Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1341

(09/2015)

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

Aplicaciones y servicios con seguridad – Recomendaciones relacionadas con la PKI

Protocolos de transferencia de correo certificado y de oficina postal certificada

Recomendación UIT-T X.1341

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–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	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Recomendaciones relacionadas con la PKI	**X.1340–X.1349**
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

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

Recomendación UIT-T X.1341

Protocolos de transferencia de correo certificado y de oficina postal certificada

Resumen

En la presente Recomendación se define el Protocolo de transferencia de correo certificado (CMTP) y el Protocolo de oficina postal certificada (CPOP) con el fin de fomentar los intercambios de correos electrónicos certificados en todo el mundo y de manera segura proporcionando confidencialidad, identificación de los corresponsales e integridad y evitando el repudio.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1341	2015-09-17	17	11.1002/1000/12352

Palabras clave

Confidencialidad, integridad, no repudio, protocolo de oficina postal (POP), protocolo de oficina postal certificada (CPOP), protocolo de transferencia de correo certificado (CMTP), protocolo de transferencia de correo simple (SMTP) , seguridad

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Introducción

En esta Recomendación se amplían las capacidades del Protocolo de transferencia de correo simple (SMTP) y del Protocolo de oficina postal versión 3 (POP3) a fin de soportar la autentificación, la seguridad y el no repudio.

Para ello se especifican dos protocolos:

– el Protocolo de transferencia de correo certificado (CMTP), que es una extensión del Protocolo de transferencia de correo simple (SMTP), es el protocolo que soporta las comunicaciones entre el emisor de los correos electrónicos y un servidor de correo, denominado servidor de correo certificado (Cmail);

– el Protocolo de oficina postal certificada (CPOP), que es una extensión del Protocolo de oficina postal versión 3 (POP3), es el protocolo que soporta las comunicaciones entre el receptor de los correos electrónicos y el servidor Cmail.

En SMTP y POP3 el tipo de mensaje se identifica mediante una instrucción, es decir, una palabra clave al inicio del mensaje. En CMTP y CPOP se han definido nuevas instrucciones y se han ampliado algunas de las de SMTP y POP3. Concretamente, se han ampliado algunas de las instrucciones para transportar notificaciones (documentos electrónicos) que permitan documentar y verificar las diversas etapas de la comunicación, desde el emisor al receptor.

CMTP y CPOP también introducen el concepto de servidor Cmail, que es una parte activa de la comunicación entre el emisor y el receptor, y permite certificar que efectivamente se ha llevado a cabo el intercambio entre las dos partes.

El correo certificado supone que se hay una infraestructura de clave pública (PKI) preexistente.

En el Anexo A, que forma parte integrante de esta Recomendación, se presenta la especificación formal de las notificaciones utilizando la técnica de Notación de definición de esquema XML (XSD).

En el Anexo B, que forma parte integrante de esta Recomendación, se presenta la especificación formal de las notificaciones, utilizando la Notación de sintaxis abstracta uno (ASN.1).

En el Anexo C, que forma parte integrante de esta Recomendación, se especifican los requisitos para los certificados de clave pública emitidos a los clientes (emisor y receptor de los correos electrónicos) y los servidores Cmail.

En el Anexo D, que forma parte integrante de esta Recomendación, se especifican los requisitos sobre la utilización de la especificación de la Seguridad de la capa de transporte (TLS).

En el Anexo E, que forma parte integrante de esta Recomendación, se especifican los identificadores de objeto definidos para servidores Cmail.

Recomendación UIT-T X.1341

Protocolos de transferencia de correo certificado y de oficina postal certificada

1 Alcance

En la presente Recomendación se especifica el procedimiento para que los correos electrónicos sean fiables en cuanto a identificación y confidencialidad se refiere.

El Protocolo de transferencia de correo certificado/Protocolo de oficina postal certificada (CMTP/CPOP) permite:

– resolver problemas de repudio con la utilización de la firma electrónica;

– resolver problemas de confidencialidad con la utilización de la encriptación;

– crear notificaciones de depósito, notificaciones de tránsito y notificaciones de recepción fiables;

– utilizar un servidor de correo certificado (Cmail) para rastrear los correos certificados y evitar su pérdida durante el proceso;

– utilizar una conexión de seguridad de capa de transporte (TLS) para ofrecer una identificación más fuerte. El servidor Cmail exige este mayor nivel de identificación.

El cumplimiento de la presente Recomendación no se considerará, ni podrá ser utilizado, como prueba del cumplimiento de ningún reglamento, ley o política nacional o regional. Los medios técnicos, organizativos y de procedimiento descritos en la presente Recomendación no garantizan en modo alguno el nivel de seguridad que un reglamento, ley o política en concreto, nacional o regional, pudiera exigir para una determinada correspondencia.

2 Referencias

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 las 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. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.520] Recomendación UIT-T X.520 (2012) | ISO/CEI 9594-6:2014, *Tecnología de la Información – Interconexión de sistemas abiertos – El directorio: Tipos de atributos seleccionados.*

[UIT-T X.680] Recomendación UIT-T X.680 (2008) | ISO/CEI 8824-1:2008, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica*.

[UIT-T X.690] Recomendación UIT-T X.690 (2008) | ISO/CEI 8825-1:2008, *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.693] Recomendación UIT-T X.693 (2008) | ISO/CEI 8825-4:2008, *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Reglas de codificación del lenguaje de marcaje extensible.*

[ISO 3166-1] ISO 3166-1:2013, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.*

[IETF RFC 822] IETF RFC 822 (1982), *Standard for the format of ARPA Internet text messages*.

[IETF RFC 1939] IETF RFC 1939 (1996), *Post office protocol – Version 3*.

[IETF RFC 2045] IETF RFC 2045 (1996), *Multipurpose internet mail extensions (MIME) – Part One: Format of internet message bodies*.

[IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) Protocol – Version 1.2*.

[IETF RFC 5321] IETF RFC 5321 (2008), *Simple mail transfer protocol*.

[XML] W3C Recommendation XML1.0 (2000), *Extensible markup language (XML) 1.0 (fifth edition).*

[XSD] W3C Recommendation XML Schema (2001), *XML schema Part 1: Structures*.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 autoridad de certificación (CA, *certification authority*) [b-UIT-T X.509]: autoridad a la cual uno o más usuarios han confiado la creación y asignación de certificados de clave pública. Facultativamente, la autoridad de certificación puede crear las claves de los usuarios.

3.1.2 validación de certificado [b-UIT-T X.509]: proceso para asegurar que un certificado era válido en un momento determinado, con posible inclusión de la construcción y el procesamiento de un trayecto de certificación, y que asegura que todos los certificados en dicho trayecto eran válidos (es decir, no habían caducado ni estaban revocados) en un determinado momento.

3.1.3 función de troceo [b-UIT-T X.509]: función (matemática) que hace corresponder valores de un dominio grande (posiblemente muy grande) con una gama más pequeña. La función de troceo es "buena" cuando los resultados de la aplicación de la función a un (gran) conjunto de valores en el dominio se distribuyen uniformemente (y aparentemente al azar) en la gama.

3.1.4 clave privada [b-UIT-T X.509]: (en un criptosistema de claves públicas) clave de un par de claves de usuario que sólo es conocida por ese usuario.

3.1.5 clave pública [b-UIT-T X.509]: (en un criptosistema de claves públicas) clave de un par de claves de usuario que es conocida públicamente.

3.1.6 certificado de clave pública (PKC, *public-key certificate*) [b-UIT-T X.509]: clave pública de un usuario, junto con alguna otra información, hecha infalsificable por firma digital con la clave privada de la autoridad de certificación que la emitió.

3.1.7 infraestructura de claves públicas (PKI, *public-key infrastructure*) [b-UIT-T X.509]: infraestructura capaz de soportar la gestión de claves públicas para los servicios de autentificación, criptación, integridad o no repudio.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 correo certificado: correo electrónico intercambiado utilizando el Protocolo de transferencia de correo certificado (CMTP) y el Protocolo de oficina postal certificada (CPOP).

3.2.2 protocolo de transferencia de correo certificado (CMTP, *certified mail transfer protocol*): protocolo de capa de aplicación por una conexión mediante el protocolo de control de transmisión/protocolo Internet (TCP/IP) basada en protocolo de transferencia de correo simple (SMTP) utilizado para enviar correo certificado.

3.2.3 protocolo de oficina postal certificada (CPOP, *certified post office protocol*): protocolo de capa de aplicación por una conexión mediante el protocolo de control de transmisión/protocolo Internet (TCP/IP) basada en protocolo de oficina postal versión 3 (POP3) utilizado para recibir correo certificado.

3.2.4 servidor Cmail: entidad fiable que participa en las transacciones de correo certificado.

3.2.5 notificación de depósito: documento electrónico firmado por el emisor y el servidor Cmail que contiene información que permite certificar que se ha depositado un correo certificado.

3.2.6 notificación de recepción: documento electrónico firmado por el receptor y el servidor Cmail que contiene información que permite certificar que el receptor ha recibido un correo certificado.

3.2.7 notificación de tránsito: documento electrónico firmado por los servidores Cmail participantes en la transacción y que contiene información que permite certificar que el correo certificado se transmitió al servidor Cmail.

3.2.8 protocolo de oficina postal versión 3 (POP3): protocolo de capa de aplicación por una conexión mediante el Protocolo de control de transmisión/Protocolo Internet (TCP/IP) utilizado para recibir correo electrónico.

