Modificada en ISO/CEI 8650:1988/Enm.1:1990.

ISO/CEI: 9596-1:1991, *Information technology – Open Systems Interconnection – Common management information protocol – Part 1: Specification*.

– Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – OSI Basic Reference Model – Part 2: Security architecture*.

3 Definiciones

A los efectos de la presente Recomendación | Norma Internacional se aplican las siguientes definiciones.

3.1 Definiciones del modelo de referencia básico

La presente Recomendación | Norma Internacional utiliza el siguiente término definido en la Rec. UIT-T X.200 | ISO/CEI 7498-1.

– sistema abierto.

3.2 Definiciones de arquitectura de seguridad

La presente Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. X.800 del CCITT | ISO 7498-2.

a) control de acceso;

b) lista de control de acceso;

c) autenticación;

d) capacidad;

e) etiqueta de seguridad;

f) política de seguridad.

3.3 Definiciones del marco de gestión

La presente Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. X.700 del CCITT | ISO 7498-4.

a) objeto gestionado;

b) entidad de aplicación de gestión de sistemas.

3.4 Definiciones de visión de conjunto del marco de seguridad

La presente Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. UIT-T X.810 | ISO/CEI 10181-1.

a) certificado de seguridad;

b) dominio de seguridad;

c) testigo de seguridad.

3.5 Definiciones del marco de control de acceso

La presente Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. UIT-T X.812 | ISO/CEI 10181-3.

a) certificado de control de acceso;

b) información de decisión de control de acceso (ADI);

c) función de decisión de control de acceso (ADF);

d) función de obligación de control de acceso (AEF);

e) información de control de acceso (ACI);

f) política de control de acceso;

g) información contextual;

h) iniciador;

i) información de decisión de control de acceso de iniciador;

j) información de control de acceso de iniciador;

k) información de control de acceso limitada a iniciador;

l) información de decisión de control de acceso de operando;

m) información de control de acceso limitada a operando;

n) información de decisión de control de acceso retenida;

o) objetivo;

p) información de decisión de control de acceso a objetivo;

q) información de control de acceso a objetivo;

r) información de control de acceso limitada a objetivo.

3.6 Definiciones de visión de conjunto de gestión de sistema

La presente Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. X.701 del CCITT | ISO/CEI 10040.

a) definiciones genéricas;

b) clase de objeto gestionado;

c) declaración de conformidad de objeto gestionado (MOCS);

d) declaración de conformidad de información de gestión (MICS);

e) operación de gestión;

f) formulario MICS;

g) formulario de MOCS;

h) notificación.

3.7 Definiciones del modelo de información de gestión

La presente Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. X.720 del CCITT | ISO/CEI 10165-1.

a) acción;

b) característica.

3.8 Definiciones de los formularios de declaración de conformidad de realización

Esta Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. UIT-T X.724 | ISO/CEI 10165-6:

a) enunciado de conformidad de relación de gestión (MRCS);

b) sumario de conformidad de gestión (MCS);

c) enunciado de definición de información de gestión (MIDS);

d) formulario de MCS;

e) formulario de MRCS.

3.9 Definiciones de gestión de informe de eventos

La presente Recomendación | Norma Internacional utiliza el siguiente término definido en la Rec. X.734 | ISO/CEI 10164-5.

– discriminador de evento hacia adelante.

3.10 Definiciones de prueba de conformidad de OSI

La presente Recomendación | Norma Internacional utiliza el siguiente término definido en la Rec. X.290 del CCITT | ISO/CEI 9646-1.

a) formulario de PICS;

b) enunciado de conformidad de implementación de protocolo;

c) declaración de conformidad de sistema.

3.11 Definiciones adicionales

3.11.1 **autoridad de dominio de seguridad**: Entidad responsable de la aplicación de una política de seguridad.

3.11.2 **tipo de operación**: Acción efectiva en un objeto gestionado como resultado de una petición de gestión.

4 Símbolos y abreviaturas

ACC Certificado de control de acceso (*access control certificate*)

ADI Información de decisión de control de acceso (*access control decision information*)

ACI Información de control de acceso (*access control information*)

ACL Lista de control de acceso (*access control list*)

ADF Función de decisión de control de acceso (*access control decision function*)

AEF Función de imposición de control de acceso (*access control enforcement function*)

CMIS Servicio común de información de control de gestión (*common management information service*)

CMIP Protocolo común de información de gestión (*common management information protocol*)

ICS Declaración de conformidad de realización (*implementation conformance statement*)

MAPDU Unidad de datos de protocolo de aplicación de gestión (*management application protocol data unit*)

MCS Sumario de conformidad de gestión (*management conformance summary*)

MICS Declaración de conformidad de información de gestión (*management information conformance statement*)

MIDS Enunciado de definición de información de gestión (*management information definition statement*)

MOCS Declaración de conformidad de objeto gestionado (*managed object conformance statement*)

MRCS Enunciado de conformidad de relación de gestión (*managed relationship conformance statement*)

PAC Certificado de atributo de privilegio (*privilege attribute certificate*)

PICS Enunciado de conformidad de implementación de protocolo (*protocol implementation conformance statement*)

SMAE Entidad de aplicación de gestión de sistemas (*systems management application entity*)

5 Convenios

La presente Recomendación | Norma Internacional utiliza las técnicas de notación para definir objetos gestionados y atributos especificadas en la Rec. X.722 del CCITT | ISO/CEI 10165-4.

6 Requisitos

Un usuario de gestión de OSI requiere que se impida el acceso no autorizado a aplicaciones de gestión e información de gestión mediante la utilización de uno o más mecanismos de control de acceso.

Se necesita control de acceso a información de gestión en cada uno de los siguientes casos:

a) para proteger la información de gestión contra la creación, supresión, modificación o revelación no autorizada por medio de operaciones de gestión de OSI;

b) asegurar que los iniciadores sólo pueden utilizar las operaciones de gestión para las cuales se les han concedido derechos de acceso durante el establecimiento de la asociación de aplicación; y

c) impedir que se transmita información de gestión a recibientes no autorizados por medio de informes de eventos confirmados o no confirmados.

NOTA – En aras de la integridad, se requiere también el control de acceso a asociaciones. Este asunto queda en estudio.

Se pueden necesitar varios niveles de control de acceso. Por ejemplo, a algunos usuarios se les puede dar acceso para lectura y escritura a atributos específicos, mientras otros sólo pueden tener acceso para lectura o ningún acceso. A algunos usuarios se les pueden conceder derechos para acceder solamente a objetos gestionados específicos, mientras que otros pueden tener acceso a un conjunto diferente de objetos gestionados. Para las operaciones de gestión, las restricciones de acceso tienen que tener en cuenta los objetos gestionados, los atributos individuales de los objetos gestionados, los valores de los atributos, el contexto del acceso y las acciones asociadas con el objeto gestionado.

Se requiere la provisión de un parámetro de control de acceso que puede ser utilizado en intercambios de gestión que emplean el CMIS.

Es necesario que los sistemas abiertos que sustentan control de acceso para aplicaciones de gestión que utilizan servicios y protocolos de gestión de OSI que se han de cumplir, presenten el mismo comportamiento de control de acceso cuando imponen el mismo conjunto de reglas de control de acceso.

Es necesario que las disposiciones contenidas en esta Recomendación | Norma Internacional no impidan la utilización de mecanismos de control de acceso no identificados en la misma.

Para efectuar la gestión de la información de control de acceso mediante la gestión de sistemas de OSI, se requiere que:

- la información esté modelada como objetos gestionados, de modo que pueda ser creada, suprimida, modificada y leída;
- sea posible determinar a qué objetivos puede tener acceso un iniciador; y
- sea posible determinar qué iniciadores pueden tener acceso a un objetivo.

Es necesario evitar, mediante una obtención delimitada, que se puedan descubrir los objetos gestionados contenidos dentro de un subárbol de información de gestión.

Es necesario que se pueda evitar la aplicación general de una operación de gestión delimitada (tal como supresión).

Es necesario que se puedan asignar etiquetas de seguridad únicas a objetivos específicos.

7 Interpretación del modelo de control de acceso

7.1 Visión de conjunto

El control de acceso para la gestión de OSI se basa en el modelo de control de acceso definido en la Rec. UIT-T X.812 | ISO/CEI 10181-3. En el modelo básico, las funciones de decisión e imposición de control de acceso se interponen entre el iniciador y el objetivo. Esta Recomendación | Norma Internacional ilustra cómo el modelo se aplica a la provisión de control de acceso para aplicaciones que utilizan servicios y protocolos de gestión de OSI.

La función de decisión de control de acceso requiere información, denominada genéricamente información de control de acceso (ACI), que se utiliza en el proceso de toma de decisión. La información de control de acceso se puede modelar como información de gestión y documentar utilizando las técnicas de notación especificadas en la Rec. X.722 del CCITT | ISO/CEI 10165-4. La presente Recomendación | Norma Internacional define cierta información de control de acceso como atributos de clases de objetos gestionados, de modo que la gestión de sistemas de OSI se pueda utilizar para intercambiar esa información entre sistemas abiertos.

NOTA – La presente Recomendación | Norma Internacional no especifica la forma o estructura real de cualquier información de control de acceso que está almacenada temporal o permanente en un sistema abierto, pero sí especifica la sintaxis abstracta de los elementos de información de control de acceso que pueden ser intercambiados entre sistemas abiertos que utilizan la gestión de sistemas de OSI.

Todos los esquemas de control de acceso identificados en la Rec. UIT-T X.812 | ISO/CEI 10181-3 – esquemas ACL, esquemas de capacidades, esquemas basados en contexto y esquemas basados en etiquetas – son aplicables a la provisión de control de acceso para aplicaciones que utilizan servicios y protocolos de gestión de OSI. Los esquemas de control de acceso se pueden utilizar solos o combinados para que el control de acceso pueda ser sustentado de acuerdo con una política de control de acceso apropiada al dominio de seguridad.

El control de acceso es controlado por una política de control de acceso. Cuando se impone una política de control de acceso específica a un grupo de elementos, la combinación de elementos más la política de control de acceso están abarcadas por un dominio de seguridad específico y dentro de un dominio de seguridad sólo se impone una política de control de acceso en cualquier momento dado.

La autenticación del usuario de la gestión de OSI y la autenticación de pares de SMAE están fuera del ámbito de la presente Recomendación | Norma Internacional. Sin embargo, los procedimientos de control de acceso definidos en la misma requieren la utilización de procedimientos de autenticación en el momento apropiado. Los posibles procedimientos de autenticación se describen en las Rec. X.217 del CCITT | ISO 8649, X.227 del CCITT | ISO 8650 y UIT-T X.509 | ISO/CEI 9594-8.

El control de acceso para la gestión de OSI se especifica como un conjunto de denegaciones y permisos para realizar operaciones de gestión. El usuario de la aplicación de gestión que invoca la operación de gestión es el iniciador y los elementos de información de gestión, por ejemplo, objetos gestionados y atributos, identificados por los parámetros de la operación de gestión, se combinan para formar el objeto u objetivos (*target*).

El control de acceso de informes de eventos se efectúa aplicando control de acceso a operaciones de gestión en discriminadores de eventos hacia adelante.

7.2 Políticas de control de acceso

Una política de control de acceso incorpora uno o más conjuntos de reglas. Es responsabilidad del realizador de la política de control de acceso asegurar que las reglas de control de acceso representan exactamente un caso de aplicación de la política de control de acceso.

Una política de control de acceso es una política de gestión específica que puede ser el objeto de la administración de política de gestión.

NOTA – La presente Recomendación | Norma Internacional no especifica la gestión de políticas de gestión y en particular no especifica ningún medio de verificar la integridad de la información de control de acceso.

Una política de control de acceso se impone mediante la utilización de uno o más esquemas de control de acceso, entre los que cabe citar:

- esquemas ACL;
- esquemas de capacidades;
- esquemas basados en contexto; y
- esquemas basados en etiquetas.

Si algunas características de un objeto gestionado (por ejemplo, atributos) están bajo la jurisdicción de diferentes políticas de seguridad, el objeto gestionado puede estar en múltiples dominios de seguridad. Cuando se aplican múltiples políticas de control de acceso a un objeto gestionado, la política de control de acceso impuesta es la que está asociada con el iniciador y el objetivo.

7.3 Información de control de acceso

La información de control de acceso comprende:

- las reglas de control de acceso;
- la identidad del iniciador de la petición de acceso (ACI de iniciador);
- las capacidades y verificaciones de seguridad asociadas con el iniciador (ACI de iniciador);
- la información perteneciente a la autenticación del iniciador (ADI retenida);
- las identidades de información de gestión (objetivos) a las cuales se ha solicitado acceso (ACI objetivos);
- las capacidades y verificaciones de seguridad asociadas con el objetivo (ACI de objetivo)
- las operaciones permitidas que se pueden ejecutar en relación con la información de gestión (ACI de iniciador, ACI de objetivo);
- la información retenida por la función de decisión de control de acceso para uso subsiguiente (ADI retenida); y
- la información contextual.

7.3.1 reglas de control de acceso: La información de control de acceso representa las operaciones permitidas y las condiciones creadas por su ejecución en un dominio de seguridad. Hay cinco clasificaciones de reglas de control de acceso que han de ser aplicadas por la función de decisión de acceso:

- **Reglas de denegación global**: Reglas de control de acceso que niegan el acceso a todos los objetivos. Si una regla global niega el acceso, no se aplicará ninguna otra regla. Si una regla global no niega el acceso, se imponen reglas de denegación de ítem.
- **Reglas de denegación de ítem**: Reglas de control de acceso que niegan el acceso a determinados objetivos. Si una regla de denegación de ítem niega el acceso, no se aplicará ninguna otra regla. Si una regla de denegación de ítem no niega el acceso, se aplican las reglas de permiso global.
- **Reglas de permiso global**: Reglas de control de acceso que permiten el acceso a todos los objetivos. Si una regla global permite el acceso, no se aplicará ninguna otra regla. Si una regla global no permite el acceso, se imponen reglas de permiso de ítem.
- **Reglas de permiso de ítem**: Reglas de control de acceso que permiten el acceso de determinados objetivos. Si una regla de control de ítem permite el acceso, no se aplicará ninguna otra regla. Si una regla de control de ítem no permite el acceso, se aplicarán las reglas por defecto.
- **Reglas por defecto**: Reglas de control de acceso que se han de aplicar cuando ninguna otra regla ha permitido o denegado específicamente el acceso. Las reglas por defecto permiten o niegan el acceso.

7.3.2 ACI limitada a acción: Información de control de acceso (tal como una etiqueta de seguridad) que está asociada con la información de gestión transportada en operaciones de gestión e informes de eventos. La ACI limitada a acción se puede utilizar también para crear y/o modificar información de control de acceso asociada con un objetivo.

7.3.3 ACI limitada a iniciador: Información de control de acceso proporcionada por el iniciador de una petición de gestión, o asociada con éste. Esta información puede ser:

- la identidad del iniciador de la operación de gestión;
- la información transportada en el parámetro de control de acceso de operaciones de gestión (por ejemplo, parámetro de control de acceso CMIS, parámetro de control de acceso de información de usuario CMIP);
- información asignada por una autoridad de dominio de seguridad; o
- una combinación de las anteriores.

El parámetro de control de acceso transportado por el CMIS puede adoptar la forma de un certificado de seguridad o de un testigo de seguridad.

NOTA – La identidad del iniciador se puede transferir de los mecanismos de autenticación utilizando procedimientos locales que están fuera del alcance de esta Recomendación | Norma Internacional.

7.3.4 ACI limitada a objetivo: Información de control de acceso que identifica la información de gestión sobre la cual se han de realizar operaciones.

7.3.5 información contextual: Información de control de acceso asociada con contexto (por ejemplo, hora del día, nivel de autenticación, lugar, limitación de recursos, participación en una relación).

7.3.6 ADI: Las ADI de acción, ADI de iniciador y ADI de objetivo se derivan de las ACI limitada a acción, ACI limitada a iniciador y ACI limitada a objetivo, respectivamente, a los fines de decisión.

7.3.7 ADI retenida: Información de control de acceso retenida por la función de decisión de control de acceso. De acuerdo con la política de control de acceso, parte de esta información puede ser retenida durante periodos de tiempo más largos que la vida de una asociación. La ADI retenida puede ser utilizada por la ADF para evaluar privilegios de acceso.

7.4 Procedimientos de control de acceso

Las reglas de control de acceso especifican los criterios de seguridad que se han de cumplir para poder acceder a la información de gestión. Las reglas pueden imponer que se ejecuten algunos de los procedimientos siguientes o todos:

- validación de ACI limitada a iniciador;
- identificación del objetivo;

- determinación de la decisión de acceso;
- modificación de la ADI retenida;
- modificación de ACI limitada a objetivo; e
- imposición de la decisión.

Antes de establecer una asociación, la información de control de acceso que representa reglas de control de acceso para ese dominio de control de acceso puede ser generada y distribuida por una autoridad de dominio de seguridad utilizando mecanismos que están fuera del ámbito de la presente Recomendación | Norma Internacional.

Los procedimientos que siguen especifican las decisiones de acceso que se han de tomar, y no dónde se han de tomar. La presente Recomendación | Norma Internacional no especifica si las decisiones se han de tomar en el sistema gestor, en el sistema gestionado, en ambos sistemas o en alguna otra parte.

Es responsabilidad del iniciador proporcionar información de control de acceso compatible con los mecanismos de control de acceso especificados por la política de seguridad.

La utilización de todos estos procedimientos o de algunos no excluye la utilización de otros procedimientos y de otros mecanismos de control de acceso no especificados por la presente Recomendación | Norma Internacional.

7.4.1 Validación de ACI limitada a iniciador

La ACI limitada a iniciador puede ser suministrada en el parámetro de control de acceso de la petición de servicio CMIS para la operación de gestión. La información puede adoptar la forma de un certificado de seguridad, por ejemplo, un certificado de control de acceso (ACC), o un testigo de seguridad.

La política de seguridad especifica cuáles de las siguientes acciones se ejecutarán:

- la integridad de la información será validada utilizando procedimientos fuera del ámbito de la presente Recomendación | Norma Internacional;
- la validez de la información se verificará comprobando que el origen de la información fue una autoridad de dominio de seguridad reconocida;
- el contenido de la información se verificará comprobando que el valor de la información estaba dentro de una gama permitida.

7.4.2 Identificación del objetivo

Un objetivo es un elemento de información que ha de ser protegido por un esquema de control de acceso. La información de gestión está contenida en el árbol de información de gestión. Se puede seleccionar un subárbol utilizando el parámetro delimitador del CMIS. Cuando este es el caso, todo el subárbol seleccionado se considera como un objetivo. La selección puede refinarse aún más mediante la utilización de los parámetros delimitador y filtro del CMIS que seleccionan objetos gestionados individuales y sus características del árbol de información de gestión. En este caso, todos los objetos gestionados seleccionados y sus características constituyen el objetivo. En la granularidad más fina, es posible seleccionar objetos gestionados individuales del árbol de información de gestión. En este caso, sólo el objeto gestionado seleccionado y sus características constituyen el objetivo.

Cualquier petición de operación de gestión dada identifica uno o más objetivos. Estos objetivos se identifican como sigue:

a) cuando el parámetro delimitador está presente en la petición, todo el subárbol de gestión abarcado por la petición es un objetivo. Es decir, la combinación de los parámetros clase de objeto gestionado de base, el caso de objeto gestionado de base, delimitador, sincronización, tipo de operación, identificador de atributo, identificador de acción, valor de argumento de información de atributo (attributeInfoArg), valor de argumento de información de acción (actionInfoArg) forman un objetivo;

b) cuando los parámetros delimitador y filtro están presentes en la petición, los objetos gestionados seleccionados y las características de estos objetos gestionados constituyen un objetivo. Es decir, cada combinación de clase de objeto gestionado de base distinto, caso de objeto gestionado de base, valor de atributo, tipo de operación, identificador de atributo, identificador de acción, valor de argumento de información de atributo, valor de argumento de información de acción formada a partir de:

   - los objetos gestionados seleccionados por los parámetros clase de objeto gestionado de base, el caso de objeto gestionado de base y delimitador, y
   - los elementos de ítem de filtro del parámetro filtro

   forman un objetivo; o

c) cada objeto gestionado distinto y sus características seleccionadas por la operación forman un objetivo. Es decir, la combinación de clase de objeto gestionado de base, clase de objeto gestionado, caso de objeto gestionado de base, caso de objeto gestionado, caso de objeto gestionado de superior, caso de objeto gestionado de referencia, caso de objeto gestionado de valor inicial, tipo de operación, identificador de atributo, identificador de acción, valor de argumento de información de atributo, valor de argumento de información de acción para cada objeto gestionado seleccionado por los parámetros de selección de objeto gestionado constituye un objetivo.

NOTA – Un objetivo incluye la operación u operaciones solicitadas para el objeto gestionado.

7.4.3 Determinación de la decisión de acceso

La función de decisión de control de acceso realizará todos los procedimientos especificados por la política de seguridad. Durante los procedimientos se puede utilizar ADI de iniciador, ADI retenida, ADI de objetivo, ADI de operando e información contextual. La política de seguridad puede incluir algunos o todos los procedimientos indicados en 7.4.3.1.

7.4.3.1 Procedimientos de decisión de acceso

Se aplicará primero el procedimiento identificado en 7.4.3.1.1.

7.4.3.1.1 Identifíquense las reglas de acceso a información de gestión que se aplican al dominio de seguridad del iniciador y al objetivo.

7.4.3.1.2 Para todas las reglas globales que niegan el acceso a iniciadores, ejecútense las pruebas aplicables de 7.4.3.2. Si alguna prueba devuelve éxito, indíquese a la función de imposición de control de acceso que la petición de operación de gestión será denegada y aplíquense los procedimientos indicados en 7.4.6; en los demás casos, aplíquese el procedimiento indicado en 7.4.3.1.3.

7.4.3.1.3 Para todas las reglas de ítem que niegan acceso a objetivos, ejecútense las pruebas aplicables de 7.4.3.2. Si alguna prueba devuelve éxito, indíquese a la función de imposición de control de acceso que la petición de operación de gestión será denegada y aplíquense los procedimientos indicados en 7.4.6, en los demás casos, aplíquese el procedimiento de 7.4.3.1.4.

7.4.3.1.4 Para todas las reglas globales que permiten acceso a los iniciadores, ejecútense las pruebas aplicables indicadas en 7.4.3.2. Si alguna prueba devuelve éxito, indíquese a la función de imposición de control de acceso que la petición de operación de gestión será permitida y aplíquense los procedimientos indicados en 7.4.4, 7.4.5 y 7.4.6; en los demás casos, aplíquese el procedimiento de 7.4.3.1.5.

7.4.3.1.5 Para todas las reglas de ítems que permiten acceso a objetivos, ejecútense las pruebas aplicables indicadas en 7.4.3.2. Si alguna prueba devuelve éxito, indíquese a la función de imposición de control de acceso que la petición de operación de gestión será permitida y aplíquense los procedimientos de 7.4.4, 7.4.5 y 7.4.6; en los demás casos, aplíquese el procedimiento de 7.4.3.1.6.

7.4.3.1.6 Si la política no ha especificado ninguna regla que permite o niega concretamente el acceso al objetivo, indíquese a la función de imposición de control de acceso que la petición de operación de gestión será permitida o denegada de acuerdo con la regla por defecto para esa operación, y se aplicará la respuesta de denegación por defecto. Si se ha de denegar la petición de operación de gestión, sólo se aplican los procedimientos indicados en 7.4.6. En los demás casos, aplíquense los procedimientos de 7.4.4, 7.4.5 y 7.4.6.

7.4.3.2 Pruebas de decisión de acceso

Las siguientes pruebas están disponibles para la función de decisión de acceso, de acuerdo con la política de seguridad. Cada prueba recibe información asociada con el iniciador y una regla que identifica las operaciones realizadas en los objetivos. Cada prueba devuelve un valor booleano, que es la veracidad o la falsedad de la proposición que «el iniciador satisface la regla».

La evaluación de una operación solicitada en un objeto gestionado objetivo específico puede requerir información sobre una clase o caso de objeto gestionado valores de superior, de referencia o inicial, que se revelará al iniciador. Si el iniciador no tiene acceso (permiso de OBTENCIÓN) a la información requerida sobre la clase o caso de objeto gestionado valores de superior, de referencia o inicial según haya sido determinado apropiadamente mediante a) a e) siguientes, la regla evaluará FALSO.

a) Cuando lo requiera un esquema ACL, la identidad, grupo o cometido del iniciador se comparará con las identidades de iniciadores asociadas con la regla. Si se encuentra concordancia idéntica y si la operación y el objetivo asociado con la petición son compatibles con las operaciones y los objetivos especificados por la regla, la regla evaluará VERDADERO. Si no hay concordancia idéntica o la operación u objetivo

asociado con la petición es incompatible con las operaciones y objetivos especificados por la regla, la regla evaluará FALSO.

b) Cuando lo requiera un esquema de capacidades como la identidad asociada con el iniciador se comparará con una lista de identidades de iniciador asociadas con la regla. Si hay concordancia idéntica que permite utilizar la capacidad y la operación y el objetivo identificados en la petición son compatibles con los especificados en la capacidad, la regla evaluará VERDADERO. Si no hay concordancia idéntica o si la operación u objetivo identificados en la petición son incompatibles con los especificados en la capacidad, la regla evaluará FALSO.

c) Cuando lo requiera un esquema basado en contexto, se comprobarán las condiciones contextuales asociadas con la regla. Si se satisfacen todas las condiciones contextuales, la regla evaluará VERDADERO; en los demás casos, la regla evaluará FALSO.

d) Cuando lo requiera un esquema basado en etiqueta, la etiqueta asociada con el iniciador será validada contra la etiqueta asociada con el objetivo. Si el algoritmo de etiqueta determina que la etiqueta asociada con el iniciador es compatible con la etiqueta asociada con el objetivo, la regla evaluará VERDADERO; en los demás casos, la regla evaluará FALSO.

e) Cuando lo requiera la política de seguridad, ejecútese cualquier otra prueba asociada con la regla.

Al evaluar las reglas de control de acceso en un dominio de seguridad que utiliza una combinación de mecanismos de control de acceso, una sola regla satisfará todos los mecanismos asociados con esa regla.

NOTA – Algunas políticas de seguridad pueden aplicar combinaciones de los esquemas de control de acceso de la regla. En este caso, la política de control de acceso identificará la precedencia de los esquemas.

7.4.4 Modificación de ADI retenida

Si lo especifica la política de seguridad, la ADI retenida por la función de decisión de control de acceso puede ser modificada utilizando la ACI del iniciador suministrada con la petición de operación de gestión. La información permanente comprende:

- la ACI que está asociada permanentemente con el iniciador;
- la ADI retenida de asociaciones anteriores;
- la ACI suministrada por el iniciador;
- la ACI obtenida como resultado del procedimiento de autenticación; e
- información contextual.

NOTA – Los mecanismos para gestionar, obtener, almacenar y recuperar ADI retenida están fuera del ámbito de la presente Recomendación | Norma Internacional.

7.4.5 Modificación de ADI de objetivo

Si lo especifica la política de seguridad, la ADI asociada con el objetivo puede ser modificada utilizando la ADI de acción que fue suministrada con la petición de operación de gestión de acuerdo con los siguientes procedimientos.

