Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.509

Corrigendum 1

(01/2007)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Directorio

Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos

Corrigendum técnico 1

Recomendación UIT-T X.509 (2005) – Corrigendum técnico 1

UIT-T

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

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.369
Redes basadas en el protocolo Internet	X.370–X.379
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.889
Aplicaciones genéricas de la notación de sintaxis abstracta uno	X.890–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LAS TELECOMUNICACIONES	X.1000–

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

NORMA INTERNACIONAL ISO/CEI 9594-8
RECOMENDACIÓN UIT-T X.509

Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos

Corrigendum técnico 1

Orígenes

El corrigendum 1 a la Recomendación UIT-T X.509 (2005) fue aprobado el 13 de enero de 2007 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8. Se publica también un texto idéntico como corrigendum técnico 1 a la Norma Internacional 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 Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

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

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

NOTA

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

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

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 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 en la dirección http://www.itu.int/ITU-T/ipr/.

© UIT 2007

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Página

NORMA INTERNACIONAL
RECOMENDACIÓN UIT-T

Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos

Corrigendum técnico 1

(Trata las resoluciones tomadas con relación a los informes de defectos 310, 311 y 314)

1) Corrección de los defectos notificados en el informe de defectos 310

Sustitúyase la nota 4 de 7.3 por el siguiente texto:

Cuando una implementación que procesa una CRL encuentra el número de serie del certificado de interés en un asiento CRL pero no reconoce una extensión crítica en el campo **crlEntryExtensions** de ese asiento CRL, no se puede utilizar esa CRL para determinar el estado del certificado. Cuando una implementación no reconoce una extensión crítica en el campo **crlExtensions** no se puede utilizar esa CRL para determinar el estado del certificado, independientemente de si aparece o no en esa CRL el número de serie del certificado de que se trate.

NOTA 4 – En estos casos la política local puede indicar acciones adicionales y/o más estrictas que las señaladas en esta Especificación, tales como buscar información del estado de revocación en otras fuentes.

Los certificados para los cuales no se puede determinar el estado de revocación no se deberían considerar cerificados válidos.

2) Corrección de los defectos notificados en el informe de defectos 311

a) Sustitúyase la nota 5 de 7.3 por el siguiente texto:

Si una extensión afecta al tratamiento de la lista (por ejemplo, es preciso revisar múltiples CRL para examinar la lista completa de certificados revocados o un asiento puede representar a una gama de certificados), entonces se debe indicar como crítica en el campo **crlExtensions** esa extensión o una extensión relacionada. Por lo tanto, una extensión crítica en el campo **crlEntryExtensions** de un asiento debe afectar únicamente al certificado especificado en ese asiento, a menos de que exista alguna extensión crítica en el campo **crlExtensions** que indique un tratamiento especial para ella. El único ejemplo de esta situación que se define en esta Especificación es la extensión de asiento CRL **certificateIssuer** y la extensión CRL relacionada **issuingDistributionPoint** cuando la **indirectCRL** booleana de esa extensión se fija a **VERDADERO**.

b) En 8.6.2.2, sustitúyase el primer párrafo después del ASN.1 por:

El componente **distributionPoint** contiene el nombre del punto de distribución en una o varias formas de nombre. Si **onlyContainsUserPublicKeyCerts** es **VERDADERO**, la CRL sólo contiene revocaciones para certificados de clave pública de entidad extrema. Si **onlyContainsCACerts** es **VERDADERO**, la CRL sólo contiene revocaciones para certificados de CA. Si **onlyContainsUserPublicKeyCerts** y **onlyContainsCACerts** son ambos falsos, la CRL contiene revocaciones tanto para certificados de clave pública de entidad extrema como certificados de CA. Una CRL no debe contener esta extensión en la **onlyContainsUserPublicKeyCerts** y **onlyContainsCACerts** estén ambos fijados a **VERDADERO**. Si **onlySomeReasons** está presente, la CRL sólo contiene revocaciones de certificados para el motivo o motivos identificados, de lo contrario la CRL tendrá revocaciones para todos los motivos. Si **indirectCRL** es **VERDADERO**, la CRL puede contener notificaciones de revocación para certificados de clave pública expedidos por autoridades que tienen un nombre diferente al nombre del expedidor de la CRL. La autoridad responsable de cada asiento es la indicada por la extensión de asiento CRL **certificateIssuer** en ese asiento o es conforme a las reglas por defecto descritas en 8.6.2.3. En consecuencia, un certificado que utilice un sistema que sea capaz de procesar una CRL en la que **indirectCRL** se fija a **VERDADERO**, también tiene que ser capaz de procesar la extensión de asiento CRL **certificateIssuer**. En este tipo de CRL, es responsabilidad del expedidor de la CRL garantizar que la CRL está completa en el sentido de que contiene todos los asientos de revocación, coherente con los indicadores **onlyContainsUserPublicKeyCerts**, **onlyContainsCACerts** y **onlySomeReasons** de todas las autoridades que identifican a este expedidor de CRL en sus certificados de clave pública.

3) Corrección de los defectos notificados en el informe de defectos 314

a) Sustitúyase el texto de 8.4.2.2 por lo siguiente:

8.4.2.2 Extensión de constricciones de nombre

Este campo, que se utilizará únicamente en un certificado de CA, indica una o varias formas de nombre que tienen limitaciones sobre sus espacios de nombre, dentro de los cuales deberán estar ubicados todos los nombres de sujeto en la misma forma de nombre en certificados subsiguientes en un trayecto de certificación. Si esta extensión está ausente, no se establecen constricciones en ninguna forma de nombre. Si esta extensión está presente pero una forma de nombre no está incluida en la extensión, entonces no se imponen constricciones en esa forma de nombre.

NOTA 1 – Puesto que puede existir un conjunto desvinculado de formas de nombre **registeredID**, no es posible limitar todas las formas de nombre posibles de los nombres de sujeto con esta extensión.

Este campo se define como sigue:

```
nameConstraints EXTENSION ::= {
        SYNTAX              NameConstraintsSyntax
        IDENTIFIED BY id-ce-nameConstraints }

NameConstraintsSyntax ::= SEQUENCE {
        permittedSubtrees       [0]     GeneralSubtrees OPTIONAL,
        excludedSubtrees        [1]     GeneralSubtrees OPTIONAL }
(ALL EXCEPT ({ -- none; at least one component shall be present -- }))

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
        base                            GeneralName,
        minimum                 [0]     BaseDistance DEFAULT 0,
        maximum                 [1]     BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)
```

Por lo menos un **permittedSubtrees** y **excludedSubtrees** deben estar presentes.

Si está presente, el componente **permittedSubtrees** especifica uno o más subárboles, para una o más formas de nombre, en los que deben estar contenidos los nombres de sujeto en certificados aceptables. Si está presente, el componente **excludedSubtrees** especifica uno o más subárboles para una o más formas de nombre que no deben incluir nombres de sujeto en certificados aceptables. Los nombres de sujeto que se comparan con subárboles especificados incluyen los presentes tanto en el campo **subject** como en la extensión **subjectAltNames** de un certificado. Cada subárbol se define mediante el nombre de la raíz del subárbol, el componente **base** y, facultativamente, dentro de dicho subárbol, mediante una zona que está vinculada por niveles superiores y/o inferiores.

El campo **minimum** especifica el límite superior de la zona dentro del subárbol. Ningún nombre cuyo componente de nombre final está por encima del nivel especificado está contenido en la zona. Un valor de **minimum** igual a cero (el valor por defecto) corresponde a la base, es decir, al nodo superior del subárbol. Por ejemplo, si **minimum** está puesto a uno, el subárbol de denominación no incluye el nodo de base pero sí incluye nodos subordinados.

