UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.812

(11/95)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

SEGURIDAD

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MARCOS DE SEGURIDAD PARA SISTEMAS ABIERTOS: MARCO DE CONTROL DE ACCESO

Recomendación UIT-T X.812

(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.812 se aprobó el 21 de noviembre de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10181-3.

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

Resumen

La presente Recomendación | Norma Internacional define un marco general para la provisión de control de acceso. El objetivo primario del control de acceso es contrarrestar la amenaza de operaciones no autorizadas con un computador o sistemas de comunicaciones; estas amenazas se subdividen frecuentemente en clases conocidas como uso no autorizado, divulgación, modificación, destrucción y denegación de servicio.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MARCOS DE SEGURIDAD PARA SISTEMAS ABIERTOS: MARCO DE CONTROL DE ACCESO

1 Alcance

Los marcos de seguridad están orientados a la aplicación de servicios de seguridad a entornos de sistemas abiertos, donde el término *sistemas abiertos* incluye áreas tales como bases de datos, aplicaciones distribuidas, ODP y OSI. Los marcos de seguridad pretenden definir los medios mediante los cuales se protegen sistemas y objetos dentro de los sistemas, así como la interacción entre sistemas. Los marcos de seguridad no se ocupan de la metodología para la construcción de sistemas o de mecanismos.

Los marcos de seguridad se ocupan de elementos de datos o de secuencias de operaciones (pero no de elementos de protocolo) que se utilizan para disponer de servicios específicos de seguridad. Dichos servicios de seguridad se pueden aplicar a la comunicación entre entidades de sistemas así como al intercambio de datos entre sistemas y a la gestión de datos por parte de los sistemas.

En el caso del control de acceso, los accesos pueden ser *a* un sistema (es decir, a una entidad que es la parte que se comunica de un sistema) o *dentro* del sistema. Los elementos de información que es necesario presentar para obtener el acceso, así como la secuencia de las operaciones necesarias para solicitar el acceso y para la notificación de los resultados del acceso, se consideran que están en el ámbito de los marcos de seguridad. Sin embargo, cualquier elemento de información u operaciones que dependen de una única aplicación y que sólo están relacionadas con el acceso local dentro de un sistema se consideran fuera del ámbito de los marcos de seguridad.

Muchas aplicaciones tienen requisitos de seguridad para la protección contra las amenazas a los recursos, incluida la información, que se derivan de la interconexión de sistemas abiertos. La Rec. X.800 del CCITT | ISO 7498-2 describe algunas amenazas habituales, así como los mecanismos de seguridad y los servicios que pueden utilizarse para protegerse contra ellos en un entorno OSI.

El proceso para determinar cuál es la utilización permitida de los recursos de un entorno de sistemas abiertos, así como para la prevención de accesos no autorizados, se denomina control de acceso. Esta Recomendación | Norma Internacional define un marco general para la provisión de los servicios de control de acceso.

Este marco de seguridad:

a) define los conceptos básicos para el control de acceso;

b) demuestra cómo se pueden especializar los conceptos básicos de control de acceso para permitir algunos servicios y mecanismos de control de acceso habituales;

c) define dichos servicios y los correspondientes mecanismos de control de acceso;

d) identifica los requisitos funcionales para los protocolos que soportan dichos servicios y mecanismos de control de acceso;

e) identifica los requisitos de gestión habituales para soportar dichos servicios y mecanismos de control de acceso;

f) se ocupa de la interacción de los servicios y mecanismos de control de acceso con otros servicios y mecanismos de seguridad.

Al igual que ocurre con otros servicios de seguridad, el control de acceso sólo puede proporcionarse en el contexto de una política de seguridad definida para una aplicación en particular. Aunque la definición de las políticas de control de acceso queda fuera del alcance de esta Recomendación | Norma Internacional, se describen algunas políticas de control de acceso.

Esta Recomendación | Norma Internacional no pretende especificar en detalle los protocolos de intercambio que pueden necesitarse a fin de proporcionar servicios de control de acceso.

Esta Recomendación | Norma Internacional no especifica mecanismos particulares para soportar dichos servicios de control de acceso ni información sobre los protocolos y servicios de gestión de seguridad.

En este contexto pueden utilizarse varios tipos de normas, incluyendo:

a) normas que incluyen el concepto de control de acceso;

b) normas que especifican servicios abstractos que incluyen el control de acceso;

c) normas que especifican la utilización de un servicio de control de acceso;

d) normas que proporcionan el significado de proporcionar el control de acceso en un entorno de sistemas abiertos; y

e) normas que especifican mecanismos de control de acceso.

Dichas normas pueden utilizar este contexto como sigue:

– los tipos de normas a, b, c, d y e pueden utilizar la terminología de este marco;

– los tipos de normas b, c, d y e pueden utilizar las facilidades definidas en la cláusula 7 de este marco; y

– las normas de tipo e pueden basarse en las clases de mecanismos definidos en la cláusula 8.

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 son objeto de revisiones, por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional 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 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.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.811 (1995) **|** ISO/CEI 10181-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de autenticación*.

– Recomendación UIT-T X.880 (1994) **|** ISO/CEI 13712-1:1995, *Tecnología de la información – Operaciones a distancia: Conceptos, modelo y notación*.

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

– Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad de 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 esta Recomendación **|** Norma Internacional, se aplican las siguientes definiciones.

3.1 Esta 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) imputabilidad;

d) autenticación;

e) información de autenticación;

f) autorización;

g) capacidad;

h) política de seguridad basada en la identidad;

i) política de seguridad basada en reglas;

j) auditoría de seguridad;

k) etiqueta de seguridad;

l) política de seguridad;

m) servicio de seguridad;

n) sensibilidad.

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

a) política de interacción segura;

b) certificado de seguridad;

c) dominio de seguridad;

d) autoridad de dominio de seguridad;

e) información de seguridad;

f) reglas de política de seguridad;

g) testigo de seguridad;

h) confianza.

3.3 Esta Recomendación | Norma Internacional hace uso de los siguientes términos definidos en la Rec. UIT-T X.200 | ISO/CEI 7498-1:

– sistema real.

3.4 A los efectos de esta Recomendación, son aplicables las siguientes definiciones:

3.4.1 certificado de control de acceso: Certificado de seguridad que contiene ACI.

3.4.2 información de decisión de control de acceso (ADI, *access control decision information***)**: La parte de la ACI (probablemente toda) que está disponible para que la ADF tome una determinada decisión de control de acceso.

3.4.3 función de decisión de control de acceso (ADF, *access control decision function***)**: Función especializada que toma las decisiones de control de acceso aplicando reglas de política de control de acceso ante una petición de acceso ADI (de iniciadores, objetivos, peticiones de acceso o que se deriva de una decisión anterior), así como el contexto en que se realiza la petición de acceso.

3.4.4 función de imposición de control de acceso (AEF, *access control enforcement function***)**: Función especializada que forma parte del trayecto de acceso entre un iniciador y un objetivo en cada petición de acceso y que impone la decisión tomada por la ADF.

3.4.5 información de control de acceso (ACI, *access control information***)**: Cualquier información utilizada con fines de control de acceso, incluyendo la información contextual.

3.4.6 política de control de acceso: Conjunto de reglas que definen las condiciones bajo las cuales puede tener lugar un acceso.

3.4.7 reglas de política de control de acceso: Reglas de política de seguridad relativas a la provisión de servicios de control de acceso.

3.4.8 testigo de control de acceso: Testigo de seguridad que contiene la ACI.

3.4.9 petición de acceso: Operación y operandos que forman parte de un intento de acceso.

3.4.10 información de decisión de control de acceso de petición de acceso; ADI de petición de acceso: ADI que se deriva de una ACI vinculada con una petición de acceso.

3.4.11 información de control de acceso de petición de acceso; ACI de petición de acceso: ACI relativa a una petición de acceso.

3.4.12 información de control de acceso vinculada con una petición de acceso; ACI vinculada con una petición de acceso: ACI vinculada con una petición de acceso.

3.4.13 acreditación: ACI vinculada al iniciador que puede compararse con las etiquetas de seguridad de los objetivos.

3.4.14 información contextual: Información relativa a o derivada del contexto en el que se realiza una petición de acceso (por ejemplo, la hora del día).

3.4.15 iniciador: Una entidad (por ejemplo, usuario humano o entidad basada en un ordenador) que intenta acceder a otras entidades.

3.4.16 información de decisión de control de acceso del iniciador; ADI del iniciador: ADI derivada de una ACI vinculada con el iniciador.

3.4.17 información de control de acceso del iniciador; ACI del iniciador: ACI relativa a un iniciador.

3.4.18 información de control de acceso vinculada con el iniciador; ACI vinculada con el iniciador: ACI vinculada con un iniciador.

3.4.19 información de decisión de control de acceso de operando; ADI de operando: ADI derivada de una ACI vinculada con el operando.

3.4.20 información de control de acceso de operando; ACI de operando: ACI relativa a los operandos de una petición de acceso.

3.4.21 información de control de acceso vinculada con el operando; ACI vinculada con el operando: ACI vinculada con los operandos de una petición de acceso.

3.4.22 ADI retenida: ADI que ha sido retenida por una ADF procedente de decisiones de control de acceso anteriores, para ser utilizada en futuras decisiones de control de acceso.

3.4.23 objetivo: Una entidad a la que se puede intentar acceder.

3.4.24 información de decisión de control de acceso del objetivo: ADI derivada de una ACI vinculada con el objetivo.

3.4.25 información de control de acceso del objetivo; ACI del objetivo: ACI relativa a un objetivo.

3.4.26 información de control de acceso vinculada con el objetivo; ACI vinculada con el objetivo: ACI vinculada con un objetivo.

4 Abreviaturas

ACI	Información de control de acceso (*access control information*)
ADI	Información de decisión de control de acceso (*access control decision information*)
ADF	Función de decisión de control de acceso (*access control decision function*)
AEF	Función de imposición de control de acceso (*access control enforcement function*)
SI	Información de seguridad (*security information*)
SDA	Autoridad del dominio de seguridad (*security domain authority*)

5 Discusión general sobre el control de acceso

5.1 Objetivo del control de acceso

A los efectos de este marco de seguridad, el objetivo primario del control de acceso es contrarrestar la amenaza de las operaciones no autorizadas en las que están involucradas un computador o un sistema de comunicaciones; frecuentemente dichas amenazas se subdividen en clases que se conocen como:

- de utilización no autorizada;
- revelación;
- modificación;
- destrucción; y
- denegación del servicio.

Los objetivos secundarios de este marco de seguridad son:

- el control de acceso mediante procesos (que pueden actuar en nombre de seres humanos o de otros procesos) a datos, a procesos diferentes o a otros recursos de computación;
- el control de acceso en un dominio de seguridad o a través de uno o más dominios de seguridad;
- el control de acceso de acuerdo con su contexto; por ejemplo, dependiendo de factores tales como hora en que se realiza el intento de acceso, ubicación de quien intenta el acceso o ruta de acceso;
- el control de acceso reactivo a cambios en la autorización durante el acceso.

5.2 Aspectos básicos del control de acceso

Las subcláusulas siguientes describen funciones de control de acceso abstractas que son en gran medida independientes de las políticas de control de acceso y del diseño de los sistemas. El control de acceso en sistemas reales está relacionado con numerosos tipos de entidades, tales como:

- entidades físicas (por ejemplo, sistemas reales);
- entidades lógicas (por ejemplo, entidades de capa OSI, ficheros, organizaciones y compañías);
- usuarios humanos.

El control de acceso en sistemas reales puede requerir un complejo conjunto de actividades. Dichas actividades son:

- establecimiento de la representación de políticas de control de acceso;
- establecimiento de representaciones de la ACI;
- asignación de la ACI a elementos (iniciadores, objetivos o peticiones de acceso);
- vinculación de la ACI a elementos;
- hacer que la ADI esté disponible para la ADF;
- realización de funciones de control de acceso;
- modificación de la ACI (en cualquier momento después de asignar valores de ACI; se incluye la revocación);
- revocación de la ADI.

Estas actividades pueden dividirse en dos grupos:

- las actividades operacionales (que ponen la ADI a disposición de la ADF y que realizan funciones de control de acceso); y
- las actividades de gestión (todas las restantes actividades).

Algunas de las actividades anteriores pueden agruparse como una sola actividad identificable en un sistema real. Aunque algunas actividades de control de acceso tienen necesariamente precedencia sobre otras, se produce a menudo el solapamiento de unas sobre otras, pudiendo algunas funciones realizarse repetitivamente.

Se presenta en primer lugar una descripción detallada de los conceptos involucrados en la realización de funciones de control de acceso, ya que todas las restantes actividades soportan a ésta.

5.2.1 Realización de funciones de control de acceso

Para los fines de esta subcláusula, las funciones fundamentales para el control de acceso se ilustran en las Figuras 5-1 y 5-2. Pueden requerirse otras funciones para el conjunto de la operación de control de acceso. En una discusión ulterior se presenta una amplia gama de formas en las que pueden implementarse dichas funciones, incluyendo distintas formas de distribución de las funciones de control de acceso y la ACI, y diferentes estilos de comunicación entre funciones de control de acceso en el mismo dominio o en dominios de seguridad cooperativos.

Las entidades y funciones básicas involucradas en el control de acceso son el iniciador, la función de refuerzo del control de acceso (AEF), la función de decisión de control de acceso (ADF) y el objetivo.

Los iniciadores pueden representar a seres humanos y a entidades basadas en computadoras que acceden o intentan acceder a los objetivos. En un sistema real, un iniciador se representa mediante una entidad basada en un computador, aunque las peticiones de acceso que, en nombre del iniciador, realiza la entidad basada en computador, pueden estar limitadas por la ACI de ésta última.

