国 际 电 信 联 盟

ITU-T X.1341

(09/2015)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务 – PKI相关建议书

经认证的邮件传输和经认证的邮局协议

ITU-T X.1341 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI 相关建议书	**X.1340–X.1349**
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1341建议书

经认证的邮件传输和经认证的邮局协议

摘要

本建议书旨在定义经认证的邮件传输协议（CMTP）和经认证的邮局协议（CPOP），以便通过提供机密性、认证、完整性和不可否认性，以一种安全的方式来促进世界电子认证邮件的交换。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1341	2015-09-17	17	11.1002/1000/12352

关键词

经认证的邮件传输协议，经认证的邮局协议，CMTP、机密性、CPOP、完整性、不可否认性、POP、邮局协议、安全、简单邮件传输协议。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

本建议书旨在扩展简单邮件传输协议（SMTP）和第3版邮局协议（POP3），以支持认证、安全性和不可否认性。

出于此目的，规定了两个协议：

– 经认证的邮件传输协议（CMTP），这是简单邮件传输协议（SMTP）的扩展，是支持电子邮件发送方与邮件服务器之间通信的协议，邮件服务服务器称为经认证的邮件（Cmail）服务器；

– 经认证的邮局协议（CPOP），这是第3版邮局协议（POP3）的扩展，是支持电子邮件接收方与Cmail服务器之间通信的协议。

在SMTP和POP3内，消息类型由命令确定，即消息开始处的关键字。为CMTP和CPOP定义了新的命令，并对一些SMTP和POP3命令进行了扩展。特别是，对一些命令进行了扩展，以便承载通知（电子文档），允许归档和验证从发送方到接收方通信的不同阶段。

CMTP和CPOP还引入了Cmail服务器的概念，在发送方与接收方之间的通信中，这是一个积极主动的合作伙伴，允许它来对双方之间确实已发生的交换进行验证。

经认证的邮件假定已建立现有的公开密钥基础设施（PKI）。

附件A，是本建议书的有机组成部分，为使用XML模式定义（XSD）标记技术的通知提供了正式规范。

附件B，是本建议书的有机组成部分，为使用抽象语法标记1（ASN.1）的通知提供了正式规范。

附件C，是本建议书的有机组成部分，详细说明了关于签发给客户端（电子邮件的发送方和接收方）和Cmail服务器的公开密钥证书的要求。

附件D，是本建议书的有机组成部分，详细说明了关于传输层安全（TLS）规范的要求。

附录E，是本建议书的有机组成部分，详细说明了为Cmail服务器定义的对象标识符。

ITU-T X.1341建议书

经认证的邮件传输和经认证的邮局协议

1 范围

本建议书旨在说明如何保障电子邮件的识别和机密性。

经认证的邮件传输协议/经认证的邮局协议（CMTP/CPOP）能够：

– 解决否认问题，因为使用了电子签名；

– 解决保密问题，因为使用了加密技术；

– 产生可靠的寄存通知、发送通知和接收通知；

– 使用经认证的邮件（Cmail）服务器来跟踪经认证的邮件，以免在处理过程中丢失

– 使用传输层安全（TLS）连接来提供更强大的识别水平。这种更强大的识别水平是Cmail服务器要求的。

遵守本建议书无法证明用户同时遵守了国家或地区法律、法规和政策。建议书中提及的技术、组织和程序手段无法确保特定国家或地区法律、法规和政策规定的通信安全。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书或其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。本建议书中引用某个文件，并非确定该文件具备建议书的地位。

[ITU-T X.520] ITU-T X.520 (2012) | ISO/IEC 9594-6建议书：2014，信息技术 — 开放系统互连 — 号码簿：选择属性类型

[ITU-T X.680] ITU-T X.680 (2008) | ISO/IEC 8824-1建议书：2008，信息技术 — 抽象语法标记1（ASN.1）：基本标记规范。

[ITU-T X.690] ITU-T X.690 (2008) | ISO/IEC 8825-1建议书：2008，信息技术 — ASN.1编码规则：基本编码规则（BER）规范，规范编码规则（CER）和区分编码规则（DER）。

[ITU-T X.693] ITU-T X.693 (2008) | ISO/IEC 8825-4建议书：2008，信息技术 — ASN.1编码规则；XML编码规则（XER）。

[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 定义

3.1 在其他处定义的术语

本建议书使用了以下在其他地方定义的术语：

3.1.1 认证机构（CA）[b-ITU-T X.509]：被一个或多个用户所信任的机构，用于创建和指派公开密钥。可选地，认证机构可创建主体的密钥。

3.1.2 证书验证[b-ITU-T X.509]：确保证书在某个特定时间有效的过程，包括可能构建和处理一个认证通路，并确保在该特定时间该通路上的所有证书是有效的（即不过期或不被撤销）。

3.1.3 散列函数[b-ITU-T X.509]：一个（数学）函数，它从一个大（可能非常大）的范围将值映射至一个较小的范围上。一个“好的”散列函数是这样一个函数，即在将之应用于范围内一个（大的）值的集合时，在整个范围内结果将均匀分布（并显然是随机的）。

3.1.4 私有密钥[b-ITU-T X.509]：（在公开密钥加密系统中）一个实体的密钥对中只有该实体知晓的那个密钥。

3.1.5 公开密钥[b-ITU-T X.509]：（在公开密钥加密系统中）用户密钥对中公开知晓的那个密钥。

3.1.6 公开密钥证书（PKC）[b-ITU-T X.509]：用户的公开密钥，以及其他一些信息，利用发放它的认证机构（CA）的私有密钥，通过数字签名不可伪造地予以提供。