3.2.9 protocolo de transferencia de correo simple (SMTP): protocolo de capa de aplicación por una conexión mediante el Protocolo de control de transmisión/Protocolo Internet (TCP/IP) utilizado para enviar correo electrónico.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

AES Norma de encriptación avanzada (*advanced encryption standard*)

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

CA Autoridad de certificación (*certification authority*)

CBC Concatenación de bloques cifrados (*cipher block chaining*)

Cmail Correo certificado (*certified mail*)

CMTP Protocolo de transferencia de correo certificado (*certified mail transfer protocol*)

CPOP Protocolo de oficina postal certificada (*certified post office protocol*)

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

DNS Sistema de nombre de dominio (*domain name system*)

id Identidad

MIME Ampliaciones polivalentes de correo de Internet (*multipurpose internet mail extensions*)

PKI Infraestructura de clave pública (*public-key infrastructure*)

POP3 Protocolo de oficina postal versión 3 (*post office protocol version 3*)

RSA Algoritmo Rivest, Shamir y Adleman (*Rivest, Shamir and Adleman algorithm*)

RSCK Clave de cifrado simétrico aleatorio (*random symmetric cipher key*)

S/MIME Ampliaciones polivalentes/seguras de correo de Internet (*secure/multipurpose Internet mail extensions*)

SMTP Protocolo de transferencia de correo simple (*simple mail transfer protocol*)

TCP/IP Protocolo de control de transmisión/protocolo Internet (*transmission control protocol/Internet protocol*)

TLS Seguridad de capa de transporte (*transport layer security*)

UTF-8 Conjunto universal de caracteres (*universal character set*) – Transformación format-8 (*transformation format-8*)

XER Reglas de codificación XML (*xml encoding rules*)

XML Lenguaje de marcaje extensible (*eXtensible markup language*)

XSD Definición de esquema XML (*XML schema definition*)

5 Convenios

Ninguno.

6 Conceptos básicos del correo certificado

En las comunicaciones por correo electrónico tradicionales que utilizan el Protocolo de transferencia de correo simple (SMTP) y el Protocolo de oficina postal versión 3 (POP3), un receptor de correo electrónico puede negar haberlo recibido, incluso cuando se añadan a la Serie de protocolos las ampliaciones seguras/polivalentes de correo de Internet (S/MIME). S/MIME permite encriptar los mensajes y autentificar al emisor, pero no ofrece pruebas de la entrega del correo.

En esta Recomendación se especifican una serie de protocolos, denominada de correo certificado, que está formada por el Protocolo de transferencia de correo certificado (CMTP) y el Protocolo de oficina postal certificada (CPOP).

En las comunicaciones SMTP/POP3, el servidor de correo no es parte activa de la comunicación, sino que únicamente reenvía los mensajes a medida que los recibe, cuando el receptor se registra en el servidor de correo. Esto es así aun cuando se utilizan S/MIME.

En el correo certificado, el servidor de correo participa activamente en la comunicación entre el emisor y el receptor de manera que el servidor Cmail puede verificar que el receptor ha aceptado recibir el correo. El correo se envía encriptado para que el servidor Cmail no pueda leer el contenido real del correo electrónico. A continuación se resume brevemente el procedimiento, cuya especificación detallada puede encontrarse en la cláusula 8.

Las interacciones entre el emisor y el servidor Cmail se especifican en la cláusula 8.

Las interacciones entre el receptor y el servidor Cmail se especifican en la cláusula 9.

7 Tipos de instrucciones de correo certificado

El correo certificado utiliza una combinación de las actuales instrucciones SMTP y POP3, algunas instrucciones SMTP y POP3 mejoradas y algunas instrucciones específicas del correo certificado. En los Cuadros 1 y 2 las instrucciones que no tienen equivalente en SMTP/POP3 se denominan "Adicional". Las instrucciones mejoradas con respecto a SMTP/POP3 se denominan "Modificada", y las instrucciones SMTP/POP3 que se utilizan tal cual se marcan con "Sin modificación".

Un tipo de instrucción se define como una palabra clave en mayúsculas que identifica un tipo de mensaje concreto y algunas especificaciones adicionales para ese tipo de mensaje.

7.1 Tipos de instrucciones CMTP

Cuadro 1 – Instrucciones CMTP

Instrucción	Función de la instrucción
CELO Adicional	Permite al servidor identificar su procesamiento de las instrucciones CMTP
DELV Adicional	Identifica el modo de entrega: certifiedMail
MAIL FROM Modificada	Identifica al emisor del mensaje; utilizado como "MAIL FROM". Si la cuenta existe en el servidor, devuelve un base64 del certificado de clave pública del emisor conocido
RCPT TO Modificada	Identifica a los receptores del mensaje; utilizado en formato "RCPT TO". Si la cuenta existe en el servidor, devuelve un base64 del certificado de clave pública del emisor conocido. Si la cuenta existe en otro servidor CMTP con el que se han realizado intercambios de claves, el servidor pregunta al segundo servidor y envía un base64 del certificado de clave pública perteneciente al receptor conocido con la instrucción CHCK RCPT
CHCK RCPT Adicional	Se envía únicamente si el receptor está anexado a un servidor Cmail distinto del servidor Cmail del emisor
DATA Modificada	Enviada por un cliente para iniciar la transferencia del contenido del mensaje, el servidor devuelve una notificación de depósito firmada por el servidor y que deberá firmar el emisor
DEPO Adicional	Enviada por un cliente para iniciar la transferencia de la notificación de depósito de contenido firmada por el servidor y contrafirmada por el emisor
SEND EVLP Adicional	Remite el sobre de un servidor Cmail a otro
HELP Sin modificación	Devuelve una lista de instrucciones soportadas por el servidor CMTP
QUIT Sin modificación	Termina la sesión

7.2 Tipos de instrucciones CPOP

Cuadro 2 – Instrucciones CPOP

Instrucción	Función de la instrucción
USER Sin modificación	Utilizada para especificar el nombre del usuario que se registra
PASS Sin modificación	Contraseña del usuario que se registra
LIST Modificada	Utilizada para establecer una lista de los mensajes y su tamaño combinado. Por ejemplo, invocar la instrucción LIST sin parámetros devolverá dos mensajes+OK (320 bytes) y la lista de los mensajes: identidad (id), longitud y modo de entrega (si procede), como CertifiedMail
RETR Modificada	Cuando N es un número entre 1 y el último número devuelto por la instrucción LIST. Esta instrucción no debe utilizarse para recuperar un mensaje marcado como borrado. De no haber tipo de entrega, el servidor envía el correo electrónico en codificación de ampliaciones polivalentes de correo de Internet (MIME). Si el modo de entrega está definido, el servidor procesa específicamente el mensaje. Por ejemplo, con CertifiedMail el servidor tantea al receptor antes de enviar el sobre con la instrucción RCPT
CHLG RESP Adicional	Enviada por el cliente para notificar la recepción del mensaje y responder a la pregunta secreta. Si la respuesta es correcta, el servidor devuelve el sobre MIME
SEND NORP Adicional	Envía la notificación de recepción firmada
HELP Sin modificación	Devuelve una lista de instrucciones soportada por el servidor CPOP
QUIT Sin modificación	Termina la sesión

8 Especificación CMTP detallada

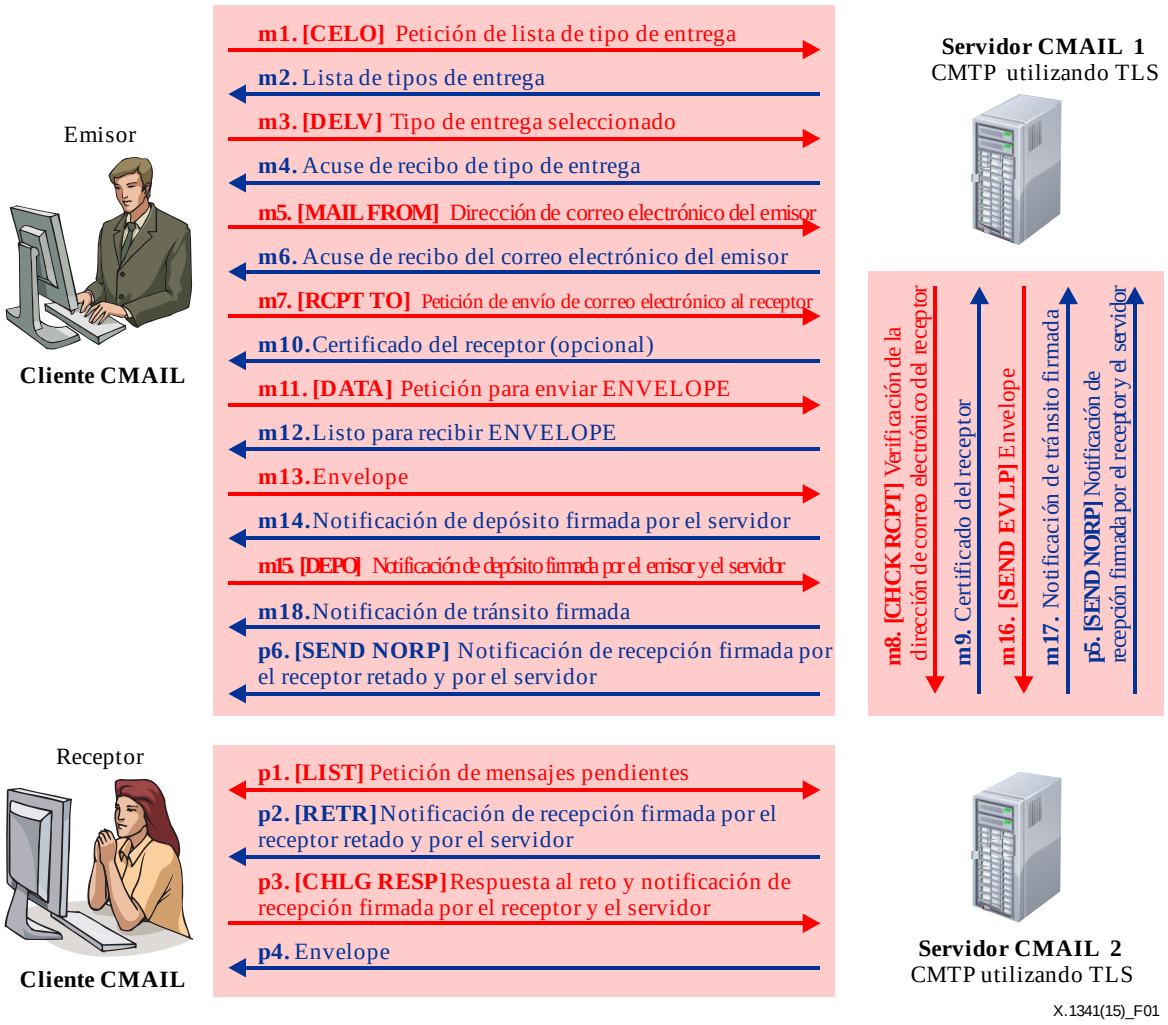

Figura 1 – Resumen de los intercambios del protocolo

Las instrucciones con el prefijo "m" son las que utiliza el protocolo CMTP y las instrucciones con el prefijo "p" son las del protocolo CPOP. En las cláusulas 8.1 a 8.18 se especifican detalladamente los intercambios m1 a m18 de la Figura 1, mientras que en la cláusula 9 se especifican detalladamente los intercambios p1 a p6.

