一文搞懂 S/MIME 邮件加密 (二)

本文接着上半部分《一文搞懂 S/MIME 邮件加密 (一)》继续讲清楚 S/MIME 邮件加密，在上半部分着重讲了 S/MIME 技术原理和两大核心产品-S/MIME 邮件证书和 S/MIME 邮件客户端。也许大家在读完上半部分的详细介绍后会提出这样的问题：为何这么好的基于国际标准的邮件加密技术从形成国际标准到现在已经 27 年了还没有得到普及应用呢？这正是一个好问题，本部分讲清这个问题，讲清楚实施 S/MIME 邮件加密到底遇到了哪些难题，并简单讲一下零信技术是如何解决这些难题的。

一、 S/MIME 技术为何没有得到普及应用？

要想成功使用 S/MIME 技术实现电子邮件加密，用户必须向 CA 购买和申请 S/MIME 邮件证书，这不仅仅是费用问题，还有一个证书申请流程，用户必须按照 CA 的流程人工手动申请证书，并在收到邮箱验证码后完成邮箱验证，对于需要绑定个人身份或单位身份的邮件证书，还需要提交相关身份证明材料，等待 CA 完成身份鉴证。一旦 CA 签发邮件证书，用户就需要配置邮件证书到支持 S/MIME 技术的邮件客户端中去，各个邮件客户端配置方法都不相同，配置过程都很繁琐。这是第一个困难—证书申请和配置。

第二个困难就是交换公钥，有了邮件证书，就得先与收件人交换公钥证书，经典的做法是向收件人发送一封数字签名明文邮件，收件人保存发件人的公钥证书，并给发件人回复一封数字签名邮件，发件人保存收件人的公钥证书，这就完成了发件人同收件人的公钥交换。如果有 100 个收件人就需要这样操作 100 次，非常繁琐。

第三个困难就是密钥管理，用户从 CA 申请到邮件证书后，必须自己管理好证书私钥和公钥，必须把这些证书导入到所有邮件客户端中使用。如果证书到期，必须重新申请新的证书，但是为了解密以前加密的邮件，必须保持已经过期的证书(含私钥)随时可用，以便解密以前的加密邮件。这些证书管理工作也是非常繁琐的，特别是必须记住证书备份时设置的私钥保护口令，一旦忘记了，就无法导入证书用于解密已加密邮件。

这三个难题往往在第一步就被难住，无法配置邮件证书到邮件客户端中使用，而第二难题交换公钥不仅仅是交换一次，证书过期了，还得重新交换公钥。第三个难题不仅仅要管理一张证书，有多个邮箱需要多张证书，并且是要管理历年以来的所有邮件证书。这个管理过程比管

理 SSL 证书还复杂，SSL 证书过期了就没有用了，无需继续管理。这三大难点就是普及 S/MIME 邮件加密的巨大障碍，使得 S/MIME 技术无法得到普及应用。

