UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.509

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Corrigendum 3
(10/2001)

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 3

Recomendación UIT-T X.509 (1997) – Corrigendum 3

(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.369
Redes basadas en el protocolo Internet	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.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 ISO/CEI 9594-8

RECOMENDACIÓN UIT-T X.509

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

CORRIGENDUM TÉCNICO 3

Resumen

Este corrigendum técnico trata las resoluciones relacionadas con los informes de defectos 272, 273, 275 y 277.

Orígenes

El corrigendum 3 a la Recomendación UIT-T X.509 (1997), preparado por la Comisión de Estudio 7 (2001-2004) del UIT-T, fue aprobado el 29 de octubre de 2001. Se publica también un texto idéntico como corrigendum técnico 3 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.

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.

ÍNDICE

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

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

CORRIGENDUM TÉCNICO 3

(Trata las resoluciones relacionadas con los informes de defectos 272, 273, 275 y 277)

1) Esto corrige los defectos señalados en el informe de defectos 272

En 12.4.2.1, añádase el siguiente texto al final del párrafo que comienza por "El componente **pathLenConstraint** estará presente solamente si…".

La constricción comienza a surtir efecto con el siguiente certificado en el trayecto. La constricción restringe la longitud del segmento del trayecto de certificación entre el certificado que contiene esta extensión y el certificado de la entidad final. No influye en el número de certificados CA en el trayecto de certificación entre la unidad fiduciaria y el certificado que contiene esta extensión. Por lo tanto, la longitud de un trayecto de certificación completo puede exceder la longitud máxima del segmento constreñido por esta extensión. La constricción controla el número de certificados CA no autoexpedidos entre el certificado CA que contiene la constricción y el certificado de la entidad final. En consecuencia, la longitud total de este segmento del trayecto, excluyendo los certificados autoexpedidos, puede exceder el valor de la constricción hasta en dos certificados. (Esto incluye los certificados en los dos puntos extremos del segmento más los certificados CA entre los dos puntos extremos que están constreñidos por el valor de esta extensión.)

2) Esto corrige los defectos señalados en el informe de defectos 273

Sustitúyase la cláusula 12.4.2.2 por lo siguiente:

12.4.2.2 Extensión de constricciones de nombre

Este campo, que se utilizará solamente en un certificado CA, indica un espacio de nombres dentro del cual tienen que estar ubicados todos los nombres de sujeto en los certificados subsiguientes en un trayecto de certificación. Este campo se define como sigue:

```
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))
```

Si están presentes, los componentes **permittedSubtrees** y **excludedSubtrees** especifican, cada uno de ellos, uno o más subárboles de denominación, cada uno definido por el nombre de la raíz del subárbol y facultativamente, dentro de ese subárbol, una zona que está limitada por un nivel superior, un nivel inferior o por ambos niveles. Si **permittedSubtrees** está presente, los nombres de sujeto dentro de estos subárboles son aceptables. Si **excludedSubtrees** está presente, todo certificado expedido por esa CA o CA subsiguientes en el trayecto de certificación que tenga un nombre de sujeto dentro de estos subárboles es inaceptable. Si están presentes **permittedSubtrees** y **excludedSubtrees** y los espacios de nombres se superponen, la instrucción de exclusión tiene preferencia sobre los nombres en la región de esa superposición. Si no se especifican subárboles permitidos ni excluidos para una forma de nombre, es aceptable cualquier nombre dentro de esa forma de nombre. Si está presente **requiredNameForms**, todos los certificados subsiguientes en el trayecto de certificación incluirán un nombre de al menos una de las formas de nombre requeridas.