8.1 CELO: Petición de lista de tipo de entrega

El tipo de instrucción se envía como un mensaje SMTP, como ocurre con la instrucción HELO, seguido de un nombre de dominio plenamente calificado. El objetivo es extraer una lista de tipos de entrega.

8.2 Lista de tipos de entrega

La lista de tipos de entrega se da en respuesta a la instrucción CELO. Se utiliza el formato SMTP con el siguiente contenido (distinción entre mayúsculas y minúsculas):

250-<Fully qualified domain name of the Cmail server>

250-8BITMIME

250-Delivery-Types CertifiedMail <other delivery types>

250 OK

En esta Recomendación sólo se especifica CertifiedMail. En futuras ediciones podrán especificarse otros tipos de entrega.

8.3 Tipo de entrega seleccionado

Este mensaje identifica el tipo de entrega a partir de los especificados en la lista de tipos de entrega. Tiene el siguiente formato (SMTP):

DELV <delivery type>

8.4 Acuse de recibo de tipo de entrega

Cuando se acepta el tipo de entrega seleccionado, este mensaje tiene el siguiente formato SMTP (sin distinción entre mayúsculas y minúsculas):

250 Delivery-Type <delivery type>OK

La siguiente respuesta se da en caso de que haya un error de sintaxis en el mensaje de entrega seleccionado:

501 Syntax: DELV <delivery type>

La siguiente respuesta se da cuando el mensaje de entrega seleccionado se envía fuera de secuencia:

501 Syntax: use CELO command first

La siguiente respuesta se da cuando se desconoce el mensaje de entrega seleccionado:

501 Unknown Delivery-Type: <delivery type>

8.5 Dirección de correo electrónico del emisor

Este mensaje se envía al servidor Cmail para solicitar el envío de un correo certificado y, facultativamente, solicitar al servidor Cmail el certificado de clave pública del emisor.

MAIL FROM <sender's email address> [CertificateRequested]

8.6 Acuse de recibo del correo electrónico del emisor

Este mensaje se envía para confirmar que la dirección de correo electrónico del emisor existe en la base de datos del servidor Cmail. Si el emisor ha solicitado su certificado de clave pública, se incluirá el certificado de clave pública del emisor:

[250 User-Certificate: <public-key certificate encoded in Base64>]

250 OK

8.7 Petición de envío de correo electrónico al receptor

Este mensaje se envía al servidor Cmail para solicitar el envío de un correo certificado al receptor y, facultativamente, solicitar al servidor Cmail el certificado de clave pública del receptor.

RCPT TO <recipient's email address> [CertificateRequested]

Esta instrucción puede utilizarse tantas veces como sea necesario para añadir a cada uno de los receptores, en caso de que haya varios. La información que indica si el receptor es "A" o "Cc" (copia) figura en el encabezamiento del sobre [IETF RFC 5321]. No se permiten receptores "CCC" (copia oculta).

8.8 Verificación de la dirección de correo electrónico del receptor por el servidor Cmail distante

Este mensaje sólo se envía si el receptor está vinculado a un servidor Cmail distinto del servidor Cmail del emisor. Se envía desde el servidor Cmail del emisor al servidor Cmail del receptor para verificar la validez de la dirección de correo electrónico y, facultativamente, solicitar el certificado de clave pública del receptor.

CHCK RCPT <recipient's email address> [CertificateRequested]

8.9 Acuse de recibo de la dirección de correo electrónico del receptor

Este mensaje se envía en respuesta a "Verificación de la dirección de correo electrónico del receptor por el servidor Cmail distante".

El siguiente mensaje confirma la dirección de correo electrónico e incluye, si así se ha solicitado, el certificado de clave pública del receptor:

[250 User-Certificate: <public-key certificate encoded in Base64>]

250 OK

Cuando no se pueda confirmar la dirección de correo electrónico, se podrán enviar los siguientes mensajes de error:

503 Sender already specified

Se enviará si es una respuesta para duplicar la solicitud.

501 Syntax: CHCK RCPT <address>

Se enviará si hay un error de sintaxis en la dirección de correo electrónico del receptor.

501 Syntax: CHCK RCPT <address> Error in parameters <parameter>

Se enviará si no se reconoce el parámetro después de la dirección de correo electrónico.

553 <email address> Invalid email address

Se enviará si la dirección de correo electrónico no existe en el servidor Cmail distante.

8.10 Acuse de recibo del correo electrónico del receptor

Este mensaje se envía para confirmar que la dirección de correo electrónico del receptor existe. Si el emisor solicita el certificado de clave pública del receptor, se incluirá el certificado de clave pública del receptor.

El siguiente mensaje confirma la dirección de correo electrónico e incluye, si así se ha solicitado, el certificado de clave pública del receptor:

[250 User-Certificate: <public-key certificate encoded in Base64>]

250 OK

Cuando no se pueda confirmar la dirección de correo electrónico, se podrán enviar los siguientes mensajes de error:

503 Error: need MAIL FROM command

Se enviará si el mensaje se envía fuera de secuencia.

452 Error: too many recipients

Se enviará si se especifican demasiados receptores.

501-6.1.1 Syntax: RCPT TO <address>

Se enviará si hay un error de sintaxis en la dirección de correo electrónico del receptor.

501-6.1.2 Syntax: RCPT TO <address> Error in parameters: <parameters>

Se enviará si no se reconoce el parámetro después de la dirección de correo electrónico.

550-5.1.1 <email address> Invalid email address.

Se enviará si la dirección de correo electrónico no existe.

8.11 Petición para enviar ENVELOPE

El emisor utiliza el siguiente formato para pedir al servidor Cmail permiso para enviar datos.

DATA

8.12 Listo para recibir ENVELOPE

Se enviará el siguiente mensaje si el servidor Cmail está listo para recibir datos:

354 Start mail input; end with <CRLF>.<CRLF>

Se enviará el siguiente mensaje cuando no se haya enviado la instrucción MAIL FROM:

503 Error: need MAIL FROM command

Se enviará el siguiente mensaje cuando no se haya enviado la instrucción RCPT TO:

503 Error: need RCPT TO command

Se enviará el siguiente mensaje cuando no se haya enviado la instrucción DELV:

503 Error: need DELV command

8.13 ENVELOPE

El cliente:

1) generará una clave de cifrado simétrico aleatorio (RSCK), por ejemplo, norma de encriptación avanzada (AES) 256;
2) encriptará el cuerpo del mensaje y los adjuntos, de haberlos, utilizando esa clave;
3) creará un mensaje MIME que contenga una parte denominada ENVELOPE con el mensaje encriptado (véase [IETF RFC 2045]);
4) finalizará el mensaje con <CR><LF>.<CR><LF>; y
5) enviará el mensaje MIME.

8.14 Notificación de depósito firmada por el servidor

250 Notice-of-deposit:

<notice of deposit signed by the Cmail server encoded in base64>

250 Ok

El servidor generará una notificación de depósito con información sobre el sobre (id del sobre, tipo de entrega y troceo MIME) y la firmará con su clave privada.

8.15 Notificación de depósito firmada por el emisor y el servidor

El emisor:

1) descodificará la notificación de depósito recibida;
2) crear un reto para cada receptor;
3) firmar la notificación de depósito firmada por el servidor con su propia clave privada;
4) codificar el resultado en base64; y

5) transmitirlo al servidor Cmail utilizando:

DEPO <notice of deposit base64 encoded>

El reto se define en la Figura A.6.

El reto contiene **SecretQuestion**, **CipherEnvelopeKey** y el certificado de clave pública del receptor.

SecretQuestion: se compone de **Request** y **Response**.

La solicitud (Request) puede contener un **RandomNumber**. La respuesta (Response) contiene el **AlgorithmIdentifier** que ha de recalcular el emisor para recibir el ENVELOPE. Este **AlgorithmIdentifier** identifica el algoritmo utilizado para calcular el troceo. El reto consiste en recuperar primero la clave de cifrado RSCK, cifrada con la clave pública del receptor, y después concatenar **RandomNumber** y la RSCK, y calcular el troceo para construir la respuesta.
A continuación se muestra un ejemplo de reto en lenguaje de marcaje extensible (XML):

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1"
Encoding="base64">5mYZWhtl0yxBa/wl7VLiiQ=</response>
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

NOTA 1 – Este reto puede utilizar las reglas de codificación distinguida (DER) de la notación de sintaxis abstracta uno (ASN.1).

NOTA 2 – El servidor no puede recalcular el troceo, pues desconoce la clave de encriptación. Sin embargo, sólo el servidor conoce el resultado previsto del cálculo de troceo.

NOTA 3 – Durante el reto con el receptor, el servidor envía únicamente la pregunta secreta y espera la respuesta del receptor.