7.4.5.1 Para la operación crear, se puede utilizar la ADI de acción para crear la ADI de objetivo específica del objeto gestionado recientemente creado. La ADI asociada con otros objetivos no puede ser modificada.

7.4.5.2 Para la operación supresión, se puede utilizar la ADI de acción para modificar o suprimir la ADI de objetivo específica del objeto u objetos gestionados suprimidos. La ADI asociada con otros objetivos no puede ser modificada.

7.4.5.3 Para las operaciones sustitución de valor de atributo, sustitución con valor por defecto, incorporación de miembro y supresión de miembro, se puede utilizar la ADI de acción para modificar ADI objetivo específica del atributo o atributos de objetivo modificados por la operación. La ADI asociada con otros objetivos no puede ser modificada.

NOTA – Con independencia de las operaciones de gestión identificadas anteriormente, se puede modificar la ADI de objetivo. La ADI asociada con objetivos puede ser creada, suprimida y modificada por medios que están fuera del ámbito de la presente Recomendación | Norma Internacional. Por ejemplo, la creación de un objeto gestionado que representa un recurso puede también crear ADI de objetivo como una consecuencia directa de la creación del objeto gestionado. Si se permite la gestión de ACI mediante la gestión de sistemas de OSI, la ADI de objetivo puede ser modificada de acuerdo con la cláusula 8.

7.4.6 Imposición de la decisión

La función de imposición de control de acceso será responsable de imponer la decisión de política indicada por la función de decisión de control de acceso.

En las siguientes subcláusulas se describe:

a) el significado de las posibles respuestas de denegación de acceso que pueden ser devueltas al iniciador como resultado de la acción efectuada por la función de imposición de control de acceso;

b) el procedimiento que ha de aplicar la función de imposición de control de acceso como resultado de una petición de operación de gestión que se recibe con ACI limitada al iniciador inválida;

c) el procedimiento que ha de ser ejecutado por la función de imposición de control de acceso como resultado de una operación de gestión que se deniega como consecuencia de una regla global que niega el acceso;

d) el procedimiento que ha de ser ejecutado por la función de imposición de control de acceso como resultado de una operación de gestión que se deniega como consecuencia de una regla de ítem que niega el acceso o como consecuencia de la regla por defecto que niega el acceso; y

e) los requisitos para registrar e informar eventos significativos para la sustentación de un esquema de control de acceso.

7.4.6.1 Imposición de negación de acceso

La imposición de acceso denegado requiere la especificación de la respuesta de negación apropiada que se ha de devolver al iniciador, y la especificación de los objetivos concretos a los cuales se niega el acceso.

Se especificará una de las siguientes acciones de respuesta de negación:

– cuando se da una respuesta de negación, la función de imposición de control de acceso asegurará que se devuelve la respuesta de error de acceso denegado al iniciador si se solicitó el servicio de operación de gestión en el modo confirmado;

– cuando no se da ninguna respuesta, la función de imposición de control de acceso asegurará que no se devuelve ninguna respuesta al iniciador;

– cuando se aborta la asociación, la función de imposición de control de acceso asegurará que se invoca el procedimiento ACSE A-ABORTO; o

– cuando se da una respuesta falsa, la función de imposición de control de acceso asegurará que se devuelve información de gestión incorrecta al iniciador si se solicitó el servicio de operación de gestión en el modo confirmado.

Si no se especifica ninguna acción de respuesta de denegación, la acción de respuesta de denegación por defecto es un asunto de política local.

La respuesta de denegación tendrá una granularidad de denegación asociada. Las posibles granularidades de negación comprenden:

– Una sola negación en el nivel de la petición de gestión total. La negación de acceso a cualquier elemento de información de gestión dará como resultado que se niega la petición total. No se realizarán operaciones de gestión en objetivos asociados con la petición.

– Una negación en el nivel de cada objeto gestionado referenciado en la petición. La negación de acceso a cualquier operación y atributo del objeto gestionado dará como resultado la negación de acceso al objeto gestionado, pero no a otros objetos gestionados asociados con la petición. No se realizará ninguna operación en objetivos asociados con el objeto gestionado al cual se niega el acceso.

– Una negación en el nivel de cada atributo dentro de cada objeto gestionado referenciado por la petición. La negación de acceso a un atributo específico dentro de un objeto gestionado dará como resultado que se niega el acceso a ese atributo, pero no a otros atributos dentro del objeto gestionado contenedor, o atributos dentro de otros objetos gestionados. No se realizará ninguna operación de gestión en los atributos específicos a los cuales se niega el acceso.

Si no se especifica la granularidad de la negación, la granularidad de negación por defecto es un asunto de política local.

NOTAS

1 Se recomienda una granularidad de negación por defecto en el nivel de la petición total para satisfacer el principio de privilegio mínimo.

2 Se recomienda una acción de imposición por defecto de ninguna respuesta o aborto de asociación para satisfacer el principio de privilegio mínimo.

7.4.6.2 Denegación como resultado de ACI limitada a iniciador inválida

Si la decisión es denegar la petición como resultado de ACI limitada a iniciador inválida:

- no se realizará ninguna operación en cualquier objetivo especificado en la petición;
- se invocará la acción de imposición de negación especificado o por defecto, con la excepción de que se cambie una acción de imposición de negación especificada de una respuesta falsa para abortar la asociación;
- se pasará por alto la granularidad especificada de la respuesta de negación, si la hubiere, y la respuesta se dará con la granularidad de la petición total.

7.4.6.3 Denegación como resultado del cumplimiento de una regla global

Si la decisión es denegar la operación de gestión como resultado de una regla global:

- no se realizará ninguna operación en ninguno de los objetivos especificados en la petición;
- se invocará la acción de imposición de negación especificado o por defecto;
- se pasará por alto la granularidad especificada de la respuesta de negación, si la hubiere, y la respuesta se dará con la granularidad de la petición total.

7.4.6.4 Denegación como resultado del cumplimiento de una regla de ítem o de una regla por defecto

Si la decisión es negar la operación de gestión en el objetivo identificado como resultado de una regla de ítem o de una regla por defecto:

- si el objetivo abarca un subárbol del árbol de información de gestión, es decir, el objetivo fue seleccionado por a) de 7.4.2, no se realizará ninguna operación en ningún objeto gestionado mantenido dentro del subárbol seleccionado;
- si el objetivo es una selección de objetos gestionados [del inciso b) de 7.4.2], no se realizará ninguna operación en esos objetos gestionados identificados por el objetivo;
- si el objetivo es uno de los identificados de acuerdo con el inciso c) de 7.4.2, no se realizará ninguna operación en ese objetivo;
- se invocará la acción de imposición de negación especificada o por defecto;
- la granularidad de la respuesta será la granularidad de denegación especificada, si se especifica, o la granularidad de negación por defecto.

NOTAS

1 En el caso de selección de múltiples objetos, el CMIS no define una respuesta adecuada para utilización en el nivel de objeto gestionado de negación. Es decir, se dará una respuesta de negación para cada atributo seleccionado.

2 En el caso de negación porque se niega el acceso a un atributo en el filtro, el CMIS no proporciona medios para indicar que la causa es el atributo filtro. Por tanto, si el objetivo es uno de los definidos en el inciso b) de 7.4.2 y se pide una respuesta de negación en el nivel de objeto gestionado, la respuesta no tiene que proporcionar una indicación del atributo que causó la negación.

7.4.6.5 Requisitos para registrar eventos significativos para el control de acceso

Si la política de seguridad impone que se registren las peticiones de operaciones de gestión, la función de imposición de control de acceso asegurará que se genera la notificación apropiada, como sigue:

- si se niega la petición de acceso, la notificación será un informe de alarma de seguridad; o
- si se permite la petición de acceso, la notificación será un informe de pista de auditoría de seguridad.

7.5 Representación de reglas de control de acceso

Una regla de control de acceso es una correspondencia de la combinación de pares (iniciador, objetivo) con el permiso de acceso (permiso o negación).

El espacio de iniciadores comprende cada usuario posible de aplicaciones de gestión. Este espacio es divisible de acuerdo con la política de seguridad (por ejemplo, esquemas ACL, esquemas de capacidad, esquemas basados en etiqueta). Debe haber tantas maneras de dividir este espacio como políticas de seguridad haya.

Los grupos de iniciadores pueden estar representados por objetos gestionados. La identificación de iniciadores depende de la política de seguridad.

El espacio de objetivos comprende cada par de valores concebibles (operación de gestión, argumento). Hay muchas maneras de dividir este espacio:

- por operación;
- por objeto gestionado;
- por clase de objeto gestionado;
- por atributo;
- por acción;
- por valor de atributo/argumento;
- por el parámetro delimitador; y
- por el parámetro sincronización.

La granularidad más fina que se puede lograr es clase de objeto gestionado, caso de objeto gestionado, operación, identificador de acción, valor de acción, identificador de atributo, valor de atributo. Cuando se permite la selección de múltiples objetos, se puede imponer el control de acceso en las combinaciones de clase de objeto gestionado, caso de objeto gestionado, delimitador y sincronización. Cuando se permite el delimitador y el filtrado, el control de acceso se puede imponer en la combinación de clase de objeto gestionado, caso de objeto gestionado, identificador de atributo y valor de atributo para cada objeto gestionado dentro del delimitador.

Los grupos de objetivos pueden ser representados por objetos gestionados.

El control de acceso se impone dentro del contexto de un dominio de seguridad. Hay cinco jerarquías de reglas de control de acceso dentro de cada dominio:

- reglas que niegan a iniciadores específicos el acceso a cualquiera de los objetivos del dominio;
- reglas que niegan a iniciadores específicos el acceso a objetivos específicos del dominio;
- reglas que permiten a iniciadores específicos el acceso a todos los objetivos del dominio;
- reglas que permiten a iniciadores específicos el acceso a objetivos específicos del dominio; y
- reglas que permiten o niegan el acceso en ausencia de cualquier otra regla que permite o niega el acceso.

8 Definiciones genéricas

La información y los procedimientos de control de acceso descritos en la cláusula 7 se pueden modelar como objetos gestionados. La Figura 1 muestra la jerarquía de herencia para las clases de objeto gestionado definidas en la presente Recomendación | Norma Internacional.

La Figura 2 muestra las relaciones entre algunos de los objetos gestionados identificados en la Figura 1.

NOTA – No todos los objetos gestionados mostrados en la Figura 1 se muestran en la Figura 2. Por razones de claridad, se omiten los objetos gestionados no incluidos en la Figura 2 (la clase de objeto gestionado de control de acceso y las etiquetas asignadas y clases de objeto gestionado derivado).

8.1 Objetos gestionados

8.1.1 Control de acceso

Esta clase de objeto gestionado comprende los elementos de información de gestión y el comportamiento comunes a todos los objetos gestionados que representan información de control de acceso. Se especifica únicamente para proporcionar un solo punto de especialización para otras clases de objetos gestionados que representan información de control de acceso.

8.1.1.1 Atributos de control de acceso

Se define el siguiente atributo obligatorio para la clase de objeto gestionado control de acceso.

8.1.1.1.1 Nombre de objeto de control de acceso

Este atributo se utiliza para identificar casos de especializaciones de la clase objeto gestionado control de acceso.

8.1.1.2 Notificación de control de acceso

Se definen las siguientes notificaciones para la clase de objeto gestionado control de acceso:

- cambio de valor de atributo;
- creación de objeto; y
- supresión de objeto.

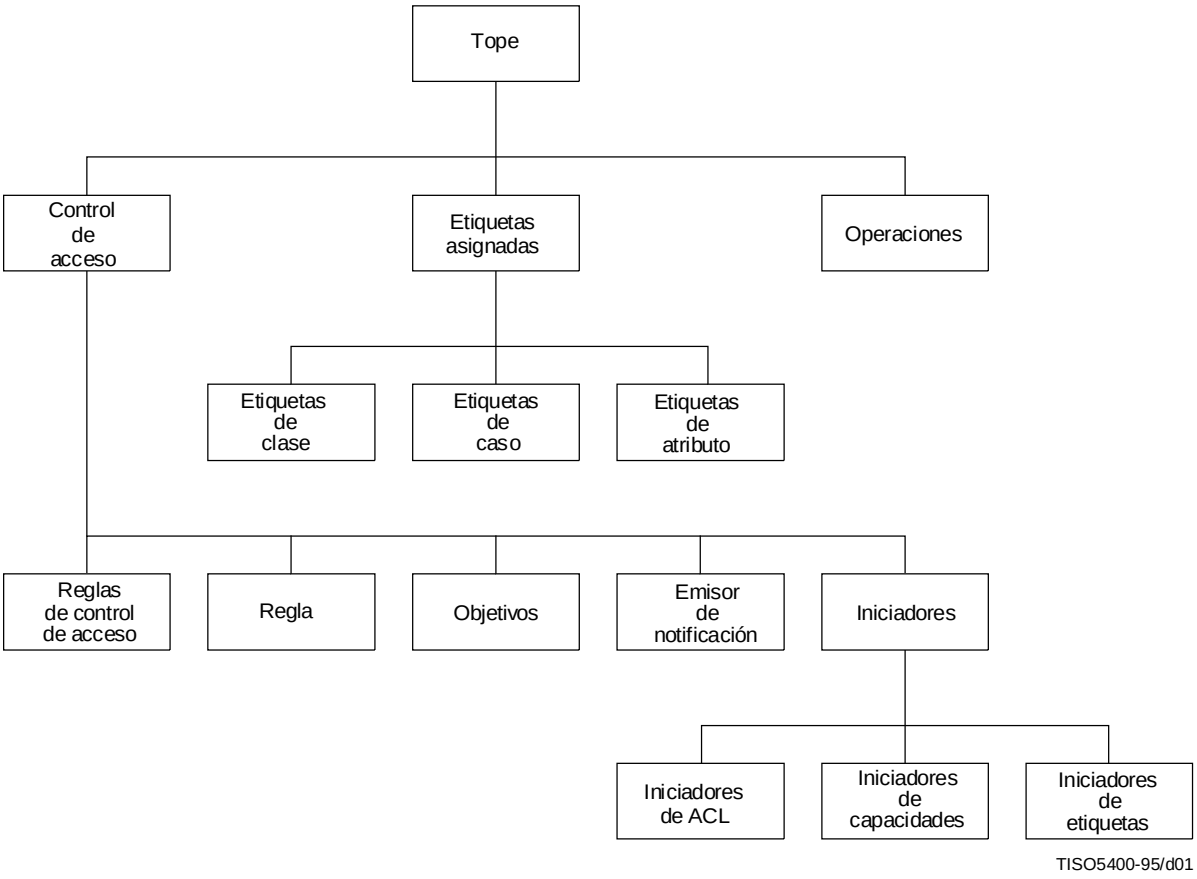

Figura 1 – Jerarquía de herencia de clases de objetos gestionados

8.1.2 Reglas de control de acceso

Los objetos gestionados reglas de control de acceso representan la función de decisión de control de acceso para un dominio de seguridad. Sus atributos y objetos gestionados reglas contenidos identifican las reglas de control de acceso para el dominio de seguridad. La clase de objeto gestionado reglas de control de acceso es una subclase de la clase de objeto gestionado control de acceso.

El objeto gestionado reglas de control de acceso contiene los otros objetos gestionados que representan reglas de control de acceso para la función de decisión de control de acceso.

8.1.2.1 Atributos de reglas de control de acceso

Se definen los siguientes atributos obligatorios para la clase de objeto gestionado reglas de control de acceso.

8.1.2.1.1 Acceso por defecto

El atributo acceso por defecto identifica, de acuerdo con 7.4.3.1.6, los derechos de acceso por defecto para cada tipo de operación.

8.1.2.1.2 Respuesta de denegación por defecto

El atributo respuesta de denegación por defecto identifica la respuesta por defecto devuelta al iniciador en el caso de que la ADF haya negado el acceso al objetivo basándose en la regla por defecto.

8.1.2.1.3 Identidad de dominio

Este atributo identifica el dominio de control de acceso que rige estas reglas de control de acceso.

8.1.2.1.4 Granularidad de denegación

Este atributo identifica el nivel en el cual se presentará la denegación de acceso, si procede.

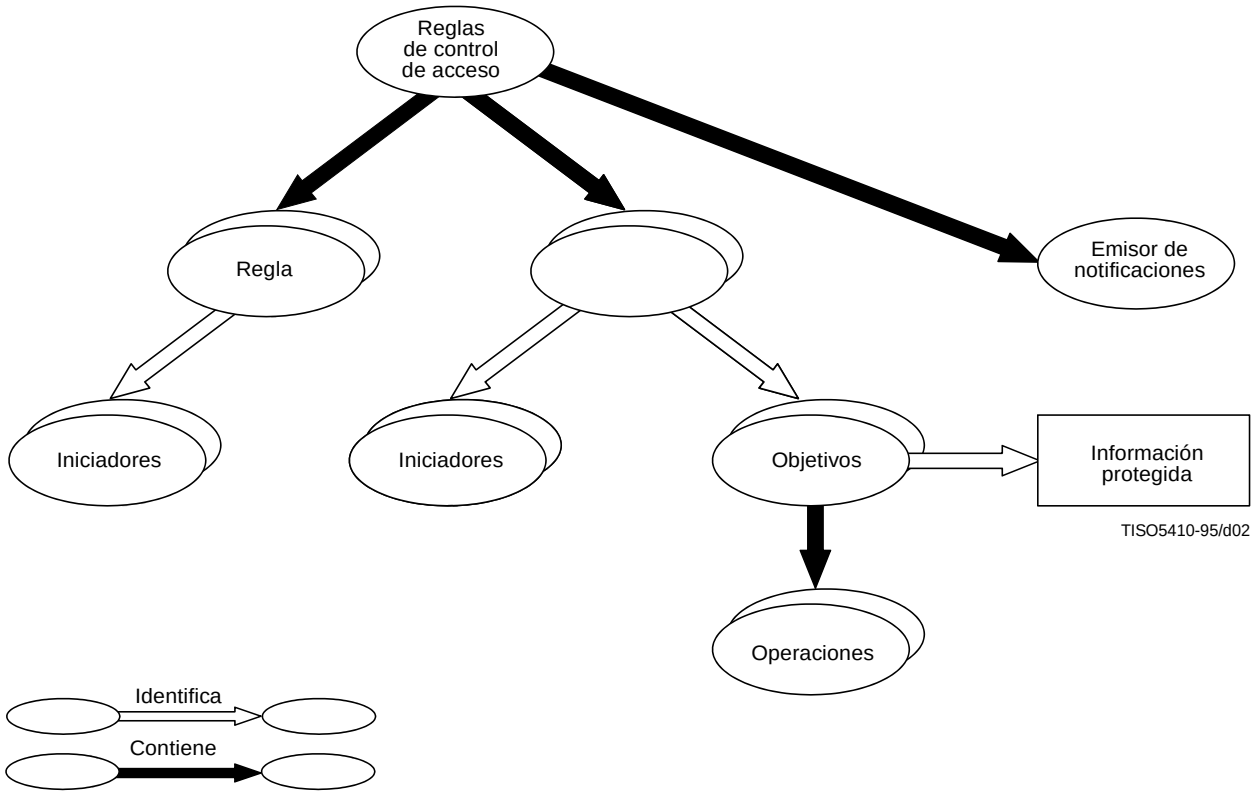

Figura 2 – Relación entre objetos gestionados

8.1.3 Regla

La clase de objeto gestionado regla representa reglas globales y de ítem. La clase de objeto gestionado regla es una subclase de la clase de objeto gestionado control de acceso.

8.1.3.1 Atributos de regla

Se definen los siguientes atributos obligatorios para la clase de objeto gestionado regla.

8.1.3.1.1 Acción de imposición

Este atributo identifica la acción que ha de ejecutar la función de imposición de control de acceso si se cumple la regla.

8.1.3.1.2 Lista de iniciadores

Este atributo con valor fijo identifica las subclases de objetos gestionados iniciadores que especifican los iniciadores a los cuales pertenece la regla.

8.1.3.1.3 Lista de objetivos

Este atributo con valor fijo identifica los objetos gestionados objetivos que especifican por si mismos los objetivos a los cuales pertenece la regla de ítem.

8.1.3.2 Lotes de planificación

Para acomodar diversos niveles de complejidad en la planificación de los periodos de actividad de las reglas, se definen para la regla lotes condicionales que se relacionan con la planificación.

Los lotes de planificación permiten que los objetos gestionados reglas transiten automáticamente entre las condiciones «vigente» y «no vigente» señalizadas por el atributo situación de disponibilidad que toma el valor { } y {offDuty} respectivamente.

8.1.3.2.1 Lote de situación de disponibilidad

Este lote estará presente si están presentes cualquiera de los otros lotes relacionados con la planificación. Si este lote no está presente, estará siempre disponible el objeto gestionado regla.

8.1.3.2.2 Lote de duración

El lote de duración proporciona la capacidad de controlar automáticamente los periodos en los cuales un objeto gestionado comienza y termina su funcionamiento. Este lote estará presente si se requiere esta funcionalidad. Si este lote y uno de los otros lotes de planificación coexisten, la situación de disponibilidad adoptará el valor {offDuty} a menos que ambos lotes señalicen actividad, en cuyo caso la situación de disponibilidad será { }.

8.1.3.2.3 Lote de planificación diaria

El lote de planificación diaria proporciona la capacidad de planificar las operaciones dentro de un periodo de 24 horas. Estará presente si se requiere esta funcionalidad. No coexistirá con el lote de planificación semanal o el lote de planificador externo.

8.1.3.2.4 Lote de planificación semanal

El lote de planificación semanal proporciona la capacidad de planificar las operaciones en un periodo de una semana. Estará presente si se requiere esta funcionalidad. No coexistirá con el lote de planificación diaria o de planificador externo.

8.1.3.2.5 Lote de planificación de planificador externo

El lote de planificación de planificador externo proporciona la capacidad de planificar operaciones utilizando una planificación definida en otro objeto gestionado. Estará presente si se requiere esta funcionalidad. No coexistirá con el lote de planificación diaria o de planificación semanal.

8.1.3.3 Lote de condiciones de estado

El lote de condiciones de estado permite que una regla funcione dentro del contexto del estado de objetos gestionados identificados. Estará presente si se requiere esta funcionalidad.

8.1.3.3.1 Atributos del lote de condiciones de estado

Se define el siguiente atributo obligatorio para el lote condiciones de estado.

8.1.3.3.1.1 Condiciones de estado

Este atributo de valor fijo identifica objetos gestionados y filtros asociados en los atributos de estos objetos gestionados.

8.1.3.4 Lote de contexto de autenticación

Cuando está presente en un objeto gestionado regla, el lote de contexto de autenticación especifica la identidad de la política de autenticación y los requisitos de autenticación que un iniciador tiene que satisfacer.

8.1.3.4.1 Atributos del lote de contexto de autenticación

Se define el siguiente atributo obligatorio para el lote de contexto de autenticación.

8.1.3.4.1.1 Contexto de autenticación

El atributo contexto de autenticación es una secuencia de identificador de política de autenticación y los requisitos identificados por el mismo.

8.1.4 Emisor de notificación

Esta clase de objeto gestionado se utiliza para poder emitir notificaciones aplicables a la provisión de control de acceso para la gestión de OSI. Los tipos de notificación aplicables comprenden determinadas alarmas de seguridad definidas en la Rec. X.736 del CCITT | ISO/CEI 10164-7 y algunas notificaciones de pista de auditoría de seguridad definidas en la Rec. X.740 del CCITT | ISO/CEI 10164-8.

Un solo objeto gestionado emisor de notificación puede estar contenido dentro de un objeto gestionado reglas de control.

8.1.4.1 Lotes de emisor de notificación

Esta clase de objeto gestionado sustenta los siguientes lotes condicionales para proporcionar una capacidad flexible de transmitir notificaciones relacionadas con el control de acceso:

- lote de alarma de violación de seguridad;
- lote de alarma de violación de tiempo;
- lote de alarma de violación operacional;
- lote de utilización de control de acceso; y
- lote de informe de servicio de control de acceso.

8.1.4.1.1 Lote de alarma de violación de seguridad

Este lote permite que se emitan una notificación de alarma de seguridad del tipo «violación de servicio o mecanismo de seguridad» y la causa «tentativa de acceso no autorizada» si las comprobaciones de control de acceso fracasasen.

8.1.4.1.2 Lote de alarma de violación de tiempo

Este lote permite que se emitan una notificación de alarma de seguridad del tipo «violación en el dominio del tiempo» y las causas «clave expirada» y «actividad fuera de horas» si las comprobaciones de control de acceso fracasasen. La causa «clave expirada» se utilizará cuando la clave identificada por el sello de certificado de control de acceso está anticuada. La causa «actividad fuera de horas» se utilizará cuando fallan las comprobaciones de hora contextual.

8.1.4.1.3 Lote de alarma de violación operacional

Este lote permite que se emitan una notificación de alarma de seguridad del tipo «violación operacional» y las causas «fuera de servicio» y «motivo no especificado» si fracasasen las comprobaciones de control de acceso. La causa «fuera de servicio» se utilizará cuando el mecanismo de control de acceso identificado no está disponible. La causa «motivo no especificado» se utilizará en otros casos.

8.1.4.1.4 Lote de utilización de control de acceso

Este lote se utiliza para contar el número de tentativas de acceso válidas e inválidas y permitir que se envíen informes de utilización que contienen esta información a un registro de pistas de auditoría de seguridad. El informe de utilización se envía con un intervalo de tiempo definido por la política de seguridad. El campo de información adicional se utiliza para transportar los valores del contador.

8.1.4.1.4.1 Atributos del lote utilización de control de acceso

Se definen los siguientes atributos para el lote de utilización de control de acceso.

8.1.4.1.4.1.1 Tentativas de acceso válidas

Este atributo se utiliza para contar el número de veces que una función de decisión de control de acceso ha autorizado un acceso.

8.1.4.1.4.1.2 Tentativas de acceso inválidas

Este atributo se utiliza para contar el número de veces que una función de control de acceso no ha autorizado un acceso.

8.1.4.1.5 Lote de informe de servicio de control de acceso

Este lote permite que se emitan notificaciones de pista de auditoría de seguridad del tipo «informe de servicio» para posible inclusión en un registro de pistas de auditoría de seguridad.

8.1.5 Objetivos

El objeto gestionado objetivos identifica un conjunto de información de gestión sujeto a control de acceso. La clase de objeto gestionado objetivos es una subclase de la clase de objeto gestionado control de acceso.

8.1.5.1 Atributos de objetivos

Se definen los siguientes atributos obligatorios para los objetos gestionados objetivos.

8.1.5.1.1 Clases de objeto gestionado

Este atributo de valor fijo identifica clases de objetos gestionados protegidos y vinculaciones de nombres asociadas facultativas.

8.1.5.1.2 Casos de objeto gestionados

Este atributo de valor fijo identifica objetos gestionados protegidos.

8.1.5.1.3 Delimitador

El atributo delimitador identifica un delimitador para la selección de objetos gestionados protegidos.

8.1.5.1.4 Filtro

Este atributo identifica un filtro que se ha de aplicar a objetos gestionados identificados por los otros atributos del objeto gestionado objetivos para determinar su inclusión como un objeto gestionado protegido.