3.1.7 公开密钥基础设施（PKI）[b-ITU-T X.509]：能够支持公开密钥管理的、能够支持鉴权、加密、完整性或不可否认服务的基础设施。

3.2 在本建议书中定义的术语

本建议书定义了以下术语：

3.2.1 经认证的邮件：利用经认证的邮件传输协议（CMTP）和经认证的邮局协议（CPOP）交换的电子邮件。

3.2.2 经认证的邮件传输协议：基于SMTP，通过TCP/IP连接用于发送经认证的邮件的应用层协议。

3.2.3 经认证的邮局协议：基于POP3、通过TCP/IP连接用于接收经认证的邮件的应用层协议。

3.2.4 Cmail服务器：涉及经认证的邮件事务的可信实体。

3.2.5 寄存通知：发送方和Cmail服务器签署的电子文件，包含可用来对经认证的邮件是否已寄存进行认证的信息。

3.2.6 接收通知：接收方和Cmail服务器签署的电子文件，包含可用来对经认证的邮件是否已被接收方接收进行认证的信息。

3.2.7 发送通知：事务中涉及的Cmail服务器签署的电子文件，包含可用来对经认证的邮件是否已被发送给Cmail服务器进行认证的信息。

3.2.8 第3版邮局协议：在使用 (TCP/IP) 连接接收邮件时应用传输层标准。

3.2.9 简单邮件传输协议：在使用 (TCP/IP) 连接发送邮件时应用传输层标准。

4 缩写词和首字母缩略语

本建议书使用了以下缩写词和首字母缩略语：

AES 高级加密标准

ASN.1 抽象语法标记1

CA 认证机构

CBC 密码块链接

Cmail 经认证的邮件

CMTP 经认证的邮件传输协议

CPOP 经认证的邮局协议

DER 区分编码规则

DNS 域名系统

id 身份

MIME 多用途互联网邮件扩展

PKI 公开密钥基础设施

POP3 第3版邮局协议

RSA Rivest、Shamir和Adleman算法

RSCK 随机对称密码密钥

S/MIME 安全/多用途互联网邮件扩展

SMTP 简单邮件传输协议

TCP/IP 传输控制协议/网际协议

TLS 传输层安全

UTF-8 UCS转换格式-8

XER XML编码规则

XML 扩展标记语言

XSD XML模式定义

5 惯例

无

6 经认证的邮件基本概念

在使用简单邮件传输协议（SMTP）和第3版邮局协议（POP3）的传统电子邮件通信中，电子邮件的接收方可以否认曾经收到过电子邮件。甚至在安全/多用途互联网邮件扩展（S/MIME）添加到协议族时，情况也这样。S/MIME提供了消息加密和发送方验证功能，但它未提供提交证明功能。

本建议书是对称为经认证的邮件协议族的详细说明，由经认证的邮件传输协议（CMTP）和经认证的邮局协议（CPOP）组成。

在SMTP/POP3通信中，邮件服务器不是通信的积极参与方，只是在接收方告知邮件服务器消息已收到后将之予以转发。甚至在应用SMIME时，情况也这样。

在经认证的邮件中，邮件服务器是发送方和接收方之间通信的积极参与方，参与方式是，允许Cmail服务器对收件方是否已收到邮件进行验证。加密发送的邮件不允许Cmail服务器读取电子邮件的实际内容。下面对该过程中做了概述，同时在条款8中给出了详细说明。

发送方与Cmail服务器之间的交互在条款8中予以详细说明。

接收方与Cmail服务器之间的交互在条款9中予以详细说明。

7 经认证的邮件命令类型

经认证的邮件利用当前SMTP和POP3命令的组合、一些增强的SMTP和POP3命令，以及一些经认证的邮件特定的命令。在表1和表2中，对在SMTP/POP3中没有对应命令的命令标记为“额外的”；增强的SMTP/POP3命令标记为“改进的”；未改变就用的SMTP/POP3命令标记为“未变的”。

一个命令类型定义为一个使用大写字母来标识一个特定消息类型以及有关该消息类型一些额外说明的关键字。

7.1 CMTP命令类型

表 1 – CMTP命令

命令	命令功能
CELO 额外的	使服务器能够确定其对CMTP命令的处理。
DELV 额外的	确定提交模式：certifiedMail。
MAIL FROM 改进的	确定消息的发送方，作为“MAIL FROM”。如果账户存在于服务器上，那么它发回一个已知发送方公开密钥证书的base64。
RCPT TO 改进的	确定消息的接收方；以“RCPT TO”格式来用。如果账户存在于服务器上，那么它发回一个已知发送方公开密钥证书的base64。如果账户存在于另一个CMTP服务器上，利用之，已完成密钥交换，那么服务器提问第二个服务器，并利用CHCK RCPT命令，发送一个属于已知接收方的、公开密钥证书的base64。
CHCK RCPT 额外的	只有当接收方连接于另一个Cmail服务器而非发送方的Cmail服务器时，才发送。
DATA 改进的	由客户端发送，以启动消息内容的传送。服务器发回一个经服务器签署并将由发送方签署的寄存通知。
DEPO 额外的	由客户端发送，以启动传送关于寄存内容的通知，它经服务器签署并经发送方会签。
SEND EVLP 额外的	将信封从一个Cmail服务器转发到另一个Cmail服务器。
HELP 未变的	返回一个CMTP服务器支持的命令清单。
QUIT 未变的	终止会话。

7.2 CPOP命令类型

表 2 – CPOP命令

命令	命令功能
USER 未变的	用于指定正在登录之用户的名字。
PASS 未变的	正在登录之用户的密码。
LIST 改进的	用于列出消息及其组合规模。例如，调用不带任何参数的LIST命令，将返回2个+OK消息（320个八位字节），以及消息清单：身份（id）、长度以及像CertifiedMail的提交模式（如果有的话）。

表 2 – CPOP命令

命令	命令功能
RETR 改进的	其中，N是介于1与LIST命令最后返回之数目之间的一个数。该命令不得用于检索已被标记为删除的消息。如果没有任何提交类型，那么服务器以多用途互联网邮件扩展（MIME）编码形式发送电子邮件。如果定义了发送模式，那么服务器对消息做专门处理。例如，对CertifiedMail，在使用RCPT命令发送信封之前，服务器对接收方提出质疑。
CHLG RESP 额外的	由客户端发送，为消息提供接收通知，并为秘密问题提供答复。如果答复是正确的，那么服务器发回MIME信封。
SEND NORP 额外的	发送经签署的接收通知。
HELP 未变的	返回一个CPOP服务器支持的命令清单。
QUIT 未变的	终止会话。