8.16 ENVELOPE entre servidores Cmail

El mensaje definido en la cláusula 8.13 se remite a otro servidor Cmail sólo si el emisor y el receptor pertenecen a distintos servidores Cmail (véase el punto m16 en la Figura 1).

SEND EVLP <MIME message>

8.17 Notificación de tránsito entre servidores Cmail firmada

Se utilizará el siguiente formato:

250 Notice-of-transit:

<notice of transit base64 encoded>

Se enviará el siguiente mensaje si el servidor Cmail recibe una notificación de tránsito:

250 Ok

Se enviará el siguiente mensaje cuando la notificación de tránsito sea incorrecta:

503 Error: incorrect Notice-of-transit

El servidor Cmail que recibe el ENVELOPE emite la notificación de tránsito.

Este servidor Cmail genera una notificación de depósito con información sobre el sobre (id de sobre, tipo de entrega y troceo MIME) y la firma con su clave privada. Esta notificación es idéntica a la notificación de depósito.

8.18 Notificación de tránsito firmada

El emisor Cmail:

1) descodificará la notificación de tránsito recibida;
2) firmará la notificación de tránsito firmada por el servidor utilizando su propia clave privada;
3) codificará el resultado en base64; y
4) lo transmitirá al servidor Cmail utilizando:

   250 Signed-notice-of-transit:

   <signed notice of transit base64 encoded>

   250 Signed-notice-of-deposit:

   <signed notice of deposit base64 encoded>

   250 Ok

9 Protocolo de oficina postal certificada (CPOP)

En las cláusulas 9.1 a 9.6 se explican los puntos p1 a p6 de la Figura 1.

9.1 Petición de mensajes pendientes

La información sobre mensajes pendientes se da utilizando el procedimiento especificado en la cláusula 5 para la instrucción LIST [IETF RFC 1939] con un parámetro adicional. Para cada línea que detalla un mensaje pendiente, se añade un parámetro adicional que indica el tipo de entrega, si no se trata de correo electrónico normal (véase el punto p1 en la Figura 1). Por ejemplo:

C: LIST

S: +OK 2 messages (320 octets)

S: 1 120

S: 2 200 CertifiedMail

S: .

Este procedimiento incluye también la extracción de todos los correos electrónicos estándar, dejando sólo los mensajes etiquetados con un tipo de entrega en el servidor Cmail.

9.2 Notificación de recepción firmada por el receptor retado y por el servidor

Para los mensajes etiquetados con un tipo de entrega, la instrucción RETR no extrae el mensaje, sino el reto y la notificación de recepción firmada por el servidor, codificada en base64. El cliente verifica la firma digital y el certificado del emisor incluido en la notificación de recepción.

Ejemplo:

C: RETR 2

El siguiente mensaje se enviará si el servidor Cmail envía la notificación de recepción:

S: +OK 200 octets

S: <the Cmail server sends the notice of reception including the challenge>

S: .

Se enviará el siguiente mensaje cuando el servidor no pueda enviar la notificación de recepción:

503 Error: impossible to send Notice-of-reception

El servidor Cmail encuentra en la notificación de depósito el nodo **Entity** relacionado con el receptor. Entonces, el servidor Cmail copia este nodo en la notificación de recepción y elimina el contenido del nodo **Response** incluido en el nodo **Entity**.

Ejemplo de nodo en la notificación de depósito:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1"
Encoding="base64">5mYZWhtl0yxBa/wl7VLiiQ=</response>
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

NOTA 1 – Este reto puede utilizar la codificación DER ASN.1.

Y el mismo nodo copiado en la notificación de recepción:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1" Encoding="base64" />
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

NOTA 2 – Este reto puede utilizar la codificación DER ASN.1.

9.3 Respuesta al reto y notificación de recepción firmada por el receptor y el servidor

El receptor:

1) descodificará la notificación de recepción recibida;
2) extraerá la RSCK;
3) calculará la respuesta al reto;
4) firmará la notificación de recepción firmada por el servidor utilizando su propia clave privada;
5) codificará el resultado en base64; y
6) lo transmitirá al servidor Cmail utilizando:

CHLG RESP <challenge response and recipient and server signed notice of reception>

El receptor descifrará el mensaje de la siguiente manera:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1" Encoding="base64"></response>
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

NOTA – Este reto puede utilizar la codificación DER ASN.1.

El receptor recupera RSCK con su clave privada descifrando el contenido del nodo **`CipherEnvelopeKey`**. A continuación, el receptor concatena **`RandomNumber`** y RSCK, lo trocea con el **`AlgorithmIdentifier`** definido y obtiene el resultado de **`SecretQuestion`**.

El receptor copia este resultado en la notificación de recepción firmada, la firma y la envía al servidor Cmail.

9.4 ENVELOPE

Si el reto está OK, el servidor Cmail envía el ENVELOPE de mismo modo que el resultado de la instrucción RETR. El receptor tiene ahora el mensaje y la clave para abrirlo.

Se enviará el siguiente mensaje cuando el servidor no pueda enviar ENVELOPE:

503 Error: impossible to send ENVELOPE

9.5 Notificación de recepción firmada por el receptor y el servidor entre servidores Cmail (facultativo)

Este mensaje sólo se enviará si el emisor y el receptor pertenecen a distintos servidores Cmail.

SEND NORP <base64 encoded Recipient and server signed notice of reception>

9.6 Notificación de recepción firmada por el receptor y el servidor

Este mensaje sólo se enviará si el emisor y el receptor pertenecen a distintos servidores Cmail.

SEND NORP <base64 encoded Recipient and server signed notice of reception>

Anexo A

Notificaciones en definición de esquema XML (XSD)

(Este anexo forma parte integrante de la presente Recomendación.)

En este anexo se especifican las notificaciones utilizando la definición de esquema XML (XSD), como se define en [XSD]. Las instancias de comunicación se codificarán en XML como se especifica en [XML] y serán conformes con las especificaciones XSD indicadas en este anexo.