8.1.5.2 Lote lista de operaciones

Este lote proporciona apoyo para el atributo tipo de operaciones como una alternativa al objeto gestionado operaciones. Sólo se puede incluir en el objeto gestionado objetivos si no contiene ningún caso del objeto gestionado operaciones.

8.1.5.2.1 Atributos del lote lista de operaciones

Se define el siguiente atributo obligatorio para el lote tipo de operaciones.

8.1.5.2.1.1 Lista de operaciones

Este atributo de valor fijo identifica los tipos de operaciones que están sujetas a las reglas que identifican el objeto gestionado objetivos que contiene estas operaciones.

8.1.6 Operaciones

El objeto gestionado operaciones identifica constricciones a tipos de operaciones para objetos gestionados identificados por el objeto gestionado objetivos contenedor.

Los tipos de operaciones son las operaciones definidas en la Rec. X.720 del CCITT | ISO/CEI 10165-1 que comprenden:

- acción;
- creación;
- supresión;
- obtención;
- sustitución;
- incorporación de miembro;
- supresión de miembro;
- sustitución con valor por defecto;
- filtro; y
- selección de múltiples objetos.

Sólo habrá un objeto gestionado operaciones para un tipo de operación específico contenido dentro de un objeto gestionado objetivos.

El tipo de operación se utiliza como el valor del atributo denominador para la clase de objeto gestionado operaciones.

Los lotes condicionales proporcionan atributos para especificar constricciones a los atributos y acciones asociadas con el tipo de operación. Además, se proporcionan atributos en lotes condicionales para imponer constricciones a los valores de los parámetros delimitador y sincronización que se autorizan en una petición de acceso con selección de múltiples objetos.

NOTA – Puede ser necesario aplicar diferentes constricciones al mismo tipo de operación, o suboperaciones para el mismo tipo de operación, para el mismo objeto u objetos gestionados. Por ejemplo, esta necesidad puede existir cuando deban aplicarse diferentes constricciones a diferentes acciones específicas para el mismo objeto u objetos gestionados. En estos casos, se creará un nuevo objeto gestionado objetivos que contienen el objeto gestionado al cual se aplica la constricción, y que contiene un objeto gestionado operaciones que especifica las nuevas constricciones que se han de aplicar para el tipo de operación.

8.1.6.1 Atributos de operaciones

Se define el siguiente atributo obligatorio para la clase de objeto gestionado operaciones.

8.1.6.1.1 Tipo de operación

Este atributo identifica el tipo de operación al cual se aplican las constricciones, y se utiliza para denominar objetos gestionados operaciones.

8.1.6.2 Notificaciones de operaciones

Se definen las siguientes notificaciones obligatorias para la clase de objeto gestionado operaciones:

a) creación de objeto;

b) supresión de objeto;

c) cambio del valor de atributo.

8.1.6.3 Lotes de operaciones

Esta clase de objeto gestionado sustenta los siguientes lotes condicionales:

– lote de identificadores de atributo;

– lote de modificación de atributo;

– lote de acciones; y

– lote de delimitador.

8.1.6.3.1 Lote de identificadores de atributo

El lote identificadores de atributo identifica atributos a los cuales se ha de controlar el acceso. Estará presente si el tipo de operación es obtención, sustitución, adición de valor, supresión de valor, sustitución con valor por defecto o filtro y no está presente si la operación es de cualquier otro tipo.

8.1.6.3.1.1 Atributos del lote de identificadores de atributo

El atributo lista de identificadores de atributo especificado en la Rec. X.721 del CCITT | ISO/CEI 10165-2 se incluye en este lote.

8.1.6.3.2 Lote de modificación de atributo

El lote de modificación de atributo identifica constricciones a la modificación de valores de atributo. Estará presente si el tipo de operación es sustitución, adición de valor, supresión de valor o creación y no está presente si la operación es de cualquier otro tipo.

8.1.6.3.2.1 Atributos del lote modificación de atributos

En este lote se incluye el atributo lista de filtros de atributos.

8.1.6.3.2.1.1 Lista de filtros de atributo

Este atributo de valor fijo identifica constricciones al valor de atributos en una petición de operación por medio de un conjunto de filtros CMIS (un filtro CMIS para cada atributo para el cual se especifican constricciones).

8.1.6.3.3 Lote de acciones

El lote de acciones identifica constricciones a los valores de información de acciones. Estará presente si el tipo de operación es acción y no estará presente si la operación es de cualquier otro tipo.

8.1.6.3.3.1 Atributos del lote de acciones

En este lote se incluye el atributo lista de filtros de acciones.

8.1.6.3.3.1.1 Lista de filtros de acciones

Este atributo de valor fijo identifica acciones y, facultativamente, constricciones a sus valores de argumento por medio de un filtro CMIS.

8.1.6.3.4 Lote de delimitador

El lote de delimitador identifica constricciones a los parámetros delimitador y sincronización de operaciones de gestión que comprenden selección de múltiples objetos. Estará presente si el tipo de operación es selección de múltiples objetos y no estará presente si la operación es de cualquier otro tipo.

NOTA – El lote de delimitador se puede utilizar, por ejemplo:

– para impedir la revelación de objetos gestionados o el acceso a los mismos durante una obtención delimitada de todo un subárbol, tal como se puede utilizar para explorar un sistema de una manera no autorizada;

– para proteger objetos gestionados dados contra supresión como parte de un subárbol, de modo que el objeto gestionado pueda ser suprimido por un determinado iniciador solamente si está direccionado directamente, nunca como parte de una supresión delimitada.

8.1.6.3.4.1 Atributos del lote de delimitador

Se definen los siguientes atributos para el lote de delimitador.

8.1.6.3.4.1.1 Filtro de delimitador

Para peticiones que seleccionan múltiples objetos gestionados, el filtro de delimitador especifica constricciones del parámetro delimitador de la petición y el identificador del atributo delimitador se utiliza (véase 8.1.5.1.3) para todos los ítems de filtro, en el filtro.

Si el filtro de delimitador no contiene ítems de filtro, todos los posibles valores del parámetro delimitador se considerarán como objetivos.

8.1.6.3.4.1.2 Filtro de sincronización

Para peticiones que seleccionan múltiples objetos gestionados, el filtro de sincronización especifica constricciones del parámetro sincronización de la petición y se utiliza el identificador de atributo de sincronización (véase 8.4.2) para todos los ítems de filtro, en el filtro. Si el filtro de sincronización no contiene ítems de filtro, todos los posibles valores del parámetro sincronización se considerarán como objetivos.

8.1.7 Iniciadores

La clase de objeto gestionado iniciadores identifica los iniciadores admisibles de operaciones de gestión.

8.1.7.1 Atributos de iniciadores

Se define el siguiente atributo obligatorio para la clase de objeto gestionado iniciadores.

8.1.7.1.1 ACI de iniciador impuesta

El atributo se utiliza para indicar si, para satisfacer el esquema de control de acceso en uso, se requiere la ACI de iniciador con cada petición de operación de gestión.

8.1.8 Iniciadores de ACL

La clase de objeto gestionado iniciadores de ACL contiene una lista de nombres u otras identidades que juntas forman una lista de control de acceso.

Múltiples objetos gestionados iniciadores de ACL pueden ser ejemplificados dentro de un objeto gestionado regla.

8.1.8.1 Atributos de iniciadores de ACL

Se define el siguiente atributo obligatorio para la clase de objeto gestionado iniciadores de ACL.

8.1.8.1.1 Lista de control de acceso

El atributo lista de control de acceso se utiliza para contener identidades de iniciadores a los que se permite o se les niega específicamente el acceso a la información de gestión.

8.1.9 Iniciadores de capacidades

El objeto gestionado iniciadores de capacidades contiene una lista de identidades.

Múltiples objetos gestionados iniciadores de capacidades se pueden ejemplificar dentro de un objeto gestionado regla.

8.1.9.1 Atributos de iniciadores de capacidades

Se define el siguiente atributo obligatorio para la clase de objeto gestionado iniciadores de capacidades.

8.1.9.1.1 Lista de identidades de capacidades

El atributo de lista de identidades de capacidades contiene un conjunto de identidades.

Las entidades pueden ser un nombre individual, nombre de grupo, nombre de cometido o nombre de aplicación, cada uno de los cuales puede estar asociado con un conjunto facultativo de pares de nombre de autoridad de dominio de seguridad y de tipo de operación; o la identidad puede estar en una forma no especificada en esta Recomendación | Norma Internacional.

8.1.10 Iniciadores de etiquetas

El objeto gestionado iniciadores de etiquetas se puede utilizar para especificar constricciones de operaciones de gestión que son adicionales a las constricciones de requerir una concordancia de compatibilidad entre la etiqueta de seguridad asociada con el iniciador y la etiqueta de seguridad asociada con el objetivo.

Si un objeto gestionado iniciadores de etiquetas está presente dentro de un objeto gestionado regla, las constricciones definidas por el objeto gestionado regla y por el objeto gestionado objetivos contenidos dentro de la misma regla serán adicionales a los requisitos de concordancia de compatibilidad de etiqueta de seguridad del esquema de control de acceso basado en etiqueta.

Si un objeto gestionado iniciadores de etiqueta no está presente dentro de un objeto gestionado reglas, no se imponen constricciones adicionales al acceso además de los requisitos de concordancia de compatibilidad de la etiqueta de seguridad del esquema de control de acceso basado en etiqueta.

Múltiples objetos gestionados iniciadores de etiqueta se pueden simplificar dentro de un objeto gestionado regla.

8.1.10.1 Atributos de iniciadores de etiqueta

Se define el siguiente atributo obligatorio para la clase de objeto gestionado iniciadores de etiqueta.

8.1.10.1.1 Etiqueta de seguridad

El atributo de etiqueta de seguridad contiene una etiqueta de seguridad.

8.1.11 Etiquetas asignadas

Este objeto gestionado es la raíz del subárbol que contiene los objetos gestionados tipo de etiqueta que, en combinación con relaciones precedentes, asignan una sola etiqueta de seguridad a objetivos. Además de proporcionar un objeto gestionado contenedor para los diferentes objetos gestionados tipo de etiqueta, este objeto gestionado proporciona una etiqueta de seguridad por defecto que se ha de asignar a elementos de gestión a los que no se ha asignado específicamente una etiqueta de seguridad.

8.1.11.1 Atributos de etiquetas asignadas

Se designan los siguientes atributos obligatorios para la clase de objeto gestionado de etiquetas asignadas.

8.1.11.1.1 Nombre de etiqueta

Este atributo se utiliza para identificar simplificaciones y especializaciones de la clase de objeto gestionado etiquetas asignadas.

8.1.11.1.2 Etiqueta de seguridad

Este atributo contiene la etiqueta de seguridad que se ha de asignar al objetivo.

8.1.12 Etiqueta de atributo

Este objeto gestionado se utiliza para asociar una sola etiqueta de seguridad a objetivos que son atributos específicos dentro de un objeto gestionado.

8.1.12.1 Atributos de etiquetas de seguridad

Se definen los siguientes atributos obligatorios para la clase de objeto gestionado etiqueta de atributo.

8.1.12.1.1 Caso de objeto gestionado

Este atributo se utiliza para identificar un objeto gestionado específico.

8.1.12.1.2 Lista de identificador de atributo

Este atributo se utiliza para identificar atributos específicos del objeto gestionado identificado por el atributo caso de objeto gestionado.

8.1.13 Etiqueta de caso

Este objeto gestionado se utiliza para asociar una sola etiqueta de seguridad a objetivos que son objetos gestionados individuales.

8.1.13.1 Atributos de etiqueta de caso

Se define el siguiente atributo obligatorio para la clase objeto gestionado etiqueta de caso.

8.1.13.1.1 Casos de objetos gestionados

Este atributo se utiliza para identificar una lista de objetivos específicos mediante su identificador de objeto gestionado.

8.1.14 Etiqueta de clase

Este objeto gestionado se utiliza para asociar una sola etiqueta de seguridad a objetivos que son clases de objetos gestionados.

8.1.14.1 Atributos de etiqueta de clase

Se define el siguiente atributo obligatorio para la clase de objeto gestionado de etiqueta de clase.

8.1.14.1.1 Clases de objeto gestionados

Este atributo se utiliza para identificar una lista de clases de objetos gestionados específicos.

8.2 Parámetros

8.2.1 Filtro de control de acceso inválido

Este error específico informa un error en un elemento de filtro de control de acceso propuesto. Su valor será una secuencia de un identificador de error, tomando uno de los valores duplicateId, heterogeneousId o invalidId y un filtro CMIS facultativo que contiene el filtro en error.

8.3 Vinculaciones de nombres

8.3.1 Regla – Regla de control de acceso

Esta vinculación de nombres proporciona reglas y especializaciones que han de estar contenidas dentro de reglas y especializaciones de control de acceso. El atributo nombre de objeto de control de acceso se utilizará para denominar las reglas. Los objetos gestionados reglas pueden ser creados por operación de gestión, con denominación automática y con objeto de referencia. Los objetos gestionados reglas pueden ser suprimidos por operación de gestión.

8.3.2 Operaciones – Objetivos

Esta vinculación de nombres proporciona objetos gestionados operaciones que han de estar contenidos dentro de objetos gestionados objetivos. El atributo tipo de operación se utilizará para denominar las operaciones. Los objetos gestionados operaciones pueden ser creados por operación de gestión y con objeto de referencia. Los objetos gestionados operaciones pueden ser suprimidos por operación de gestión.

8.3.3 Emisor de notificación – Regla de control de acceso

Esta vinculación de nombres proporciona un solo objeto gestionado emisor de notificación contenido dentro de un objeto gestionado reglas de control de acceso. El emisor de notificación puede ser creado, creado con objeto de referencia y suprimido por operación de gestión. Puede ser denominado automáticamente.

8.3.4 Etiqueta de atributo – Etiquetas asignadas

Esta vinculación de nombres proporciona que los objetos gestionados etiqueta de atributo estén contenidos dentro de objetos gestionados etiquetas asignadas. Los objetos gestionados de etiqueta de atributo pueden ser creados y suprimidos por operación de gestión.

8.3.5 Etiqueta de caso – Etiquetas asignadas

Esta vinculación de nombres proporciona que los objetos gestionados etiqueta de caso estén contenidos dentro de objetos gestionados etiquetas asignadas. Los objetos gestionados de etiqueta de caso pueden ser creados y suprimidos por operación de gestión.

8.3.6 Etiqueta de clase – Etiquetas asignadas

Esta vinculación de nombres proporciona que los objetos gestionados de etiqueta de clase estén contenidos dentro de objetos gestionados etiquetas asignadas. Los objetos gestionados etiqueta de clase pueden ser creados y suprimidos por operación de gestión.

8.4 Atributos

Los siguientes atributos no se definen para cualquier lote o clase de objetos gestionados pero se utilizan para especificar otros atributos y para el filtrado.

8.4.1 Filtro de control de acceso

Este atributo de valor fijo identifica constricciones del valor de los parámetros de operaciones de gestión. Cada elemento es un filtro CMIS, direccionado a un solo elemento de información de gestión. Cada elemento de información de gestión está direccionado en un elemento de este atributo, como máximo. Un conjunto vacío indica que todos los valores posibles son objetivos.

8.4.2 Sincronización

Este valor de atributo representa el parámetro sincronización de operaciones de gestión. Se utiliza para representar filtros de este parámetro.

8.5 Definiciones genéricas importadas

La presente Recomendación | Norma Internacional utiliza las siguientes definiciones genéricas de las Recomendaciones X.730 del CCITT | ISO/CEI 10164-1, X.731 del CCITT | ISO/CEI 10164-2, X.732 del CCITT | ISO/CEI 10164-3, X.734 del CCITT | ISO/CEI 10164-5, X.736 del CCITT | ISO/CEI 10164-7 y X.740 del CCITT | ISO/CEI 10164-8:

- lista de identificadores de atributo;
- notificación de cambio de valor de atributo;
- lote de situación de disponibilidad;
- contador;
- lote de planificación diaria;
- constructivo de discriminador;
- lote de duración;
- lote de planificación de planificador externo;

- miembro;
- caso de objeto gestionado;
- notificación de creación de objeto;
- notificación de supresión de objeto;
- violación operacional;
- violación del servicio o mecanismo de seguridad;
- informe de servicio;
- violación en el dominio del tiempo;
- informe de utilización; y
- lote de planificación semanal.

8.6 Cumplimiento

Las definiciones de clases de objetos gestionados sustentan las funciones definidas en la presente Recomendación | Norma Internacional incorporando la especificación de objetos gestionados, atributos y notificaciones definidos en la presente Recomendación | Norma Internacional y en las Recomendaciones X.721 del CCITT | ISO/CEI 10165-2, X.736 del CCITT | ISO/CEI 10164-7 y X.740 del CCITT | ISO/CEI 10164-8. El mecanismo de referencia se define en la Rec. X.722 del CCITT | ISO/CEI 10165-4.

9 Definición de servicios

9.1 Introducción

Se puede aplicar control de acceso a información de gestión. El control de acceso aplicado puede cambiar de acuerdo con el tiempo o por cambios de la política de control de acceso. Por consiguiente, es necesario proporcionar un mecanismo para administrar el servicio de control de acceso.

9.2 Servicio de control de acceso

Este servicio prevé la administración de las reglas de control de acceso utilizadas por un sistema.

El servicio permite que sean administrados objetos gestionados de las siguientes clases

- reglas de control de acceso; y
- reglas.

9.2.1 Iniciación de reglas de control de acceso

El servicio PT-CREACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema abierto que cree las clases de objetos gestionados enumeradas en 9.2.

9.2.2 Modificación de reglas de control de acceso

El servicio PT-FIJACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir que otro sistema abierto cambie los valores de atributos de las clases de objetos gestionados enumerados en 9.2.

9.2.3 Terminación de reglas de control de acceso

El servicio PT-SUPRESIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema que suprima las clases de objetos gestionados enumeradas en 9.2.

9.3 Servicio de administración de objetivos

Este servicio se utiliza para administrar los objetos gestionados objetivos que identifican la información de gestión protegida por el control de acceso.

9.3.1 Iniciación de objetivos de control de acceso

El servicio PT-CREACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema que cree clases de objetos gestionados objetivos.

9.3.2 Modificación de objetivos de control de acceso

El servicio PT-FIJACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir que otro sistema cambie los valores de los atributos de la clase de objeto gestionado objetivos.

9.3.3 Terminación de objetivos de control de acceso

El servicio PT-SUPRESIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema que suprima casos de la clases de objeto gestionado objetivos.

9.4 Servicio de administración de iniciadores

Este servicio se utiliza para administrar subclases de los objetos gestionados iniciadores.

9.4.1 Iniciación de iniciadores de control de acceso

El servicio PT-CREACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema que cree casos de subclases de la clase objeto gestionado iniciadores.

9.4.2 Modificación de iniciadores de control de acceso

El servicio PT-FIJACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir que otro sistema cambie los valores de atributos de subclases de la clase de objeto gestionado iniciadores.

9.4.3 Terminación de iniciadores de control de acceso

El servicio PT-SUPRESIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema que suprima subclases de casos de la clase de objeto gestionado iniciadores.

9.5 Servicio de administración de operaciones

Este servicio se utiliza para administrar los objetos gestionados operaciones.

9.5.1 Iniciación de operaciones de control de acceso

El servicio PT-CREACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema que cree casos de la clase objeto gestionado operaciones.

9.5.2 Modificación de operaciones de control de acceso

El servicio PT-FIJACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema que cambie los valores de atributo de la clase de objeto gestionado operaciones.

9.5.3 Terminación de operaciones de control de acceso

El servicio PT-SUPRESIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema abierto que suprima casos de la clase de objeto gestionado operaciones.

9.6 Servicio de administración de etiquetas

Este servicio se utiliza para administrar los objetos gestionados etiquetas asignadas, etiqueta de atributo, etiqueta de caso y etiqueta de clase.

9.6.1 Iniciación de operaciones de control de etiquetas

El servicio PT-CREACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema que cree casos de las clases de objeto gestionados etiquetas asignadas, etiqueta de atributo, etiqueta de caso y etiqueta de clase.

9.6.2 Modificación de operaciones de control de acceso

El servicio PT-FIJACIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir que otro sistema cambie los valores de los atributos de las clases de objetos gestionados etiquetas asignadas, etiqueta de atributo, etiqueta de caso y etiqueta de clase.

9.6.3 Terminación de operaciones de control de acceso

El servicio PT-SUPRESIÓN definido en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para que un sistema abierto pueda pedir a otro sistema que suprima casos de las clases de objeto gestionados etiquetas asignadas, etiqueta de atributo, etiqueta de caso y etiqueta de objeto.

9.7 Servicio de notificación de control de acceso

Este servicio permite que se transmitan informes de eventos pertinentes a la supervisión y administración de un servicio de control de acceso de un sistema abierto a otro. La función de informe de alarma de seguridad especificada en la Rec. X.736 del CCITT | ISO/CEI 10164-7 se utiliza para enviar informes de alarma y registros de pistas de auditoría de seguridad relacionados con tentativas de acceso ilegal a información de gestión, mientras que la función pista de auditoría de seguridad especificada en la Rec. X.740 del CCITT | ISO/CEI 10164-8 se utiliza para enviar informes relacionados con el uso general del servicio de control de acceso.

10 Unidades funcionales

Los objetos de atributos para función de control de acceso constituyen una sola unidad funcional de gestión de sistema.

11 Protocolo

11.1 Elementos de procedimiento

La presente Recomendación | Norma Internacional utiliza los elementos de procedimientos definidos en las Recomendaciones X.730 del CCITT | ISO/CEI 10164-1, X.736 del CCITT | ISO/CEI 10164-7 y X.740 del CCITT | ISO/CEI 10164-8 para los servicios descritos en la cláusula 9. No hay elementos de procedimiento específicos de esta Recomendación | Norma Internacional.

11.2 Sintaxis abstracta

11.2.1 Objetos gestionados

En el Cuadro 1 se muestra la relación entre los objetos gestionados de control de acceso y los objetos gestionados, cuya sintaxis abstracta se especifica en el Anexo A.

11.2.2 Atributos

El Cuadro 2 identifica la relación entre los atributos de control de acceso y los atributos de gestión cuya sintaxis abstracta se especifica en el Anexo A.

11.2.3 Grupos de atributos

No hay grupos de atributos definidos por esta función de gestión de sistema.

11.2.4 Acciones

No hay acciones definidas por esta función de gestión de sistema.

11.2.5 Notificaciones

No hay notificaciones definidas por esta función de gestión de sistema.

Cuadro 1 – Objetos gestionados

Objeto gestionado	Clase de objeto gestionado
Control de acceso	accessControl
Reglas de control de acceso	accessControlRules
Iniciadores de ACL	aclInitiators
Etiquetas asignadas	assignedLabels
Etiqueta de atributo	attributeLabel
Iniciadores de capacidades	capabilityInitiators
Etiqueta de clase	classLabel
Etiqueta de caso	instanceLabel
Iniciadores de etiqueta	labelInitiators
Emisor de notificaciones	notificationEmitter
Operaciones	operations
Reglas	rule
Objetivos	targets

11.2.6 Parámetros

El Cuadro 3 muestra la relación entre los parámetros de control de acceso y los parámetros de gestión cuya sintaxis abstracta se especifica en el Anexo A.

11.3 Negociación de unidades funcionales de control de acceso

Esta Especificación asigna el identificador de objeto:

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

como un valor del tipo ASN.1 **FunctionalUnitPackageId** definido en la Rec. X.701 del CCITT | ISO/CEI 10040 que se utiliza para negociar la siguiente unidad funcional:

0 unidad funcional control de acceso

donde el número identifica la posición de bit asignada a la unidad funcional y el nombre hace referencia a la unidad funcional definida en 10.

Dentro del contexto de aplicación de gestión de sistemas, el mecanismo para negociar la unidad funcional de control de acceso se describe en la Rec. X.701 del CCITT | ISO/CEI 10040.

NOTA – El requisito para negociar unidades funcionales es especificado por el contexto de aplicación.

12 Relación con otras funciones

Las notificaciones de creación de objeto y de supresión de objeto definidas en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utilizan para informar la creación y supresión, respectivamente, de casos de clases de objetos gestionados definidos en la presente Recomendación | Norma Internacional.

Cuadro 2 – Atributos de gestión

Atributo de control de acceso	Nombre de atributo
Filtro de control de acceso	accessControlFilter
Nombre de objeto de control de acceso	accessControlObjectName
Lista de filtros de acciones	actionFilterList
Lista de filtros de atributos	attributeFilterList
Contexto de autenticación	authenticationContext
Lista de identidades de capacidades	capabilityIdentitiesList
Acceso por defecto	defaultAccess
Respuesta de denegación por defecto	defaultDenialResponse
Granularidad de denegación	denialGranularity
Identidad de dominio	domainIdentity
Acción de imposición	enforcementAction
Filtro	filter
ACI de iniciador impuesta	initiatorACImandated
Lista de iniciadores	initiatorsList
Tentativas de acceso inválidas	invalidAccessAttempts
Nombre de etiqueta	labelName
Clases de objetos gestionados	managedObjectClasses
Casos de objetos gestionados	managedObjectInstances
Tipo de operación	operationType
Lista de operaciones	operationsList
Delimitador	scope
Filtro de delimitador	scopeFilter
Etiqueta de seguridad	securityLabel
Condiciones de estado	stateConditions
Sincronización	synchronization
Filtro de sincronización	synchronizationFilter
Lista de objetivos	targetsList
Tentativas de acceso válidas	validAccessAttempts

Cuadro 3 – Parámetros de gestión

Parámetros de control de acceso	Nombre de parámetro
Filtro de control de acceso inválido	invalidAccessControlFilter

La notificación de cambio de valor de atributo definida en la Rec. X.730 del CCITT | ISO/CEI 10164-1 se utiliza para informar cambios de valores de atributos en casos de los objetos gestionados definidos en la presente Recomendación | Norma Internacional.

Las notificaciones de violación operacional, violación de servicio o mecanismo de seguridad y violación en el dominio del tiempo definidas en la Rec. X.736 del CCITT | ISO/CEI 10164-7 se utilizan para informar alarmas de seguridad asociadas con la operación de los mecanismos de control de acceso.

Las notificaciones de informe de servicio y utilización de servicio definidas en la Rec. X.740 del CCITT | ISO/CEI 10164-8 se utilizan para transportar informes de pistas de autoría de seguridad asociados con la utilización de servicios y los mecanismos de control de acceso.

La gestión de información de control de acceso puede utilizar los siguientes servicios de gestión de sistemas definidos en la Rec. X.730 del CCITT | ISO/CEI 10164-1:

- PT-CREACIÓN;
- PT-SUPRESIÓN;
- PT-FIJACIÓN; y
- PT-OBTENCIÓN.

La política de seguridad puede estipular que estos servicios se utilicen por una asociación segura, de modo que la ACI esté protegida contra revelación o modificación no deseadas.

13 Conformidad

Las realizaciones que alegan conformarse con esta Recomendación | Norma Internacional cumplirán los requisitos de conformidad definidos en las subcláusulas siguientes.

13.1 Conformidad estática

La realización se ajustará a los requisitos de la presente Recomendación | Norma Internacional en el cometido de gestor, el cometido de agente, o ambos cometidos. Se alegará conformidad como mínimo con un cometido del Cuadro B.1.

