UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.841

(10/2000)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

Seguridad

Tecnología de la información – Técnicas de seguridad – Objetos de información de seguridad para control de acceso

Recomendación UIT-T X.841

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

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 declaraciones 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 de transmisión de datos por satélite	X.350–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.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–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	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	**X.800–X.849**
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999

Para más información, véase la Lista de Recomendaciones del UIT-T.

NORMA INTERNACIONAL 15816

RECOMENDACIÓN UIT-T X.841

TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – OBJETOS DE INFORMACIÓN DE SEGURIDAD PARA CONTROL DE ACCESO

Resumen

Esta Recomendación | Norma Internacional proporciona definiciones de objeto que, en muchas ocasiones, son necesarias en normas de seguridad para evitar la existencia de múltiples definiciones diferentes de la misma funcionalidad. Mediante el uso de la notación de sintaxis abstracta uno (ASN.1) se asegura la precisión de estas definiciones.

Esta Recomendación | Norma Internacional trata solamente los aspectos estáticos de los objetos de información de seguridad (SIO).

Orígenes

La Recomendación UIT-T X.841, preparada por la Comisión de Estudio 7 (1997-2000) del UIT-T, fue aprobada por la Asamblea Mundial de Normalización de las Telecomunicaciones (Montreal, 27 de septiembre – 6 de octubre de 2000). Se publica un texto idéntico como Norma Internacional ISO/CEI 15816.

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. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asemblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

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.

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.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Introducción

La presente Recomendación | Norma Internacional sobre objetos de información de seguridad (SIO) para control de acceso proporciona definiciones de objeto que, en muchas ocasiones, son necesarias en normas de seguridad para evitar la existencia de múltiples definiciones diferentes de la misma funcionalidad. La precisión de estas definiciones se obtiene mediante la utilización de la notación de sintaxis abstracta uno (ASN.1) definida en la Rec. UIT-T X.680 (1997) | ISO/CEI 8824-1:1998 y en la Rec. UIT-T X.681 (1997) | ISO/CEI 8824-2:1998.

La gestión de seguridad tiene por finalidad asegurar que los recursos, incluida la información, estén protegidos de una manera adecuada, y eficaz con relación al costo. Para proteger los intereses privados y los derechos de propiedad intelectual, las organizaciones necesitan controlar el tratamiento de su información. Pueden causarse graves daños o trastornos al originador o tenedor de información sensible si, por ejemplo, se libera dicha información y se permite que llegue a manos de terceras personas que no están autorizadas para recibirla (trasgresión de la confidencialidad), o que se modifique en cualquier forma (trasgresión de la integridad). Cada organización debe cerciorarse de que protege adecuadamente sus informaciones y recursos, en todas las formas, durante su almacenamiento, procesamiento, así como durante la transmisión, entre organizaciones y en el interior de la organización, a través de redes privadas y públicas. Cuando las actividades de las organizaciones deban tener una mayor amplitud, éstas deberán tener la certeza de que sus recursos estarán adecuadamente protegidos cuando sean detentados o procesados por otros.

El desarrollo de objetos de información de seguridad para control de acceso está motivado por la flexibilidad e interoperabilidad en la gestión de la seguridad que se obtienen cuando se utilizan estructuras comunes para funciones similares. Esta Recomendación | Norma Internacional tiene por objeto lograr una normalización de las etiquetas de seguridad y de métodos alternativos para el control de acceso.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – OBJETOS DE INFORMACIÓN DE SEGURIDAD PARA CONTROL DE ACCESO

1 Alcance

El campo de aplicación de esta Recomendación | Norma Internacional comprende:

a) la definición de directrices para especificar la sintaxis abstracta de objetos de información de seguridad (SIO, *security information objects*) genéricos y específicos;

b) la especificación de SIO para control de acceso genéricos;

c) la especificación de SIO para control de acceso específicos.

El campo de aplicación de esta Recomendación | Norma Internacional abarca solamente la "estática" de los SIO por medio de definiciones sintácticas en términos de descripciones ASN.1 y explicaciones semánticas adicionales. No abarca la "dinámica" de los SIO, por ejemplo las reglas para su creación y supresión. La dinámica de los SIO es un asunto de implementación local.

2 Referencias normativas

Las siguientes Recomendaciones y 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 los participantes en acuerdos basados en la presente Recomendaciones | Normas Internacionales investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y las Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualemente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

- Recomendación UIT-T X.411 (1999) | ISO/CEI 10021-4:2001, *Tecnología de la información – Sistemas de tratamiento de mensajes – Sistema de transferencia de mensajes: Definición del servicio abstracto y procedimientos.*
- Recomendación UIT-T X.500 (2001) | ISO/CEI 9594-1:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Visión de conjunto de conceptos, modelos y servicios*.
- Recomendación UIT-T X.501 (2001) | ISO/CEI 9594-2:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos*.
- Recomendación UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificado de clave pública y de atributos*.
- Recomendación UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica*.
- Recomendación UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de objetos de información.*
- Recomendación UIT-T X.682 (1997) | ISO/CEI 8824-3:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones.*

- Recomendación UIT-T X.683 (1997) | ISO/CEI 8824-4:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de especificaciones de la notación de sintaxis abstracta uno.*
- Recomendación UIT-T X.690 (1997) | ISO/CEI 8825-1:1998, *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida*.
- Recomendación CCITT X.722 (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.741 (1995) | ISO/CEI 10164-9:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Objetos y atributos para el control de acceso*.
- Recomendación UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores*.
- Recomendación UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.
- Recomendación UIT-T X.830 (1995) | ISO/CEI 11586-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de las capas superiores: Sinopsis, modelo y notación.*

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

- 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 – 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 **compartimentalización**: Definida en ISO/CEI DIS 2382-8.

3.2 **clase de SIO genérica**: Clase de SIO en la que los tipos de datos para uno o más de los componentes no están especificados completamente.

3.3 **objeto de información**: Definido en Rec. UIT-T X.681 | ISO/CEI 8824-2.

3.4 **clase de objeto de información**: Definido en Rec. UIT-T X.680 | ISO/CEI 8824-1.

3.5 **identificador de objeto (OID, *object identifier*)**: Definido en Rec. UIT-T X.680 | ISO/CEI 8824-1.

3.6 **sello**: Definido en Rec.UIT-T X.810 | ISO/CEI 10181-1.

3.7 **autoridad de seguridad**: Entidad encargada de la administración de una normativa de seguridad dentro de un dominio de seguridad.

3.8 **dominio de seguridad**: Colección de usuarios y sistemas sometidos a una normativa común de seguridad.

3.9 **objeto de información de seguridad**: Ejemplar de una clase de SIO.

3.10 **clase de objeto de información de seguridad**: Clase de objeto de información que ha sido especialmente adaptada para la utilización de seguridad.

3.11 **etiqueta de seguridad**: Definida en la Rec. CCITT X.800 | ISO 7498-2.

3.12 **normativa de seguridad**: Definida en ISO/CEI DIS 2382-8.

3.13 **fichero de información de normativas de seguridad**: Una construcción que conlleva información de normativa de seguridad específica del dominio.

3.14 **clase de SIO específica**: Clase de SIO en la que los tipos de datos para todos los componentes están especificados completamente.

4 Abreviaturas

A los efectos de la presente Recomendación | Norma Internacional se aplican las siguientes siglas:

ASN.1 Notación de sintaxis abstracta uno (*abstract syntax notation one*)

EE Entidad de extremo (*end entity*)

IT Tecnología de la información (*information technology*)

OID Identificador de objeto (*object identifier*)

RBAC Control de acceso basado en reglas (*rule based access control*)

SIO Objeto de información de seguridad (*security information object*)

SPIF Fichero de información de normativas de seguridad (*security policy information file*)

5 Convenios

5.1 Descripción de las clases de objeto de información de seguridad

Una clase de SIO comprende:

- un valor para un identificador de clase de SIO
- un conjunto de una o más especificaciones de tipos de datos, una para cada componente contenido en la clase de SIO; y
- un enunciado de la semántica asociada al uso de la clase de SIO.