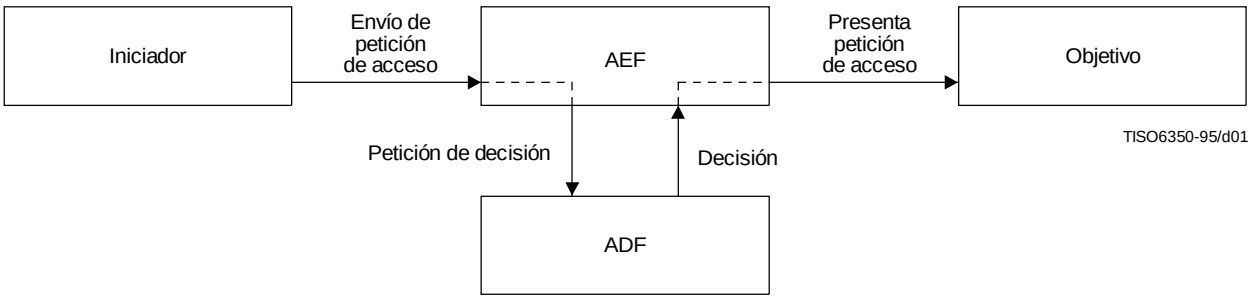

Figura 5-1 – Ilustración de funciones fundamentales de control de acceso

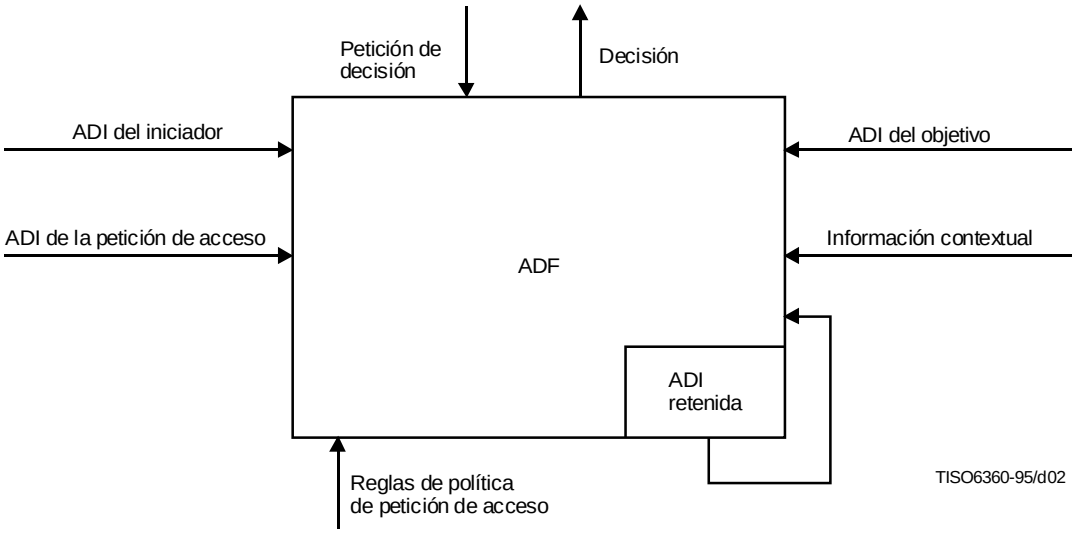

Figura 5-2 – Ilustración de la ADF

Los objetivos representan entidades basadas en ordenador o entidades de comunicación a la que se intenta acceder o que son accedidas por el iniciador. Un objetivo puede ser, por ejemplo, una entidad de capa OSI, un fichero o un sistema real.

Una petición de acceso representa la operación y los operandos que forman parte de un intento de acceso.

La AEF asegura que el iniciador sólo realiza sobre el objetivo accesos permitidos, tal como determina la ADF. Cuando un iniciador realiza una petición para realizar un acceso al objetivo, la AEF informa a la ADF que se requiere una decisión para tomar una determinación.

A fin de realizar esta decisión, se facilita a la ADF la petición de acceso (como parte de la petición de decisión) así como los siguientes tipos de información de decisión de control de acceso (ADI):

- ADI del iniciador (ADI que se deriva de ACI vinculada con el iniciador);
- ADI del objetivo (ADI que se deriva de ACI vinculada con el objetivo);
- ADI de la petición de acceso (ADI que se deriva de ACI vinculada con la petición de acceso).

El resto de la información que se aporta a la ADF está constituida por las reglas de política de control de acceso (a partir de la autoridad del dominio de seguridad de la ADF) así como cualquier información contextual necesaria para interpretar la ADI o la política. La ubicación del iniciador, la hora de acceso o el trayecto de comunicación utilizado son ejemplos de información contextual.

En base a la información aportada, y posiblemente a partir de ADI de decisiones previas, la ADF concluye en permitir o denegar al iniciador el intento de acceso al objetivo. La decisión se traslada a la AEF que permite que la petición de acceso pase al objetivo o bien toma las medidas oportunas.

Frecuentemente, las sucesivas peticiones de acceso realizadas por un iniciador sobre un objetivo están relacionadas. Un ejemplo típico es una aplicación que abre una conexión a un proceso de aplicación de un objetivo equivalente y realiza varios accesos utilizando la misma (retenida) ADI. En algunas peticiones de acceso sucesivas enviadas en la conexión, puede ser necesario proporcionar a la ADF ADI adicional para que se permita el acceso solicitado. Otras veces, la política de seguridad puede exigir que determinadas peticiones de acceso entre uno o más iniciadores y uno o más objetivos estén sujetas a restricciones. En estos casos, la ADF puede utilizar ADI retenida procedente de decisiones anteriores que incluían múltiples iniciadores y objetivos para tomar la decisión sobre una petición de acceso en concreto.

Para los fines de esta subcláusula, una petición de acceso implica una única transacción de un iniciador con un objetivo, si es que la AEF lo permite. Aunque algunas peticiones de acceso entre un iniciador y un objetivo son completamente independientes de otras, ocurre con frecuencia que entre dos entidades tiene lugar un conjunto de peticiones de acceso relacionadas, como por ejemplo, un paradigma de pregunta-respuesta. En estos casos, las entidades toman el papel de iniciador y objetivo según convenga, de forma simultánea o alternativa, al tiempo que las funciones de control de acceso se realizan para cada petición de acceso posiblemente por componentes de AEF independientes, componentes de ADF y políticas de control de acceso.

5.2.2 Otras actividades de control de acceso

5.2.2.1 Establecimiento de representaciones de políticas de control de acceso

Las políticas de control de acceso normalmente se establecen en un lenguaje natural en forma de principios genéricos; por ejemplo: sólo empleados de un cierto rango pueden consultar la información sobre el salario de los empleados. La conversión de estos principios en reglas constituye una actividad de diseño de ingeniería que debe preceder a otras actividades de control de acceso, y no forma parte del objetivo de este marco de seguridad. En la cláusula 6 se incluye una visión general de los conceptos propios de las políticas de control de acceso.

5.2.2.2 Establecimiento de representaciones de ACI

En esta actividad, se elige cuáles son las representaciones de ACI en sistemas reales (estructuras de datos) y para el intercambio entre sistemas reales (las sintaxis). En este marco de seguridad se describe una amplia gama de representaciones posibles. Las representaciones ACI deben soportar los requisitos de políticas de control de acceso específicas. Algunas representaciones ACI pueden ser adecuadas para ser utilizadas en sistemas reales y entre sistemas reales. Pueden utilizarse distintas representaciones de ACI con propósitos diferentes y entre elementos específicos.

Las representaciones de ACI elegidas pueden considerarse plantillas para la asignación de valores de ACI específicos a elementos en un dominio de seguridad (tal como se discute en la subcláusula siguiente). Un aspecto a considerar en el establecimiento de representaciones de ACI son los tipos y gamas de valores de ACI que pueden asignarse a los elementos en un dominio de seguridad (pero no los tipos que pueden asignarse a elementos específicos).

La representación de la ACI intercambiada entre sistemas reales para la gestión del control de acceso o para el intercambio de ACI entre entidades y funciones de control de acceso pueden ser objeto de normalización OSI. La representación de ACI en sistemas reales o su presentación ante una ADF local, no son asuntos sujetos a la normalización OSI. La protección del intercambio de ACI se describe en 7.2. Para las aplicaciones OSI (y posiblemente para otras), es conveniente considerar las representaciones de ACI como atributos que constan de pares de valores de atributo y tipo-atributo.

5.2.2.3 Asignación de ACI a iniciadores y objetivos

En esta actividad, los tipos de atributos y los valores de atributos de ACI que se asignan a un elemento, son diseñados por una SDA, sus agentes o por otras entidades (por ejemplo, los propietarios de los recursos). Dichas entidades pueden

especificar o modificar las asignaciones de ACI de acuerdo a la política del dominio de seguridad. Las ACI asignadas por una entidad pueden estar limitados por la ACI que otra entidad ha vinculado a la misma. La asignación de ACI a elementos es una actividad que continúa conforme se añaden nuevos elementos a un dominio de seguridad.

NOTA – El acto administrativo de otorgar «derechos de acceso» se suele denominar autorización. Este significado se incluye en la asignación de ACI a iniciadores u objetivos.

La ACI puede ser información acerca de una entidad o sobre relaciones entre entidades. La ACI asignada a un iniciador puede referirse exclusivamente a dicho iniciador, o puede referirse a las relaciones entre un iniciador y una serie de objetivos específicos, o entre dicho iniciador y posibles contextos. De esta forma, la ACI asignada a un iniciador puede incluir ACI de iniciador, ACI de objetivo o información contextual. De igual forma, la ACI asignada a un objetivo puede incluir ACI de objetivo, ACI de iniciador (de uno o más iniciadores) o información contextual.

En el funcionamiento real, la ACI debe estar vinculada a un elemento (véase 5.2.2.4) de forma que la ADF que utilice ADI derivada de la ACI vinculada considere verosímil dicha información. De esta forma, aunque la asignación de ACI a elementos es un requisito previo a la constitución de ACI vinculada, sólo la ACI que está vinculada a un elemento se presenta en un sistema abierto real.

5.2.2.4 Vinculación de la ACI con iniciadores, objetivos y peticiones de acceso

La vinculación de la ACI a elementos (por ejemplo, iniciador, objetivo o petición de acceso) crea un enlace de seguridad entre dicho elemento y la ACI asignada al mismo. La vinculación garantiza a las funciones de control de acceso y a otros elementos que la ACI es realmente asignada al elemento en particular y que no ha habido modificación desde que se realizó la vinculación. La vinculación se realiza utilizando un servicio de integridad. Existen varios mecanismos de vinculación, incluyendo algunos que dependen de la ubicación del elemento y de la ACI, y otros que dependen de algún proceso de firma criptográfica o de sellado. Es necesario proteger la integridad de la vinculación de ACI a elementos, tanto en los sistemas del iniciador como del objetivo (por ejemplo, mediante funciones de sistemas operativos tales como protección de archivos y separación de procesos), así como en el intercambio de ACI. Dado que pueden existir varias representaciones posibles de la ACI de un elemento (dentro de los sistemas y entre los sistemas), se pueden utilizar distintos mecanismos de vinculación para la misma ACI. En el contexto de algunas políticas de seguridad, debe mantenerse la confidencialidad de la ACI.

La vinculación de ACI a elementos es una actividad continuada en tanto que se añaden nuevos elementos a un dominio de seguridad. Una SDA, sus agentes u otra entidad autorizada puede suprimir o añadir vinculaciones ACI de acuerdo con la política de seguridad en vigor. Una SDA puede modificar la ACI vinculada con un elemento si ello es preciso para expresar cambios en la política de seguridad o en los atributos. La ACI vinculada puede incluir indicadores del periodo de validez, minimizando así la ACI que puede ser necesario revocar ulteriormente.

El momento en que una ACI se vincula a un elemento, así como la entidad hace que se invoque el mecanismo de vinculación, dependen del tipo de elemento. La SDA o sus agentes facilitan a los iniciadores las ACI vinculadas a ellos, estando éstas disponibles cuando los iniciadores realizan los accesos.

Cuando los objetivos se convierten en accesibles, disponen de ACI que han sido vinculadas a ellos por una SDA o por sus agentes. Los objetivos que son creados por una aplicación en nombre de un usuario o de otra aplicación, disponen de ACI vinculada a ellos en el instante de la creación o después de la misma. La ACI vinculada a dichos objetivos puede estar restringida por las limitaciones en la vinculación de la ACI con el usuario o la aplicación.

La ACI queda vinculada a una petición de acceso por un usuario o una aplicación, o por una SDA o sus agentes en nombre del usuario o la aplicación, antes de que se intente el acceso. De nuevo, la ACI vinculada a la petición de acceso puede estar restringida por las limitaciones de la ACI vinculada con el usuario o la aplicación. Ocurre a menudo que una petición de acceso da lugar a la creación de una nueva entidad objetivo (por ejemplo, cuando se transfiere un fichero entre sistemas). Dicha ACI del objetivo puede especificarse (o derivarse) de la ACI vinculada a la petición de acceso.

5.2.2.5 Poner la ADI a disposición de la ADF

Si tanto la política de control de acceso como los mecanismos de vinculación utilizados lo permiten, el iniciador o el objetivo pueden seleccionar un subconjunto de la ACI vinculada con un iniciador o con un objetivo para ser utilizado por la ADF en la toma de decisiones de control de acceso específicas. La ACI vinculada con un elemento puede quedar temporalmente vinculada con otro elemento, por ejemplo, cuando una entidad actúa en nombre de otra.

A fin de que puedan realizar sus funciones, las diversas ADI de la Figura 5-2 deben estar disponibles para las ADF. Nótese que en esta subcláusula no se hace ninguna suposición sobre la distribución física de las entidades, las funciones o la ADI, ni tampoco sobre cómo se hacen llegar las aportaciones a la ADF. En 5.3, 5.4 y en el Anexo D se presentan algunas posibles relaciones entre entidades y componentes de control de acceso distribuidas.

Existen tres posibilidades para la ADI del iniciador, la ADI del objetivo o la ADI de la petición de acceso:

a) la ADI puede ubicarse previamente en uno o más componentes ADF después de la asignación de valores de ADF;

b) la ADI puede derivarse de la ACI vinculada que se ha entregado a los componentes de ADF durante el proceso de control de acceso (posiblemente junto con el acceso que se ha intentado);

c) la ADI puede derivarse de la ACI vinculada que se ha obtenido de otras fuentes (por ejemplo, de un agente del servicio de guías). El iniciador o el objetivo obtienen la ACI vinculada [que la ADF no distingue de b)], o la ADF obtiene la ACI vinculada según se necesita [que ni el iniciador ni el objetivo distinguen de a)].

No se especifica cómo la ADF obtiene la ACI vinculada y deriva la ADI. El iniciador no entrega necesariamente la ACI vinculada con el iniciador, ni el objetivo entrega necesariamente la ACI vinculada con el objetivo, ni tampoco la ACI vinculada con la petición de acceso es necesariamente entregada con una petición de acceso.

La ADF debe poder determinar inequívocamente que la ADI se ha derivado de una ACI vinculada a elementos por una SDA adecuada. En 7.2 se describen los medios para garantizarlo.

5.2.2.6 Modificación de la ACI

La SDA puede modificar la ACI asignada y vinculada con un elemento según sea necesario para expresar atributos de seguridad cambiantes. La ACI puede modificarse en cualquier instante manteniendo su asignación a elementos. Si la modificación reduce los accesos permitidos por el iniciador o por los objetivos, este cambio puede requerir la revocación de la ACI y de la ADI que se ha derivado de ella, y que pueden ser retenidas por las ADF.

5.2.2.7 Revocación de la ACI

Una vez que se revoca la ACI, cualquier intento de utilización de la ADI que se ha derivado de dicha ACI debe dar lugar a un acceso no permitido. Debe evitarse cualquier intento de utilizar la ADI que se derivó de la ACI antes de que ésta fuera revocada; si éste se produce debe dar lugar a un acceso denegado. Si una vez que la ACI se revoca continúan los accesos en base a la ADI previamente derivada, la política de control de acceso en vigor puede exigir la terminación del acceso.

5.2.3 Envío de la ACI

En sistemas distribuidos es habitual que haya entidades que piden a otras entidades que realicen accesos en su nombre. Las entidades asumen los papeles de iniciador o de objetivo, aunque no todas las entidades pueden asumir ambos. Una entidad puede asumir simultáneamente el papel de iniciador en relación con una entidad al tiempo que constituye en sí misma un objetivo en relación con otra entidad que actúa como iniciador.

La Figura 5-3 muestra la noción básica de una entidad A que pide a otra entidad B que realice un acceso en su nombre a otra entidad C. La Figura 5-3 no muestra las diversas componentes de control de acceso que pueden verse involucradas en dicha cadena de acceso.

