电子邮件证书自动化：CA 机构新的增长机遇

2026 年 11 月 16 日

传统 SSL/TLS 证书市场已经发生了深刻变化。免费证书以及各类平台捆绑提供的证书服务，已经占据了 DV 证书市场的绝大部分份额，传统商业 CA 机构因此面临越来越大的市场压力。继续主要依赖传统 SSL 证书销售，已经难以支撑长期可持续的增长。那么，CA 机构下一步应当到哪里寻找新的增长机会？

S/MIME 邮件证书自动化，正是一个值得关注的答案。

一、市场机遇：S/MIME 已经具备自动化条件

1.1 标准已经就绪，实施差距正是市场机遇

S/MIME 是一项成熟的国际标准和国密标准技术，可用于电子邮件数字签名、发件人身份验证和邮件内容加密。然而，它的实际应用仍远未达到应有的普及程度。主要原因在于，普通用户和许多组织在申请、安装、配置、续期和管理 S/MIME 证书时，仍然面临较高的技术门槛。

推动 S/MIME 更易部署的重要进展之一，是基于 ACME 的邮件证书自动化机制被纳入 S/MIME 基线要求。2025 年 7 月 2 日，CA/Browser Forum 在 SMC012 投票通过后发布了《S/MIME 基线要求》1.0.10 版，将定义 S/MIME ACME 机制的 RFC 8823 纳入相关要求。这为自动化签发 S/MIME 证书以及验证邮箱控制权建立了标准化路径。对于国密邮件证书自动化，零信技术也已经牵头制定了《自动化证书管理协议》草案。

但标准发布，并不意味着所有 CA 都已经部署了 S/MIME ACME 服务能力。CA 仍需投入资源进行服务端实现、部署和运营准备；电子邮件客户端及应用程序也必须支持相应的自动化流程。

这一实施落差恰恰蕴含着市场机遇。CA 不必等待生态中的每个环节都独立完成 ACME 改造，另一条务实路径已经具备可行性：通过现有 CA 系统 API，接入外部 ACME 自动化服务。

零信技术正是提供这类自动化与集成能力的技术合作伙伴。CA 无需立即自行开发并运营完整的 S/MIME ACME 服务，零信技术即可将 CA 现有的证书签发 API 接入 ACME 自动化流程，并与零信邮 App 连接。这种方式能够帮助 CA 利用现有 S/MIME 标准，在显著减少进入 S/MIME 自动化市场所需时间和投入的同时，尽快推出相关邮件证书自动化服务。

©2026 零信技术（深圳）有限公司

1.2 为什么是现在？

以下因素使 S/MIME 自动化成为 CA 机构当前值得把握的重要机遇：

- **技术成熟**：S/MIME 已经能够通过标准化的数字签名、身份验证和邮件加密机制，为电子邮件通信提供保护。
- **自动化框架已经标准化**：国际标准 RFC 8823 和相应的国密标准为 S/MIME 证书签发提供了基于 ACME 的自动化框架。
- **市场需求尚未充分释放**：证书管理的复杂性，仍然是阻碍 S/MIME 广泛应用的重要因素。
- **安全意识持续提升**：个人和组织越来越需要可信的邮件身份，以及对敏感邮件通信内容的加密保护。
- **AI 正在改变 BEC 攻击的威胁态势**：随着 AI 在邮件中的普及使用，攻击者可以大规模生成高度逼真、具有针对性的假冒邮件，传统以邮件内容特征为主的安全检测方式将面临更大挑战。基于 S/MIME 数字签名的密码学发件人身份，能够帮助收件人验证发件人身份，并检测签名内容是否被篡改。
- **已有成熟的自动化先例**：ACME 通过自动化证书申请、签发、部署和续期，在 SSL 证书普及过程中发挥了重要作用。尽早布局 S/MIME 证书自动化的 CA，有机会在市场发展过程中抢占先机，并参与塑造这一新兴市场。
- **存在可直接采用的实施路径**：零信技术已经实现了通过 CA 现有 API 与自动化 S/MIME 证书管理及应用工作流集成起来。

市场需要的不只是更多 S/MIME 证书供应，而是让普通用户真正能够方便地申请、配置、续期并使用 S/MIME 证书。SSL 证书自动化的发展历程已经证明，基于标准的自动化能够带来怎样的市场变化。ACME 帮助证书签发和续期成为可规模化、广泛采用的服务。尽早参与 S/MIME 自动化的 CA，有机会在证书可信数字身份发展的下一阶段取得先发优势。

