UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Q.817

(01/2001)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Q: CONMUTACIÓN Y SEÑALIZACIÓN

Interfaz Q3

Certificados digitales de la infraestructura de claves públicas de la red de gestión de las telecomunicaciones y perfiles de listas de revocación de certificados

Recomendación UIT-T Q.817

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE Q

CONMUTACIÓN Y SEÑALIZACIÓN

SEÑALIZACIÓN EN EL SERVICIO MANUAL INTERNACIONAL	Q.1–Q.3
EXPLOTACIÓN INTERNACIONAL SEMIAUTOMÁTICA Y AUTOMÁTICA	Q.4–Q.59
FUNCIONES Y FLUJOS DE INFORMACIÓN PARA SERVICIOS DE LA RDSI	Q.60–Q.99
CLÁUSULAS APLICABLES A TODOS LOS SISTEMAS NORMALIZADOS DEL UIT-T	Q.100–Q.119
ESPECIFICACIONES DE LOS SISTEMAS DE SEÑALIZACIÓN N.° 4 Y N.° 5	Q.120–Q.249
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.° 6	Q.250–Q.309
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN R1	Q.310–Q.399
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN R2	Q.400–Q.499
CENTRALES DIGITALES	Q.500–Q.599
INTERFUNCIONAMIENTO DE LOS SISTEMAS DE SEÑALIZACIÓN	Q.600–Q.699
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.° 7	Q.700–Q.799
INTERFAZ Q3	**Q.800–Q.849**
SISTEMA DE SEÑALIZACIÓN DIGITAL DE ABONADO N.° 1	Q.850–Q.999
RED MÓVIL TERRESTRE PÚBLICA	Q.1000–Q.1099
INTERFUNCIONAMIENTO CON SISTEMAS MÓVILES POR SATÉLITE	Q.1100–Q.1199
RED INTELIGENTE	Q.1200–Q.1699
REQUISITOS Y PROTOCOLOS DE SEÑALIZACIÓN PARA IMT-2000	Q.1700–Q.1799
RED DIGITAL DE SERVICIOS INTEGRADOS DE BANDA ANCHA (RDSI-BA)	Q.2000–Q.2999

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

Recomendación UIT-T Q.817

Certificados digitales de la infraestructura de claves públicas de la red de gestión de las telecomunicaciones y perfiles de listas de revocación de certificados

Resumen

En esta Recomendación se indica la forma en que pueden utilizarse los certificados digitales y las listas de revocación de certificados en la RGT y se proporcionan los requisitos necesarios para el uso de certificados y de extensiones de la lista de revocación de certificados.

Orígenes

La Recomendación UIT-T Q.817, preparada por la Comisión de Estudio 4 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 19 de enero de 2001.

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

Recomendación UIT-T Q.817

Certificados digitales de la infraestructura de claves públicas de la red de gestión de las telecomunicaciones y perfiles de listas de revocación de certificados

1 Alcance, objetivo y aplicación

1.1 Alcance

Esta Recomendación tiene por objeto promover el interfuncionamiento entre elementos de la red de gestión de las telecomunicaciones (RGT) que utilizan la infraestructura de claves públicas (PKI) como soporte de las funciones relacionadas con la seguridad. Se aplica a todas las interfaces y realizaciones de la RGT. Es independiente de la pila de protocolos de comunicación o del protocolo de gestión de red que se emplee. Las posibilidades de utilización que ofrece la PKI se pueden aprovechar en una amplia gama de funciones de seguridad, tales como las de autenticación, integridad, no repudio e intercambio de claves (UIT-T M.3016). Sin embargo, la presente Recomendación no especifica si deben implementarse esas funciones, con o sin PKI.

La PKI ha resultado ser un método eficaz y aplicable a escala variable a efectos de autenticación segura, no repudio y de distribución y gestión de claves de criptación, y de otros parámetros relacionados con la seguridad. La PKI se basa en certificados digitales. La Recomendación UIT-T X.509 especifica el formato de esos certificados. Los certificados digitales X.509 pueden contener cualquier número de extensiones. Para que una PKI sustente el interfuncionamiento entre elementos de la RGT, dichos elementos deben poder procesar el mismo conjunto de extensiones de certificados. En teoría, todos los elementos de una RGT deberán mostrar el mismo comportamiento al procesar extensiones de certificados. La presente Recomendación especifica las extensiones de certificados que ha de sustentar una PKI de RGT, para promover un interfuncionamiento seguro entre elementos de RGT. Proporciona además comportamientos por defecto para el procesamiento de esas extensiones.

