



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**X.509**

**Corrigendum 3**  
(04/2004)

SERIE X: REDES DE DATOS Y COMUNICACIÓN  
ENTRE SISTEMAS ABIERTOS

Directorio

---

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

**Corrigendum técnico 3**

Recomendación UIT-T X.509 (2000) – Corrigendum  
técnico 3

---

RECOMENDACIONES UIT-T DE LA SERIE X  
REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

<b>REDES PÚBLICAS DE DATOS</b>	
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
<b>INTERCONEXIÓN DE SISTEMAS ABIERTOS</b>	
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
<b>INTERFUNCIONAMIENTO ENTRE REDES</b>	
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
<b>SISTEMAS DE TRATAMIENTO DE MENSAJES</b>	
<b>DIRECTORIO</b>	<b>X.500–X.599</b>
<b>GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS</b>	
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
<b>GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS</b>	
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
<b>SEGURIDAD</b>	
<b>APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS</b>	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
<b>PROCESAMIENTO DISTRIBUIDO ABIERTO</b>	
<b>SEGURIDAD DE LAS TELECOMUNICACIONES</b>	<b>X.1000–</b>

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

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

**Corrigendum técnico 3**

**Orígenes**

El corrigendum 3 a la Recomendación UIT-T X.509 (2000) fue aprobado el 29 de abril de 2004 por la Comisión de Estudio 17 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8. 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.

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.

© UIT 2004

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

## ÍNDICE

	<i>Página</i>
1) Corrección de los defectos notificados en el informe de defectos 281 .....	1
2) Corrección de los defectos notificados en el informe de defectos 282 .....	2
3) Corrección de los defectos notificados en el informe de defectos 289 .....	2
4) Corrección de los defectos notificados en el informe de defectos 291 .....	2
5) Corrección de los defectos notificados en el informe de defectos 296 .....	3
6) Corrección de los defectos notificados en el informe de defectos 298 .....	3
7) Corrección de los defectos notificados en el informe de defectos 299 .....	3
8) Corrección de los defectos notificados en el informe de defectos 300 .....	6
9) Corrección de los defectos notificados en el informe de defectos 301 .....	6
10) Corrección de los defectos notificados en el informe de defectos 304 .....	6
11) Corrección de los defectos notificados en el informe de defectos 305 .....	6



**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 3**

(Trata las resoluciones tomadas con relación a los informes de defectos 281, 282, 289, 291, 296, 298, 299, 300, 301, 304 y 305.)

En una versión anterior aprobada de este corrigendum técnico que no se publicó se resolvía el informe de defectos 280. Tras votarse la aprobación del proyecto de corrigendum técnico en que se resolvía dicho informe de defectos, los implementadores se dieron cuenta de que los métodos introducidos en la cuarta edición para tratar la revocación de clave pública y de atributo tenían errores. El texto que resuelve el informe de defectos 305 permite trasladar a la cuarta edición el método especificado en la tercera. Dado que la publicación del texto que resuelve el informe de defectos 280 ya no es la adecuada y puede confundir a quienes utilicen la cuarta edición, dicho texto se suprime de esta versión del corrigendum técnico.

**1) Corrección de los defectos notificados en el informe de defectos 281**

*En la cláusula 8.6.2.6, añádase el párrafo siguiente después del código ASN.1:*

El valor de tipo **CRLDistPointsSyntax** es el que se define en la extensión de puntos de distribución de CRL de 8.6.2.1.

*Sustitúyase la cláusula B.5.1.4 por la siguiente:*

Para determinar si una CRL es una de las CRL indicadas mediante una extensión de punto de distribución de CRL o por la extensión CRL más reciente, se deberán cumplir todas las siguientes condiciones:

- o bien el campo de punto de distribución en la extensión de punto de distribución expedidor de la CRL tendrá que estar ausente (sólo si no se busca un DP de CRL crítica), o uno de los nombres en el campo de punto de distribución de la extensión de DP CRL o de la CRL más reciente tendrá que concordar con uno de los nombres en el campo de punto de distribución en la extensión de punto de distribución expedidor de la CRL. Como alternativa, uno de los nombres en el campo **cRLIssuer** de la extensión del DP de CRL o de la CRL más reciente puede concordar con uno de los nombres en el punto de distribución del IDP; y
- si el certificado es un certificado de entidad final, la CRL no contendrá el campo **onlyContainsAuthorityCerts** fijado a **VERDADERO** en la extensión de punto de distribución de expedidor de la CRL; y
- si **onlyContainsAuthorityCerts** está fijado a **VERDADERO** en la extensión de punto de distribución expedidor de la CRL, entonces el certificado que se está comprobando tendrá que contener la extensión **basicConstraints** con el componente **CA** fijado a **VERDADERO**; y
- si el campo **reasons (motivos)** está presente en la extensión de DP de la CRL o de la CRL más frecuente, el campo **onlySomeReasons** estará ausente de la extensión de punto de distribución expedidor de la CRL o contener por lo menos uno de los códigos de motivo afirmados en la extensión de DP de la CRL o de la CRL más reciente; y
- si el campo **cRLIssuer** está ausente de la extensión pertinente (bien sea DP de CRL o CRL más reciente), la CRL deberá estar firmada por la misma CA que firmó el certificado; y
- si el campo **cRLIssuer** está presente en la extensión pertinente (bien sea DP de CRL o CRL más reciente), la CRL deberá estar firmada por el expedidor de CRL identificado en el campo **cRLIssuer** y la CRL tendrá que contener la extensión de punto de distribución expedidor cuyo campo **indirectCRL** esté puesto a **VERDADERO**.

