零信 AI 邮探秘之七：标准遵循

RFC 8823：将 HTTPS 证书自动化带入 S/MIME 证书自动化

2026 年 9 月 22 日

HTTPS 之所以操作简单，并非因为 SSL 证书不再复杂，而是因为 SSL 证书管理已经被转移到软件系统中。ACME（自动化自动化管理环境）将证书请求、验证、颁发和续期转变为自动化工作流程。S/MIME 长期以来一直为电子邮件提供加密技术，但证书申请和生命周期管理与电子邮件客户端是相互分离的，需要用户各自操作两边。为什么电子邮件加密没有达到同等的证书自动化水平？

1. HTTPS 让证书管理实现自动化，电子邮件也可以如此。

HTTPS 的成功通常被描述为一段关于加密自动化的故事，但从运维角度来看，其中最重要的一项是把证书管理逐渐转移到了软件系统之中。RFC 8555 对 ACME 进行了标准化，使软件能够与证书服务通信、证明对某项资源的控制权、获取证书，并在需要续期时重复这一过程，从而让用户不再需要手动处理证书申请和部署。

S/MIME 长期以来一直提供电子邮件安全所需的密码学能力，但围绕这些密码学能力展开的使用，却仍然停留在邮件应用之外。S/MIME 证书将公钥与电子邮件身份绑定，并支持签名、验签、加密和解密，而对于用户而言，真正的挑战在于申请证书、证明对邮箱的控制权、获取签发后的证书、在邮件客户端中完成配置，以及持续维护证书的有效状态。

如果这些操作始终作为独立的管理流程存在，S/MIME 就仍然是一项需要用户学习和管理的安全能力；但如果这些操作能够成为邮件客户端本身的一部分，证书就可以开始表现得更像 HTTPS 基础设施，而不是一项需要单独管理的工作。这也带来了一个基本问题：为什么电子邮件还没有实现同等水平的证书自动化？

2. RFC 8823 定义了 S/MIME 所缺失的 ACME 层

RFC 8823 于 2021 年 4 月由 IETF 发布，通过引入“email”标识符类型以及用于证明对电子邮件地址控制权的 email-reply-00 挑战机制，对面向终端用户的 S/MIME 证书扩展了 ACME 服务。该规范尤其值得关注的一点在于，它并没有把邮件客户端视为被动接收证书的终

端；相反，它明确描述了一种内置 ACME 客户端的邮件用户代理（Mail User Agent，MUA），该客户端能够理解 ACME 扩展，被称为“ACME-email-aware” MUA，并可以通过用户界面实现证书管理自动化。

这一架构所带来的意义非常重要，因为 CA 可以为 S/MIME 证书提供 ACME 服务以及自动签发所需的服务器端机制，但电子邮件证书最终仍然必须在邮件客户端中使用。当邮件客户端理解 ACME 工作流程后，它就能够发起证书申请、识别预期的验证挑战邮件、参与邮箱验证、获取证书，并将证书提供给 S/MIME 操作，而无需用户在彼此无关的两个工具软件之间来回切换。

因此，RFC 8823 所描述的不只是另一种证书验证机制，而是一条让证书自动化更靠近证书实际使用场景的路径，使邮件客户端成为证书生命周期中的主动参与者，而不再只是某个由其他系统签发的证书最终被交付到的目的地。

3. RFC 8823 如何将邮箱连接到 ACME

RFC 8823 所定义的工作流程说明了为什么邮件客户端支持 ACME 非常重要。整个过程始于用户为某个电子邮件地址申请 S/MIME 证书，随后 ACME 客户端使用新的“email”标识符创建订单，而 ACME 服务器则创建一项电子邮件地址挑战。对于支持 ACME-email-aware 的 MUA 而言，客户端可以自动获取并解析这一挑战，而不需要用户自行理解并手动转移其中的相关信息。

RFC 8823 定义了一种由两部分组成的令牌模型，其中一个令牌组件通过挑战邮件发送，另一个则通过 HTTPS 获取；ACME 客户端将这两个组件组合起来，计算所需的密钥授权值并准备响应。随后，MUA 按照 RFC 所定义的格式发送响应邮件，而 ACME 客户端则通知 ACME 服务器并检查授权状态。一旦挑战验证通过，证书申请即可完成最终处理，并获取签发后的 S/MIME 证书。

