UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.509

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Corrigendum 1

(03/2000)

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

Directorio

Tecnología de la información – Interconexión de sistemas abiertos – El Directorio: Marco de autenticación

Corrigendum técnico 1

Recomendación UIT-T X.509 – Corrigendum 1

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	X.270–X.279
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	**X.500–X.599**
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600–X.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999

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

NORMA INTERNACIONAL 9594-8

RECOMENDACIÓN UIT-T X.509

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – EL DIRECTORIO: MARCO DE AUTENTICACIÓN

CORRIGENDUM TÉCNICO 1

Orígenes

El corrigendum 1 a la Recomendación UIT-T X.509 se aprobó el 31 de marzo de 2000. Su texto se publica también, en forma idéntica, como corrigendum técnico 1 a la Norma ISO/CEI 9594-8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

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

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

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – EL DIRECTORIO: MARCO DE AUTENTICACIÓN

CORRIGENDUM TÉCNICO 1

1) Resolución al informe de defectos 9594/200

Subcláusula 12.6.2

Añádase lo siguiente al final del párrafo que comienza con "Si esta extensión se indica como crítica mediante banderas"*:*

"Cuando se utilicen puntos de distribución para distribuir información CRL a todos los códigos de motivo de revocación y todos los certificados expedidos por una CA incluyan el **crlDistributionPoint** como una extensión crítica, no es necesario que la CA publique también una CRL completa del asiento de CA".

2) Resolución al informe de defectos 9594/201

Subcláusula 12.6.3.1

Trasládese la segunda frase del segundo párrafo "Si este campo está ausente …expedidor de CRL" *al primer párrafo inmediatamente antes de la frase* "Este campo se define como sigue:"

Añádase un punto y aparte después de la frase reubicada, de forma que "Este campo se define como sigue:" *sea un párrafo independiente inmediatamente antes de la notación ASN.1.*

3) Resolución al informe de defectos 9594/212

Subcláusula 12.7.6

Añádase lo siguiente a la subcláusula 12.7.6:

"g) **authorityKeyIdentifier** concuerda si el valor de este componente en el valor de atributo almacenado equivale al del valor presentado; no hay concordancia si el valor de atributo almacenado no contiene extensión de identificador de clave de autoridad o si no todos los componentes del valor presentado están presentes en el valor de atributo almacenado."

4) Resolución al informe de defectos 9594/213

Subcláusula 12.7.6 d)

Sustitúyase el texto de 12.7.6 d) por lo siguiente:

"d) **reasonFlags** concuerda si cualquiera de los bits que están fijados en el valor presentado están fijados también en los componentes **onlySomeReasons** de la extensión de punto de distribución expedidor

del valor de atributo almacenado; también concuerda si el valor de atributo almacenado no tiene ninguna **reasonFlags** en la extensión de punto de distribución expedidor, o si el valor de atributo almacenado no incluye ninguna extensión de punto de distribución expedidor;

NOTA – Aunque una CRL concuerde con un determinado valor de **reasonFlags**, la CRL puede no incluir notificaciones de revocación con ese código de motivo."

5) Resolución al informe de defectos 9594/218

Subcláusula 12.7.2 j)

Sustitúyase el texto de 12.7.6 j) por lo siguiente:

"j) **policy** concuerda si por lo menos un miembro de los **CertPolicySet** presentados aparece en la extensión de políticas de certificado en el valor de atributo almacenado; no hay concordancia si no hay extensión de políticas de certificado en el valor de atributo almacenado;"

6) Resolución al informe de defectos 9594/220

Subcláusula 11.2, Nota 3

En la nota 3, en la segunda frase sustitúyase "estará ausente" *por* "*podrá estar ausente*".

En la nota 3, al principio de la tercera frase, sustitúyase "Esto puede permitir" *por* "Si está ausente **version**, esto puede permitir".

En la nota 3, al principio de la cuarta frase, sustitúyase "Una implementación que soporta la versión 2 (o una versión superior) de las CRL puede ser capaz de" *por* "Una implementación que soporta la versión 2 (o una versión superior) de las CRL, puede también, en ausencia de **version**...".

7) Resolución al informe de defectos 9594/185

Cláusula 8

Añádase el texto siguiente inmediatamente después de la ASN.1 para **certificatePair***:*

"El atributo **cACertificate** de un asiento de directorio CA se utilizará para almacenar certificados autoexpedidos (si existen) y certificados expedidos a esa CA por las CA en el mismo dominio que dicha CA.

Los elementos **forward** del atributo **crossCertificatePair** de un asiento de directorio de CA se utilizará para almacenar todos los certificados salvo los autoexpedidos por dicha CA. De forma optativa, los elementos **reverse** del atributo **crossCertificatePair** de un asiento de directorio de CA pueden incluir un subconjunto de certificados expedidos por esta CA y otras CA. Cuando tanto los elementos **forward** como los **reverse** están presentes en un único valor de atributo, el nombre de expedidor en un certificado deberá concordar con el nombre de sujeto en el otro y viceversa, y la clave pública de sujeto en un certificado deberá ser capaz de verificar la firma digital en el otro certificado y viceversa.