5.2 Correspondencia de las clases de objeto de información de seguridad genérica

Una clase de SIO genérica es una clase de SIO en la que los tipos de datos para uno o más componentes no están especificados completamente. Una clase de SIO específica es una clase de SIO en la que los tipos de datos para todos los componentes están especificados completamente. Una clase de SIO genérica corresponde a una familia de clases de SIO específicas.

5.3 Composición de los objetos de información de seguridad

La especificación de cada SIO en esta Recomendación | Norma Internacional consta de las siguientes partes:

- una descripción del SIO;
- una explicación de la utilización del SIO;
- una descripción de los componentes del SIO.

La descripción de los componentes del SIO incluye la especificación en ASN.1 y el identificador de la clase de objeto que se define.

6 Especificación de objetos de información de seguridad

Cuando se identifica una nueva necesidad de un SIO, se seguirán los pasos descritos más adelante para promover la reutilización de especificaciones existentes y tratar de evitar la existencia de especificaciones diferentes que satisfacen las mismas necesidades:

- Si esta Recomendación | Norma Internacional define un SIO que satisface la nueva necesidad, se utilizará la definición contenida en esta Recomendación | Norma Internacional.
- En la definición del nuevo SIO deben utilizarse componentes de SIO definidos en esta Recomendación | Norma Internacional, si satisfacen en parte la nueva necesidad.

En las siguientes subcláusulas se incluyen especificaciones de los SIO que han sido desarrollados para soportar el control de acceso. En el anexo A se incluye como un módulo una definición ASN.1 completa de los objetos de información de seguridad examinados en esas subcláusulas. Dicho módulo se identifica como sigue:

```
id-SIOsAccessControl-MODULE OBJECT IDENTIFIER ::= {
        joint-iso-itu-t sios(24) specification(0) modules(0) accessControl(0)}
```

6.1 Etiqueta de confidencialidad

6.1.1 Introducción

Por lo general, las organizaciones tienen una o varias normativas de seguridad en las que se prevé la agrupación de datos en compartimentos que habrán de ser protegidos y tratados de la misma forma. La normativa de seguridad define la protección que habrá de aplicarse a cada compartimento.

Entre los aspectos de seguridad expresados por una normativa de seguridad, indicados en una etiqueta de seguridad, están los siguientes:

- el nivel de protección que habrá de darse a los datos almacenados en un sistema;
- quién está autorizado para el acceso a datos, procesos o recursos;
- marcas de seguridad que deben aparecer en toda presentación del material, impresa o en pantalla;
- requisitos de encaminamiento y cifrado para la transmisión de datos entre sistemas;
- requisitos de protección contra copias no autorizadas;
- métodos para el almacenamiento de datos;
- algoritmos de cifrado que habrán de utilizarse;
- métodos para la autenticación de entidades;
- si las operaciones sobre los objetos habrán o no de ser auditoría;
- si es o no necesario impedir que los destinatarios se nieguen a recibir un objeto;
- si se requieren o no firmas digitales para la autenticación de los datos y, en caso afirmativo, las firmas de quiénes.

Cuando los datos se conservan en un sistema IT, o cuando se transmiten electrónicamente entre los sistemas, dichos datos son etiquetados para indicar el compartimento a que pertenecen y, en consecuencia, la forma en que habrán de tratarse para fines de seguridad. La etiqueta podrá identificarse independientemente de la información protegida, pero tiene que estar vinculada lógicamente a ésta. La integridad de las etiquetas, y la integridad de su vinculación a la información, deberán estar garantizadas. Esto permite a los sistemas y redes IT tomar decisiones que influyen en la seguridad, tales como las relativas al control de acceso y al encaminamiento, sin necesidad de ganar acceso a la información que se protege. La etiqueta de seguridad puede asociarse a cualquier objeto de datos en un sistema IT, tales como documentos, mensajes de correo electrónico, ventanas de presentación visual, entradas en una base de datos, entradas en el directorio y formularios electrónicos. Las etiquetas están concebidas para ser utilizadas cuando los objetos se almacenan y se transfieren (en particular, entre sistemas), y cuando son tratados por aplicaciones que funcionan atendiendo a las etiquetas, incluido el caso de aplicaciones que crean nuevos objetos a partir de objetos existentes.

Cuando se deba transferir datos etiquetados entre diferentes dominios de seguridad, los dominios deben acordar la normativa de seguridad que habrá de aplicarse a esos datos. Si las etiquetas especificadas por la normativa aplicada en un dominio son diferentes de las especificadas por la normativa para datos compartidos, la normativa para datos compartidos especificará la traducción entre los dos conjuntos de etiquetas.

Las etiquetas por sí solas no bastan para garantizar la seguridad de la información. La normativa de seguridad que se aplica a la información debe ser impuesta por cada organización mientras la información etiquetada se encuentre dentro de su esfera de control. Se supone que todas las organizaciones, individuos y sistemas IT que procesan un ítem de información conocen la normativa de seguridad aplicable a esa información. Las organizaciones que intercambian información deben mantener una mutua relación de confianza, para poder tener la certeza de que la información se tratará de conformidad con las normativas de seguridad convenidas.

6.1.2 Especificación ASN.1 de la etiqueta

La etiqueta de confidencialidad se identifica como sigue:

```
id-ConfidentialityLabel OBJECT IDENTIFIER  ::= {
        joint-iso-itu-t sios(24) specification(0) securityLabels(1) confidentiality(0)}

ConfidentialityLabel  ::=  SET {
        security-policy-identifier      SecurityPolicyIdentifier OPTIONAL,
        security-classification         INTEGER(0..MAX) OPTIONAL,
        privacy-mark                    PrivacyMark OPTIONAL,
        security-categories             SecurityCategories OPTIONAL }
(ALL EXCEPT({-- none; at least one component shall be present --}))
```

```
SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

PrivacyMark ::= CHOICE {
  pString                PrintableString (SIZE(1..ub-privacy-mark-length)),
  utf8String             UTF8String (SIZE(1..ub-privacy-mark-length))
}

ub-privacy-mark-length INTEGER ::= 128 -- as defined in ITU-T Rec. X.411 | ISO/IEC 10021-4

SecurityCategories ::= SET SIZE (1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
     type [0]   SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
     value      [1]   SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type})
}

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= {…}
```

En el anexo B se da un ejemplo de la expansión de la clase de objeto de información TYPE-IDENTIFIER

6.1.3 Métodos de vinculación para etiquetas de confidencialidad

6.1.3.1 Método de vinculación 1

Una copia de los datos (D) y una copia de la etiqueta de seguridad (L) se almacenan juntas como un registro de datos, dentro de la demarcación de seguridad del sistema. Se supone que el sistema es capaz de proteger la integridad de la etiqueta de seguridad, y la integridad y posiblemente el secreto de los datos. El sistema deberá proporcionar una protección tal, que un usuario o una aplicación no autorizados no puedan alterar los datos ni la etiqueta de seguridad asociada a éstos. Con este método de vinculación no se necesita una función criptográfica para vincular los datos y la etiqueta de seguridad.

6.1.3.2 Método de vinculación 2

A partir de D y L se calcula una firma digital no secreta (S) utilizando un algoritmo de firma digital (SigAlg) y la clave privada (X) de un algoritmo de clave pública. Esto es,

$$S = SigAlg(X,f(D),L)$$

La firma digital se almacena junto con D y L en un solo registro de datos. La firma digital generada vincula L a D. En esta definición, f es una función pública tal que f(D) no revela información sobre D.

Con este método de vinculación no es necesario que L y S estén almacenados dentro de la misma demarcación de seguridad del sistema. Si se invoca un servicio criptográfico con un valor incorrecto de L, D o S, se detecta la inconsistencia. Esto se consigue utilizando la clave pública del algoritmo de clave pública como una clave de verificación para verificar la firma.