A.1 Aspectos generales de XSD

Véanse Figuras A.1 a A.10

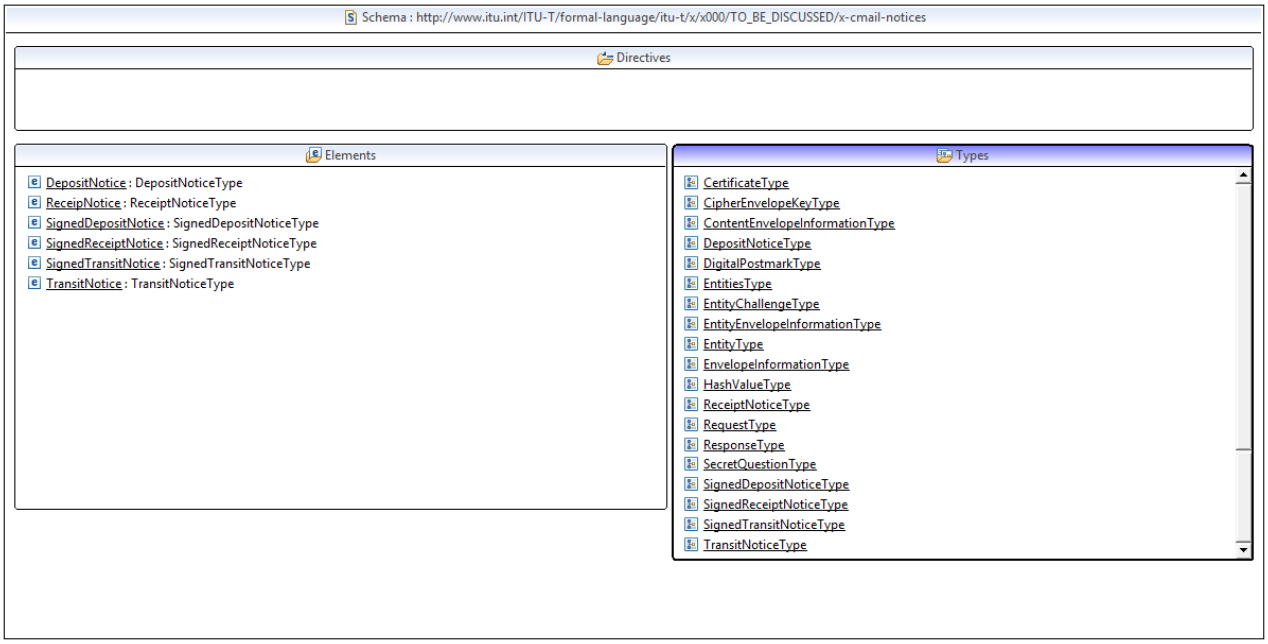

Figura A.1 – Lista de elementos y tipos

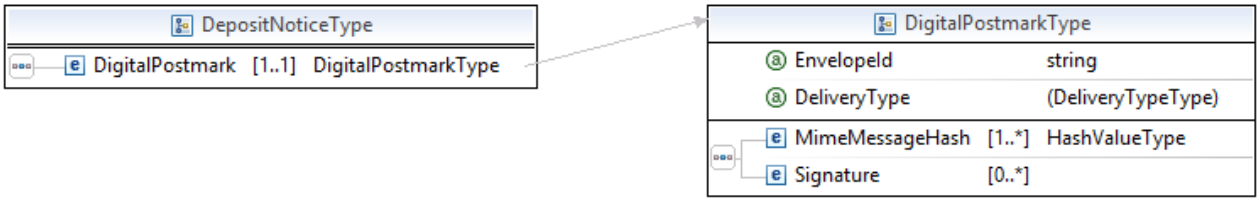

Figura A.2 – Notificación de depósito

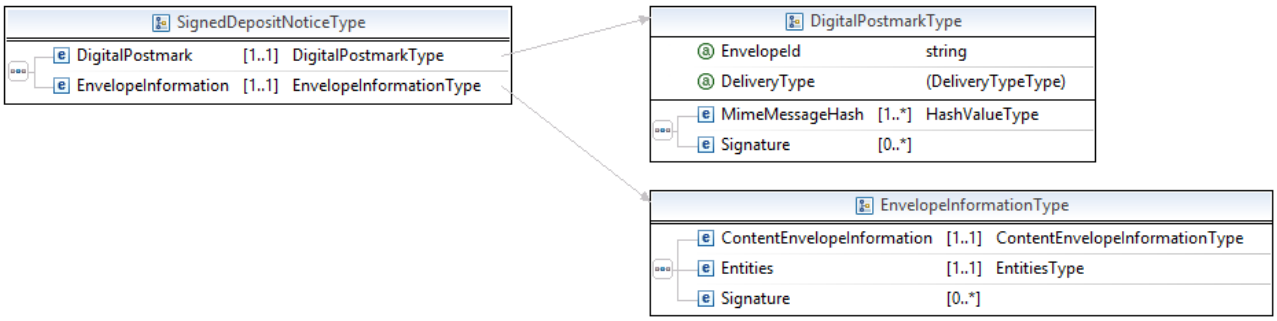

Figura A.3 – Notificación de depósito firmada

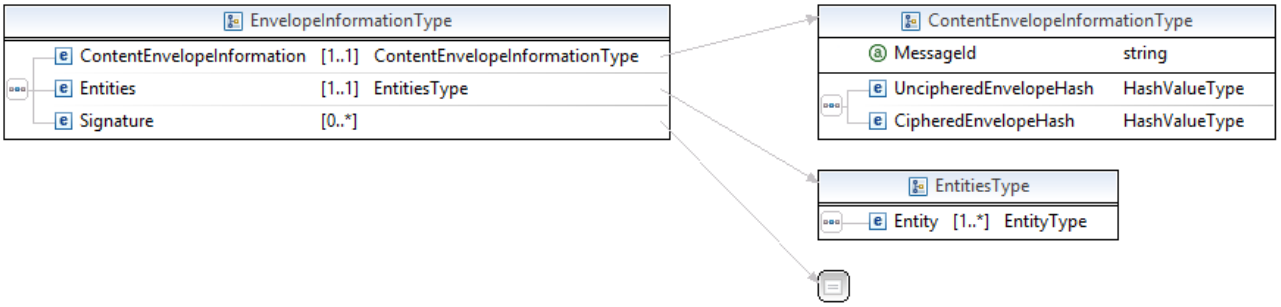

Figura A.4 – Tipo de información del sobre

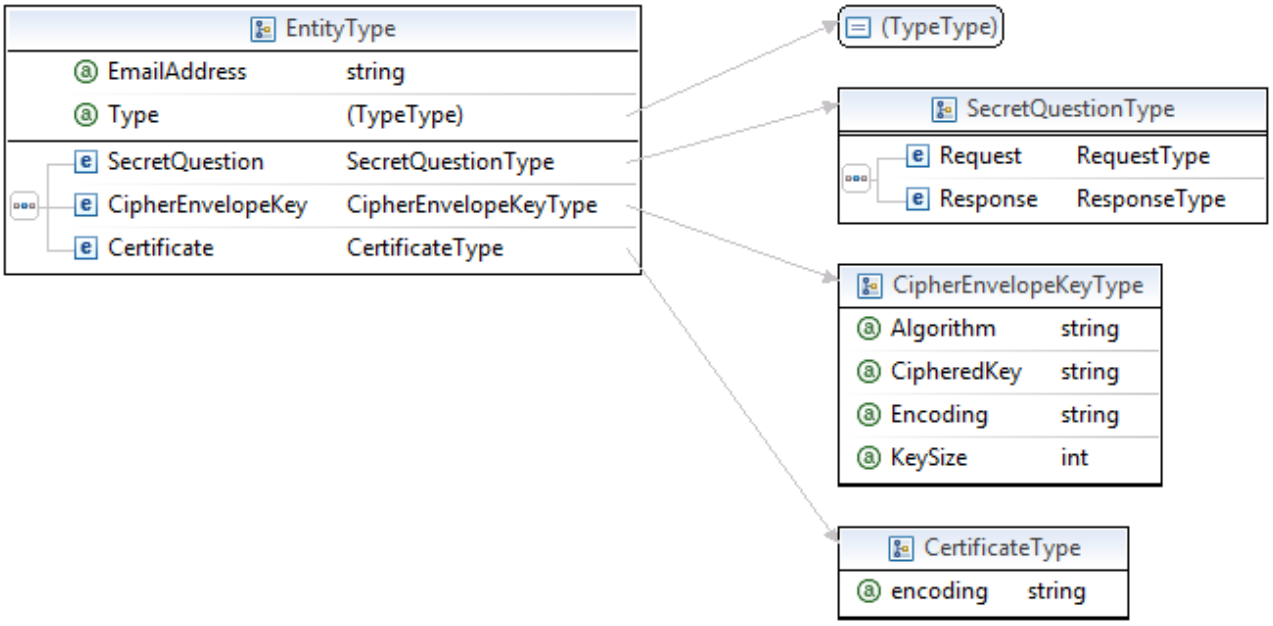

Figura A.5 – Tipo de entidad

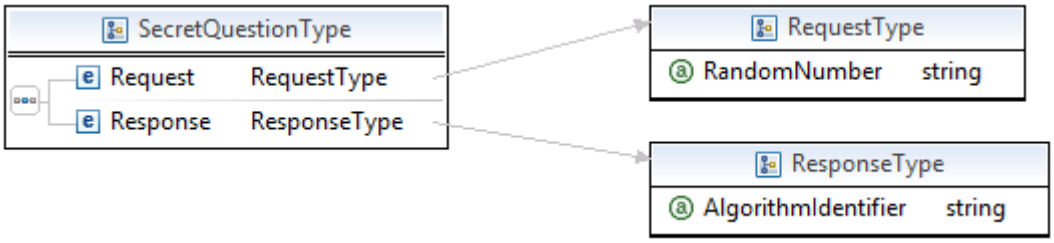

Figura A.6 – Reto

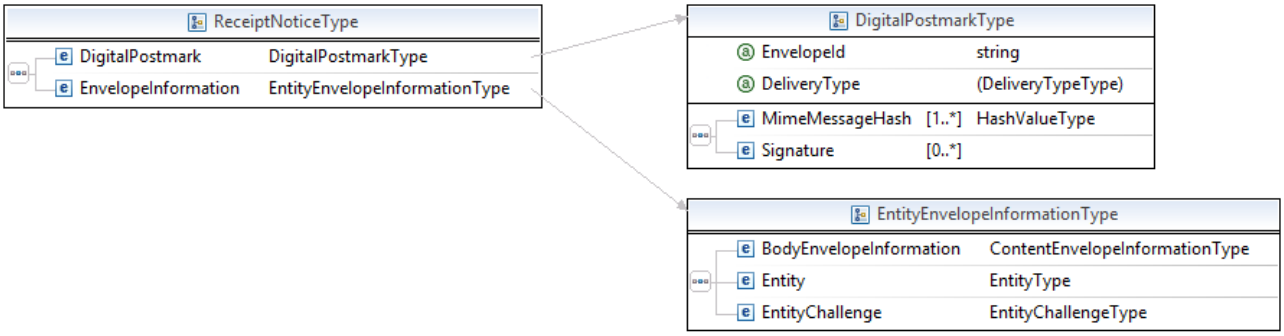

Figura A.7 – Notificación de recepción

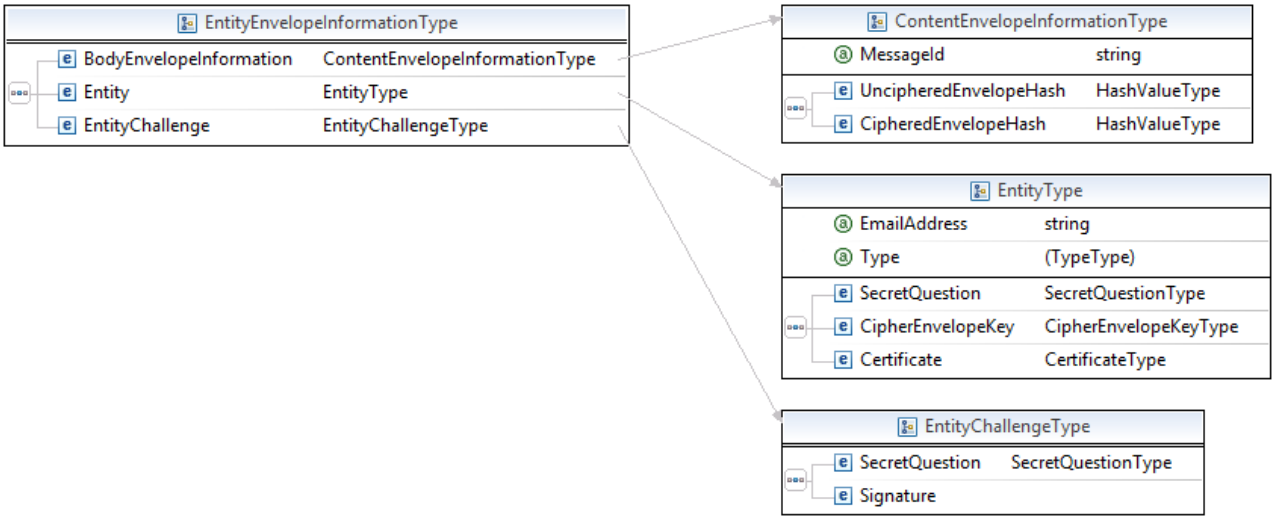

Figura A.8 – Respuesta del receptor al reto

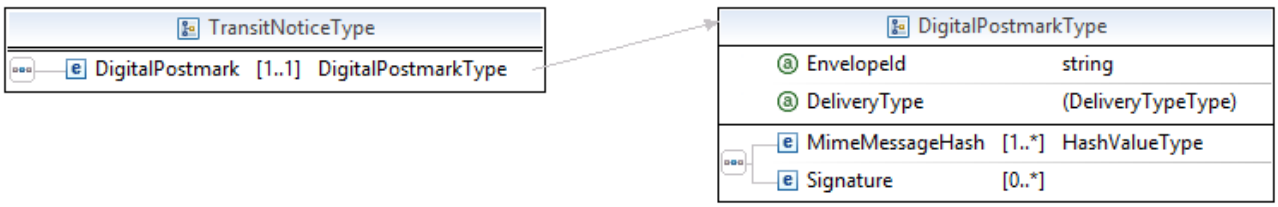

Figura A.9 – Notificación de tránsito

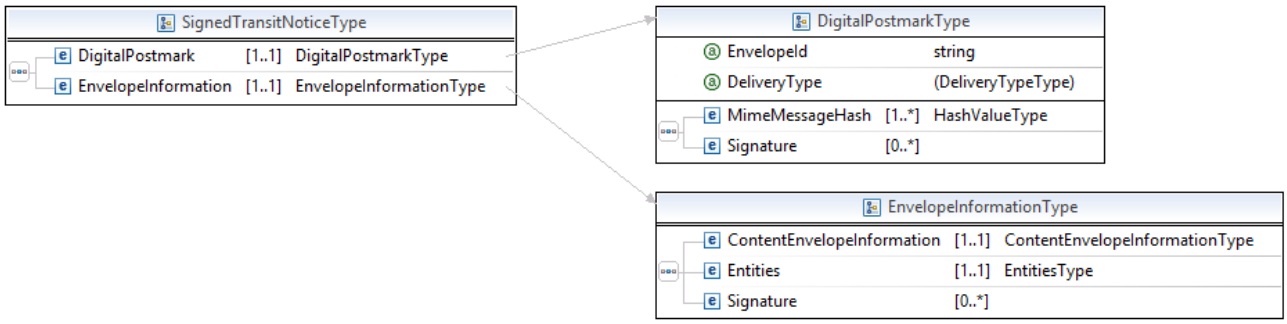

Figura A.10 – Notificación de tránsito firmada

A.2 Especificación formal de notificaciones en XSD

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices"
     elementFormDefault="qualified" xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

  <import namespace="http://www.w3.org/2009/xmldsig11#"
    schemaLocation="http://www.w3.org/TR/xmldsig-core1/xmldsig11-schema.xsd" />
  <import namespace="http://www.w3.org/2009/xmldsig-properties"
    schemaLocation="http://www.w3.org/TR/xmldsig-properties/xmldsig-properties.xsd" />

  <import namespace=http://www.w3.org/2000/09/xmldsig#
    schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd" />

  <element name="DepositNotice" type="tns:DepositNoticeType"></element>
  <element name="SignedDepositNotice" type="tns:SignedDepositNoticeType"></element>
  <element name="TransitNotice" type="tns:TransitNoticeType"></element>
  <element name="SignedTransitNotice" type="tns:SignedTransitNoticeType"></element>
  <element name="ReceipNotice" type="tns:ReceiptNoticeType"></element>
  <element name="SignedReceiptNotice" type="tns:SignedReceiptNoticeType"></element>

  <complexType name="DigitalPostmarkType">
    <sequence>
      <element name="MimeMessageHash" type="tns:HashValueType"
        maxOccurs="unbounded" minOccurs="1">
      </element>
      <element name="Signature" type="ds:SignatureType"
        maxOccurs="unbounded" minOccurs="0">
      </element>
    </sequence>
    <attribute name="EnvelopeId" type="string" use="required"></attribute>
    <attribute name="DeliveryType" use="required">
      <simpleType>
        <restriction base="string">
          <enumeration value="CertifiedMail"></enumeration>
        </restriction>
      </simpleType>
    </attribute>
  </complexType>

  <complexType name="EnvelopeInformationType">
    <sequence>
      <element name="ContentEnvelopeInformation"
        type="tns:ContentEnvelopeInformationType" maxOccurs="1" minOccurs="1">
      </element>
      <element name="Entities" type="tns:EntitiesType"
        maxOccurs="1" minOccurs="1">
      </element>
      <element name="Signature" type="ds:SignatureType"
        maxOccurs="unbounded" minOccurs="0">
      </element>
    </sequence>
  </complexType>
```

```
<complexType name="ContentEnvelopeInformationType">
  <sequence>
    <element name="UncipheredEnvelopeHash" type="tns:HashValueType"></element>
    <element name="CipheredEnvelopeHash" type="tns:HashValueType"></element>
  </sequence>
  <attribute name="MessageId" type="string"></attribute>
</complexType>

<complexType name="SecretQuestionType">
  <sequence>
    <element name="Request" type="tns:RequestType"></element>
    <element name="Response" type="tns:ResponseType"></element>
  </sequence>
</complexType>

<complexType name="EntityType">
  <sequence>
    <element name="SecretQuestion" type="tns:SecretQuestionType"></element>
    <element name="CipherEnvelopeKey"
      type="tns:CipherEnvelopeKeyType">
    </element>
    <element name="Certificate" type="tns:CertificateType"></element>
  </sequence>
  <attribute name="EmailAddress" type="string" use="required">