Cuando está presente un elemento **reverse**, no es necesario almacenar en el mismo valor de atributo el valor del elemento directo y el valor del elemento inverso; en otras palabras, se pueden almacenar en un valor de atributo único o en dos valores de atributo.

En el caso de certificados v3, ninguno de los certificados CA anteriores incluirá una extensión **basicConstraints** con un valor **cA** fijado a **FALSO**.

La definición de dominio depende únicamente de la política local."

Asimismo, sustitúyase la figura 4 por la siguiente:

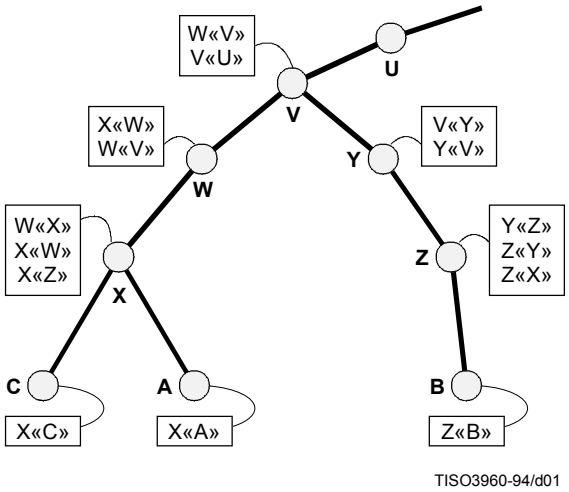

Figura 4 – Trayecto de certificación – Ejemplo teórico

8) Resolución al informe de defectos 9594/204

Subcláusula 12.6.3.1

En la primera frase después de la ASN.1, suprímase "no expirados".

Añádase lo siguiente como nueva segunda frase en el primer párrafo después de la ASN.1:

"Después de que un certificado aparezca en una CRL, se suprime de una CRL subsiguiente, cuando el certificado ha caducado".

9) Resolución al informe de defectos 9594/222

Añádase lo siguiente a la subcláusula 12.1:

"Política de certificados

El marco de autenticación contiene tres tipos de entidades: el usuario de certificado, la autoridad de certificación y el sujeto de certificado (o entidad final). Cada entidad funciona sometida a obligaciones con las otras dos entidades y, en contrapartida, disfruta de garantías limitadas ofertadas por ellos. Estas obligaciones y garantías se definen en una política de certificados. Una política de certificados es un documento (normalmente en lenguaje claro). Se puede referenciar mediante un único identificador, que puede estar definido en la extensión de políticas de certificados del certificado expedido por la autoridad de certificación, a la entidad final y a la que está ligado el usuario de certificados. Se puede expedir un certificado de conformidad con una o más de una política. Una autoridad de políticas realiza una definición de la política y asigna el identificador. El conjunto de políticas administradas por una autoridad de políticas se denomina un dominio de políticas. Todos los certificados se expiden de acuerdo con una política, incluso cuando la política no está registrada en ningún sitio, ni referenciada en el certificado. La presente Recomendación | Norma Internacional no prescribe el estilo ni el contenido de la política de certificados.

El usuario de certificado puede estar ligado a sus obligaciones en la política de certificados mediante el acto de importar una clave pública de autoridad y utilizando ésta como un vínculo de confianza, o vinculándose a un certificado que incluya el identificador de política asociado. La autoridad de certificación puede estar ligada a ***sus*** obligaciones mediante

la política por el hecho de expedir un certificado que incluya el identificador de política asociado. Además, la entidad final puede estar ligada a ***sus*** obligaciones en la política mediante el acto de solicitar y aceptar un certificado que incluya el identificador de política asociado y utilizando la clave privada correspondiente. Implementaciones que no utilicen la extensión de políticas de certificados lograrán la vinculación necesaria mediante otros medios.

El que una entidad declare sencillamente su conformidad a una política no satisface normalmente los requisitos de garantía de las demás entidades en el marco. Necesitan alguna razón para creer que las otras partes realizan una implementación fiable de la política. Sin embargo, si está establecido explícitamente en la política, los usuarios de certificado pueden aceptar las garantías de la autoridad de certificación de que sus entidades finales están de acuerdo en estar ligadas a sus obligaciones mediante la política, sin tener que confirmarlo directamente con ellas. Este aspecto de la política de certificados está fuera del ámbito de la presente Recomendación | Norma Internacional.

Una autoridad de certificación puede establecer limitaciones en la utilización de sus certificados para controlar el riesgo que asume al expedir certificados. Por ejemplo, puede restringir la comunidad de usuarios de certificado, los propósitos para los cuales pueden utilizar sus certificados y/o el tipo y cantidad de daños que puede asumir en el caso de un fallo por su parte, o aquellos de sus entidades finales. Estos asuntos deben definirse en la política de certificados.