6.1.3.3 Método de vinculación 3

A partir de D y L se calcula un código de autenticación de mensaje (MAC, *message authentication code*) no secreto utilizando un modo generación-MAC de un algoritmo de cifrado (MacAlg) y una clave de algoritmo MAC (K-MAC) secreta. Esto es,

$$MAC = MacAlg(K\text{-}MAC,f(D),L)$$

El código MAC se almacena junto con D y L en un solo registro de datos. El MAC generado vincula L a D. En esta definición, f es una función pública tal que f(D) no revela información sobre D.

Con este método de vinculación no es necesario que L y MAC estén almacenados dentro de la demarcación de seguridad del sistema. Si se invoca un servicio criptográfico con un valor incorrecto de L, D o MAC, se detecta la inconsistencia. Esto se consigue calculando un MAC de referencia utilizando los valores proporcionados de L y D y una copia de K-MAK, y comparando el resultado con el MAC proporcionado.

6.2 Fichero de información de normativas de seguridad

6.2.1 Introducción

Una normativa de seguridad (o política de seguridad) en su forma más simple es un conjunto de criterios para la provisión de servicios de seguridad. Con respecto al control de acceso, la normativa de seguridad es un subconjunto de una normativa de seguridad de nivel-sistema más elevado que define los medios para imponer normativas de control de acceso entre iniciadores y receptores. El mecanismo de control de acceso:

- permitirá la comunicación cuando una normativa específica la permita, y
- denegará la comunicación cuando una normativa específica no la permita explícitamente.

Una normativa de seguridad es la base para las decisiones tomadas por el mecanismo de control de acceso. La información de normativa de seguridad específica del dominio se transporta mediante el fichero de información de normativas de seguridad.

El fichero de información de normativas de seguridad contiene una secuencia de lo siguiente:

- **versionInformation** – indica la versión de la sintaxis ASN.1 y semántica asociada de la especificación de fichero de información de normativas de seguridad.
- **updateInformation** – indica la vigencia de los datos del fichero de información de normativas de seguridad.
- **securityPolicyIdData** – identifica la normativa de seguridad a que se aplica el fichero de información de normativas de seguridad.
- **privilegeId** – indica el OID que identifica la sintaxis incluida en la categoría de seguridad de atributo de aprobación de seguridad de certificados basados en medidas de seguridad, utilizados conjuntamente con el fichero de información de normativas de seguridad. La sintaxis indicada por **privilegeId** tiene que estar en consonancia con la indicada por **rbacId**.
- **securityClassifications** – hace corresponder la clasificación de la etiqueta de seguridad a una clasificación el atributo aprobación de seguridad, y también proporciona correspondencias de equivalencia.
- **rbacId** – identificador de objeto de control de acceso basado en regla, que identifica la sintaxis incluida en la categoría de seguridad **securityLabel** que se utiliza conjuntamente con el fichero de información de normativas de seguridad. La sintaxis indicada por **rbacId** tiene que ser consistente con la indicada por **privilegeId**.
- **securityCategories** – hace corresponder las categorías de seguridad de la etiqueta de seguridad a las categorías de seguridad en el atributo aprobación de seguridad, y también proporciona correspondencias de equivalencia.
- **equivalentPolicies** – reúne todas las normativas equivalentes en el SPIF.
- **defaultSecurityPolicyIdData** – identifica la normativa de seguridad que se aplicará si se reciben datos sin una etiqueta de seguridad.
- **extensions** – proporciona un mecanismo para incluir capacidades adicionales a medida que se identifiquen futuras necesidades.

El fichero de información de normativas de seguridad es un objeto firmado para protegerlo contra cambios no autorizados.

6.2.2 Especificación ASN.1 del fichero de información de normativas de seguridad

El fichero de información de normativas de seguridad se define por la siguiente sintaxis:

```
SecurityPolicyInformationFile  ::=  SIGNED {EncodedSPIF}

EncodedSPIF  ::=  TYPE-IDENTIFIER.&Type( SPIF )

SPIF  ::=  SEQUENCE    {
        versionInformation                      VersionInformationData DEFAULT v1,
        updateInformation                       UpdateInformationData,
        securityPolicyIdData                    ObjectIdData,
        privilegeId                             OBJECT IDENTIFIER,
        rbacId                                  OBJECT IDENTIFIER,
        securityClassifications         [0]     SEQUENCE OF SecurityClassification OPTIONAL,
        securityCategories              [1]     SEQUENCE OF SecurityCategory OPTIONAL,
```

```
equivalentPolicies          [2]     SEQUENCE OF EquivalentPolicy OPTIONAL,
defaultSecurityPolicyIdData [3]     ObjectIdData OPTIONAL,
extensions                  [4]     Extensions OPTIONAL }
```

6.2.2.1 Información de versión

El campo **versionInformation** indica la versión de la sintaxis ASN.1 y la semántica asociada.

```
VersionInformationData ::= INTEGER { v1(0) } (0..MAX)
```

6.2.2.2 Información de actualización

updateInformationData es una secuencia de informaciones relativas a la versión específica de los datos SPIF. El **sPIFVersionNumber** distingue entre diferentes versiones de la información SPIF para la normativa de seguridad identificada en **securityPolicyIdData** en el SPIF. **creationDate** indica cuándo se generó el SPIF. El **originatorDistinguishedName** identifica el firmante del SPIF. El **keyIdentifier** identifica la clave utilizada para firmar el SPIF.

```
UpdateInformationData ::= SEQUENCE    {
    sPIFVersionNumber               INTEGER (0..MAX),
    creationDate                    GeneralizedTime,
    originatorDistinguishedName     Name,
    keyIdentifier                   OCTET STRING OPTIONAL }
```

6.2.2.3 Datos de ID de normativa de seguridad

Los **securityPolicyIdData** identifican la normativa de seguridad a que se aplica el SPIF. Los **securityPolicyIdData** se definen como **ObjectIdData**, donde **ObjectIdData** es una secuencia de **objectId** y **objectIdName**. Un **objectId** es el identificador de objeto (OID) asignado a un objeto específico, mientras que el **objectIdName** es una cadena que especifica un objeto concreto.

```
ObjectIdData ::= SEQUENCE {
    objectId            OBJECT IDENTIFIER,
    objectIdName        ObjectIdName }
ObjectIdName ::= DirectoryString {ubObjectIdNameLength}
```

6.2.2.4 Identificador de privilegio

El identificador de objeto **privilegeId** identifica la sintaxis que se incluye en la categoría seguridad atributo aprobación de seguridad de certificados basados en medidas de seguridad, utilizados conjuntamente con el SPIF.

6.2.2.5 Identificador RBAC

El identificador de objeto **rbacId** identifica la sintaxis que se incluye en las categorías de seguridad **securityLabel** utilizadas conjuntamente con el SPIF. La sintaxis indicada por **rbacId** tiene que estar en consonancia con la indicada por **privilegeId**.

6.2.2.6 Clasificaciones de seguridad

Una **SecurityClassification** SEQUENCE está presente en el SPIF para cada valor de clasificación de seguridad definido para la normativa de seguridad identificada en **securityPolicyIdData**. Éste es un elemento OPTIONAL.

El **labelAndCertValue** representa el valor asignado a esta clasificación en la etiqueta de seguridad y el valor entero que representa la ubicación binaria de esta clasificación de seguridad en el atributo aprobación de seguridad **classList BIT STRING**.

El **classificationName** es una cadena que identifica esta clasificación utilizada por la aplicación para determinar el texto que habrá de presentarse al usuario cuando se seleccione o visione el valor de clasificación en una etiqueta de seguridad.

Las **equivalentClassifications** son una secuencia de valores de clasificación (definidos en normativas de seguridad distintas de **securityPolicyIdData**) que son equivalentes al **SecurityClassification labelAndCertValue**.