二、解决方案：无需改造 CA 系统，快速加入 S/MIME 自动化市场

2.1 保留现有 CA 基础设施，增加 S/MIME 自动化能力

零信技术合作模式最重要的优势在于实施简单。CA 无需改造现有 CA 系统，无需重新设计证书签发流程，也不必立即自行开发完整的 S/MIME ACME 服务。零信技术可以基于 CA 现有 API 提供自动化与集成层。

©2026 零信技术（深圳）有限公司

CA 仍然完全掌控现有业务和证书服务，包括：

(1) 证书产品、证书政策和定价；

(2) 客户关系和销售渠道；

(3) 身份验证和邮箱控制权验证；

(4) 证书签发及信任服务；

(5) 现有 CA 基础设施和运营流程。

零信技术提供必要的 S/MIME 自动化能力，将 CA 现有服务与自动化 S/MIME 应用连接起来。

2.2 CA 需要提供什么？

参与合作的 CA 需要提供：

(1) 现有 S/MIME 证书产品及证书签发能力；

(2) 根据现有系统能力，提供用于证书申请、验证流程、证书签发和证书获取的 API；

(3) 现有身份鉴证及证书签发流程；

(4) 证书政策、产品定价和客户支持。

CA 仍然是证书签发机构，并继续对证书签发决策及其信任服务承担责任。

2.3 零信技术提供什么

零信技术提供：

(1) 与 CA 现有证书服务进行 API 集成；

(2) 用于 S/MIME 证书管理的 ACME 自动化服务；

(3) CSR 自动提交及证书申请处理；

(4) 根据 CA 的证书政策和 API 能力，对接其验证流程，包括验证信息交互和挑战处理；

(5) 获取已签发证书，并将证书交付给申请证书的应用；

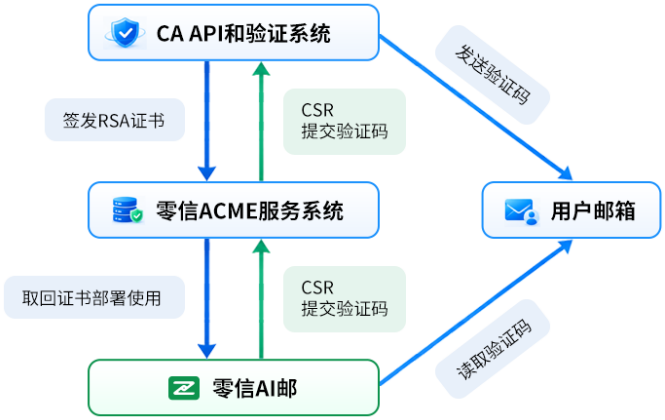
(6) 通过零信 AI 邮实现证书自动配置和生命周期管理。

具体集成流程可以根据各 CA 现有 API 能力和证书签发政策进行适配。本方案并不要求所有 CA 使用完全相同 API 及邮箱验证和证书签发流程。

©2026 零信技术（深圳）有限公司

2.4 集成流程如何运作

整个工作流程如下图所示：



(1) 用户通过零信邮 App 发起 S/MIME 证书申请；

(2) 零信邮 App 将证书申请请求和 CSR 提交给零信 ACME 服务系统；

(3) 零信 ACME 服务系统通过 CA 现有的传统 API 接口连接 CA；

(4) CA 执行所需的验证流程，并向用户的邮箱发送验证码；

(5) 零信邮 App 读取验证邮件，提取验证码，并将其提交给零信 ACME 服务系统；

(6) 零信 ACME 服务系统通过 CA 传统 API 接口将验证码提交给 CA；

(7) CA 按照自身的证书政策完成证书签发流程；

(8) 零信 ACME 服务系统通过 API 取回已签发的证书，并将其返回给零信邮 App；

(9) 零信邮 App 自动配置证书，用于邮件数字签名和加密。

用户无需再手动处理复杂的证书安装和配置过程。我们的目标是将证书申请和使用转化为真正可用、自动化的邮件安全体验。

2.5 在现有 S/MIME 证书销售页面增加一个选项

参与合作的 CA 可以保留现有 S/MIME 证书产品和销售流程，只需在证书购买页面增加一个简单选项，如下图所示：



©2026 零信技术（深圳）有限公司

选择该选项的客户即可使用零信 AI 邮自动完成证书申请与配置和生命周期管理。CA 仍以自己的品牌销售证书，并保留原有证书政策和定价；零信技术则在后台提供自动化和应用集成能力。这样，CA 无需大幅调整现有商业模式，就能增加一项新的服务。