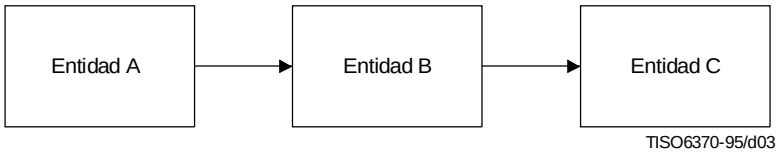

Figura 5-3 – Envío de la ACI

Existen diversas variaciones sobre este concepto básico. Las variaciones son claramente diferentes en las combinaciones de ACI requeridas por la política en vigor y que deben estar presentes para permitir que tengan lugar dichos accesos encadenados y en cómo dicha ACI está disponible para los componentes de control de acceso pertinentes. Con algunas políticas, B puede no necesitar más ACI para realizar el acceso en lugar de A que la que ya está vinculada a ella misma; con otras políticas, B sólo utilizará la ACI que obtiene de A y que es relevante para el acceso; en general, debe utilizarse ACI vinculada con A y con B.

Algunos ejemplos permiten tener una idea de la variedad de casos posibles:

a) Entre las posibilidades más sencillas está aquella por la que A pide a B que realice un acceso para el cual la ACI de B es suficiente.

b) A puede proporcionar parte o toda la ACI necesaria para que el acceso solicitado sea autorizado por los correspondientes componentes de control de acceso:

   1) A puede proporcionar dicha ACI entregándosela a B junto con la petición de acceso.

   2) A puede solicitar una autorización previa a C antes de pedir a B que realice el acceso. En este caso, A entregaría la ACI a C, el cual a su vez, proporcionaría a A un testigo. Este testigo se enviaría a B junto con la petición de acceso, reconociendo C el testigo como prueba de una autorización anterior. (Véase en el Anexo F información adicional sobre este caso.)

La Figura 5-3 generaliza el proceso a cualquier número de entidades intermedias, siendo la AEF de la última entidad la que toma una decisión de acceso en base fundamentalmente a la ACI obtenida de una o más entidades de la secuencia. El Anexo B contiene información adicional sobre la interacción entre iniciadores y objetivos en las secuencias complejas de acceso indirecto.

NOTA – El diseñador de una política de control de acceso debe ser consciente de que si no se toman todas las precauciones posibles, dicho tipo de acceso transitivo puede permitir accesos que no lo están de una forma directa.

5.3 Distribución de los componentes de control de acceso

Una AEF o una ADF pueden estar compuestas de uno o más componentes de control de acceso. Las funciones de control de acceso pueden estar distribuidas entre dichos componentes según permita la política de control de acceso. Las funciones de control de acceso básicas presentadas anteriormente son independientes de consideraciones relativas a la ubicación de los componentes, a las comunicaciones entre ellos o a su posible distribución.

Entre cada iniciador-objetivo se sitúa una AEF de forma que el iniciador pueda actuar sobre un objetivo sólo a través de dicha AEF. Existen varias posibilidades de realización práctica de componentes de ADF y AEF. Un componente de ADF puede o no estar coubicado (estrechamente acoplado) con un componente de AEF. Un componente de ADF puede servir a uno o más componentes de AEF. Igualmente, un componente de AEF puede utilizar uno o más componentes de ADF.

La coubicación (acoplamiento estrecho) de un componente AEF y de un componente ADF puede resultar beneficiosa en lo que respecta a eficiencia y prontitud (reducción del retardo), e igualmente puede evitar la necesidad de proteger las comunicaciones entre la AEF y la ADE. Los componentes de ADF que sirven a varios componentes de AEF pueden resultar ventajosos reduciendo la necesidad de distribuir la ACI y haciendo que determinadas funciones de seguridad asociadas, como por ejemplo la auditoría, sean menos complejas.

En el Anexo D se incluye una descripción de los componentes de AEF y ADF, ubicación y ejemplos de relaciones que se aplican a un único iniciador y un único objetivo. La ubicación de los componentes puede basarse en una o más de las consideraciones siguientes.

5.3.1 Control de acceso de entrada

Una SDA puede considerar que el control de acceso de entrada en un objetivo es suficiente. En ese caso, un componente de la AEF del objetivo fuerza una política de control de acceso de entrada pudiendo recibir el objetivo una petición que no sea conforme con la política de control de acceso para el objetivo. Ello significa que las peticiones de acceso enviadas por el iniciador alcanzan la AEF del objetivo y están sujetas a examen por la AEF del objetivo para garantizar que se satisface la política de control de acceso que ha sido impuesta por el componente de la ADF.

5.3.2 Control de acceso de salida

Una SDA puede considerar que es importante prevenir accesos no autorizados a objetivos mediante componentes de control de acceso locales al iniciador (por ejemplo, cuando la implementación del sistema de control de acceso no es de alta calidad o si los recursos de red disponibles no deben facilitarse sin comprobar antes que el acceso solicitado ha sido

autorizado), en cuyo caso es necesario el control de acceso de salida por parte de un iniciador de la AEF. En este caso, un iniciador no puede realizar un acceso que no sea conforme a la política de control de acceso del dominio de seguridad del iniciador.

5.3.3 Control de acceso interpuesto

Una SDA puede llegar a la conclusión que es importante filtrar los accesos entre iniciadores y objetivos, en cuyo caso, se interpone una AEF entre el iniciador y el objetivo. La AEF interpuesta puede imponer las políticas de control de acceso de entrada y de salida. Dichas políticas de control de acceso pueden ser independientes de las políticas de control de acceso de los dominios de seguridad del iniciador y del objetivo.

5.4 Distribución de los componentes de control de acceso a través de múltiples dominios de seguridad

Los dominios de seguridad pueden relacionarse de tal forma que los recursos de un dominio de seguridad pueden ser accedidos desde otro dominio de seguridad. Pueden estar involucrados múltiples dominios de seguridad, pero frecuentemente no todos ellos son distintos. Algunos de los dominios de seguridad aportan la ACI, algunos ejercen control sobre un acceso y otros hacen ambas cosas. Dichos dominios de seguridad pueden incluir:

- el dominio de seguridad en el que la ACI está vinculada al iniciador;
- el dominio de seguridad en el que reside el iniciador;
- el dominio de seguridad en el que la ACI está vinculada a la petición de acceso;
- el dominio de seguridad en el que la ACI está vinculada al objetivo;
- el dominio de seguridad en el que reside el objetivo;
- los dominios de seguridad en los que se toman las decisiones de control de acceso;
- los dominios de seguridad en los que se imponen las decisiones de control de acceso.

El proceso de control de acceso es entonces similar al caso en que todos los componentes de AEF y de ADF se encuentran bajo la misma SDA, tal como se describe en 5.3, con la complicación adicional de las relaciones entre las SDA y entre los dominios, así como de las comunicaciones entre los dominios.

Las comunicaciones entre los dominios incluyen:

- las notificaciones entre las SDA o sus agentes sobre nuevos vínculos de la ACI o sobre modificaciones de la misma;
- las peticiones, cuando tienen lugar los intentos de acceso, para verificar y traducir representaciones de la ACI y políticas de control de acceso, así como las respuestas a dichas peticiones;
- las peticiones para el acceso y las respuestas a dichas peticiones.

5.5 Amenazas al control de acceso

La ACI y las funciones de control de acceso pueden estar distribuidas en varios sistemas reales y dominios de seguridad. Las ACI pueden establecer comunicaciones entre ellas a través de medios poco fiables y pueden ser tratadas por componentes que funcionan bajo distintas SDA. Cuando están involucrados varias SDA, se necesita una relación de confianza entre ellas. Entre las amenazas que deben de tenerse en cuenta están las siguientes:

- usurpación de identidad por parte de una entidad que aparenta ser una AEF o una ADF válida;
- cortocircuitar una AEF;
- interceptación, reproducción y modificación de la ACI o de otras comunicaciones relacionadas con el control de acceso;
- utilización de la ACI por un iniciador distinto al deseado;
- utilización de la ACI para un objetivo distinto del deseado;
- utilización de la ACI para una petición de acceso distinta de la deseada;
- utilización de la ACI en una ADF equivocada;
- utilización de la ACI fuera de los límites deseados.

En 7.2 se describen mecanismos para conseguir protección contra amenazas al control de acceso.

6 Políticas de control de acceso

Las políticas de control de acceso expresan requisitos de seguridad en un dominio de seguridad. Una política de control de acceso es un conjunto de reglas impuestas por las ADF. Existen varias consideraciones que pueden incluirse en las políticas de control de acceso y en sus expresiones en forma de reglas. Una o varias de dichas consideraciones pueden ser aplicables a una política de seguridad concreta. Algunos mecanismos de control de acceso pueden acomodar más fácilmente que otros determinadas consideraciones (véase la cláusula 8).

NOTA – No se consideran aquí políticas de seguridad que podrían satisfacerse mediante mecanismos de control de acceso, pero que están relacionadas con otros servicios de seguridad (por ejemplo, confidencialidad, integridad).

Dos aspectos importantes y distintos de una política de control de acceso es la forma en que ésta se expresa y se gestiona (véanse 6.1 y 6.2). Es habitual que las políticas de control de acceso administrativamente impuestas se expresen e implementen utilizando etiquetas de seguridad, mientras que las políticas de control de acceso seleccionadas por los usuarios se expresan e implementan de forma diferente. No obstante, la expresión de las políticas de control de acceso, su gestión y el mecanismo utilizado para sustentarlas son lógicamente independientes unas de otras.

6.1 Expresión de la política de control de acceso

6.1.1 Categorías de las políticas de control de acceso

La Rec. X.800 del CCITT | ISO 7498-2 identifica dos categorías de política de seguridad, la política de seguridad basada en las reglas y la política de seguridad basada en la identidad. Las políticas de control de acceso basadas en las reglas se aplican a todas las peticiones de acceso de cualquier iniciador sobre cualquier objetivo en un dominio de seguridad. Las políticas de control de acceso basadas en la identidad se basan en reglas específicas para cada iniciador, o grupo de iniciadores, entidades que actúan en nombre de iniciadores u originadores que actúan con un rol especial. El contexto puede modificar las políticas de control de acceso basadas en las reglas o basadas en la identidad. Las reglas del contexto específico pueden definir completamente la política en vigor. Los sistemas reales utilizan normalmente una combinación de dichos tipos de políticas; se utiliza una política basada en reglas, también se suele utilizar simultáneamente una política basada en la identidad.

6.1.2 Grupos y roles

Las políticas de control de acceso que se establecen en términos de grupos de iniciadores o de iniciadores que actúan con roles específicos son tipos particulares de políticas basadas en la identidad.

Un grupo es un conjunto de iniciadores cuyos miembros se consideran equivalentes cuando se aplica una determinada política de control de acceso. Los grupos permiten el acceso a objetivos concretos por parte de un conjunto de iniciadores sin tener que incluir necesariamente la identidad de cada uno de ellos en la ACI del objetivo, y sin tener que asignar la misma ACI a cada iniciador. La composición de un grupo viene determinada en función de una acción de gestión; la posibilidad de crear o modificar grupos está sujeta al control de acceso. Puede requerirse la auditoría de las peticiones de acceso realizadas por el grupo sin hacer distinción entre los miembros.

El rol caracteriza las funciones que un usuario está autorizado a realizar en una organización. Un rol específico se puede aplicar a un solo individuo (por ejemplo, al director de departamento) o a varios individuos (por ejemplo, cajero, responsable de préstamos, miembro del comité de dirección).

Los grupos y los roles pueden utilizarse de forma jerárquica para combinar identidades de iniciadores, grupos y roles.

6.1.3 Etiquetas de seguridad

Las políticas de control de acceso que se establecen en términos de etiquetas de seguridad son tipos particulares de políticas de seguridad basadas en las reglas. Los iniciadores y los objetivos se asocian independientemente con etiquetas de seguridad. Las decisiones de acceso se basan en comparar las etiquetas de seguridad del iniciador y del objetivo. Estas políticas se expresan mediante reglas que describen qué accesos pueden tener lugar entre iniciadores y objetivos con etiquetas de seguridad específicas.

La expresión de las políticas de control de acceso en términos de etiquetas de seguridad son de especial utilidad cuando se utilizan como una forma de proporcionar integridad o confidencialidad.

6.1.4 Políticas de control de acceso de múltiples iniciadores

Existen muchas políticas de control de acceso que se establecen en base a múltiples iniciadores. Dichas políticas pueden identificar iniciadores individuales, iniciadores que son miembros del mismo o de diferentes grupos, iniciadores que ejercen roles diferentes, o bien, una combinación de los anteriores. Dichas políticas de control de acceso de partes múltiples incluyen, por ejemplo, lo siguiente:

- Individuos que son identificados de forma específica deben ponerse de acuerdo en un acceso específico para ellos. Suele ocurrir más frecuentemente que iniciadores que asumen roles específicos deben de acordar un acceso, como por ejemplo, presidente de compañía o un tesorero.
- Dos miembros de grupos diferentes deben acordar un acceso, tales como directivo de la compañía o miembro del consejo de dirección. En este ejemplo, la política en vigor puede exigir que el mismo individuo no pueda actuar en ambos grupos, de forma que las identidades individuales y la pertenencia a un grupo forma parte de la ADI utilizada por la ADF.
- Un número determinado de miembros de un grupo (posiblemente la mayoría del mismo) debe acordar un acceso.

6.2 Gestión de la política

En esta subcláusula se identifican tres aspectos de todo el espectro posible de gestión de la política de control de acceso.

6.2.1 Políticas fijas

Las políticas fijas son aquellas que siempre se aplican y no pueden modificarse, por ejemplo, por estar imbricadas en la propia construcción del sistema.

6.2.2 Políticas impuestas administrativamente

Las políticas establecidas por imposición administrativa son aquellas que se aplican en todo momento y no pueden ser modificadas o sólo pueden serlo por personas debidamente autorizadas.

6.2.3 Políticas seleccionables por el usuario

Las políticas seleccionables por el usuario son aquéllas que están disponibles a petición del iniciador o del objetivo y que sólo se aplican a peticiones de acceso que implican sólo a dicho iniciador u objetivo o a recursos de los mismos.

6.3 Granularidad y contenido

Las políticas de control de acceso pueden definir objetivos con un nivel variable de granularidad. Cada nivel de granularidad puede tener su propia política, lógicamente independiente, y puede autorizar la utilización de distintos componentes de AEF y ADF (aunque pueden utilizar la misma ADI). Por ejemplo, el control de acceso a un servidor de una base de datos puede estar orientado a la totalidad del mismo, es decir, un iniciador no está autorizado a acceder en absoluto a dicha base de datos o, por contra, puede acceder a la totalidad de la misma. De forma alternativa, el control de acceso puede estar orientado a ficheros en particular, registros dentro de ficheros o incluso elementos de datos dentro de registros. Una base de datos puede disponer de un árbol de información de guía, cuyo acceso puede estar sometido a control a un nivel de granularidad que comprenda todo el árbol, a nivel de subárboles dentro del árbol, o de entradas en un árbol, o incluso al nivel de atributos de entradas. Otro ejemplo de granularidad es un sistema de computador y las aplicaciones dentro del mismo.