El **hierarchyValue** indica la posición relativa del **SecurityClassification labelAndCertValue** en la jerarquía de clasificaciones de seguridad, en la normativa de seguridad indicada por los **securitypolicyIdData**. El **hierarchyValue** tiene que ser único dentro de la normativa de seguridad.

markingData identifica la información de marcación ligada al objeto de datos. **markingData** se compone de cadenas y códigos de marcación que identifican el lugar en que se presenta físicamente la cadena. Si la **markingPhrase** está ausente, el **markingCode** se aplica al **SecurityClassification classificationName**.

Cuando se selecciona una categoría de seguridad o una clasificación de seguridad para incluirla en la etiqueta de seguridad, el campo **requiredCategory** del SPIF asociado, si está presente, indica las categorías de seguridad que también hay que incluir en la etiqueta de seguridad, junto con el valor seleccionado. Si el campo **requiredCategory** no está presente, el valor seleccionado no depende de ninguna de las categorías de seguridad.

Si la operación **OptionalCategoryGroup** es **onlyOne**, la categoría de seguridad (y sólo una de las categorías de seguridad) incluida en **categoryGroup** tiene que incluirse en la etiqueta de seguridad. Si la operación **OptionalCategoryGroup** es **oneOrMore**, una o más de las categorías de seguridad incluidas en **categoryGroup** tienen que incluirse el etiqueta de seguridad. Si la operación **OptionalCategoryGroup** es **all**, todas las categorías de seguridad incluidas en **categoryGroup** tienen que incluirse en la etiqueta de seguridad. El usuario deberá seleccionar cada valor. Si están presentes múltiples **OptionalCategoryGroups** en **requiredCategories**, hay que cumplir el requisito expresado por todos los **OptionalCategoryGroups**. **categoryGroup** es una secuencia de **OptionalCategoryData**. El identificador de objeto **optCatDataId** especificará una sintaxis para uso en el campo **OptionalCategoryData categorydata** que esté en consonancia con las especificadas por **rbacId**, **privilegeId** y los identificadores de objeto de tipo **SecurityCategory** del SPIF.

El componente **obsolete**, cuando está fijado a TRUE, indica que una clasificación anteriormente válida es ahora obsoleta. Tal clasificación puede asociarse con objetos de datos antiguos, pero no con los nuevos.

```
SecurityClassification ::= SEQUENCE {
        labelAndCertValue                   LabelAndCertValue,
        classificationName                  ClassificationName,
        equivalentClassifications   [0]     EquivalentClassifications OPTIONAL,
        hierarchyValue                      INTEGER,
        markingData                 [1]     MarkingDataInfo OPTIONAL,
        requiredCategory            [2]     OptionalCategoryGroups OPTIONAL,
        obsolete                            BOOLEAN DEFAULT FALSE       }

LabelAndCertValue ::= INTEGER (0..MAX)
ClassificationName ::= DirectoryString { ubClassificationNameLength }
EquivalentClassifications ::= SEQUENCE SIZE(0..MAX) OF EquivalentClassification

EquivalentClassification ::= SEQUENCE {
        securityPolicyId            OBJECT IDENTIFIER,
        labelAndCertValue           LabelAndCertValue,
        applied Applied }

Applied ::= INTEGER {
        encrypt (0),
        decrypt (1),
        both    (2) }
 (encrypt | decrypt | both)

MarkingDataInfo ::= SEQUENCE SIZE(1..MAX) OF MarkingData

MarkingData ::= SEQUENCE {
        markingPhrase               MarkingPhrase OPTIONAL,
        markingCodes                MarkingCodes OPTIONAL }
  (ALL EXCEPT({-- none; at least one component shall be present --}))

MarkingPhrase ::= DirectoryString { ubMarkingPhraseLength }

MarkingCodes ::= SEQUENCE SIZE(1..MAX) OF MarkingCode

MarkingCode ::= INTEGER {
        pageTop                     (1),
        pageBottom                  (2),
        pageTopBottom               (3),
        documentEnd                 (4),
        noNameDisplay               (5),
        noMarkingDisplay            (6),
        unused                      (7),
        documentStart               (8),
        suppressClassName           (9) }

OptionalCategoryGroups ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryGroup

OptionalCategoryGroup ::= SEQUENCE {
        operation                   Operation,
        categoryGroup               CategoryGroup }
```

```
Operation ::= INTEGER {
        onlyOne                 (1),
        oneOrMore               (2),
        all                     (3)}
(onlyOne | oneOrMore | all)

CategoryGroup ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryData
OptionalCategoryData ::= SEQUENCE {
        optCatDataId            OC-DATA.&id({CatData}),
        categorydata            OC-DATA.&Type({CatData}{@optCatDataId }) }

OC-DATA ::= TYPE-IDENTIFIER
CatData OC-DATA ::= { ... }
```

6.2.2.7 Categorías de seguridad

Una **SecurityCategory SEQUENCE** está presente en el SPIF para cada categoría de seguridad definida para la normativa de seguridad identificada en **securityPolicyIdData**. La sintaxis de **SecurityCategory** se define en la etiqueta de confidencialidad presentada en 6.1. La sintaxis definida para uso en el campo valor de **SecurityCategory** que se indica por el identificador de objeto de tipo **SecurityCategory** tiene que estar en consonancia con la sintaxis indicada por los identificadores de objeto **privilegeId**, **rbacId** y **optCatDataID**.

6.2.2.8 Normativas equivalentes

equivalentPolicies es una lista de todas las normativas de seguridad para las que se han incluido valores en el SPIF como valores equivalentes. El **securityPolicyId** es un identificador de objeto que identifica la normativa de seguridad equivalente. El **securityPolicyName** es una cadena de directorio facultativa que identifica el nombre de la normativa de seguridad equivalente.

```
EquivalentPolicy ::= SEQUENCE {
        securityPolicyId        OBJECT IDENTIFIER,
        securityPolicyName      SecurityPolicyName  OPTIONAL}

SecurityPolicyName ::= DirectoryString {ubObjectIdNameLength}
```

6.2.2.9 Identificador de normativa de seguridad por defecto

El valor para **defaultSecurityPolicyIdData** soporta la interoperabilidad con aplicaciones que no soportan el control de acceso. Se hace referencia a este identificador de objeto cuando no se utiliza etiqueta de seguridad.

Obsérvese que la normativa de seguridad por defecto se hará corresponder a un solo nivel de clasificación. Cuando un valor de clasificación de seguridad se hace corresponder a una normativa de seguridad por defecto, la **SecurityClassification SEQUENCE** del SPIF para el valor designado incluirá una **equivalentClassification SEQUENCE** en la que el **policyId** se fija al identificador de objeto normativa de seguridad por defecto (default security policy).

6.2.2.10 Extensiones

El campo **extension** es una secuencia de información que prevé la futura expansión del SPIF a medida que se identifiquen necesidades adicionales, al mismo tiempo que se mantiene la interoperabilidad con anteriores implementaciones del SPIF. Contiene los componentes extnId, **critical**, y **extnValue**. La sintaxis ha sido importada de la Rec. UIT-T X.509 | ISO/CEI 9594-8.

Una extensión puede designarse como crítica o no crítica. Un sistema que utiliza SPIF RECHAZARÁ el SPIF si encuentra una extensión crítica que no reconoce; en cambio, puede no tener en cuenta una extensión no crítica. Se debe obrar con cautela cuando se tenga el propósito de adoptar extensiones críticas que pudieran impedir la utilización en un contexto general.

```
Extensions ::= SEQUENCE OF Extension

Extension ::= SEQUENCE {
        extnId                  EXTENSION.&id ({ExtensionSet}),
        critical                BOOLEAN DEFAULT FALSE,
        extnValue               OCTET STRING
          -- contains a DER encoding of a value of type &ExtnType
          -- for the extension object identified by extnId -- }

ExtensionSet EXTENSION ::= { ... }
```

```
EXTENSION ::= CLASS {
        &id                             OBJECT IDENTIFIER UNIQUE,
        &ExtnType }
WITH SYNTAX { SYNTAX &ExtnType IDENTIFIED BY &id }
```

6.3 Atributo aprobación de seguridad

6.3.1 Introducción

El atributo aprobación de seguridad se utiliza para definir las autorizaciones concedidas a una determinada entidad de usuario o de aplicación. Las autorizaciones concedidas a una entidad de usuario o de aplicación pueden ser un subconjunto de la totalidad de la normativa (o de las normativas) de seguridad de la organización. Como una alternativa, las autorizaciones pueden abarcar la totalidad de la normativa de seguridad.