2.6 将标准转化为市场机遇，无需等待

CA 现在就可以利用现有 API 和基础设施进入 S/MIME 自动化市场，而不必等到自行开发并部署完整的 S/MIME ACME 服务之后再行动。零信技术提供集成和自动化层，零信邮 App 与零信 S/MIME 自动化网关则将自动化证书管理和实用的 S/MIME 能力带入真实的邮件工作流。

三、商业价值：最少投入，创造最大回报

对 CA 而言，这一合作的价值不只是增加一个证书产品，更在于扩大证书销售机会，同时降低传统 S/MIME 应用所伴随的运营复杂度。

3.1 开拓新的收入来源

通过提供 S/MIME 证书自动化服务，CA 可以触达过去因 S/MIME 使用复杂而难以转化的客户群体，包括：

(1) 希望拥有可信邮件身份的个人用户
(2) 需要对邮件进行数字签名和加密的专业人士
(3) 中小企业
(4) 寻求标准化邮件安全方案的企业
(5) 有监管、合规或信息保密要求的组织

自动化能够降低 S/MIME 的使用门槛，帮助 CA 将过去尚未释放的需求转化为实际证书销售。

3.2 降低技术支持开支

证书安装、配置、续期和故障排查所带来的技术支持负担，是阻碍 S/MIME 普及的主要因素之一。自动化能够减少其中大量人工操作。通过零信邮 App 和网关管理证书配置和生命周期操作，参与合作的 CA 有望大幅减低客户支持请求和运营开支，同时改善客户体验。

©2026 零信技术（深圳）有限公司

3.3 改善客户体验，提高客户留存

当证书服务能够可靠地融入客户日常邮件工作流时，客户更愿意持续使用。自动化证书管理也减少了用户理解复杂 PKI 操作流程的必要，从而有助于提高客户满意度、增加续期机会，并增强长期客户关系。

3.4 形成市场差异化

随着 SSL 证书市场竞争日益白热化，CA 需要通过提供超越单纯证书签发的服务来建立差异化优势。S/MIME 自动化服务为 CA 提供了一个务实的机会：不仅提供可信证书，还让客户能够更方便地使用证书。

3.5 无需从零建设，即可进入新市场

更重要的是，CA 无需先投入资源建设全新的自动化应用平台，也不必独立开发自动化生态中的每一个组件。借助现有 API 和零信技术平台，CA 可以专注于自身最擅长的领域：身份验证、证书签发和信任服务。

自动化和应用集成工作由零信技术负责。这一策略的核心，是以尽可能少的新增投入开拓新的市场，并创造额外的证书收入。

四、双赢合作：CA 与零信技术

这一合作建立在双方能力互补的基础上，而不是相互竞争。双方各自专注于自身最擅长的领域。

4.1 CA：证书签发与信任服务

CA 仍然是可信证书的签发机构，负责提供证书产品、身份验证、证书签发服务、证书政策及相关信任基础设施，同时保留自己的品牌、定价、客户关系以及证书签发控制权。

4.2 零信技术：自动化与集成

零信技术提供连接 CA 服务与实际应用的技术能力。其两项核心能力是：

(1) 证书管理自动化

(2) 密码应用自动化

©2026 零信技术（深圳）有限公司

在 S/MIME 领域，零信技术将 CA 现有 API 接入自动化证书管理工作流，并将这些流程与邮件应用集成。零信技术并不取代 CA，而是作为自动化与集成层，帮助 CA 通过现有证书服务为客户创造更多价值。

4.3 零信 AI 邮：让 S/MIME 融入日常通信

零信 AI 邮将证书自动化能力转化为面向个人用户和组织的实用服务。

- **ZTmail App：面向个人用户和中小企业**

零信邮 App 通过自动化证书管理，将邮件数字签名、验签、加密和解密融入日常邮件工作流，让 S/MIME 更易于使用。

- **零信 S/MIME 自动化网关：面向企业组织**

零信 S/MIME 自动化网关通过 SMTP 和 IMAP 代理方式与现有邮件基础设施集成，为组织提供 S/MIME 自动化能力。组织无需要求用户更换现有邮件客户端，即可实现邮件签名、验签、加密、解密和证书管理的自动化。

