UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.509

Corrigendum 2
(02/2001)

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 2

Recomendación UIT-T X.509 (1997) – Corrigendum 2

(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 2

Orígenes

El corrigendum 2 a la Recomendación UIT-T X.509 (1997) , preparado por la Comisión de Estudio 7 (2001-2004) del UIT-T, fue aprobado el 2 de febrero de 2001. Se publica también un texto idéntico como corrigendum técnico 2 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 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 2

NOTA – El presente corrigéndum técnico subsume los proyectos de los corrigenda técnicos 8 y 9.

1) Informes de defectos resueltos por el proyecto de corrigendum técnico 8

(Subsume las resoluciones correspondientes a los informes de defectos 226, 227 y 240).

1.1) Lo que sigue corrige defectos notificados en el informe de defectos 226

En 11.2, suprimir el segundo párrafo:

"Los certificados son producidos … poco probable un eventual peligro.".

1.2) Lo que sigue corrige defectos notificados en el informe de defectos 227

En 12.2.2.1, añadir las dos oraciones siguientes al final del párrafo que empieza con "Las autoridades de certificación asignarán …"

El componente **keyIdentifier** se puede utilizar para seleccionar certificados de la autoridad de certificación durante la construcción del trayecto. El par **authorityCertIssuer**, **authoritySerialNumber** sólo se puede utilizar para otorgar preferencia a un certificado con respecto a otros durante la construcción del trayecto.

1.3) Lo que sigue corrige defectos notificados en el informe de defectos 240

Deberán introducirse las siguientes correcciones en el módulo **authenticationFramework** *de la versión de 1997 del anexo A:*

1) *Añadir* **id-mr** *a la lista de objetos importados del módulo* **UsefulDefinitions** *en el módulo* **authenticationFramework**.

2) *Añadir* **AttributeType**, **Attribute** *y* **MATCHING-RULE** *al conjunto de objetos importados en el módulo* **authenticationFramework** *del módulo* **InformationFramework**.

3) *Añadir* **GeneralNames** *al conjunto de objetos importados en el módulo* **authenticationFramework** *del módulo* **CertificateExtensions**.

4) *Considerar la adición de la definición siguiente al módulo* **authenticationFramework** *porque se importa en otro módulo de las Recomendaciones de la serie X.500, pero nunca se había incluido en el texto de 1997 de esta Recomendación:*

```
HASH {ToBeHashed}          ::=     SEQUENCE {
    algorithmIdentifier            AlgorithmIdentifier,
    hashValue                      BIT STRING ( CONSTRAINED BY {
        -- must be the result of applying a hashing procedure to the DER-encoded octets --
        -- of a value of --ToBeHashed } ) }
```

5) *Añadir las asignaciones de OID siguientes en el módulo* **authenticationFramework***:*

id-at-attributeCertificateRevocationList OBJECT IDENTIFIER ::= {id-at 59}

id-mr-attributeCertificateMatch OBJECT IDENTIFIER ::= {id-mr 42}

6) *Añadir* **Time** *al conjunto de objetos importados en el módulo* **CertificateExtensions** *del módulo* **authenticationFramework**.

7) *En el módulo* **CertificateExtensions***, y en el texto principal, 12.7.2, sustituir:*

CertPolicySet ::= SEQUENCE (1..MAX) OF CertPolicyId

por:

CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId

2) Informes de defectos resueltos por el proyecto de corrigendum técnico 9

(Subsume las resoluciones a los informes de defectos 244, 256, 257 y 258).

2.1) Lo que sigue corrige a los defectos notificados en el informe de defectos 244

En la cláusula 8:

En el párrafo que empieza "El campo de **extensiones** permite añadir nuevos ...", *añadir al final del mismo las dos frases siguientes:*

Cuando una implementación que utiliza certificado reconoce y es capaz de procesar una extensión, la implementación que utiliza certificado procesará la extensión independientemente del valor de la bandera de condición crítica. Obsérvese que cualquier extensión que es declarada no crítica mediante banderas producirá un comportamiento incoherente entre los sistemas que utilizan certificado que procesarán la extensión y los sistemas que utilizan certificado que no reconocen la extensión la ignorarán.

Añadir inmediatamente después del párrafo que empieza "Si dentro de la extensión aparecen elementos desconocidos ...":

Una CA tiene tres opciones con respecto a una extensión:

i) puede excluir la extensión en el certificado;

ii) puede incluir la extensión y declararla no crítica mediante banderas;

iii) puede incluir la extensión y declararla crítica mediante banderas.

Una máquina de validación tiene dos posibles acciones que tomar con respecto a una extensión:

i) puede ignorar la extensión y aceptar el certificado (todas las demás cosas son iguales);

ii) puede procesar la extensión y aceptar o rechazar el certificado según el contenido de la extensión y las condiciones en las que se produce el procesamiento (por ejemplo, los valores vigentes de las variables de procesamiento del trayecto).

Algunas extensiones sólo pueden ser marcadas como críticas. En estos casos una máquina de validación que entiende la extensión, la procesa y la aceptación o el rechazo de certificado depende (al menos en parte) del contenido de la extensión. Una máquina de validación que no entiende la extensión rechaza el certificado.

Algunas extensiones sólo pueden ser marcadas como no críticas. En estos casos, una máquina de validación que entiende la extensión la procesa y la aceptación o el rechazo del certificado depende (al menos en parte) del contenido de la extensión. Una máquina de validación que no entiende la extensión acepta el certificado (a menos que factores distintos de esta extensión provoquen su rechazo).