Si está presente **permittedSubtrees**, se aplica lo siguiente a todos los certificados subsiguientes en el trayecto. Si cualquier certificado contiene un nombre de sujeto (en el campo **subject** o en la extensión **subjectAltNames**) de una forma de nombre para la cual se especifican subárboles permitidos, el nombre caerá dentro de al menos uno de los subárboles especificados. Si cualquier certificado contiene solamente nombres de sujeto de formas de nombre diferentes de aquéllas para las cuales se especificaron subárboles permitidos, no se requiere que los nombres de sujeto caigan dentro de alguno de los subárboles especificados. Por ejemplo, supóngase que se especifican dos subárboles permitidos, uno para la forma de nombre DN y el otro para la forma de nombre rfc822, que no se especifican subárboles excluidos, pero se especifica **requiredNameForms** con el bit **directoryName** y el bit **rfc822Name** presentes. Un certificado que contuviera solamente nombres diferentes de un nombre de directorio o de un nombre rfc822 sería inaceptable. En cambio, si no se especificara **requiredNameForms**, tal certificado sería aceptable. Por ejemplo, supóngase que se especifican dos subárboles permitidos, uno para la forma de nombre DN y el otro para la forma de nombre rfc822, que no se especifican subárboles excluidos, y que no está presente **requiredNameForms**. Un certificado que contuviera solamente un DN y en el que el DN está dentro del subárbol permitido especificado sería aceptable. Un certificado que contuviera tanto un DN como un nombre rfc822 y en el que solamente uno de ellos está dentro de su subárbol permitido especificado sería inaceptable. También sería aceptable un certificado que contuviera solamente nombres diferentes de un nombre DN o un nombre rfc822.

Si está presente **excludedSubtrees**, todo certificado expedido por la CA sujeto o CA subsiguientes en el trayecto de certificación que tenga un nombre de sujeto (en el campo **subject** o en la extensión **subjectAltNames**) dentro de estos subárboles es inaceptable. Por ejemplo, supóngase que se especifican dos subárboles excluidos, uno para la forma de nombre DN y el otro para la forma de nombre rfc822. Un certificado que solamente contuviera un DN y en el que el DN está dentro del subárbol excluido especificado sería inaceptable. Un certificado que contuviera tanto un nombre DN como un nombre rfc822 y en el que al menos uno de ellos está dentro de su subárbol excluido especificado sería inaceptable.

Cuando un sujeto de certificado tiene múltiples nombres de la misma forma de nombre (incluyendo, en el caso de la forma de nombre **directoryName**, el nombre en el campo sujeto del certificado si no es nulo) se comprobará la consistencia de todos esos nombres con una constricción de nombre de esa forma de nombre.

Si está presente **requiredNameForm**, todos los certificados subsiguientes en el trayecto de certificación incluirán un nombre de sujeto de al menos una de las formas de nombre requeridas.

De las formas de nombre disponibles mediante el tipo **GeneralName**, solamente se pueden utilizar en los campos **permittedSubtrees** y **excludedSubtrees** aquellas que tengan una estructura jerárquica bien definida. La forma de nombre **directoryName** satisface este requisito; cuando se utiliza esta forma de nombre, un subárbol de denominación corresponde a un subárbol del DIT.

El campo **minimum** especifica el límite superior de la zona dentro del subárbol. Todos los nombres cuyo componente de nombre final está por encima del nivel especificado no están contenidos 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 excluye el nodo de base pero incluye nodos subordinados.

El campo **maximum** especifica el nivel inferior de la zona dentro del subárbol. Los nombres cuyo último componente están 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. La ausencia de un componente **maximum** 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.

A opción del expedidor del certificado, esta extensión puede ser crítica o no crítica. Se recomienda que se señale como crítica; de lo contrario, un usuario de certificado no podrá comprobar que los certificados subsiguientes en un trayecto de certificación están situados en el espacio de nombres previsto por la CA expedidora.

Las implementaciones conformes no están obligadas a reconocer todas las formas de nombre posibles.

Si la extensión está presente y está señalada como crítica, una implementación que emplea certificado reconocerá y procesará todas las formas de nombre para las cuales haya tanto una especificación de subárbol (permitido o excluido) en la extensión, como un valor correspondiente en el campo **subject** o en la extensión **subjectAltNames** de cualquier certificado subsiguiente en el trayecto de certificación. Si una forma de nombre no reconocida aparece tanto en la especificación de subárbol como en un certificado subsiguiente, ese certificado se tratará como si se hubiese encontrado una extensión crítica no reconocida. Si cualquier nombre de sujeto en el certificado cae dentro de un subárbol excluido, el certificado es inaceptable. Si se especifica un subárbol para una forma de nombre que no esté contenida en algún certificado subsiguiente, se puede ignorar ese subárbol. Si el componente **requiredNameForms** especifica solamente formas de nombre no reconocidas, ese certificado se debe tratar como si hubiese encontrado una extensión crítica no reconocida. De lo contrario, al menos una de las formas de nombre reconocidas aparecerá en todos los certificados subsiguientes en el trayecto.

