

默认加密，天生智能

为什么邮件通信需要一个自动化密码应用层

2026 年 9 月 11 日

二十多年来，互联网一直在持续走向加密通信。HTTPS 是最清晰的例子。过去，证书申请、部署、信任和续期需要专业知识；如今，这些复杂性已经被浏览器、云平台、CA 和自动化基础设施吸收，用户几乎感觉不到它们的存在。网站运营者现在可以在每次发布网页时不再考虑如何申请和部署证书，因为信息基础设施已经替他们处理了这些事情。但电子邮件没有这么幸运，是时候必须同样实现自动化加密了。

1. S/MIME 已经成熟，为什么邮件加密还没有成为常态？

Web 安全已经成功完成转型，而互联网最早的应用——电子邮件却没有完成同样的转型。几十年来，S/MIME 一直提供基于标准的邮件加密、数字签名和基于数字证书的可信身份。底层密码学已经成熟，现代邮件客户端也能够支持所需的密码学操作。然而，S/MIME 仍然远未成为日常邮件的默认能力。因此，问题并不是邮件能否被加密，而是为什么这项技术一直没有真正运行起来。

原因在于，S/MIME 横跨了多个长期分别演进的技术层。CA 负责验证身份并签发邮件证书。邮件客户端使用证书和私钥进行签名、加密、解密和验签。管理员和用户则需要把这两端连接起来，同时还要处理证书申请、密钥管理、证书安装、续期、替换、吊销以及信任决策。每一个组件都可以把自己的工作做好，但整体使用体验仍然是割裂的。

这就是 S/MIME 长期存在的应用鸿沟。邮件证书存在，邮件客户端存在，密码算法也存在，但一直缺少一个被广泛采用的应用层，把完整流程变成自动且可用的体验。这个应用缺口很容易被忽视，因为每一项技术单独看似乎都已经具备。但一旦进入日常使用和规模化部署，缺失的两端连接就成为了核心问题。

现在，标准体系也正在朝同一个方向发展。RFC 8823 定义了用于自动化终端用户 S/MIME 证书管理的 ACME 扩展，而 S/MIME ACME RFC8823 被纳入国际标准《S/MIME 证书基线要求》和国密标准《自动化证书管理协议》，为自动化证书流程提供了更强的基础。其意义并不是 S/MIME 突然变得可行，而是整个生态正在越来越多地提供标准化机制，去消除一项已经证明其密码学价值的成熟技术所面临的运维摩擦。

2. 缺失的那一层，正位于邮件证书与邮件应用之间

这一点非常重要，因为证书自动化标准本身，并不会自动产生一个真正可用的加密邮件体验。即使证书可以自动签发，用户或管理员仍然可能需要解决：它如何成为邮件应用所使用的证书、对应的私钥如何管理、如何发现收件人的证书，以及如何让签名和加密成为发送与接收邮件时的正常流程。

因此，S/MIME 的问题既是证书问题，也是应用问题。CA 负责信任和证书签发。邮件客户端负责通信以及密码学的实际使用。真正缺失的是一个能够把身份、证书、密钥管理和邮件行为连接成连续工作流的应用层。

零信 AI 邮正是围绕这一理念构建的。零信 AI 邮不把 S/MIME 当作一项需要用户学习和操作的证书功能，而是把 S/MIME 视为一种应该自动运行的密码应用。目标是把 CA 和信任基础设施连接到实际的邮件收发行为中，让证书生命周期管理和密码操作成为应用体验的一部分，而不是各自相互独立的项目。

