

让国密邮件加密真正可落地

2026 年 10 月 8 日

四部委（网信办、中央编办、工信部和公安部）于 2024 年 5 月 22 日联合发布了《[互联网政务应用安全管理规定](#)》(以下简称《规定》)，第二条将“互联网电子邮件系统”明确纳入互联网政务应用范畴。这意味着机关事业单位的邮件系统，需要满足政务应用在网络安全与数据安全方面的全部要求。第三十五条进一步明确：“鼓励机关事业单位基于商用密码技术对电子邮件数据的存储进行安全保护。”

一个更具体的现状是：目前市场上还没有一个成熟的邮件客户端，能够原生支持国密邮件证书实现 S/MIME 加密。国际上常用的邮件客户端，如 Outlook、雷鸟（Thunderbird）、苹果邮件等都原生支持 RSA 算法邮件证书的 S/MIME 加密。用户在这些客户端里导入一张 RSA 算法邮件证书，就可以收发加密邮件。但同样的流程，换到 SM2 国密邮件证书就走不通：这些国际客户端不支持 SM2 算法邮件证书，不支持 SM2 算法的 S/MIME 消息封装。

可以看出：一方面，政策方向是清晰的，但“鼓励”不等于“可用”。另一方面，如果市场上没有真正可落地的解决方案，再明确的政策要求也难以执行。这是政务邮件国密加密长期面临的真实困境：要求已经到位，CA 也能签发国密邮件证书，瓶颈在应用层。结果是：政务用户被告知要用商用密码技术保护政务邮件，却找不到一个能用的国密邮件客户端。

一、S/MIME 技术早已成熟，但“应用缺口”始终存在

S/MIME（安全多用途互联网邮件扩展）诞生至今已超过三十年。CA 能签发邮件证书，密码算法也早已就绪。但为什么邮件加密始终没有像 HTTPS 加密那样，成为一项默认能力？

零信技术将这个问题定义为“应用缺口”：它存在于 CA 签发的邮件证书与用户实际使用证书的邮件客户端之间。在国际生态中，这个缺口能被“手动操作”填补。用户可以从 CA 购买一张 RSA 邮件证书，打开雷鸟或 Outlook 的“账户设置—端到端加密—管理 S/MIME 证书”，导入证书，再把证书绑定到邮箱账户。整个过程需要用户理解证书文件格式、密码保护、证书与邮箱的绑定关系。即使如此繁琐，至少能用。

但在国密生态中，这个缺口是无法人工填补的。用户即便拿到了 SM2 邮件证书，也没有邮件客户端可以导入和使用。国际客户端不支持国密算法，国产邮件客户端也普遍不原生支持国密邮件证书导入并采用国密算法加解密。

这就是政务邮件加密面临的应用场景，也是我国 CA 机构的困局，SSL 证书市场已是大势已去，CA 机构本想借势《规定》能在邮件证书上有所作为，但即使能签发 SM2 邮件证书，政务用户没法用，还是徒然。因为要让每一封政务邮件实现国密保护，需要的不只是一张国密证书，而是一套把身份、证书、密钥与邮件行为连接成连续工作流的应用层。而这个应用层，在国内市场长期空白。

二、国密邮件证书自动化，是破局的关键

网上也能搜到个别的国产邮件安全解决方案声称支持国密邮件证书加密，但是如果仍然走国际邮件证书虽然有邮件客户端支持，但仍然未普及应用的老路是走不通的。邮件证书面临一个与 SSL 证书也曾面对过的困境，那就是人工证书申请、部署使用太困难。而可喜的是：SSL 证书已经依赖 ACME 国际标准（RFC 8555）实现了全球普及应用，这让普及邮件证书实现 S/MIME 加密看到了希望，于是也就有了 RFC8823，一个基于 RFC8555 的邮件证书自动化扩展标准。但标准归标准，没有邮件客户端去实现这个标准还是徒然。

这不仅仅是国际算法邮件证书自动化的困局，也是国密算法邮件证书自动化的困局。零信技术早在 2023 年就开始着手研发基于 RFC8555 和 RFC8823 的邮件证书自动化，最重要的一步就是牵头制定《自动化证书管理规范》密码行业标准，该标准不仅支持双算法 SSL 证书的自动化管理，同时也支持双算法邮件证书的自动化管理，这为实现国密邮件证书的普及应用打下了标准基础，让紧接着的邮件客户端研发有了明确的方向，那就是让邮件客户端成为邮件证书生命周期管理中的主动参与者。