    <annotation>
      <documentation>Email address has to be in RFC 822format</documentation>
    </annotation></attribute>
  <attribute name="Type" use="required">
    <simpleType>
      <restriction base="string">
        <enumeration value="from"></enumeration>
        <enumeration value="to"></enumeration>
        <enumeration value="cc"></enumeration>
        <enumeration value="transit"></enumeration>
      </restriction>
    </simpleType>
  </attribute>
</complexType>

<complexType name="CipherEnvelopeKeyType">
  <attribute name="Algorithm" type="string"></attribute>
  <attribute name="CipheredKey" type="string"></attribute>
  <attribute name="Encoding" type="string"></attribute>
  <attribute name="KeySize" type="int"></attribute>
</complexType>

<complexType name="CertificateType">
  <attribute name="encoding" type="string"></attribute>
</complexType>

<complexType name="EntitiesType">
  <sequence>
    <element name="Entity" type="tns:EntityType"
      maxOccurs="unbounded" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="SignedDepositNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
    <element name="EnvelopeInformation"
      type="tns:EnvelopeInformationType" maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>
```

```
<complexType name="DepositNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="TransitNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="SignedTransitNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
    <element name="EnvelopeInformation"
      type="tns:EnvelopeInformationType" maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="ReceiptNoticeType">
  <sequence>
    <element name="DigitalPostmark"
      type="tns:DigitalPostmarkType">
    </element>
    <element name="EnvelopeInformation"
      type="tns:EntityEnvelopeInformationType">
    </element>
  </sequence>
</complexType>

<complexType name="SignedReceiptNoticeType">
  <sequence>
    <element name="DigitalPostmark"
      type="tns:DigitalPostmarkType">
    </element>
    <element name="EnvelopeInformation"
      type="tns:EntityEnvelopeInformationType">
    </element>
  </sequence>
</complexType>

<complexType name="HashValueType">
  <attribute name="AlgorithmOID">
    <simpleType>
      <restriction base="string">
        <enumeration value="1.3.14.3.2.26"></enumeration>
        <enumeration value="2.16.840.1.101.3.4.2.1"></enumeration>
      </restriction>
    </simpleType>
  </attribute>
</complexType>

<complexType name="EntityEnvelopeInformationType">
  <sequence>
    <element name="BodyEnvelopeInformation" type="tns:ContentEnvelopeInformationType">
    </element>
    <element name="Entity" type="tns:EntityType"></element>
    <element name="EntityChallenge" type="tns:EntityChallengeType"></element>
  </sequence>
</complexType>
```

```
  <complexType name="EntityChallengeType">
    <sequence>
      <element name="SecretQuestion" type="tns:SecretQuestionType"></element>
      <element name="Signature" type="ds:SignatureType"></element>
    </sequence>
  </complexType>

  <complexType name="RequestType">
    <attribute name="RandomNumber" type="string"></attribute>
  </complexType>

  <complexType name="ResponseType">
    <attribute name="AlgorithmIdentifier" type="string"></attribute>
  </complexType>

</schema>
```

Anexo B

Notificaciones en ASN.1

(Este anexo forma parte integrante de la presente Recomendación.)

En este anexo se especifican las notificaciones en notación de sintaxis abstracta uno (ASN.1), como se define en [UIT-T X.680]. Las notificaciones pueden codificarse con las reglas de codificación distinguida (DER) ASN.1, como se define en [UIT-T X.690], o utilizando las reglas de codificación XML ampliadas (EXTENDED-XER), como se especifica en [UIT-T X.693]. En este último caso, el XML resultante de esta codificación es idéntico al XML generado de conformidad con la XDS definida en el Anexo A.