El campo **maximum** especifica el límite inferior de la zona dentro del subárbol. Los nombres cuyo último componente está por debajo del nivel especificado no están contenidos en la zona. Un valor de **maximum** de cero corresponde a la base, es decir, a la parte superior del subárbol. Un componente **maximum** ausente indica que no se debe imponer un límite inferior en la zona dentro del subárbol. Por ejemplo, si **maximum** está puesto a uno, el subárbol de denominación excluye todos los nodos, excepto la base del subárbol y sus subordinados inmediatos.

El conjunto de todos los **permittedSubtrees** y **excludedSubtrees** para una forma de nombre constituye el espacio de nombre constreñido para la forma de nombre. Todos los nombres de sujeto, en certificados expedidos por la CA de sujeto y por CA subsiguientes en un trayecto de certificación, que son de una forma de nombre constreñida, se deben encontrar en el espacio de nombre constreñido para que el certificado sea aceptable.

permittedSubtrees, si está presente**,** especifica los subárboles en los que deben encontrarse todos los nombres de sujeto que pertenecen a una forma de nombre constreñida para que el certificado sea aceptable. Si **excludedSubtrees** está presente, es inaceptable cualquier certificado expedido por una CA de sujeto o CA subsiguientes en el trayecto de certificación que tenga un nombre de sujeto dentro de esos subárboles. Si tanto **permittedSubtrees** como **excludedSubtrees** están presentes para una forma de nombre y los espacios de nombre se solapan, la declaración de exclusión tiene preferencia.

Si ninguna de las formas de nombre del nombre sujeto en el certificado está limitada por esta extensión, el certificado es aceptable.

En algunos casos, puede ser necesario expedir más de un certificado para satisfacer los requisitos de las constricciones de nombres. El anexo G muestra dos situaciones de este tipo. Por ejemplo, si se definen constricciones de nombres para múltiples formas de nombre, pero un certificado tiene que cumplir las constricciones de nombre solo para una de las formas de nombre (O lógico en las constricciones), se deberían expedir múltiples certificados, cada uno de ellos constriñendo una única forma de nombre.

De las formas de nombre disponibles en el tipo **GeneralName** sólo se pueden utilizar en este campo las formas de nombre que tienen una estructura jerárquica bien definida.

La forma de nombre **directoryName** satisface este requisito cuando al usar esta forma de nombre un subárbol de denominación corresponde a un subárbol DIT. Un **certificado** se considera subordinado a **base** (y por lo tanto a ser un candidato dentro del subárbol) si la **SEQUENCE** de **RDN**, que forma el DN completo en **base**, es idéntico a la **SECUENCIA** inicial del mismo número de **RDN** que forman la primera parte del DN del sujeto (en el campo **subject** o **directoryName** de la extensión **subjectAltNames**) del **certificate**. El **DN** del sujeto del **certificate** puede tener **RDN** adicionales en esta secuencia que no aparezcan en el DN en **base**. Se utiliza la regla de concordancia **distinguishedNameMatch** para comparar el valor de **base** con la secuencia inicial de **RDN** en el DN del sujeto del certificado.

No se requieren implementaciones conformes para reconocer todas las formas de nombre posibles. Si la extensión está notificada como crítica y una implementación que utiliza certificado no reconoce una forma de nombre utilizada en cualquier componente **base**, el certificado se debe tratar como si se hubiera encontrado una extensión crítica no reconocida. Si la extensión está notificada como no crítica y una implementación que utiliza certificados no reconoce una forma de nombre utilizada en cualquier componente **base**, entonces se puede ignorar ese subárbol.

NOTA 2 – Cuando se prueban nombres de sujeto de certificado para su coherencia con una constricción de nombre, se deben procesar y no ignorar los nombres en extensiones de nombre alternativas de sujeto no críticas.

Esta extensión puede, según el criterio del expedidor del certificado, ser crítica o no crítica. Se recomienda que se considere como crítica, porque en otro caso un usuario de certificado puede pasar por alto que certificados subsiguientes en un trayecto de certificado están ubicados en los espacios de nombre constreñidos pretendidos por la CA expedidora.