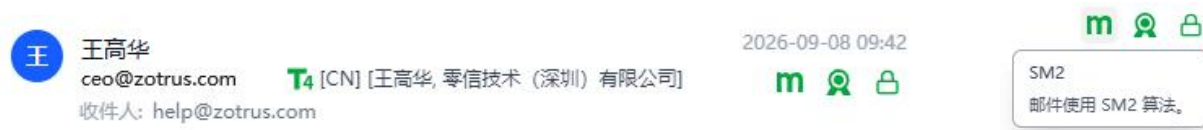
这意味着：国密邮件证书的自动化签发、部署、续期和替换，第一次有了标准支撑。国密邮件加密的核心，是将国际通用的 S/MIME 协议与国密算法相结合。这一技术路径也有明确的国家标准和密码行业标准支撑：

- **GB/Z 19717-2005**《基于多用途互联网邮件扩展（MIME）的安全报文交换》，提供了基于 MIME 协议为邮件提供鉴别、完整性、机密性等安全服务的方法，是 S/MIME 的国家标准版本；
- **GM/T 0010-2023**《SM2 密码算法加密签名消息语法规范》，规定了使用 SM2 算法进行加密和签名操作的标准化封装格式；
- **GB/T 35275-2017**《信息安全技术 SM2 密码算法加密签名消息语法规范》，同样用于实现基于国密 SM2 邮件证书的邮件自动加密。

这三个标准的叠加，为国密 S/MIME 提供了从框架到算法封装的完整技术依据。

三、零信 AI 邮的落地实践：从免费版到政务合规

零信 AI 邮的核心设计是：将邮件证书管理自动化与邮件客户端合为一体，让证书管理成为应用体验的一部分，而非独立的技术技能。



免费版提供完整的证书自动化管理和 S/MIME 密码学能力，包括免费邮件证书申请、验证、签发后取回使用、邮件加密、解密、数字签名、签名验证、证书管理和可信身份展示。这不是功能受限的试用版，而是完整的密码学工作流。区别仅在于身份认证等级和信任范围。免费版的国密邮件证书由零信 CA 签发，让每一位用户都能零成本获得完整的国密加密能力。

收费版面向对邮件身份有更高要求的专业用户，面向政务、金融等对 CA 资质有明确要求的场景，国密邮件证书将由国密合规 CA 根签发，满足合规要求。但无论邮件证书来自哪家 CA，申请、验证、签发、部署、续期、替换的全部流程，都由零信 AI 邮的同一套证书自动化引擎完成。用户在不同信任域、不同身份级别之间切换时，底层是同一套证书生命周期管理流程。

国密算法支持是基础能力。用户可以在零信 AI 邮 App 一键自动申请 SM2 算法邮件证书，也可以同时申请 RSA 和 SM2 双算法邮件证书。RSA 算法保障全球互通兼容，SM2 算法保障国密合规，一封邮件双算法按需选用。SM2 算法的 256 位密钥强度对标 RSA 算法 3072 位，运算速度更快、机器性能消耗更小。

零信 AI 邮 App 提交的是证书签名请求（CSR）给 CA 系统，而非私钥，私钥本地生成并加密存储，并自动加密备份到用户自己的邮箱中，以便设备间恢复使用。云端证书自动化管理与本地密码学控制被明确分开。

邮件在客户端完成国密加密，以密文形态经由国密传输通道落盘存储。服务器端数据库中的邮件正文和附件本身就是密文，没有私钥无法解密。这正是 GB/T 39786《信息安全技术 信息系统密码应用基本要求》对“数据存储机密性”要求的技术实现路径。

四、让国密邮件加密成为默认能力

《互联网政务应用安全管理规定》为政务邮件的国密加密指明了方向。但合规要求要真正落地，需要的是可用的解决方案。S/MIME 技术已经成熟了三十年，国密算法也早已就绪。真正缺失的，是那个把身份、证书、密钥与邮件行为连接成连续工作流的应用层。

零信 AI 邮补齐了应用缺口，填补了国密邮件客户端的空白，国产邮件客户端加上国产密码算法遵循国家标准和国密标准，让国密邮件加密通过免费版实现“人人可用”，而专业版则为

政务等合规场景自动化对接国密合规 CA 根。零信 AI 邮不仅让国密邮件加密从“无法用”到“可用”，更是通过实现自动化国密邮件证书管理实现了“默认”。

让 S/MIME 成为普惠通信能力，让国密邮件加密成为默认。零信 AI 邮，默认加密，天生智能。

王高华

2026 年 10 月 8 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 296 篇(共 88 万 8 千多字)和英文 137 篇(19 万 5 千多单词)。