NOTA – Cuando se verifique la presencia de los campos **reasons (motivos)** y **cRLIssuer**, se considerará la prueba exitosa solamente cuando el campo en cuestión esté presente en el mismo **DistributionPoint** de la

extensión de DP de la CRL o de la CRL más reciente para la cual hay una correspondencia de nombre en el campo de punto de distribución correspondiente de la extensión IDP en la CRL.

## 2) Corrección de los defectos notificados en el informe de defectos 282

En el párrafo de la cláusula 7, que sigue a la definición del campo *versión* y en el que sigue a la definición del campo *extensiones* sustitúyase:

"indicadas en 7.5.2.2 de la Rec. UIT-T X.519 | ISO/CEI 9594-5"

por:

"indicadas en 12.2.2 de la Rec. UIT X.519 | ISO/CEI 9594-5".

En la cláusula 7.3, añádase el siguiente párrafo nuevo inmediatamente después de la Nota 6 y en la cláusula 12.1, inmediatamente después de la definición del campo *extensiones*:

"Si la extensión no está marcada como crítica, se hará caso omiso de los elementos desconocidos que figuren en la misma de conformidad con las reglas de extensibilidad indicadas en 12.2.2 de la Rec. UIT-T X.519 | ISO/CEI 9594-5."

## 3) Corrección de los defectos notificados en el informe de defectos 289

Sustitúyase el texto de la cláusula 10.1, apartado c, por el siguiente:

- c) un conjunto de políticas inicial formado por uno o más identificadores de políticas de certificado, que indica que a efectos del procesamiento del trayecto de certificación cualquiera de estas políticas sería aceptable para el usuario del certificado; esta entrada puede también tomar el valor especial *cualquier política*, pero no puede ser nula;

Sustitúyase completamente la cláusula 10.5.4, por la siguiente:

### 10.5.4 Procesamiento final

Una vez se hayan tramitado todos los certificados en el trayecto, se realizan las siguientes acciones:

- a) Determinar el conjunto de políticas constreñidas por las autoridades a partir del cuadro correspondiente. Si éste está vacío, dicho conjunto es vacío o nulo. Si el conjunto de políticas constreñidas por la autoridad [0, profundidad de trayecto] es cualquier política el conjunto de políticas constreñidas por la autoridad es cualquier política. De lo contrario, dicho conjunto es, para cada fila en el cuadro, el valor en la célula más a la izquierda que no contenga el identificador cualquier política.
- b) Calcular el conjunto de políticas constreñidas por las autoridades mediante la intersección de los conjuntos de políticas constreñidas por la autoridad y de política inicial.
- c) Si está puesto el indicador de política explícita, verificar que ni el conjunto de políticas constreñidas por las autoridades ni el conjunto de políticas constreñidas por el usuario sean vacíos.

Si falla cualquiera de las pruebas anteriores, se ha de terminar el procedimiento, retornar una indicación de fallo, un código de motivo adecuado el indicador de política explícita, el conjunto de política constreñida por las autoridades y el conjunto de política constreñidas por el usuario. Si el fallo se debe a que el conjunto de políticas constreñidas por el usuario está vacío, el trayecto es válido conforme a la(s) política(s) constreñida(s) por las autoridades, pero inaceptable para el usuario.

Si ninguna de estas pruebas falla en el certificado final, se termina el procedimiento, se retorna una indicación de éxito junto con el indicador de políticas explícita, el conjunto de políticas constreñidas por las autoridades y el conjunto de políticas constreñidas por el usuario.

## 4) Corrección de los defectos notificados en el informe de defectos 291

En la cláusula 3.3.44, en la definición del "certificado de clave pública", sustitúyase "infalsificable por cifrado" por "infalsificable por firma digital".

En la cláusula 3.1, añádase "firma digital" a la lista de términos definidos en la Rec. CCITT X.800 | ISO/CEI 7498-2. Conservar el orden alfabético y reenumerar los demás elementos de la lista.

## 5) Corrección de los defectos notificados en el informe de defectos 296

En la cláusula B.5.1.1, en la primera frase, añádase "emitido por el expedidor de CRL" inmediatamente después de "y de CA".