El atributo aprobación de seguridad tiene tres componentes: **policyId**, **classList**, y, facultativamente, **securityCategory**, como se muestra en la siguiente figura 1.

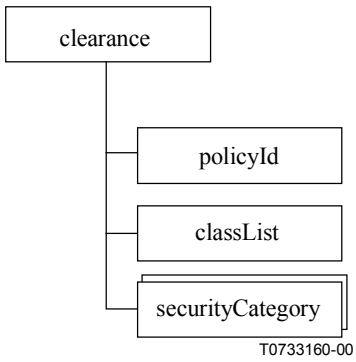

Figura 1 – Estructura del atributo aprobación de seguridad (clearance)

El identificador de objeto **policyId** identifica el componente o componentes facultativos que estarán presentes. El componente **classList** define las aprobaciones de seguridad concedidas al usuario y las aprobaciones de seguridad jerárquicas indicadas por **ClassList**, que se define en la Rec. UIT-T X.501 | ISO/CEI 9594-2. Se podrían definir, en otra parte, otras listas no jerárquicas para incluirlas en otros objetos de información de seguridad o para direccionarlas en categorías de seguridad. El componente **securityCategory** identifica cualquier número de categorías de seguridad con mapas de bits restrictivos o permisivos, así como categorías de seguridad enumeradas restrictivas o permisivas, asignadas al usuario. Esta estructura se ilustra en la figura 2.

6.3.2 Definición del atributo aprobación de seguridad

El atributo aprobación de seguridad se define así:

```
clearance  ATTRIBUTE  ::= { WITH SYNTAX    Clearance
        ID                              id-at-clearance }

id-at-clearance OBJECT IDENTIFIER  ::= {
  joint-iso-itu-t (2) ds (5) attributeType (4) clearance (55) }

Clearance  ::= SEQUENCE {
        policyId                        OBJECT IDENTIFIER,
        classList                       ClassList DEFAULT {unclassified},
        securityCategories              SecurityCategories  OPTIONAL}

ClassList  ::= BIT STRING {
        unmarked                        (0),
        unclassified                    (1),
        restricted                      (2),
        confidential                    (3),
        secret                          (4),
        topSecret                       (5)    }

SecurityCategories  ::= SET SIZE(1..MAX) OF SecurityCategory
   -- SecurityCategory is defined in the confidentiality label given in subclause 6.1.2
```

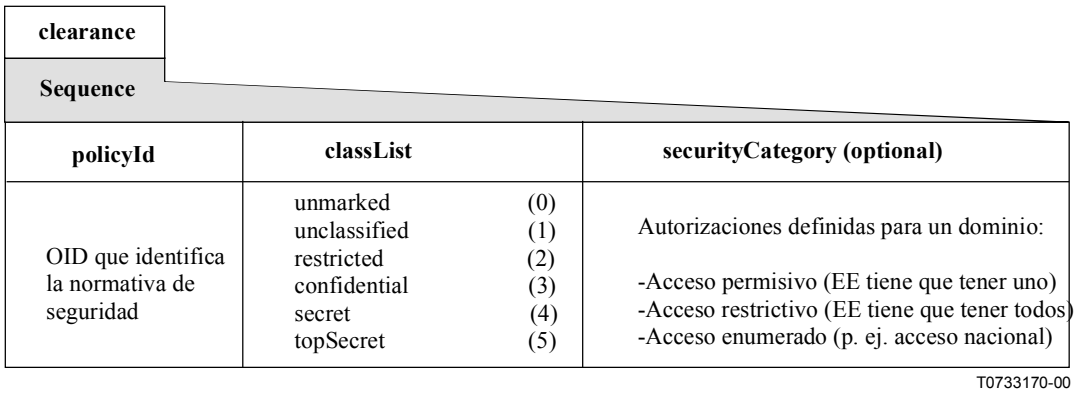

Figura 2 – Campos del atributo aprobación de seguridad (clearance)

7 Interacción de objetos de información de seguridad

7.1 Comparación de las estructuras de las clases de objetos de información de seguridad

La figura 3 permite comparar las estructuras de la etiqueta de confidencialidad, el atributo aprobación de seguridad de la Rec. UIT-T X.501 | ISO/CEI 9594-2, y el SPIF. Los componentes equivalentes en estas estructuras pueden ser examinados en programas de aplicación para obtener una funcionalidad específica. En 7.2 se examina la obtención de la funcionalidad de control de acceso mediante el empleo de estas tres estructuras.

7.2 Interacción de objetos de información de seguridad para el control de acceso

El control de acceso incluye el concepto de comunicar autorizaciones a iniciadores o usuarios mediante el empleo de un atributo aprobación de seguridad y la asignación de parámetros de sensibilidad a objetos deseados por medio de una etiqueta de seguridad. Se utiliza el SPIF para interpretar estas autorizaciones y parámetros de sensibilidad. Los programas de aplicación utilizan el SPIF para aplicar sensibilidades a objetos deseados, extraer sensibilidades leyéndolas en las etiquetas, leer y afirmar autorizaciones en certificados, y determinar correspondencias válidas de normativas en los distintos dominios de normativas de seguridad.

Los mecanismos utilizados para transportar autorizaciones y sensibilidades son las clasificaciones y las categorías. Las clasificaciones y categorías son afirmadas en un atributo aprobación de seguridad insertado en un certificado de usuario, con lo que se transporta la autorización de ese usuario. Las clasificaciones y categorías son también afirmadas en una etiqueta de seguridad del objeto, con lo que se transportan las sensibilidades de ese objeto. Se permite el acceso a un objeto cuando las autorizaciones transportadas en el atributo aprobación de seguridad de un usuario son suficientes en comparación con las sensibilidades transportadas en la etiqueta de seguridad del objeto deseado. La figura 4 ilustra las interacciones entre los SIO aquí definidos, para obtener el control de acceso en un entorno de almacenamiento de datos. Las autorizaciones en el atributo aprobación de seguridad del propietario de los datos, contenidas en el certificado asociado con el propietario de los datos, establecen límites en cuanto a las autorizaciones (procedentes del SPIF); el propietario de los datos deberá cumplir estos límites en lo que respecta a la autorizaciones que puede afirmar en la etiqueta para los datos deseados. La etiqueta se vincula a los datos, y se almacena. Para ganar acceso a datos que se encuentran en el dispositivo de almacenamiento, el atributo aprobación de seguridad del usuario, contenido en el certificado asociado con el propietario de los datos, se compara con la etiqueta vinculada a los datos deseados en la función decisión de control de acceso. Si en la etiqueta de seguridad existen sensibilidades permisivas, se comprueban dichas sensibilidades para cerciorarse de que al menos una de las sensibilidades presentes en cada rótulo permisivo de la etiqueta de seguridad está también autorizada en el certificado (autorización o autorizaciones permisivas) que permite el acceso al objeto de datos deseado a través de la función ejecución de control de acceso. En la figura 5 se muestra un escenario similar de control de acceso para un entorno de mensajería.