Si esta extensión está presente y está marcada como crítica, entonces un sistema que utilice certificados debe comprobar que el trayecto de certificación que se está procesando es coherente con el valor de esta extensión.

El anexo G contiene ejemplos de utilización de la extensión constricciones de nombres.

b) *En 10.5.2 suprímase el apartado c) y vuélvanse a nombrar los apartados d), e), f), g), h) como c), d), e), f), g) respectivamente.*

c) *Sustitúyanse las siguientes definiciones ASN.1 asociadas con la* **nameConstraints EXTENSION** *en el anexo A.2.*

```
nameConstraints EXTENSION ::= {
        SYNTAX                  NameConstraintsSyntax
        IDENTIFIED BY           id-ce-nameConstraint }

NameConstraintsSyntax ::= SEQUENCE {
        permittedSubtrees       [0]     GeneralSubtrees OPTIONAL,
        excludedSubtrees        [1]     GeneralSubtrees OPTIONAL,
        requiredNameForms       [2]     NameForms OPTIONAL  }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
        base                    GeneralName,
        minimum                 [0]     BaseDistance DEFAULT 0,
        maximum                 [1]     BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)

NameForms  ::= SEQUENCE {
        basicNameForms   [0]    BasicNameForms OPTIONAL,
        otherNameForms   [1]    SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER OPTIONAL }
(ALL EXCEPT ({ -- none; i.e.: at least one component shall be present -- }))
```

```
BasicNameForms  ::= BIT STRING {
        rfc822Name                (0),
        dNSName                   (1),
        x400Address               (2),
        directoryName             (3),
        ediPartyName              (4),
        uniformResourceIdentifier (5),
        iPAddress                 (6),
        registeredID              (7) }  (SIZE (1..MAX))
```

por lo siguiente:

```
nameConstraints EXTENSION ::= {
        SYNTAX                          NameConstraintsSyntax
        IDENTIFIED BY                   id-ce-nameConstraints }

NameConstraintsSyntax ::= SEQUENCE {
        permittedSubtrees       [0]     GeneralSubtrees OPTIONAL,
        excludedSubtrees        [1]     GeneralSubtrees OPTIONAL }
(ALL EXCEPT ({ -- none; at least one component shall be present -- }))

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
        base                            GeneralName,
        minimum                 [0]     BaseDistance DEFAULT 0,
        maximum                 [1]     BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)
```

d) Sustitúyase la siguiente asignación de identificador de objeto en A.2.

```
id-ce-nameConstraint OBJECT IDENTIFIER ::= {id-ce 30 1}
```

por:

```
id-ce-nameConstraints OBJECT IDENTIFIER ::= {id-ce 30}
```

e) Sustitúyase el conjunto siguiente de OID no utilizado en esta Especificación en A.2.

```
-- The following OBJECT IDENTIFIERS are not used by this Specification:
-- {id-ce 2}, {id-ce 3}, {id-ce 4}, {id-ce 5}, {id-ce 6}, {id-ce 7},
-- {id-ce 8}, {id-ce 10}, {id-ce 11}, {id-ce 12}, {id-ce 13},
-- {id-ce 22}, {id-ce 25}, {id-ce 26}, {id-ce 30}
```

por:

```
-- The following OBJECT IDENTIFIERS are not used by this Specification:
-- {id-ce 2}, {id-ce 3}, {id-ce 4}, {id-ce 5}, {id-ce 6}, {id-ce 7},
-- {id-ce 8}, {id-ce 10}, {id-ce 11}, {id-ce 12}, {id-ce 13},
-- {id-ce 22}, {id-ce 25}, {id-ce 26}
```

f) Sustitúyase el texto de G.3 por lo siguiente:

G.3 Uso de la extensión constricciones de nombre

G.3.1 Ejemplos de formato de certificado con extensión constricciones de nombre

Los CA pueden imponer diversas restricciones en los nombres de sujeto (en el campo **subject** o en la extensión **subjectAltName**) de certificados subsiguientes en un trayecto de certificación, incluyendo la extensión constricciones de nombres en los certificados de CA que emiten. Esta subcláusula describe ejemplos de certificados de CA que incluyen la extensión constricciones de nombre junto con una indicación de los requisitos para que certificados subsiguientes sean aceptables en un trayecto de certificación relacionado.