```
CMAIL {itu-t(0) recommendation(0) x(24) cmail(1341) asn1Module(1) cmail(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS String
     FROM XSDv2 {joint-iso-itu-t asn1(1) specification(0) modules(0)
          xsd-module(2) version2(2)};

DepositNotice         ::= DepositNoticeType

SignedDepositNotice   ::= SignedDepositNoticeType

TransitNotice         ::= TransitNoticeType

SignedTransitNotice   ::= SignedTransitNoticeType

ReceiptNotice         ::= ReceiptNoticeType

SignedReceiptNotice   ::= SignedReceiptNoticeType

DigitalPostmarkType   ::= SEQUENCE {
     mimeMessageHash SEQUENCE (SIZE(1..MAX)) OF
          mimeMessageHash HashValueType,
     signature  SEQUENCE (SIZE(0..MAX)) OF
          signature  SignatureType,
     envelopeId String,
     deliveryType    ENUMERATED {
          certifiedMail,
          ...
          }
     }

EnvelopeInformationType    ::= SEQUENCE {
     contentEnvelopeInformation ContentEnvelopeInformationType,
     entities              EntitiesType,
     signature        SEQUENCE (SIZE(0..MAX)) OF
          signature SignatureType
     }

ContentEnvelopeInformationType  ::= SEQUENCE {
     uncipheredEnvelopeHash     HashValueType,
     cipheredEnvelopeHash HashValueType,
     messageId        String
     }

SecretQuestionType    ::= SEQUENCE {
     request          RequestType,
     response   ResponseType
     }
```

```
EntityType ::= SEQUENCE {
     secretQuestion       SecretQuestionType,
     cipheredEnvelopeKey  CipheredEnvelopeKeyType,
     certificate          CertificateType,
     emailAddress         String
          (CONSTRAINED BY
          {-- "Email address has to be in IETF RFC 822 format --}),
     type ENUMERATED {
          from,
          to,
          cc,
          transit
          }
     }

CipheredEnvelopeKeyType    ::= SEQUENCE {
     algorithm  String,
     cipherededKey   String,
     encoding   String,
     keySize         String
     }

CertificateType ::= SEQUENCE {
     encoding   String
     }

EntitiesType    ::= SEQUENCE {
     entity          SEQUENCE(SIZE(1..MAX)) OF entity EntityType
     }

SignedDepositNoticeType    ::= SEQUENCE {
     digitalPostmark      DigitalPostmarkType,
     envelopeInformation  EnvelopeInformationType
     }

DepositNoticeType     ::= SEQUENCE {
     digitalPostmark      DigitalPostmarkType
     }

TransitNoticeType     ::= SEQUENCE {
     digitalPostmark      DigitalPostmarkType
     }

SignedTransitNoticeType    ::= SEQUENCE {
     digitalPostmark      DigitalPostmarkType,
     envelopeInformation  EnvelopeInformationType
     }

ReceiptNoticeType     ::= SEQUENCE {
     operatorPostmark     DigitalPostmarkType
     }

SignedReceiptNoticeType    ::= SEQUENCE {
     operatorPostmark     DigitalPostmarkType,
     envelopeInformation  EntityEnvelopeInformationType
     }

HashValueType   ::= SEQUENCE {
     algorithmOID    ENUMERATED {
          sha-1,
          sha-256
          }
     }

EntityEnvelopeInformationType   ::= SEQUENCE {
     bodyEnvelopeInformation   ContentEnvelopeInformationType,
     entity               EntityType,
     entityChallenge      EntityChallengeType
     }
```

```
EntityChallengeType  ::= SEQUENCE {
      secretQuestion _SecretQuestionType,
      signature  SignatureType
      }

RequestType     ::= SEQUENCE {
      randomNumer     String
      }

ResponseType    ::= SEQUENCE {
      algorithmIdentifier  String
      }

SignatureType   ::= String

ENCODING-CONTROL XER
      GLOBAL-DEFAULTS MODIFIED-ENCODINGS
      [NAME AS CAPITALIZED] DigitalPostmarkType.mimeMessageHash
      [UNTAGGED] DigitalPostmarkType.mimeMessageHash
      [NAME AS CAPITALIZED] DigitalPostmarkType.signature.*
      [UNTAGGED] DigitalPostmarkType.signature
      [NAME AS CAPITALIZED] DigitalPostmarkType.envelopeId
      [ATTRIBUTE] DigitalPostmarkType.envelopeId
      [NAME AS CAPITALIZED] DigitalPostmarkType.deliveryType
      [ATTRIBUTE] DigitalPostmarkType.deliveryType
      [TEXT AS CAPITALIZED] DigitalPostmarkType.delivetyType:certifiedMail
      [NAME AS CAPITALIZED] EnvelopeInformationType.contentEnvelopeInformation
      [NAME AS CAPITALIZED] EnvelopeInformationType.entities
      [NAME AS CAPITALIZED] EnvelopeInformationType.signature
      [UNTAGGED] EnvelopeInformationType.signature
      [NAME AS CAPITALIZED]
           ContentEnvelopeInformationType.uncipheredEnvelopeHash
      [NAME AS CAPITALIZED]
           ContentEnvelopeInformationType.cipheredEnvelopeHash
      [NAME AS CAPITALIZED] ContentEnvelopeInformationType.messageId
      [ATTRIBUTE] ContentEnvelopeInformationType.messageId
      [NAME AS CAPITALIZED] SecretQuestionType.request
      [NAME AS CAPITALIZED] SecretQuestionType.response
      [NAME AS CAPITALIZED] EntityType.secretQuestion
      [NAME AS CAPITALIZED] EntityType.cipheredEnvelopeKey
      [NAME AS CAPITALIZED] EntityType.certificate
      [NAME AS CAPITALIZED] EntityType.emailAddress
      [ATTRIBUTE] EntityType.emailAddress
      [NAME AS CAPITALIZED] EntityType.type
      [ATTRIBUTE] EntityType.type
      [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.algorithm
      [ATTRIBUTE] CipheredEnvelopeKeyType.algorithm
      [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.cipheredKey
      [ATTRIBUTE] CipheredEnvelopeKeyType.cipheredKey
      [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.encoding
      [ATTRIBUTE] CipheredEnvelopeKeyType.encoding
      [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.keysize
      [ATTRIBUTE] CipheredEnvelopeKeyType.keysize
      [NAME AS CAPITALIZED] CertificateType.encoding
      [ATTRIBUTE] CertificateType.encoding
      [UNTAGGED] EntitiesType.entity
      [NAME AS CAPITALIZED] EntitiesType.entity.*
      [NAME AS CAPITALIZED] SignedDepositNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedDepositNoticeType.envelopeInformation
      [NAME AS CAPITALIZED] DepositNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] TransitNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedTransitNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedTransitNoticeType.envelopeInformation
      [NAME AS CAPITALIZED] ReceiptNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedReceiptNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedReceiptNoticeType.envelopeInformation
      [NAME AS CAPITALIZED] HashValueType.algorithmOID
      [ATTRIBUTE] HashValueType.algorithmOID
      [TEXT AS "1.3.14.3.2.26"] HashValueType.algorithmOID:sha-1
      [TEXT AS "2.16.840.1.101.3.4.2.1"] HashValueType.algorithmOID:sha-256
```

```
      [NAME AS CAPITALIZED]
           EntityEnvelopeInformationType.BodyEnvelopeInformation
      [NAME AS CAPITALIZED]
           EntityEnvelopeInformationType.entityChallenge
      [NAME AS CAPITALIZED] EntityChallengeType.secretQuestion
      [NAME AS CAPITALIZED] EntityChallengeType.signature
      [NAME AS CAPITALIZED] RequestType.randomNumber
      [ATTRIBUTE] RequestType.randomNumber
      [NAME AS CAPITALIZED] ResponseType.algorithmIdentifier
      [ATTRIBUTE] ResponseType.algorithmIdentifier

END
```

Anexo C

Requisitos de componentes de infraestructura de clave pública

(Este anexo forma parte integrante de la presente Recomendación.)

C.1 Introducción

En este anexo se presentan los requisitos de los certificados de clave pública emitidos a servidores Cmail y clientes.

C.2 Certificado de clave pública de entidad extrema emitido en un servidor Cmail

Un certificado de clave pública de entidad extrema emitido a un servidor Cmail deberá tener el siguiente contenido:

a) Se especificará la versión 3.

b) La CA generará números de serie no secuenciales.

c) En el campo sujeto se incluirá un nombre distinguido de directorio con un único componente utilizando el tipo de atributo **dnsName**, como se define en [UIT-T X.520]. El valor será un nombre registrado en el sistema de nombre de dominio (DNS).

d) Habrá una extensión de nombre alternativo sujeto con dos elementos:

- el **rfc822Name** alternativo se tomará para uno de los elementos y será la dirección de correo electrónico del administrador del servidor Cmail;
- el **directoryName** alternativo se tomará para el otro elemento e incluirá un nombre distinguido con los siguientes componentes:
  - **countryName** estará presente y contendrá un código de tres letras (alfa-3) de [ISO 3166-1];
  - **organizationName** estará presente y contendrá el nombre fiable de la organización que gestiona el servidor Cmail;
  - **streetAddress** estará presente y contendrá el nombre de la calle y el número de la casa;
  - **localityName** estará presente y contendrá el nombre de la localidad;
  - **stateOrProvinceName** estará presente, de ser necesario, para la identificación unívoca. En caso contrario, estará ausente;
  - **postalCode** estará presente y contendrá el código postal de la localidad.

e) La extensión **certificatePolicies** estará presente y, como mínimo, contendrá el identificador de objeto **{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailServer(1)}** para indicar que el certificado de clave pública se emite de conformidad con esta Recomendación.

C.3 Certificado de clave pública de entidad extrema emitido a un cliente Cmail

Un certificado de clave pública de entidad extrema emitido a un cliente Cmail tendrá el siguiente contenido:

a) Se especificará la versión 3.

b) La autoridad de certificación generará números de serie no secuenciales.

c) En el campo sujeto se incluirá un nombre distinguido de directorio con los siguientes componentes:

- **surname** estará presente si el cliente es un particular, pero estará ausente si el cliente es una organización;
- **givenName** estará presente si está presente el apellido (surname). En caso contrario, estará ausente;
- **initials** puede estar presente, si está presente **surname**. En caso contrario, estará ausente;
- **generationQualifier** puede estar presente, si está presente **surname**. En caso contrario, estará ausente;
- **organizationName** estará presente si el cliente no es un particular. En caso contrario, estará ausente. De estar presente, contendrá el nombre fiable de la organización a que pertenece el cliente;
- **streetAddress** estará presente y contendrá el nombre de la calle y el número de la casa;
- **localityName** estará presente y contendrá el nombre de la localidad;
- **stateOrProvinceName** estará presente, de ser necesario, para la identificación unívoca. En caso contrario, estará ausente;
- **postalCode** estará presente y contendrá el código postal de la localidad;
- **countryCode3c** estará presente y contendrá un código de tres letras (alfa-3) de [ISO 3166-1].

d) La extensión **subjectAltName** estará presente y contendrá un elemento, como se indica a continuación:

- **rfc822Name** contendrá la dirección de correo electrónico del administrador del servidor Cmail.

e) La extensión certificatePolicies estará presente y contendrá, como mínimo, el identificador de objeto **{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailClient(2)}** para indicar que el certificado de clave pública se ha emitido de acuerdo con esta Recomendación.

C.4 Requisitos de validación de información

Antes de emitir un certificado de clave pública, el emisor verificará:

a) que el sujeto (solicitante) es el detentor registrado del nombre de dominio que se ha de incluir en el certificado de clave pública;

b) la existencia física del sujeto;

c) la existencia operativa del sujeto (actividad comercial);

d) que el sujeto es una entidad reconocida fiable;

e) el nombre y la dirección que se han de incluir en el certificado de clave pública;

f) que el **organizationName** que se ha de incluir en el certificado de clave pública es un nombre fiable y reconocido que identifica al sujeto.

Anexo D

Requisitos de seguridad de capa de transporte (TLS)

(Este anexo forma parte integrante de la presente Recomendación.)

Se soportará [IETF RFC 5246] o sus versiones posteriores.

En la negociación, ni el servidor Cmail ni el cliente aceptarán una conexión donde se intente negociar una versión TLS anterior a TLS 1.2.

La aplicación soportará la siguiente serie cifrada:

– TLS_DH_RSA_WITH_AES_256_CBC_SHA256

Anexo E

Identificadores de objeto definidos en esta Recomendación

(Este anexo forma parte integrante de esta Recomendación.)

En esta Recomendación se definen los siguientes identificadores de objeto:

a) identificador de objeto asociado al módulo ASN.1:

{itu-t recommendation(0) x(24) cmail(1341) asn1module(0) cmail(1)}

b) identificador de objeto utilizado por la extensión certificatePolicies de un servidor Cmail:

{itu-t recommendation(0) x(24) cmail(1341) certificateProfile(2) cmailServer(1)}

c) identificador de objeto utilizado por la extensión certificatePolicies de un cliente Cmail:

{itu-t recommendation(0) x(24) cmail(1341) certificateProfile(2) cmailClient(2)}

Apéndice I

Formato de sobre y notificaciones

(Este apéndice no forma parte integrante de la presente Recomendación.)

En este apéndice se dan ejemplos de la codificación de las notificaciones.

I.1 Notificación de depósito

La notificación de depósito contiene información sobre el emisor, el sobre y está formada por el servidor Cmail y por el emisor.

Representa una prueba de depósito para el emisor, que puede utilizarla en caso de litigio.

La especificación formal de la notificación de depósito puede encontrarse en el Anexo A.

Ejemplo: fichero "1373360283931.deposit.notice"