零信邮 App 和零信 S/MIME 自动化网关共同构成两种实施路径，使个人、企业及各类组织都能够使用 S/MIME 证书自动化和 S/MIME 自动化服务。

4.4 市场扩大，各方受益

这一合作不是零和商业模式，而是旨在共同扩大 S/MIME 证书市场：

(1) CA 获得更多证书客户和新的收入机会

(2) 零信技术拓展开放的证书自动化生态

(3) 零信邮通过参与合作的 CA 触达更多用户和组织

(4) 用户获得实用、自动化的邮件安全服务

参与合作的 CA 越多，客户的选择就越丰富；支持 S/MIME 自动化的应用就会越多，整个生态的价值也就越来越大。

五、建设开放的 S/MIME 自动化生态

零信技术希望与全球 CA 携手合作，共同建设开放、可互操作的 S/MIME 自动化生态。我们欢迎国际大型 CA 和区域性 CA 参与合作。该合作模式不具有排他性，各 CA 均可保留自己的品牌、证书产品、定价、政策、验证流程和客户关系。

©2026 零信技术（深圳）有限公司

零信技术提供统一的自动化与集成能力，使不同 CA 的服务能够通过一致的应用体验提供给用户。这有助于减少生态碎片化，让 S/MIME 自动化服务惠及更广泛的市场。

5.1 支持 S/MIME 标准持续发展

零信技术还计划申请加入 CA/浏览器论坛 S/MIME 证书工作组。我们相信，来自证书自动化平台和邮件应用的实际实施经验，能够为 S/MIME 标准的持续发展提供有价值的实践视角。

我们的目标是推动标准、CA 服务、自动化平台和邮件应用协同发展，形成更加成熟的生态。

5.2 超越商业机遇：共同提升全球邮件安全

S/MIME 自动化的意义并不局限于 CA 和技术服务商的商业利益。电子邮件仍然是全球最重要的通信渠道之一，但对普通用户而言，邮件级别的身份可信和内容保护仍未得到普遍应用。TLS 保护的是邮件系统之间传输过程中的通信安全，但仅有传输加密，并不能提供与 S/MIME 相同的端到端邮件内容保护。S/MIME 通过数字签名和邮件加密弥补了这一差距：

(1) 数字签名帮助收件人验证发件人身份，并检测签名邮件是否发生变化

(2) 邮件加密帮助保护邮件内容，防止未经授权的访问

(3) 基于证书的身份为可信数字通信提供基础

相关技术已经成熟，标准也已建立。过去缺少的是一种简单易用的方式，让这些能力真正融入日常邮件中。通过降低证书管理的复杂度，并将 S/MIME 集成到日常邮件工作流中，零信技术希望让可信、加密的电子邮件得到更广泛的应用。

这不仅是 CA 机构新的商业机遇，也是共同提升全球电子邮件安全水平的机会。

六、让 S/MIME 自动化，共同拓展全球市场

传统 SSL 证书市场已经发生变化。对商业 CA 而言，寻找新的增长机会已不再是可选项。S/MIME 蕴含着可观的市场机遇，但要释放这一潜力，关键是让证书申请、配置、续期和使用变得简单。

标准已经就绪，技术已经成熟，市场需要的是切实可行的落地方案。

CA 无需等待自行完成完整的 ACME 实施。通过将现有 API 与零信技术自动化服务集成，CA 就能够以较少的新增投入进入 S/MIME 自动化市场。

超越 API 集成：更广泛的合作机会

©2026 零信技术（深圳）有限公司

虽然 API 集成是 CA 快速进入 S/MIME 证书自动化市场最直接、最务实的方式，但零信技术与 CA 机构的合作并不局限于这一模式。根据各 CA 的业务战略和市场覆盖能力，双方还可以探索零信技术代理销售 CA 签发的邮件证书，以及为 CA 提供 OEM 品牌版本的零信邮 App 和 零信 S/MIME 自动化网关等合作方式。

零信技术欢迎全球 CA 机构与我们交流，探索灵活多样的合作模式，共同扩大市场覆盖、创造新的收入机会，并加速 S/MIME 安全应用的普及，让更多个人和组织能够使用可信、加密的电子邮件。

零信技术，让密码学建立信任，让自动化实现安全，让人工智能提升效率。

王高华

2026 年 11 月 16 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 302 篇（共 91 万 8 千多字）和英文 143 篇（20 万 9 千多单词）。

©2026 零信技术（深圳）有限公司