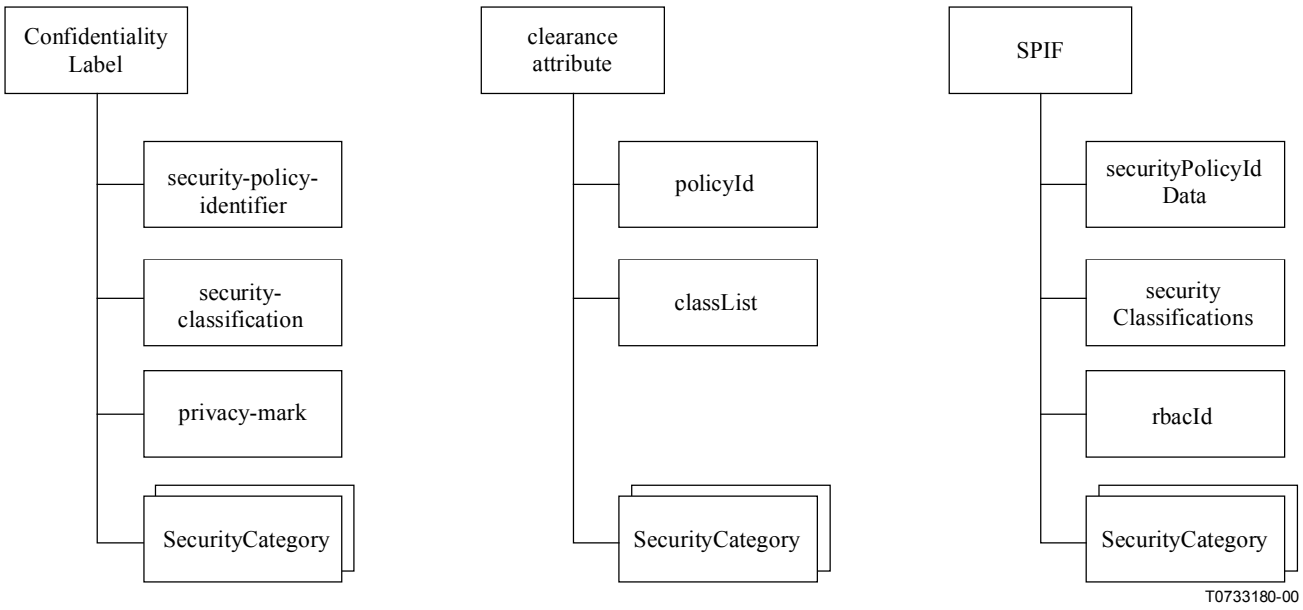

Figura 3 – Comparación de clases de objeto equivalentes

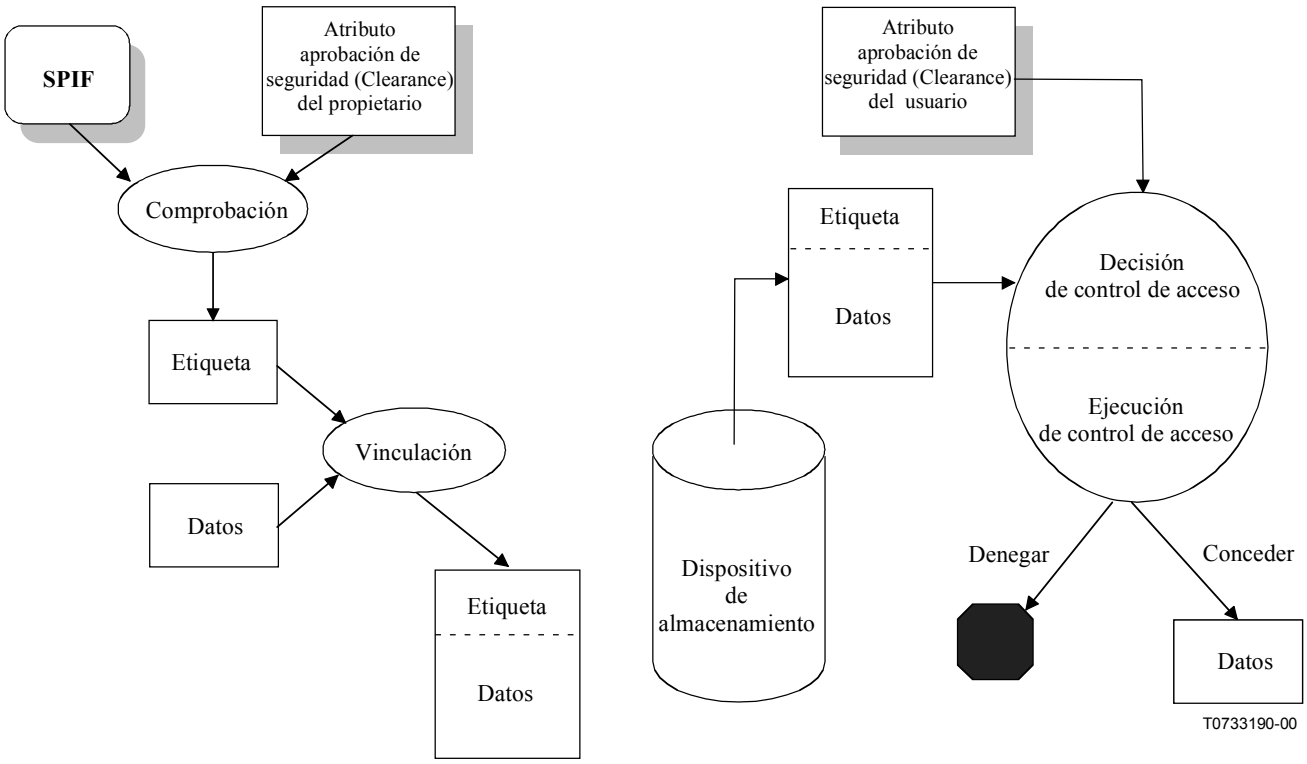

Figura 4 – Control de acceso al dispositivo de almacenamiento

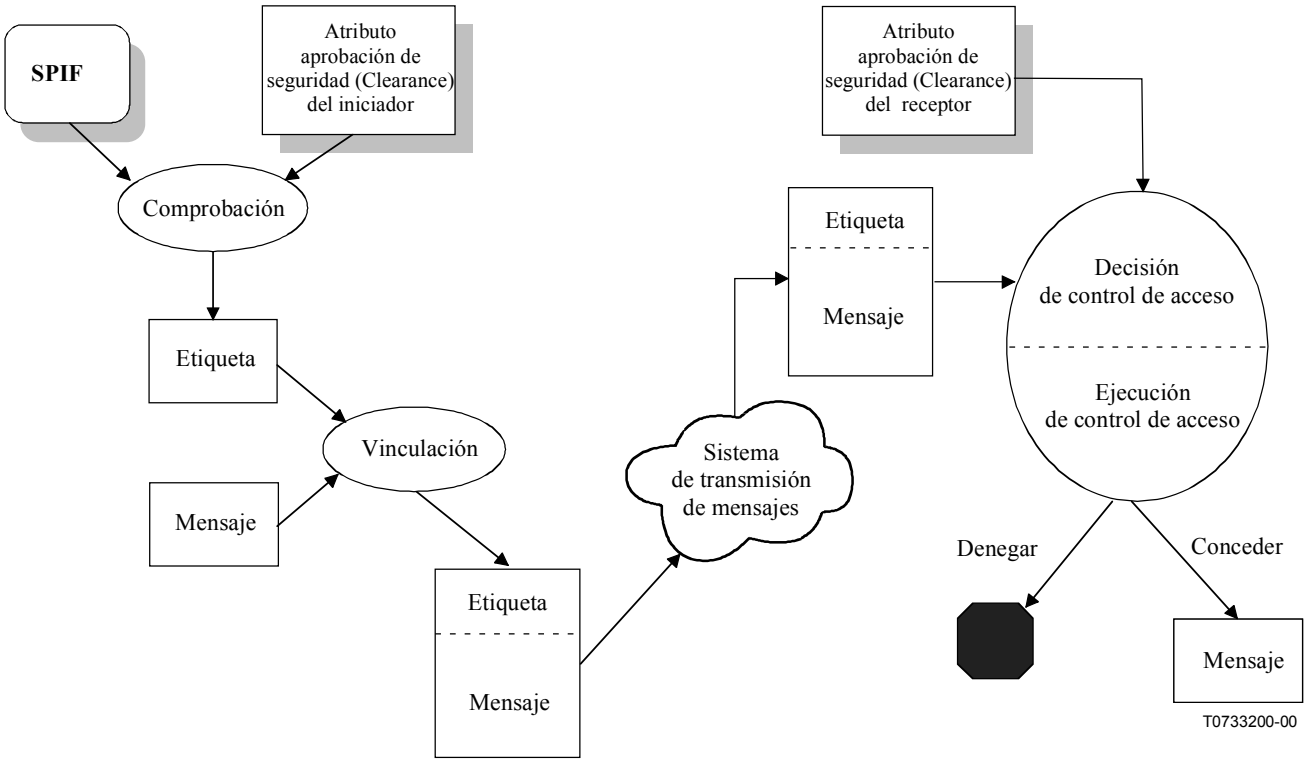

Figura 5 – Control de acceso en un escenario de mensajería

Anexo A

Objetos de información de seguridad para control de acceso en ASN.1

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

Este anexo incluye todas las definiciones de tipos, valores y clases de objetos de información contenidos en esta Recomendación | Norma Internacional en forma de módulo ASN.1.

```
SIOsAccessControl-MODULE  {
   joint-iso-itu-t sios(24) specification(0) modules(0) accessControl(0)
}
       DEFINITIONS IMPLICIT TAGS ::= BEGIN

-- EXPORTS All; --

IMPORTS

   id-at-clearance
      FROM EnhancedSecurity        -- ITU-T Rec. X.501 | ISO/IEC 9594-2 --

   ATTRIBUTE, Name
      FROM InformationFramework    -- ITU-T Rec. X.501 | ISO/IEC 9594-2 --

   Extensions
      FROM CertificateExtensions   -- ITU-T Rec. X.509 | ISO/IEC 9594-8 --

   DirectoryString {}
      FROM SelectedAttributeTypes; -- ITU-T Rec. X.520 | ISO/IEC 9594-6 --

id-ConfidentialityLabel OBJECT IDENTIFIER  ::=  {joint-iso-itu-t sios(24) specification(0)
securityLabels(1) confidentiality(0)}

ConfidentialityLabel  ::=  SET {
   security-policy-identifier  SecurityPolicyIdentifier  OPTIONAL,
   security-classification     INTEGER(0..MAX)  OPTIONAL,
   privacy-mark                PrivacyMark  OPTIONAL,
   security-categories         SecurityCategories  OPTIONAL
}
 (ALL EXCEPT({-- none; at least one component shall be present --}))

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER
```

```
PrivacyMark ::= CHOICE {
   pString     PrintableString (SIZE(1..ub-privacy-mark-length)),
   utf8String  UTF8String (SIZE(1..ub-privacy-mark-length))
}

ub-privacy-mark-length INTEGER ::= 128  -- as defined in X.411

SecurityCategories ::= SET SIZE(1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
   type   [0] SECURITY-CATEGORY.&id({SecurityCategoriesTable}),
   value  [1] EXPLICIT SECURITY-CATEGORY.&Type(
                              {SecurityCategoriesTable}{@type})
}

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= {
   ...  -- objects defined as needed --
}

SecurityPolicyInformationFile ::= SIGNED { EncodedSPIF }

-- Type EncodedSPIF is an open type constrained to be a value
-- of type SPIF. This open type representation is an opaque
-- string of hexadecimal characters suitable for signature
-- and signature verification operations.

EncodedSPIF ::= TYPE-IDENTIFIER.&Type( SPIF )

SPIF ::= SEQUENCE {
   versionInformation           VersionInformationData  DEFAULT v1,
   updateInformation            UpdateInformationData,
   securityPolicyIdData         ObjectIdData,
   privilegeId                  OBJECT IDENTIFIER,
   rbacId                       OBJECT IDENTIFIER,
   securityClassifications      [0] SecurityClassifications  OPTIONAL,
   securityCategories           [1] SPIF-SecurityCategories  OPTIONAL,
   equivalentPolicies           [2] EquivalentPolicies  OPTIONAL,
   defaultSecurityPolicyIdData  [3] ObjectIdData  OPTIONAL,
   extensions                   [4] Extensions  OPTIONAL
}
```

```
VersionInformationData ::= INTEGER { v1(0) } (0..MAX)

UpdateInformationData ::= SEQUENCE {
   sPIFVersionNumber           SPIFVersionNumber,
   creationDate                GeneralizedTime,
   originatorDistinguishedName  Name,
   keyIdentifier               OCTET STRING  OPTIONAL
}

SPIFVersionNumber ::=  INTEGER (0..MAX)

ObjectIdData ::= SEQUENCE {
   objectId      OBJECT IDENTIFIER,
   objectIdName  ObjectIdName
}

ObjectIdName ::= DirectoryString { ubObjectIdNameLength }

SecurityClassifications ::=