El contenido puede utilizarse para controlar el acceso a un conjunto de objetivos especificando una política que permita el acceso a dichos objetivos sólo si se autoriza el acceso a un objetivo que los abarque. El contenido puede aplicarse también a subgrupos de iniciadores que estén contenidos en un grupo más grande. A menudo, el concepto de contenido se aplica a objetivos que están relacionados unos con otros, tales como ficheros de bases de datos o elementos de datos de registros. En el caso de un elemento que esté contenido en otro es necesario que el iniciador goce del derecho de acceso exigido para «pasar a través» del elemento continente antes de intentar el acceso al elemento contenido. Los diseñadores de estas políticas de seguridad deben de aplicar todas las precauciones posibles ya que puede ocurrir que con estas políticas de seguridad, el acceso que es denegado por una política pueda ser autorizado por otra sin ser ése el objetivo deseado.

6.4 Reglas de herencia

Un nuevo elemento puede crearse copiando un elemento existente, modificando un elemento existente, por combinación de elementos existentes o construyéndolo nuevo. La ACI del nuevo elemento puede depender de factores tales como

la ACI de su creador o la ACI de los elementos que fueron copiados, modificados o combinados. Existen reglas de herencia que especifican dichas dependencias, aunque el creador del elemento puede estar autorizado a imponer restricciones adicionales a la ACI.

Las reglas de la herencia son la parte de la política de control de acceso que determina la creación o modificación de la ACI, o la aplicación indirecta de una ACI a un elemento en base a su pertenencia a un dominio de seguridad o por el hecho de que un objetivo esté contenido en otro.

Las reglas de herencia pueden heredarse por el hecho de copiar, modificar o combinar elementos. Se puede autorizar a un iniciador que copie un objetivo para su propio uso, pero está prohibido realizar copias adicionales para permitir que otros iniciadores lo copien o lo utilicen. En otros casos puede ocurrir que una vez que se ha realizado una copia no exista control alguno sobre sus usos ulteriores.

Cuando un elemento está contenido en otro, alguna (o toda) su ACI puede implementarse a partir de la ACI del elemento que lo contiene de acuerdo con las reglas de herencia. Dichas reglas de herencia pueden simplificar la administración o uniformar las políticas aplicadas a un gran número de elementos.

6.5 Precedencia entre las reglas de la política de control de acceso

Es posible que las reglas de la política de control de acceso estén en conflicto unas con otras. Las reglas de precedencia explican el orden en que se aplican las reglas de política de control de acceso, así como cuáles son las reglas que tienen prioridad sobre otras. Por ejemplo, si las reglas A y B de una política de control de acceso dan lugar a que de forma independiente una ADF tome una decisión diferente frente a una petición de acceso, una regla de precedencia puede dar prioridad a la regla A, en cuyo caso la regla B no se consideraría, o bien la regla de precedencia puede hacer que ambas reglas permitan que se autorice el acceso a la petición.

Las reglas de precedencia pueden necesitarse para la utilización de la ACI vinculada al iniciador cuando el iniciador actúa como miembro de un grupo o en un rol en particular. La regla de precedencia puede permitir que la ACI del iniciador se combine con la ACI del grupo o del rol que ha asumido, en cuyo caso, debe también especificar cómo se deben combinar las ACI que están en conflicto unas con otras. Alternativamente, la regla de precedencia puede exigir que sólo la ACI del grupo o rol se aplique a una petición de acceso específica.

En los casos en los que una petición de acceso involucre múltiples dominios de seguridad, deben observarse los principios descritos en la Rec. X.810 | ISO/CEI 10181-1 relativos a políticas de interacción seguras.

6.6 Reglas de políticas de control de acceso por defecto

Una política de control de acceso puede incluir reglas de política de control de acceso por defecto. Éstas se utilizan cuando uno o más iniciadores no han recibido explícitamente la autorización o denegación para acceder a un objetivo determinado. Por ejemplo, una regla de política de control de acceso por defecto puede permitir acceder a un objetivo si el acceso no ha sido prohibido explícitamente por otra regla de política de control de acceso aplicada a la ADI que sea relevante.

6.7 Correspondencia de políticas entre dominios de seguridad cooperativos

Cuando se realiza el control de acceso para peticiones de acceso entre dominios de seguridad cooperativos, existe a veces la necesidad de hacer corresponder o traducir la ACI vinculada a la petición de acceso. Ello puede deberse al hecho de que los dominios de seguridad tengan distintas representaciones para la ACI o de la distinta interpretación que dos dominios de seguridad hagan de la misma ACI. Se enumeran algunos ejemplos de información para los que puede ser necesario establecer la correspondencia entre dominios de seguridad cooperativos:

- identificadores individuales, de grupo o de rol (por ejemplo, el identificador individual de JSmith en el dominio de seguridad X debe ser identificado como el identificador individual de XJSmith en el dominio de seguridad Y);
- los roles y sus atributos (por ejemplo, *el administrador de seguridad* de una red privada conectada a un operador público, debe ser reconocido como *administrador de seguridad de abonado* desde la red del operador público);
- identificadores individuales para el rol o grupo (por ejemplo, cuando a todos los individuos de una red privada se les hace corresponder un rol individual de abonado en la red de un operador público).

7 Información y facilidades de control de acceso

7.1 ACI

Tal como se describe en esta subcláusula, los tipos de información de control de acceso (ACI) incluyen iniciador, objetivo, petición de acceso, operación e información contextual. Como parte de las funciones de control de acceso, puede ser necesario el intercambio de ACI entre sistemas reales. Cuando tiene lugar dicho intercambio, es esencial que las entidades cooperativas hayan acordado la misma interpretación de la sintaxis abstracta. La presentación que se hace de la ACI en ésta fundamenta la descripción detallada que se hace en la cláusula 8 de los esquemas de control de acceso.

NOTA – A fin de maximizar el interfuncionamiento entre sistemas reales, existe la necesidad de normalizar la representación de la ACI. Los tipos de ACI que no se considera necesario normalizar (por ejemplo, la ADI retenida) no son objetivo de esta cláusula.

En función de la política de seguridad elegida, es necesario definir cuál es la ACI requerida.

7.1.1 ACI del iniciador

La ACI del iniciador es la relativa a un iniciador.

Los siguientes son algunos ejemplos de ACI de iniciador:

a) la identidad del control de acceso de un individuo;

b) el identificador del grupo jerárquico del que se afirma la pertenencia;

c) el identificador del grupo funcional del que se afirma la pertenencia;

d) los identificadores de los roles que se pueden asumir;

e) indicadores de sensibilidad;

f) indicadores de integridad.

NOTA – La identidad de control de acceso individual no es necesariamente la misma que la que se utiliza para la autenticación, auditoría o tasación. La identidad de control de acceso individual es única dentro del nombre del espacio de la SDA (véase el Anexo C).

7.1.2 ACI del objetivo

La ACI del objetivo es la relativa a un objetivo.

Los siguientes son algunos ejemplos de ACI de objetivo:

a) identidades de control de acceso del objetivo;

b) indicadores de sensibilidad;

c) indicadores de integridad;

d) identificador del contenedor de un objetivo.

7.1.3 ACI de la petición de acceso

La ACI de la petición de acceso es la relativa a una petición de acceso.

Los siguientes son algunos ejemplos de ACI de petición de acceso:

a) clase de operación permitida (por ejemplo, lectura, escritura);

b) nivel de integridad requerido para utilizar la operación;

c) tipo de datos de la operación.

7.1.4 ACI del operando

La ACI del operando es la relativa a un operando de petición de acceso.

Los siguientes son algunos ejemplos de ACI de operando:

a) indicadores de sensibilidad;

b) indicadores de integridad.

7.1.5 Información contextual

Los siguientes son ejemplos de información contextual:

a) periodos de tiempo: un acceso sólo se otorga dentro de periodos de tiempo especificados con precisión, tales como día, semana, mes, año, etc.;

b) ruta: un acceso sólo se otorga si la ruta utilizada tiene unas características específicas;

c) ubicación: un acceso sólo se otorga a iniciadores de un sistema determinado, estaciones de trabajo o terminales, o sólo a iniciadores situados en una ubicación física concreta;

d) estado del sistema: un acceso sólo se otorga a una ADI en particular cuando el sistema se encuentra en un estado específico (por ejemplo, durante el periodo de recuperación de un siniestro);

e) fortaleza de la autenticación: un acceso sólo se otorga cuando se utiliza un mecanismo de autenticación con un nivel de fortaleza mínimo;

f) otros accesos actualmente activos para éste u otros iniciadores.

7.1.6 ACI vinculada con el iniciador

La ACI vinculada con el iniciador puede contener la ACI del iniciador, alguna ACI del objetivo así como información contextual seleccionada. En la cláusula 8 se describen algunas formas de ACI vinculadas con el iniciador, tales como etiquetas de seguridad, capacidades y certificados de control de acceso. Algunos ejemplos son:

a) ACI del iniciador;

b) una identidad de control de acceso del objetivo y los accesos permitidos sobre el objetivo (es decir, las capacidades);

c) la ubicación del iniciador.

7.1.7 ACI vinculada con el objetivo

La ACI vinculada con el objetivo puede contener alguna ACI del iniciador, ACI de objetivo, e información contextual seleccionada. En la cláusula 8 se describen algunas formas de ACI vinculadas con el iniciador, tales como etiquetas y listas de control de acceso. Se enumeran a continuación algunos ejemplos:

a) identidades de control de acceso de iniciadores individuales así como los accesos al objetivo para los que tienen autorización de acceso o ésta ha sido denegada;

b) identidades de control de acceso a miembros de grupos jerárquicos así como los accesos al objetivo para los que tienen autorización de acceso o ésta ha sido denegada;

c) identidades de control de acceso a miembros de grupos funcionales así como los accesos al objetivo para los que tienen autorización de acceso o ésta ha sido denegada;

d) identidades de control de acceso de rol así como los accesos al objetivo a los que éstos tienen autorización de acceso o ésta ha sido denegada;

e) las autoridades y los accesos a los que éstas están autorizadas.

7.1.8 ACI vinculada con una petición de acceso

Una ACI vinculada con una petición de acceso puede contener una ACI del iniciador, ACI del objetivo e información contextual. Se enumeran a continuación algunos ejemplos:

a) las parejas iniciador/objetivo autorizadas a participar en un acceso;

b) los objetivos que están autorizados a participar en un acceso;

c) los iniciadores que están autorizados a participar en un acceso.

7.2 Protección de la ACI

7.2.1 Certificados de control de acceso

Las ACI intercambiadas entre sistemas reales requieren protección contra una amplia variedad de amenazas al control de acceso, tal como se describe en 5.5. Es necesario poder verificar la autoridad bajo la que se ha generado la ACI; esta verificación la realiza la ADF que utiliza la ADI que se deriva de dicha ACI. Una forma de facilitar esta verificación es empaquetando la ACI en un certificado de seguridad firmado o sellado por la autoridad de emisión. Dicho paquete se denomina certificado de control de acceso.

Un certificado de control de acceso puede contener información en diversas formas, muchas de las cuales son habituales para la protección de certificados de seguridad que se describen en la Rec. UIT-T X.810 | ISO/CEI 10181-1.

Se pueden incluir los siguientes elementos de información específicos del iniciador:

- la ACI del iniciador;
- los medios para validar la vinculación del certificado de control de acceso con un iniciador en particular, de forma que éste no pueda ser utilizado por otro iniciador;
- un identificador para una cuenta a la que se puede tasar el acceso;
- identificadores para las entidades responsables del acceso con fines de contabilidad o auditoría;
- el número de veces que puede utilizarse un certificado de control de acceso por parte de un iniciador en particular.

Pueden incluirse los elementos de información siguientes que son propios del objetivo:

- la ACI del objetivo;
- los medios para validar la vinculación del certificado de control de acceso con un objetivo específico de forma que no pueda ser utilizado para acceder a otro objetivo;
- el número de veces que puede utilizarse un certificado de control de acceso por parte de un iniciador en particular.

Pueden incluirse los elementos de información siguientes que son propios de la petición de acceso:

- los medios para validar la vinculación del certificado de control de acceso con una petición de acceso específica de forma que no pueda ser utilizado con otra petición de acceso;
- los medios para validar la vinculación del certificado de control de acceso con una o más peticiones de acceso de forma que pueda ser utilizado con otra petición de acceso (por ejemplo, para enviar el control de acceso);
- el número de veces que puede utilizarse un certificado de control de acceso para acceder a un objetivo en particular;
- la ACI de la petición de acceso.

7.2.2 Testigos de control de acceso

La ACI también puede protegerse ubicándola en un testigo de seguridad. El testigo de seguridad, a diferencia de un certificado de control de acceso que es firmado o sellado por una autoridad, puede ser producido por el iniciador. En el caso de control de acceso, el testigo de seguridad es relevante para la ACI vinculada con la petición de acceso.

La SDA puede proporcionar un certificado de control de acceso que puede ser utilizado en varias peticiones de acceso. Sin embargo, el iniciador puede generar un testigo de seguridad para vincular el certificado de control de acceso con una petición de acceso en particular.

Un testigo de seguridad puede contener información en diversas formas, muchas de las cuales son habituales para proteger testigos de seguridad y se describen en la Rec. UIT-T X.810 | ISO/CEI 10181-1.

Los mismos elementos de información propios del iniciador, el objetivo y la petición de acceso, que pueden incluirse en un certificado de control de acceso pueden también incluirse en un testigo de control de acceso.

7.3 Facilidades de control de acceso

En este punto se identifican una serie de facilidades de control de acceso que pueden utilizarse para proporcionar control de acceso en sistemas reales. Se hacen descripciones genéricas de facilidades de control de acceso independientes de mecanismos concretos. No se recomienda ninguna interfaz de primitiva específica para su utilización en sistemas reales.

NOTA – Aunque las facilidades de control de acceso se describen de forma genérica, muestran cuál es la tendencia general para proporcionar servicios de control de acceso. Sin embargo, por el hecho de que no figuren en esta subcláusula no debe presuponerse la invalidez de otros posibles enfoques.

Las facilidades de control de acceso se dividen en dos grupos, a saber, las relacionadas con la gestión que puede invocar, por ejemplo, un administrador de seguridad, y las relacionadas con la operación de control de acceso. En particular, las facilidades relacionadas con la gestión incluyen las actividades de «vinculación de ACI con elementos», tal como se describe en 5.2.2.4, «modificación de la ACI», como se describe en 5.2.2.6 y «revocación de la ACI», como se describe en 5.2.2.7. Las facilidades relacionadas con la operación sustentan las actividades de «hacer que la ADI está disponible para la ADF», tal como se describe en 5.2.2.5, y «realizando las funciones de control de acceso», tal como se describe en 5.2.1. Cuando los sistemas reales o los dominios de seguridad utilizan diferentes representaciones de la ACI, se requieren facilidades adicionales para hacer corresponder entre sí las distintas representaciones de la ACI.

