零信浏览器是如何实现邮件证书自动化管理的？

目前全球市场邮件加密方法有很多，常用的邮件加密技术是 S/MIME，常用的邮件客户端都支持 S/MIME 邮件证书加密，但是需要用户向 CA 申请邮件证书并配置到邮件客户端中去使用，这个过程同申请 SSL 证书并安装到 Web 服务器上使用一样也是非常痛苦的。要想普及邮件加密技术，必须借鉴 SSL 证书自动化管理成功经验，搞定邮件证书自动化管理，本文就讲讲零信浏览器是如何搞定邮件证书自动化管理以实现邮件加密自动化的。

一、 邮件证书自动化管理是必由之路

正如大家看到的 HTTPS 加密在全球市场已经基本实现了普及应用，虽然我国还没有实现，这个普及 HTTPS 加密的功劳当然应该归功于由 LE 全球率先实现的 SSL 证书自动化管理服务以及后来牵头制定的 RFC8555 ACME 国际标准，使得全球超过 90%的 SSL 证书都已经实现了自动化签发和部署，从而快速实现了 HTTPS 加密的普及应用。

要想实现普及 S/MIME 邮件加密的目标，也只有实现自动化邮件证书管理这一条路，因为传统方式的向 CA 申请邮件证书和配置邮件证书到邮件客户端中去使用非常难，导致了无法普及实现 S/MIME 邮件加密。同 HTTPS 加密自动化实现路径一样，要实现 S/MIME 加密自动化，也只有邮件客户端厂商牵头才能实现，而目前笔者并没有看到全球领先的三大邮件客户端苹果邮件、谷歌 Gmail 和微软 Outlook 有计划提供邮件证书自动化服务，虽然这些邮件客户端都支持 S/MIME 邮件加密，但是都是需要用户申请邮件证书并配置使用的手动方式支持。

二、 目前全球市场是否有邮件证书自动化管理先例？

大家可以中文搜索“邮件加密自动化”或英文搜索“email encryption automation”，除了笔者写的几篇相关的文章外，应该找不到肯定的答案。但是，笔者发现微软 Office 365 已经提供电子邮件加密服务，也可以理解为是自动化实现的，虽然笔者还没有机会测试，但从官网看到的信息可以肯定的是，这是一个类似 PGP/IBC 加密的解决方案，用户使用 Outlook 可以无缝阅读加密邮件，如果不是 Outlook，则会收到一个链接，可以在线阅读加密邮件，这显然是一个云端加解密的解决方案，其前提是电子邮件已经在微软云上，这并不是一个真正的端到端加密解

决方案。

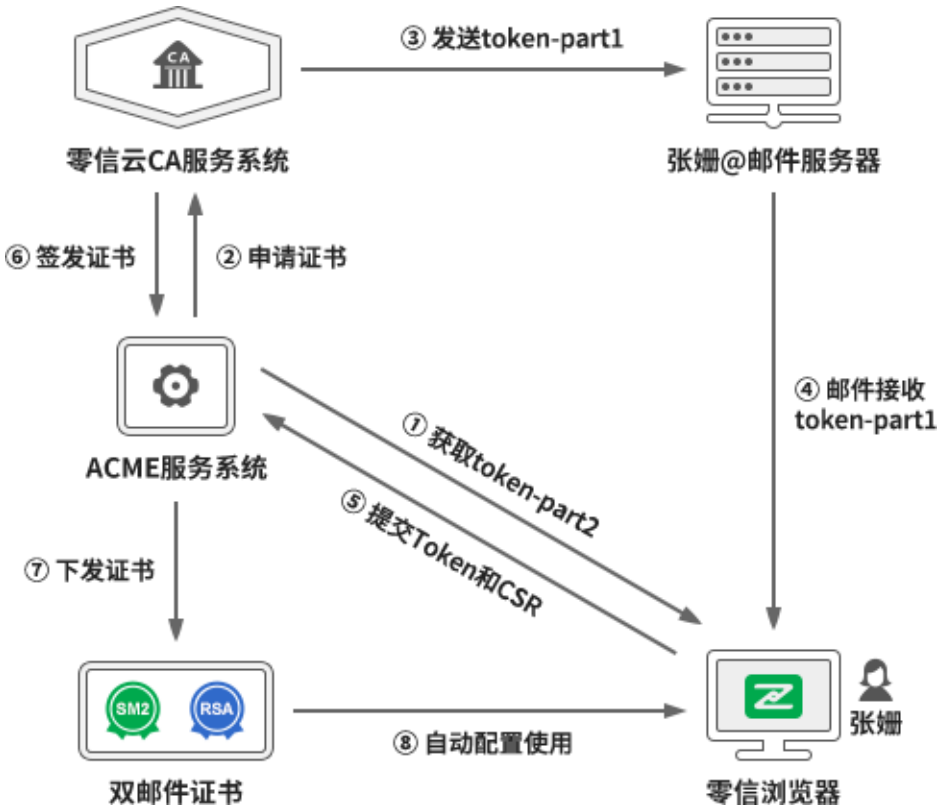
其他邮件加密解决方案如果支持 S/MIME，则一定是要用户向 CA 申请邮件证书和手动配置邮件证书的方案，要么就是其他五花八门的加密方案。笔者并没有看到像 ACME 这样的基于国际标准的自动化邮件证书管理解决方案，但已经有一家英国公司于 2021 年 4 月提交了一个基于 ACME 标准 RFC8555 的用于邮件证书自动化管理的 RFC 提案-RFC8823，这个提案的状态为 Informational, 属于非标准跟踪类，这类提案是指一些有关特定议题的互联网社区的信息，并不代表是社区共识和建议，仅供下一步考虑和验证是否成为实验类标准。笔者仔细研究了这个标准提案，发现其存在的问题是要求邮件客户端回复一个特定的邮件给 CA 指定邮箱完成邮箱验证，这个非常不合理，不符合目前用户向 CA 申请邮件证书的流程，用户收到验证码后复制粘贴验证码到证书申请页面，或者直接点击验证链接完成邮箱验证，这样 CA 就无需建设一个自动化接收和处理用户回复的邮件的系统。不仅如此，笔者还发现了一个小错误并提交了 RFC 勘误表，这个勘误表已经被接受。