Se puede incluir información adicional en la extensión de políticas de certificados en forma de calificadores de política para ayudar a las entidades afectadas a entender las disposiciones de la política.

Certificación cruzada

Una autoridad de certificación puede ser el sujeto de un certificado expedido por otra autoridad de certificación. En este caso, el certificado se denomina un certificado cruzado, la autoridad de certificación que es el sujeto del certificado se denomina la autoridad de certificación sujeto y la autoridad de certificación que expide el certificado cruzado la autoridad de certificación intermedia (véase la figura 1). Tanto el certificado cruzado como el certificado de la entidad final pueden contener una extensión de políticas de certificados.

Las garantías y obligaciones compartidas por una autoridad de certificación sujeto, por la autoridad de certificación intermedia y por el usuario de certificado se definen mediante la política de certificados identificada en el certificado cruzado, en cumplimento de lo cual la autoridad de certificación sujeto puede actuar como, o en nombre de, una entidad final. Además, las garantías y obligaciones compartidas por el sujeto de certificado, la autoridad de certificación sujeto y la autoridad de certificación intermedia se definen mediante la política de certificados identificada en un certificado de entidad final, según la cual una autoridad de certificación intermedia puede actuar como, o en nombre de, un usuario de certificado.

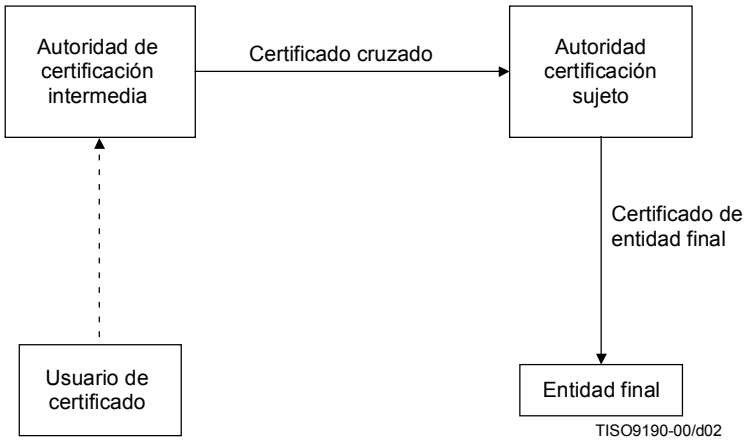

Figura 1 – Certificación cruzada

Un trayecto de certificación se considera válido mediante el conjunto de políticas que son comunes a todos los certificados en el trayecto.

Una autoridad de certificación intermedia puede, a su vez, ser el sujeto de un certificado expedido por otra autoridad de certificación, creando así trayectos de certificación de longitudes superiores a dos certificados. Además, puesto que la confianza se degrada al crecer los trayectos de certificación en longitud, se precisan controles para asegurar que los certificados de entidad final con un nivel de confianza asociado inaceptablemente bajo serán rechazados por el usuario de certificado. Esto forma parte de la función del procedimiento de procesamiento de certificación.

Además de la situación descrita anteriormente, deben considerarse dos casos especiales:

1) la autoridad de certificación no utiliza la extensión de certificados para transmitir sus requisitos de política a los usuarios de certificado; y

2) el usuario de certificado o la autoridad de certificación intermedia delega la tarea de controlar la política a la siguiente autoridad en el trayecto.

En el primer caso, el certificado no contendrá ninguna extensión de política de certificados. Por ello, el conjunto de políticas que validan el trayecto será nulo. Aunque, a pesar de todo, el trayecto puede ser válido. Los usuarios de certificado tendrán que seguir asegurándose de que están utilizado el certificado de conformidad con las políticas de las autoridades en el trayecto.

En el segundo caso, el usuario de certificado o la autoridad de certificación intermedia incluirán el valor especial *cualquier política* en el *conjunto de políticas inicial* o un certificado cruzado. Cuando un certificado incluya el valor especial *cualquier política*, no podrá incluir ningún otro identificador de política de certificados. El identificador *cualquier política* no tendrá ningún calificador de política asociado.

El usuario de certificado puede asegurar que todas sus obligaciones se envían de conformidad con la norma fijando el indicador *política explícita inicial*. De esta forma, sólo se aceptan en el trayecto las autoridades que utilizan la extensión de políticas de certificados normalizada como forma de lograr la vinculación y los usuarios de certificado no tienen obligaciones adicionales. Puesto que las autoridades también asumen obligaciones cuando actúan como, o en nombre de, un usuario de certificación, pueden asegurar que todas sus obligaciones se envían de conformidad con la presente Recomendación | Norma Internacional incluyendo **requireExplicitPolicy** en el certificado cruzado.