7.3.1 Facilidades relacionadas con la gestión

De entre las actividades que se describen en 5.2.2, no se tratan aquí el establecimiento de la política y las representaciones de la ACI, así como la asignación de la ACI a elementos. La facilidad instalar la ACI está relacionada con la vinculación de la ACI con elementos. Las facilidades cambiar la ACI y revocar la ACI están relacionadas con la modificación y revocación de la ACI. Las facilidades destinadas a activar y desactivar los componentes de control de acceso y a listar la ACI de un elemento son adicionales a las actividades descritas en 5.2.1.

- Instalar la ACI – Esta facilidad vincula un conjunto inicial de ACI (por ejemplo, las capacidades que pueden utilizar los iniciadores, las etiquetas de seguridad que pueden utilizar los iniciadores y los objetivos y las ACL para los objetivos) con un elemento.
- Cambio de la ACI – Esta facilidad modifica (por ejemplo, añade o suprime) la ACI vinculada con un elemento.
- Revocar la ACI – Esta facilidad revoca la utilización de ACI vinculada a un elemento de forma que la ACI deja de ser relevante para dicho elemento. Difiere de cambiar la ACI en que también se revoca cualquier ADI relacionada con dicha ACI.
- Revocar la ADI retenida – Esta facilidad revoca la validez de ADI retenida.
- Listar la ACI – Esta facilidad lista la ACI que está vinculada con un elemento dado.
- Desactivar componente – Esta facilidad desactiva, es decir no permite, la utilización de un componente con función de control de acceso. En el caso de un componente de la AEF, la facilidad inhibe todos los accesos a través de dicho componente de la AEF (se evitan así accesos a objetivos que están atendidos exclusivamente por dicho componente de la AEF).
- Reactivar un componente – Esta facilidad permite reactivar la utilización de un componente con función de control de acceso.

7.3.2 Facilidades relacionadas con la operación

Las facilidades relacionadas con la operación se deben usar como se indica a continuación, pero debe notarse que no todas las interacciones de control de acceso necesitan de todos los pasos aquí señalados:

a) El iniciador de la primera petición de acceso de una actividad determina las SDA para los elementos involucrados en dicha actividad utilizando la facilidad de identificar las autoridades de seguridad de confianza (véase la Rec. UIT-T X.810 | ISO/CEI 10181-1).

b) Se establece una política de interacción segura para ser utilizada en la actividad (véase la Rec. UIT-T X.810 | ISO/CEI 10181-1).

c) La ACI está vinculada con elementos tal como se describe en 5.2.2.4 utilizando las facilidades de adquirir y generar la ACI.

d) La ADI está disponible para la ADF mediante la utilización de la facilidad de verificar la ACI vinculada y derivar la ADI.

e) Utilizando la facilidad de obtención de información contextual se logra disponer de la información contextual, según lo requiera la política de interacción segura.

f) La decisión de control de acceso se obtiene por medio de la facilidad decidir acceso.

Tal como se describe en 7.2, muchas de las facilidades descritas a continuación utilizan ACI protegida (para asegurar la integridad o confidencialidad según lo requiera la política de seguridad).

7.3.2.1 Adquirir la ACI vinculada con el iniciador

Esta facilidad permite disponer de la ACI vinculada con el iniciador, un certificado de control de acceso o un testigo de control de acceso que incluya la ACI vinculada con el iniciador, con anterioridad a una petición de acceso.

La invoca un iniciador o la ADF.

Las entradas a la misma pueden incluir:

- identidad del iniciador autenticado (tal como se obtiene la facilidad verificar, según define la Rec. UIT-T X.811 | ISO/CEI 10181-2);
- el criterio de selección de la ACI vinculada con el iniciador;

- el periodo de validez;
- la identidad de un objetivo o de un grupo de objetivos;
- una política de interacción segura.

Las salidas de la misma pueden incluir:

- el estado (éxito o fracaso de adquirir la facilidad vinculada con el iniciador);
- la ACI vinculada con el iniciador, el certificado de control de acceso o el testigo de control de acceso que contiene la ACI vinculada con el iniciador.

7.3.2.2 Adquirir la ACI vinculada con el objetivo

Esta facilidad obtiene la ACI vinculada con el objetivo.

Es invocada por la ADF.

Las entradas a la misma pueden incluir:

- la identidad del objetivo;
- el criterio de selección de la ACI vinculada con el objetivo;
- el periodo de validez;
- una política de interacción segura.

Las salidas de la misma pueden incluir:

- el estado;
- la ACI vinculada con el objetivo.

7.3.2.3 Generar la ACI vinculada con la petición de acceso

Esta facilidad vincula la ACI vinculada con el iniciador, la ACI de petición de acceso y la ACI vinculada con el operando, con una petición de acceso necesaria para tomar una decisión de control de acceso.

Es invocada por el iniciador.

Las entradas a la misma pueden incluir:

- la ACI vinculada con el iniciador (un certificado de control de acceso que contiene la ACI vinculada con el iniciador o la ADI retenida);
- la ACI vinculada con el operando;
- la identidad del objetivo;
- las operaciones y los operandos;
- el periodo de validez;
- una política de interacción segura.

Las posibles salidas de la misma pueden incluir:

- el estado;
- la ACI vinculada a la petición de acceso;
- el testigo de petición de acceso;
- el certificado de control de acceso (generado por una SDA en nombre del iniciador);
- la ADI retenida.

NOTA – La primera de una secuencia de peticiones de acceso puede devolver la ADI retenida, la cual puede utilizarse en lugar de la ACI vinculada con el iniciador.

7.3.2.4 Verificar la ACI vinculada y derivar la ADI

Esta facilidad verifica la validez de la ACI vinculada y deriva la ADI a partir de la misma. Si algunas o todas las ADI están previamente almacenadas en la ADF, este servicio se vería reforzado o sustituido por la recuperación de la ADI previamente almacenada.

Es invocada por la ADF.

Las entradas a la misma pueden incluir:

- la ACI vinculada (al iniciador, objetivo, petición de acceso u operando);
- el testigo de control de acceso;
- el certificado de control de acceso;
- las operaciones y los operandos;
- el periodo de validez;
- una política de interacción segura.

Las salidas de la misma pueden incluir:

- el estado;
- la operación y los operandos;
- la ADI (del iniciador, objetivo, petición de acceso u operando).

7.3.2.5 Obtener información contextual

Esta facilidad permite obtener la información contextual requerida para tomar una decisión de control de acceso.

Es invocada por el iniciador o la ADF.

Las entradas a la misma pueden incluir:

- las operaciones y los operandos;
- la información contextual requerida;
- una política de interacción segura.

Las salidas de la misma pueden incluir:

- el estado;
- la información contextual.

7.3.2.6 Decidir acceso

Esta facilidad determina si se permite un acceso.

Es invocada por la ADF.

Las entradas a la misma pueden incluir:

- las operaciones y los operandos;
- la ADI del iniciador;
- la ADI del operando;
- la ADI del objetivo;
- la información contextual;
- la ADI retenida;
- una política de interacción segura.

Las salidas de la misma pueden incluir:

- la decisión de control de acceso;
- el periodo de validez de la decisión;
- la secuencia de peticiones de acceso autorizadas;
- la ADI retenida.

8 Clasificación de los mecanismos de control de acceso

8.1 Introducción

Un mecanismo de control de acceso se compone de un esquema de control de acceso (por ejemplo, basado en listas de control de acceso, capacidades, etiquetas y contexto) y en los mecanismos de apoyo que proporcionan la ADI a la ADF para dicho esquema. En este punto se describen una serie de esquemas de control de acceso que se definen en términos

de la ACI que es necesario mantener en diversas ubicaciones (sobre todo en el iniciador o en el objetivo) y de los mecanismos comunes que se utilizan en la facilidad decidir acceso descrita en 7.3.2.6. Se describen el esquema básico y las variaciones más probables o comunes sobre dicho esquema.

En esta cláusula se describen las principales categorías de esquemas y mecanismos de control de acceso; su objetivo es mostrar que distintos esquemas, cada uno con sus ventajas e inconvenientes pueden coexistir en un marco único. Los esquemas típicos de control de acceso pueden definirse en términos de la ACI vinculada con el iniciador o vinculada con el objetivo de la forma siguiente:

a) Si se considera un conjunto de parejas (identidad del objetivo, tipo de operación) como la ACI vinculada con el iniciador y de identidades de objetivos como la ACI vinculada con el objetivo, aplicando una política de control de acceso adecuada, se obtiene lo que en esencia constituye un esquema de capacidades.

b) Si se considera lo que comúnmente se llama «acreditación» y «clasificación» como la ACI vinculada con el iniciador y la ACI vinculada con el objetivo respectivamente, aplicando una política de control de acceso adecuada, se obtiene lo que en esencia constituye un esquema basado en la etiqueta.

c) Si se considera la identidad del iniciador como la ACI vinculada con el iniciador y un conjunto de parejas (identidad del iniciador, tipo de operación) como la ACI vinculada con el objetivo, aplicando una política de control de acceso adecuada, se obtiene lo que en esencia constituye un esquema de lista de control de acceso.

d) Normalmente, junto con otros esquemas de control de acceso, se utilizan reglas relativas a información contextual, aunque éstas deban utilizarse solas para crear un esquema de control de acceso. La información contextual puede formar parte de la ACI vinculada con el iniciador, la ACI vinculada con la petición de acceso o la ACI vinculada con el objetivo, o bien puede ponerse a disposición de la ADF con independencia de otra ACI.

Es fácil vislumbrar variantes más sofisticadas del caso a) anterior en las que la identidad del objetivo se convierte en un tipo de objetivo con más de un objetivo en poder de un atributo «tipo» dado, proporcionando la aplicación un mayor campo de aplicación. Es un avance considerar este atributo «tipo» como una «acreditación» que se compara con la etiqueta de seguridad, llegándose al caso b) anterior. De igual forma, cada uno de los tres primeros esquemas pueden considerarse como casos particulares unos de otros. Cada esquema puede concebirse como parte de un todo continuo en el que los esquemas se superponen y no son totalmente diferentes.

Cuando los nombres de iniciadores se utilizan en los objetivos como ACI vinculada al objetivo (por ejemplo, en entradas de ACL), se dificulta la gestión diaria de la ACI vinculada con el objetivo en sistemas con una población dinámica de iniciadores. A la inversa, cuando los nombres de iniciadores se utilizan como la ACI vinculada al iniciador (por ejemplo, en capacidades) también se dificulta la gestión diaria en sistemas con una población dinámica de objetivos.

Por lo tanto, la gestión es claramente un factor que influye en la elección de la expresión de la política, y por tanto, resulta inadecuado definir una norma para todos los sistemas basado en uno u otro enfoque en particular. En la práctica, un sistema requerirá probablemente una serie de esquemas de control de acceso de orígenes diferentes.

8.2 Esquema de la ACL

8.2.1 Características básicas

Las características básicas de un esquema de lista de control de acceso son las siguientes:

a) el control de acceso se gestiona como una lista de parejas (cualificador del iniciador, cualificador de la operación) que constituye la ACI vinculada con el objetivo e identificadores individuales, de grupo o de rol que constituyen la ACI vinculada con el iniciador;

b) esta clase de esquema de control de acceso es conveniente cuando se requiere una granularidad muy fina de control de acceso;

c) esta clase de control de acceso es conveniente cuando existen unos pocos iniciadores o agrupaciones de iniciadores;

d) esta clase de esquema de control de acceso es conveniente para revocar el acceso a un objetivo o grupo de objetivos;

e) esta clase de esquema de control de acceso es conveniente cuando la gestión de control de acceso se realiza en base a cada objetivo en lugar de en base al iniciador;

f) esta clase de esquema de control de acceso no es conveniente cuando la población de iniciadores individuales o en grupos se modifica con frecuencia, pero sí lo es cuando las poblaciones de objetivos son dinámicas.

8.2.2 ACI

8.2.2.1 ACI vinculada con el iniciador

En un esquema de ACL, un identificador individual, de grupo o de rol es la ACI primaria vinculada con el iniciador.

8.2.2.2 ACI vinculada con el objetivo

En un esquema de ACL, una ACL es la ACI primaria vinculada con el objetivo. Una ACL es un conjunto o secuencia de entradas. Cada entrada tiene dos campos:

a) *Cualificador del iniciador*

En una ACL sencilla, el cualificador es el identificador distintivo de un iniciador al cual se aplica un «cualificador de operación» (véase más adelante). Sin embargo, el cualificador del iniciador puede ser menos específico, representando una ACI de iniciador más general, tal como su rol o pertenencia a un grupo.

b) *Cualificador del operador*

Describe las operaciones o las clases de operaciones (es una petición de acceso), permitidas o denegadas para el cualificador del iniciador asociado.

NOTA – Para ajustar aún más las condiciones de acceso pueden imponerse, además de las operaciones o las clases de operaciones, limitaciones a los valores de los operandos para refinar las condiciones del acceso deseado.

8.2.3 Mecanismos de apoyo

Pueden utilizarse dos mecanismos para obtener la ACI vinculada con el iniciador a partir de la cual se deriva la ADI requerida por la facilidad decidir acceso:

a) *La autenticación*

Si el control de acceso se basa en la identidad de un iniciador individual, dicha identidad puede ser validada, directa o indirectamente, utilizando la autenticación.

Si el control de acceso se basa en la identidad de grupo o de rol, la identidad autenticada es un parámetro para la facilidad adquirir ACI vinculada con el iniciador que es utilizada para obtener un grupo o rol validado.

b) *Los certificados de control de acceso o los testigos de control de acceso*

El iniciador obtiene un certificado o un testigo de control de acceso (o ambos) utilizando la facilidad de adquirir ACI vinculada con el iniciador. El iniciador vincula entonces dicho testigo o certificado de control de acceso con una petición de acceso utilizando la facilidad de generar ACI vinculada con la petición de acceso, siendo finalmente verificado por la ADF mediante la facilidad de verificar ACI vinculada y derivar ADI.

La aceptación de la autoridad de certificación identificada en un certificado de control de acceso, o del iniciador en el caso de un testigo de control de acceso, forma parte de la facilidad de verificar ACI vinculada y derivar ADI.

La ADI del iniciador (es decir, los identificadores individuales, de grupo o de rol), la petición de acceso y la ADI del objetivo (es decir, el cualificador de petición de acceso) son parámetros de la facilidad decidir acceso. Mediante un algoritmo de correspondencia adecuado la ADI del iniciador y la operación que se deriva de la petición de acceso se comparan con cada entrada de la lista de control de acceso (cualificador del iniciador y cualificador de la petición de acceso). La decisión de control de acceso se toma en función de si se establece dicha correspondencia. La indicación devuelta informa que se deniega el acceso si existe correspondencia con una lista de exclusiones o si no existe correspondencia con una lista de inclusiones. En otro caso, la decisión devuelta informa que se otorga el acceso.

8.2.4 Variaciones de este esquema

En esta subcláusula se describen variaciones habituales al esquema de lista de control de acceso antes descrito.

8.2.4.1 Las ACL ordenadas

En algunas ACL que utilizan secuencias de entradas, la regla para la búsqueda consiste en que la primera entrada que cualifica da por terminada la búsqueda. Por lo tanto, el orden de dichas ACL es relevante, permitiendo la expresión de políticas en las que los iniciadores individuales pueden ver denegado el acceso aunque en otros casos más generales, por ejemplo, para iniciadores de grupo, se otorgue a éstos el derecho de acceso.