      SEQUENCE SIZE(0..MAX) OF SecurityClassification

SPIF-SecurityCategories ::=
      SEQUENCE SIZE(0..MAX) OF SecurityCategory

EquivalentPolicies ::=
      SEQUENCE SIZE(0..MAX) OF EquivalentPolicy

SecurityClassification ::= SEQUENCE {
   labelAndCertValue          LabelAndCertValue,
   classificationName         ClassificationName,
   equivalentClassifications  [0] EquivalentClassifications  OPTIONAL,
   hierarchyValue             INTEGER,
   markingData                [1] MarkingDataInfo  OPTIONAL,
   requiredCategory           [2] OptionalCategoryGroups  OPTIONAL,
   obsolete                   BOOLEAN  DEFAULT FALSE
}

LabelAndCertValue ::= INTEGER(0..MAX)

ClassificationName ::= DirectoryString { ubClassificationNameLength }

EquivalentClassifications ::=
     SEQUENCE SIZE(0..MAX) OF EquivalentClassification
```

```
EquivalentClassification ::= SEQUENCE {
   securityPolicyId   OBJECT IDENTIFIER,
   labelAndCertValue  LabelAndCertValue,
   applied            Applied
}

Applied ::= INTEGER {
   encrypt (0),
   decrypt (1),
   both    (2)
}
 (encrypt | decrypt | both)

MarkingDataInfo ::= SEQUENCE SIZE(1..MAX) OF MarkingData

MarkingData ::= SEQUENCE {
   markingPhrase  MarkingPhrase  OPTIONAL,
   markingCodes   MarkingCodes  OPTIONAL
}
 (ALL EXCEPT({-- none; at least one component shall be present --}))

MarkingPhrase ::= DirectoryString { ubMarkingPhraseLength }

MarkingCodes ::= SEQUENCE SIZE(1..MAX) OF MarkingCode

MarkingCode ::= INTEGER {
   pageTop           (1),
   pageBottom        (2),
   pageTopBottom     (3),
   documentEnd       (4),
   noNameDisplay     (5),
   noMarkingDisplay  (6),
   unused            (7),
   documentStart     (8),
   suppressClassName (9)
}

OptionalCategoryGroups ::=
      SEQUENCE SIZE(1..MAX) OF OptionalCategoryGroup
```

```
OptionalCategoryGroup ::= SEQUENCE {
   operation      Operation,
   categoryGroup  CategoryGroup
}

Operation ::= INTEGER {
   onlyOne   (1),
   oneOrMore (2),
   all       (3)
}
 (onlyOne | oneOrMore | all)

CategoryGroup ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryData

OptionalCategoryData ::= SEQUENCE {
   optCatDataId  OC-DATA.&id({CatData}),
   categorydata  OC-DATA.&Type({CatData}{@optCatDataId })
}

OC-DATA ::= TYPE-IDENTIFIER

CatData OC-DATA ::= {
   ...  -- defined as needed --
}

EquivalentPolicy ::= SEQUENCE {
   securityPolicyId    OBJECT IDENTIFIER,
   securityPolicyName  SecurityPolicyName  OPTIONAL
}

SecurityPolicyName ::= DirectoryString { ubObjectIdNameLength }

clearance ATTRIBUTE ::= {
   WITH SYNTAX  Clearance
   ID           id-at-clearance
}

Clearance ::= SEQUENCE {   -- Automatic tags applied
   policyId            [0] OBJECT IDENTIFIER,
   classList           [1] ClassList  DEFAULT { unclassified },
   securityCategories  [2] SecurityCategories  OPTIONAL
}
```

```
ClassList ::= BIT STRING {
   unmarked     (0),
   unclassified (1),
   restricted   (2),
   confidential (3),
   secret       (4),
   topSecret    (5)
}

-- upper bound values

ubObjectIdNameLength        INTEGER ::= 256
ubClassificationNameLength  INTEGER ::= 256
ubMarkingPhraseLength       INTEGER ::= 256

-- information object classes --

ALGORITHM ::= CLASS {
   &id    OBJECT IDENTIFIER  UNIQUE,
   &Type  OPTIONAL
}
  WITH SYNTAX { OID &id [PARMS &Type] }

-- parameterized types --

SIGNED { ToBeSigned } ::= SEQUENCE {
   toBeSigned  ToBeSigned,
   algorithm   AlgorithmIdentifier{{SignatureAlgorithms}},
   signature   BIT STRING
}

AlgorithmIdentifier { ALGORITHM:IOSet } ::= SEQUENCE {
   algorithm   ALGORITHM.&id({IOSet}),
   parameters  ALGORITHM.&Type({IOSet}{@algorithm}) OPTIONAL
}

SignatureAlgorithms ALGORITHM ::= {
  ... -- defined as needed --
}

END  -- SecurityInformationObjects --
```