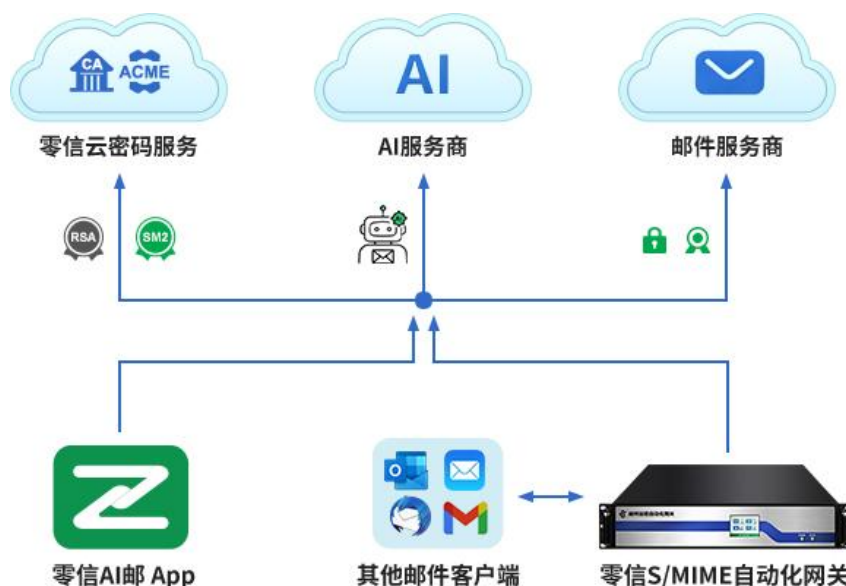
这也解释了为什么零信 AI 邮并不是为了替换现有邮件生态而设计。目标是连接已经能够正常工作的各个组成部分：PKI、CA、邮件系统、现有邮件客户端和邮件安全基础设施。真正缺失的价值，是增加一个自动化密码应用层，让这些组件能够作为一个实用的 S/MIME 系统一起工作。

由此形成的是一种不同的邮件加密思路。与其要求用户或管理员从证书、密钥、客户端和策略中自行组装一个邮件加密系统，不如让应用层把这些组件作为一个连续过程运行。底层技术仍然基于标准；真正改变的是运行模式。

3. 要让 S/MIME 覆盖互联网规模，需要两条路径

一旦理解了这个应用缺口，另一个现实问题也会变得清晰：邮件的使用存在两个完全不同的层级。个人和小型团队需要一个能够让密码技术变得简单的应用，而不需要他们具备证书专业知识。组织则需要一种基础设施模式，把同样的能力应用到大量邮箱中，与现有邮件安全控制集成，并持续运行于组织级规模。只解决其中一个问题，并不能让 S/MIME 成为互联网邮件的普遍能力。

因此，零信 AI 邮提供两条互补的实现路径。零信 AI 邮 App 面向个人和小型团队，把 S/MIME 自动化直接带入邮件应用体验。零信邮件加密自动化网关则解决组织侧的问题，把 S/MIME 自动化放入邮件基础设施中。这两条路径本质上都是在实现同一个缺失的应用层：一条把密码应用自动化带到用户身边，另一条把它带入组织的通信基础设施。



同样的原则也适用于信任。零信 AI 邮使用两个信任域，使不同的通信需求不必被强行放进同一种模式。零信生态信任 面向组织级 S/MIME 部署，以及零信生态内的可信身份。全球生态信任则使用国际认可的 公共 CA 信任，用于需要在零信 AI 邮生态之外获得广泛认可的通信场景。两个信任域共同构成一套 S/MIME 自动化体系中的互补信任路径。

这种区分很重要，因为加密与信任相关，但并不相同。加密保护消息内容；数字签名和基于证书的身份则提供建立密码学可验证身份信号的机制。因此，一个真正实用的 S/MIME 系统既需要保护消息的能力，也需要让可信身份能够进入正常通信流程。

要让 S/MIME 得到广泛采用，互联网邮件的两端都必须被解决。不能只让企业部署变得可行，却把个人和小型组织继续留在原有的证书复杂性中；也不能只让一个人的邮箱变得简单，而组织级部署仍然困难。可规模化实施的模式必须同时让这两个层级的邮件加密通信变得切实可用。