二、 零信技术是如何解决 S/MIME 加密应用难题的？

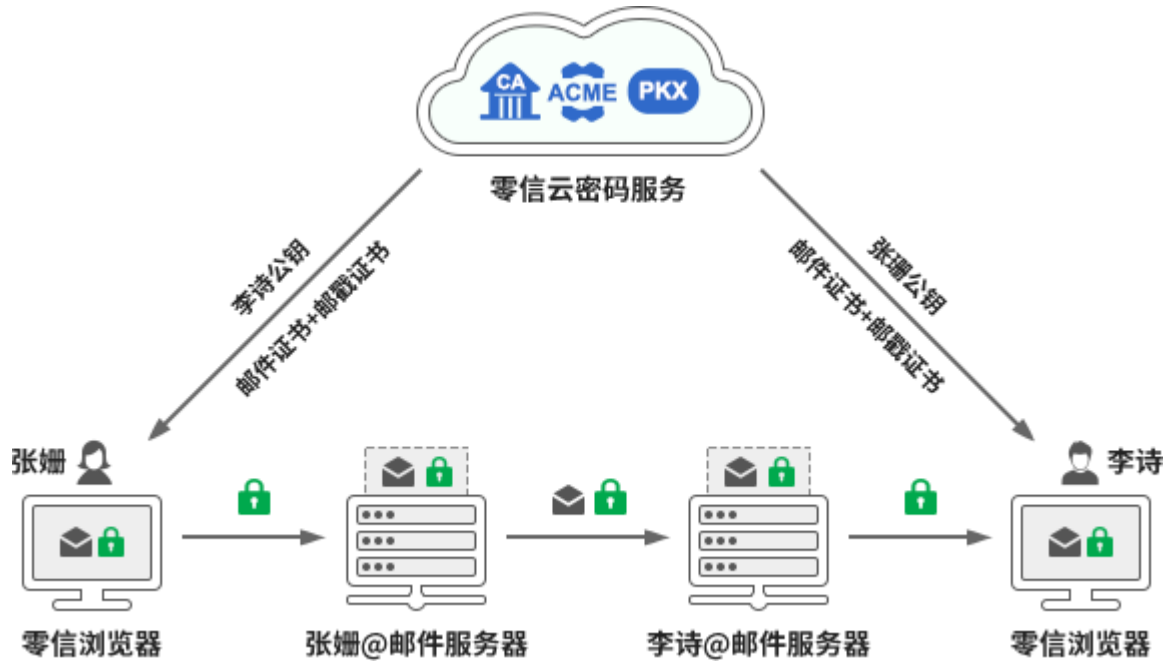
要想解决 S/MIME 邮件加密所面临的三大难题，必须向普及 HTTPS 加密学习，像 SSL 证书一样实现自动化管理，自动化邮件证书申请、自动化邮箱验证、自动化证书配置使用、自动化交换公钥、自动化管理邮件证书。这些自动化难度比 SSL 证书自动化管理更难，因为这是涉及到每一个邮件用户的自动化证书管理，而 SSL 证书只需在每个网站上实现即可，不涉及到每个网站访问者。

零信技术针对以上 S/MIME 邮件加密三大难题提出相应的自动化解决方案，这个解决方案必须是邮件客户端和 CA 系统的合二为一，必须彻底解决目前存在的邮件客户端只管用证书和 CA 系统只管发证书的没有融合的现状。其实，这个融合能力就是零信技术的优势，笔者(公司创始人)从事 CA 业务 18 年，从事邮件客户端开发 4 年，深知这两者的融合之道。

为了解决第一个证书申请和配置难题，零信技术借鉴 SSL 证书自动化管理国际标准(ACME)，同时参考邮件证书自动化管理 RFC 标准提案，实现了双算法 S/MIME 邮件证书的自动化签发和配置使用，用户只需设置好邮箱，能正常收发电子邮件，零信浏览器会自动对接零信云 CA 系统，为用户自动化申请和配置双算法邮件证书，为电子邮件加密和数字签名做好了证书准备。用户无需向 CA 购买和申请邮件证书，无需人工手动完成邮箱验证，无需繁琐地配置邮件证书，一切自动化完成。

为了解决第二个公钥交换难题，零信技术建设了公钥交换系统，用户在给收件人写邮件时，零信浏览器会自动连接零信公钥交换系统获取收件人的公钥证书，用户写完邮件后点击发送就是发送了加密邮件，无需事先同收件人交换公钥，这就解决了公钥交换难题，让用户可以无感发送加密邮件。

为了解决第三个密钥管理难题，零信技术的创新解决方案是使用用户自己的邮箱来备份保存用户密钥和公钥证书，只要用户邮箱在，加密密钥就在，零信浏览器就可以自动获取加密密钥来解密所有已加密邮件，无论是用已经过期的证书加密的还是用未过期的证书加密的，也无论是在哪个设备上，都可以自动化获得用户曾经使用过的密钥来自动化解密已加密邮件，用户根本不用操心密钥管理问题。