8.2.4.2 Las ACL con iniciadores agrupados

La información de la ACL puede estructurarse para que se refleje la agrupación de derechos de acceso similares de un conjunto de iniciadores. Además, cuando los objetivos se agrupan, la ACL puede asociarse con grupos de objetivos. Puede utilizarse una jerarquía de ACL en la que las ACL de mayor nivel proporcionan información de control de acceso de poca granularidad para grupos grandes de objetivos que pueden verse invalidada por las ACL para subgrupos de objetivos.

8.2.4.3 Las ACL con cualificador de objetivo

Este caso es especialmente relevante cuando no se asocia una lista de control de acceso con un objetivo en particular. Debe especificarse un objetivo para cada entrada de la ACL. Las entradas de la ACL se estructuran como una tripleta:

- cualificador de iniciador;
- cualificador de petición de acceso; y
- cualificador de objetivo.

El algoritmo de correspondencia es el que compara la ACI del iniciador, la petición de acceso y la ACI del objetivo con cada entrada de cualificador de iniciador, cualificador de acción y cualificador de objetivo de la lista de control de acceso.

8.2.4.4 Las ACL con objetivos agrupados

Este caso implica la compartición de una sola ACL entre muchos objetivos, de forma que éstos se ven afectados por las decisiones derivadas de una ACL. Cuando un solo objetivo se ve sujeto al criterio de decisión de más de una ACL, la política de control de acceso del mecanismo de la ACL debe de definir la regla para combinar las decisiones resultantes.

8.2.4.5 Las ACL con cualificador de contexto

Este caso implica la utilización de información contextual. Las entradas de la ACL están estructuradas como una tripleta:

- cualificador de iniciador;
- cualificador de petición de acceso; y
- cualificador de contexto.

El cualificador de contexto es un cualificador adicional que describe las restricciones de contexto para dicha entrada. El algoritmo de correspondencia compara la ACI del iniciador, la petición de acceso y la información contextual con cada entrada de cualificador de iniciador, cualificador de acción y cualificador de contexto de la lista de control de acceso.

8.2.4.6 Las ACL con correspondencia parcial

En algunas implementaciones se soportan los cualificadores de correspondencia parcial, en los que partes de la identidad u otra ACI del iniciador debe de hacerse corresponder con el cualificador del iniciador. Por ejemplo, si un iniciador tiene un nombre que consta de una secuencia jerárquica de nombres componentes (tales como país, organización, unidad organizacional, nombre personal), la ACL puede construirse de forma que reconozca uno o más componentes que pueden ser considerados como identidades de grupo.

8.2.4.7 Las ACL sin cualificadores de petición de acceso

En esta variante de esquema de ACL, los conjuntos o secuencias de entrada de una ACL no contienen cualificadores de petición de acceso. En la facilidad decidir acceso no interviene, por tanto, ningún cualificador de petición de acceso. Si se autoriza el acceso de un iniciador, la autorización se extiende a todas las peticiones de acceso.

8.3 Esquema de la capacidad

8.3.1 Características básicas

Las características básicas del esquema de la capacidad son las siguientes:

a) 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;

b) este esquema de control de acceso es pertinente cuando existe un número reducido de objetivos;

c) este esquema de control de acceso no es conveniente para revocar el acceso a un objetivo, salvo que sea posible identificar de forma individual las capacidades que se venían ofreciendo al iniciador; sin embargo, es conveniente para que la SDA de un iniciador revoque los derechos de acceso de dicho iniciador;

d) este esquema de control de acceso es conveniente cuando la gestión de control de acceso la realizan los iniciadores;

e) este esquema de control de acceso es conveniente cuando existen «muchos» usuarios o «muchos» grupos de usuarios que acceden a «pocos» objetivos, estando objetivos y usuarios en distintos dominios de seguridad.

NOTA – La utilización de contraseñas para el control de acceso es similar, aunque diferente, de las capacidades. Las características básicas de las contraseñas son las siguientes:

– el control de acceso está basado en la ACI que comparten iniciador y objetivo;

– el control de acceso depende de que en el iniciador y en el objetivo así como en la transferencia, se mantenga la confidencialidad de la ACI (frecuentemente es difícil mantener la confidencialidad de las contraseñas);

– los cambios de las contraseñas pueden resultar difíciles si varios iniciadores comparten la misma.

8.3.2 ACI

8.3.2.1 ACI vinculada con el iniciador

La ACI vinculada con el iniciador es un conjunto de capacidades.

Una capacidad consta de dos componentes principales:

a) el nombre del objetivo o del conjunto de objetivos;

b) la lista de operaciones que están autorizadas sobre dicho objetivo.

Las capacidades pueden transportarse en un certificado de control de acceso firmado o sellado bajo la autoridad de la SDA.

8.3.2.2 ACI vinculada con el objetivo

La ACI vinculada con el objetivo es un conjunto de entradas. Cada entrada tiene dos componentes:

a) la identidad de la SDA;

b) las operaciones que puede autorizar la SDA.

8.3.3 Mecanismos de apoyo

Mediante la facilidad adquirir la ACI vinculada con el iniciador, éste obtiene un certificado de control de acceso o un testigo de control de acceso. El iniciador lo vincula con una petición de acceso mediante la facilidad generar la ACI vinculada con la petición de acceso. Finalmente, la ADF lo verifica utilizando la facilidad verificar vinculación de ACI y derivar ADI.

La ADI del iniciador (es decir, los contenidos de la capacidad), el nombre de la operación y la ADI del objetivo son parámetros de la facilidad decidir acceso. Se verifica si la ADI del objetivo es uno de los nombres de objetivo de la capacidad, e igualmente se comprueba si la operación es una de las que se mencionan en la capacidad. Si ambas verificaciones son exitosas se permite el acceso.

La facilidad decidir acceso deniega el acceso cuando:

a) la capacidad presente no se considera válida; o

b) el acceso al objetivo se ha conseguido mediante operaciones que la SDA autorizó indebidamente (es decir, la SDA no puede autorizar dichas operaciones); o

c) la operación que se deriva de la petición de acceso no se corresponde con la capacidad.

8.3.4 Variaciones de este esquema - Capacidades sin operaciones específicas

En esta variación del esquema de capacidad, ésta no contiene ningún conjunto de operaciones permitidas, y no se suministra el nombre de ninguna operación a la facilidad decidir acceso. Si se autoriza el acceso de un iniciador, se autoriza para todas las operaciones.

8.4 Esquema basado en la etiqueta

8.4.1 Características básicas

Las características básicas del esquema basado en la etiqueta son las siguientes:

a) Este esquema utiliza etiquetas de seguridad que pueden asignarse a iniciadores y objetivos, así como datos que se transfieren entre sistemas.

b) Este esquema es más conveniente cuando hay muchos iniciadores que acceden a muchos objetivos y sólo se requiere una granularidad poco fina del control de acceso.

c) Cuando se producen determinadas restricciones en la política, este esquema puede utilizarse para controlar el flujo de datos en un dominio de seguridad. Las etiquetas de seguridad también son convenientes para proporcionar el control de acceso entre dominios de seguridad.

d) Las operaciones que están permitidas no están explícitamente incluidas en la ACI vinculada con el iniciador o con el objetivo, pero se definen como parte de la política de seguridad.

NOTAS

1 Las etiquetas no son necesariamente estructuras sencillas.

2 Cuando un iniciador es un usuario humano (o el proceso de un iniciador representa a un usuario humano), la etiqueta vinculada con el iniciador se denomina a menudo acreditación. En estos casos, la etiqueta vinculada con el objetivo se denomina clasificación.

8.4.2 ACI

8.4.2.1 ACI vinculada con el iniciador

La ACI vinculada con el iniciador es una etiqueta de seguridad.

8.4.2.2 ACI vinculada con el objetivo

La ACI vinculada con el objetivo es una etiqueta de seguridad.

NOTA – Las representaciones de la ACI vinculada con el iniciador y de la ACI vinculada con el objetivo se estructuran normalmente de forma que se facilita su comparación, aunque no se utiliza la misma representación para ambas. En la Rec. UIT-T X.810 | ISO/CEI 10181-1 se describe la traducción de las representaciones de información de seguridad.

8.4.2.3 ACI vinculada con el operando

Los operandos de una petición de acceso pueden tener etiquetas vinculadas a ellos. Los operandos con etiqueta son un caso particular de datos con etiqueta.

Se deben garantizar dos propiedades de los datos con etiqueta: la integridad de la vinculación de la etiqueta a los datos y el derecho del iniciador a crear datos con dicha etiqueta.

Cuando se dan determinadas restricciones en la política, el etiquetado de seguridad puede utilizarse para proporcionar control de acceso general a los datos de un dominio de seguridad o entre dominios de seguridad.

Algunos ejemplos de datos con etiqueta son los siguientes:

– documentos;

– mensajes;

– unidades de datos sin conexión;

– ficheros que están siendo transferidos.

8.4.3 Mecanismos de apoyo

Pueden utilizarse cuatro mecanismos para obtener la ACI vinculada con el iniciador o la ACI vinculada con el objetivo utilizada en la facilidad decidir acceso.

a) *Utilizando certificados de control de acceso o testigos de control de acceso*

Véase 8.2.3.

b) *Utilizando la autenticación y la búsqueda*

La ADF obtiene una identidad del iniciador autenticado y la utiliza para buscar su acreditación.

c) *Utilizando un canal con etiqueta*

La acreditación del iniciador o la etiqueta de los datos puede estar implícita en la etiqueta del canal utilizado para transmitir la petición de acceso. La integridad de la vinculación de una etiqueta a un canal puede garantizarse por medio de un servicio de integridad. La garantía de que el canal se ha asignado «correctamente» puede obtenerse haciendo que sea el proveedor del servicio de comunicaciones quien lo verifique. Igualmente, la garantía de que la entidad objetivo está autorizada para aceptar un canal puede conseguirse haciendo que el proveedor del servicio de comunicaciones verifique la autorización antes de que se establezca el canal.

d) *Utilizando datos con etiqueta*

La acreditación del iniciador puede estar implícita en las etiquetas de los operandos de la petición de acceso. La integridad de la vinculación de una etiqueta con los datos puede ser proporcionada por la integridad del canal subyacente, o bien, utilizando un código de verificación de integridad o una firma de seguridad sobre los datos y la etiqueta de seguridad que produce la SDA.

Para proteger un objetivo puede utilizarse una etiqueta de seguridad como ACI del objetivo. Las reglas de acceso definen los permisos de acceso (operaciones) que se otorgan en función de cuáles son la etiqueta de seguridad del iniciador y la etiqueta de seguridad asignada al objetivo.

Si la política de seguridad exige que la ACI incluida en la etiqueta de seguridad se utilice como la ACI del objetivo, puede controlarse el flujo total de datos con destino y origen en el objetivo. De esta forma, el flujo de datos con destino y origen en los objetivos de los dominios de seguridad pueden analizarse aplicando la misma política de seguridad.

Pueden crearse objetivos dentro de otros objetivos. La etiqueta de seguridad del objetivo contenedor limita las etiquetas de seguridad que pueden asignarse al objetivo contenido según las reglas de la política de seguridad pertinente.

Los siguientes son algunos ejemplos de objetivos a los que se pueden aplicar etiquetas:

- n-entidades OSI;
- entradas al servicio de guías;
- campos de ficheros;
- entradas a bases de datos.

8.4.4 Los canales con etiqueta como objetivos

El creador de un canal (por ejemplo, la SDA) asigna una etiqueta de seguridad a un canal. Para utilizar el canal, la ACI del iniciador y la etiqueta de seguridad asignada al canal constituyen entradas a la facilidad decidir acceso. Es decir, se trata al canal como un objetivo. Las etiquetas de los datos transportados en un canal deben ser consistentes con la etiqueta del mismo.

La etiqueta asignada a un canal puede también utilizarse para controlar la ruta del mismo. En términos OSI, las entidades de capa N y los sistemas de retransmisión acceden a las conexiones de capa N-1 o unidades de datos sin conexión, es decir, las entidades deben cumplir las reglas de acceso para las conexiones de capa N-1 o unidades de datos sin conexión.

Los siguientes son ejemplos de canales etiquetados:

- asociaciones-A;
- conexiones de capa-n OSI;
- canales entre procesos.

8.5 Esquema basado en el contexto

8.5.1 Características básicas

En algunos casos, la ADF puede requerir información contextual para interpretar la ADI o las reglas de la política de seguridad. Las características básicas de un esquema basado en el contexto son las siguientes:

a) 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;

b) este esquema es conveniente para reforzar las reglas que son aplicables a todos los iniciadores.

8.5.2 ACI

8.5.2.1 Listas de control de contexto

Las listas de control de contexto son secuencias de entradas. Cada entrada tiene dos campos:

a) *Cualificador de contexto*

El cualificador de contexto es una secuencia de condiciones contextuales (por ejemplo, hora, ruta, ubicación) a las que se aplica un cualificador de operación. Cada condición contextual se asocia individualmente con una sentencia verdadera o falsa.

b) *Cualificador de operación*

Describe las operaciones que están permitidas para el cualificador de contexto asociado.

8.5.2.2 Información contextual

Esta información se obtiene a partir del contexto en el que se realiza la petición de acceso.

El contexto depende del entorno en el que la ADF recibe la petición de acceso. Existen varias formas de obtener información contextual, como por ejemplo, a partir de una interfaz de servicio en capas subyacentes o una interfaz de gestión local.

8.5.3 Mecanismos de apoyo

La ADF utiliza la facilidad obtener información contextual para obtener dicha información. La información contextual y las peticiones de acceso constituyen entradas a la facilidad decidir acceso. La operación solicitada que se deriva de la petición de acceso así como la información contextual proporcionada se comparan con el cualificador de la operación y el cualificador de contexto respectivamente, a fin de determinar si el acceso ha sido permitido o denegado.

8.5.4 Variaciones de este esquema

En algunas listas de control de contexto que utilizan secuencias de entradas, la regla de búsqueda consiste en que la primera entrada cualificada terminada la búsqueda. Para todas las entradas la regla es que se deniega el acceso si la información contextual no cumple todas las condiciones contextuales. De esta forma, se permitirían por ejemplo, políticas como las que permiten una operación en particular sólo desde determinadas ubicaciones y durante un periodo de tiempo dado, pero no si se utiliza una ruta en concreto.

9 Interacción con otros servicios y mecanismos de seguridad

En este punto se describen cómo pueden utilizarse otros mecanismos y servicios de seguridad para sustentar el control de acceso. No se describe la utilización del control de acceso para sustentar otros servicios de seguridad.

9.1 Autenticación

A veces no se entiende cabalmente la naturaleza de los servicios de control de acceso y de autenticación. Aunque existen aspectos comunes e interrelaciones, los servicios son diferentes. Algunos esquemas de control de acceso (por ejemplo, las ACL), descansan en identidades y, por lo tanto, requieren de la autenticación para garantizar la identidad. Una autenticación exitosa puede hacer que el iniciador obtenga algunas ACI. Nótese que en algunos sistemas la facilidad de verificación para la autenticación y la ADF están coubicados. En estos casos, el intercambio de autenticación es el único protocolo visible. En sistemas distribuidos, estas funciones no están necesariamente coubicadas y puede utilizarse una ACI de iniciador diferente. La identidad se considera entonces sólo como parte de la ACI vinculada con el iniciador.