Correspondencia de políticas

Algunos trayectos de certificación pueden cruzar fronteras entre dominios de políticas. Las garantías y obligaciones según la cuales se expide el certificado cruzado pueden ser materialmente equivalentes a alguna o a todas las garantías y obligaciones según las cuales la autoridad de certificación sujeto expide certificados a entidades finales, incluso cuando las autoridades de política bajo las que operan las dos autoridades de certificación puedan haber seleccionado identificadores únicos diferentes para dichas políticas materialmente equivalentes. En este caso, la autoridad de certificación intermedia puede incluir una extensión de correspondencias de políticas en el certificado cruzado. En la extensión de correspondencias de políticas, la autoridad de certificación intermedia asegura al usuario de certificado que seguirá disfrutando de las garantías habituales y que debe seguir cumpliendo sus obligaciones habituales, incluso cuando entidades subsiguientes en el trayecto de certificación operan en un dominio de políticas diferente. La autoridad de certificación intermedia incluirá una o más correspondencias para cada una de las políticas de un subconjunto bajo las que expidió el certificado cruzado, y no deberá incluir correspondencias para ninguna otra política. Si una o más de las políticas de certificados según las cuales opera la autoridad de certificación sujeto es idéntica a aquellas según las cuales opera la autoridad de certificación intermedia (es decir, tiene el mismo identificador único), entonces estos identificadores serán excluidos de la extensión de correspondencia de políticas, pero se incluirán en la extensión de políticas de certificados.

La correspondencia de políticas convierte todos los identificadores de políticas en certificados a lo largo del trayecto de certificación hasta el identificador de la política equivalente, como lo reconoce el usuario de certificado.

Las políticas no se corresponderán con el valor especial *cualquier política*.

Los usuarios de certificado pueden determinar que no se pueden vincular a certificados expedidos en un dominio de política distinto de su propio dominio, incluso cuando una autoridad de certificación intermedia fiable pueda determinar su política como materialmente equivalente a su propia política. Puede hacer esto fijando la entrada de *inhibición de correspondencia de política inicial* en el procedimiento de validación del trayecto. Además, una autoridad de certificación intermedia puede tomar una determinación similar en nombre de sus usuarios de certificado. Para asegurar que los usuarios de certificado cumplen correctamente este requisito, puede poner **inhibitPolicyMapping** en una extensión de constricciones de política.

Procesamiento de trayecto de certificación

El usuario de certificado debe elegir entre dos estrategias:

1) puede requerir que el trayecto de certificación sea válido mediante por lo menos una de un conjunto de políticas predeterminado por el usuario; o

2) puede solicitar al módulo de validación de trayecto que indique el conjunto de políticas para el cual el trayecto de certificación es válido.

La primera estrategia puede ser la más adecuada cuando el usuario de certificado conoce, a priori, el conjunto de políticas aceptables para el uso que se pretende.

La segunda estrategia puede ser la más adecuada cuando el usuario de certificado desconoce, a priori, el conjunto de políticas aceptables para el uso que se pretende.

En primer lugar, el procedimiento de validación del trayecto de certificación indicará que el trayecto sólo es válido si es válido bajo una o mas de las políticas especificadas en el *conjunto de políticas inicial*, y devolverá el subconjunto del *conjunto de políticas inicial* para el cual el trayecto es válido. En segundo lugar, el procedimiento de validación del trayecto de certificación puede indicar que el trayecto no es válido mediante el *conjunto de políticas inicial*, pero si es válido mediante un conjunto diferente: el *authorities-constrained-policy-set*. Entonces, el usuario de certificado tiene que determinar si la utilización pretendida del certificado está de acuerdo con una o más de las políticas de certificados para las que el trayecto es válido. Al incluir el *conjunto de políticas inicial* en *cualquier política*, el usuario de certificado puede lograr que le procedimiento devuelva un resultado válido si el trayecto es válido mediante cualquier política (sin especificar).

Certificados autoexpedidos

Existen tres circunstancias bajo las cuales una autoridad de certificación puede expedir un certificado a sí mismo:

1) como forma adecuada de codificar su clave pública para su comunicación y almacenamiento por sus usuarios de certificado;

2) para certificar utilizaciones clave diferentes de la firma de certificado y de CRL (como sello temporal); y

3) para sustituir sus propios certificados caducados.

Estos tipos de certificado se denominan certificados autoexpedidos y se pueden reconocer mediante el hecho de que los nombres de expedidor y de sujeto que constan son idénticos. Para fines de validación del trayecto, los certificados autoexpedidos del primer tipo se verifican con la clave pública contenida en ellos, y si se encuentran en el trayecto deberán ignorarse.

Los certificados autoexpedidos del segundo tipo sólo pueden aparecer como certificados finales en el trayecto y deben ser procesados como certificados finales.

Los certificados autoexpedidos del tercer tipo (también conocidos como certificados intermedios autoexpedidos) puede aparecer como certificados intermedios en el trayecto.