Anexo B

Ampliación de la sintaxis de la SECURITY-CATEGORY

(Este anexo no es parte integrante de la presente Recomendación | Norma Internacional)

La clase de objeto de información SECURITY-CATEGORY se define como la clase **TYPE-IDENTIFIER** incorporada.

```
SECURITY-CATEGORY  ::=  TYPE-IDENTIFIER
```

Esta útil clase de objeto de información se especifica en el anexo A a la Rec. UIT-T X.681 | ISO/CEI 8824-2 como:

```
TYPE-IDENTIFIER ::= CLASS {
     &id    OBJECT IDENTIFIER UNIQUE,
     &Type
}
     WITH SYNTAX { &Type IDENTIFIED BY &id }
```

La clase **SECURITY-CATEGORY** tiene dos campos denominados **&id** y **&Type**. El campo **&id** se define como un valor del tipo **OBJECT IDENTIFIER**, y el campo **&Type** es un tipo abierto. Un tipo abierto puede ser cualquier tipo ASN.1.

Cuando objetos de esta clase se utilizan como miembros de un conjunto de objetos de información, la definición del campo **&id** requiere que cada objeto del conjunto contenga un valor de identificador de objeto único. La definición de clase incluye además una declaración **WITH SYNTAX** que especifique una notación que puede ser utilizada para definir objetos de información de la clase **SECURITY-CATEGORY**.

SecurityCategoriesTable es un conjunto de objetos de información de la clase **SECURITY-CATEGORY**. Se define como:

```
SecurityCategoriesTable SECURITY-CATEGORY ::= {
     ...  -- objects defined as needed --
}
```

El conjunto **SecurityCategoriesTable** contiene un marcador de ampliación, "...", pero no objetos de información. Objetos de la clase **SECURITY-CATEGORY** se pueden especificar individualmente utilizando la notación **WITH SYNTAX** proporcionada en la definición de la clase. Los ejemplos de objeto que siguen muestran que cualquier tipo ASN.1, simple o complejo, puede ser utilizado para crear un objeto de información.

```
-- Type 1 - restrictive attributes

restrictiveBitMap SECURITY-CATEGORY ::= {
     AttributeFlags IDENTIFIED BY id-restrictiveBitMap
}

AttributeFlags ::= BIT STRING

-- Type 2 - hierarchical attributes

enumeratedAttributes SECURITY-CATEGORY ::= {
     AttributeList IDENTIFIED BY id-enumeratedAttributes
}

AttributeList ::= SET SIZE(1..MAX) OF LabelAttribute

-- Type 5 - all attributes in the range(s)

rangeSet SECURITY-CATEGORY ::= {
     RangeList IDENTIFIED BY id-rangeSet
}

RangeList ::= SET SIZE(1..MAX) OF LabelAttributeRange

-- Type 6 - release attributes

permissiveBitMap SECURITY-CATEGORY ::= {
     PermissiveBitMap IDENTIFIED BY id-permissiveBitMap

}

PermissiveBitMap ::= BIT STRING
```

```
-- Type 7 – for markings with no formal access control --

freeFormField SECURITY-CATEGORY ::= {
     FreeFormField IDENTIFIED BY id-freeFormField
}

FreeFormField ::= SEQUENCE {
   name   SECURITY-CATEGORY.&id({Fields}),
   field  SECURITY-CATEGORY.&Type({Fields}{@name})
}

Fields SECURITY-CATEGORY ::= {
   ...  -- defined as needed --
}
```

Aquí, los campos **&Type** de los objetos contienen tipos ASN.1 denominados **AttributeFlags**, **AttributeList**, **RangeList**, **PermissiveBitMap** y **FreeFormField**. Los campos **&id** contienen valores de identificadores de objeto únicos denominados **id-restrictiveBitMap**, **id-enumeratedAttributes**, **id-rangeSet**, **id-permissiveBitMap** e **id-freeFormField**.

Estos objetos se pueden añadir a una versión de la implementación del **SecurityCategoriesTable** por nombre de objeto para formar un conjunto de categorías de seguridad a partir de la unión de los objetos:

```
SecurityCategoriesTable SECURITY-CATEGORY ::= {
       restrictiveBitMap |
       enumeratedAttributes  |
       rangeSet      |
       permissiveBitMap
       freeFormField,
       ...  -- expect other objects --
}
```

De manera alternativa, las definiciones de objetos se pueden añadir directamente al conjunto de objetos de información **SecurityCategoriesTable**:

```
SecurityCategoriesTable SECURITY-CATEGORY ::= {
       --
       --    &Type                                &id
       --
       { AttributeFlags   IDENTIFIED BY id-restrictiveBitMap    } |
       { AttributeList    IDENTIFIED BY id-enumeratedAttributes } |
       { RangeList        IDENTIFIED BY id-rangeSet             } |
       { PermissiveBitMap IDENTIFIED BY id-permissiveBitMap     } |
       { FreeFormField    IDENTIFIED BY id-freeFormField       },
       ...  -- expect other objects --
  }
```

Esta visión del conjunto de categorías de seguridad presenta un cuadro de cuatro filas, cada una de las cuales tiene dos columnas, una columna para **&id** y otra para **&Type**.

El tipo **SecurityCategory** se define como una secuencia de dos componentes denominados tipo y valor.

```
SecurityCategory ::= SEQUENCE {
       type   [0] SECURITY-CATEGORY.&id({SecurityCategoriesTable}),
       value  [1] EXPLICIT SECURITY-CATEGORY.&Type(
                           {SecurityCategoriesTable}{@type})
}
```

Cada uno de sus componentes se especifica en términos de los campos **&id** y **&Type** de la clase **SECURITY-CATEGORY**. El componente tipo se especifica en términos del campo **&id** y debe ser un valor del tipo **OBJECT IDENTIFIER**. El componente valor se especifica mediante el campo **&Type** y puede ser un valor de cualquier tipo ASN.1.

El conjunto de objetos de información **SecurityCategoriesTable** se utiliza para formar una constricción de tabla de los valores válidos de los componentes tipo y valor de **SecurityCategory**. La constricción de tabla tiene dos columnas, una para cada campo de la clase **SECURITY-CATEGORY**.

El valor de identificador de objeto único especificado por el campo **&id** del componente tipo selecciona una fila de la tabla. La notación **@type** selecciona la columna de **&Type** asociada con el valor de **&id** de la fila seleccionada. El marcador de ampliación del conjunto **SecurityCategoriesTable** indica que una aplicación deberá prever objetos distintos de los especificados explícitamente en el conjunto.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Transmisiones de señales radiofónicas, de televisión y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos y comunicación entre sistemas abiertos**
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2001