Para simplificar estos ejemplos, sólo se utiliza el nombre DN (directoryName) en la extensión constricciones de nombre.

G.3.1.1 Ejemplos de *permittedSubtrees*

(1-1) Si el certificado de CA contiene la extensión constricciones de nombre siguiente, para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, debe ser igual o estar subordinada a Acme Inc. en U.S. (es decir, {C=US, O=Acme Inc}) para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base(directoryName**) {C=US, O=Acme Inc}}}	(vacío)

(1-2) Si el certificado de CA contiene la extensión constricciones de nombre siguiente para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, debe ser igual o estar subordinado a Acme Inc. In U.S. (es decir, {C=US, O=Acme Inc}) para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **maximum 1**}}	(vacío)

(1-3) Si el certificado de CA contiene la extensión constricciones de nombre siguiente para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, debe ser igual o estar subordinado a Acme Inc. In U.S. (es decir, {C=US, O=Acme Inc}) para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **minimum 1**}}	(vacío)

(1-4) Si el certificado de CA contiene la extensión constricciones de nombre siguiente para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, debe ser igual o estar subordinado a Acme Inc. In U.S. (es decir, {C=US, O=Acme Inc}) para que ese certificado sea aceptable, o ser igual y estar subordinado a Acme Ltd. en U.K.. (es decir, {C=UK, O=Acme Ltd}) para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=UK, O=Acme Ltd}}}	(vacío)

G.3.1.2 Ejemplos de *excludedSubtrees*

(2-1) Si el certificado de CA contiene la extensión constricciones de nombre siguiente para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, no debe ser igual ni estar subordinado a Acme Corp. en Canadá (es decir, {C=CA, O=Acme Corp}) para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
(vacío)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}}}

(2-2) Si el certificado de CA contiene la siguiente extensión constricciones de nombre para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, no debe estar subordinado a cada subordinado inmediato de Acme Corp. en Canadá (es decir, {C=CA, O=Acme Corp}) para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
(vacío)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}, **minimum 2**}}

(2-3) Si el certificado de CA contiene la siguiente extensión constricciones de nombre para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, no debe ser igual que Acme Corp. en Canadá (es decir, {C=CA, O=Acme Corp}) para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
(vacío)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}, **maximum 0**}}

(2-4) Si el certificado de CA contiene la siguiente extensión constricciones de nombre para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, no debe ser igual ni estar subordinado a Acme Corp. en Canadá (es decir, {C=CA, O=Acme Corp}), ni ser igual ni estar subordinado a la Asia Acme en Japón (es decir, {C=JP, O=Asia Acme}) para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
(vacío)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}}, {**base**(**directoryName**) {C=JP, O=Asia Acme}}}

G.3.1.3 Ejemplos de permittedSubtrees y excludedSubtrees

(3-1) Si el certificado de CA contiene la siguiente extensión constricciones de nombre para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, debe ser igual o estar subordinado a Acme Inc. en U.S. (es decir, {C=US, O=Acme Inc}), salvo la unidad de organización R&D de Acme Inc. y los subordinados de organización de R&D para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	{{**base**(**directoryName**) {C=US, O=Acme Inc, OU=R&D}}}

(3-2) Si el certificado de CA contiene la siguiente extensión constricciones de nombre para todos los certificados subsiguientes en el trayecto de certificación, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN, si existe, debe ser igual a uno de los subordinados inmediatos de Acme Inc. en U.S. (es decir, {C=US, O=Acme Inc}), salvo la unidad de organización Purchasing (es decir, {C=US, O=Acme Inc, OU=Purchasing}) para que ese certificado sea aceptable.