4. AI：从可信通信走向智能通信

邮件不仅正在变得更加安全，也正在变得更加智能。生成式 AI 正在改变人们起草、翻译、总结和处理邮件的方式；与此同时，同样的技术也让钓鱼邮件、假冒身份邮件和商业邮件欺诈变得更加具有迷惑性。这带来了一个重要区别：AI 可以帮助人们理解邮件并采取行动，但它不应该成为密码学信任的替代品。更强的模式，是把两者结合起来。

零信 AI 邮的理念是“默认加密，天生智能”，用户可以选择自己信任的 AI 服务，并使用自己的 API Key 连接 AI 服务。这里的重点并不只是给邮件客户端增加一个 AI 按钮，而是在日常通信 workflows 中提供 AI 的同时，让用户继续掌握与 AI 服务之间的关系。AI 服务商的选

择以及 API 密钥仍然由用户决定，而不是让用户被绑定到某一个专有 AI 服务上。

第一 AI 应用是提升生产力。用户选择的 AI 服务可以帮助用户起草或润色邮件、翻译内容、总结长对话、提取任务，以及识别需要回复的信息。这些能力可以减少人们处理邮件所花费的时间，同时不改变通信本身的信任模型。

第二 AI 应用是提升安全性。AI 可以帮助分析可疑邮件，解释为什么某条消息可能存在风险，识别与钓鱼或假冒相关的模式，并帮助用户理解普通邮箱地址与具有密码学支撑的身份之间的区别。在这种模式下，AI 是安全决策的助手，而不是信任本身的来源。

这一点在攻击者开始使用 AI 让欺诈通信更加逼真的现在尤其重要。密码学可以建立可验证的身份基础并保护消息内容；AI 则可以帮助收件人更好地理解这类可信通信，并更有效地采取行动。两者结合，比单独使用任何一种技术都更有价值：密码学建立信任，AI 帮助人们高效且安全地使用这种可信通信。

这是零信 AI 邮的核心原则之一，用户应该继续掌握自己的加密私钥；当用户选择使用 AI 时，也应该掌握与所选 AI 服务之间的 API 密钥。应用层应该让密码学变得简单，但不应该掩盖两个根本问题：谁控制密钥，以及谁在处理这些信息。

5. 从“技术可行”走向“默认通信能力”

互联网 Web 应用的发展历史表明，当用户不再需要管理实现加密所需的复杂机制时，加密才能得到广泛采用。密码学当然重要，但真正推动转型的，是证书、信任、续期和部署被基础设施和应用吸收。

邮件应用也需要完成同样的转型。S/MIME 已经提供了消息加密、数字签名和基于证书身份的密码学基础，PKI 提供信任模型，CA 提供身份鉴证和证书签发。邮件客户端提供通信界面。ACME 则提供了越来越标准化的证书自动化机制。真正缺失的，是把这些能力连接起来，使个人和组织能够持续使用的应用程序和系统。

这正是零信 AI 邮希望承担的角色。它并不要求互联网重新发明另一套邮件加密标准，而是希望把一个已经存在的各个标准组件的工作自动化协同完成。当身份、证书、密钥和密码学操作成为正常邮件体验的一部分时，加密就可以从用户或管理员需要主动配置的事情，变成邮件系统本身自然完成的事情。

零信 AI 邮的发布并不只是增加了另一个邮件安全产品，而是完成数字信任与日常通信之间缺失的那一层。个人、小型企业和大型企业都需要实用的方法来使用相同的底层密码学原则，只是部署模式不同。只有同时解决个人侧和组织侧的问题，S/MIME 才有可能真正成为互联网

邮件的默认能力。

而随着邮件越来越多地由 AI 辅助，可信通信也应该变得更加智能，同时不能因此失去控制。S/MIME 提供密码学基础，自动化让它变得好用，AI 帮助人们使用它。用户自己的密钥以及由用户选择的 AI 连接方式，让控制权留在应该属于它的位置。

零信 AI 邮，默认加密，天生智能。

欢迎零信 AI 邮今天正式来到世界，欢迎大家今天正式来到零信 AI 邮的世界。

王高华

2026 年 9 月 11 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 283 篇(共 83 万 6 千多字)和英文 125 篇(17 万 3 千多单词)。