En la práctica, cuando se sustituye una clave que se encuentra a punto de caducidad, una autoridad de certificación solicitará la expedición de cualquier certificado cruzado ligado que precise para su clave pública de sustitución antes de utilizar la clave. No obstante, si se encuentran certificados autoexpedidos en el trayecto, se procesarán como certificados intermedios, con la siguiente excepción: no contribuyen a la longitud del trayecto para fines de procesamiento del componente **pathLenConstraint** de la extensión **basicContraints** y de los valores *salto de certificados* asociados con los indicadores *inhibición de correspondencias de políticas pendiente* y *política explícita pendiente*".

En la subcláusula 12.2.2.6, añádase lo siguiente después de la segunda frase del primer párrafo:

"La presencia de esta extensión en un certificado de la entidad de extremo indica las políticas de certificados con respecto a las cuales este certificado es válido. La presencia de esta extensión en un certificado expedido por una CA a otra CA indica las políticas de certificados con respecto a las cuales este certificado puede utilizarse con el fin de validar trayectos de certificación."

Añádase el siguiente texto en la subcláusula 12.2.2.6, después de la primera frase del primer párrafo:

"La lista de políticas de certificados se utiliza para determinar la validez de un trayecto de certificación, según se describe en 12.4.3. Los cualificadores opcionales no se utilizan en el procedimiento de tramitación del trayecto de certificación, pero se proporcionan los correspondientes cualificadores como resultado de dicho proceso para la aplicación que utiliza el certificado con el fin de determinar si un trayecto válido se adecua a la transacción de que se trate."

En la subcláusula 12.2.2.7, reemplácese la frase "Esta extensión es siempre no crítica"*, por lo siguiente:*

"Esta extensión puede, si así lo desea el expedidor del certificado, ser crítica o no crítica. Se recomienda que sea crítica puesto que de otro modo puede ocurrir que el usuario del certificado no interprete correctamente la estipulación de la CA expedidora."

Añádase la siguiente nueva subcláusula 12.4.2.4:

"12.4.2.4 Inhibición de cualquier política

Este campo especifica una constricción que indica que cualquier política no se considera una correspondencia explícita para otras políticas de certificados en lo que concierne a la parte restante del trayecto de certificación.

```
inhibitAnyPolicy ::= EXTENSION {
        SYNTAX SkipCerts
IDENTIFIED BY {id-ce-inhibitAnyPolicy }}
```

Esta extensión puede, si así lo desea el expedidor del certificado, ser crítica o no crítica. Se recomienda que sea crítica, puesto que de otro modo puede ocurrir que el usuario del certificado no interprete correctamente la estipulación de la CA expedidora."

Añádase lo siguiente en la lista de OID en el módulo certificateExtensions consignado en el anexo A:

"**id-ce-inhibitAnyPolicy OBJECT IDENTIFIER ::= {id-ce 54}**"

Sustitúyase la subcláusula 12.4.3 con lo siguiente:

"12.4.3 Procedimiento de procesamiento del trayecto de certificación

El procesamiento del trayecto de certificación se realiza en un sistema que tiene que utilizar la clave pública de una entidad final distante, por ejemplo, un sistema que está verificando una firma digital generada por una entidad distante. Las políticas de certificado, las constricciones básicas, las constricciones de nombre y las extensiones de constricciones de política han sido diseñadas para facilitar la implementación automática e independiente de la lógica del procesamiento del trayecto de certificación.

A continuación figura un esbozo de un procedimiento para validar trayectos de certificación. Una implementación será equivalente funcionalmente al comportamiento externo resultante de este procedimiento. El algoritmo utilizado por una implementación determinada para derivar las salidas correctas a partir de las entradas dadas no está normalizado.

Las entradas al procedimiento de procesamiento de trayecto de certificación son:

a) un conjunto de certificados que comprenden un trayecto de certificación;

b) un valor de clave pública o identificador público de confianza (si la clave está almacenada internamente en el módulo de procesamiento del trayecto de certificación), que se ha de utilizar para verificar el primer certificado en el trayecto de certificación;

c) un *conjunto de políticas inicial* que comprende uno o más identificadores de políticas de certificado, que indican que cualquiera de estas políticas sería aceptable al usuario del certificado para los fines de procesamiento del trayecto de certificación; esta entrada puede tomar también el valor especial *cualquier política*;

d) un valor de indicador de *política explícita inicial*, que indica si un identificador de política aceptable tiene que aparecer explícitamente en el campo de extensión de políticas de certificado de todos los certificados en el trayecto;

e) un valor de indicador de *inhibición de correspondencia de políticas inicial*, que indica si la correspondencia de políticas está prohibida en el trayecto de certificación;

f) un valor de indicador de *inhibición de políticas inicial*, que indica si el valor especial **anyPolicy**, si està presente en una extensión de políticas de certificado, se considera una concordancia para cualquier valor de políticas de certificado en un conjunto constreñido.

g) la fecha/hora actual (si no está disponible internamente en el módulo de procesamiento de trayecto de certificación).