由此可见，零信技术是采用了端云一体的创新方案实现了邮件证书自动化、公钥交换自动化和密钥管理自动化，这三个自动化保证了用户可以无感地实现电子邮件加解密，电子邮件数字签名和验签，自动化实现了 S/MIME 加密和数字签名。并且这个自动化服务是完全免费的，免费配置邮件证书，免费实现电子邮件加密和数字签名。

三、 零信技术 S/MIME 邮件加密自动化服务还做了哪些改进和增强？

零信技术不仅实现了邮件证书自动化、公钥交换自动化和密钥管理自动化，而且基于现有数字签名技术和时间戳技术为电子邮件数字签名服务增加了电子邮戳服务，就像传统纸质信件有邮戳一样，自动化为每一封发出的数字签名邮件附署了时间戳签名，确保了电子邮件发送时间可信。

电子邮件数字签名保证了邮件发送者的身份可信和不可否认，电子邮件加密保证了邮件内容的完整性和机密性，而电子邮戳则保证了电子邮件发送时间可信和不可否认，特别适用于需要证明电子邮件发送时间的互联网应用，这是一个全球独家创新应用。

在密钥管理方面，传统的解决方案是采用云密钥管理系统，这的确能解决用户自己管理密钥的难题，但是这并不能解决用户担心的隐私保护问题，如何做好云密钥的安全管理和权限管理是关键，用户也许并不放心由第三方来保管用于加解密的密钥。零信技术改进了密钥管理方案，既保证了密钥在云端保存的可靠性和可用性，又保证了是用户自己管理自己的密钥，在自己的邮箱中保存自己的密钥，这是一个鱼和熊掌可兼得的完美解决方案。这个创新的密钥管理解决方案实现了加密密钥的云端自主保管。

还有一个改进就是 S/MIME 加密的实现手段，传统的方式是开发一个独立的邮件客户端软件，这也是大家常用的实现手段。但是，考虑到用户习惯使用了某个邮件客户端而不想再安装其他邮件客户端的实际应用场景，零信技术则是直接在零信浏览器中集成邮件客户端，让用户无需安装独立的邮件客户端软件。而对于没有安装零信浏览器的用户，大多数用户都会在电脑上安装多个浏览器，如果需要多安装一个浏览器来实现电子邮件加密自动化还是能接受的，毕竟零信浏览器不仅仅是一个必须的支持国密算法的免费国密浏览器，而且还是一个 PDF 阅读器，同时还是一个加密邮件客户端，这样的浏览器再装一个也无妨。更何况安装了零信浏览器就自动给 Windows 打补丁支持国密算法，自动配置的免费电子邮件证书也可以同时用于 Outlook 解密已加密邮件，一举多得。

四、 S/MIME 技术只有自动化实现才能普及应用

通过本文上半部的详细讲解，大家了解 S/MIME 技术的发展历史，S/MIME 加密和数字签名的实现原理，了解 S/MIME 证书和 S/MIME 邮件客户端。本下部分详细解释了为何 S/MIME 技术落地应用难，以及讲解了零信技术是如何创新解决这个难题的。

正如大家熟悉的 HTTPS 加密普及应用得益于 SSL 证书自动化管理一样，S/MIME 加密普及应用也只有 S/MIME 证书自动化管理一条路可走！只有实现了 S/MIME 证书自动化管理，才真正迈出了 S/MIME 技术落地应用第一步。零信技术不仅迈出了这一步，而且实现了第二步的公钥交换自动化，实现了第三步的密钥管理自动化，还创新增加了电子邮戳自动化，四个自动化完美地实现了 S/MIME 标准技术的落地应用，为普及应用 S/MIME 技术来保障全球电子邮件安全扫除了所有技术壁垒，让古老的电子邮件能更加安全地为全人类服务。

王高华

2025 年 2 月 24 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 203 篇(共 59 万 3 千多字)和英文 86 篇(11 万 3 千多单词)。