En la cláusula B.5.1.1, sustitúyase el tercer guión por el siguiente:

- O bien la extensión de punto de distribución expedidor no contendrá el campo de punto de distribución o uno de los nombres en dicho campo corresponderán con el campo **issuer** en la CRL; y

En la cláusula B.5.1.2, sustitúyase el tercer guión por el siguiente:

- O bien la extensión de punto de distribución expedidor no contendrá el campo de punto de distribución o uno de los nombres en dicho campo corresponderán con el campo **issuer** en la CRL; y

En la cláusula B.5.1.3, sustitúyase el tercer guión por el siguiente:

- O bien el punto de distribución expedidor no contendrá el campo de punto de distribución o uno de los nombres en dicho campo corresponderán con el campo **issuer** en la CRL; y

En la cláusula B.5.1.4, en el primer guión, sustitúyase la última frase por la siguiente:

- Si el campo de punto de distribución no está en el certificado de DP de la CRL, uno de los nombres en el campo **CRLIssuer** de dicho certificado podrá también corresponder con uno de los nombres en el DP del IDP. Si tanto el campo de punto de distribución como el **CRLIssuer** están ausentes del certificado del DP de la CRL, el campo **issuer** del certificado podrá corresponder con uno de los nombres en el DP del IDP; y

## 6) Corrección de los defectos notificados en el informe de defectos 298

En la cláusula 7.3, añádase un nuevo punto "d" a la lista que viene después de la frase "una autoridad que expide y revoca posteriormente certificados":

- d) cuando se utilicen solamente CRL particionadas, se emitirá un conjunto completo de CRL particionadas que cubra todo el conjunto de certificados sobre los cuales se notificará el estado de revocación mediante el mecanismo CRL. Es decir, todo el conjunto de las CRL particionadas será equivalente a una CRL completa para el mismo conjunto de certificados, si el expedidor de la CRL no estaba utilizando CRL particionadas.

En la cláusula 8.6.2.2, añádase el siguiente texto nuevo inmediatamente después de la primera frase:

Cuando se utilicen solamente CRL particionadas, todo el conjunto de éstas cubrirá el conjunto completo de certificados cuyo estado de revocación se notificará utilizando el mecanismo CRL. Es decir, el conjunto completo de CRL particionadas será equivalente a una CRL completa para el mismo conjunto de certificados, si el emisor de CRL no estaba utilizando CRL particionadas.

## 7) Corrección de los defectos notificados en el informe de defectos 299

Insértense los párrafos siguientes como una nueva cláusula 7.4:

### 7.4 Repudio de una firma digital

Todo participante en un evento puede decidir ulteriormente repudiar cualquier cosa que haya sido firmada digitalmente por otro participante. Por ejemplo, se puede negar la participación en un establecimiento de clave o en el origen de un mensaje de correo electrónico firmado, de la misma manera que es posible negar haber firmado un documento para evitar la responsabilidad que implique su contenido. Puede ocurrir que el repudio no funcione. En el marco de no repudio de la Rec. UIT-T X.813 | ISO/CEI 10181-4, se describe el siguiente proceso de resolución de disputas:

- 1) generación de evidencia;
- 2) transferencia, almacenamiento y recuperación de evidencia;
- 3) verificación de evidencia; y
- 4) resolución de controversias.

La evidencia generada puede incluir, entre otras cosas:

- registro de auditoría relacionados con el evento y aserción de intento;

## ISO/CEI 9594-8:2001/cor.3:2005 (S)

- declaraciones realizadas ante notarios terceras partes;
- declaraciones de política;
- información firmada digitalmente, que incluya registro de auditoría y declaraciones notariales;
- indicaciones de tiempo de la información firmada digitalmente;
- certificados que soportan la firma digital;
- la información de revocación adecuada publicada y disponible al momento de la controversia; y
- cualquiera otra revocación de certificado que haya ocurrido después del evento que pudiese indicar que el compromiso de clave se realizó antes de ese instante.

Es posible preservar de diferentes maneras la integridad de los datos almacenados de modo que pueda probarse como evidencia, por ejemplo, el control de acceso, el almacenamiento mediante funciones generadoras por parte de terceros de confianza de datos generados, firmas digitales. Puede también ocurrir que se deba aumentar periódicamente la protección de dichos datos almacenados a fin de contrarrestar las mejoras en el procesamiento por computador y/o el análisis criptográfico.

NOTA – Si bien esta Especificación de directorio no especifica ni el tipo y cantidad de evidencia generada ni el nivel de integridad, cabe esperar que será acorde con el riesgo involucrado.

Es posible que para la verificación de evidencia sea necesario revalidar las firmas digitales de datos, por ejemplo mensajes, documentos, certificados, CRL e indicaciones de tiempo utilizadas en el proceso de validación inicial. El hecho de que un certificado haya expirado no impide que se utilice para revalidar las firmas creadas durante su periodo de validez. Se puede utilizar un certificado revocado siempre y cuando se establezca que era válido en el momento de ocurrir el evento que origina la disputa.