Si se alega conformidad para soportar el cometido de gestor, la implementación deberá soportar como mínimo una notificación o una operación de gestión de, al menos, uno de los objetos gestionados especificados en la presente Recomendación | Norma Internacional. Los requisitos, de conformidad para dichas operaciones de gestión en el cometido de gestor se identifican en el Cuadro B.3 y en otros cuadros a los que se hace referencia en el Anexo B.

Si se alega conformidad para soportar el cometido de agente, la implementación deberá soportar uno o más ejemplares de la clase *access control rules managed object* identificada en el Cuadro B.4.

El sistema soportará la sintaxis abstracta derivada de las reglas de codificación especificadas en la Rec. X.209 del CCITT | ISO/CEI 8825 denominadas {joint-iso-ccitt asn1(1) basic encoding(1)} para los tipos de datos abstractos referenciados por las definiciones que se alega soportar.

13.2 Conformidad dinámica

Las realizaciones que alegan conformarse con la presente Recomendación | Norma Internacional admitirán los elementos de procedimiento de definiciones de semántica correspondientes a las definiciones que alegan soportar.

13.3 Requisito de conformidad de información de gestión

Cualquier formulario MCS, MICS, MOCS, MRCS y MIDS que se conforma con la presente Recomendación | Norma Internacional será técnicamente idéntico a los formularios especificados en los Anexos B, C, D, E y F conservando la numeración de los cuadros y el número de índice de los ítems, y difiriendo solamente en la paginación y encabezamiento de las páginas.

El suministrador de una realización que alega conformarse con la presente Recomendación | Norma Internacional rellenará un ejemplar del resumen de conformidad de gestión (MCS) que figura en el Anexo B como parte de los requisitos de conformidad, junto con otros formularios ICS referenciados como aplicables en ese MCS. Un formulario ICS que se conforma con la presente Recomendación | Norma Internacional:

- describirá una realización que se ajusta a la presente Recomendación | Norma Internacional;
- habrá sido rellenado de acuerdo con las instrucciones que figuran en la Rec. UIT-T X.724 | ISO/CEI 10165-6;
- contendrá la información necesaria para identificar de manera única al suministrador y a la realización.

Las alegaciones de conformidad con la información de gestión definida en la presente Recomendación | Norma Internacional en las clases de objetos gestionados definidas en otra parte incluirán los requisitos del formulario MIDS en el formulario MOCS para la clase de objetos gestionados.

Anexo A

Definición de información de gestión

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

A.1 Atribución de identificadores de objeto

Esta Recomendación | Norma Internacional atribuye los siguientes identificadores de objeto:

```
AccessControlDefinitions{ joint-iso-ccitt(2) ms(9) function(2) part9(9) asn1Module(2) 1 }

DEFINITIONS ::= BEGIN

        accessControl-Object OBJECT IDENTIFIER ::=
            { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) }

        accessControl-Package OBJECT IDENTIFIER ::=
            { joint-iso-ccitt(2) ms(9) function(2) part9(9) package (4) }

        accessControl-Parameter OBJECT IDENTIFIER ::=
            { joint-iso-ccitt(2) ms(9) function(2) part9(9) parameter(5) }

        accessControl-NameBinding OBJECT IDENTIFIER ::=
            { joint-iso-ccitt(2) ms(9) function(2) part9(9) nameBinding(6) }

        accessControl-Attribute OBJECT IDENTIFIER ::=
            { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) }

END
```

A.2 Definición de clases de objeto gestionado de control de acceso

A.2.1 Clase de objeto de control de acceso

La clase de objeto gestionado de control de acceso se utiliza para proporcionar una información común de cambio de atributo de denominación y de valor de atributo para objetos gestionados que representan información de control de acceso. No está prevista la instanciación.

```
accessControl  MANAGED OBJECT CLASS
        DERIVED FROM "CCITT Rec. X.721 | ISO/IEC 10165-2:1992": top;
        CHARACTERIZED BY accessControlPackage PACKAGE
            BEHAVIOUR accessControlBehaviour BEHAVIOUR
                DEFINED AS
                    ! The access control managed object class shall emit the object creation and object deletion
                    notifications. Specializations of the access control managed object class shall define the conditions
                    under which attribute value change notifications are to be emitted. ! ;;
            ATTRIBUTES          accessControlObjectName  GET;
            NOTIFICATIONS       "CCITT Rec. X.721 | ISO/IEC 10165-2:1992": attributeValueChange,
                                "CCITT Rec. X.721 | ISO/IEC 10165-2:1992": objectCreation,
                                "CCITT Rec. X.721 | ISO/IEC 10165-2:1992": objectDeletion;;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) accessControl(1) };
```

A.2.2 Reglas de control de acceso

La clase de objeto gestionado reglas de control de acceso (accessControlRules) se utiliza para definir una representación de las reglas de control de acceso. Se requiere un objeto gestionado reglas de control de acceso por función de decisión de acceso dentro de un dominio de seguridad.

```
accessControlRules MANAGED OBJECT CLASS
        DERIVED FROM accessControl;

        CHARACTERIZED BY accessControlRulesPackage PACKAGE
            BEHAVIOUR accessControlRulesBehaviour BEHAVIOUR
                DEFINED AS
                    ! An access control rules managed object may contain rule managed objects, each of which
                    represents a global or an item rule. It shall use those rules in the application of the procedures of 7.4
                    in accordance with the policy of the access control domain.
```

An attribute value change notification shall be emitted when any attribute of this object class is modified.

NOTE – An access control rules managed object may contain rule managed objects which are in conflict for a given initiator, target pair. The procedures of 7.4.3.1 ensure that the principle of least privilege applies.

! ;;

ATTRIBUTES

defaultAccess	**REPLACE-WITH-DEFAULT DEFAULT VALUE AccessControl-ASN1Module.denyAll GET-REPLACE,**
domainIdentity	**GET-REPLACE,**
denialGranularity	**GET-REPLACE,**
defaultDenialResponse	**GET-REPLACE;;;**

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) accessControlRules(2) };

A.2.3 Regla

rule MANAGED OBJECT CLASS
DERIVED FROM accessControl;
CHARACTERIZED BY rulePackage PACKAGE
BEHAVIOUR ruleBehaviour BEHAVIOUR
DEFINED AS

! Each rule identifies its nature - to grant or deny access. In the case where the enforcement action attribute has a value of allow, then access is permitted, else the enforcement action attribute defines the type of denial response made to the initiator of the management operation.

A rule managed object may include characteristics to represent a context for the rule.

One such context is a scheduling capability. When included, the scheduling packages control the value of the availability status attribute which shall exhibit the value { off duty } when the schedule requires that the rule not be available and the value {} otherwise.

Another context is the state of other managed objects. When included, the state conditions package identifies managed objects and filters upon their attributes. This rule shall only pertain if the managed objects exist and the filters evaluate to TRUE.

The initiator list attribute identifies initiator managed objects which identify initiators within the context of one or more access control schemes. If the list is empty, the rule shall apply to all initiators.

The targets list attribute identifies the target managed objects which specify the targets to which the rule pertains. If the list is empty, the rule is a global rule otherwise it is an item rule.

The creation and deletion of rules shall be signalled by object creation and object deletion notifications respectively.

An attribute value change notification shall be emitted when any attribute of this object class is modified. ! ;;

ATTRIBUTES

enforcementAction	**REPLACE-WITH-DEFAULT DEFAULT VALUE AccessControl-ASN1Module.denyAccess GET-REPLACE,**
initiatorsList	**GET-REPLACE ADD-REMOVE,**
targetsList	**GET-REPLACE ADD-REMOVE;;;**

CONDITIONAL PACKAGES

"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": availabilityStatusPackage
PRESENT IF ! Any of the scheduling packages (duration, daily, weekly, external) are present. !,

"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": duration
PRESENT IF ! The object is to be available from a specified start time, indefinitely or until aspecified stop time. !,

"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": dailyScheduling
PRESENT IF ! Both the weekly scheduling package and external scheduler package are not present and daily scheduling is supported. !,

"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": weeklyScheduling
PRESENT IF ! Both the daily scheduling package and external scheduler package are not present and weekly scheduling is supported. !,

"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": externalScheduler
PRESENT IF ! Both the daily scheduling package and weekly scheduling package are not present and external scheduling is supported. !,

stateConditionsPackage PACKAGE
BEHAVIOUR stateConditionsBehaviour BEHAVIOUR
DEFINED AS
! When this package is present in a rule managed object, the filters identified by the state conditions attribute shall be evaluated for the managed objects identified by that attribute. If the managed objects are not available or the filters evaluates to FALSE then the rule shall evaluate to FALSE. If the filters evaluate to TRUE, then the rule shall evaluate to TRUE. ! ;;
ATTRIBUTES stateConditions GET-REPLACE ADD-REMOVE;
REGISTERED AS
{ joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) stateConditionsPackage(1) };
PRESENT IF ! The state of another managed object provides a context for this rule. !,

authenticationContextPackage PACKAGE
BEHAVIOUR authenticationContextBehaviour BEHAVIOUR
DEFINED AS
! When this package is present in a rule managed object, then the authentication requirements specified by the authentication context attribute shall be satisfied before any further evaluation of the access rights of an initiator is performed.

If the authentication requirements are not satisfied, then the rule shall evaluate to FALSE. ! ;;
ATTRIBUTES authenticationContext GET-REPLACE;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) (2) };
PRESENT IF ! The authentication context is required. !;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) rule(3) };

A.2.4 Emisor de notificación

notificationEmitter MANAGED OBJECT CLASS
DERIVED FROM accessControl;
CHARACTERIZED BY accessControlNotificationEmitterPkg PACKAGE
BEHAVIOUR accessControlNotificationEmitterDefinition BEHAVIOUR
DEFINED AS
! This managed object class enables an access control scheme to report on potential or actual attacks on the security of management applications and management information. An instance of this managed object class shall support at least one of the conditional packages defined below. ! ;;;
CONDITIONAL PACKAGES

securityViolationAlarmPkg PACKAGE
BEHAVIOUR securityViolationAlarmBehaviour BEHAVIOUR
DEFINED AS
! 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. ! ;;
NOTIFICATIONS
"Rec. X.721 | ISO/IEC 10165-2:1992": securityServiceOrMechanismViolation;

REGISTERED AS
{ joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) securityViolationAlarmPkg(3) };
PRESENT IF ! the security policy requires that this security alarm type shall be emitted if the access control checks fail. !,

timeViolationAlarmPkg PACKAGE
BEHAVIOUR timeViolationAlarmBehaviour BEHAVIOUR
DEFINED AS
! 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. ! ;;

NOTIFICATIONS
"Rec. X.721 | ISO/IEC 10165-2:1992": timeDomainViolation;
REGISTERED AS
{ joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) timeViolationAlarmPkg(4) };
PRESENT IF ! the security policy requires that this security alarm type shall be emitted when either out of hours activity is detected or an expired key has been used. !,

operationalViolationAlarmPkg PACKAGE
BEHAVIOUR operationalViolationAlarmBehaviour BEHAVIOUR
DEFINED AS
! 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. ! ;;
NOTIFICATIONS
"Rec. X.721 | ISO/IEC 10165-2:1992": operationalViolation;
REGISTERED AS
{ joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) operationalViolationAlarmPkg(5) };
PRESENT IF ! the security policy requires that this security alarm type shall be emitted when either the access control mechanism is unavailable or the security policy identifies further causes. !,

accessControlUsagePkg PACKAGE
BEHAVIOUR accessControlUsagePkgBehaviour BEHAVIOUR
DEFINED AS
! 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. ! ;;
ATTRIBUTES
validAccessAttempts,
invalidAccessAttempts;
NOTIFICATIONS
"Rec. X.740 | ISO/IEC 10164-8:1992": usageReport;
REGISTERED AS
{ joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) accessControlUsagePkg(6) };
PRESENT IF ! the security policy requires that the number of valid and invalid access attempts are logged. !,

accessControlServiceReportPkg PACKAGE
BEHAVIOUR accessControlServiceReportPkgBehaviour BEHAVIOUR
DEFINED AS
! This package allows security audit trail notifications of type 'service report' to be emitted for possible inclusion in a security audit trail log. ! ;;
NOTIFICATIONS
"Rec. X.740 | ISO/IEC 10164-8:1992": serviceReport;
REGISTERED AS
{ joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) accessControlServiceReportPkg(7) };
PRESENT IF ! the security policy requires that service reports are logged. !;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) notificationEmitter(4) };

A.2.5 Objetivos

La clase de objeto gestionado objetivos se utiliza para identificar los objetos gestionados a los cuales el acceso está controlado.

targets MANAGED OBJECT CLASS
DERIVED FROM accessControl;
CHARACTERIZED BY targetsPackage PACKAGE
BEHAVIOUR targetsBehaviour BEHAVIOUR
DEFINED AS
! Targets identify managed objects within the security domain. These managed objects are identified according to the following rules:

a) all managed objects within the security domain and belonging to the managed object classes identified by the managed object classes attribute are identified with specified name bindings;

b) all managed objects within the security domain identified explicitly by the managed object instances attribute are identified;

c) each managed object selected according to a) and b) shall be regarded as a base managed object for selecting managed objects according to the scope and filter attributes; and

d) all managed objects selected according to c) shall be regarded as the target managed objects.

Unless the targets managed object contains operations managed objects, the targets managed object identifies all operations upon the selected managed objects.

An attribute value change notification shall be emitted when any attribute of this managed object is modified. ! ;;

ATTRIBUTES
managedObjectClasses GET-REPLACE ADD-REMOVE,
managedObjectInstances GET-REPLACE ADD-REMOVE,
scope GET-REPLACE,
filter GET-REPLACE;;;
CONDITIONAL PACKAGES
operationsListPackage PACKAGE
BEHAVIOUR operationsListPackBehav BEHAVIOUR
DEFINED AS
! This package provides support for the operations list attribute as an alternative to the operations managed object. It may only be included in the targets managed object if the targets managed object contains no instantiation of the operations managed object.
! ;;
ATTRIBUTES
operationsList GET-REPLACE ADD-REMOVE;;
REGISTERED AS
{ joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) operationsListPackage(15) }
PRESENT IF ! No contained Operations object !

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) targets(5) };

A.2.6 Operaciones

Las instanciaciones del objeto gestionado operaciones identifican las operaciones que pueden realizarse sobre la información de gestión especificada (identificada por el objeto gestionado objetivos).

operations MANAGED OBJECT CLASS
DERIVED FROM "CCITT Rec. X.721 | ISO/IEC 10165-2 :1992": top;
CHARACTERIZED BY operationsPackage PACKAGE
BEHAVIOUR operationsBehaviour BEHAVIOUR
DEFINED AS
! The operations managed object identifies constraints on operation types for managed objects identified by the containing targets managed object.

The operation type is specified by the operation type attribute, which is also the naming attribute for the operations managed object class.

The constraints on the operation type, some of which are peculiar to the operation type, are specified by other attributes contained in conditional packages.

When a target managed object identifies the managed object specified in the access request, and contains one or more operations managed objects, then an access request shall satisfy the following conditions for the containing rule to be satisfied:

a) the access request matches the operation type for one of the operations managed objects contained in the target; and

b) the constraints specified for the operation type are satisfied.

The operations managed object shall emit the object creation notification when it it is created and the object deletion notification when it is deleted. An attribute value change notification shall be emitted when any attribute of this managed object class is modified. ! ;;
ATTRIBUTES
operationType GET;

NOTIFICATIONS
"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": attributeValueChange,
"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": objectCreation,
"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": objectDeletion;;;

CONDITIONAL PACKAGES

attributeIdsPackage PACKAGE
BEHAVIOUR attributeIdsBehaviour BEHAVIOUR
DEFINED AS
! The attributes identified by the attribute identifier list attribute shall be part of the target. If the attribute identifier list attribute is empty, then all attributes shall be part of the target for the identified operation for the managed objects identified by the containing targets managed object. ! ;;
ATTRIBUTES "CCITT Rec. X.721 | ISO/IEC 10165-2:1992": attributeIdentifierList
GET-REPLACE ADD-REMOVE;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) attributeIdsPackage(8) };
PRESENT IF ! operation type is get, replace with default or filter !,

attributeModificationPackage PACKAGE
BEHAVIOUR attributeModificationBehaviour BEHAVIOUR
DEFINED AS
! The attribute values identified by the attribute filter list attribute shall be part of the target. If the attribute filter list attribute is empty, then all attributes and their values shall be part of the target for the identified operation for the managed objects identified by the containing targets managed object. If the attribute filter list attribute identifies an attribute without constraining its value, then all values of that attribute shall be part of the target for the identified operation for the managed objects identified by the containing targets managed object. ! ;;
ATTRIBUTES
attributeFilterList GET-REPLACE ADD-REMOVE;
REGISTERED AS
{ joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) attributeModificationPackage(9) };
PRESENT IF ! operation type is replace, add, remove or create !,

actionsPackage PACKAGE
BEHAVIOUR actionsBehaviour BEHAVIOUR
DEFINED AS
! The action values identified by the action filter list attribute shall be part of the target. If the action filter list attribute is empty, then all actions and their information values shall be part of the target for the identified operation for the managed objects identified by the containing targets managed object. If the action filter list attribute identifies an action without constraining its information value, then all values of that action information shall be part of the target for the identified operation for the managed objects identified by the containing targets managed object.

NOTE – For the purposes of filtering, parameters of actions may be identified as attributes using the parameter template defined in CCITT Rec. X.722 | ISO/IEC 10165-4.

! ;;
ATTRIBUTES
actionFilterList GET-REPLACE ADD-REMOVE;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) actionsPackage(10) };
PRESENT IF ! operation type is action !,

scopePackage PACKAGE
BEHAVIOUR scopeBehaviour BEHAVIOUR
DEFINED AS
! The scope and synchronization values identified by the scope and synchronization attributes shall be part of the target. ! ;;
ATTRIBUTES
scopeFilter GET-REPLACE,
synchronizationFilter GET-REPLACE;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) scopePackage(11) };
PRESENT IF ! operation type is multiple object selection !;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) operations(6) };

A.2.7 Iniciadores

La clase de objeto gestionado iniciadores se utiliza para identificar un conjunto de posibles solicitantes de operación. El medio exacto de identificar a los iniciadores depende de la política de seguridad. La clase de objeto gestionado iniciadores no está prevista para instanciación, pero está prevista para especialización con el fin de que los solicitantes de operación puedan ser identificados de conformidad con una política de seguridad dada. Se recomienda que todos los lotes que proporcionan atributos para identificar a los solicitantes estén registrados, de manera que el atributo lotes pueda utilizarse para identificar la política.

```
initiators MANAGED OBJECT CLASS
        DERIVED FROM accessControl;
        CHARACTERIZED BY initiatorsPackage PACKAGE
            BEHAVIOUR initiatorsBehaviour BEHAVIOUR
                DEFINED AS
                    ! Initiators identify individual requestors of management operations in accordance with the
                    applicable access control schemes. The diversity of possible schemes prohibits a single
                    representation of initiators. Specializations of the initiators managed object class provide attributes
                    to identify requestors in accordance with given access control schemes.

                    Where a specialization identifies more than one access control scheme, it shall also contain
                    behaviour to resolve conflicts of rights associated with the different schemes. ! ;;
            ATTRIBUTES
                initiatorACImandated    REPLACE-WITH-DEFAULT
                                        DEFAULT VALUE AccessControl-ASN1Module.false
                                        GET-REPLACE;;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) initiators(7) };
```

A.2.8 Iniciadores de ACL

```
aclInitiators MANAGED OBJECT CLASS
        DERIVED FROM initiators;
        CHARACTERIZED BY aclPackage PACKAGE
            BEHAVIOUR aclInitiatorsBehaviour BEHAVIOUR
                DEFINED AS
                    ! This managed object class is used to support an ACL based access control scheme.

                    The ACL initiators managed object class contains a list of names or other identities that together
                    form an access control list. The identity of a management operation requestor shall be matched with
                    the entries of an access control list to evaluate whether the requestor is an authorized initiator.

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

                    An attribute value change notification shall be emitted when any attribute of this object class is
                    modified. ! ;;
            ATTRIBUTES
                accessControlList       GET-REPLACE ADD-REMOVE;
        REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) aclPackage(12) };;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) aclInitiators(8) };
```

A.2.9 Iniciadores de capacidad

```
capabilityInitiators MANAGED OBJECT CLASS
        DERIVED FROM initiators;
        CHARACTERIZED BY capabilityPackage PACKAGE
            BEHAVIOUR capabilityInitiatorsBehaviour BEHAVIOUR
                DEFINED AS
                    ! The capability initiators managed object class contains a list of identities that are used to
                    determine whether the security capability associated with the access request is allowed to be used by
                    the initiator of the request.

                    The identity associated with the access request is matched with the contents of the capability identity
                    list attribute to evaluate whether the security capability associated with the access request is allowed
                    to be used by the initiator of the request.
```

The identities may be an individual name, group name, role name, or application name 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 unspecified within this Recommendation | International Standard.

NOTE – When a capability scheme is used, rule managed objects that specify deny permission are not required. The absence of the identity in the capability identities list attribute results in the capability not being valid. In addition, targets managed objects and associated operations managed objects are not required, unless further access constraints are required to enforce local security policy refinements of the containing security domain policy.

An attribute value change notification shall be emitted when any attribute of this object class is modified. ! ;;

ATTRIBUTES

capabilityIdentitiesList GET-REPLACE;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) capabilityPackage(13) };;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) capabilityInitiators(9) };

A.2.10 Iniciadores de etiqueta

labelInitiators MANAGED OBJECT CLASS

DERIVED FROM initiators;

CHARACTERIZED BY labelPackage PACKAGE

BEHAVIOUR labelInitiatorsBehaviour BEHAVIOUR

DEFINED AS

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

Access shall be granted or denied to an initiator in accordance with the containing rule only if the initiator's security label is a member of the set of security labels identified by the security label attribute, the operation on the target conforms to the conditions specified by the relevant targets managed object and operations managed objects associated with the rule, and the security label of the initiator is compatible with the security label assigned to the target.

NOTE – Association of a security label with a target must have occurred prior to the use of that label in the above procedure. Security labels are associated with targets using the assigned labels, attribute label, instance label, and class label managed objects and associated procedures described in 7.4.

An attribute value change notification shall be emitted when any attribute of this object class is modified. ! ;;

ATTRIBUTES

securityLabel GET-REPLACE;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) labelPackage(14) };;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) labelInitiators(10) };

A.2.11 Etiquetas asignadas

assignedLabels MANAGED OBJECT CLASS

DERIVED FROM top;

CHARACTERIZED BY assignedLabelsPackage PACKAGE

BEHAVIOUR assignedLabelsPkgBehav BEHAVIOUR

DEFINED AS

! This managed object contains the attribute label, instance label and class label managed objects that, in combination with precedence relationships, assign a single security label to targets.

There shall be only one managed object of this class per access control decision function.

To assure association of a single security label with a target, a precedence relationship is specified between and within attribute label, instance label and class label managed objects classes as follows:

– Between class precedence relationships

Attribute label managed object > instance label managed object > object label managed object

– Within class precedence relationships.

All attribute label, instance label, and class label managed objects shall be considered to be ordered within their respective managed object class according to the value of the naming attribute for the managed object.

The value of the security label attribute within the attribute label, instance label, or class label managed object which references the target, either directly or indirectly, has the greatest class precedence, and is first in the lexicographical order within the class, shall be associated with the target.

If a security label is not associated with a target by an attribute label, instance label, or class label managed object, the default security label contained in the security label attribute of this managed object shall be associated with the target.

The assigned labels managed object class shall emit the object creation notification when a managed object of this class is created, and shall emit the object deletion notification when a managed object of this class is deleted. An attribute value change notification shall be emitted when any attribute of this managed object class is modified. !;;

ATTRIBUTES
labelName GET,
securityLabel GET;
NOTIFICATIONS "CCITT Rec. X.721 | ISO/IEC 10165-2:1992": attributeValueChange,
"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": objectCreation,
"CCITT Rec. X.721 | ISO/IEC 10165-2:1992": objectDeletion;;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) assignedLabels(11) };

A.2.12 Etiqueta de atributo

attributeLabel MANAGED OBJECT CLASS
DERIVED FROM assignedLabels;
CHARACTERIZED BY attributeLabelPackage PACKAGE
BEHAVIOUR attributeLabelPkgBehav BEHAVIOUR
DEFINED AS
! This managed object associates a security label with specific attributes within a managed object.

The security label is the value contained in the security label attribute.

The attributes are the values contained in the attribute identifier list attribute.

The managed object is the value contained in the managed object instance attribute.

There may be multiple managed objects of this class contained within an assigned labels managed object.

The behaviour of attribute label managed objects relative to others within its class, and managed objects within the instance label and class label managed object classes, shall be as defined in the assigned labels managed object behaviour. ! ;;
ATTRIBUTES
"CCITT Rec. X.721 | ISO 10165-2:1992": managedObjectInstance GET,
"CCITT Rec. X.721 | ISO 10165-2:1992": attributeIdentifierList GET;;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) attributeLabel(12) };

A.2.13 Etiqueta de instancia

instanceLabel MANAGED OBJECT CLASS
DERIVED FROM assignedLabels;
CHARACTERIZED BY instanceLabelPackage PACKAGE
BEHAVIOUR instanceLabelPkgBehav BEHAVIOUR
DEFINED AS
! This managed object associates a security label with specific managed objects.

The security label is the value contained in the security label attribute.

The managed object identifiers are contained in the managed object instances attribute.

There may be multiple managed objects of this class contained within an assigned labels managed object.