A fin de facilitar la armonización con otras industrias, la presente Recomendación toma como precedentes la serie de Recomendaciones UIT-T X.500, en particular la UIT-T X.509, y la Petición de Comentarios (RFC) relacionada con la PKI 2459 del Grupo de Tareas sobre Ingeniería de Internet (IETF).

1.2 Objetivo

El objetivo de esta Recomendación es proporcionar un mecanismo interoperable y aplicable a escala variable de distribución y gestión de claves dentro de una RGT, a través de todas las interfaces, y de apoyo al servicio de no repudio a través de la interfaz X.

1.3 Aplicación

Esta Recomendación se aplica a todas las interfaces Q y X de la RGT, con independencia del protocolo de comunicación. Se refiere a la información sobre claves públicas y revocación de claves públicas utilizada por, o intercambiada entre, elementos de RGT.

Según los requisitos concretos de la aplicación, la RGT podría utilizar, en lugar de certificados, claves públicas definidas previamente que se distribuyen por medios que están fuera del alcance de esta Recomendación.

2 Referencias normativas

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas la Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Normas internacionales

– UIT-T M.3016 (1998), *Visión general de la seguridad en la red de gestión de las telecomunicaciones.*

– UIT-T Q.812 (1997), *Perfiles de protocolo de capa superior para las interfaces Q3 y X.*

– UIT-T X.500 (2001) | ISO/CEI 9594-1:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Visión de conjunto de conceptos, modelos y servicios.*

– UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marco para certificados de claves públicas y de atributos.*

– UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica.*

– UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de objetos de información.*

– UIT-T X.682 (1997) | ISO/CEI 8824-3:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones.*

– UIT-T X.683 (1997) | ISO/CEI 8824-4:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de especificaciones de notación de sintaxis abstracta uno.*

– UIT-T X.690 (1997) | ISO/CEI 8825-1:1998, *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida.*

– UIT-T X.736 (1992) | ISO/CEI 10164-7:1992, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función señaladora de alarmas de seguridad.*

– UIT-T X.740 (1992) | ISO/CEI 10164-8:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de pista de auditoría de seguridad.*

2.2 Otras normas

– IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure – Certificate and CRL Profile.*

– IETF RFC 2251 (1997), *Lightweight Directory Access Protocol (v3).*

3 Definiciones

Esta Recomendación utiliza las definiciones de servicios de seguridad y mecanismos de seguridad especificados en la UIT-T M.3016. Además, utiliza las definiciones de los elementos de una infraestructura de claves públicas especificados en la RFC 2459.

4 Abreviaturas

ASN.1 Notación de sintaxis abstracta uno (*abstract syntax notation one*)

BER Reglas básicas de codificación (*basic encoding rules*)

CA Autoridad de certificación (*certification authority*)

CRL Lista de revocación de certificados (*certificate revocation list*)

DER Reglas de codificación distinguida (*distinguished encoding rules*)

IETF Grupo de tareas especiales de ingeniería en Internet (*internet engineering task force*)

OID Identificador de objeto (*object identifier*)

PKCS Criptosistema de claves públicas (*public key cryptography standard*)

PKI Infraestructura de claves públicas (*public key infrastructure*)

RA Autoridad de registro (*registration authority*)

RFC Petición de comentarios (*request for comments*)

RSA Rivest Shamir Adelman

UIT-T Unión Internacional de Telecomunicaciones – Sector de Normalización de las Telecomunicaciones

5 Visión de conjunto

La **infraestructura de claves públicas (PKI)** se está revelando como la solución de menor costo, aplicable a escala variable, para la seguridad de la RGT. La presente Recomendación tiene por objeto promover el interfuncionamiento entre componentes de la PKI de diferentes suministradores de productos y proveedores de servicios, así como el interfuncionamiento entre diferentes empresas o administraciones. En esta cláusula se da una visión de conjunto de alto nivel de la PKI de la RGT.