Aún cuando toda esta evidencia descrita se considere técnicamente válida, puede ocurrir que el firmante repudie con éxito el mensaje basándose en otras condiciones, por ejemplo, el intento, la comprensión o las competencias del signatario.

*Sustitúyase la cláusula 8.2.2.3 por lo siguiente:*

### 8.2.2.3 Extensión de utilización de claves

Este campo identifica la utilización para la cual se emitió el certificado. Esta utilización inicial puede verse restringida aún más por la política. Es posible declarar esta política en una definición de política de certificado, un contrato u otra especificación. No obstante, una política no reemplazará la restricción indicada por un bit **KeyUsage**, es decir una política de certificado no puede permitir que el certificado sea utilizado para una firma digital si **KeyUsage** indica que sólo puede hacerse a través de un acuerdo de claves.

El hecho de fijar un valor específico de **KeyUsage** en un certificado no indica, en un caso de comunicación, que las partes actúan de conformidad con dicho valor, por ejemplo al firmar un documento. Los métodos de definición mediante los cuales las partes pueden señalar su disposición a establecer un ejemplar particular de comunicación (por ejemplo, el compromiso relativo al contenido de dicho ejemplar particular) queda fuera del alcance de esta Especificación de directorio, pero se puede prever que habrá varios métodos. Si bien no se recomienda, es posible utilizar el contenido del certificado, por ejemplo la política de certificado, para señalar la intención de firmar. No obstante, puesto que la señal se hizo cuando la CA expidió certificado, es probable que esta utilización no cumpla con el requisito de que la declaración de intención se haga en el momento de la firma del signatario.

Se puede fijar más de un bit en un ejemplar de la extensión **keyUsage**. Al fijar múltiples bit no cambiará el significado de cada uno de ellos sino que se indicará que es posible utilizar el certificado a todos los efectos indicados por los bits en cuestión. Es posible que esta operación presente varios riesgos. En el anexo informativo tbd se presenta un resumen de ellos. El texto propuesto en el comentario número 4 de AFNOR proveniente del Resumen de Votación del proyecto de Corrigendum Técnico 6, SC6 N12648 se incluirá en este anexo.

Este campo se define del modo siguiente:

```
keyUsage EXTENSION ::= {
  SYNTAX          KeyUsage
  IDENTIFIED BY   id-ce-keyUsage }

KeyUsage ::= BIT STRING {
  digitalSignature      (0),
  contentCommitment    (1),
  keyEncipherment      (2),
  dataEncipherment     (3),
  keyAgreement         (4),
  keyCertSign          (5),
  cRLSign              (6),
```

**encipherOnly** (7),  
**decipherOnly** (8) }

Los bits en el tipo **KeyUsage** son:

- a) **digitalSignature**: para verificar firmas digitales que se utilizan con un servicio de autenticación de entidad, de autenticación de origen de datos y/o de integridad;
- b) **contentCommitment**: para verificar las firmas digitales cuyo propósito es señalar que el signatario compromete con contenido firmado. La CA puede restringir aún más la utilización del certificado a fin de soportar el tipo de compromiso, por ejemplo a través de una política de certificado. El tipo exacto de compromiso del signatario, por ejemplo "revisado y aprobado" o "con la intención de restringirlo" puede indicarse en el contenido firmado, por ejemplo el propio documento firmado o alguna otra información firmada.

Puesto que la firma de un compromiso de contenido se considera como una transacción firmada digitalmente, no es necesario fijar en el certificado bit **digitalSignature**. No obstante, de hacerlo no se afectará el nivel de compromiso que el firmante adquiere al firmar el documento.

Cabe observar que si bien no es incorrecto referirse a este bit **keyUsage** utilizando el identificador **nonRepudiation**, sin embargo se desaconseja. Independientemente de qué identificador se utilice, la semántica de este bit es la especificada en la presente Especificación de directorio.

- c) **keyEncipherment**: para claves de cifrado u otra información de seguridad, por ejemplo, para transporte de claves.
- d) **dataEncipherment**: para cifrar datos de usuario, pero no claves ni otra información de seguridad como en el apartado c) anterior;
- e) **keyAgreement**: para su utilización como una clave de acuerdo de clave pública.
- f) **keyCertSign**: para verificar una firma de CA en certificados.

Puesto que la CA considera la firma de un certificado como un compromiso con el contenido del certificado, no es necesario fijar en el certificado ni el bit **digitalSignature** ni el bit **contentCommitment**. Si se fija uno de ellos, o ambos, no se afecta el nivel de compromiso que el signatario ha adquirido al firmar el certificado.