Los valores indicados en c), d), e) y f) dependerán de los requisitos de política de la combinación de aplicaciones de usuario que tiene que utilizar la clave pública de la entidad final certificada.

Obsérvese que, por el hecho de que estas son entradas individuales al proceso de validación del trayecto, un usuario de certificado puede limitar la confianza que deposita en una determinada clave pública de confianza, a un determinado conjunto de políticas de certificado. Esto puede obtenerse asegurando que una determinada clave pública solo forma parte de la entrada al proceso cuando la entrada *conjunto de políticas inicial* incluye políticas para las cuales el usuario del certificado confía en esa clave pública. Dado que otra entrada al proceso es el propio trayecto de certificación, este control podría ejercerse para cada una de las transacciones.

Las salidas del procedimiento son:

a) una indicación de éxito o fracaso de la validación del trayecto de certificación;

b) si la validación fracasa, un código de diagnóstico que indica el motivo del fallo;

c) el conjunto de políticas de autoridades constreñidas y sus calificadores asociados según los cuales es válido el trayecto de certificación, o el valor especial *cualquier política*;

d) el conjunto de políticas de usuario constreñido, formado a partir de la intersección del *conjunto de políticas constreñidas de la autoridad* y del *conjunto de política inicial*;

e) *el indicador de política explícita*, que indica si el usuario de certificado o una autoridad en el trayecto necesita que se identifique una política aceptable para cualquier certificado en el trayecto; y

f) detalles de cualquier correspondencia de políticas que aparezcan en el procesamiento del trayecto de certificación.

NOTA – Si la validación tiene éxito, el sistema que utiliza certificado puede elegir no utilizar el certificado como resultado de los valores de calificadores de política u otra información de certificado.

El procedimiento utiliza el siguiente conjunto de variables de estado:

a) *conjunto de políticas constreñidas de la autoridad:* Un cuadro de identificadores y calificadores de política de los certificados del trayecto de certificación (las filas representan políticas, sus calificadores y el historial de correspondencias, y las columnas representan certificados en el trayecto de certificación);

b) *subárboles permitidos*: Un conjunto de especificaciones de subarbol que define subárboles dentro de los cuales deben aparecer todos los nombres de sujetos en certificados subsiguientes en el trayecto de certificación o pueden tomar el valor especial *ilimitado*;

c) *subárboles excluidos* : Un conjunto (posiblemente vacío) de especificaciones de subarbol (cada una de las cuales comprende un nombre de base de subarbol e indicadores de nivel máximo y mínimo) que definen subárboles dentro de los cuales no puede aparecer ningún nombre de sujeto en un certificado subsiguiente en el trayecto de certificación;

d) *indicador de política explícito*: Indica si una política aceptable tiene que ser explícitamente identificada en cada certificado en el trayecto;

e) *profundidad del trayecto*: Número entero siguiente al número de certificados en el trayecto de certificación para los que se ha completado el procesamiento;

f) *indicador de inhibición de correspondencia de políticas*: Indica si se inhibe la correspondencia de políticas;

g) *indicador de inhibición de cualquier política*: Indica si el valor especial **anyPolicy** se considera una concordancia para cualquier política de certificado específica.

h) *constricciones pendientes*: Detalla las constricciones de *política explícita*, *inhibición de correspondencia de políticas* y/o *inhibición de cualquier política* que han sido estipuladas pero que no han sido aún aplicadas. Hay dos indicadores de un bit denominados *política explícita pendiente, inhibición de correspondencia de políticas pendiente e inhibición de cualquier política pendiente*; para cada uno de estos indicadores hay también, un entero denominado *salto de certificados* que representa el número de certificados que hay que saltar aún antes de que se haga efectiva la constricción.

El procedimiento conlleva un paso de inicialización, seguido por una serie de pasos de procesamiento de certificados. El paso de inicialización comprende:

a) escribir *cualquier política* en las columnas cero y primera de la fila cero del cuadro *conjunto de políticas constreñidas de la autoridad*;

b) inicializar la variable *subárboles permitidos* a *ilimitados*;

c) inicializar la variable *subárboles excluidos* a un conjunto vacío;

d) inicializar el *indicador de política explícita* al valor *política explícita inicial*;

e) inicializar *profundidad de trayecto* a uno;

f) inicializar el *indicador de inhibición de correspondencia de políticas* al valor *inhibición política de correspondencia de políticas inicial*;

g) inicializar los dos indicadores *constricciones pendientes* a no fijados.

Cada certificado se procesa en turno, comenzando con el certificado firmado que utilizan clave pública de entrada. Se considera que el último certificado es el certificado final; cualquiera otros certificados que se consideran certificados intermedios.