La PKI de la RGT consta de los **componentes** siguientes:

Una **autoridad de certificación (CA)**, expedidora de **certificados de clave pública** para todas las entidades de RGT que necesitan comunicaciones seguras, así como para cualquier entidad externa que necesite comunicar de manera segura con entidades de RGT. La CA expide también certificados a autoridades de certificación ajenas a la RGT. La CA publica, según se requieran, **listas de revocación de certificados (CRL)**. Una CRL contiene los números de serie de los certificados que han sido revocados (por ejemplo, porque la clave ha quedado en situación comprometida o porque el sujeto de que se trate ya no forma parte de la empresa) y cuyo periodo de validez no ha expirado todavía. La CA emplea normalmente un ordenador a prueba de manipulaciones guardado con la máxima seguridad[1]. El término CA se utiliza también para referirse a una organización (más bien que a un dispositivo) que expide certificados como un servicio, percibiendo normalmente por ello una tasa.

El formato más frecuente de un certificado es tal como se especifica en UIT-T X.509. La UIT-T X.509 define varios campos obligatorios. Además, prevé la adición de un número cualquiera de **extensiones**. Cada extensión se marca como crítica o no crítica. Si una entidad que procesa un certificado encuentra una extensión no crítica que no reconoce, puede hacer caso omiso de la misma. Si una entidad que procesa un certificado encuentra una extensión crítica que no reconoce, debe rechazar el certificado. La UIT-T X.509 permite también extensiones de las CRL y de asientos de una CRL particular. El interfuncionamiento en una RGT o entre varias RGT requiere, como mínimo,

[1] Los requisitos de seguridad física y la seguridad de los sistemas de un ordenador a prueba de manipulaciones quedan fuera del alcance de la presente Recomendación.

el pleno acuerdo sobre todas las extensiones críticas (si hay alguna) de los certificados utilizados en aplicaciones de RGT.

Una **autoridad de registro (RA)**, verificadora de la autenticidad de cada entidad (NE (elemento de red), OS (sistema de operaciones), WS (estación de trabajo), empleado, cliente, suministrador, etc.) que pudiera recibir un certificado de clave pública de la CA de la RGT. La RA suele estar formada por un pequeño número de administradores de seguridad con acceso a la CA.

La RA publica normalmente una **declaración de política de certificación** (CPS, *certification policy statement***)** que especifica las condiciones (por ejemplo, verificación de identidades) en que se expediría un certificado.

La PKI incluye un **directorio** para el almacenamiento y la distribución de los certificados y las CRL. La UIT-T X.500 contiene la base del directorio. En UIT-T Q.812 figura un perfil para la utilización del protocolo de acceso al directorio (DAP, *directory access protocol*) X.500. Sin embargo, los directorios basados en el perfil de PKI del IETF del LDAP (lightweight DAP, un subconjunto del DAP), versión 3, pueden estar disponibles con mayor facilidad que los directorios basados en UIT-T X.500.

Cualquier **entidad de RGT** necesitará interactuar con el directorio de PKI de RGT para extraer y recibir certificados de otras entidades, así como listas de revocación de certificados (las CRL). Tendrá que poder procesar los certificados y las CRL. Cualquier entidad de RGT necesitará también la capacidad de construir y procesar trayectos de certificación

Los componentes de PKI de RGT han de interactuar mediante **protocolos** normalizados. En la figura 1 se ilustran las interacciones entre componentes de PKI de RGT.