- g) **cRLSign**: para verificar una firma de autoridad en las CRL.  
 Al considerarse que la firma de una CRL implica que el emisor de la CRL se compromete con su contenido, no es necesario fijar en el certificado ni el bit **digitalSignature** ni el bit **contentCommitment**. Si uno de éstos, o ambos, se fija esto no afecta el nivel de compromiso que el signatario adquiere al firmar la CRL.
- h) **encipherOnly**: clave de acuerdo de clave pública para su utilización sólo en datos de cifrado utilizados con el bit **keyAgreement** también fijado (el significado con otro bit de utilización de clave fijado no está definido).
- i) **decipherOnly**: clave de acuerdo de clave pública para su utilización únicamente en datos de descifrado utilizados con el bit **keyAgreement** también fijado (el significado con otro bit de utilización de clave fijado no está definido).

Se debería indicar en las especificaciones de aplicación cuál de los bits **digitalSignature** o **contentCommitment** son adecuados para la utilización. Cuando una aplicación que firma conozca la intención del firmante respecto a su compromiso con el contenido, dicha aplicación firmará y soportará dicha firma mediante un certificado que tenga el bit **digitalSignature** fijado en su extensión **keyUsage**.

Aun cuando se haya verificado una firma digital a través de un certificado que tenga solamente el bit **digitalSignature** fijado, es posible que haya otros factores externos a la verificación de la firma digital que cumplan una función a la hora de determinar la intención de quien firma. Por otra parte, aunque se haya verificado una firma digital utilizando un certificado que tenga solamente el bit **contentCommitment** fijado, quien firma puede argüir factores externos para negar su compromiso con el contenido firmado.

El bit **keyCertSign** se utiliza solamente en los certificados de la CA. Si **KeyUsage** está fijado a **keyCertSign**, el valor de la componente **CA** de la extensión **basicConstraints** se fijará a **TRUE**. Las CA también pueden usar otro de los bits de utilización de clave definidos en **KeyUsage**, por ejemplo **digitalSignature** para proporcionar autenticación e integridad en transacciones de administración en línea.

Esta extensión puede, ser o no crítica, a opción del expedidor del certificado.

Si la extensión se indica como crítica o no crítica mediante banderas, pero el sistema que utiliza certificado la reconoce, se utilizará el certificado solamente cuando se haya fijado a uno el bit de utilización de clave. Si la extensión se indica como no crítica mediante una bandera y el sistema que utiliza certificado no lo reconoce, se hará caso omiso de esta

extensión. Cuando se fija a cero un bit quiere decir que la clave no está destinada a dicho propósito. Si la extensión está presente y todos sus bits fijados a cero, la clave está destinada a algún propósito diferente de los ya mencionados.

## 8) Corrección de los defectos notificados en el informe de defectos 300

*En la cláusula 10.5.1, punto b), sustitúyase la primera frase por la siguiente:*

Para un certificado intermedio de versión 3, verificar si está presente esta **basicConstraints** y si el componente **CA** en la extensión **basicConstraints** es VERDADERO.

## 9) Corrección de los defectos notificados en el informe de defectos 301

*En la cláusula B.5.2, reemplazar la segunda frase del tercer guión, por la siguiente:*

La CRL básica es la CRL a la que se hace referencia en la dCRL o una posterior.

## 10) Corrección de los defectos notificados en el informe de defectos 304

*En el anexo F, desplazar la definición siguiente:*

**id-ea-rsa**      **OBJECT IDENTIFIER ::= {id-ea-1}**

*después del texto siguiente:*

*"-- the following object identifier assignments reserve values assigned to deprecated functions"*

*suprimir:*

*-- object identifier assignments --*

## 11) Corrección de los defectos notificados en el informe de defectos 305

*En la cláusula 8.6.2, añádase el siguiente nuevo punto c) a la lista y renumérese el resto de los puntos de dicha lista:*

- c) **AAissuingDistributionPoint**;

*En la cláusula 8.6.2, sustitúyase la segunda frase del segundo párrafo por la siguiente:*

El punto de distribución expedidor, el punto de distribución expedidor AA, el indicador de CRL delta y la actualización básica se utilizarán únicamente como extensiones CRL.

*Añádase el párrafo siguiente al final de la cláusula 8.6.2 e inmediatamente antes de la cláusula 8.6.2.1:*

Si bien las extensiones de punto de distribución expedidor y de punto de distribución expedidor AA tienen la misma utilidad, se aplican a certificados diferentes. La primera sirve solamente para certificados de clave pública emitidos a usuarios y/o CA, mientras que la segunda se aplica únicamente a certificados de atributo emitidos a usuarios y AA así como a certificados de clave pública emitidos a SOA. Cuando una misma CRL cubra todos estos tipos de certificados, ésta deberá incluir ambas extensiones. Cabe observar que la extensión de alcance de la CRL definida en 8.5.2.5 también es similar a estas dos extensiones. No obstante, se sabe que esta extensión es errónea y se desaconseja su utilización. Se debe utilizar la extensión de punto de distribución expedidor y/o la de punto de distribución expedidor AA en lugar de la de alcance de CRL.