Se aplican las siguientes comprobaciones a un certificado:

a) comprobar que la firma verifica que las fechas son válidas, que los nombres del sujeto del certificado y del expedidor del certificado encadenan correctamente y que el certificado no ha sido revocado;

b) para un certificado intermedio, si está presente en el certificado el campo de extensión de constricciones básico, comprobar que el componente **cA** está presente y está puesto a verdadero. Si el componente **pathLenConstraint** está presente, comprobar que el trayecto de certificación actual no viola esa constricción (ignorando certificados autoexpedidos intermedios);

c) si no está presente la extensión de políticas de certificados, fijar a cero el *conjunto de políticas constreñidas de la autoridad* suprimiendo todas las filas del cuadro *conjunto de políticas constreñidas de las autoridades*;

d) si la extensión de políticas del certificado está presente, para cada política, *P*, en otra extensión distinta a **anyPolicy**, adjuntar los calificadores de políticas asociados con *P* a cada fila en el cuadro *conjunto de política constreñidas de la autoridad* cuya entrada a la columna [*profundidad de trayecto*] limita el valor *P*. Si ninguna fila en el cuadro *conjunto de políticas constreñidas de la autoridad* contiene *P* en sus entradas a las columnas [*profundidad de trayecto*] pero el valor en *conjunto de políticas constreñidas de la autoridad* [0, *profundidad de trayecto*] es cualquier política, añadir una nueva fila al cuadro duplicando la fila de orden cero y transcribir el identificador de política *P* junto con sus calificadores en la entrada a la columna [*profundidad de trayecto*] de la nueva fila;

e) si la extensión de políticas del certificado está presente y no incluye el valor **anyPolicy** o si se fija el *indicador de inhibición de cualquier política*, suprimir cualquier fila para la cual la entrada a la columna [*profundidad de trayecto*] contiene el valor *cualquier política* junto con cualquier fila para la cual la entrada a la columna [*profundidad de trayecto*] no contiene une de los valores en la extensión de políticas del certificado;

f) si la extensión de políticas del certificado está presente e incluye el valor **anyPolicy** y no se fija el *indicador de inhibición de cualquier polica*, añadir los calificadores de políticas asociados con **anyPolicy** a cada fila en el cuadro *conjunto de políticas constreñidas de la autoridad* cuya entrada a la columna [*profundidad de trayecto*] contiene el valor *cualquier política* o contiene un valor que no aparece en la extensión de políticas del certificado;

g) si el certificado no es un certificado autoexpedido intermedio, comprobar que el nombre de sujeto está dentro del espacio de nombre dado por el valor de *subárboles permitidos* y no se encuentra dentro del espacio de nombre dado por el valor *subárboles excluidos*.

Para un certificado intermedio, se realizan las siguientes acciones de grabación de constricción, para establecer correctamente las variables de estado para el procesamiento del siguiente certificado:

a) si la extensión **nameConstraints** con un componente **permittedSubtrees** está presente en el certificado, fijar la variable de estado *subárboles permitidos* a la intersección de su valor anterior y al valor indicado en la extensión del certificado;

b) si la extensión **nameConstraints** con un componente **excludedSubtrees** está presente en el certificado, fijar la variable de estado *subárboles excluidos* a la unión de su valor previo y del valor indicado en la extensión del certificado;

c) si está fijado el *indicador de inhibición de correspondencia de políticas*:

   – procesar cualquier extensión de correspondencias de políticas situando, para cada correspondencia identificada en la extensión, todas las filas del cuadro *conjunto de políticas constreñidas de las autoridades* cuyos valores de la columna [*profundidad de trayecto*] es igual al valor de política de dominio de expedidor en la extensión y borrar la fila;

d) si el *indicador de inhibición de correspondencia de políticas* no está fijado:

- procesar cualquier extensión de correspondencias de políticas situando, para cada correspondencia identificada en la extensión, todas las filas del cuadro *conjunto de políticas constreñidas de las autoridades* cuyo valor de la columna [*profundidad de trayecto*] es igual al valor de política de dominio de expedidor en la extensión, y escribir el valor de política de dominio de sujeto proveniente de la extensión en la columna [*profundidad de trayecto* + 1] de la misma fila. Si la extensión corresponde a una política de dominio de expedidor con más de una política de dominio de sujeto, entonces la fila afectada deberá copiarse y se deberá añadir una nueva entrada a cada fila. Si el valor del *conjunto de políticas constreñidas de las autoridades* [0, *profundidad de trayecto*] es *cualquier política*, escribir entonces cada identificador de política de dominio de expedidor proveniente de la extensión correspondencias de políticas en la columna [*profundidad de trayecto*], duplicando filas cuando sea necesario y manteniendo calificadores si existen, y escribir el valor de la política de dominio de sujeto proveniente de la extensión en la columna [*profundidad de trayecto* +1] de la misma fila;
- si el indicador *inhibición de correspondencia de políticas pendiente* está fijado y el certificado no es autoexpedido, disminuir el correspondiente valor *salto de certificados* y, si este valor llega a cero, fijar el indicador *inhibición de correspondencias de políticas*;
- si la constricción **inhibitPolicyMapping** está presente en el certificado hacer los siguiente: para un valor de **SkipCerts** de 0, fijar el *indicador inhibición de correspondencia de políticas*. Para cualquier otro valor **SkipCerts**, fijar el indicador *inhibición de correspondencia de políticas pendiente*, y fijar el correspondiente valor *salto de certificados* al valor de **SkipCerts** o al valor anterior de *salto de certificados*, el que sea menor (si el indicador *inhibición de correspondencia de políticas pendiente* estaba ya fijado);