8 详细的CMTP规范说明

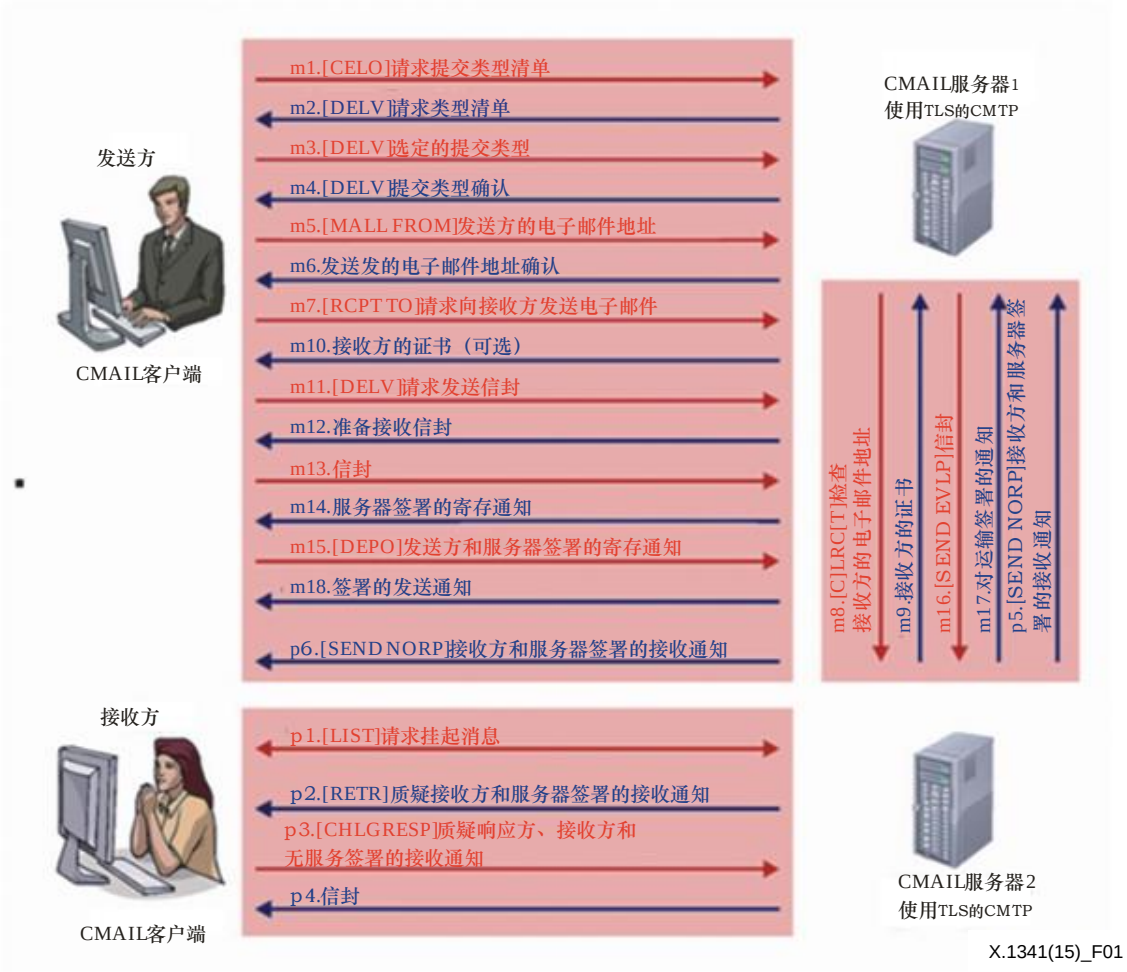

图 1 – 协议交换概述

命令前缀为“m”，用在CMTP协议中；命令前缀为“p”，用在CPOP协议中。条款8.1详细说明了图1中m1-m18的交换过程；条款8.2详细说明了p1-p6的交换过程。

8.1 CELO：请求提交类型清单

命令类型作为一条SMTP消息予以发送，类似于HELO命令，紧随其后的是一个完全合格的域名。其目的旨在检索提交类型清单。

8.2 提交类型清单

响应CELO命令，给出了提交类型清单。以SMTP格式，内容如下所示（不分大小写）：

250 – <Cmail服务器完全合格的域名>

250 – 8BITMIME

250 – 提交类型CertifiedMail <其他提交类型>

250 OK

本建议书仅对CertifiedMail做规范说明。未来版本可对其他的提交类型做出规范说明。

8.3 选定的提交类型

此邮件从提交类型列表中标识指定的交付类型。它具有以下（SMTP）格式：

DELV <提交类型>

8.4 提交类型确认

在选定的提交类型被接受的情况下，本消息有以下SMTP格式（不分大小写）：

250 提交类型 <提交类型> OK

当在选定的提交消息中出现语法错误的情况下，给出以下响应：

501 语法：DELV <提交类型>

当在序列外发布选定的提交消息时，给出以下响应：

501 语法：首先使用CELO命令

当选定的提交消息未知时，给出以下响应：

501 未知的提交类型：<提交类型>

8.5 发送方的电子邮件地址

本消息被发送至Cmail服务器，以请求发送一个经认证的邮件，选择地，从Cmail服务器处请求发送方的公开密钥证书。

MAIL FROM <发送方的电子邮件地址> [CertificateRequested]

8.6 发送方的电子邮件确认

发送本消息，以确认发送方的电子邮件地址存在于Cmail服务器数据库中。如果发送方请求其公共密钥证书，那么包括发送方的公开密钥证书：

[250 用户证书：<以Base64编码的公开密钥证书>]

250 OK

8.7 请求向接收方发送电子邮件

向Cmail服务器发送本消息，以请求向接收方发送一个经认证的邮件，可选地，从Cmail服务器处请求接收方的公开密钥证书。

RCPT TO <接收方的电子邮件地址> [CertificateRequested]

如果有几个接收方的话，为了增加各个接收方，根据需要可多次使用本命令。指明接收方是“To”还是“CC”的信息包含在信封头中[IETF RFC 5321]。“BCC”接收方是不允许的。

8.8 通过远程Cmail服务器检查接收方的电子邮件地址

只有当接收方连接于另一个Cmail服务器而非发送方的Cmail服务器时，才发送本消息。从发送方的Cmail服务器发给接收方的Cmail服务器，以检查电子邮件地址的有效性，可选地，请求接收方的公开密钥证书。

CHCK RCPT <接收方的电子邮件地址> [CertificateRequested]

8.9 接收方的电子邮件地址确认

发送本消息，以响应“由远程Cmail服务器来检查接收方的电子邮件地址”。

如果是这样请求的话，那么以下用于确认电子邮件地址，包括接收方的公开密钥证书：

[250 用户证书：<以Base64编码的公开密钥证书>]

250 OK

在电子邮件地址不能得到确认的情况下，可发送以下错误消息：

503 发送方已经指定

如果它是一个对双重请求的响应，那么应予发送。

501 语法：CHCK RCPT <地址>

如果在接收方的电子邮件地址中存在语法错误，那么应予发送。

501 语法：CHCK RCPT <地址> 参数中的错误：<参数>

如果电子邮件地址后的参数不被认可，那么应予发送。

553 <邮件地址> 无效的电子邮件地址

如果电子邮件地址不存在于远程Cmail服务器中，那么应予发送。

8.10 接收方的电子邮件确认

发送本消息，以确认接收方的电子邮件地址是否存在。如果发送方请求接收方的公开密钥证书，那么包括接收方的公开密钥证书。

如果是这样请求的话，那么以下用于确认电子邮件地址，包括接收方的公开密钥证书：

[250 用户证书：<以Base64编码的公开密钥证书>]