La política de control de acceso puede describir las relaciones entre la autenticación y el control de acceso. Por ejemplo, si un mecanismo menos seguro autentifica al iniciador, la política de control de acceso puede dictar que algunas operaciones (por ejemplo, modificar) no puedan ser realizadas sobre el objetivo. Por otra parte, estas operaciones serían las permitidas si el iniciador fuera autentificado por un mecanismo más seguro.

9.2 Integridad de los datos

El servicio de integridad de los datos puede utilizarse para asegurar la integridad de las entradas y salidas dentro y entre los componentes de control de acceso; por ejemplo, para evitar la modificación de las capacidades, las ACL y la información contextual que se han transferido o almacenado.

9.3 Confidencialidad de los datos

Algunas políticas de seguridad pueden requerir el servicio de confidencialidad de los datos para establecer la confidencialidad de algunas entradas y salidas en y entre componentes de control; por ejemplo, para proteger contra una excesiva concentración o agregación de información sensible.

9.4 Auditoría

La ACI puede utilizarse para auditar las peticiones de acceso de un iniciador en particular. Puede ser necesario recopilar varios registros de auditoría para poder identificar exactamente qué peticiones de acceso ha realizado cada iniciador.

Una política de auditoría puede requerir que se registren algunos o todos los mecanismos de acceso. Una política de auditoría puede también necesitar información sobre el funcionamiento del mecanismo de control de acceso que debe registrarse (por ejemplo, las circunstancias en las que se han denegado los accesos). Una política de control de acceso puede requerir que no ocurran accesos que no hayan sido auditados, en cuyo caso, el mecanismo de control depende funcionalmente de un servicio de registro fiable.

En los casos en que se requiere contabilizar al iniciador, éste se ve sometido a la autenticación antes de un acceso. Es importante entender que aunque la autenticación y el control de acceso están a menudo fuertemente relacionados, no se realizan siempre bajo el control de las mismas autoridades, ni necesitan que las funciones estén coubicadas. La información utilizada para la autenticación puede ser necesaria para obtener la ACI vinculada con el iniciador (para más información véanse 8.5 y 9.1).

Es posible proporcionar el acceso anónimo con contabilidad en la forma siguiente:

- El iniciador obtiene de una SDA una ACI que incluye un identificador de auditoría asociado. Se registra la adquisición de la ACI: la identidad del iniciador y el identificador de auditoría se mantienen en un registro de auditoría de la ACI que genera el dominio de seguridad.

- El iniciador utiliza su ACI vinculada con el iniciador para acceder al objetivo. La ADF del dominio de seguridad objetivo que recibe la ACI vinculada con el iniciador, almacena el identificador de auditoría y la petición de acceso en su registro de auditoría.

- Una SDA que acceda a la información de auditoría desde el dominio de seguridad objetivo y de la ACI vinculada con el iniciador que genera el dominio de seguridad puede identificar al iniciador utilizando al identificador de auditoría. De esta forma pueden contabilizarse los accesos del iniciador.

Si existe algún conflicto entre el deseo de anonimato del iniciador y los requisitos del dominio de seguridad objetivo sobre el conocimiento de la identidad del iniciador, el acceso puede ser rechazado; la decisión depende de la política de control de acceso del dominio de seguridad objetivo.

9.5 Otros servicios relacionados con el acceso

El control de acceso no es el único servicio que se realiza cuando se hace la petición de acceso. La auditoría (véase el punto anterior), la contabilidad y la tasación son otros servicios relacionados con la seguridad que funcionan cuando se realiza una petición de acceso:

- el servicio de auditoría registra información arbitraria sobre la petición de acceso;

- el servicio de contabilidad audita específicamente el nombre o los nombres de las entidades responsables de invocar la petición de acceso;

- el servicio de tasación garantiza que se debite una cuenta por una cantidad adecuada para ser utilizada por el recurso accedido.

La información requerida en una petición de acceso para soportar cada uno de dichos servicios es lógicamente diferente. La ADI proporcionada para el control de acceso, el nombre de cuenta para la tasación y la identificación de la entidad responsable de la contabilidad, pueden ser diferentes. Sin embargo, en algunas realizaciones prácticas se debe utilizar la misma información (por ejemplo, la identidad del control de acceso) para cada una de ellas. Ello puede dar a lugar a cierta confusión, especialmente en presencia de peticiones de acceso transmitidas. Es preferible mantener separados los distintos tipos de información.

Anexo A

Intercambio de certificados de control de acceso entre componentes

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

A.1 Introducción

El objetivo de este anexo es proporcionar un ejemplo práctico de cómo se envían certificados de control de acceso entre componentes, en donde algunos componentes actúan al mismo tiempo como objetivos e iniciadores y para establecer los requisitos generales para transferir múltiples certificados de control de acceso entre distintos componentes en un acceso encadenado.

A.2 Transferencia de certificados de control de acceso

La visión general de los marcos de seguridad describe una serie de mecanismos que permiten a una entidad utilizar un certificado de seguridad para transferir este derecho a otras entidades. En situaciones en las que una entidad B realiza peticiones de acceso en nombre de otra entidad, A, pueden utilizarse estos mecanismos para transferir el derecho de utilizar un certificado de control de acceso desde A hasta B.

A.3 Transferencia de múltiples certificados de control de acceso

En algunos casos puede ser necesario utilizar varios certificados de control de acceso para realizar una interacción compleja. Este requisito se ilustra mediante un ejemplo, ofreciéndose así una visión de las fuentes y la utilización de los distintos certificados de control de acceso que pueden requerirse. Se identifican tres clases de certificados de control de acceso, cada uno con características diferentes. Finalmente, el ejemplo se amplía para ofrecer una visión más general.

A.3.1 Ejemplo

Se supone que la aplicación A2 puede ser accedida por la aplicación A1 utilizada por el usuario U. Los accesos los solicita A1 sobre A2. Sin embargo, A2 puede utilizar los servicios de otra aplicación A3 para satisfacer la petición de acceso; a su vez, A3 puede necesitar los servicios de la aplicación A4, tal como se ilustra en la Figura A-1.

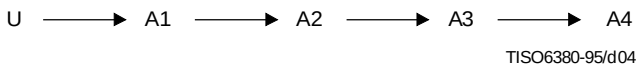

Figura A.1 – Transferencia de múltiples certificados de control de acceso

Considérese primero la relación entre A1 y A2 y los certificados de control de acceso que deben estar asociados con un acceso solicitado por A1 sobre A2. Pueden requerirse dos certificados de control de acceso: para el usuario U y para la aplicación A1.

Existen tres clases de certificados de control de acceso que pueden ser necesarios para el usuario U y para la aplicación A1:

- los certificados de control de acceso necesarios para acceder a A2 y válidos para todas las operaciones;
- los certificados de control de acceso necesarios para acceder a A2 y válidos para un conjunto específico de operaciones;
- los certificados de control de acceso necesarios para acceder a A2 y válidos para una sola operación.

En principio, cada certificado de control de acceso puede obtenerse de una SDA distinta.

Los certificados de control de acceso válidos para todas las operaciones se envían al comienzo de una conexión o de una asociación.

Cuando los certificados de control de acceso definen un conjunto de operaciones, éstas permanecen sin modificar hasta que se reciben otros certificados de control de acceso de esta clase.

Los certificados de control de acceso válidos para una sola operación están vinculados a dicha operación.

A.3.2 Generalización

Considérese a continuación la relación entre A2 y A3 y los certificados de control de acceso que deben estar asociados con un acceso solicitado por A2 sobre A3. Pueden necesitarse tres certificados de control de acceso: para el usuario U, para la aplicación A1 y para la aplicación A2.

Los certificados de control de acceso para que el usuario U y la aplicación A1 los utilicen con A2, pueden o no ser útiles con A3. Si lo son, cada uno de dichos certificados pueden ser de cualquiera de las tres clases antes descritas. Si no lo son, el usuario U o la aplicación A1 (o ambos) deben, cuando se realiza un acceso sobre A2, proporcionar un certificado de control de acceso para ser utilizado en A3; este certificado puede, a su vez, ser de cualquiera de las tres clases anteriores.

Este esquema puede generalizarse para la relación entre A3 y A4, con posibles certificados adicionales necesarios desde U, A1 o A2.

A.3.3 Simplificaciones

Normalmente sólo se necesita el certificado de control de acceso del usuario U o el certificado de control de acceso de la aplicación A1. Un certificado de control de acceso de U para ser utilizado en A2 puede ser enviado por A1 aunque no sea utilizado en A1.

Anexo B

Control de acceso en el modelo de referencia OSI

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

NOTA – Este texto se basa en la Rec. X.800 del CCITT | ISO 7498-2.

B.1 General

El control de acceso puede establecerse durante el establecimiento de la fase de transferencia de datos de una conexión o durante la propia conexión. Este servicio está disponible en protocolos orientados a la conexión y en protocolos sin conexión.

B.2 Utilización del control de acceso en las capas OSI

El control de acceso sólo es relevante en las capas siguientes de la OSI:

- capa de red (capa 3);
- capa de transporte (capa 4);
- capa de aplicación (capa 7).

B.2.1 Utilización del control de acceso en la capa de red

Cuando se utiliza el control de acceso en la capa de red éste permite el control de acceso hacia y desde los nodos de red, nodos de subred o relevadores. El control de acceso en la capa de red puede servir a muchos objetivos. Por ejemplo, permite que un sistema extremo controle el establecimiento de conexiones de red y rechace las llamadas no deseadas. Permite también que una o varias subredes controlen la utilización de los recursos de la capa de red. En algunos casos, esta última finalidad se relaciona con la tarificación por la utilización de la red.

Los mecanismos de control de acceso utilizados por la capa de red se encuentran dentro de la misma capa.

B.2.2 Utilización del control de acceso en la capa de transporte

Cuando se utiliza el control de acceso en la capa de transporte éste permite el control de acceso hacia y desde las entidades de sesión. No pueden controlarse independientemente distintas aplicaciones que sean soportadas por el mismo sistema extremo si éstas comparten una conexión de transporte.

Los mecanismos utilizados por la capa de transporte se encuentran dentro de la misma capa.

B.2.3 Utilización de control de acceso en la capa de aplicación

Véase la interconexión de sistemas abiertos – Modelo de seguridad de la capa superior (ISO 10745).

Anexo C

No unicidad de las identidades de control de acceso

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

Se exponen dos ejemplos para demostrar problemas potenciales que pueden surgir en la asignación y utilización de identidades de control de acceso.

- Si al nombre de un usuario, Pierre Durand, supuestamente muy común, se le asigna en un dominio de seguridad en particular la cadena de caracteres «Pierre Durand» como su identidad de control de acceso individual, la misma cadena de caracteres puede utilizarse en un atributo de control para otorgar algunos accesos permitidos a dicho usuario. Pierre Durand puede abandonar este dominio de seguridad y otra persona que también se llame Pierre Durand puede entrar ulteriormente en el mismo y recibir la identidad de control de acceso individual «Pierre Durand». Si la cadena de caracteres «Pierre Durand» es un atributo de control, el nuevo Pierre Durand podrá realizar accesos que estaban permitidos al antiguo Pierre Durand.

- Si a un objetivo se le asigna una cadena de caracteres como su identidad de control de acceso en un dominio de seguridad, la misma cadena de caracteres puede utilizarse en un atributo de privilegio para otorgar algunos accesos permitidos a un usuario. Dicho objetivo puede ser borrado del dominio de seguridad y, posteriormente, puede crearse otro objetivo con la misma identidad de control de acceso. Si no se ha modificado el atributo de privilegio concedido al usuario, será válido para el acceso al nuevo objetivo.

Las identidades de control de acceso deben de ser únicas dentro de un dominio de seguridad. Sin embargo, una identidad puede ser válida sólo durante determinados periodos de tiempo o quizás, efectivos indefinidamente. Cuando una identidad sólo es válida durante periodos de tiempo determinados, en cualquier momento un tipo de atributo dado que tenga como valor de atributo dicha identidad de control de acceso, tiene un significado específico. No obstante, si no se toman las precauciones necesarias, pueden reutilizarse el mismo tipo y valor de atributo. Si existe aún algún caso de tipo o valor de atributo anterior en el dominio de seguridad, puede tener lugar una violación de seguridad.

Existen dos formas de solucionar este problema. Antes de definir un nuevo tipo o valor de atributo de control de acceso, la SDA debe garantizar que dicho tipo o valor de atributo de control de acceso:

- no está asignado actualmente; o

- no ha sido utilizado nunca.

En el primer caso, la SDA necesita estar segura de que cada vez que un tipo o valor de un atributo de control de acceso se elimina, no queda ningún iniciador ni objetivo que posea dicho tipo de atributo de control de acceso o valor de atributo de control de acceso. Cuando ello no es posible, debe de definirse el periodo de validez (implícito o explícito) para cada tipo o valor de atributo de control de acceso. En dicho periodo de validez, es necesario seguir la pista de todos los tipos o valores de atributos de control de acceso.

En el segundo caso, debe definirse una única identidad de control de acceso (también llamada identificador permanente) que es un valor asignado solamente una vez y que no puede ser reutilizado.

Anexo D

Distribución de las componentes de control de acceso

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

Las funciones de control de acceso básicas, AEF y ADF, pueden constar de uno o más componentes que, cuando se combinan, realizan las funciones de la AEF o de la ADF (componentes de AEF-«AEC», y componentes de ADF-«ADC»). En 5.2, estas funciones se presentan independientemente de consideraciones sobre la ubicación de los componentes, la comunicación entre ellos o su posible distribución. En 5.4 se describe el control de acceso entre componentes bajo el control de distintas SDA.

D.1 Aspectos considerados

En la discusión ulterior son de particular interés:

- el número y ubicación de los AEC y los ADC; y
- la interacción entre los iniciadores, los AEC, los ADC y los objetivos.

En cualquier dominio de seguridad, entre cada pareja iniciador-objetivo pueden interponerse uno o más AEC, de forma que un iniciador pueda actuar sobre un objetivo, sólo a través de los AEC. Se pueden dar varias situaciones relativas a los AEC y los ADC, a saber:

- una AEF puede estar distribuida de diversas formas; éstas se describen en D.3 y se ilustran en las Figuras D.1, D.2 y D.3;
- un ADC puede estar o no coubicado (estrechamente emparejado) con un AEC;
- un ADC puede servir un solo AEC o varios AEC;
- un AEC puede utilizar un solo ADC o varios ADC.

Existen varias posibles ordenaciones de las comunicaciones entre los componentes que estén presentes.

D.2 Ubicaciones de los AEC y los ADC

Los AEC pueden ser parte integral (interna) de un sistema extremo o estar interpuestos (externos) entre el sistema extremo y la red utilizada para comunicar con otros sistemas extremos, tal como se ilustra en la Figura D.1. Algunos sistemas reales pueden utilizar AEC integrales e interpuestos para gestionar diferentes aspectos del control de acceso. Las ventajas e inconvenientes de los AEC externos e internos se relacionan con la política, con la confianza que despierten las implementaciones y con otras consideraciones que no se tiene aquí en cuenta.