其意义并不在于每一种实现都必须把这些协议步骤暴露给用户；恰恰相反，重点在于标准规范为邮件客户端提供了一条路径，使其能够将底层交互作为应用工作流程的一部分来处理，从而让证书申请和签发成为实现层面的细节，而不再是用户在使用安全电子邮件之前必须理解的另一项任务。

4. CA 提供 ACME 服务只是整个流程的一半

这就引出了一个重要区别：协议支持与产品支持并不是一回事。支持 ACME 的 S/MIME

证书服务可以提供实现自动签发所需的服务器端机制，但仅有这种能力并不能形成完整的邮件证书自动化体验，因为整个工作流程的另一半，是实际使用该证书的邮件客户端。

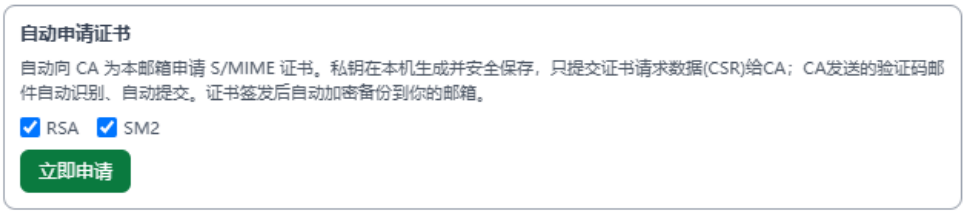
独立的 ACME 工具可以与 ACME 服务通信，但普通用户仍然可能需要在证书工具、邮箱和邮件客户端之间来回切换，之后还可能需要单独导入或配置已经签发的邮件证书。RFC 8823 正是通过明确描述这两种模式来体现这一差异：MUA 可以内置 ACME 客户端，也可以由独立的客户端处理证书申请。

ACME-email-aware 模式是一种更加深入应用层的集成方式，因为邮件客户端本身已经能够访问邮箱，也已经知道最终获得的证书将用于电子邮件加密和数字签名。因此，它可以把证书申请变成邮件工作流程中的原生组成部分，而这正是 S/MIME 开始接近自动化 HTTPS 证书所采用的运行模式的关键节点。

5. 零信 AI 邮 App 将 RFC 8823 变成可运行的工作流程

零信 AI 邮 App 以 RFC 8823 所描述的 ACME-email-aware MUA 模型为基础，将证书申请直接集成到邮件客户端中，而不是要求用户先在其他地方获取 S/MIME 证书，再将其导入邮件客户端。整个流程遵循一个清晰的顺序：申请 → 验证 → 签发 → 自动配置 → 续期。但真正重要的是，这些阶段在同一个应用中彼此衔接，而不是被拆分成一系列独立的管理任务。

用户从 App 发起证书申请后，由证书自动化服务处理请求；当验证邮件到达时，App 可以将预期的邮件识别为证书工作流程的一部分，而一旦邮箱验证成功并由 CA 签发证书，App 就可以获取证书并将其配置用于 S/MIME。此后的流程还可以继续进入生命周期管理，而不是在首次签发时结束，从而使续期同样成为应用持续运行的一部分。



这就是 ACME-email-aware MUA 概念的实际意义：证书不再是一个用户必须先学习如何管理的独立对象，用户也不必先完成一套证书管理流程才能使用电子邮件加密，因为证书管理已经成为负责处理用户电子邮件的应用本身的一部分。

6. 零信 AI 邮从内测实现走向公开产品

零信 AI 邮于 2026 年 8 月在内部测试中实现了这一证书自动化能力，并随后于 2026 年 9 月 11 日发布了零信 AI 邮 App 全球公测版。此次公开发布将自动化 S/MIME 证书申请带入邮件客户端，并同时支持 RSA 和 SM2 算法的证书工作流程。

这一时间线之所以重要，是因为它区分了标准讨论与产品实现。RFC 8823 自 2021 年起就已经描述了 ACME-email-aware MUA 模型，而 CA/Browser Forum 在 2025 年的 SMC012 投票采用了面向 S/MIME 自动化的 ACME，在 S/MIME 证书基线要求中加入了基于 ACME 的邮箱控制权验证机制。零信 AI 邮在 2026 年 8 月份的实现，则把这一模型的应用侧真正带入了一款电子邮件客户端产品中。