250 OK

在电子邮件地址不能得到确认的情况下，可发送以下错误消息：

503 错误：需要MAIL FROM命令

如果在序列外发送消息，那么应予发送。

452 错误：接收方太多

如果指定了太多的接收方，那么应予发送。

501-6.1.1 语法：RCPT TO <地址>

如果在接收方的电子邮件地址中存在语法错误，那么应予发送。

501-6.1.2 语法：RCPT TO <地址> 参数中的错误：<参数>

如果电子邮件地址后的参数不被认可，那么应予发送。

550-5.1.1 <电子邮件地址> 无效的电子邮件地址

如果电子邮件地址不存在，那么应予发送。

8.11 请求发送ENVELOPE

发送方使用以下格式来请求Cmail服务器允许发送数据：

DATA

8.12 准备接收ENVELOPE

如果Cmail服务器准备接收数据，那么发送以下消息：

354 开始邮件输入；以<CRLF>.<CRLF>结束。

当尚未发送MAIL FROM命令时，发送以下消息：

503错误：需要MAIL FROM命令

当尚未发送RCPT TO命令时，发送以下消息：

503 错误：需要RCTP TO命令

当尚未发送DELV命令时，发送以下消息：

503 错误：需要DELV命令

8.13 ENVELOPE

客户端应：

1. 生成一个随机的对称密码密钥（RSCK），如高级加密标准（AES）256；
2. 如果有的话，使用该密钥，对消息正文和附件进行加密；
3. 建立一个包含称为ENVELOPE部分的MIME消息，它包含经过加密的消息（参见[IETF RFC 2045]）；
4. <CR><LF>.<CR><LF>结束消息；以及
5. 发送MIME消息。

8.14 服务器签署的寄存通知

250 寄存通知

<以base64编码、由Cmail服务器签署的寄存通知>

250 OK

服务器生成一个寄存通知，包含关于信封的信息（信封id、提交类型和mime散列），并用私钥签署之。

8.15 发送方和服务器签署的寄存通知

发送方应：

1. 对收到的寄存通知进行解码；
2. 质疑各个接收方；
3. 使用其自身的私有密钥对经服务器签署的寄存通知进行签署；
4. 以base64对结果进行编码；以及
5. 使用以下命令将之发送至Cmail服务器：

DEPO <以base64编码的寄存通知>

质疑在附近A图A.6 – 质疑中进行定义。

质疑包含**SecretQuestion**, **CipherEnvelopeKey**以及接收方的公开密钥证书。

SecretQuestion: 由一个**Request**和一个**Response**组成

Request可包含一个**RandomNumber**。Response包含**AlgorithmIdentifier**，由发送方重新计算，以便接收ENVELOPE。该**AlgorithmIdentifier**确定用于计算散列的算法。质疑包括首先恢复密码密钥RSCK、利用接收方的公开密钥进行加密，然后连接**RandomNumber**和RSCK、计算散列来构建响应。

在可扩展标记语言（XML）中的质疑例子如下所示：

```
<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>
```

注1 – 该质疑可使用抽象语法标记1（ASN.1）区分的编码规则（DER）。

注2 – 服务器不能重新计算散列，原因是它不知道加密密钥。不过，只有服务器知道来自散列计算的预期结果。

注3 – 在接收方质疑期间，服务器只发送秘密问题，并等待接收方的答复。

8.16 Cmail服务器之间的ENVELOPE

只有当发送方和接收方连接于不同的Cmail服务器时（参见图1中的条目m16），才将条款8.13中定义的消息转发给另一个Cmail服务器。

SEND EVLP <MIME 消息>

8.17 Cmail服务器之间签署的寄存通知

应使用以下格式：

250 发送通知：

<以base64编码的发送通知>

如果Cmail服务器收到一个发送通知，那么发送以下消息：

250 Ok

当发送通知不正确时，发送以下消息：

503 错误：错误的发送通知

由接收ENVELOPE的Cmail创建发送通知。

本Cmail服务器生成一个寄存通知，包含关于信封的信息（信封id、提交类型和mime散列），并以其私有密钥签署之。本通知与寄存通知是一样的。

8.18 签署的发送通知

Cmail发送方服务器应：

1. 对收到的发送通知进行解码；
2. 使用其自身的私有密钥对经服务器签署的发送通知进行签署；
3. 以base64对结果进行编码；以及

4. 使用以下命令将之发送至Cmail服务器：

250 经签署的发送通知：

<以base64编码、经签署的发送通知>

250 经签署的寄存通知

<以base64编码、经签署的寄存通知>

250 Ok

9 经认证的邮局协议（CPOP）

图1的p1到p6的解释参见9.1 到 9.6节。

9.1 请求挂起消息

以一个额外的参数，用[IETF RFC 1939]中的LIST命令，使用第5节中规定的程序，执行关于挂起消息的信息。对每一个用于详细说明挂起消息的行，如果它不是一个标准的电子邮件，那么添加额外的参数，以指明提交类型（参见图1中的p1项）。例如：

C：LIST

S： +OK 2消息（320个八位字节）

S：1120

S：2200 CertifiedMail

S：.

本程序还包括检索所有标准的电子邮件，只留下Cmail服务器上以提交类型标记的消息。

9.2 质疑接收方和服务器签署的接收通知

对以提交类型标记的消息，RETR命令不检索消息，但检索质疑以及以base64编码、经服务器签署的接收通知。客户端对包含在接收通知中的数字签名和发送方证书进行验证。

例如：

C：RETR 2

如果Cmail服务器发送接收通知，那么发送以下消息：

S： +OK 200 八位字节

S： <Cmail服务器发送接收通知，包括质疑>

S：.