The behaviour of instance label managed objects relative to others within its class, and managed objects within the attribute label and class label managed object classes, shall be as defined in the assigned labels managed object behaviour. ! ;;
ATTRIBUTES
managedObjectInstances GET;;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) instanceLabel(13) };

A.2.14 Etiqueta de clase

```
classLabel MANAGED OBJECT CLASS
        DERIVED FROM assignedLabels;
        CHARACTERIZED BY  classLabelPackage  PACKAGE
            BEHAVIOUR  classLabelPkgBehav BEHAVIOUR
                DEFINED AS
                    ! This managed object associates a security label with specific managed object classes.

                    The security label is the value contained in the security label attribute.

                    The managed object class identifiers are contained in the managed object classes attribute.

                    There may be multiple managed objects of this class contained within an assigned labels managed
                    object.

                    The behaviour of class label managed objects relative to others within its class, and managed objects
                    within the attribute label and instance label managed object classes, shall be as defined in the
                    assigned labels managed object behaviour.  ! ;;
        ATTRIBUTES
            managedObjectClasses        GET;;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) managedObjectClass(3) classLabel(14) };
```

A.3 Definición de vinculaciones de nombre

A.3.1 Regla – Regla de control de acceso

```
rule-accessControlRules NAME BINDING
        SUBORDINATE OBJECT CLASS  rule AND SUBCLASSES;
        NAMED BY
            SUPERIOR OBJECT CLASS  accessControlRules AND SUBCLASSES;
            WITH ATTRIBUTE         accessControlObjectName;
        CREATE WITH-AUTOMATIC-INSTANCE-NAMING, WITH-REFERENCE-OBJECT;
        DELETE ONLY-IF-NO-CONTAINED-OBJECTS;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) nameBinding(6) rule-accessControlRules(1) };
```

A.3.2 Operaciones – Objetivos

```
operations-targets NAME BINDING
        SUBORDINATE OBJECT CLASS  operations AND SUBCLASSES;
        NAMED BY
            SUPERIOR OBJECT CLASS  targets AND SUBCLASSES;
            WITH ATTRIBUTE         operationType;
        CREATE WITH-REFERENCE-OBJECT;
        DELETE ONLY-IF-NO-CONTAINED-OBJECTS;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) nameBinding(6) operations-targets(2) };
```

A.3.3 Emisor de notificación – Reglas de control de acceso

```
notificationEmitter-accessControlRules NAME BINDING
        SUBORDINATE OBJECT CLASS  notificationEmitter AND SUBCLASSES;
        NAMED BY
            SUPERIOR OBJECT CLASS  accessControlRules AND SUBCLASSES;
            WITH ATTRIBUTE         accessControlObjectName;
        CREATE WITH-AUTOMATIC-INSTANCE-NAMING;
        DELETE ONLY-IF-NO-CONTAINED-OBJECTS;
REGISTERED AS
   { joint-iso-ccitt(2) ms(9) function(2) part9(9) nameBinding(6) notificationEmitter-accessControlRules(3) };
```

A.3.4 Etiqueta de atributo – Etiquetas asignadas

```
attributeLabel-assignedLabels NAME BINDING
        SUBORDINATE OBJECT CLASS  attributeLabel AND SUBCLASSES;
        NAMED BY
            SUPERIOR OBJECT CLASS  assignedLabels AND SUBCLASSES;
            WITH ATTRIBUTE         labelName;
        CREATE;
        DELETE ONLY-IF-NO-CONTAINED-OBJECTS;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) nameBinding(6) attributeLabel-assignedLabels(4) };
```

A.3.5 Etiqueta de instancia – Etiquetas asignadas

```
instanceLabel-assignedLabels NAME BINDING
        SUBORDINATE OBJECT CLASS  instanceLabel AND SUBCLASSES;
        NAMED BY
            SUPERIOR OBJECT CLASS  assignedLabels AND SUBCLASSES;
            WITH ATTRIBUTE         labelName;
        CREATE;
        DELETE;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) nameBinding(6) instanceLabel-assignedLabels(5) };
```

A.3.6 Etiqueta de clase – Etiquetas asignadas

```
classLabel-assignedLabels NAME BINDING
        SUBORDINATE OBJECT CLASS  classLabel AND SUBCLASSES;
        NAMED BY
            SUPERIOR OBJECT CLASS  assignedLabels AND SUBCLASSES;
            WITH ATTRIBUTE         labelName;
        CREATE;
        DELETE;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) nameBinding(6) classLabel-assignedLabels(6) };
```

A.4 Definición de parámetros

A.4.1 Filtro de control de aceso inválido

```
invalidAccessControlFilter PARAMETER
        CONTEXT SPECIFIC-ERROR;
            WITH SYNTAX AccessControlDefinitions.InvalidAccessControlFilter;
                BEHAVIOUR  invalidAccessControlFilterBehaviour  BEHAVIOUR
                    DEFINED AS
                        ! This CMIS processing failure 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.  ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) parameter(5) invalidAccessControlFilter(1) };
```

A.5 Definición de atributos

A.5.1 Lista de control de acceso

```
accessControlList ATTRIBUTE
        WITH ATTRIBUTE SYNTAX  AccessControlDefinitions.AccessControlList;
        MATCHES FOR EQUALITY, SET-COMPARISON, SET-INTERSECTION;
        BEHAVIOUR aclBehaviour BEHAVIOUR
            DEFINED AS
                ! This attribute is used to specify a list of initiators for use in an access control list based scheme.
                Initiators are identified by individual name, anonymous reference or by group name, roles or application
                entity titles. Initiators may be associated with specified applications. Individual group names may be used
                in conjunction with the OSI Directory.

                The attribute enables either an initiator name or a proxy name to be used. The initiator name form may
                be syntactically either a distinguished name or an application entity title, whilst the proxy name takes the
                form of an object identifier and value.

                The distinguished name form may be used either to identify a specific initiator, a group of initiators or a
                particular role.

                The application entity title name form identifies the application entity title, and by reference the system
                that initiated the request.

                The proxy name form is used when the name form is not a specific initiator, a group of initiators, a role
                or an application entity title. The proxy therefore allows the initiator to be anonymous.  ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) accessControlList(1) };
```

A.5.2 Filtro de control de acceso

El atributo siguiente se define a efectos de herencia.

```
accessControlFilter ATTRIBUTE
        WITH ATTRIBUTE SYNTAX AccessControlDefinitions.FilterList;
        MATCHES FOR EQUALITY, SET-COMPARISON, SET-INTERSECTION;
        BEHAVIOUR accessControlFilterBehaviour BEHAVIOUR
            DEFINED AS
                ! This set-valued attribute provides a set of CMIS filters for constraining the parameters of management
                operations. If the set is empty, the CMIS filter shall be regarded as identifying all possible targets
                identifiable by the derived attribute.

                For any given CMIS filter of the set, every CMIS filter item shall identify the same attribute. Attempts to
                violate this constraint shall result in the invalid access control filter specific error with error identifier of
                heterogenousIds.

                No attribute shall be associated with more than one CMIS filter. Attempts to violate this constraint
                shall result in the invalid access control filter specific error with error identifier of duplicateIds.

                All values of the attribute identifier fields of CMIS filter items shall identify management information
                that is valid for the given specialization of this attribute. Any violation shall result in the invalid access
                control filter specific error with the error identifier of invalid identifier. ! ;;
        PARAMETERS invalidAccessControlFilter;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) accessControlFilter(2) };
```

A.5.3 Nombre de objeto de control de acceso

```
accessControlObjectName ATTRIBUTE
        WITH ATTRIBUTE SYNTAX AccessControlDefinitions.AccessControlObjectName;
        MATCHES FOR EQUALITY, SUBSTRINGS;
        BEHAVIOUR accessControlObjectNameBehaviour  BEHAVIOUR
            DEFINED AS
                ! This attribute is used to identify instantiations of specializations of the access control managed object
                class. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) accessControlObjectName(3) };
```

A.5.4 Lista de filtros de acción

```
actionFilterList ATTRIBUTE
        WITH ATTRIBUTE SYNTAX AccessControlDefinitions.ActionFilterList;
        MATCHES FOR EQUALITY,  SET-INTERSECTION,  SET-COMPARISON;
        BEHAVIOUR actionFilterlistBehaviour BEHAVIOUR
            DEFINED AS
                ! This set-valued attribute identifies actions and, optionally, constraints upon their argument values by
                means of a CMIS filter.

                For any given CMIS filter of the set, every CMIS filter item shall identify the same attribute. Attempts to
                violate this constraint shall result in the invalid access control filter specific error with error identifier of
                heterogenousIds.

                No attribute shall be associated with more than one CMIS filter. Attempts to violate this constraint shall
                result in the invalid access control filter specific error with error identifier of duplicateIds.

                All values of the attribute identifier fields of CMIS filter items shall identify management information
                that is valid for the given specialization of this attribute. Any violation shall result in the invalid access
                control filter specific error with the error identifier of invalid identifier. ! ;;
        PARAMETERS  invalidAccesscontrolFilter;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) actionFilterList(4) };
```

A.5.5 Lista de filtros de atributo

```
attributeFilterList ATTRIBUTE
        DERIVED FROM accessControlFilter;
        BEHAVIOUR attributeFilterListBehaviour BEHAVIOUR
            DEFINED AS
```

! This attribute identifies constraints upon the values of attributes.

If an attribute is identified without constraints upon its value e.g.

{ item : present : globalForm : accessControlList }

Then all values of the attribute are identified.

If the set is empty, then there are no constraints. ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) attributeFilterList(5) };

A.5.6 Contexto de autenticación

authenticationContext ATTRIBUTE
WITH ATTRIBUTE SYNTAX AccessControlDefinitions.AuthenticationContext;
BEHAVIOUR authenticationContextPackageBehaviour BEHAVIOUR
DEFINED AS
! The authentication context attribute is a sequence of authentication policy identifier and the requirements identified thereby. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) authenticationContext(6) };

A.5.7 Lista de identidades de capacidad

capabilityIdentitiesList ATTRIBUTE
WITH ATTRIBUTE SYNTAX AccessControlDefinitions.CapabilityIdentitiesList;
MATCHES FOR EQUALITY, SET-COMPARISON, SET-INTERSECTION;
BEHAVIOUR capabilityBehaviour BEHAVIOUR
DEFINED AS
! 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 unspecified within this Recommendation | International Standard. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) capabilityIdentitiesList(7) };

A.5.8 Acceso por defecto

defaultAccess ATTRIBUTE
WITH ATTRIBUTE SYNTAX AccessControlDefinitions.DefaultAccess;
MATCHES FOR EQUALITY;
BEHAVIOUR defaultAccessBehaviour BEHAVIOUR
DEFINED AS
! The default access attribute identifies, in accordance with 7.4.3.1.6, the default access rights for each operation type. Its value is a sequence enumerating the enforcement action for each operation type. The default value of the attribute shall be to deny all operations with the access denied response. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) defaultAccess(8) };

A.5.9 Respuesta de negación por defecto

defaultDenialResponse ATTRIBUTE
WITH ATTRIBUTE SYNTAX AccessControlDefinitions.DenialResponse;
MATCHES FOR EQUALITY;
BEHAVIOUR denialResponseBehaviour BEHAVIOUR
DEFINED AS
! This attribute defines the denial response to be returned in the event that the denial has been made as a result of the default rule having been satisfied. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) defaultDenialResponse(9) };

A.5.10 Granularidad de negación

denialGranularity ATTRIBUTE
WITH ATTRIBUTE SYNTAX AccessControlDefinitions.DenialGranularity;
MATCHES FOR EQUALITY;
BEHAVIOUR denialGranularityBehaviour BEHAVIOUR
DEFINED AS
! This attribute identifies the level at which denial of access shall be exhibited, if at all. It shall take one of the values request, object, and attribute. If the value is request, then the entire request shall be denied if any target in that request is denied. If the value is object, then the request for that managed object shall

be denied if any target within the request for that object is denied. If the value is attribute, then the request shall be denied at the attribute level. ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) denialGranularity(10) };

A.5.11 Identidad de dominio

domainIdentity ATTRIBUTE

WITH ATTRIBUTE SYNTAX AccessControlDefinitions.DomainIdentity;

MATCHES FOR EQUALITY;

BEHAVIOUR domainNameBehaviour BEHAVIOUR

DEFINED AS

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

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) domainIdentity(11) };

A.5.12 Acción de imposición

enforcementAction ATTRIBUTE

WITH ATTRIBUTE SYNTAX AccessControlDefinitions.EnforcementAction;

MATCHES FOR EQUALITY;

BEHAVIOUR enforcementActionBehaviour BEHAVIOUR

DEFINED AS

! This attribute identifies the action to be taken by the enforcement function if the rule is satisfied. It shall take one of the values, deny with response (the default value), deny without response, abort association, deny with false response and allow. ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) enforcementAction(12) };

A.5.13 Filtro

filter ATTRIBUTE

DERIVED FROM "CCITT Rec. X.721 | ISO/IEC 10165-2:1992": discriminatorConstruct;

BEHAVIOUR filterBehaviour BEHAVIOUR

DEFINED AS

! 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. ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) filter(13) };

A.5.14 ACI de iniciador obligatoria

initiatorACImandated ATTRIBUTE

WITH ATTRIBUTE SYNTAX AccessControlDefinitions.Boolean;

MATCHES FOR EQUALITY;

BEHAVIOUR initiatorACImandatedBehaviour BEHAVIOUR

DEFINED AS

! The initiator ACI mandated attribute is of type boolean. 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. An attribute value of TRUE indicates that initiator ACI is required in each management operation request, whilst a value of FALSE indicates that no initiator ACI is required. In the event that the attribute has a value of TRUE and the management operation request does not contain initiator ACI, then access will be denied. ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) initiatorACImandated(14) };

A.5.15 Lista de iniciadores

initiatorsList ATTRIBUTE

DERIVED FROM "CCITT Rec. X.721 | ISO/IEC 10165-2:1992": member;

BEHAVIOUR initiatorsListBehaviour BEHAVIOUR

DEFINED AS

! This set-valued attribute identifies the sub-classes of initiator managed objects which specify the initiators to which the rule pertains. It shall be an error to attempt to include a value in the initiators list attribute that is not the name of an initiators managed object. ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) initiatorsList(15) };

A.5.16 Intentos de acceso inválidos

```
invalidAccessAttempts  ATTRIBUTE
        DERIVED FROM "Rec. X.721 | ISO/IEC 10165-2:1992": counter;
        BEHAVIOUR invalidAccessAttemptBehaviourPkg  BEHAVIOUR
            DEFINED AS
                ! This attribute is used to count the number of occasions that an access control decision function has not
                authorized the access. The attribute takes the form of a not-settable counter as defined by CCITT
                Rec. X.721 | ISO/IEC 10165-2.  ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) invalidAccessAttempts(16) };
```

A.5.17 Nombre de etiqueta

```
labelName  ATTRIBUTE
        WITH ATTRIBUTE SYNTAX  AccessControlDefinitions.LabelName;
        MATCHES FOR EQUALITY, ORDERING;
        BEHAVIOUR  labelNameBehaviourPkg  BEHAVIOUR
            DEFINED AS
                !  This attribute assigns a name of type integer to security labels. This enables a check for ordering to take
                place.  ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) labelName(17) };
```

A.5.18 Clases de objeto gestionado

```
managedObjectClasses ATTRIBUTE
        WITH ATTRIBUTE SYNTAX AccessControlDefinitions.ObjectClassList;
        MATCHES FOR EQUALITY SET-COMPARISON, SET-INTERSECTION;
        BEHAVIOUR managedObjectClassesBehaviour BEHAVIOUR
            DEFINED AS
                !  This set-valued attribute identifies protected managed object classes and optional associated name
                bindings.

                Any attempt to include a value not known to be a managed object class within the domain shall result in
                the CMIS invalid attribute value error.  ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) managedObjectClasses(18) };
```

A.5.19 Instancias de objeto gestionado

```
managedObjectInstances ATTRIBUTE
        DERIVED FROM "CCITT Rec. X.721 | ISO/IEC 10165-2:1992": member;
        BEHAVIOUR managedObjectInstancesBehaviourPkg  BEHAVIOUR
            DEFINED AS
                !  This set-valued attribute identifies protected managed objects.  ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) managedObjectInstances(19) };
```

A.5.20 Tipo de operación

```
operationType ATTRIBUTE
        WITH ATTRIBUTE SYNTAX AccessControlDefinitions.OperationType;
        MATCHES FOR EQUALITY;
            BEHAVIOUR operationTypeBehaviourPkg  BEHAVIOUR
                DEFINED AS
                    !  This read-only attribute is used for naming operations managed objects. It may take one of the
                    values: get, replace, add member, remove member, replace with default, multiple object selection,
                    filter, create, delete, and action.  ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) operationType(20) };
```

A.5.21 Lista de operaciones

```
operationsList  ATTRIBUTE
        WITH ATTRIBUTE SYNTAX  AccessControlDefinitions.OperationsList;
        MATCHES FOR EQUALITY,  SET-COMPARISON,  SET-INTERSECTION;
        BEHAVIOUR  operationsListBehaviourPkg  BEHAVIOUR
            DEFINED AS
                ! This set-valued attribute identifies operations that are to be granted or denied, according to permissions
                in the containing rule managed object, on targets identified by the targets managed object. Operations
                are identified by the operation type. This attribute may be used when no conditional constraints are
                imposed on the parameters of the operation.  ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) operationsList(21) };
```

A.5.22 Alcance

```
scope ATTRIBUTE
        WITH ATTRIBUTE SYNTAX AccessControlDefinitions.Scope;
        MATCHES FOR EQUALITY;
        BEHAVIOUR scopeBehaviourPkg  BEHAVIOUR
            DEFINED AS
                ! The scope attribute identifies a scope for the selection of protected managed objects. ! ;;

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) scope(22) };
```

A.5.23 Filtro de alcance

```
scopeFilter ATTRIBUTE
        DERIVED FROM accessControlFilter;
        BEHAVIOUR scopeFilterBehaviour BEHAVIOUR
            DEFINED AS
                ! For requests that select multiple managed objects the scope filter specifies constraints on the scope
                parameter of the request, and the scope attribute identifier is used for all the filter items in the filter.

                This attribute identifies a filter upon the scope parameter of management operations. It shall have none
                or one element. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) scopeFilter(23) };
```

A.5.24 Etiqueta de seguridad

```
securityLabel ATTRIBUTE
        WITH ATTRIBUTE SYNTAX AccessControlDefinitions.SecurityLabel;
        MATCHES FOR EQUALITY, SET-COMPARISON, SET-INTERSECTION;
        BEHAVIOUR securityLabelBehaviour BEHAVIOUR
            DEFINED AS
                ! The security label attribute contains a security label. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) securityLabel(24) };
```

A.5.25 Condiciones de estado

```
stateConditions ATTRIBUTE
        WITH ATTRIBUTE SYNTAX AccessControlDefinitions.StateConditions;
        MATCHES FOR EQUALITY;
        BEHAVIOUR stateConditionsPackageBehaviour BEHAVIOUR
            DEFINED AS
                ! This attribute identifies a managed object and a filter upon the attributes of that managed object.
                ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) stateConditions(25) };
```

A.5.26 Sincronización

Este atributo proporciona un identificador de atributo y una sintaxis de filtrado para el parámetro de sincronización de aplicaciones de gestión.

```
synchronization ATTRIBUTE
        WITH ATTRIBUTE SYNTAX AccessControlDefinitions.CMISSync;
        BEHAVIOUR synchronizationBehaviour BEHAVIOUR
            DEFINED AS
                ! This attribute value represents the synchronization parameter of management operations. It is used to
                represent filters upon this parameter. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) synchronization(26) };
```

A.5.27 Filtro de sincronización

```
synchronizationFilter ATTRIBUTE
        DERIVED FROM accessControlFilter;
        BEHAVIOUR synchronizationFilterBehaviour BEHAVIOUR
            DEFINED AS
                ! For requests that select multiple managed objects the synchronization filter specifies constraints on the
                synchronization parameter of the request and the synchronization attribute identifier is used for all the
                filter items in the filter.

                This attribute identifies a filter upon the synchronization parameter of management operations. It shall
                have none or one element. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) synchronizationFilter(27) };
```

A.5.28 Lista de objetivos

```
targetsList ATTRIBUTE
        DERIVED FROM "Rec. X.721 | ISO/IEC 10165-2:1992": member;
        BEHAVIOUR targetsListBehaviour BEHAVIOUR
            DEFINED AS
                ! This set-valued attribute identifies the targets managed objects which themselves specify the targets to
                which the item rule pertains. It shall be an error to attempt to include a value which is not known to be
                the name of a targets managed object. ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) targetsList(28) };
```

A.5.29 Intentos de acceso válidos

```
validAccessAttempts  ATTRIBUTE
        DERIVED FROM "Rec. X.721 | ISO/IEC 10165-2:1992": counter;
        BEHAVIOUR validAccessAttemptBehaviourPkg  BEHAVIOUR
            DEFINED AS
                !  This attribute is used to count the number of occasions that an access control decision function has
                authorized the access. The attribute takes the form of a not-settable counter as defined by CCITT
                Rec. X.721 | ISO/IEC 10165-2.  ! ;;
REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) attribute(7) validAccessAttempts(29) };
```

A.6 Definiciones de sintaxis abstracta

```
AccessControlDefinitions { joint-iso-ccitt ms(9) function(2) part9(9) asn1Module(2) 1 }

DEFINITIONS IMPLICIT TAGS  ::=  BEGIN

IMPORTS

AttributeId, CMISFilter, CMISSync, ObjectClass, ObjectInstance, Scope, ActionTypeId
   FROM CMIP-1 { joint-iso-ccitt ms(9) cmip(1) modules(0) protocol(3) }

DistinguishedName
   FROM InformationFramework { joint-iso-ccitt ds(5) modules(1) informationFramework(1) }

FunctionalUnitPackage
   FROM SMASE-A-ASSOCIATE-Information { joint-iso-ccitt ms(9) smo(0) negotiationAbstractSyntax(1) version1(1) }

AETitle
   FROM ACSE-1 { joint-iso-ccitt association-Control(2) abstractSyntax(1) apdus(0) version(1) }

DiscriminatorConstruct
   FROM Attribute-ASN1Module { joint-iso-ccitt ms(9) smi(3) part2(2) asn1Module(2) 1 };

AccessControlList  ::= SET OF CHOICE  {     proxy              [0] Proxy,
                                            initiatorName      [1] InitiatorName }

InitiatorName  CHOICE {  individualName    [1]  IMPLICIT DistinguishedName,
                         groupName         [2]  IMPLICIT DistinguishedName,
                         role              [3]  IMPLICIT DistinguishedName,
                         application       [4]  IMPLICIT  AETitle  }

Proxy ::= SEQUENCE {  proxyId          [0] IMPLICIT OBJECT IDENTIFIER,
                      proxyValue       [1] ANY DEFINED BY proxyId }

AccessControlObjectName ::= GraphicString

ActionFilterList  ::=  SET OF SEQUENCE  {  actionTypeId              ActionTypeId,
                                           attributeFilterList       FilterList  OPTIONAL }

AuthenticationContext ::= SEQUENCE
                      {  authenticationPolicyId      [0] IMPLICIT OBJECT IDENTIFIER,
                         requirements                [1] ANY DEFINED BY authenticationPolicyId }

Boolean ::= BOOLEAN

false Boolean ::= FALSE
```

```
CapabilityIdentitiesList      ::=       SET OF CHOICE  {
        knownForm       [0]             SEQUENCE       {
                initiatorName           InitiatorName,
                sdaList                 SdaList  OPTIONAL  },
        unknownForm     [1]             SEQUENCE       {
                identifier              IMPLICIT OBJECT IDENTIFIER,
                value                   ANY DEFINED BY identifier  }}

SdaList ::= SET OF SEQUENCE  {
        securityDomainAuthorityName     SecurityDomainAuthorityName,
        operationType                   OperationType  }

DefaultAccess ::= SEQUENCE              {
                action                  [0] IMPLICIT EnforcementAction DEFAULT deny,
                create                  [1] IMPLICIT EnforcementAction DEFAULT deny,
                delete                  [2] IMPLICIT EnforcementAction DEFAULT deny,
                get                     [3] IMPLICIT EnforcementAction DEFAULT deny,
                replace                 [4] IMPLICIT EnforcementAction DEFAULT deny,
                addMember               [5] IMPLICIT EnforcementAction DEFAULT deny,
                removeMember            [6] IMPLICIT EnforcementAction DEFAULT deny,
                replaceWithDefault      [7] IMPLICIT EnforcementAction DEFAULT deny,
                multipleObjectSelection [8] IMPLICIT EnforcementAction DEFAULT deny,
                filter                  [9] IMPLICIT EnforcementAction DEFAULT deny }

denyAll DefaultAccess ::= {}

DenialResponse  ::=  EnforcementAction          ENUMERATED
                                        {       denyWithResponse (0),
                                                denyWithoutResponse (1),
                                                abortAssociation (2),
                                                denyWithFalseResponse (3) }

DenialGranularity  ::=  ENUMERATED              {       request(0),
                                                        object(1),
                                                        attribute(2) }

DomainIdentity  ::=  CHOICE   {         domainName      DistinguishedName,
                                        privateName     OCTET STRING  }

EnforcementAction ::= ENUMERATED {      denyWithResponse (0),
                                        denyWithoutResponse (1),
                                        abortAssociation (2),
                                        denyWithFalseResponse (3),
                                        allow (4)  }

Deny    EnforcementAction  ::=  denyWithResponse

FilterList ::= SET OF CMISFilter

InvalidAccessControlFilter ::= SEQUENCE
                                {       errorId         ENUMERATED
                                                {       duplicateId(0),
                                                        heterogeneousId(1),
                                                        invalidId(2) },
                                        filter          CMISFilter OPTIONAL }

LabelName  ::=  INTEGER

ObjectClassList ::= SET OF SEQUENCE     {   objectClass     [0]   ObjectClass,
                                            nameBinding     [1]   OBJECT IDENTIFIER  OPTIONAL}

OperationsList  ::=  SET OF OperationType

OperationType ::= INTEGER  {    action (0),
                                create (1),
                                delete (2),
                                get (3),
                                replace (4),
                                addMember (5),
                                removeMember (6),
                                replaceWithDefault (7),
                                multipleObjectSelection (8),
                                filter (9)  }
```

```
SecurityLabel ::= SET OF CHOICE {
        initiatorLabel      [1] IMPLICIT SEQUENCE {
            clearance CHOICE {
                localForm       [0] IMPLICIT INTEGER,
                globalForm      [1] IMPLICIT OBJECT IDENTIFIER },
            category            [2] IMPLICIT BIT STRING OPTIONAL } }

SecurityDomainAuthorityName ::= CHOICE {
domainAuthorityName                 [1] IMPLICIT DistinguishedName,
alternativeAuthorityName            [2] IMPLICIT Proxy }

StateConditions ::= SET OF SEQUENCE  {  conditionalObject       ObjectInstance,
                                        state                   CMISFilter }

END
```

Anexo B

Formulario de MCS[5)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

B.1 Introduction

B.1.1 Purpose and structure

The management conformance summary (MCS) is a statement by a supplier that identifies an implementation and provides information on whether the implementation claims conformance to any of the listed set of document that specify conformance requirements to OSI management.

The MCS proforma is a document, in the form of a questionnaire that when completed by the supplier of an implementation becomes the MCS.

B.1.2 Instructions for completing the MCS proforma to produce an MCS

The supplier of the implementation shall enter an explicit statement in each of the boxes provided. Specific instruction is provided in the text which precedes each table.

B.1.3 Symbols, abbreviations and terms

For all annexes of this Recommendation | International Standard, the following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2 and ITU-T Rec. X.296 | ISO/IEC 9646-7, are used for the Status column:

m Mandatory;

o Optional;

c Conditional;

x Prohibited;

– Not applicable or out of scope.

NOTES

1 'c', 'm', and 'o' are prefixed by "c:" when nested under a conditional or optional item of the same table;

2 'o' may be suffixed by ".N" (where N is a unique number) for selectable options among a set of status values. Support of at least one of the choices (from the items with the same value of N) is required.

The following requirements are commonly used throughout this MCS proforma:

c1: if B.1/1 then m else o

For all annexes of this Recommendation | International Standard, the following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2 and ITU-T Rec. X.296 | ISO/IEC 9646-7, are used for the Support column:

Y Implemented

N Not implemented

– No answer required

Ig The item is ignored (i.e. processed syntactically but not semantically).

B.1.4 Table format

Some of the tables in this Recommendation | International Standard have been split because the information is too wide to fit on the page. Where this occurs, the index number of the first block of columns are the index numbers of the corresponding rows of the remaining blocks of columns. A complete table reconstructed from the constituent parts should have the following layout:

Index	First block of columns	Second block of columns	Etc.

5) Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de MCS de este anexo a fin de que pueda ser utilizado para los fines previstos, y pueden además publicar el MCS cumplimentado. En la Rec. UIT-T X.724 | ISO/CEI 10165-6 se especifican las instrucciones para rellenar el formulario de MCS.

In this Recommendation | International Standard the constituent parts of the table appear consecutively, starting with the first block of columns.

When a table with sub-rows is too wide to fit on a page, the continuation table(s) have been constructed with index numbers identical to the index numbers in the corresponding rows of the first table, and with sub-index numbers corresponding to the sub-rows within each indexed row. For example, if Table X.1 has 2 rows and the continuation of Table X.1 has 2 sub-rows for each row, the tables are presented as follows:

Table X.1 – Title

					Support		
Index	A	B	C	D	E	F	G
1	a	b	–				
2	a	b	–				

Table X.1 *(continued)* **– Title**

Index	Sub-index	H	I	J	K	L
1	1.1	h	i	j		
	1.2	h	i	j		
2	2.1	h	i	j		
	2.2	h	i	j		

A complete table reconstructed from the constituent parts should have the following layout:

					Support								
Index	A	B	C	D	E	F	G	Sub-index	H	I	J	K	L
1	a	b	–					1.1	h	i	j		
								1.2	h	i	j		
2	a	b	–					2.1	h	i	j		
								2.2	h	i	j		

References made to cells within tables shall be interpreted as references within reconstructed tables. In the example above, the reference X.1/1d corresponds to the blank cell in column G for row with Index 1, and X.1/1.2b corresponds to the blank cell in column L for row with sub-index 1.2.

B.2 Identification of the implementation

B.2.1 Date of statement

The supplier of the implementation shall enter the date of this statement in the box below. Use the format DD-MM-YYYY.

Date of statement

B.2.2 Identification of the implementation

The supplier of the implementation shall enter information necessary to uniquely identify the implementation and the system(s) in which it may reside, in the box below.

B.2.3 Contact

The supplier of the implementation shall provide information on whom to contact if there are any queries concerning the contents of the MCS or any referenced implementation conformance statement, in the box below.

B.3 Identification of the Recommendations | International Standards in which the management information is defined

The supplier of the implementation shall enter the title, reference number and date of the publication of the Recommendations | International Standards which specifies the management information to which conformance is claimed, in the box below.

Recommendations | International Standards to which conformance is claimed

B.3.1 Technical corrigenda implemented

The supplier of the implementation shall enter the reference numbers of implemented technical corrigenda which modify the identified Recommendations | International Standards, in the box below.

B.3.2 Amendments implemented

The supplier of the implementation shall state the titles and reference numbers of implemented amendments to the identified Recommendations | International Standards, in the box below.

B.4 Management conformance summary

The supplier of the implementation shall state the capabilities and features supported and provide summary of conformance claims to Recommendations | International Standards using the tables in this annex.

The supplier of the implementation shall specify the roles that are supported, in Table B.1.

Table B.1 – Roles

Index	Roles supported	Status	Support	Additional information
1	Manager role support	o.1		
2	Agent role support	o.1		

The supplier of the implementation shall specify support for the systems management functional unit, in Table B.2.

Table B.2 – Systems management functional unit

		Manager		Agent		
Index	Systems management functional unit name	Status	Support	Status	Support	Additional information
1	Access control functional unit	c1		c2		

c1: if B.1/1a then o else –.

c2: if B.1/2a then o else –.

The supplier of the implementation shall specify support for management information in the manager role, in Table B.3.

Table B.3 – Manager role minimum conformance requirement

Index	Item	Status	Support	Additional information
1	Operations on managed objects	c3		
2	Object creation notification for access control managed object	c4		
3	Object deletion notification for access control managed object	c4		
4	Attribute value change notification for access control managed object	c4		

c3: if B.2/1a then o else (if B.1/1a then o.2 else –).

c4: if B.2/1a then m else (if B.2/2a then o else (if B.1/1a then o.2 else –)).

NOTE – Manager role minimum conformance requires support for at least one of the items identified in this table. Support for the functional unit identified in Table B.2 mandates support for some of those items. Conditions c3 and c4 express both of these requirements.

The supplier of the implementation shall specify support for management information in the agent role, in Table B.4.

Table B.4 – Agent role minimum conformance requirement

Index	Item	Status	Support	Table reference	Additional information
1	Access control rules managed object	c5			
2	Rule managed object	c6			
3	Notification emitter managed object	c6			
4	Targets managed object	c6			
5	Operations managed object	c6			
6	ACL initiators managed object	c6			
7	Capability initiators managed object	c6			
8	Label initiators managed object	c6			
9	Assigned labels managed object	c6			
10	Attribute label managed object	c6			
11	Instance label managed object	c6			
12	Class label managed object	c6			
13	Sub-classes of log records associated with notifications emitted by sub-classes of access control managed object class	c7			

c5: if B.1/2a then m else –.

c6: if B.1/2a then o else –.

c7: if B.1/2a and B.5/1a then m else –.

NOTE – The Table reference column is the notification, attribute or managed object table reference of the MOCS supplied by the supplier of the managed object which claims to import the notification or attribute from this Recommendation | International Standard.

Table B.5 – Logging of event records

Index		Status	Support	Additional information
1	Does the implementation support logging of event records in the agent role?	c8		

c8: if B.1/2a then o else –.

NOTE 1 – Conformance to this Recommendation | International Standard does not require conformance to CCITT Rec. X.735 | ISO/IEC 10164-6.

The supplier of the implementation shall provide information on claims of conformance to any of the Recommendations | International Standards summarized in Tables B.6 to B.9. For each Recommendation | International Standard that the supplier of the implementation claims conformance to, the corresponding conformance statement(s) shall be completed, or referenced by, the MCS. The supplier of the implementation shall complete the Support, Table numbers and Additional information columns.

In Tables B.6 to B.9 the Status column is used to indicate whether the supplier of the implementation is required to complete the referenced tables or referenced items. Conformance requirements are as specified in the referenced tables or referenced items and are not changed by the value of the MCS Status column. Similarly, the Support column is used by the supplier of the implementation to indicate completion of the referenced tables or referenced items.

Table B.6 – PICS support summary

Index	Identification of the document that includes the PICS proforma	Table numbers of PICS proforma	Description	Constraints and Values	Status	Support	Table numbers of PICS	Additional Information
1	CCITT Rec. X.730 | ISO/IEC 10164-1	Annex E all tables	SM application context	OBJECT IDENTIFIER	m			

NOTE 2 – Conformance to the MAPDUs defined in this Recommendation | International Standard can be claimed by completing the corresponding tables in the MICS and MOCS annexes of the referenced standards.

Table B.7 – MOCS support summary

Index	Identification of the document that includes the MOCS proforma	Table numbers of MOCS proforma	Description	Constraints and Values	Status	Support	Table numbers of MOCS	Additional Information
1	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.1 to D.5	accessControl-Rules	–	m			
2	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.6 to D.10	rule	–	o			
3	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.11 to D.15	notification-Emitter	–	o			
4	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.16 to D.20	targets	–	o			
5	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.21 to D.26	operations	–	o			
6	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.27 to D.31	aclInitiators	–	o			
7	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.32 to D.36	capability-Initiators	–	o			
8	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.37 to D.41	labelInitiators	–	o			
9	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.42 to D.46	assignedLabels	–	o			
10	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.47 to D.51	attributeLabel	–	o			
11	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.52 to D.56	instanceLabel	–	o			
12	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex D, Tables D.57 to D.61	classLabel	–	o			

Table B.7 *(concluded)* **– MOCS support summary**

Index	Identification of the document that includes the MOCS proforma	Table numbers of MOCS proforma	Description	Constraints and Values	Status	Support	Table numbers of MOCS	Additional Information
13	CCITT Rec. X.730 | ISO/IEC 10164-1	Annex C, all tables	objectCreation, objectDeletion, and AttributeValue Change	–	c9			
14	CCITT Rec. X.736 | ISO/IEC 10164-7	Annex C, all tables	securityAlarm-record	–	c9			
15	CCITT Rec. X.740 | ISO/IEC 10164-8	Annex D, all tables	securityAudit-Trailrecord	–	c9			
c9: if B.4/13a then m else –.								

Table B.8 – MRCS support summary

Index	Identification of the document that includes the MRCS proforma	Table numbers of MRCS proforma	Description	Constraints and Values	Status	Support	Table numbers of MRCS	Additional Information
1	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex E, all tables	rule-access ControlRules name binding	–	c10			
2	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex E, all tables	operations-targets name binding	–	c11			
3	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex E, all tables	notification Emitter-access ControlRules name binding	–	c12			
4	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex E, all tables	attributeLabel-assignedLabels name binding	–	c13			
5	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex E, all tables	instanceLabel assignedLabels name binding	–	c14			
6	ITU-T Rec. X.741 | ISO/IEC 10164-9	Annex E, all tables	classLabel-assignedLabels name binding	–	c15			
7	CCITT Rec. X.740 | ISO/IEC 10164-8	Item D.1/1	logRecord-log name binding	–	c16			
c10: if B.4/2a then o else –. c11: if B.4/5a then o else –. c12: if B.4/3a then o else –. c13: if B.4/10a then o else –. c14: if B.4/11a then o else –. c15: if B.4/12a then o else –. c16: if B.5/1a then o else –.								

Table B.9 – MICS support summary

Index	Identification of the document that includes the MICS proforma	Table numbers of MICS proforma	Description	Constraints and Values	Status	Support	Table numbers of MICS	Additional Information
1	ITU-T Rec. X.741 | ISO/IEC 10164-9	Tables C.1 and C.2	management operations	–	c17			
2	CCITT Rec. X.730 | ISO/IEC 10164-1	Table B.1	objectCreation, objectDeletion and attributeValue Change notifications	–	c18			
c17: if B.3/1a then m else –. c18: if B.3/2a or B.3/3a or B.3/4a then m else –.								

Anexo C

Formulario de MICS[6)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

C.1 Introduction

The purpose of this MICS proforma is to provide a mechanism for a supplier of an implementation which claims conformance in the manager role to management information specified in this Recommendation | International Standard, to provide conformance information in a standard form.

C.2 Instructions for completing the MICS proforma to produce a MICS

The MICS proforma contained in this annex is comprised of information in tabular form, in accordance with ITU-T Rec. X.724 | ISO/IEC 10165-6. In addition to the general guidance given in ITU-T Rec. X.724 | ISO/IEC 10165-6, the Additional information column shall be used to identify the object classes for which the management operations are supported. The supplier of the implementation shall state which items are supported in the tables below and if necessary, provide additional information.

C.3 Symbols, abbreviations and terms

The following abbreviations are used throughout the MICS proforma:

dmi-att **joint-iso-ccitt ms(9) smi(3) part2(2) attribute(7)**

ac-att **joint-iso-ccitt ms(9) function(2) part9(9) attribute(7)**

The notations used for the Status and Support columns are specified in B.1.3.

C.4 Statement of conformance to the management information

C.4.1 Attributes

The specifier of a manager role implementation that claims to support management operations on the attributes specified in this Recommendation | International Standard shall import a copy of Table C.1 and complete it.

C.4.2 Create and delete management operations

The specifier of a manager role implementation that claims to support the create or delete management operations on the managed objects specified in this Recommendation | International Standard shall import a copy of Table C.2 and complete it.

---

6) Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de MICS de este anexo a fin de que pueda ser utilizado para los fines previstos, y pueden además publicar el MICS cumplimentado.

Table C.1 – Attribute support

				Set by create		Get	
Index	Attribute template label	Value of object identifier for the attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	c19		o.3	
2	nameBinding	{dmi-att 63}	–	c19		o.3	
3	packages	{dmi-att 66}	–	c19		o.3	
4	allomorphs	{dmi-att 50}	–	c19		o.3	
5	availabilityStatus	{dmi-att 33}	–	–		o.3	
6	startTime	{dmi-att 68}	–	c19		o.3	
7	stopTime	{dmi-att 69}	–	c19		o.3	
8	intervalsOfDay	{dmi-att 57}	–	c19		o.3	
9	weekMask	{dmi-att 71}	–	c19		o.3	
10	schedulerName	{dmi-att 67}	–	c19		o.3	
11	attributeIdentifierList	{dmi-att 8}	–	c19		o.3	
12	managedObjectInstance	{dmi-att 61}	–	c19		o.3	
13	accessControlList	{ac-att 1}	–	c19		o.3	
14	accessControlFilter	{ac-att 2}	–	c19		o.3	
15	accessControlObjectName	{ac-att 3}	–	c19		o.3	
16	actionFilterList	{ac-att 4}	–	c19		o.3	
17	attributeFilterList	{ac-att 5}	–	c19		o.3	
18	authenticationContext	{ac-att 6}	–	c19		o.3	
19	capabilityIdentitiesList	{ac-att 7}	–	c19		o.3	
20	defaultAccess	{ac-att 8}	–	c19		o.3	
21	defaultDenialResponse	{ac-att 9}	–	c19		o.3	
22	denialGranularity	{ac-att 10}	–	c19		o.3	
23	domainIdentity	{ac-att 11}	–	c19		o.3	
24	enforcementAction	{ac-att 12}	–	c19		o.3	
25	filter	{ac-att 13}	–	c19		o.3	
26	initiatorACImandated	{ac-att 14}	–	c19		o.3	
27	initiatorsList	{ac-att 15}	–	c19		o.3	
28	invalidAccessAttempts	{ac-att 16}	–	c19		o.3	
29	labelName	{ac-att 17}	–	c19		o.3	
30	managedObjectClasses	{ac-att 18}	–	c19		o.3	
31	managedObjectInstances	{ac-att 19}	–	c19		o.3	
32	operationType	{ac-att 20}	–	c19		o.3	
33	operationsList	{ac-att 21}	–	c19		o.3	
34	scope	{ac-att 22}	–	c19		o.3	
35	scopeFilter	{ac-att 23}	–	c19		o.3	
36	securityLabel	{ac-att 24}	–	c19		o.3	
37	stateConditions	{ac-att 25}	–	c19		o.3	
38	synchronization	{ac-att 26}	–	c19		o.3	
39	synchronizationFilter	{ac-att 27}	–	c19		o.3	
40	targetsList	{ac-att 28}	–	c19		o.3	
41	validAccessAttempts	{ac-att 29}	–	c19		o.3	

Table C.1 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	o.3		–		–		–		
7	o.3		–		–		–		
8	o.3		o.3		o.3		o.3		
9	o.3		o.3		o.3		o.3		
10	–		–		–		–		
11	o.3		o.3		o.3		–		
12	o.3		–		–		–		
13	o.3		o.3		o.3		o.3		
14	–		–		–		–		
15	–		–		–		–		
16	o.3		o.3		o.3		–		
17	o.3		o.3		o.3		–		
18	o.3		–		–		–		
19	o.3		–		–		–		
20	o.3		–		–		o.3		
21	o.3		–		–		–		
22	o.3		–		–		–		
23	o.3		–		–		–		
24	o.3		–		–		o.3		
25	o.3		–		–		–		
26	o.3		–		–		o.3		
27	o.3		o.3		o.3		–		
28	–		–		–		–		
29	–		–		–		–		
30	o.3		o.3		o.3		–		
31	o.3		o.3		o.3		–		
32	–		–		–		–		
33	o.3		o.3		o.3		–		
34	o.3		–		–		–		
35	o.3		–		–		–		
36	o.3		–		–		o.3		
37	o.3		o.3		o.3		–		
38	–		–		–		–		
39	o.3		–		–		–		
40	o.3		o.3		o.3		–		
41	–		–		–		–		

c1: if C2/1a or C2/3a or C2/5a or C2/7a or C2/9a or C2/11a or C2/13a or C2/15a or C2/17a or C2/19a or C2/21a or c2/23a then o else –.

Table C.2 – Create and delete support

Index	Operation	Constraints and values	Status	Support	Additional information
1	Create support	Access control rules managed object	o		
1.1	Create with reference object	Access control rules managed object	–		
2	Delete support	Access control rules managed object	o		
3	Create support	Rule managed object	o		
3.1	Create with reference object	Rule managed object	c:o		
4	Delete support	Rule managed object	o		
5	Create support	Notification emitter managed object	o		
5.1	Create with reference object	Notification emitter managed object	c:o		
6	Delete support	Notification emitter managed object	o		
7	Create support	Targets managed object	o		
7.1	Create with reference object	Targets managed object	–		
8	Delete support	Targets managed object	o		
9	Create support	Operations managed object	o		
9.1	Create with reference object	Operations managed object	c:o		
10	Delete support	Operations managed object	o		
11	Create support	ACL initiators managed object	o		
11.1	Create with reference object	ACL initiators managed object	–		
12	Delete support	ACL initiators managed object	o		
13	Create support	Capability initiators managed object	o		
13.1	Create with reference object	Capability initiators managed object	–		
14	Delete support	Capability initiators managed object	o		
15	Create support	Label initiators managed object	o		
15.1	Create with reference object	Label initiators managed object	–		
16	Delete support	Label initiators managed object	o		
17	Create support	Assigned labels managed object	o		
17.1	Create with reference object	Assigned labels managed object	–		
18	Delete support	Assigned labels managed object	o		
19	Create support	Attribute label managed object	o		
19.1	Create with reference object	Attribute label managed object	–		
20	Delete support	Attribute label managed object	o		
21	Create support	Class label managed object	o		
21.1	Create with reference object	Class label managed object	–		
22	Delete support	Class label managed object	o		
23	Create support	Instance label managed object	o		
23.1	Create with reference object	Instance label managed object	–		
24	Delete support	Instance label managed object	o		

Anexo D

Formulario de MOCS[7)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

D.1 Introduction

The purpose of this MOCS proforma is to provide a mechanism for a supplier of an implementation which claims conformance to a managed object class, to provide conformance information in a standard form.

D.2 Instructions for completing the MOCS proforma to produce a MOCS

The MOCS proforma contained in this annex is comprised of information in tabular form, in accordance with ITU-T Rec. X.724 | ISO/IEC 10165-6. The supplier of the implementation shall state which items are supported in the tables below and if necessary, provide additional information.

D.3 Symbols, abbreviations and terms

The following abbreviations are used throughout the MOCS proforma:

dmi-att **joint-iso-ccitt ms(9) smi(3) part2(2) attribute(7)**

dmi-nb **joint-iso-ccitt ms(9) smi(3) part2(2) nameBinding(6)**

dmi-not **joint-iso-ccitt ms(9) smi(3) part2(2) notification(10)**

dmi-pkg **joint-iso-ccitt ms(9) smi(3) part2(2) package(4)**

ac-obj **joint-iso-ccitt ms(9) function(2) part9(9) managedObjectClass(3)**

ac-att **joint-iso-ccitt ms(9) function(2) part9(9) attribute(7)**

ac-nb **joint-iso-ccitt ms(9) function(2) part9(9) nameBinding(6)**

ac-par **joint-iso-ccitt ms(9) function(2) part9(9) parameter(5)**

ac-pkg **joint-iso-ccitt ms(9) function(2) part9(9) package(4)**

sat-att **joint-iso-ccitt ms(9) function(2) part8(8) attribute(7)**

sat-not **joint-iso-ccitt ms(9) function(2) part8(8) notification(10)**

The notations used for the Status and Support columns are specified in B.1.3.

D.4 Access control rules managed object class

D.4.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the access control rules managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.1.

Table D.1 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	accessControlRules	{ac-obj 2}		

7) Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de MOCS de este anexo a fin de que pueda ser utilizado para los fines previstos, y pueden además publicar el MOCS cumplimentado. En la Rec. UIT-T X.724 | ISO/CEI 10165-6 se especifican las instrucciones para rellenar el formulario de MOCS.

If the answer to the actual class question in the managed object class support Table D.1 is "N", the supplier of the implementation shall supply the actual class support details, in Table D.2.

Table D.2 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.4.2 Packages

See Table D.3.

Table D.3 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c20		
3	allomorphicPackage	{dmi-pkg 17}	–	c21		
4	accessControlPackage	–	–	m		
5	accessControlRulesPackage	–	–	m		
c20: if D.3/3 then m else –. c21: if D.1/1b then – else m.						

D.4.3 Attributes

See Table D.4.

Table D.4 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c22		c22	
4	allomorphs	{dmi-att 50}	–	c23		c23	
5	accessControlObjectName	{ac-att 3}	–	m		m	
6	defaultAccess	{ac-att 8}	–	m		m	
7	defaultDenialResponse	{ac-att 9}	–	m		m	
8	denialGranularity	{ac-att 10}	–	m		m	
9	domainIdentity	{ac-att 11}	–	m		m	
c22: if D.3/2 then m else –. c23: if D.3/3 then m else –.							

Table D.4 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	m		–		–		m		
7	m		–		–		–		
8	m		–		–		–		
9	m		–		–		–		

D.4.4 Notifications

See Table D.5.

Table D.5 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	attributeValueChange	{dmi-not 1}	–	m			
2	objectCreation	{dmi-not 6}	–	m			
3	objectDeletion	{dmi-not 7}	–	m			

Table D.5 *(continued)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeIdentifierList	{dmi-att 8}	–	o		
	1.3	attributeValueChangeDefinition	{dmi-att 10}	–	m		
	1.3.1	attributeId	–	–	m		
	1.3.2	oldAttributeValue	–	–	o		
	1.3.3	newAttributeValue	–	–	m		
	1.4	notificationIdentifier	{dmi-att 16}	–	c24		
	1.5	correlatedNotifications	{dmi-att 12}	–	o		
	1.5.1	correlatedNotification	–	–	c:m		
	1.5.2	sourceObjectInst	–	–	c:o		
	1.5.2.1	distinguishedName	–	–	c:o.4		
	1.5.2.2	nonSpecificForm	–	–	c:o.4		
	1.5.2.3	localDistinguishedName	–	–	c:o.4		
	1.6	additionalText	{dmi-att 7}	–	o		
	1.7	additionalInformation	{dmi-att 6}	–	–		

Table D.5 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c25		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.5		
	2.4.2.2	nonSpecificForm	–	–	c:o.5		
	2.4.2.3	localDistinguishedName	–	–	c:o.5		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	–		
3	3.1	sourceIndicator	{dmi-att 26}	–	o		
	3.2	attributeList	{dmi-att 9}	–	o		
	3.3	notificationIdentifier	{dmi-att 16}	–	c26		
	3.4	correlatedNotifications	{dmi-att 12}	–	o		
	3.4.1	correlatedNotification	–	–	c:m		
	3.4.2	sourceObjectInst	–	–	c:o		
	3.4.2.1	distinguishedName	–	–	c:o.6		
	3.4.2.2	nonSpecificForm	–	–	c:o.6		
	3.4.2.3	localDistinguishedName	–	–	c:o.6		
	3.5	additionalText	{dmi-att 7}	–	o		
	3.6	additionalInformation	{dmi-att 6}	–	o		

c24: if D.5/1.5 then m else o.

c25: if D.5/2.4 then m else o.

c26: if D.5/3.4 then m else o.

D.5 Rule managed object class

D.5.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the rule managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.6.

Table D.6 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	rule	{ac-obj 3}		

If the answer to the actual class question in the managed object class support Table D.6 is “N”, the supplier of the implementation shall supply the actual class support details, in Table D.7.

Table D.7 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.5.2 Packages

See Table D.8.

Table D.8 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c27		
3	allomorphicPackage	{dmi-pkg 17}	–	c28		
4	accessControlPackage	–	–	m		
5	rulePackage	–	–	m		
6	availabilityStatusPackage	{dmi-pkg 22}	–	o		
7	duration	{dmi-pkg 26}	–	o		
8	dailyScheduling	{dmi-pkg 25}	–	o		
9	weeklyScheduling	{dmi-pkg 29}	–	o		
10	externalScheduler	{dmi-pkg 27}	–	o		
11	stateConditionsPackage	{ac-pkg 1}	–	o		
12	authenticationContextPackage	{ac-pkg 2}	–	o		
c27: if D.8/3 or any of D.8/6 through D.8/12 then m else –. c28: if D.6/1.b then – else m.						

D.5.3 Attributes

See Table D.9.

Table D.9 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c29		c29	
4	allomorphs	{dmi-att 50}	–	c30		c30	
5	accessControlObjectName	{ac-att 3}	–	m		m	
6	enforcementAction	{ac-att 12}	–	m		m	
7	initiatorsList	{ac-att 15}	–	m		m	
8	targetsList	{ac-att 28}	–	m		m	
9	availabilityStatus	{dmi-att 33}	–	–		c31	

Table D.9 *(continued)* **– Attribute support**

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
10	startTime	{dmi-att 68}	DMI default	c32		c32	
11	stopTime	{dmi-att 69}	DMI default	c32		c32	
12	intervalsOfDay	{dmi-att 57}	DMI default	c33		c33	
13	weekMask	{dmi-att 71}	–	c34		c34	
14	schedulerName	{dmi-att 67}	–	c35		c35	
15	stateConditions	{ac-att 25}	–	c36		c36	
16	authenticationContext	{ac-att 6}	–	c37		c37	

Table D.9 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	m		–		–		m		
7	m		m		m		–		
8	m		m		m		–		
9	–		–		–		–		
10	c32		–		–		–		
11	c32		–		–		c38		
12	c33		–		–		c33		
13	c34		c34		c34		c34		
14	x		–		–		–		
15	c36		c36		c36		–		
16	c37		–		–		–		

c29: if D.8/2 then m else –.
c30: if D.8/3 then m else –.
c31: if D.8/6 then m else –.
c32: if D.8/7 then m else –.
c33: if D.8/8 then m else –.
c34: if D.8/9 then m else –.
c35: if D.8/10 then m else –.
c36: if D.8/11 then m else –.
c37: if D.8/12 then m else –.
c38: if D.6/1b then x else –.

D.5.4 Notifications

See Table D.10.

Table D.10 – Notification support

Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Support		Additional information
					Confirmed	Non-confirmed	
1	attributeValueChange	{dmi-not 1}	–	m			
2	objectCreation	{dmi-not 6}	–	m			
3	objectDeletion	{dmi-not 7}	–	m			

Table D.10 *(continued)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeIdentifierList	{dmi-att 8}	–	o		
	1.3	attributeValueChangeDefinition	{dmi-att 10}	–	m		
	1.3.1	attributeId	–	–	m		
	1.3.2	oldAttributeValue	–	–	o		
	1.3.3	newAttributeValue	–	–	m		
	1.4	notificationIdentifier	{dmi-att 16}	–	c39		
	1.5	correlatedNotifications	{dmi-att 12}	–	o		
	1.5.1	correlatedNotification	–	–	c:m		
	1.5.2	sourceObjectInst	–	–	c:o		
	1.5.2.1	distinguishedName	–	–	c:o.7		
	1.5.2.2	nonSpecificForm	–	–	c:o.7		
	1.5.2.3	localDistinguishedName	–	–	c:o.7		
	1.6	additionalText	{dmi-att 7}	–	o		
	1.7	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c40		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.8		
	2.4.2.2	nonSpecificForm	–	–	c:o.8		
	2.4.2.3	localDistinguishedName	–	–	c:o.8		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		
3	3.1	sourceIndicator	{dmi-att 26}	–	o		
	3.2	attributeList	{dmi-att 9}	–	o		
	3.3	notificationIdentifier	{dmi-att 16}	–	c41		

Table D.10 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
3	3.4	correlatedNotifications	{dmi-att 12}	–	o		
(cont.)	3.4.1	correlatedNotification	–	–	c:m		
	3.4.2	sourceObjectInst	–	–	c:o		
	3.4.2.1	distinguishedName	–	–	c:o.9		
	3.4.2.2	nonSpecificForm	–	–	c:o.9		
	3.4.2.3	localDistinguishedName	–	–	c:o.9		
	3.5	additionalText	{dmi-att 7}	–	o		
	3.6	additionalInformation	{dmi-att 6}	–	o		
c39: if D.10/1.5 then m else –. c40: if D.10/2.4 then m else –. c41: if D.10/3.4 then m else –.							