Extensión **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **minimum 1**, **maximum 1**}}	{{**base**(**directoryName**) {C=US, O=Acme Inc, OU=Purchasing}}}

G.3.2 Ejemplos de manejo de certificados con la extensión constricciones de nombre

Esta subcláusula describe ejemplos de cómo se validan los nombres de sujeto (en el campo **subject** o en la extensión **subjectAltName**) durante el procesamiento del certificado con las variables de estado de tratamiento del trayecto, es decir, *permitted-subtrees* y *excluded-subtrees*.

Para simplificar estos ejemplos, sólo se utilizan las formas de nombre DN (**directoryName**) y nombre rfc822 (**rfc822Name**) en la extensión constricciones de nombre.

G.3.2.1 Constricciones de espacios de nombre mediante *permitted-subtress* en la forma de nombre DN

En este caso, para que el certificado sea aceptable, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**) en la forma de nombre DN que aparece en el certificado en cuestión debe satisfacer la limitación impuesta por la variable de estado de procesamiento de trayecto *permitted-subtrees*.

(1-1) Está presente un subárbol permitido para DN.

Variables de estado de procesamiento de trayecto	
permitted-subtrees	*excluded-subtrees*
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	NINGUNO

Ejemplos de certificado aceptable

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
6	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}

Ejemplos de certificado inaceptable

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=*Acme Ltd*, OU=Purchasing}
3	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
4	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=*Acme Ltd*, OU=Accounting}

(1-2) Están presentes dos subárboles permitidos para DN.

Variables de estado de procesamiento de trayecto	
permitted-subtrees	*excluded-subtrees*
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=US, O=Acme Ltd}}}	NINGUNO

Ejemplos de certificado aceptable

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing}
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU= Accounting}
6	**subject** = {} **subjectAltName(rfc822Name)** = manager@purchasing.acme.com

Ejemplos de certificado inaceptable

1	**subject** = {C=US, O=*Acme International*, OU=Accounting}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme International*, OU=Accounting}
3	**subject** = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
4	**subject** = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Corp*, OU=Accounting}
5	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com

G.3.2.2 Constricciones de espacios de nombre mediante *excluded-subtrees* en la forma de nombre DN

En este caso, para que el certificado sea aceptable, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**), en la forma de nombre DN que figura en el certificado en cuestión, debe satisfacer la limitación impuesta por la variable de estado de procesamiento de trayecto *excluded-subtrees*.

(2-1) Está presente un subárbol excluido para DN.

Variables de estado de procesamiento de trayecto	
permitted-subtrees	*excluded-subtrees*
NINGUNO	{{**base**(**directoryName**) {C=US, O=Acme Ltd}}}

Ejemplos de certificado aceptable

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}
6	**subject** = {} **subjectAltName(rfc822Name)** = manager@purchasing.acme.com

Ejemplos de certificado inaceptable

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Ltd*, OU=Accounting}

(2-2) Están presentes dos subárboles excluidos para DN.

Variables de estado de procesamiento de trayecto	
permitted-subtrees	*excluded-subtrees*
NINGUNO	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=US, O=Acme Ltd}}}

Ejemplos de certificado aceptable

1	**subject** = {C=US, O=Acme International, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing}
3	**subject** = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme N.Y, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com
5	**subject** = {} **subjectAltName(rfc822Name)** = purchasing@acme-international.com

Ejemplos de certificado inaceptable

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
3	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Accounting}
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com

G.3.2.3 Constricciones de espacios de nombre mediante *permitted-subtrees* en múltiples formas de nombre

En este caso, para que el certificado sea aceptable, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**), en la forma de nombre DN o en la forma de nombre rfc822 que figura en el certificado en cuestión, debe satisfacer la limitación impuesta por la variable de estado de procesamiento de trayecto *permitted-subtrees*.