也就是说：目前全球市场还没有真正基于 S/MIME 标准实现的端到端邮件加密自动化先例，零信技术将开启这个先例，全球率先独家实现，并且是双算法(RSA 和 SM2)邮件证书的自动化管理。

三、 零信浏览器全球率先开启自动化邮件证书管理(AECM)

零信技术实现的邮件证书自动化管理是在牵头制定的《自动化证书管理规范》国密标准实现双算法 SSL 证书自动化管理的基础上增加了电子邮件证书的自动化管理，这个自动化流程也同时参考了 RFC8823，改进了其自动化提交验证码的流程，由邮件客户端自动读取含有验证码的邮件内容并直接提交给 ACME 服务系统自动化完成邮箱验证，而无需邮件客户端回复邮件提交验证码。这个改进的流程已更新到《自动化证书管理规范》标准草案中。

具体工作流程如下图所示，用户在零信浏览器设置好邮箱账号，由零信浏览器自动对接零信 ACME 服务系统获取验证码的第二部分 token-part2，零信云密码服务系统发送验证码的第一部分 token-part1 到用户申请邮件证书的邮箱中，由零信浏览器内置的邮件客户端把通过两个渠道拿到的两部分验证码合并为完整的 Token 和 CSR 文件提交给 ACME 服务系统完成邮箱控制权验证和证书申请，这样 CA 系统就可以签发双算法邮件证书了，证书签发后由零信浏览器负责对接 ACME 服务系统取回证书并配置使用。这整个过程就是自动化邮件证书管理流程(AECM)，实现了电子邮件证书的自动申请、自动验证、自动签发和自动配置使用。



零信自动化邮件证书管理(AECM)是在成熟的 SSL 证书自动化管理(ACME)基础上专门为邮件证书自动化管理设计的系统，不仅可以实现自动化签发国际算法 RSA/ECC 邮件证书，同时自动化签发国密算法 SM2 邮件证书，免费为用户自动化配置双算法邮件证书，以实现自适应加密算法的电子邮件数字签名和加密，零信浏览器默认优先采用国密算法实现邮件加密和数字签名，用户可选默认密码算法。

为了保证电子邮件发送时间可信，零信技术创新地引入了电子邮戳(Email Timestamp)的概念，在自动化给用户配置邮件证书的同时自动配置双算法时间戳证书-电子邮戳证书，并自动配置到零信浏览器中使用，为用户发出的每一封电子邮件实现数字签名的同时参考相关标准附署时间戳签名，以证明每一封发出的电子邮件的发送时间可信。

零信浏览器免费为每个设置好的用户邮箱自动化配置了 6 张证书，RSA 算法和 SM2 算法各 3 张，分别是一张 MV 邮件签名证书、一张 MV 邮件加密证书和一张 MV 电子邮戳证书。传统 CA 签发的 RSA 算法邮件证书是同时含有签名和加密两个密钥用法的单证书，零信技术采用了双用法分离模式，无论是 RSA 算法还是 SM2 算法都采用单密钥用法证书，这是为了保证用户在第二个设备使用零信邮件加密服务时能共用同一张加密证书以解密以前的加密邮件，但是每个新设备都会自动配置新的签名证书，用于区分和标识新设备。也就是说，每个邮箱只有一张加密证书，但有多张签名证书，这就是为何采用密钥用法分离的单密钥用法证书的主要

原因。对于收费用户，零信浏览器还将为用户自动化配置相应认证级别的 IV/OV/SV 邮件签名证书，默认都是双算法双证书，用户可自己设置何等认证级别的邮件签名证书为默认签名证书。

零信技术全球率先基于 ACME 标准和参考 RFC8823 提案实现了邮件证书的自动化管理，只有这样才能为普及邮件加密扫除了第一个主要障碍，使得采用 S/MIME 邮件加密技术实现邮件加密有了核心部件—S/MIME 邮件证书。更重要的是：零信邮件加密自动化服务配置的邮件证书是完全免费的，只有这样才能实现普及应用 S/MIME 邮件证书实现电子邮件加密，切实保障全球电子邮件的在途和在云安全。

有诗为证：

邮件加密第一关，
邮件证书自动化。
自动化配置证书，
完全免费普应用。

王高华

2024 年 10 月 30 日于深圳

2024.10.30
16:20:31
+08'00'

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 187 篇(共 53 万 5 千多字)和英文 76 篇(9 万 6 千多单词)。