D.6 Notification emitter managed object class

D.6.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the notification emitter managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.11.

Table D.11 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	notificationEmitter	{ac-obj 4}		

If the answer to the actual class question in the managed object class support Table D.11 is “N”, the supplier of the implementation shall supply the actual class support details, in Table D.12.

Table D.12 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.6.2 Packages

See Table D.13.

Table D.13 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c42		
3	allomorphicPackage	{dmi-pkg 17}	–	c43		
4	accessControlPackage	–	–	m		
5	accessControlNotificationEmitterPkg	–	–	m		
6	securityViolationAlarmPkg	{ac-pkg 3}	–	o		
7	timeViolationAlarmPkg	{ac-pkg 4}	–	o		
8	operationalViolationAlarmPkg	{ac-pkg 5}	–	o		
9	accessControlUsagePkg	{ac-pkg 6}	–	o		
10	accessControlServiceReportPkg	{ac-pkg 7}	–	o		
c42: if D.13/3 or D.13/6 through D.13/10 then m else –. c43: if D.11/1b then – else m.						

D.6.3 Attributes

See Table D.14.

Table D.14 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c44		c44	
4	allomorphs	{dmi-att 50}	–	c45		c45	
5	accessControlObjectName	{ac-att 3}	–	m		m	
6	invalidAccessAttempts	{ac-att 16}	–	c46		c46	
7	validAccessAttempts	{ac-att 29}	–	c46		c46	

Table D.14 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	–		–		–		–		
7	–		–		–		–		

c44: if D.13/2 then m else –.
c45: if D.13/3 then m else –.
c46: if D.13/9 then m else –.

D.6.4 Notifications

See Table D.15.

Table D.15 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	attributeValueChange	{dmi-not 1}	–	m			
2	objectCreation	{dmi-not 6}	–	m			
3	objectDeletion	{dmi-not 7}	–	m			
4	securityServiceOrMechanism Violation	{dmi-not 13}	–	c47			
5	timeDomainViolation	{dmi-not 15}	–	c48			
6	operationalViolation	{dmi-not 8}	–	c49			
7	usageReport	{sat-not 2}	–	c50			
8	serviceReport	{sat-not 1}	–	c51			

c47: if D.13/6 then m else –.
c48: if D.13/7 then m else –.
c49: if D.13/8 then m else –.
c50: if D.13/9 then m else –.
c51: if D.13/10 then m else –.

Table D.15 *(continued)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeIdentifierList	{dmi-att 8}	–	o		
	1.3	attributeValueChangeDefinition	{dmi-att 10}	–	m		
	1.3.1	attributeId	–	–	m		
	1.3.2	oldAttributeValue	–	–	o		
	1.3.3	newAttributeValue	–	–	m		
	1.4	notificationIdentifier	{dmi-att 16}	–	c52		
	1.5	correlatedNotifications	{dmi-att 12}	–	o		
	1.5.1	correlatedNotification	–	–	c:m		
	1.5.2	sourceObjectInst	–	–	c:o		
	1.5.2.1	distinguishedName	–	–	c:o.10		
	1.5.2.2	nonSpecificForm	–	–	c:o.10		
	1.5.2.3	localDistinguishedName	–	–	c:o.10		
	1.6	additionalText	{dmi-att 7}	–	o		
	1.7	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c53		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.11		
	2.4.2.2	nonSpecificForm	–	–	c:o.11		
	2.4.2.3	localDistinguishedName	–	–	c:o.11		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		
3	3.1	sourceIndicator	{dmi-att 26}	–	o		
	3.2	attributeList	{dmi-att 9}	–	o		
	3.3	notificationIdentifier	{dmi-att 16}	–	c54		
	3.4	correlatedNotifications	{dmi-att 12}	–	o		
	3.4.1	correlatedNotification	–	–	c:m		
	3.4.2	sourceObjectInst	–	–	c:o		
	3.4.2.1	distinguishedName	–	–	c:o.12		
	3.4.2.2	nonSpecificForm	–	–	c:o.12		
	3.4.2.3	localDistinguishedName	–	–	c:o.12		
	3.5	additionalText	{dmi-att 7}	–	o		
	3.6	additionalInformation	{dmi-att 6}	–	o		
4	4.1	securityAlarmCause	{dmi-att 21}	–	m		
	4.2	securityAlarmSeverity	{dmi-att 23}	–	m		
	4.3	securityAlarmDetector	{dmi-att 22}	–	m		
	4.3.1	mechanism	–	–	o		
	4.3.2	object	–	–	o		
	4.3.3	application	–	–	o		
	4.4	serviceUser	{dmi-att 25}	–	m		

Table D.15 *(continued)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
4 *(cont.)*	4.4.1	identifier	–	–	o		
	4.4.2	details	–	–	o		
	4.5	serviceProvider	{dmi-att 24}	–	m		
	4.5.1	identifier	–	–	o		
	4.5.2	details	–	–	o		
	4.6	notificationIdentifier	{dmi-att 16}	–	c55		
	4.7	correlatedNotifications	{dmi-att 12}	–	o		
	4.7.1	correlatedNotification	–	–	c:m		
	4.7.2	sourceObjectInst	–	–	c:o		
	4.7.2.1	distinguishedName	–	–	c:o.13		
	4.7.2.2	nonSpecificForm	–	–	c:o.13		
	4.7.2.3	localDistinguishedName	–	–	c:o.13		
	4.8	additionalText	{dmi-att 7}	–	o		
	4.9	additionalInformation	{dmi-att 6}	–	o		
5	5.1	securityAlarmCause	{dmi-att 21}	–	m		
	5.2	securityAlarmSeverity	{dmi-att 23}	–	m		
	5.3	securityAlarmDetector	{dmi-att 22}	–	m		
	5.3.1	mechanism	–	–	o		
	5.3.2	object	–	–	o		
	5.3.3	application	–	–	o		
	5.4	serviceUser	{dmi-att 25}	–	m		
	5.4.1	identifier	–	–	o		
	5.4.2	details	–	–	o		
	5.5	serviceProvider	{dmi-att 24}	–	m		
	5.5.1	identifier	–	–	o		
	5.5.2	details	–	–	o		
	5.6	notificationIdentifier	{dmi-att 16}	–	c56		
	5.7	correlatedNotifications	{dmi-att 12}	–	o		
	5.7.1	correlatedNotification	–	–	c:m		
	5.7.2	sourceObjectInst	–	–	c:o		
	5.7.2.1	distinguishedName	–	–	c:o.14		
	5.7.2.2	nonSpecificForm	–	–	c:o.14		
	5.7.2.3	localDistinguishedName	–	–	c:o.14		
	5.8	additionalText	{dmi-att 7}	–	o		
	5.9	additionalInformation	{dmi-att 6}	–	o		
6	6.1	securityAlarmCause	{dmi-att 21}	–	m		
	6.2	securityAlarmSeverity	{dmi-att 23}	–	m		
	6.3	securityAlarmDetector	{dmi-att 22}	–	m		
	6.3.1	mechanism	–	–	o		
	6.3.2	object	–	–	o		
	6.3.3	application	–	–	o		
	6.4	serviceUser	{dmi-att 25}	–	m		
	6.4.1	identifier	–	–	o		
	6.4.2	details	–	–	o		
	6.5	serviceProvider	{dmi-att 24}	–	m		

Table D.15 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
6 *(cont.)*	6.5.1	identifier	–	–	o		
	6.5.2	details	–	–	o		
	6.6	notificationIdentifier	{dmi-att 16}	–	c57		
	6.7	correlatedNotifications	{dmi-att 12}	–	o		
	6.7.1	correlatedNotification	–	–	c:m		
	6.7.2	sourceObjectInst	–	–	c:o		
	6.7.2.1	distinguishedName	–	–	c:o.15		
	6.7.2.2	nonSpecificForm	–	–	c:o.15		
	6.7.2.3	localDistinguishedName	–	–	c:o.15		
	6.8	additionalText	{dmi-att 7}	–	o		
	6.9	additionalInformation	{dmi-att 6}	–	o		
7	7.1	notificationIdentifier	{dmi-att 16}	–	c58		
	7.2	correlatedNotifications	{dmi-att 12}	–	o		
	7.2.1	correlatedNotification	–	–	c:m		
	7.2.2	sourceObjectInst	–	–	c:o		
	7.2.2.1	distinguishedName	–	–	c:o.16		
	7.2.2.2	nonSpecificForm	–	–	c:o.16		
	7.2.2.3	localDistinguishedName	–	–	c:o.16		
	7.3	additionalText	{dmi-att 7}	–	o		
	7.4	additionalInformation	{dmi-att 6}	–	o		
8	8.1	serviceReportCause	{at-att 1}	–	m		
	8.2	notificationIdentifier	{dmi-att 16}	–	c59		
	8.3	correlatedNotifications	{dmi-att 12}	–	o		
	8.3.1	correlatedNotification	–	–	c:m		
	8.3.2	sourceObjectInst	–	–	c:o		
	8.3.2.1	distinguishedName	–	–	c:o.17		
	8.3.2.2	nonSpecificForm	–	–	c:o.17		
	8.3.2.3	localDistinguishedName	–	–	c:o.17		
	8.4	additionalText	{dmi-att 7}	–	o		
	8.5	additionalInformation	{dmi-att 6}	–	o		

c52: if D.15/1.5 then m else –.

c53: if D.15/2.4 then m else –.

c54: if D.15/3.4 then m else –.

c55: if D.15/4.7 then m else –.

c56: if D.15/5.7 then m else –.

c57: if D.15/6.7 then m else –.

c58: if D.15/7.2 then m else –.

c59: if D.15/8.3 then m else –.

D.7 Targets managed object class

D.7.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the targets managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.16.

Table D.16 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	targets	{ac-obj 5}		

If the answer to the actual class question in the managed object class support Table D.16 is "N", the supplier of the implementation shall supply the actual class support details, in Table D.17.

Table D.17 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.7.2 Packages

See Table D.18.

Table D.18 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c60		
3	allomorphicPackage	{dmi-pkg 17}	–	c61		
4	accessControlPackage	–	–	m		
5	targetsPackage	–	–	m		
6	operationsListPackage	{ac-pkg 15}	–	o		

c60: if D.18/3 or D.18/6 then m else –.

c61: if D.16/1b then – else m.

D.7.3 Attributes

See Table D.19.

Table D.19 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c62		c62	
4	allomorphs	{dmi-att 50}	–	c63		c63	
5	accessControlObjectName	{ac-att 3}	–	m		m	
6	managedObjectClasses	{ac-att 18}	–	m		m	
7	managedObjectInstances	{ac-att 19}	–	m		m	
8	scope	{ac-att 22}	–	m		m	
9	filter	{ac-att 13}	–	m		m	
10	operationsList	{ac-att 21}	–	c64		c64	

Table D.19 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	m		m		m		–		
7	m		m		m		–		
8	m		m		–		–		
9	m		m		–		–		
10	c64		c64		c64		–		

c62: if D.18/2 then m else –.
c63: if D.18/3 then m else –.
c64: if D.18/6 then m else –.

D.7.4 Notifications

See Table D.20.

Table D.20 – Notification support

Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Support		Additional information
					Confirmed	Non-confirmed	
1	attributeValueChange	{dmi-not 1}	–	m			
2	objectCreation	{dmi-not 6}	–	m			
3	objectDeletion	{dmi-not 7}	–	m			

Table D.20 *(continued)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeIdentifierList	{dmi-att 8}	–	o		
	1.3	attributeValueChangeDefinition	{dmi-att 10}	–	m		
	1.3.1	attributeId	–	–	m		
	1.3.2	oldAttributeValue	–	–	o		
	1.3.3	newAttributeValue	–	–	m		
	1.4	notificationIdentifier	{dmi-att 16}	–	c65		
	1.5	correlatedNotifications	{dmi-att 12}	–	o		
	1.5.1	correlatedNotification	–	–	c:m		
	1.5.2	sourceObjectInst	–	–	c:o		
	1.5.2.1	distinguishedName	–	–	c:o.18		
	1.5.2.2	nonSpecificForm	–	–	c:o.18		
	1.5.2.3	localDistinguishedName	–	–	c:o.18		
	1.6	additionalText	{dmi-att 7}	–	o		
	1.7	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c66		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.19		
	2.4.2.2	nonSpecificForm	–	–	c:o.19		
	2.4.2.3	localDistinguishedName	–	–	c:o.19		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		
3	3.1	sourceIndicator	{dmi-att 26}	–	o		
	3.2	attributeList	{dmi-att 9}	–	o		
	3.3	notificationIdentifier	{dmi-att 16}	–	c67		
	3.4	correlatedNotifications	{dmi-att 12}	–	o		

Table D.20 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
3	3.4.1	correlatedNotification	–	–	c:m		
(cont.)	3.4.2	sourceObjectInst	–	–	c:o		
	3.4.2.1	distinguishedName	–	–	c:o.20		
	3.4.2.2	nonSpecificForm	–	–	c:o.20		
	3.4.2.3	localDistinguishedName	–	–	c:o.20		
	3.5	additionalText	{dmi-att 7}	–	o		
	3.6	additionalInformation	{dmi-att 6}	–	o		
c65: if D.20/1.5 then m else –. c66: if D.20/2.4 then m else –. c67: if D.20/3.4 then m else –.							

D.8 Operations managed object class

D.8.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the operations managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.21.

Table D.21 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	operations	{ac-obj 6}		

If the answer to the actual class question in the managed object class support Table D.21 is "N", the supplier of the implementation shall supply the actual class support details, in Table D.22.

Table D.22 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.8.2 Packages

See Table D.23.

Table D.23 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c68		
3	allomorphicPackage	{dmi-pkg 17}	–	c69		
4	accessControlPackage	–	–	m		
5	operationsPackage	–	–	m		
6	attributeIdsPackage	{ac-pkg 8}	–	o		
7	attributeModificationPackage	{ac-pkg 9}	–	o		
8	actionsPackage	{ac-pkg 10}	–	o		
9	scopePackage	{ac-pkg 11}	–	o		
c68: if D.23/3 or D.23/6 or D.23/7 or D.23/8 or D.23/9 then m else –. c69: if C.21/1b then – else m.						

D.8.3 Attributes

See Table D.24.

Table D.24 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c70		c70	
4	allomorphs	{dmi-att 50}	–	c71		c71	
5	operationType	{ac-att 20}	–	m		m	
6	attributeIdentifierList	{dmi-att 8}	–	c72		c72	
7	attributeFilterList	{ac-att 5}	–	c73		c73	
8	actionFilterList	{ac-att 4}	–	c74		c74	
9	scopeFilter	{ac-att 23}	–	c75		c75	
10	synchronizationFilter	{ac-att 27}	–	c75		c75	

Table D.24 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	–		–		–		–		
7	c73		c73		c73		–		
8	c74		c74		c74		–		
9	c75		–		–		–		
10	c75		–		–		–		

c70: if D.23/2 then m else –.
c71: if D.23/3 then m else –.
c72: if D.23/6 then m else –.
c73: if D.23/7 then m else –.
c74: if D.23/8 then m else –.
c75: if D.23/9 then m else –.

D.8.4 Notifications

See Table D.25.

Table D.25 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	attributeValueChange	{dmi-not 1}	–	m			
2	objectCreation	{dmi-not 6}	–	m			
3	objectDeletion	{dmi-not 7}	–	m			

Table D.25 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeIdentifierList	{dmi-att 8}	–	o		
	1.3	attributeValueChangeDefinition	{dmi-att 10}	–	m		
	1.3.1	attributeId	–	–	m		
	1.3.2	oldAttributeValue	–	–	o		
	1.3.3	newAttributeValue	–	–	m		
	1.4	notificationIdentifier	{dmi-att 16}	–	c76		
	1.5	correlatedNotifications	{dmi-att 12}	–	o		
	1.5.1	correlatedNotification	–	–	c:m		
	1.5.2	sourceObjectInst	–	–	c:o		
	1.5.2.1	distinguishedName	–	–	c:o.21		
	1.5.2.2	nonSpecificForm	–	–	c:o.21		
	1.5.2.3	localDistinguishedName	–	–	c:o.21		
	1.6	additionalText	{dmi-att 7}	–	o		
	1.7	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c77		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.22		
	2.4.2.2	nonSpecificForm	–	–	c:o.22		
	2.4.2.3	localDistinguishedName	–	–	c:o.22		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		
3	3.1	sourceIndicator	{dmi-att 26}	–	o		
	3.2	attributeList	{dmi-att 9}	–	o		
	3.3	notificationIdentifier	{dmi-att 16}	–	c78		
	3.4	correlatedNotifications	{dmi-att 12}	–	o		
	3.4.1	correlatedNotification	–	–	c:m		
	3.4.2	sourceObjectInst	–	–	c:o		
	3.4.2.1	distinguishedName	–	–	c:o.23		
	3.4.2.2	nonSpecificForm	–	–	c:o.23		
	3.4.2.3	localDistinguishedName	–	–	c:o.23		
	3.5	additionalText	{dmi-att 7}	–	o		
	3.6	additionalInformation	{dmi-att 6}	–	o		

c76: if D.25/1.5 then m else –.

c77: if D.25/2.4 then m else –.

c78: if D.25/3.4 then m else –.

D.8.5 Parameters

The supplier of the implementation shall state which items are supported in Table D.26 and if necessary provide additional information.

Table D.26 – Parameter support

					Support		
Index	Parameter template label	Value of parameter identifier	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	invalidAccessControlFilter	{ac-par 1}	–	c79			
c79: if D.23/7 or D.23/9 then o else –.							

D.9 ACL initiators managed object class

D.9.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the ACL initiators managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.27.

Table D.27 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	aclInitiators	{ac-obj 8}		

If the answer to the actual class question in the managed object class support Table D.27 is "N", the supplier of the implementation shall supply the actual class support details, in Table D.28.

Table D.28 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.9.2 Packages

See Table D.29.

Table D.29 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c80		
3	allomorphicPackage	{dmi-pkg 17}	–	c81		
4	accessControlPackage	–	–	m		
5	initiatorsPackage	–	–	m		
6	aclPackage	{ac-pkg 12}	–	m		
c80: if D.29/3 then m else –. c81: if D.26/1b then – else m.						

D.9.3 Attributes

See Table D.30.

Table D.30 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c82		c82	
4	allomorphs	{dmi-att 50}	–	c83		c83	
5	accessControlObjectName	{ac-att 3}	–	m		m	
6	initiatorACImandated	{ac-att 14}	–	m		m	
7	accessControlList	{ac-att 1}	–	m		m	

Table D.30 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	m		–		–		m		
7	m		m		m		–		
c82: if D.30/2 then m else –. c83: if D.30/3 then m else –.									

D.9.4 Notifications

See Table D.31.

Table D.31 – Notification support

Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Support		Additional information
					Confirmed	Non-confirmed	
1	attributeValueChange	{dmi-not 1}	–	m			
2	objectCreation	{dmi-not 6}	–	m			
3	objectDeletion	{dmi-not 7}	–	m			

Table D.31 *(continued)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeIdentifierList	{dmi-att 8}	–	o		
	1.3	attributeValueChangeDefinition	{dmi-att 10}	–	m		
	1.3.1	attributeId	–	–	m		
	1.3.2	oldAttributeValue	–	–	o		
	1.3.3	newAttributeValue	–	–	m		
	1.4	notificationIdentifier	{dmi-att 16}	–	c84		
	1.5	correlatedNotifications	{dmi-att 12}	–	o		
	1.5.1	correlatedNotification	–	–	c:m		
	1.5.2	sourceObjectInst	–	–	c:o		
	1.5.2.1	distinguishedName	–	–	c:o.24		
	1.5.2.2	nonSpecificForm	–	–	c:o.24		
	1.5.2.3	localDistinguishedName	–	–	c:o.24		
	1.6	additionalText	{dmi-att 7}	–	o		
	1.7	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c85		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.25		
	2.4.2.2	nonSpecificForm	–	–	c:o.25		
	2.4.2.3	localDistinguishedName	–	–	c:o.25		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		
3	3.1	sourceIndicator	{dmi-att 26}	–	o		
	3.2	attributeList	{dmi-att 9}	–	o		
	3.3	notificationIdentifier	{dmi-att 16}	–	c86		
	3.4	correlatedNotifications	{dmi-att 12}	–	o		

Table D.31 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
3	3.4.1	correlatedNotification	–	–	c:m		
(cont.)	3.4.2	sourceObjectInst	–	–	c:o		
	3.4.2.1	distinguishedName	–	–	c:o.26		
	3.4.2.2	nonSpecificForm	–	–	c:o.26		
	3.4.2.3	localDistinguishedName	–	–	c:o.26		
	3.5	additionalText	{dmi-att 7}	–	o		
	3.6	additionalInformation	{dmi-att 6}	–	o		
c84: if D.31/1.5 then m else –. c85: if D.31/2.4 then m else –. c86: if D.31/3.4 then m else –.							

D.10 Capability initiators managed object class

D.10.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the capability initiators managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.32.

Table D.32 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	capabilityInitiators	{ac-obj 9}		

If the answer to the actual class question in the managed object class support Table D.32 is “N”, the supplier of the implementation shall supply the actual class support details, in Table D.33.

Table D.33 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.10.2 Packages

See Table D.34.

Table D.34 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c87		
3	allomorphicPackage	{dmi-pkg 17}	–	c88		
4	accessControlPackage	–	–	m		
5	initiatorsPackage	–	–	m		
6	capabilityPackage	{ac-pkg 13}	–	m		
c87: if D.34/3 then m else –. c88: if D.31/1b then – else m.						

D.10.3 Attributes

See Table D.35.

Table D.35 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c89		c89	
4	allomorphs	{dmi-att 50}	–	c90		c90	
5	accessControlObjectName	{ac-att 3}	–	m		m	
6	initiatorACImandated	{ac-att 14}	–	m		m	
7	capabilityIdentitiesList	{ac-att 7}	–	m		m	

Table D.35 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	m		–		–		m		
7	m		–		–		–		
c89: if D.34/2 then m else –. c90: if D.34/3 then m else –.									

D.10.4 Notifications

See Table D.36.

Table D.36 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	attributeValueChange	{dmi-not 1}	–	m			
2	objectCreation	{dmi-not 6}	–	m			
3	objectDeletion	{dmi-not 7}	–	m			

Table D.36 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeIdentifierList	{dmi-att 8}	–	o		
	1.3	attributeValueChangeDefinition	{dmi-att 10}	–	m		
	1.3.1	attributeId	–	–	m		
	1.3.2	oldAttributeValue	–	–	o		
	1.3.3	newAttributeValue	–	–	m		
	1.4	notificationIdentifier	{dmi-att 16}	–	c91		
	1.5	correlatedNotifications	{dmi-att 12}	–	o		
	1.5.1	correlatedNotification	–	–	c:m		
	1.5.2	sourceObjectInst	–	–	c:o		
	1.5.2.1	distinguishedName	–	–	c:o.27		
	1.5.2.2	nonSpecificForm	–	–	c:o.27		
	1.5.2.3	localDistinguishedName	–	–	c:o.27		
	1.6	additionalText	{dmi-att 7}	–	o		
	1.7	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c92		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.28		
	2.4.2.2	nonSpecificForm	–	–	c:o.28		
	2.4.2.3	localDistinguishedName	–	–	c:o.28		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		
3	3.1	sourceIndicator	{dmi-att 26}	–	o		
	3.2	attributeList	{dmi-att 9}	–	o		
	3.3	notificationIdentifier	{dmi-att 16}	–	c93		
	3.4	correlatedNotifications	{dmi-att 12}	–	o		
	3.4.1	correlatedNotification	–	–	c:m		
	3.4.2	sourceObjectInst	–	–	c:o		
	3.4.2.1	distinguishedName	–	–	c:o.29		
	3.4.2.2	nonSpecificForm	–	–	c:o.29		
	3.4.2.3	localDistinguishedName	–	–	c:o.29		
	3.5	additionalText	{dmi-att 7}	–	o		
	3.6	additionalInformation	{dmi-att 6}	–	o		

c91: if D.36/1.5 then m else –.

c92: if D.36/2.4 then m else –.

c93: if D.36/3.4 then m else –.

D.11 Label initiators managed object class

D.11.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the label initiators managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.37.

Table D.37 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	labelInitiators	{ac-obj 10}		

If the answer to the actual class question in the managed object class support Table D.37 is "N", the supplier of the implementation shall supply the actual class support details, in Table D.38.

Table D.38 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.11.2 Packages

See Table D.39.

Table D.39 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c94		
3	allomorphicPackage	{dmi-pkg 17}	–	c95		
4	accessControlPackage	–	–	m		
5	initiatorsPackage	–	–	m		
6	labelPackage	{ac-pkg 14}	–	m		
c94: if D.39/3 then m else –. c95: if D.37/1b then – else m.						

D.11.3 Attributes

See Table D.40.

Table D.40 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c96		c96	
4	allomorphs	{dmi-att 50}	–	c97		c97	
5	accessControlObjectName	{ac-att 3}	–	m		m	
6	initiatorACImandated	{ac-att 14}	–	m		m	
7	securityLabel	{ac-att 24}	–	m		m	

Table D.40 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	m		–		–		m		
7	m		–		–		–		

c96: if D.39/2 then m else –.
c97: if D.39/3 then m else –.

D.11.4 Notifications

See Table D.41.

Table D.41 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	attributeValueChange	{dmi-not 1}	–	m			
2	objectCreation	{dmi-not 6}	–	m			
3	objectDeletion	{dmi-not 7}	–	m			

Table D.41 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeIdentifierList	{dmi-att 8}	–	o		
	1.3	attributeValueChangeDefinition	{dmi-att 10}	–	m		
	1.3.1	attributeId	–	–	m		
	1.3.2	oldAttributeValue	–	–	o		
	1.3.3	newAttributeValue	–	–	m		
	1.4	notificationIdentifier	{dmi-att 16}	–	c98		
	1.5	correlatedNotifications	{dmi-att 12}	–	o		
	1.5.1	correlatedNotification	–	–	c:m		
	1.5.2	sourceObjectInst	–	–	c:o		
	1.5.2.1	distinguishedName	–	–	c:o.30		
	1.5.2.2	nonSpecificForm	–	–	c:o.30		
	1.5.2.3	localDistinguishedName	–	–	c:o.30		
	1.6	additionalText	{dmi-att 7}	–	o		
	1.7	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c99		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.31		
	2.4.2.2	nonSpecificForm	–	–	c:o.31		
	2.4.2.3	localDistinguishedName	–	–	c:o.31		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		
3	3.1	sourceIndicator	{dmi-att 26}	–	o		
	3.2	attributeList	{dmi-att 9}	–	o		
	3.3	notificationIdentifier	{dmi-att 16}	–	c100		
	3.4	correlatedNotifications	{dmi-att 12}	–	o		
	3.4.1	correlatedNotification	–	–	c:m		
	3.4.2	sourceObjectInst	–	–	c:o		
	3.4.2.1	distinguishedName	–	–	c:o.32		
	3.4.2.2	nonSpecificForm	–	–	c:o.32		
	3.4.2.3	localDistinguishedName	–	–	c:o.32		
	3.5	additionalText	{dmi-att 7}	–	o		
	3.6	additionalInformation	{dmi-att 6}	–	o		

c98: if D.41/1.5 then m else –.

c99: if D.41/2.4 then m else –.

c100: if D.41/3.4 then m else –.