Están presentes un subárbol permitido para DN y otro subárbol permitido para **rfc822Name**.

Variables de estado de procesamiento de trayecto	
permitted-subtrees	*excluded-subtrees*
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) {acme.com}}	NINGUNO

Ejemplos de certificado aceptable

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}
4	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com
6	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com

Ejemplos de certificado inaceptable

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
3	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-inc.com*
4	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-ltd.com*

G.3.2.4 Constricciones de espacios de nombre mediante *excluded-subtrees* en las formas de nombre múltiples

En este caso, para que el certificado sea aceptable, cada nombre de sujeto (en el campo **subject** o en la extensión **subjectAltName**), en la forma de nombre DN o en la forma de nombre rfc822 que figura en el certificado en cuestión, debe satisfacer la limitación impuesta por la variable de estado de procesamiento de trayecto *excluded-subtrees*.

Variables de estado de procesamiento de trayecto	
permitted-subtrees	*excluded-subtrees*
NINGUNO	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) {acme.com}}}

Ejemplos de certificado aceptable

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-ltd.com

Ejemplos de certificado inaceptable

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
4	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-inc.com
5	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
6	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Accounting}

G.3.3 Ejemplos en los que se necesitan múltiples certificados cruzados con extensiones de constricción de nombre

En algunos casos puede ser necesario emitir más de un certificado de una CA a otro para lograr los resultados deseados. Este podría ser el caso si algunos de los requisitos de constricciones de nombre entran en conflicto o si se necesita una evaluación disociada de diferentes formas de nombre.

G.3.3.1 Requisitos para constricciones de espacio de nombre en conflicto

Se supone que Acme Corporation tiene 20 filiales en los EE.UU.

Widget Corporation quiere establecer certificados cruzados en la CA central de Acme Corporation, pero quiere que sólo la comunidad Widget utilice los certificados Acme para sujetos que cumplan los criterios siguientes:

- Filial 1 a filial 19 de Acme Corporation, todas las secciones son aceptables como sujetos;
- Filial 20 de Acme Corporation, todas las secciones son inaceptables como sujetos, salvo para sujetos de la sección de adquisiciones.

Esto podría lograrse utilizando dos certificados de la forma siguiente: el primer certificado tendría un **permittedSubtrees** de {base: C=US, O=Acme} y un **excludedSubtrees** de {base: C=US, O=Acme, OU=branch20}. El segundo certificado tendría un **permittedSubtrees** de {base: C=US, O=Acme, OU=branch20, OU=Purchasing}.

G.3.3.2 Evaluación disociada de las constricciones de espacio de nombre

Supongamos que la CA de una organización X expide certificados que contienen nombres de dominios de Internet en el subárbol x.com, mientras que otra CA de la organización Y expide certificados que contienen nombres distinguidos X.500 en el subárbol o=y, c=US. Supongamos, además, que la CA de la organización A ha establecido certificados cruzados con las CA de ambas organizaciones, X e Y, y que una tercera CA de la organización B desea certificación cruzada con la CA de A y además desea confiar en los certificados expedidos por las CA de X y de Y. Si la CA de B expide un certificado cruzado a la CA de A que contenga una extensión constricciones de nombre con subárboles permitidos de x.com y o=y, c=US (además del espacio de nombre de la CA de A), entonces si la CA de X o la CA de Y añaden formas de nombre adicionales a sus certificados que contengan nombres distinguidos o nombres de dominio (respectivamente) sus certificados ya no serán válidos para reunir partes que tengan la CA de B como su agente de confianza. Una solución a este problema es que la CA de B debería expedir dos certificados cruzados a la CA de A, uno con una extensión de constricciones de nombre con el subárbol permitido de x.com y otro que contenga el subárbol permitido o=y, c=US.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
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 multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
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, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2007