*En la cláusula 8.5.2.5 (extensión de ámbito de CRL) sustitúyase el párrafo siguiente:*

Cabe destacar que la extensión **issuingDistributionPoint** y la extensión **crlScope** pueden chocar y no se pretende que se utilicen juntas. Sin embargo, si la CRL contiene tanto una extensión **issuingDistributionPoint** como una extensión **crlScope**, entonces un certificado se considera dentro del ámbito de la CRL si y sólo si cumple los criterios de ambas extensiones. Si la CRL no contiene ninguna de las extensiones **issuingDistributionPoint** o **crlScope**, entonces el ámbito es el ámbito completo de autoridad y la CRL puede ser utilizada por cualquier certificado proveniente de esa autoridad.

por:

Cabe destacar que la extensión **issuingDistributionPoint** y la extensión **crlScope** pueden chocar y no se pretende que se utilicen juntas. Sin embargo, si la CRL contiene tanto una extensión **issuingDistributionPoint** como una **crlScope** entonces un certificado de clave pública se considera dentro del ámbito de la CRL si y sólo si cumple los criterios de ambas extensiones. Si la CRL contiene una extensión **AAissuingDistributionPoint**, mas no una extensión **issuingDistributionPoint** o **crlScope**, el certificado de clave pública no se incluye en su ámbito. Si la CRL no contiene una extensión **issuingDistributionPoint**, **AAissuingDistributionPoint**, o **crlScope**, entonces se trata del ámbito completo de la autoridad, y es posible utilizar la CRL para cualquier certificado de dicha autoridad. De igual manera las extensiones **AAissuingDistributionPoint** y **crlScope** pueden chocar y no se pretende que se utilicen juntas. No obstante, si la CRL contiene tanto una extensión **AAissuingDistributionPoint** como una **crlScope**, entonces el certificado de atributo se considera dentro del ámbito de la CRL si y sólo si cumple los criterios de ambas extensiones. Si la CRL contiene una extensión **issuingDistributionPoint**, mas no una **AAissuingDistributionPoint** o **crlScope**, entonces su ámbito no incluye certificados de atributo. Si la CRL no contiene una extensión **issuingDistributionPoint**, **AAissuingDistributionPoint**, o **crlScope**, entonces el ámbito es el ámbito completo de la autoridad, y es posible utilizar la CRL para cualquier certificado proveniente de dicha autoridad.

Reemplazar la cláusula 8.6.2.2 por la siguiente:

### 8.6.2.2 Extensión de punto de distribución expedidor

Este campo de extensión de CRL identifica el punto de distribución de CRL para los certificados de clave pública de esta CRL particular, e indica si ésta es indirecta, o está limitada únicamente a un subconjunto de la información de revocación. La limitación se puede basar en un subconjunto del contenido del certificado o en un subconjunto de motivos de revocación. La CRL está firmada por la clave pública del expedidor de la CRL – los puntos de distribución de CRL no tienen su propio par de claves. No obstante, para una CRL distribuida por el directorio, la CRL está almacenada en el asiento del punto de distribución de CRL, que no puede ser el asiento de directorio del expedidor de ésta. Si el campo punto de distribución expedidor, el campo punto de distribución expedidor AA, y el campo ámbito de la CRL están ausentes, la CRL contendrá asientos a todos los certificados de clave pública válidos no revocados expedidos por el emisor de la CRL. Cuando no haya ni campo de punto de distribución de emisor ni de ámbito de CRL, pero sí el de punto de distribución de emisor AA, el ámbito de la CRL no cubrirá certificados de clave pública.

(Nota del Editor: Al compilar la próxima edición de la Rec. UIT-T X.509, obsérvese que hay una frase adicional que se ha de añadir al párrafo anterior de acuerdo con el corrigendum técnico 3 y de la Resolución del informe de defectos 298.)

Cuando aparece un certificado en una CRL, es posible borrarlo de una CRL posterior tras su expiración. Este campo se define así:

```
issuingDistributionPoint EXTENSION ::= {
    SYNTAX IssuingDistPointSyntax
    IDENTIFIED BY id-ce-issuingDistributionPoint }
```

```
IssuingDistPointSyntax ::= SEQUENCE {
```

```
-- If onlyContainsUserPublicKeyCerts and onlyContainsCACerts are both FALSE, the CRL covers both certificate types --
```

```
    distributionPoint          [0] DistributionPointName OPTIONAL,
    onlyContainsUserPublicKeyCerts [1] BOOLEAN DEFAULT FALSE,
    onlyContainsCACerts        [2] BOOLEAN DEFAULT FALSE,
    onlySomeReasons            [3] ReasonFlags OPTIONAL,
    indirectCRL                 [4] BOOLEAN DEFAULT FALSE }
```