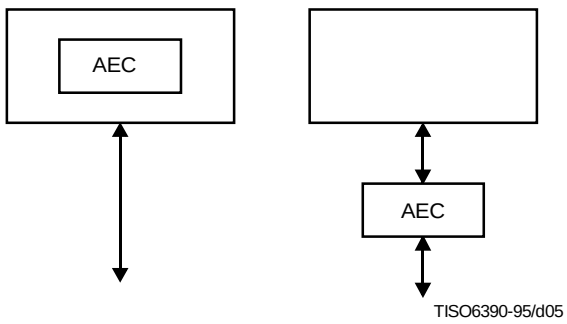

Figura D.1 – Implementaciones internas y externas de la AEF

Igualmente, los ADC pueden ser internos o externos a los sistemas extremos, tal como se ilustra en la Figura D.2. Los ADC que sirven a un solo AEC externo, es probable pero no necesario, que también sean externos. Los ADC que sirven varios AEC en distintos sistemas extremos son normalmente externos. Tal como se ha señalado antes, un sistema extremo puede utilizar varios AEC para distintos aspectos del control de acceso. En dichos casos, un solo ADC, interno o externo, puede servir a dichos AEC, pudiendo utilizarse varios ADC con el mismo fin. La coubicación (emparejamiento estrecho) de un AEC y un ADC puede tener ventajas en lo relativo a eficiencia y tiempo (reducción del retardo).

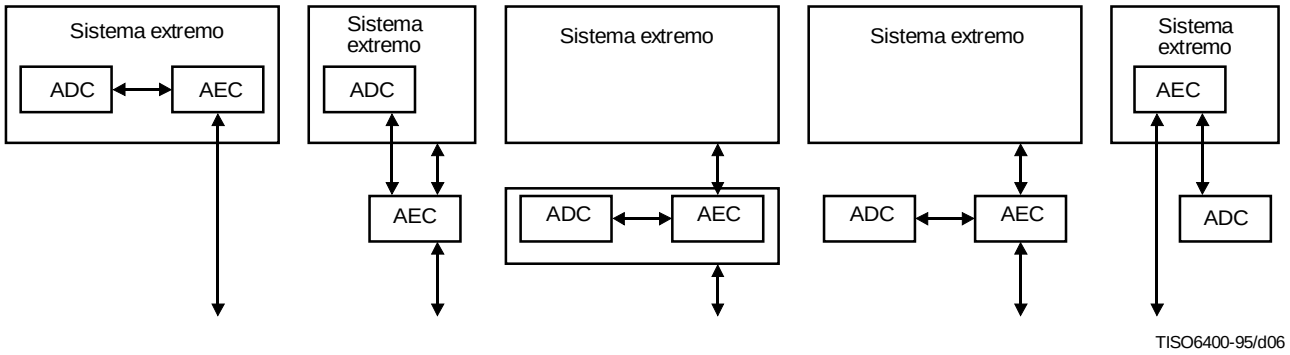

Figura D.2 – Implementaciones de la AEF y la ADF

D.3 Interacciones entre componentes de control de acceso

La ADF puede implementarse en base a uno o varios componentes de ADF e igualmente la AEF puede implementarse en base a uno o varios componentes de AEF. En este punto se describen cuáles son las relaciones entre las componentes de control de acceso, que se ilustran en la Figura D.3. Las relaciones aquí descritas sólo se aplican a un solo iniciador y a un solo objetivo. Otros ejemplos pueden incluir un AEC que utilice más de un ADC.

En (a), el iniciador (I) hace su petición de acceso directamente al AEC del objetivo, el cual lo presenta para su aprobación al ADC. Si se aprueba el acceso, el AEC notifica el objetivo (T) de la petición.

En (b), el iniciador hace su petición de acceso directamente al AEC del objetivo, el cual lo presenta para su aprobación al ADC. Si se aprueba el acceso, el AEC notifica el objetivo de la petición.

Existe una correlación entre funcionalidad y ubicación en (a) y (b). El AEC realiza el control de acceso de salida o de entrada o bien ambos, y por lo tanto, el AEC puede ser llamado iniciador, objetivo o AEC interpuesto.

En (c), el iniciador hace su petición de acceso al AEC interpuesto, el cual lo presenta para su aprobación al ADC. Si se aprueba el acceso, el AEC notifica el objetivo de la petición.

En (d), la interacción es una composición de (a) y (b), siendo el mismo ADC el que aprueba la petición de acceso para los AEC del iniciador y del objetivo. El iniciador hace su petición de acceso al AEC del iniciador, el cual solicita aprobación al ADC. Si se aprueba el acceso, el AEC del iniciador presenta el acceso solicitado al AEC del objetivo, que a su vez, lo presenta para su aprobación al ADC. También si se aprueba el acceso, el AEC del objetivo notifica el objetivo de la petición.

En (e) y (f), los AEC separados imponen el control de acceso de entrada y de salida. En (e), la interacción es similar a (c) excepto en que ambos AEC deben aprobar el acceso solicitado. En (f) la interacción es una composición de (a) y (b), con AEC separados.

La descripción anterior es de naturaleza muy simple. No obstante, son posibles interacciones más complejas entre el iniciador, el objetivo y los AEC, de forma que se incluya el secuenciamiento, anidamiento y las entradas recurrentes.

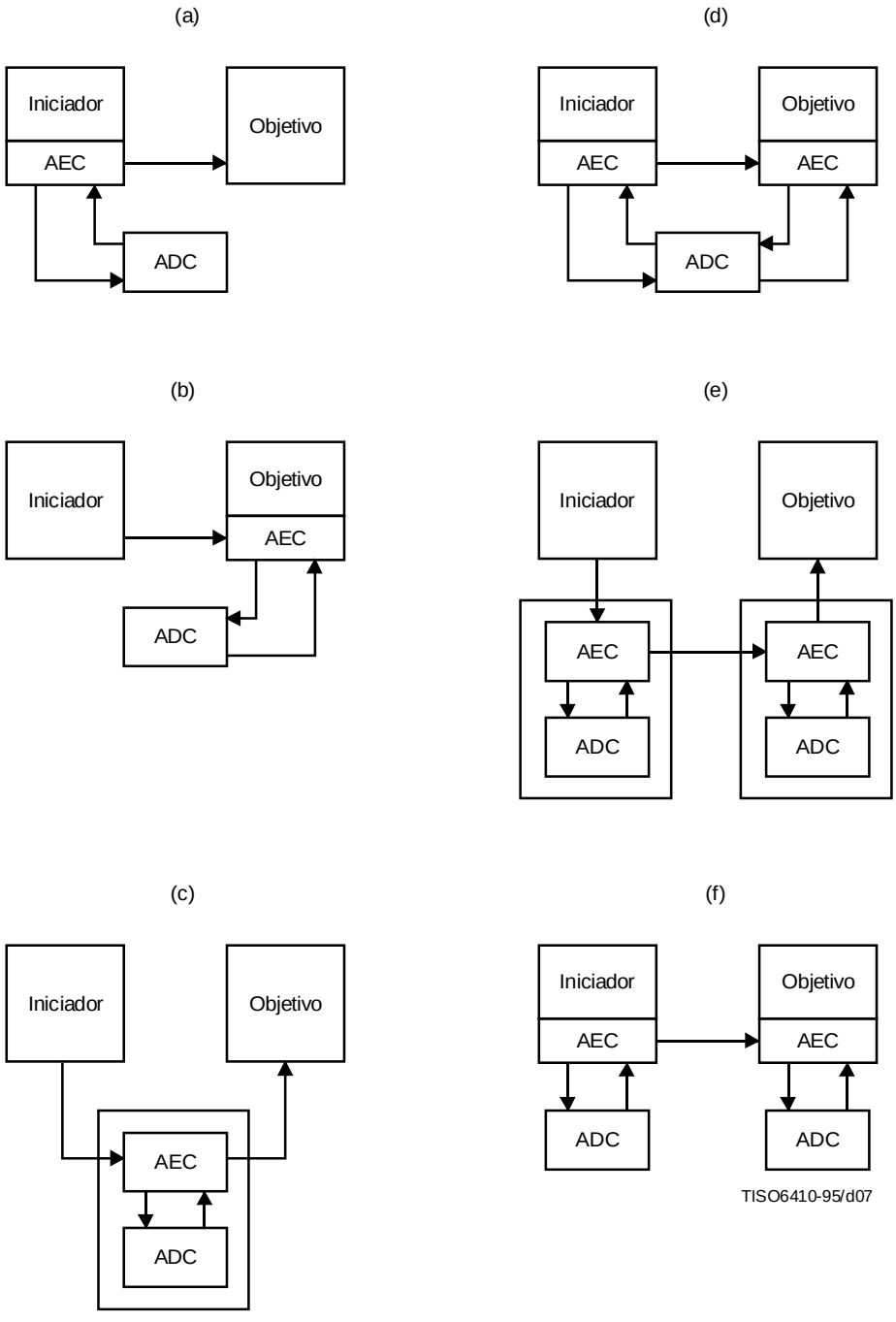

Figura D.3 – Relaciones de componentes

Anexo E

Políticas basadas en las reglas frente a políticas basadas en la identidad

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

Las políticas de control de acceso basadas en las reglas son a menudo concebidas como políticas basadas en etiquetas de seguridad, donde los iniciadores disponen de acreditaciones tales como «secreto» o «técnica» y los objetivos protegidos disponen de clasificaciones que se denominan de igual forma.

Una política de control de acceso basada en la identidad es una política en la que se concede o deniega el acceso a usuarios individuales, a grupos o a roles en base a su identidad o su ACI.

Cuando se hace un examen detallado, se aprecia que no existe una clara distinción entre una política de control de acceso basada en reglas y una política de control de acceso basada en la identidad: las acreditaciones de la política basada en las reglas y la ACI del iniciador son prácticamente los mismos. Las acreditaciones relacionadas con una política de control de acceso pueden considerarse como una ACI de iniciador específica. Si bajo una política basada en las reglas los usuarios poseen acreditaciones individuales no jerárquicas y unívocas, dichas acreditaciones son equivalentes a las identidades de los usuarios, y las clasificaciones de los objetivos son equivalentes a entradas de listas de control de acceso.

Otra distinción que a menudo se hace entre las políticas basadas en las reglas y las políticas basadas en la identidad es que las políticas basadas en las reglas se aplican administrativamente, mientras que las basadas en la identidad son seleccionables por el usuario. En los términos de este marco de seguridad, la distinción radica en el control de acceso a la ACI cuando ésta se trata como un objetivo (con fines de modificación). Esta distinción no es muy clara: existe una amplia variedad de alternativas posibles para la centralización o distribución del control que, dependiendo de la política de control de acceso, varía entre una política aplicada administrativamente hasta una política totalmente seleccionable por el usuario. Esto refleja los requisitos que impone el mundo real, puestos de manifiesto a través de los administradores de seguridad o sus agentes (por ejemplo, gestores de departamentos o jefes de equipo) frente a políticas de control de acceso con base individual.

Anexo F

Mecanismo para permitir el envío de ACI mediante un iniciador

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

Este esquema implica tres entidades:

- el iniciador A;
- la entidad C; y
- la entidad B.

El objetivo de este esquema es permitir que un iniciador inicie la transferencia de información directamente desde la entidad C a la entidad B sin implicar al iniciador A durante la fase de transferencia.

El iniciador accede en primer lugar a la entidad C y proporciona la ACI vinculada con el iniciador de forma que puede concederse el acceso. La entidad C proporciona entonces alguna información al iniciador que será utilizada ulteriormente por la entidad B para acceder a la entidad C. Se compone de dos partes:

- una referencia unívoca a la entidad C durante el periodo de validez de la referencia; y
- una clave criptográfica protegida utilizando un servicio confidencial entre la entidad C y el iniciador.

Para realizar un acceso sobre la entidad C, la entidad B necesita obtener del iniciador A la referencia y la clave criptográfica. Mientras la clave criptográfica viaja desde el iniciador a la entidad B, se protege mediante un servicio de confidencialidad.

La referencia y la clave criptográfica son finalmente empleadas por la entidad B para generar la ACI vinculada con la petición de acceso que se compone de la referencia y de un valor de verificación criptográfico calculado mediante la clave criptográfica.

La entidad C concede el acceso si la clave criptográfica utilizada para generar el valor de verificación criptográfico corresponde a uno asociado con la referencia.

Anexo G

Descripción esquemática del servicio de seguridad de control de acceso

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

<table>
<tr><td colspan="3" rowspan="4">Descripción del servicio de seguridad</td><td rowspan="3">Elemento</td><td colspan="3">Entidades: Iniciador, objetivo.</td></tr>
<tr><td colspan="3">Funciones: Función de imposición de control de acceso (AEF), función de decisión de control de acceso (ADF).</td></tr>
<tr><td colspan="3">Información: Información de control de acceso (ACI), información de decisión de control de acceso (ADI), información contextual, reglas de la política.</td></tr>
<tr><td colspan="4">Finalidad de las entidades: interpretar la información que permite a los iniciadores acceder a objetivos sólo tal como están autorizados.</td></tr>
<tr><td rowspan="5">FACILIDADES</td><td rowspan="3">Facilidades relacionadas con la gestión</td><td>Entidad</td><td colspan="4">Autoridad del dominio de seguridad (SDA)</td></tr>
<tr><td>Función</td><td colspan="4"></td></tr>
<tr><td colspan="5">– Instalar ACI
– Modificar ACI
– Revocar ACI
– Revocar ADI
– Listar ACI
– Desactivar componente
– Reactivar componente</td></tr>
<tr><td rowspan="2">Facilidades relacionadas con la operación</td><td>Entidad</td><td colspan="2">Iniciador</td><td>Objetivo</td><td></td></tr>
<tr><td>Función</td><td colspan="2"></td><td></td><td>ADF</td></tr>
<tr><td colspan="2">– Identificar autoridad distante
– Establecer una política de interacción segura
– Adquirir ACI
– Generar ACI
– Revocar ADI</td><td>– Adquirir ACI
– Revocar ADI</td><td colspan="2">– Adquirir ACI
– Verificar ACI y derivar ADI
– Obtener ACI contextual
– Decidir acceso</td></tr>
<tr><td rowspan="3">INFORMACIÓN</td><td>Elementos de datos gestionados por la SDA</td><td colspan="5">– Identificadores (SDA, iniciador, objetivo, política de interacción segura, grupos, roles.)
– Criterio de selección de la ACI
– Periodo de validez
– Marcación de sensibilidad
– Marcación de integridad</td></tr>
<tr><td>Información utilizada en las operaciones</td><td colspan="5">– ACI/ADI (de iniciador, vinculado con iniciador, de objetivo, vinculado con el objetivo, de petición de acceso, vinculado con la petición de acceso, de operando, vinculado con el operando, de intercambio, contextual, retenida.)
– Lista de control de acceso
– Capacidad
– Etiqueta
– Certificado de control de acceso
– Testigo de control de acceso</td></tr>
<tr><td>Información de control</td><td colspan="5">– Periodo de tiempo
– Estado del sistema
– Representación de la política de control de acceso
– Fortaleza de la autenticación
– Ruta de las comunicaciones</td></tr>
</table>