```
Received: from localhost ([127.0.0.1])
        by begmeil
        with SMTP (SubEthaSMTP null) id HIWV8HF9
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 10:58:14 +0200 (CEST)
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=depositNotice.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs
ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk
bG9wZWQtc2lnbmF0dXJlIi8+CiAgICAgICA8L1RyYW5zZm9ybXM+CiAgICAgICA8RGln
...
ICAgPFJTQUtleVZhbHVlPgogICAgICAgICA8TW9kdWx1cz5tMkFSUURXUGJBMmgvMzJEQWs4
ICAgICAgICAgIDxFeHBvbmVudD5BUUFCPC9FeHBvbmVudD4KICAgICAgICAgIDwvUlNBS2V5VmFs
dWU+CiAgICAgICAgPC9LZXlWYWx1ZT4KICAgICAgPC9LZXlJbmZvPgogICAgPC9EaWduYXR1cmU+
CiAgPC9lbnZlbG9wSW5mb3JtYXRpb24+CjwvbGV0dGVyRGVwb3NpdFBvc3RtYXJrPgo=
```

I.2 Notificación de recepción

La notificación de recepción contiene información sobre el emisor, el sobre, el reto para abrir el sobre y está firmada por el servidor Cmail y por el receptor.

Representa una prueba de recepción para el emisor, que puede utilizarla en caso de litigio.

La especificación formal de la notificación de recepción puede encontrarse en el Anexo A.

Ejemplo: fichero "1373360283931.laura.prin@legalbox.com.receipt.notice"

```
Received: from begmeil get hostname ([127.0.0.1])
        by localhost
        with SMTP (LegalBox POP Server v1.0) id HIWX27L5
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 11:49:01 +0200 (CEST)
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=receiptNotice.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs
ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk
PjEzNzMzNjAyODM5MzE8L2VudmVsb3BJZD4KICAgIDxkZWxpdmVyeU1vZGU+Y2VydGlmaWVkTGV0
dGVyPC9kZWxpdmVyeU1vZGU+CiAgICA8bWltZU1lc3NhZ2VIYXNoPgogICAgICA8c2hhMT5hNTVk
ZDhmYWU0Mzg2M2VmYWRmMWY3ZjM3MmEwYmU1MmEwMGRhYTFkPC9zaGExPgogICAgPC9taW1lTWVz
...
MDkwSDl0NFVkTTdWVU92bjY3WlU2aTJvVSt3b3lGR2tYMDJ3YkVMM2pDYmpJCm5VR1BwUGpoT3Zo
dzNPTy9mYmhKVk13dkM2NXB1MTl1cnA2M05kS0tHNlBuNjZtQkVnUldxZ2cvTVBITmZmWkhrOXFs
WExSSXhETi8Kb0ZnS285RmI0NExlSzBnZ3Vyb1Y2azNicm1TeGM1UnpYVWNxTzdwbldUN0FoNFl6
WXJJUHdYL1hjS1VqbXYxZi9JZjQ5VHVnWGtLcgpodklyOG9qUkdQcEdPdlB4cWR5QWNQR1BOUVRY
NFJrc29kSEVwdz09PC9Nb2R1bHVzPgogICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb25l
bnQ+CiAgICAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICAgIDwvS2V5VmFsdWU+CiAgICAgIDwv
S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogICAgPC9lbnZlbG9wZWQtc2hhbGVuZ2U+CjwvbGV0dGVy
RGVwb3NpdFBvc3RtYXJrPgo=
```

I.3 Notificación de tránsito

La notificación de tránsito contiene información sobre el emisor, el sobre, el reto para abrir el sobre y está firmada por los servidores Cmail.

Representa una prueba del tránsito para el emisor, que puede utilizarla en caso de litigio.

La especificación formal de la notificación de tránsito puede encontrarse en el Anexo A.

Ejemplo: fichero "1373360283931.laura.prin@legalbox.com.receipt.notice"

```
Received: from begmeil get hostname ([127.0.0.1])
        by localhost
        with SMTP (LegalBox POP Server v1.0) id HIWX27L5
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 11:49:01 +0200 (CEST)
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=receiptNotice.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs
ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk
PjEzNzMzNjAyODM5MzE8L2VudmVsb3BJZD4KICAgIDxkZWxpdmVyeU1vZGU+Y2VydGlmaWVkTGV0
dGVyPC9kZWxpdmVyeU1vZGU+CiAgICA8bWltZU1lc3NhZ2VIYXNoPgogICAgICA8c2hhMT5hNTVk
ZDhmYWU0Mzg2M2VmYWRmMWY3ZjM3MmEwYmU1MmEwMGRhYTFkPC9zaGExPgogICAgPC9taW1lTWVz
...
MDkwSDl0NFVkTTdWVU92bjY3WlU2aTJvVSt3b3lGR2tYMDJ3YkVMM2pDYmpJCm5VR1BwUGpoT3Zo
dzNPTy9mYmhKVk13dkM2NXB1MTl1cnA2M05kS0tHNlBuNjZtQkVnUldxZ2cvTVBITmZmWkhrOXFs
WExSSXhETi8Kb0ZnS285RmI0NExlSzBnZ3VyblY2azNicm1TeGM1UnpYVWNxTzdwbldUN0FoNFl6
WXJJUHdYL1hjS1VqbXYxZi9JZjQ5VHVnWGtLcgpodklyOG9qUkdQcEdPdlB4cWR5QWNQR1BOUVRY
NFJrc29kSEVwdz09PC9Nb2R1bHVzPgogICAgICAgICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb251
bnQ+CiAgICAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICAgIDwvS2V5VmFsdWU+CiAgICAgIDwv
S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogICAgPCEtLSBvcmVjaXBpZW50Q2hhbGVuZ2U+CjwvbGV0dGVy
RGVwb3NpdFBvc3RtYXJrPgo=
```

I.4 ENVELOPE

ENVELOPE es un mensaje MIME que contiene el contenido del correo electrónico cifrado con encriptación AES.

Ejemplo: fichero "1373360283931.certifiedLetter.msg"

```
Received: from localhost ([127.0.0.1])
        by begmeil
        with SMTP (SubEthaSMTP null) id HIWV8HF9
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 10:58:03 +0200 (CEST)
Date: Tue, 9 Jul 2013 10:57:51 +0200 (CEST)
From: david.keller@legalbox.com
To: laura.prin@legalbox.com
Message-ID: proto_cmtp_1373360269856
Subject: =?UTF-8?Q?Bienvenue_=C3=A0_CMTP!?=
MIME-Version: 1.0
Content-Type: multipart/mixed;
       boundary="----=_Part_1_1013939722.1373360271613"

------=_Part_1_1013939722.1373360271613
Content-Type: multipart/mixed;
       boundary="----=_Part_0_2062834323.1373360271584"

------=_Part_0_2062834323.1373360271584
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=envelop

RG44gUlyr1A/L+ps0R+yKMUpgPcJACmcRQdLZSMoLnm07gtRataSAWkG5qnc/f5Q

------=_Part_0_2062834323.1373360271584--

------=_Part_1_1013939722.1373360271613--
```

Bibliografía

[b-UIT-T X.509] Recomendación UIT-T X.509 (2012) | ISO/CEI 9594-8:2014, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2016