El componente **distributionPoint** contiene el nombre del punto de distribución en una o varias formas de nombres. Si **onlyContainsUserPublicKeyCerts** es verdadero, la CRL contiene revocaciones para los certificados de clave pública de entidad extremo. Si **onlyContainsCACerts** es verdadero, la CRL contiene revocaciones para certificados de CA. Si tanto **onlyContainsUserPublicKeyCerts** como **onlyContainsCACerts** son falsos, la CRL contiene revocaciones para certificados de clave pública de entidad extrema y certificados CA. Si **onlySomeReasons** está presente, la CRL únicamente contiene revocaciones de certificado de clave pública para los motivos identificados o motivos, de lo contrario tendrá revocaciones para todos los motivos. Si **indirectCRL** es verdadero, es posible que la CRL contenga notificaciones de revocación para certificados de clave pública de otras autoridades diferentes de la expedidora de la CRL. La autoridad que se encarga de cada asiento viene indicada por la extensión del asiento CRL del expedidor de certificado en dicha entrada o es conforme a las reglas pálidas por defecto que se describen en 8.6.2.3. En una tal CRL, es responsabilidad de su expedidor garantizar que está completa en el sentido de que contiene todos los asientos de revocación, coherente con los indicadores **onlyContainsUserPublicKeyCerts**, **onlyContainsCACerts**, y **onlySomeReasons**, para todas las autoridades que identifican este expedidor de CRL en su certificado de clave pública.

En el caso de las CRL distribuidas a través del directorio se aplican las reglas siguientes. Si la CRL es una dCRL se la distribuirá a través del atributo **deltaRevocationList** del punto de distribución asociado o, si no se ha identificado un punto de distribución, a través del atributo **deltaRevocationList** de la entrada de expeditor CRL, sin importar la configuración de los tipos de certificado cubiertos por la CRL. A menos que la CRL sea una dCRL:

- Se distribuirá una CRL que tenga fijada **onlyContainsCACerts** y no contenga una extensión **AAIssuingDistributionPoint**, mediante el atributo **authorityRevocationList** del punto de distribución asociado o, si no se define punto de distribución, mediante el atributo **authorityRevocationList** de la entrada de expeditor CRL.
- Se distribuirá una CRL que tenga fijado **onlyContainsCACerts** y que contenga una extensión **AAIssuingDistributionPoint** con el **containsUserAttributeCerts** fijado a falso, a través del atributo **authorityRevocationList** del punto de distribución asociado o, de no haber un punto de distribución identificado, mediante el atributo **authorityRevocationList** de la entrada de expeditor de CRL.
- Se distribuirá una CRL que tenga solamente **onlyContainsCACerts** puesto a falso a través del atributo **certificateRevocationList** del punto de distribución asociado o, si no se ha identificado el punto de distribución, mediante el atributo **certificateRevocationList** de la entrada de expeditor CRL.
- Se distribuirá una CRL que contenga tanto una extensión **issuingDistributionPoint** como una **AAIssuingDistributionPoint** con **containsUserAttributeCerts** fijado, mediante el atributo **certificateRevocationList** del punto de distribución asociado o, si no se ha identificado un punto de distribución, a través del atributo **certificateRevocationList** de la entrada de expeditor de CRL.

Esta extensión siempre es crítica. Un usuario de certificado que no entienda dicha extensión no puede suponer que la CRL contiene una lista completa de certificados revocados o la autoridad identificada. Las CRL que no contengan extensiones críticas no podrán contener todas las entradas actuales de CRL correspondientes a la autoridad que expide, incluidas aquéllas para los certificados de usuarios revocados y certificados de autoridad.

NOTA 1 – Los medios que utilizan las autoridades para comunicar la información de revocación a los expedidores de CRL están fuera del alcance de esta Especificación de directorio.

NOTA 2 – Cuando una autoridad publique una CRL con **onlyContainsUserPublicKeyCerts** o **onlyContainsCACerts** puestas a verdadero, garantizará que todos los certificados CA cubiertos por dicha CRL contengan la extensión **basicConstraints**.

*Añádase la siguiente nueva cláusula:*

#### 8.6.XX Extensión del punto de distribución expedidor AA

Este campo de extensión CRL identifica el punto de distribución CRL para los certificados de atributo de esta CRL particular, e indica si la CRL es indirecta, o está limitada a abarcar solamente un subconjunto de la información de revocación. La limitación se puede basar en un subconjunto del contenido del certificado o en un subconjunto de motivos de revocación. La CRL está firmada por la clave privada del expeditor de CRL – los puntos de distribución de CRL no tienen sus propios pares de claves. Sin embargo, para una CRL distribuida por el directorio, la CRL está almacenada en el asiento del punto de distribución de CRL que puede no ser el asiento del directorio del expeditor de la CRL. Si la CLR no contiene la extensión de punto de distribución expedidor, ni la extensión de punto de distribución de expedidor AA, ni tampoco el campo ámbito de CRL, la CRL contendrá asientos para todos los certificados de atributo que no hayan expirados y que son revocados emitidos por el expeditor de CRL. Si la CLR no contiene el campo de punto de distribución expedidor AA ni el campo de ámbito de CRL están ausentes, pero, sin embargo, contiene el punto de distribución expedidor, el ámbito de la CRL no incluirá los certificados de atributo.