Algunas extensiones pueden ser marcadas como críticas o no críticas. En estos casos, una máquina de validación que entiende la extensión la procesa y la aceptación o el rechazo del certificado depende (al menos en parte) del contenido de la extensión, independientemente de la bandera de condición crítica. Una máquina de validación que no entiende la extensión acepta el certificado si la extensión es marcada como no crítica (a menos que factores distintos de esta extensión provoquen su rechazo) y rechaza el certificado si la extensión está marcada como crítica.

Cuando una CA considera la inclusión de una extensión en un certificado, lo hace con la esperanza de que su propósito será apoyado siempre que sea posible. Si es necesario que el contenido de la extensión se considere antes de confiar en el certificado, una CA declararía la extensión crítica. Esto debe hacerse en el entendimiento de que cualquier máquina de validación que no procese la extensión rechazará el certificado (probablemente limitando el conjunto de aplicaciones que puede verificar el certificado). La CA puede marcar ciertas extensiones como no críticas para obtener compatibilidad hacia atrás con aplicaciones de validación que no puedan procesar las extensiones. Cuando la necesidad de compatibilidad hacia atrás y de interoperabilidad con aplicaciones de validación incapaces de procesar las extensiones es más vital que la aptitud de la CA para poner en vigor las extensiones, estas extensiones opcionalmente críticas se marcarían entonces como no críticas. Es sumamente probable que las CA pongan extensiones opcionalmente críticas como no críticas durante un periodo de transición, en el cual las aplicaciones de procesamiento de certificados de los verificadores son convertidas en aplicaciones que puedan procesar las extensiones.

En la claúsula l2.1:

En el párrafo que comienza "En un certificado o CRL, una extensión se indica ...", *añadir la frase siguiente inmediatamente después de la tercera frase que termina* "... pasando por alto la extensión"*:*

Si una extensión es declarada no crítica mediante banderas, un sistema que utiliza certificado y que reconoce la extensión, procesará la extensión.

En la claúsula 12.2.2.3:

En el párrafo que empieza "Si la extensión se indica como no crítica mediante banderas ...", *sustituir la segunda frase por la siguiente:*

Si esta extensión está presente, y el sistema que utiliza certificado reconoce o procesa el tipo de extensión **keyUsage**, el sistema que utiliza certificado asegurará que el certificado se utilizará sólo para los fines para los cuales el bit de utilización de clave correspondiente se ha puesto a uno.

En la claúsula 12.2.2.4:

En el párrafo que empieza "Si la extensión se indica como no crítica ...", *sustituir la segunda frase por la siguiente:*

"Si esta extensión está presente, y el sistema que utiliza certificado reconoce o procesa el tipo de extensión **extendedKeyUsage**, el sistema que utiliza certificado asegurará que el certificado se utilizará solamente para uno de los fines indicados.

En la claúsula 12.4.2.1:

En el cuarto párrafo que sigue a la ASN.1, sustituir: "Si esta extensión está presente y se indica como crítica mediante banderas, entonces:" *por el siguiente:*

Si esta extensión está presente y se indica como crítica mediante banderas, o se indica como no crítica mediante banderas pero es reconocida por el sistema que utiliza certificados, entonces:

En la claúsula 12.4.2.2:

Sustituir la última frase "si esta extensión está presente y está indicada como crítica mediante banderas ..." *por la siguiente:*

Si esta extensión está presente y está indicada como crítica mediante banderas, o está indicada como no crítica pero es reconocida por el sistema que utiliza el certificado, este sistema comprobará entonces que el trayecto de certificación que se procesa concuerda con el valor en esta extensión.

2.2) Correcciones a los defectos indicados en el informe de defectos 256

En la cláusula 8:

En el primer párrafo de la descripción del atributo par de certificados cruzados (que empieza "los elementos **directos** ..."*), añadir como tercera frase la siguiente:*

Si una CA emite un certificado a otra CA, y la CA de destino no es una subordinada de la CA emisora en una jerarquía, la CA emisora debe colocar ese certificado en el elemento **reverse** del atributo **crossCertificatePair** de su propia inserción de directorio.

2.3) Correcciones a los defectos indicados en el informe de defectos 257

En la cláusula 8, en el constructivo ASN.1 **CertificatePair***:*

Sustituir **forward** *por* **issuedByThisCA** *y*
Sustituir **reverse** *por* **issuedToThisCA** *y en el texto asociado hacer los cambios que a continuación se indican.*

En el texto descriptivo, en toda la Recomendación UIT-T X.509, actualizar el texto convenientemente para reflejar estos nuevos términos. Esto incluye las siguientes cláusulas específicas:

- *texto descriptivo general en la cláusula 8;*
- *texto ASN.1 y descriptivo del atributo par de certificados cruzados en la cláusula 8;*
- *texto ASN.1 y descriptivo de las reglas de concordancia asociadas en la cláusulas 12.7.3 y 12.7.4; y*
- *los constructivos ASN.1 duplicados en el anexo A.*

Añadir además el texto siguiente tras el párrafoque comienza por "El elemento **directo** ..."*:*

En anteriores ediciones se ha utilizado el término **forward** en lugar de **issuedByThisCA**, y el término **reverse** en lugar de **issuedByThisCA**.

2.4) Correcciones a los defectos indicados en el informe de defectos 258

En la cláusula 8, añadir el siguiente nuevo párrafo al final de la cláusula, inmediatamente antes de la primera subcláusula 8.1:

Cada certificado de un trayecto de certificación será único. No puede aparecer ningún certificado más de una vez en un valor del componente **theCACertificates** del **CertificationPath** o en un valor **certificate** en el componente **CrossCertificates** del **ForwardCertificationPath**.

En 12.4.3, añadir la siguiente nota inmediatamente después del apartado a) un conjunto de certificados ...

NOTA – Cada certificado de un trayecto de certificación es único. Un trayecto que contiene el mismo certificado dos o más veces no es un trayecto de certificación válido.

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

Ginebra, 2002