当服务器无法发送接收通知时，发送以下消息：

503 错误：不可能发送接收通知

Cmail服务器在寄存通知中查找与接收方有关的节点**`Entity`**。然后，Cmail服务器在接收通知中拷贝该节点，并删去包括在**`Entity`**节点中的**`Response`**节点的内容。

例如，在寄存通知中的一个节点：

```
<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>
```

注1 – 该质疑可使用ASN.1 DER编码。

在接收通知中拷贝相同的节点：

```
<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>
```

注2 – 该质疑可使用ASN.1 DER编码。

9.3 质疑响应方、接收方和服务器签署的接收通知

接收方应：

1. 对收到的接收通知进行解码；
2. 检索RSCK；
3. 计算质疑响应；
4. 使用其自身的私有密钥对经服务器签署的接收通知进行签署；
5. 以base64对结果进行编码；以及
6. 使用以下命令将之发送至Cmail服务器：

CHLG RESP <质疑响应和接收方以及服务器签署的接收通知>

接收方对消息进行解密，如下所示：

```
<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>
```

注 – 该质疑可使用ASN.1 DER编码。

通过解密节点**CipherEnvelopeKey**的内容，接收方使用其私有密钥恢复RSCK。然后，接收方连接**RandomNumber**和RSCK，使用定义的**AlgorithmIdentifier**散列之，获得**SecretQuestion**的结果。

接收方在签署的接收通知中拷贝该结果，签署之，并将之发送至Cmail服务器。

9.4 ENVELOPE

如果质疑是OK，那么Cmail服务器以相同的方式发送ENVELOPE，作为命令RETR的结果。接收方现有打开它的消息和密钥。

当服务器不能发送ENVELOPE时，发送以下消息：

503错误：不可能发送ENVELOPE

9.5 Cmail服务器之间接收方和服务器签署的寄存通知（可选）

只有当发送方和接收方连接于不同的Cmail服务器上时，才发送本消息。

SEND NORP <以base64编码的接收方和服务器签署的接收通知>

9.6 接收方和服务器签署的接收通知

只有当发送方和接收方连接于不同的Cmail服务器上时，才发送本消息。

SEND NORP <以base64编码的接收方和服务器签署的接收通知>

附件 A

XML模式定义（XSD）中的通知

（本附件是本建议书的组成部分。）

本附件利用如[XSD]中所规定的XML模式定义（XSD），提供了关于各通知的规范说明。在XML中，对一个通信实例进行了编码，如[XML]中所规定的那样，并符合在本附件中给出的XSD规范。

A.1 XSD概述

参见A.1到A.10.