Cuando aparece un certificado en una CRL, es posible borrarlo de las CRL posteriores después de su expiración.

Este campo se define del modo siguiente:

```
AAIssuingDistributionPoint EXTENSION : : = {
    SYNTAX AAIssuingDistPointSyntax
    IDENTIFIED BY id-ce-AAIssuingDistributionPoint }

AAIssuingDistPointSyntax ::= SEQUENCE {
    distributionPoint           [0] DistributionPointName OPTIONAL,
    onlySomeReasons            [1] ReasonFlags OPTIONAL,
    indirectCRL                 [2] BOOLEAN DEFAULT FALSE,
    containsUserAttributeCerts [3] BOOLEAN DEFAULT TRUE,
    containsAACerts             [4] BOOLEAN DEFAULT TRUE,
    containsSOAPublicKeyCerts  [5] BOOLEAN DEFAULT TRUE }
```

La componente **distributionPoint** contiene el nombre del punto de distribución en una o varias formas de nombre. Si el campo contiene **onlySomeReasons**, la CRL contendrá únicamente las revocaciones para los certificados de atributo correspondientes al motivo o motivos identificados, de lo contrario la CRL contendrá revocaciones para todos los motivos.

Si **indirectCRL** es verdadero, es probable que la CRL contenga notificaciones de revocación para certificados de atributo de autoridades diferentes de aquella que expide la CRL. La autoridad responsable de cada asiento viene indicada por la extensión de asientos CRL del expedidor de certificado en dicho asiento o de conformidad con las reglas por defecto descritas en 8.6.2.3. En dicha CRL, es responsabilidad del expedidor CRL garantizar que ésta sea completa en el sentido de que contenga todos los asientos de revocación, coherente con los indicadores **containsUserAttributeCerts**, **containsAACerts**, **containsSOAPublicKeyCerts** y **onlySomeReasons**, de todas las autoridades que identifican este expedidor CRL en su certificado de atributo.

Si **containsUserAttributeCerts** es verdadero, la CRL contendrá revocaciones para certificados de atributo expedidos a entidades extremas que no son AA. Si **containsAACerts** es verdadero, la CRL contendrá revocaciones para certificados de atributo expedidos a entidades que sí son AA.

Si **containsSOAPublicKeyCerts** es verdadero, la CRL contendrá revocaciones para certificados de clave pública expedidos a una entidad que es una SOA a efectos de gestión de privilegios (es decir certificados que contienen la extensión **SOAIdentifier**). En el caso de CRL distribuidas a través del directorio se aplican las siguientes reglas: si la CRL es una dCRL, se distribuirá mediante el atributo **deltaRevocationList** del punto de distribución asociado o, si no se ha identificado punto de distribución, a través del atributo **deltaRevocationList** del asiento de expedidor de CRL, independientemente de la configuración de los tipos de certificados abarcados por la CRL. Al menos que la CRL sea una CRL:

- Se distribuirá una CRL que no contenga una extensión **issuingDistributionPoint** que tenga fijado únicamente **containsAACerts** y/o **containsSOAPublicKeyCerts**, mediante el atributo **attributeAuthorityRevocationList** del punto de distribución asociado o, si no se ha identificado punto de distribución, a través del atributo **attributeAuthorityRevocationList** del asiento de emisor de CRL.
- Se distribuirá una CRL que no contenga una extensión **issuingDistributionPoint** que tenga fijado **containsUserAttributeCerts** (con o sin **containsAACerts** y/o **containsSOAPublicKeyCerts** también fijado), mediante el atributo **attributeCertificateRevocationList** del punto de distribución asociado o, si no hay un punto de distribución identificado, a través del atributo **attributeCertificateRevocationList** del asiento de expedidor de CRL.
- Se distribuirá, de conformidad con 8.6.2.2, una CRL que contenga una extensión **issuingDistributionPoint**.

Esta extensión es siempre es crítica. Un usuario de certificado que no entienda esta extensión no puede suponer que la CRL contiene una lista completa de certificados revocados de la autoridad identificada. La CRL que no contengan extensiones críticas contendrán todos los asientos actuales de CRL para todos los certificados de usuario y de autoridad revocados.

NOTA 1 – Los mecanismos mediante los cuales las autoridades comunican la información de revocación a la CRL están fuera del alcance de esta Especificación de directorio.

NOTA 2 – Cuando una autoridad publique una CRL con **containsAACerts** fijado a verdadero y **containsUserAttributeCerts** no puesto a verdadero, la autoridad garantizará que los certificados AA cubiertos por esta CRL contengan la extensión **basicAttConstraints**.

NOTA 3 – Cuando una autoridad publica una CRL con **containsSOAPublicKeyCerts** puesto a verdadero, garantizará que todos los certificados SOA abarcados por esta CRL contengan la extensión **SOAIdentifier**.





## 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
<b>Serie X</b>	<b>Redes de datos y comunicación entre sistemas abiertos</b>
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