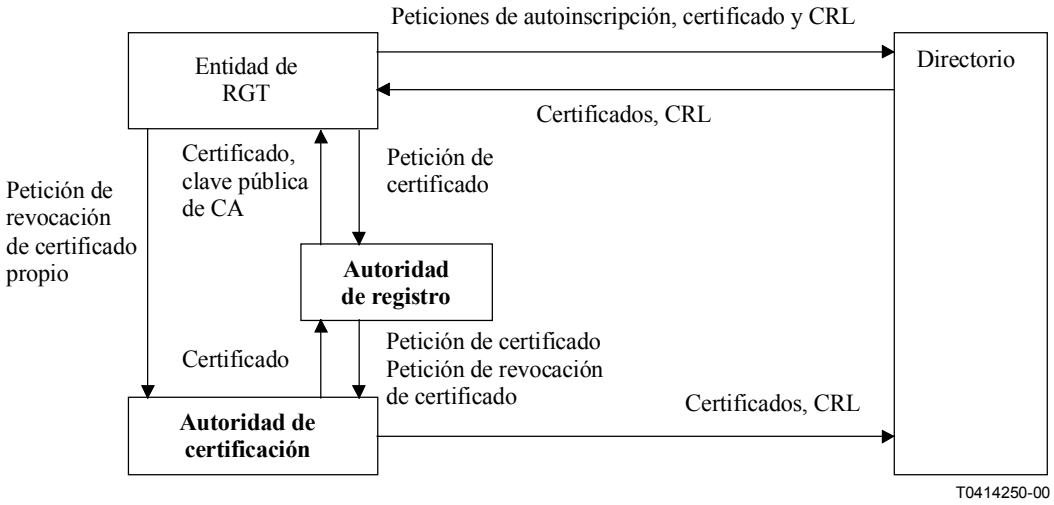

Figura 1/Q.817 – Interacción entre componentes de PKI de RGT

6 Extensiones de certificados

La PKI del IETF utiliza los **certificados** definidos en UIT-T X.509. Ese formato permite un cierto número de **extensiones**. La PKI del IETF incluye numerosas extensiones, que se indican más adelante. Las extensiones se definen en la Petición de Comentarios del IETF 2459. Esta Recomendación se basa en la RFC 2459 que es parte normativa de la presente especificación por referencia.

En esta Recomendación figura un perfil específico de RGT de la RFC 2459, sin repetir texto de esa RFC.

Esta Recomendación contiene las directrices, indicadas a continuación, de aplicación por defecto en el procesamiento de extensiones de certificados. Cada administración puede elegir comportamientos diferentes en base a su política de seguridad:

- Si una extensión no crítica que DEBE estar presente, está en cambio ausente o tiene un valor no válido, el certificado deberá ser aceptado y procesado. Al mismo tiempo, el evento será registrado en un registro de auditoría de seguridad y se enviará una alarma de seguridad. Tanto el registro de auditoría de seguridad como la alarma de seguridad deberán incluir una copia del certificado, una copia del mensaje que contiene el certificado, indicación de la hora en que se recibió el certificado y la entidad que detectó la discrepancia.
- Si está presente una extensión no crítica que debiera no estarlo, el certificado deberá ser aceptado y procesado. Al mismo tiempo, el evento será registrado en un registro de auditoría de seguridad y se enviará una alarma de seguridad de bajo nivel. Tanto el registro de auditoría de seguridad como la alarma de seguridad deberán incluir una copia del certificado, una copia del mensaje que contiene el certificado, indicación de la hora en que se recibió el certificado y la entidad que detectó la discrepancia.
- Si una entidad final no reconoce una extensión crítica, no proseguirá con el procesamiento del certificado. Al mismo tiempo, el evento será registrado en un registro de auditoría de seguridad y se enviará una alarma de seguridad. Tanto el registro de auditoría de seguridad como la alarma de seguridad deberán incluir una copia del certificado, una copia del mensaje que contiene el certificado, indicación de la hora en que se recibió el certificado y la entidad que detectó la discrepancia. La entidad final responderá a la entidad que envía el certificado (explícitamente o implícitamente por referencia) con un mensaje en el que indique que el certificado contiene una extensión crítica no reconocida.
- Si una entidad final encuentra un valor no válido en una extensión crítica, no proseguirá con el procesamiento del certificado. Al mismo tiempo, el evento será registrado en un registro de auditoría de seguridad y se enviará una alarma de seguridad. Tanto el registro de auditoría de seguridad como la alarma de seguridad deberán incluir una copia del certificado, una copia del mensaje que contiene el certificado, indicación de la hora en que se recibió el certificado y la entidad que detectó la discrepancia. La entidad final no responderá a la entidad que envía el certificado (ni explícitamente ni implícitamente por referencia).

A menos que se indique otra cosa, estas extensiones pueden ser utilizadas tanto en certificados de CA como en certificados de entidad final.

6.1 Identificador de clave de autoridad

Esta extensión se define y requiere en UIT-T X.509.

Esta extensión la requieren la RFC 2459 y la presente Recomendación en todos los certificados conformes, excepto en los certificados firmados por la propia CA en donde puede ser omitida.

Esta extensión es siempre no crítica.