因此，这一成果并不只是一个 ACME 端点或一个证书订购网站，而是一款将证书申请、邮箱验证、证书安装和续期连接成完整运行流程的电子邮件应用，把 RFC 8823 所描述的协议模型真正带到了用户发送和接收加密电子邮件的实际场景中。

7. 一个应用，两种密码学环境

零信 AI 邮同时支持 RSA 和 SM2 双算法邮件证书自动化，这一实现同时表明，证书自动化并不需要绑定于单一的密码学环境。为了实现国际互操作性，RSA 仍然是 S/MIME 证书的重要模式；而在我国商用密码环境中，基于 SM2 算法的邮件证书则构成了另一套重要的证书生态。零信 AI 邮 App 可以在同一应用工作流程中，同时实现 RSA 和 SM2 双算法 S/MIME 证书的自动申请和部署，这得益于零信技术牵头制定了参考 RFC8555 和 RFC 8823 的中国商用密码行业标准《自动化证书管理协议》。

这意味着，用户不需要仅仅因为底层算法和信任基础设施不同，就需要学习两套完全不同的证书管理流程。相反，应用层可以提供一致的使用体验，而证书自动化服务和 CA 基础设施负责处理相应的证书流程，从而即使底层密码学环境发生变化，整体运营工作流程仍然能够保

持不变。

将证书生命周期管理视为邮件应用基础设施，所带来的实际优势之一正是如此：复杂性可以留在应用边界之下，而面向用户的工作流程则能够在不同的证书和信任环境之间保持一致。

8. 零信生态信任：完成证书自动化闭环

零信 AI 邮的实践实际上已经超越了邮件客户端本身。零信 AI 邮 App、零信 S/MIME 自动化网关、零信 ACME 服务系统、零信 CA 系统以及零信生态信任的 MV 证书共同形成了一个集成的信任与自动化闭环，不仅提供支持 ACME 的客户端体验，同时也提供了在零信生态信任域内运行这一工作流程所需的相应证书基础设施。

对于用户而言，实际结果是，证书的申请、验证、签发、部署和续期可以在不中断为独立管理流程的情况下完成，而不必把证书管理变成另一套管理工作。这正是 RFC 8823 所描述的架构从协议概念走向产品实现的地方：RFC 提供了应用模型，而零信 AI 邮则在邮件客户端中实现这一模型，并将其连接到自身的证书自动化和信任基础设施。

更广泛的生态问题可以留到后续讨论。当前最直接的技术任务，是让核心工作流程真正端到端运行起来，使证书自动化不只是作为一种协议能力存在，而是被真正集成到证书实际被使用的应用之中。

9. RFC 8823 定义路径，零信 AI 邮让这条路径真正可用。

RFC 8823 并不取代 S/MIME，也没有试图重新设计 CA 生态。它所做的事情更加聚焦：为面向终端用户的 S/MIME 证书提供 ACME 扩展支持，并明确认识到邮件客户端可以直接参与证书自动化；而当证书管理长期被视为发生在邮件客户端之前或之外的一项活动时，这一点很容易被忽视。

多年来，证书生命周期一直作为一项独立的管理流程来处理，最终再将生成的证书交付给真正需要使用它的应用。RFC 8823 描述了另一条路径：邮件客户端本身成为自动化系统的一部分，并能够参与证书申请、邮箱验证、证书获取，以及最终进入实际 S/MIME 使用的过程。

零信 AI 邮将这一模型应用于一款实际运行的产品：App 可以发起证书申请、参与邮箱验证、获取签发后的证书、将其用于 S/MIME，并继续管理证书生命周期，而零信生态信任则提供这一工作流程当前所依赖的集成证书与信任环境。其更广泛的意义与 HTTPS 类似：当协议复杂性消失在软件系统之中时，自动化才能真正释放其最大的价值，让用户无需先成为证书管理员，也能够像发送明文邮件一样发送加密和数字签名邮件。

标准定义实现路径，零信 AI 邮让这条路真正可用。

王高华

2026 年 9 月 22 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 292 篇(共 87 万 2 千多字)和英文 134 篇(18 万 8 千多单词)。