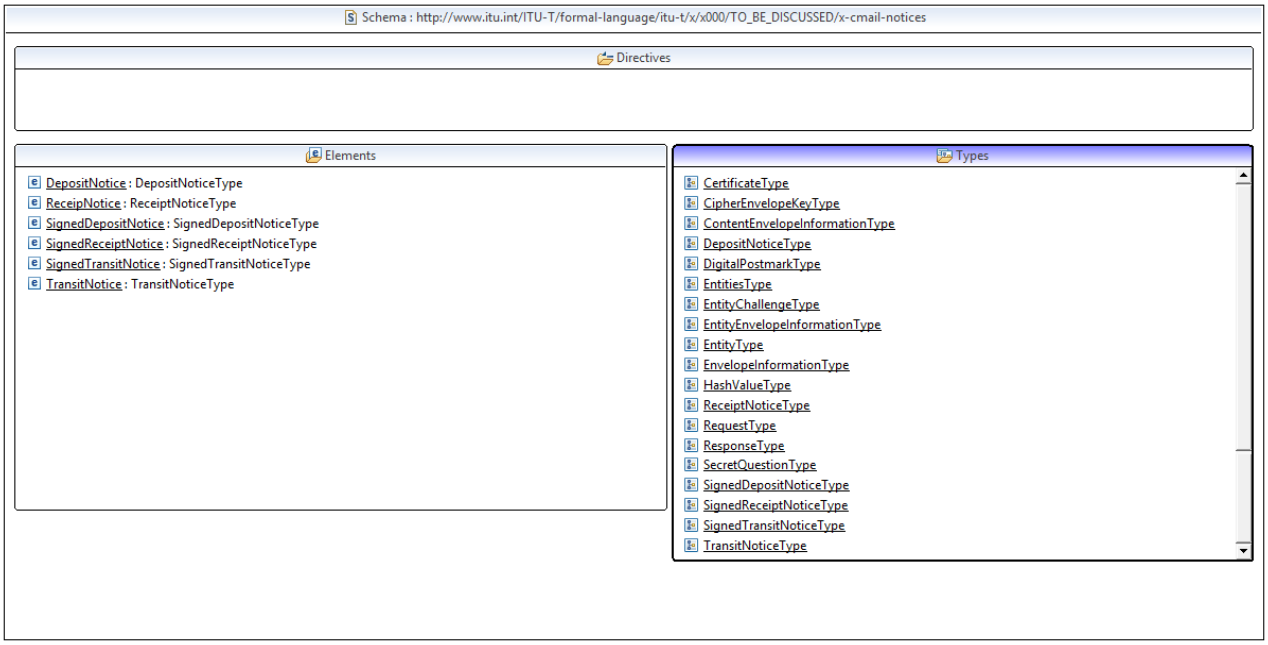

图 A.1 – 要素和类型清单

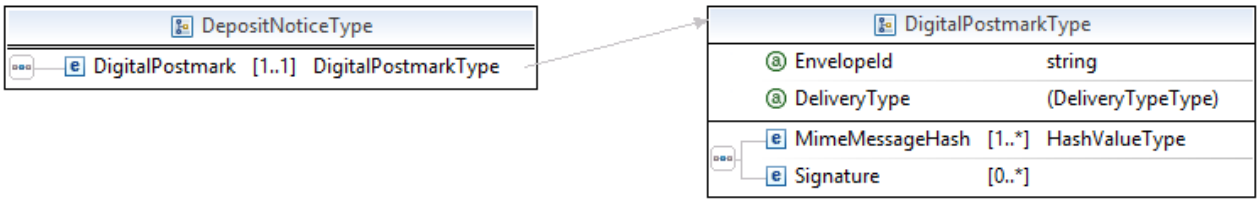

图 A.2 – 寄存通知

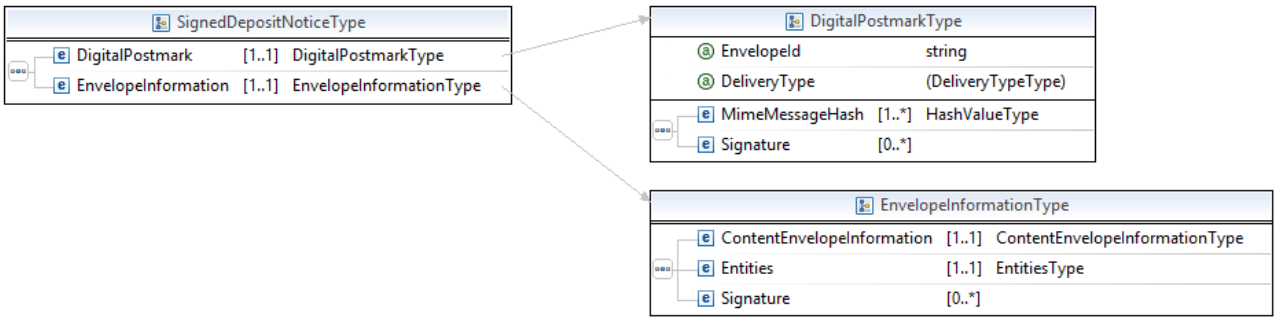

图 A.3 – 经签署的寄存通知

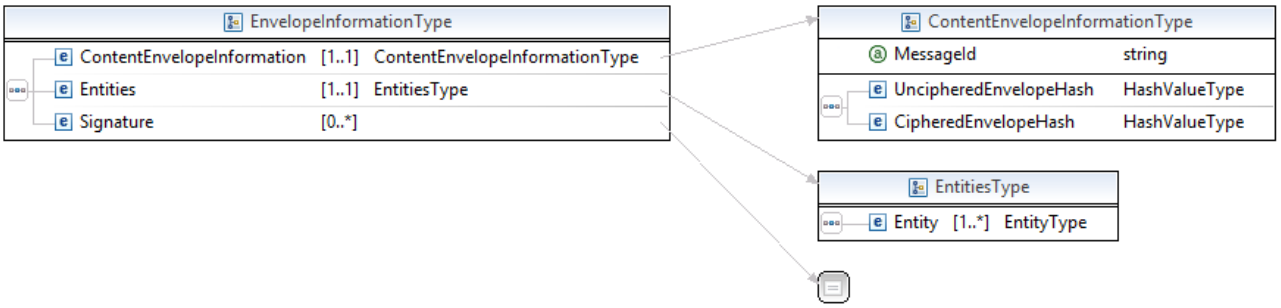

图 A.4 – 信封信息类型

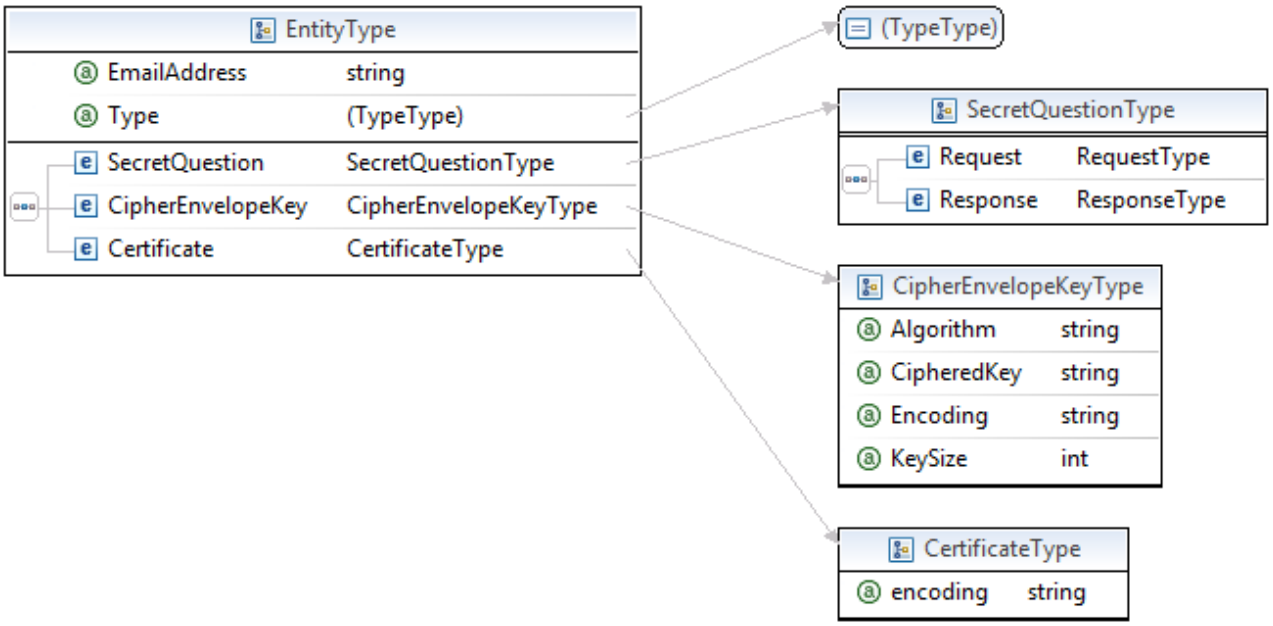

图 A.5 – 实体类型

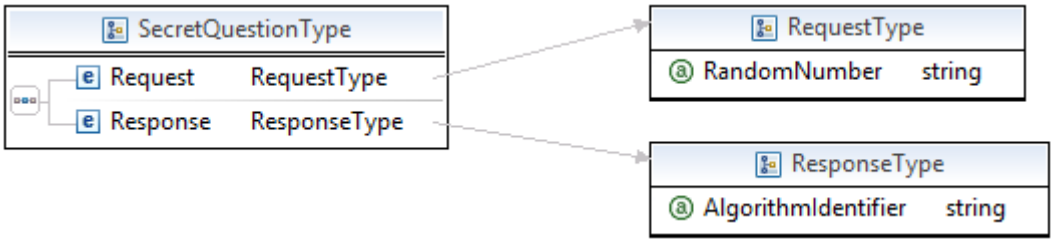

图 A.6 – 质疑

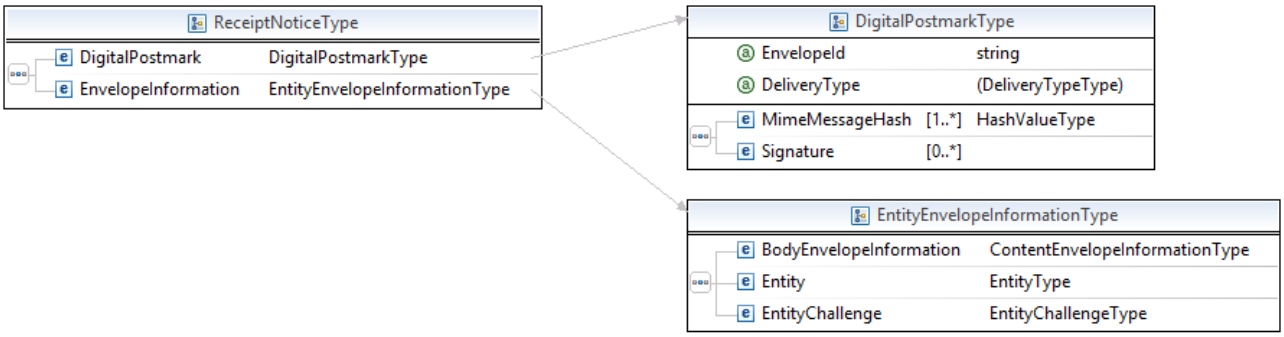

图 A.7 – 接收通知

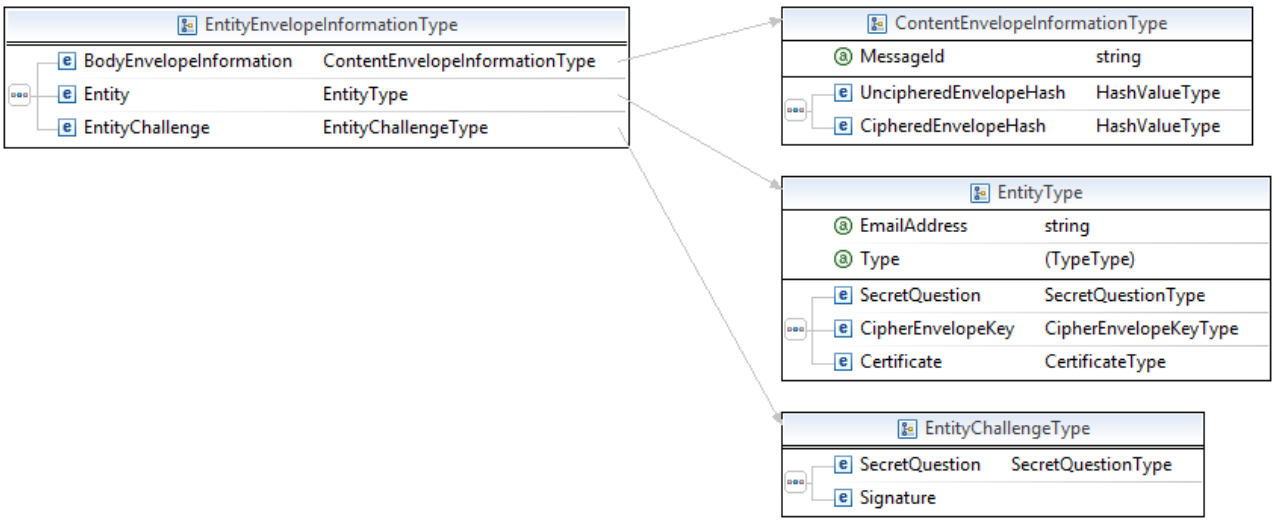

图 A.8 – 接收方对质疑的回答

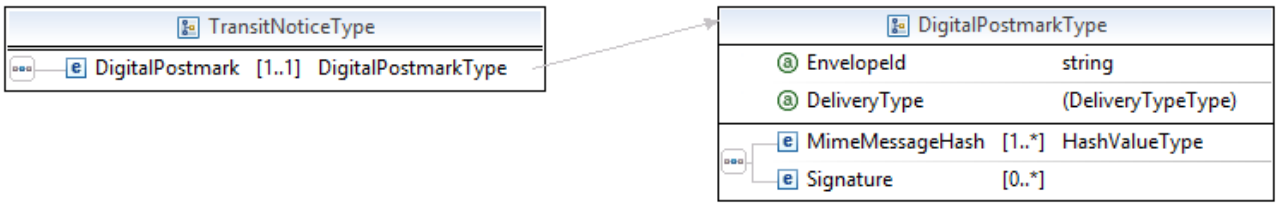