El identificador de clave será la representación BIT STRING de troceo SHA-1 de 160 bits de la clave pública (excluyendo el rótulo, la longitud y el número de bits no utilizados). La RFC 2459 indica la construcción de la BIT STRING (cadena de bits) para diversos tipos de clave pública.

6.2 Identificador de clave de sujeto

Esta extensión se define y requiere en UIT-T X.509.

Esta extensión la requiere la RFC 2459.

Esta extensión la requiere esta Recomendación en todos los certificados de CA conformes.

Esta extensión es facultativa para certificados de entidad final que interactúan a través de la interfaz X.

No deberá ser utilizada para certificados de entidad final que interactúan solamente a través de interfaces Q.

Esta extensión es siempre no crítica.

El identificador de clave será la representación BIT STRING de troceo SHA-1 de 160 bits de la clave pública (excluyendo el rótulo, la longitud y el número de bits no utilizados). La RFC 2459 indica la construcción de la BIT STRING (cadena de bits) para diversos tipos de clave pública.

6.3 Utilización de claves

Esta extensión se define y requiere en UIT-T X.509.

Esta extensión es facultativa para certificados de entidad final que interactúan a través de la interfaz X.

No deberá ser utilizada para certificados de entidad final que interactúan solamente a través de interfaces Q.

Esta extensión será ser crítica si está presente.

6.4 Periodo de utilización de clave privada

Esta extensión se define y requiere en UIT-T X.509.

Esta extensión no se recomienda en la RFC 2459.

Esta extensión es facultativa en esta Recomendación; si está presente, deberá marcarse como no crítica.

6.5 Políticas de certificados

En los certificados que se han de utilizar a través de la interfaz Q esta extensión es facultativa, no se recomienda su utilización y deberá marcarse como no crítica.

En certificados que se han de utilizar a través de la interfaz X esta extensión es facultativa, se recomienda su utilización y puede marcarse como crítica.

Esta extensión no se necesita para entidades que interactúan solamente a través de la interfaz Q. La RA puede decidir sobre políticas de certificación diferentes para elementos de RGT diferentes, imponiendo políticas más estrictas para elementos con privilegios de acceso más amplios. La función de control de acceso a los recursos de la RGT se basaría entonces solamente en la identidad autenticada del iniciador y los privilegios de acceso de ese iniciador, no en la política de certificación del certificado del iniciador.

Esta extensión es de utilidad para entidades que interactúan a través de la interfaz X, por ello, esas entidades deberán poder procesarla. Se recomienda la inclusión de esta extensión para certificados expedidos a entidades que, según lo previsto, van a interactuar a través de la interfaz X.

Si esta extensión está presente, deberá constar de un solo OID.

6.6 Correspondencia de políticas

La RFC 2459 especifica que esta extensión es siempre no crítica y sólo puede estar presente en certificados de CA.

Esta extensión no se necesita para certificados de CA de RGT si el certificado se expide solamente dentro de esa RGT (es decir, para interacciones de interfaz Q). A las entidades finales que interactúan solamente a través de interfaces Q no se les exige que procesen esta extensión.

Esta extensión puede estar presente en certificados de CA utilizados para interacciones de interfaz X.

6.7 Nombre alternativo de sujeto

Esta extensión no se necesita para interacciones de RGT a través de la interfaz Q. Si está presente, deberá estar marcada como no crítica (lo que significa que debe estar presente el nombre distinguido del sujeto). A las entidades finales que interactúan solamente a través de interfaces Q no se les exige que procesen esta extensión.

Esta extensión puede ser de utilidad para algunas interacciones a través de la interfaz X. En tales casos su utilización deberá ser tal como se especifica en la RFC 2459.

6.8 Nombre alternativo de expedidor

A las entidades de RGT no se les exige que procesen esta extensión. Si está presente, deberá estar marcada como no crítica.

6.9 Atributos de directorio de sujeto

Esta extensión no se recomienda para aplicaciones de RGT. Su utilización es facultativa.

Si está presente, deberá estar marcada como no crítica.

6.10 Constricciones básicas

Esta extensión deberá estar presente en todos los certificados de CA y estar marcada como crítica.

Esta extensión no estará presente en ningún certificado de entidad final.

6.11 Constricciones de nombre

Esta extensión puede estar presente en certificados de CA y deberá estar marcada como crítica.