D.12 Assigned labels managed object class

D.12.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the assigned labels managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.42.

Table D.42 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	labelInitiators	{ac-obj 10}		

If the answer to the actual class question in the managed object class support Table D.42 is “N”, the supplier of the implementation shall supply the actual class support details, in Table D.43.

Table D.43 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.12.2 Packages

See Table D.44.

Table D.44 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c101		
3	allomorphicPackage	{dmi-pkg 17}	–	c102		
4	assignedLabelsPackage	–	–	m		
c101: if D.44/3 then m else –. c102: if D.42/1b then – else m.						

D.12.3 Attributes

See Table D.45.

Table D.45 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c103		c103	
4	allomorphs	{dmi-att 50}	–	c104		c104	
5	labelName	{ac-att 17}	–	m		m	
6	securityLabel	{ac-att 24}	–	m		m	

Table D.45 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	–		–		–		m		
c103: if D.44/2 then m else –. c104: if D.44/3 then m else –.									

D.12.4 Notifications

See Table D.46.

Table D.46 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	objectCreation	{dmi-not 6}	–	m			
2	objectDeletion	{dmi-not 7}	–	m			

Table D.46 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeList	{dmi-att 9}	–	o		
	1.3	notificationIdentifier	{dmi-att 16}	–	c105		
	1.4	correlatedNotifications	{dmi-att 12}	–	o		
	1.4.1	correlatedNotification	–	–	c:m		
	1.4.2	sourceObjectInst	–	–	c:o		
	1.4.2.1	distinguishedName	–	–	c:o.33		
	1.4.2.2	nonSpecificForm	–	–	c:o.33		
	1.4.2.3	localDistinguishedName	–	–	c:o.33		
	1.5	additionalText	{dmi-att 7}	–	o		
	1.6	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c106		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.34		
	2.4.2.2	nonSpecificForm	–	–	c:o.34		
	2.4.2.3	localDistinguishedName	–	–	c:o.34		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		
c105: if D.46/1.4 then m else –. c106: if D.46/1.4 then m else –.							

D.13 Attribute labels managed object class

D.13.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the access control rules managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.47.

Table D.47 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	attributeLabel	{ac-obj 12}		

If the answer to the actual class question in the managed object class support Table D.47 is “N”, the supplier of the implementation shall supply the actual class support details, in Table D.48.

Table D.48 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.13.2 Packages

See Table D.49.

Table D.49 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c107		
3	allomorphicPackage	{dmi-pkg 17}	–	c108		
4	assignedLabelsPackage	–	–	m		
5	attributeLabelPackage	–	–	m		
c107: if D.49/3 then m else –. c108: if D.47/1b then – else m.						

D.13.3 Attributes

See Table D.50.

Table D.50 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c109		c109	
4	allomorphs	{dmi-att 50}	–	c110		c110	
5	labelName	{ac-att 17}	–	m		m	
6	securityLabel	{ac-att 24}	–	m		m	
7	managedObjectInstance	{dmi-att 61}	–	m		m	
8	attributeIdentifierList	{dmi-att 8}	–	m		m	

Table D.50 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	–		–		–		m		
7	m		–		–		–		
8	m		–		–		–		
c109: if D.48/2 then m else –. c110: if D.49/3 then m else –.									

D.13.4 Notifications

See Table D.51.

Table D.51 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	objectCreation	{dmi-not 6}	–	m			
2	objectDeletion	{dmi-not 7}	–	m			

Table D.51 *(continued)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeList	{dmi-att 9}	–	o		
	1.3	notificationIdentifier	{dmi-att 16}	–	c111		
	1.4	correlatedNotifications	{dmi-att 12}	–	o		
	1.4.1	correlatedNotification	–	–	c:m		
	1.4.2	sourceObjectInst	–	–	c:o		
	1.4.2.1	distinguishedName	–	–	c:o.35		
	1.4.2.2	nonSpecificForm	–	–	c:o.35		
	1.4.2.3	localDistinguishedName	–	–	c:o.35		
	1.5	additionalText	{dmi-att 7}	–	o		
	1.6	additionalInformation	{dmi-att 6}	–	o		

Table D.51 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c112		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.36		
	2.4.2.2	nonSpecificForm	–	–	c:o.36		
	2.4.2.3	localDistinguishedName	–	–	c:o.36		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		
c111: if D.51/1.4 then m else –. c112: if D.51/2.4 then m else –.							

D.14 Instance label managed object class

D.14.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the instance label managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.52.

Table D.52 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	instanceLabel	{ac-obj 13}		

If the answer to the actual class question in the managed object class support Table D.52 is “N”, the supplier of the implementation shall supply the actual class support details, in Table D.53.

Table D.53 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.14.2 Packages

See Table D.54.

Table D.54 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c113		
3	allomorphicPackage	{dmi-pkg 17}	–	c114		
4	assignedLabelPackage	–	–	m		
5	instanceLabelPackage	–	–	m		
c113: if D.53/3 then m else –. c114: if D.51/1b then – else m.						

D.14.3 Attributes

See Table D.55.

Table D.55 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c115		c115	
4	allomorphs	{dmi-att 50}	–	c116		c116	
5	labelName	{ac-att 17}	–	m		m	
6	securityLabel	{ac-att 24}	–	m		m	
7	managedObjectInstances	{ac-att 19}	–	m		m	

Table D.55 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	–		–		–		m		
7	m		–		–		–		
c115: if D.53/2 then m else –. c116: if D.53/3 then m else –.									

D.14.4 Notifications

See Table D.56.

Table D.56 – Notification support

Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Support		Additional information
					Confirmed	Non-confirmed	
1	objectCreation	{dmi-not 6}	–	m			
2	objectDeletion	{dmi-not 7}	–	m			

Table D.56 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeList	{dmi-att 9}	–	o		
	1.3	notificationIdentifier	{dmi-att 16}	–	c117		
	1.4	correlatedNotifications	{dmi-att 12}	–	o		
	1.4.1	correlatedNotification	–	–	c:m		
	1.4.2	sourceObjectInst	–	–	c:o		
	1.4.2.1	distinguishedName	–	–	c:o.37		
	1.4.2.2	nonSpecificForm	–	–	c:o.37		
	1.4.2.3	localDistinguishedName	–	–	c:o.37		
	1.5	additionalText	{dmi-att 7}	–	o		
	1.6	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c118		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.38		
	2.4.2.2	nonSpecificForm	–	–	c:o.38		
	2.4.2.3	localDistinguishedName	–	–	c:o.38		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		

c117: if D.56/1.4 then m else –.

c118: if D.56/2.4 then m else –.

D.15 Class label managed object class

D.15.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the class label managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table D.57.

Table D.57 – Managed object class support

Index	Managed object class template label	Value of object identifier for class	Support of all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	classLabel	{ac-obj 14}		

If the answer to the actual class question in the managed object class support Table D.57 is "N", the supplier of the implementation shall supply the actual class support details, in Table D.58.

Table D.58 – Actual class support

Index	Actual managed object class template label	Value of object identifier for actual class	Additional information

D.15.2 Packages

See Table D.59.

Table D.59 – Package support

Index	Package template label	Value of object identifier for package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c119		
3	allomorphicPackage	{dmi-pkg 17}	–	c120		
4	assignedLabelsPackage	–	–	m		
5	classLabelPackage	–	–	m		
c119: if D.57/3 then m else –. c120: if D.55/1b then – else m.						

D.15.3 Attributes

See Table D.60.

Table D.60 – Attribute support

				Set by Create		Get	
Index	Attribute template label	Value of object identifier for attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	m		m	
2	nameBinding	{dmi-att 63}	–	m		m	
3	packages	{dmi-att 66}	–	c121		c121	
4	allomorphs	{dmi-att 50}	–	c122		c122	
5	labelName	{ac-att 17}	–	m		–	
6	securityLabel	{ac-att 24}	–	m		m	
7	managedObjectClasses	{ac-att 18}	–	m		m	

Table D.60 *(concluded)* **– Attribute support**

	Replace		Add		Remove		Set to Default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	–		–		–		m		
7	–		–		–		–		
c121: if D.59/2 then m else –. c122: if D.59/3 then m else –.									

D.15.4 Notifications

See Table D.61.

Table D.61 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	objectCreation	{dmi-not 6}	–	m			
2	objectDeletion	{dmi-not 7}	–	m			

Table D.61 *(concluded)* **– Notification support**

Index	Sub-index	Notification field name label	Value of object identifier of attribute type associated with field	Constraints and values	Status	Support	Additional information
1	1.1	sourceIndicator	{dmi-att 26}	–	o		
	1.2	attributeList	{dmi-att 9}	–	o		
	1.3	notificationIdentifier	{dmi-att 16}	–	c123		
	1.4	correlatedNotifications	{dmi-att 12}	–	o		
	1.4.1	correlatedNotification	–	–	c:m		
	1.4.2	sourceObjectInst	–	–	c:o		
	1.4.2.1	distinguishedName	–	–	c:o.39		
	1.4.2.2	nonSpecificForm	–	–	c:o.39		
	1.4.2.3	localDistinguishedName	–	–	c:o.39		
	1.5	additionalText	{dmi-att 7}	–	o		
	1.6	additionalInformation	{dmi-att 6}	–	o		
2	2.1	sourceIndicator	{dmi-att 26}	–	o		
	2.2	attributeList	{dmi-att 9}	–	o		
	2.3	notificationIdentifier	{dmi-att 16}	–	c124		
	2.4	correlatedNotifications	{dmi-att 12}	–	o		
	2.4.1	correlatedNotification	–	–	c:m		
	2.4.2	sourceObjectInst	–	–	c:o		
	2.4.2.1	distinguishedName	–	–	c:o.40		
	2.4.2.2	nonSpecificForm	–	–	c:o.40		
	2.4.2.3	localDistinguishedName	–	–	c:o.40		
	2.5	additionalText	{dmi-att 7}	–	o		
	2.6	additionalInformation	{dmi-att 6}	–	o		

c123: if D.61/2.4 then m else –.

c124: if D.61/3.4 then m else –.

Anexo E

Formulario de MRCS para vinculación de nombres[8)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

E.1 Introduction

The purpose of this MRCS proforma for name bindings is to provide a mechanism for a supplier which claims conformance to a name binding to provide conformance information in a standard form.

E.2 Instructions for completing the MRCS proforma for name binding to produce a MRCS

The MRCS proforma contained in this annex is comprised of information in tabular form, in accordance with ITU-T Rec. X.724 | ISO/IEC 10165-6. The supplier of the implementation shall state which items are supported in Table E.1 and if necessary provide additional information.

Notations used in the Status and Support columns are specified in B.1.3.

E.3 Symbols, abbreviations and terms

The following abbreviation is used in this proforma:

ac-nb **joint-iso-ccitt ms(9) function(2) part9(9) nameBinding(6)**

E.4 Statement of conformance to the name binding

See Table E.1.

Table E.1 – Name binding support

Index	Name binding template label	Value of object identifier for name binding	Constraints and values	Status	Support	Additional information
1	rule-accessControlRules	{ac-nb 1}	–	o		
2	operations-targets	{ac-nb 2}	–	o		
3	notificationEmitter-accessControlRules	{ac-nb 3}	–	o		
4	attributeLabel-assignedLabels	{ac-nb 4}	–	o		
5	instanceLabel-assignedLabels	{ac-nb 5}	–	o		
6	classLabel-assignedLabels	{ac-nb 6}	–	o		

8) Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de MRCS de este anexo a fin de que pueda ser utilizado para los fines previstos, y pueden además publicar el MRCS cumplimentado. En la Rec. UIT-T X.724 | ISO/CEI 10165-6 se especifican las instrucciones para rellenar el formulario de MRCS.

Table E.1 *(concluded)* **– Name binding support**

Index	Sub-index	Operation	Constraints and values	Status	Support	Additional information
1	1.1	Create support	–	m		
	1.1.1	Create with automatic instance naming	–	m		
	1.1.2	Create with reference object	–	m		
	1.2	Delete support	–	m		
	1.2.1	Delete only if no contained objects	–	m		
	1.2.2	Delete contained objects	–	–		
2	2.1	Create support	–	m		
	2.1.1	Create with automatic instance naming	–	–		
	2.1.2	Create with reference object	–	m		
	2.2	Delete support	–	m		
	2.2.1	Delete only if no contained objects	–	m		
	2.2.2	Delete contained objects	–	–		
3	3.1	Create support	–	m		
	3.1.1	Create with automatic instance naming	–	m		
	3.1.2	Create with reference object	–	m		
	3.2	Delete support	–	m		
	3.2.1	Delete only if no contained objects	–	m		
	3.2.2	Delete contained objects	–	–		
4	4.1	Create support	–	m		
	4.1.1	Create with automatic instance naming	–	–		
	4.1.2	Create with reference object	–	–		
	4.2	Delete support	–	m		
	4.2.1	Delete only if no contained objects	–	–		
	4.2.2	Delete contained objects	–	–		
5	5.1	Create support	–	m		
	5.1.1	Create with automatic instance naming	–	–		
	5.1.2	Create with reference object	–	–		
	5.2	Delete support	–	m		
	5.2.1	Delete only if no contained objects	–	–		
	5.2.2	Delete contained objects	–	–		
6	6.1	Create support	–	m		
	6.1.1	Create with automatic instance naming	–	–		
	6.1.2	Create with reference object	–	–		
	6.2	Delete support	–	m		
	6.2.1	Delete only if no contained objects	–	–		
	6.2.2	Delete contained objects	–	–		

Anexo F

Formulario de MIDS (parámetros)[9)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

F.1 Introduction

The purpose of this MIDS proforma for parameters is to provide a mechanism for a supplier which claims conformance to the parameter to provide conformance information in a standard form.

F.2 Instructions for completing the MIDS proforma for parameters to produce a MIDS

The MIDS proforma contained in this annex is comprised of information in tabular form, in accordance with ITU-T Rec. X.724 | ISO/IEC 10165-6. The supplier of the implementation shall state which items are supported in Table F.1 and if necessary provide additional information.

Notations used in the Status and Support columns are specified in B.1.3.

F.3 Symbols, abbreviations and terms

The following abbreviation is used in this proforma:

ac-par **joint-iso-ccitt ms(9) function(2) part9(9) parameter(5)**

F.4 Instructions for completing the MIDS proforma

The specifier of a managed object class that claims to support the notifications specified by ITU-T Rec. X.741 | ISO/IEC 10164-9 shall import a copy of this annex and complete it according to the instructions specified in ITU-T Rec. X.724 | ISO/IEC 10165-6.

Table F.1 – Parameter support

					Support		
Index	Parameter template label	Value of parameter identifier	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	invalidAccessControlFilter	{ac-par 1}	–	o			

9) Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de MIDS de este anexo a fin de que pueda ser utilizado para los fines previstos, y pueden además publicar el MIDS cumplimentado. En la Rec. UIT-T X.724 | ISO/CEI 10165-6 se especifican las instrucciones para rellenar el formulario de MIDS.

Anexo G

Parámetros de control de acceso del CMIS

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

G.1 Certificado de control de acceso

Esta información puede utilizarse para especificar el parámetro de control de acceso que puede utilizarse con el CMIP. La especificación de una política de control de acceso puede incluir su propia definición de esta información.

Un certificado de control de acceso (ACC, *access control certificate*), conocido también como certificado de acceso privilegiado (PAC, *privilege access certificate*) puede contener los siguientes tipos de información:

- la identidad del dominio de seguridad y la autoridad del dominio de seguridad;
- la información de control de acceso requerida por la política de control de acceso. Esta información puede ser una o varias de las capacidades del iniciador, el nombre del iniciador, o etiquetas de seguridad;
- el momento en que la información de control de acceso pasa a ser válida;
- el momento en que la información de control de acceso deja de ser válida;
- el momento en que el ACC fue creado;
- información que puede ser utilizada para comprobaciones de integridad.

NOTA – Varias organizaciones están normalizando ACC apropiados. Entre estas organizaciones pueden mencionarse el Subcomité 27 de la ISO/CEI, la asociación europea de fabricantes de computadoras (ECMA, *european computer manufacturers association*), etc. Se alienta a los realizadores a que investiguen la posibilidad de utilizar los ACC de estas organizaciones.

Anexo H

Relación con la Rec. UIT-T X.812 | ISO/CEI 10181-3: Marcos de seguridad en sistemas abiertos – Control de acceso

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

H.1 Introducción

Los procedimientos y la información de gestión definidos en esta Recomendación | Norma Internacional están destinados a ser utilizados junto con los esquemas de control de acceso descritos en la Rec. UIT-T X.812 | ISO/CEI 10181-3. Este anexo informativo relaciona la terminología, los procedimientos y la información de gestión definidos en esta Recomendación | Norma Internacional con la terminología, los procedimientos y los requisitos de información de gestión pertinentes descritos en la Rec. UIT-T X.812 | ISO/CEI 10181-3.

H.2 Sinopsis de la terminología pertinente de la Rec. UIT-T X.812 | ISO/CEI 10181-3

Es necesario entender los términos siguientes definidos en la Rec. UIT T X.812 | ISO/CEI 10181-3 para relacionar la terminología, los procedimientos y los requisitos de información de gestión ahí descritos con la terminología, los procedimientos y la información de gestión definidos en esta Recomendación | Norma Internacional.

- *ACI vinculada a iniciador:* Información de control de acceso vinculada a un iniciador, es decir información transmitida con una petición de acceso o asociada con el iniciador de una petición a través de mecanismos locales. Puede incluir ACI de iniciador, algunas ACI de objetivo e información contextual seleccionada. Como ejemplos pueden citarse: etiquetas de seguridad asociadas con iniciadores, capacidades, certificados de control de acceso e información contextual, tal como la localización de iniciador.

- *ACI vinculada a objetivo:* Información de control de acceso vinculada a un objetivo, es decir información vinculada al objetivo a través de información almacenada directamente en la base de información de gestión de seguridad o indicada en la base de información de gestión de seguridad como información suministrada a través de mecanismos locales. Como ejemplos pueden citarse: etiquetas de seguridad asociadas con objetivos (información de gestión protegida), identidades en listas de control de acceso, operaciones admitidas o garantizadas en los objetivos, autoridades de dominio de seguridad y el acceso garantizado a ellas, así como información contextual tal como la información de fecha y hora.

Los elementos de información de gestión definidos en esta Recomendación | Norma Internacional son ACI vinculadas a objetivo para su utilización con los esquemas de control de acceso definidos en la Rec. UIT T X.812 | ISO/CEI 10181-3.

H.3 Esquema de lista de control de acceso (ACL, *access control list*)

Como se especifica en la Rec. UIT T X.812 | ISO/CEI 10181-3 para un esquema de ACL, «el control de acceso se gestiona como una lista de parejas (cualificador del iniciador, cualificador de la petición de acceso) que constituye la ACI vinculada con el objetivo e identificadores individuales, de grupo o de rol que constituyen la ACI vinculada con el iniciador». Opcionalmente, puede incluirse un cualificador de contexto para algunas variaciones en un esquema de control de acceso.

El cualificador de iniciador es la identidad, el grupo o el rol únicos de un iniciador al que se aplica el cualificador de petición de acceso.

El cualificador de petición de acceso describe las limitaciones de las peticiones de acceso (operaciones y objetivos asociados) para las cuales el acceso ha de garantizarse o negarse a la identidad indicada en el cualificador de iniciador asociado.

El cualificador de contexto describe las limitaciones contextuales que han de añadirse a las limitaciones de cualificador de petición de acceso para algunas variaciones en el esquema de la ACL.

La información relativa a las parejas de (cualificador de iniciador, cualificador de petición de acceso) y al cualificador de contexto opcional es representada en esta Recomendación | Norma Internacional como información situada en un objeto gestionado regla que contiene uno o más objetos gestionados iniciador de ACL y uno o más objetos gestionados objetivo. La información adicional sobre petición de acceso se representa en el único objeto gestionado reglas de control de acceso que está activo para la política de seguridad aplicada.

La información relativa al cualificador de iniciador, al cualificador de petición de acceso y al cualificador de contexto se almacena en diferentes objetos gestionados, como se indica a continuación:

Cualificador de iniciador:

- un nombre de iniciador o identificador de mandatario situado en un elemento del atributo de lista de control de acceso de un objeto gestionado iniciadores de ACL.

Cualificador de petición de acceso:

- uno o más objetivos identificados por atributos en un objeto gestionado objetivos;
- limitaciones asociadas a operaciones y atributos en el objeto gestionado operaciones contenido en el objeto objetivo y que es específico del tipo de operación solicitada;
- permiso de acceso localizado en el objeto gestionado regla;
- permiso de acceso por defecto para cada tipo de operación, nombre de dominio de seguridad, granularidad de respuestas de negación localizadas en atributos del objeto gestionado reglas de control de acceso.

Cualificador de contexto:

- limitaciones contextuales localizadas en el objeto gestionado regla asociada en la forma de limitaciones relativas a la disponibilidad de planificación de la regla, condiciones de estado relativas a la información contenida en otros objetos gestionados que representan recursos, y autenticación.

La información de gestión definida en esta Recomendación | Norma Internacional puede utilizarse en diferentes variaciones del esquema de control de acceso, o combinaciones de tales variaciones, tal como se define en la Rec. UIT-T X.812 | ISO/CEI 10181-3. Remítase a la Rec. UIT-T X.812 | ISO/CEI 10181-3 para los detalles acerca de las siguientes variaciones:

- *ACL sin cualificador de petición de acceso:* Representadas por «reglas globales», tal como se define en esta Recomendación | Norma Internacional, que no contienen objetos gestionados objetivos ni operaciones asociador.
- *ACL con cualificador de contexto:* Representadas por objetos gestionados reglas que contienen información contextual. La regla puede ser «reglas globales» tal como se describe anteriormente, o «reglas individuales» tal como se define en esta Recomendación | Norma Internacional, que contienen iniciadores de ACL, objetivos, y posiblemente objetos gestionados operaciones.
- *ACL con objetivos agrupados:* Representadas por reglas individuales con múltiples objetivos protegidos especificados por los objetos gestionados objetivos contenidos.
- *ACL con cualificador de objetivo:* Representadas por reglas individuales.
- *ACL con iniciadores agrupados:* Parcialmente representadas por una combinación de reglas globales e individuales. Debe suministrarse información local adicional para controlar el orden de procesamiento de las reglas con el fin de tener en cuenta la granularidad de control de acceso a los subgrupos dentro de un grupo.
- *ACL ordenadas parcialmente:* Representadas por una combinación de reglas globales e individuales – con información local adicional suministrada para controlar el orden de búsqueda al procesar reglas y sus listas de control de acceso asociadas.

H.4 Esquema de capacidad

Como se estipula en la Rec. UIT-T X.812 | ISO/CEI 10181-3 para un esquema de capacidad, «el control de acceso se gestiona en términos de la ACI vinculada con el iniciador (una capacidad) la cual define el conjunto de reglas permitidas sobre un conjunto identificado de objetivos».

De conformidad con la Rec. UIT-T X.812 | ISO/CEI 10181-3, una ACI vinculada con el objetivo incluye identificadores individuales, de grupo y de rol, y posiblemente una lista de nombres de autoridad de dominio de seguridad y las operaciones asociadas.

Las ACI vinculadas con objetivos para un esquema de capacidad están situadas todas en el atributo de capacidad de los objetos gestionados iniciadores de capacidad.

Se identifican dos variaciones para el esquema de control de acceso de capacidad:

- *capacidades sin operaciones específicas:* Debe incluirse en la información vinculada con el objetivo únicamente un identificador individual, de grupo y de rol.
- *capacidades con limitaciones por autoridad:* La lista adicional de nombres de autoridad de dominio de seguridad y los atributos asociados deben proporcionarse en la ACI vinculada con el objetivo.

H.5 Esquema basado en la etiqueta

Como se estipula en la Rec. UIT-T X.812 | ISO/CEI 10181-3 para un esquema basado en la etiqueta, «este esquema utiliza etiquetas de seguridad que pueden asignarse a iniciadores y objetivos, así como datos que se transfieren entre sistemas».

De conformidad con la Rec. UIT-T X.812 | ISO/CEI 10181-3, una ACI vinculada con el objetivo consiste en una (sola) etiqueta de seguridad asociada con cada objetivo.

Esta Recomendación | Norma Internacional proporciona un mecanismo para asociar una sola etiqueta de seguridad con un objetivo. La etiqueta está situada en un objeto gestionado tipo de etiqueta junto con un objetivo o conjunto de objetivos identificado asociado. El orden de evaluación de los objetos gestionados etiqueta se define de manera que una sola y única etiqueta pueda asociarse con un objetivo.

H.6 Esquema basado en el contexto

Como se estipula en la Rec. UIT-T X.812 | ISO/CEI 10181-3 para un esquema basado en el contexto, el «control de acceso se gestiona en relación con la ACI vinculada con el iniciador o con el objetivo, o de forma independiente, como información que se obtiene de la ADF».

De conformidad con la Rec. UIT-T X.812 | ISO/CEI 10181-3, las listas de control de contexto contienen inscripciones que tienen dos campos:

- *cualificador de contexto:* Una secuencia de condiciones contextuales (por ejemplo, hora, ruta, localización) a las que se aplica un cualificador de operación. Cada condición contextual está asociada individualmente con un enunciado «verdadero» o «falso».
- *cualificador de operación:* La operación admitida para el cualificador de contexto asociado.

Esta Recomendación | Norma Internacional no especifica directamente limitaciones contextuales en la forma de una lista de control de contexto, sino que sitúa:

- la información de cualificador de contexto en los objetos gestionados regla en la forma de información de planificación, condiciones de estado de valores de atributo en otros objetos gestionados, y limitaciones contextuales de autenticación;
- la información de cualificador de operación en el objeto gestionado objetivos (atributo lista de operaciones), en el objeto gestionado operaciones (atributo de tipo de operación), o es implícitamente cualquier operación en el caso de reglas globales, que no contienen objetos gestionados objetivos y operaciones.

El apareamiento de los objetos gestionados reglas con sus objetos gestionados objetivos y operaciones, o en el caso de reglas globales cualquier operación implícita, puede considerarse como una lista de control de contexto.

La única variación del esquema de lista de control de contexto descrita en la Rec. UIT-T X.812 | ISO/CEI 10181-3 requiere una búsqueda ordenada de la lista de control de contexto. Esta variación puede realizarse únicamente si se especifica información local adicional para controlar la búsqueda de los objetos gestionados regla y objetivos u operaciones.