图 A.9 – 发送通知

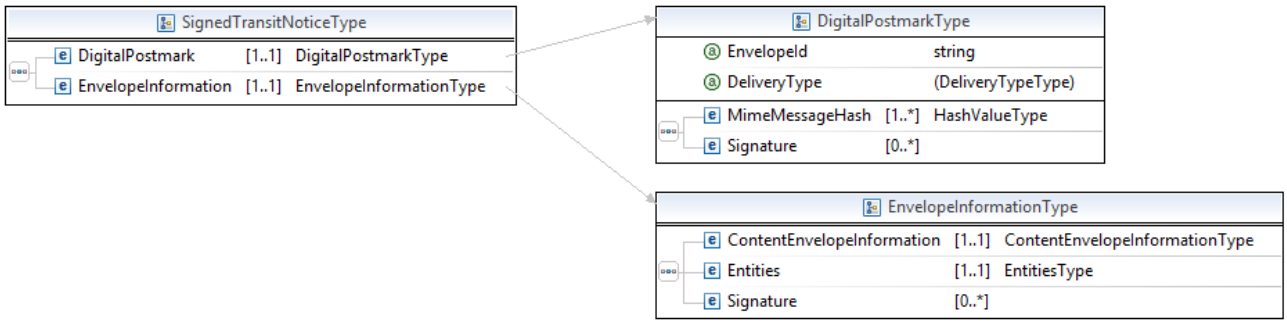

图 A.10 – 经签署的发送通知

A.2 XSD中通知的正式规范

```
<?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>
```

附件 B

ASN.1中的通知

（本附件是本建议书的组成部分。）

本附件提供了关于抽象语法标记1（ASN.1）中各注释的规范说明，如[ITU-T X.680]中所规定的那样。可使用ASN.1区分编码规则（DER）来对各通知进行编码，如[ITU-T X.690]中所规定的那样，或者可使用扩展XML编码规则（EXTENDED-XER）来对各通知进行编码，如[ITU-T X.693]中所规定的那样。在后一种情况中，来自该编码的XML等同于根据XDS生成的XML，如附件A中所规定的那样。

```
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
```