Esta extensión no estará presente en ningún certificado de entidad final.

6.12 Constricciones de políticas

Esta extensión es facultativa. Puede estar marcada como crítica o como no crítica.

Si el certificado es expedido por una CA a otra CA del mismo dominio de seguridad, se recomienda que esta extensión se marque como no crítica. En este caso no se requiere que los elementos de red (NE) la procesen.

Si el certificado es expedido por una CA a otra CA de otro dominio de seguridad o de otra administración, esta extensión deberá marcarse como crítica. Administraciones diferentes están siempre en dominios de seguridad diferentes, por lo que es preciso que las pasarelas que soportan las interfaces X procesen esta extensión.

6.13 Utilización de clave extendida

Esta extensión no será utilizada para aplicaciones de RGT. Sin embargo, una entidad de RGT que soporta interacciones de interfaz X puede encontrar este campo en certificados expedidos por una CA externa.

Esta extensión no se utilizará en certificados que vayan a ser utilizados para aplicaciones de interfaz Q.

Esta extensión es facultativa en certificados que vayan a ser utilizados para aplicaciones de interfaz X.

Si esta extensión está presente, deberá estar marcada como crítica.

6.14 Puntos de distribución de CRL

Esta extensión se recomienda para certificados utilizados a través de la interfaz X. Esta extensión es facultativa para certificados utilizados en transacciones de interfaz Q.

NOTA – Se solicitan contribuciones relativas a la criticidad de esta extensión.

6.15 Acceso a información de autoridad

Esta extensión no se utilizará en certificados que vayan a ser utilizados a través de interfaces Q. Puede ser utilizada en certificados que vayan a ser utilizados a través de interfaces X. Si está presente, deberá estar marcada como no crítica.

7 Extensiones de lista de revocación de certificados (CRL)

La PKI del IETF utiliza las **CRL** definidas en la versión 1993 de UIT-T X.509. Especifica además varias extensiones de la CRL básica. (Las extensiones se definen en la Petición de Comentarios 2459.)

7.1 Identificador de clave de autoridad

Esta extensión deberá estar presente y estar marcada como no crítica.

7.2 Nombre alternativo de expedidor

Esta extensión no deberá ser utilizada en transacciones de interfaz Q de RGT. Puede estar presente en certificados utilizados a través de una interfaz X. Si está presente, deberá estar marcada como no crítica.

7.3 Número de CRL

Esta extensión deberá estar presente y estar marcada como no crítica.

7.4 Indicador de CRL delta

Esta extensión es facultativa para las CRL que sustentan transacciones de interfaz Q. No es necesaria si el administrador de la RGT decide no expedir listas de revocación de certificados (CRL) delta. La utilización de esta extensión ofrece al administrador de la RGT más flexibilidad en la distribución de información de la CRL. Puede estar presente en CRL externas. Si está presente, deberá estar marcada como crítica.

7.5 Punto de distribución expedidor

Esta extensión es facultativa. Para aplicaciones de RGT no deberá utilizarse el campo OPTIONAL (facultativo) onlySomeReasons.

Puede estar presente en CRL externas. Si está presente, deberá estar marcada como crítica.

8 Extensiones para asientos individuales en las CRL

La PKI del IETF indica varias extensiones para **asientos individuales en una CRL**. (Las extensiones se definen en la Petición de Comentarios 2459.)

8.1 Código de motivo

Esta extensión es facultativa. Si está presente, deberá estar marcada como no crítica.

8.2 Código de instrucción de retención

Esta extensión es facultativa. No es necesaria en las CRL que sustentan transacciones de interfaz Q. Esta extensión puede estar presente en CRL externas. Si está presente esta extensión, deberá estar marcada como no crítica.

8.3 Fecha de no validez

Esta extensión es facultativa. No es necesaria en las CRL que sustentan transacciones de interfaz Q. Esta extensión puede estar presente en CRL externas. Si está presente, deberá estar marcada como no crítica.

8.4 Expedidor de certificado

Esta extensión no deberá utilizarse para listas de revocación de certificados (CRL) que sustentan transacciones de interfaz Q. Esta extensión puede estar presente en CRL externas. Si está presente, deberá estar marcada como crítica.

SERIES DE RECOMENDACIONES DEL UIT-T

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

Ginebra, 2001