Si la extensión está presente y está señalada como no crítica y una implementación que emplea certificado no reconoce una forma de nombre utilizada en cualquier componente **base**, se puede ignorar esa especificación de subárbol. Si la extensión está señalada como no crítica y cualquiera de las formas de nombre especificadas en el componente **requiredNameForms** no es reconocida por la implementación que emplea certificado, el certificado se tratará como si estuviese ausente el componente **requiredNameForms**.

En 12.4.3 añádase una nueva variable de procesamiento de trayecto como sigue y renumérense los incisos subsiguientes como corresponda:

d) *required-name-forms:* Un conjunto (que puede estar vacío) de conjuntos de formas de nombre. Para cada conjunto de formas de nombre, cada certificado subsiguiente contendrá un nombre de una de las formas de nombre en el conjunto.

En 12.4.3 añádase un nuevo paso de inicialización como sigue y renumérense los incisos subsiguientes como corresponda:

d) Inicialícese *required-name-forms* a un conjunto vacío;

En 12.4.3, añádase un paso a las comprobaciones que se aplican a todos los certificados, como sigue:

h) Si el certificado no es un certificado autoexpedido intermedio, y si no es un conjunto vacío, para cada conjunto de formas de nombre en *required-name-forms* comprobar que, en el certificado, hay un nombre de sujeto de una de las formas de nombre en el conjunto.

En 12.4.3, añádase un paso a las acciones de registro de constricciones que se aplican a los certificados intermedios, como sigue:

c) Si la extensión **nameConstraints** con un componente **requiredNameForms** está presente en el certificado, fijar la variable *required-name-forms* a la unión (lógica) de su valor anterior y el conjunto constituido por el conjunto de formas de nombre especificadas en la extensión de certificado. Si el componente **requiredNameForms** contiene más de una forma de nombre, la variable *required-name-forms* indicará que un nombre de al menos una de las formas de nombre indicadas en esta extensión estará presente en todos los certificados subsiguientes. La unión (lógica) de un valor anterior de la variable *required-name-forms* con el valor procedente de la extensión del certificado actual es un conjunto de conjuntos que indica requisitos para todos los certificados subsiguientes. Por ejemplo, si la variable actual *required-name-forms* se fija de modo que se requiera que ya sea un nombre DN o un nombre rfc822 esté presente en los certificados y la extensión actual en el certificado que se procesa indica que se requieren ya sean nombres rfc822 o nombres DNS, la unión (lógica) resultante que es la nueva variable *required-name-forms* indica que cada uno de los certificados subsiguientes debe tener ya sea un nombre rfc822 o tanto un nombre DN como un nombre DNS.

En el anexo A, módulo **certificateExtensions***, actualícese la ASN.1 para la extensión* **nameConstraints** *como se ha indicado antes.*

En el anexo A, módulo **certificateExtensions***, añádase lo siguiente:*

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

En el anexo A, módulo **certificateExtensions***, suprímase lo siguiente:*

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

En el anexo A, módulo **certificateExtensions***, añádase lo siguiente al conjunto de OID no utilizados en esta Especificación:*

id-ce 30

3) Esto corrige los defectos señalados en el informe de defectos 275

En 12.2.2.4, añádase lo siguiente como un nuevo segundo párrafo a continuación de la ASN.1 para la extensión **extKeyUsage**.

Una CA puede aseverar any-extended-key-usage mediante la utilización del identificador **anyExtendedKeyUsage**. Esto permite a una CA expedir un certificado que contenga OID para utilizaciones de clave extendida que puedan ser requeridas por aplicaciones que emplean certificado, sin restringir el certificado a solamente esas utilizaciones de claves. Si la utilización de clave extendida restringiera la utilización de claves, la inclusión de este OID eliminaría esa restricción.

```
anyExtendedKeyUsage  OBJECT IDENTIFIER  ::= { 2 5 29 37 0 }
```

4) Esto corrige los defectos señalados en el informe de defectos 277

En 12.4.2.3, en la última oración del primer párrafo,

Sustitúyase "que es el sujeto de un certificado subsiguiente" *por* "que es el expedidor de un certificado subsiguiente".

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	Redes de cable y transmisión de programas radiofónicos y televisivos, 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

Impreso en Suiza
Ginebra, 2002