附件 C

关于公开密钥基础设施组成部件的要求

（本附件是本建议书的组成部分。）

C.1 引言

本附件提供关于签发给Cmail服务器和客户端的、公开密钥证书的要求。

C.2 Cmail服务器终端实体公开密钥证书

签发给Cmail客户端的、一个终端实体的公开密钥证书应有以下内容：

a) 对第3版做详细说明。

b) CA生成非时序的序列号。

c) 主体字段应持有一个带组成部件的目录区分名单，其单个组成部件使用**dnsName**属性类型，如[ITU-T X.520]中所定义。值应为一个经注册的DNS名称。

d) 主体选择性名称扩展应以两个元素给出：

- 对一个元素采用**rfc822Name**选择，应为Cmail服务器管理员的电子邮件地址。
- 对另一个元素采用**directoryName**选择，应持有带以下组成部件的区分名称：
  - **countryName**应出现，并应持有[ISO 3166-1]的三字母代码（alpha-3）；
  - **organizationName**应出现，并应持有管理Cmail服务器之组织的可信名称；
  - **streetAddress**应出现，并应持有街道名称和门牌号码；
  - **localityName**应出现，并应持有所在地点的名称；
  - 如果唯一标识需要的话，那么**stateOrProvinceName**应出现；否则，不应出现。
  - **postalCode**应出现，并应持有地点的邮政编码。

e) **certificatePolicies**扩展应出现，并至少应持有对象标识符**{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailServer(1)}**，以发出信号，指明已根据本建议书签发公开密钥证书。

C.3 Cmail客户端终端实体公开密钥证书

签发给Cmail客户端的、一个终端实体的公开密钥证书应有以下内容：

a) 对第3版做详细说明。

b) CA生成非时序的序列号。

c) 主体字段应持有一个带组成部件的目录区分名单，如下所示：

- 如果客户端是一个个体的话，那么**surname**应出现，但如果客户端是一个组织的话，那么**surname**不应出现。
- 如果**surname**出现的话，那么**givenName**应出现，否则它不应出现。
- 如果**surname**出现的话，那么**initials**应出现，否则它不应出现。
- 如果**surname**出现的话，那么**generationQualifier**可出现，否则它不应出现。
- **organizationName**应当现在如果客户端不是一个居住的人，那么**organizationName**应出现，否则它不应出现。如果出现，那么应持有客户端所属之组织的可信名称。
- **streetAddress**应出现，并应持有街道名称和门牌号码。
- **localityName**应出现，并应持有所在地点的名称。
- 如果唯一标识需要的话，那么**stateOrProvinceName**应出现，否则它不应出现。
- **postalCode**应出现，并应持有地点的邮政编码。
- **countryCode3c**应出现，并应持有[ISO 3166-1]的三字母代码（alpha-3）。

d) **subjectAltName**扩展应出现，应包含如下所述的一个元素：
   - **rfc822Name**应持有Cmail服务器管理员的电子邮件地址。

e) **certificatePolicies**扩展应出现，并至少应持有对象标识符**{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailServer(1)}**，以发出信号，指明已根据本建议书签发公开密钥证书。

C.4 信息验证要求

在签发一个公开密钥证书前，签发者应验证：

a) 验证主体（申请者）为包括在公开密钥证书中、经注册的域名持有者。

b) 验证主体的物理存在。

c) 验证主体的操作存在（业务活动）。

d) 验证主体是一个可信的、公认的实体。

e) 验证将置于一个公开密钥证书中的姓名和地址信息。

f) 验证将进入一个公开密钥证书中的**organizationName**是一个用于标识主体的、可信和公认的名称。

附件 D

关于传输层安全（TLS）的要求

（本附件是本建议书的组成部分。）

应支持[IETF RFC 5246]或之后版本。

在谈判中，无论是Cmail服务器还是客户端，都不得接受以下连接，即连接试图协商采用早于TLS 1.2的TLS版本。

一个实施方案应支持以下密码族：

– TLS_DH_RSA_WITH_AES_256_CBC_SHA256

附件 E

在本建议书中定义的对象标识符

（本附件是本建议书的组成部分。）

本建议书定义了以下对象标识符：

a) ASN.1模块相关的对象标识符：

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

b) cmail服务器certificatePolicies扩展使用的对象标识符：

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

c) cmail客户端certificatePolicies扩展使用的对象标识符：

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

附录 I

信封和通知格式

（本附录不是本建议书的组成部分。）

本附录提供了有关通知编码的例子。

I.1 寄存通知

寄存通知包含关于发送方的信息、信封，由Cmail服务器和发送方联合签署。

对发送方而言，这是关于寄存的一个证据，在诉讼中，可利用之。

正式的寄存通知规范说明可在附件A中找到。

例如：文件“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+CiAgICAgICAgPC9SGln
...
ICAgPFJTQUtleVZhbHVlPgogICAgICAgICA8TW9kdWx1cz5tMkFSUURXUGJBMmgvMzJEQWs4
ICAgICAgICAgIDxFeHBvbmVudD5BUUFCPC9FeHBvbmVudD4KICAgICAgICAgIDwvUlNBS2V5VmFs
dWU+CiAgICAgICAgPC9LZXlWYWx1ZT4KICAgICAgICA8L0tleUJmZvPgogICAgPC9TaWduYXR1cmU+
CiAgPC9lbnZlbG9wSW5mb3JtYXRpb24+CjwvbGV0dGVyRGVwb3NpdFBvc3RtYXJrPgo=
```

I.2 接收通知

接收通知包含关于发送方的信息、信封、对打开信封的质疑，由Cmail服务器和接收方联合签署。

对发送方而言，这是关于接收的一个证据，在诉讼中，可利用之。

正式的接收通知规范说明可在附件A中找到。

例如：文件“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
NFJrc29kSEVWdzhBPC9Nb2R1bHVzPgogICAgICAgICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb25l
bnQ+CiAgICAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICAgIDwvS2V5VmFsdWU+CiAgICAgIDwv
S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogIDwvcmVjaXBpZW50Q2hhbGVuZ2U+CjwvbGV0dGVy
RGVwb3NpdFBvc3RtYXJrPgo=
```

I.3 发送通知

寄存通知包含关于发送方的信息、信封、对打开信封的质疑，由Cmail服务器联合签署。

对发送方而言，这是关于发送的一个证据，在诉讼中，可利用之。

正式的发送通知规范说明可在附件A中找到。

例如：文件“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
NFJrc29kSEVWdzhBPC9Nb2R1bHVzPgogICAgICAgICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb25l
bnQ+CiAgICAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICAgIDwvS2V5VmFsdWU+CiAgICAgIDwv
S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogIDwvcmVjaXBpZW50Q2hhbGVuZ2U+CjwvbGV0dGVy
RGVwb3NpdFBvc3RtYXJrPgo=
```

I.4 ENVELOPE

ENVELOPE是一个MIME消息，包含通过AES加密技术进行加密的电子邮件内容。

例如：文件“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--
```

参考书目

[b-ITU-T X.509] ITU-T X.509 (2012) | ISO/IEC 9594-8建议书：2014，信息技术 – 开放系统互连 – 号码簿：公开密钥和属性证书框架。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2016年，日内瓦