e) para cualquier fila no modificada en ninguno de los pasos c) o d), anteriores (y para cualquier fila en el caso de que no esté presente una extensión de correspondencia de certificado), escribir el identificador de política de la columna [*profundidad de trayecto*] en la columna [*profundidad de trayecto* +1] de la fila;

f) si no se fija el indicator de inhibición de cualquier política:

- si el indicador de inhibición de cualquier política pendiente está fijado y el certificado no es autoexpedido, disminuir el valor de salto de certificados correspondiente y, si este valor es cero, fijar el indicador de inhibición de cualquier política;
- si la constricción **inhibitAnyPolicy** está presente en el certificado, hacer lo siguiente: para un valor **SkipCerts** de o, fijar el indicador de inhibición de cualquier política. Para los demás valores **SkipCerts**, fijar el indicador de inhibición de cualquier política pendiente y fijar los correspondientes valores salto de certificados al valor **SkipCerts** o al valor anterior de salto de certificados, el que sea menor (si el indicador de inhibición de cualquier política pendiente ya estaba fijado);

g) incrementar profundidad de trayecto.

Para todos los certificados, se realizan entonces las actuaciones siguientes:

a) si el *indicador de políticas explícito* no está fijado:

- si está fijado el *indicador de políticas explícito pendiente* y el certificado no es un certificado intermedio autoexpedido, disminuir el valor correspondiente *salto de certificado* y, si este valor llega a cero, fijar el *indicador de política explícita*;
- si la constricción **requireExplicitPolicy** está presente en el certificado, hacer lo siguiente: para un valor **SkipCerts** de 0, fijar el *indicador de política explícita*; para cualquier otro valor **SkipCerts**, fijar el indicador política explícita pendiente y fijar los correspondientes valores salto de certificados al valor **SkipCerts** o al valor anterior de *salto de certificados*, el que sea menor (si el indicador *inhibición de cualquier política pendiente* ya estaba fijado);
- si el componente **requireExplicitPolicy** y el trayecto de certificación incluye un certificado expedido por una CA designada, es necesario que todos los certificados en el trayecto contengan en la extensión de políticas de certificados un identificador aceptable de políticas. Un identificador aceptable de políticas es un identificador de la política de certificados requerida por el usuario del trayecto de certificación, el identificador de una política que haya sido declarada equivalente, mediante la correspondencia de políticas, o *cualquier política*. La CA designada es la CA expedidora del certificado que contiene esta extensión (si el valor de **requireExplicitPolicy** es 0) o una CA objeto de un certificado ulterior en el trayecto de certificación (según se indique mediante un valor no nulo).

Para el certificado final, se realizarán las siguientes actuaciones:

a) si el *indicador de política explícita* está fijado, comprobar que el cuadro *conjunto de políticas constreñidas de la autoridad* no está vacío. Si cualquiera de estas dos comprobaciones fracasa, se deberá terminar el procediminento, devolviendo una indicación de fallo, un código de motivo adecuado, un *indicador de política explícita* y valores nulos en el *conjunto de políticas constreñidas del usuario* y el cuadro *conjunto de políticas constreñidas de la autoridad*.

Si ninguna de las mencionadas comprobaciones fracasa en el certificado final, se calculará el *conjunto de políticas constreñidas del usuario* formando la intersección del *conjunto de políticas constreñidas de la autoridad y* el *conjunto de políticas* inicial. Si el *conjunto de políticas constreñidas de la autoridad* [0, *profundidad de trayecto*] es *cualquier política*, el *conjunto de políticas constreñidas de la autoridad* es *cualquier política*. De lo contrario, el c*onjunto de políticas constreñidas de la autoridad* es, para cada fila en el cuadro, el valor en la célula situada más a la izquierda que no contiene el identificador *cualquier política*. Después de esto, se termina el procedimiento, y se devuelve una indicación de éxito junto con el *indicador de política explícita*, el cuadro *conjunto de políticas constreñidas de la autoridad* y el *conjunto de políticas constreñidas del usuario*. Si la intersección del *conjunto de políticas constreñidas de la autoridad* y el *conjunto de polítcas constreñidas del usuario* es nulo, el trayecto es válido en virtud de una o más políticas constreñidas de la autoridad pero ninguno es aceptable para el usuario."

SERIES DE RECOMENDACIONES DEL UIT-T

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

Ginebra, 2000