让 S/MIME 成为普惠通信能力

2026 年 9 月 11 日

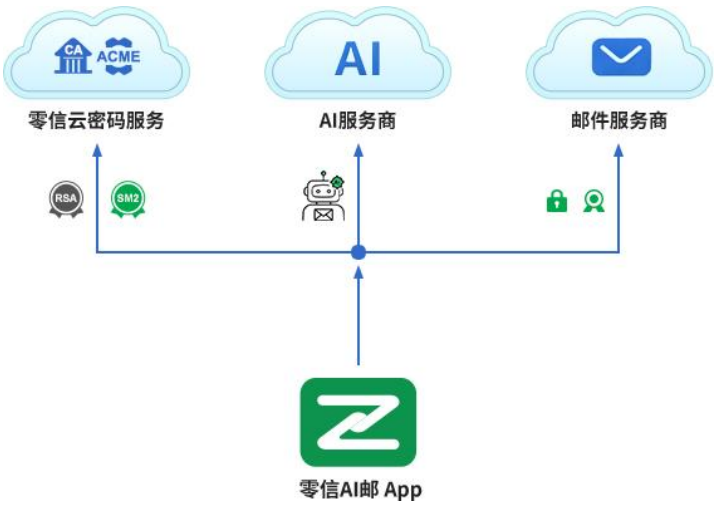
S/MIME 是安全多用途互联网邮件扩展的缩写，用于电子邮件数字签名和加密。这个国际标准已经存在数十年，常用邮件客户端也已经支持以实现了密码学相关操作，CA 机构也能够签发将身份与密码学密钥绑定的邮件证书。但这项技术诞生数十年都没有真正得到应用，其根本原因是没有一个软件能提供把各种相关的组件连接成一个普通人可以使用的体验，无法成为保障个人邮件通信安全的默认能力。

1.S/MIME 已经成熟，但应用层的缺口依然存在

这一问题在个人用户和中小企业层面尤其明显。即使邮件证书已经可以从 CA 机构申请，但用户仍可能需要理解申请、验证、安装、私钥处理、证书选择、续期，以及证书与邮箱账户之间的关系。即使常用的邮件客户端已经支持 S/MIME，但证书与应用在实际操作上彼此分离。结果就是：这项技术在技术上能够工作，却没有表现得像一个正常的互联网服务。

这就是“应用缺口”：它存在于 CA 签发的证书与实际使用证书的邮件应用之间。CA 可以建立身份并签发证书，邮件客户端可以执行数字签名、加密、解密和验签。但缺少的是一层应用逻辑，把身份、证书、密钥与邮件行为连接成一个连续的工作流。

零信 AI 邮正是围绕这一连接设计的。它不是要求用户自己把这些组件拼装起来，而是将邮件证书生命周期自动化与邮件客户端结合起来。整个流程可以覆盖申请、验证、签发、部署、续期和替换，让密码学操作成为日常邮件行为的一部分，而不再是一个独立的技术技能。



其意义远不只是方便。如果 S/MIME 要从专业部署走向更广泛的应用，个人邮箱也必须成为自动化模型的一部分。企业基础设施可以解决组织侧的问题，但互联网同样由个人、专业人士、家庭、小型企业和分布式团队组成。只解决组织部署的一套模型，不可能覆盖全球互联网邮件通信的全部场景。

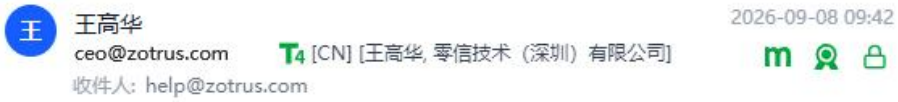
2. 邮件需要的不只是加密，还需要可信身份

邮件加密回答的是一个基本问题：邮件内容能否免于未经授权的获取？而可信通信还需要回答另一个问题：邮件背后究竟是谁？在钓鱼、假冒和商业邮件欺诈越来越逼真的环境中，仅仅一个发件人邮箱地址已经是很弱的身份信号。经过密码学签名的邮件可以携带更强的证据，但只有当应用能够让收件人理解这些证据时，它们才真正具有实际价值。

这正是创新的邮件客户端开始超越“阅读和发送邮件工具”的地方，它可以成为数字信任的用户界面。应用不必只向收件人显示一个发件人邮箱地址，而可以显示与经过验证的数字签名相关联的身份信息。零信 AI 邮的设计目标，就是让这种身份信息成为邮件体验的一部分，让收件人能够看到签名邮件背后的真实身份和信任级别，而不必自己阅读和解释邮件证书。

这一身份模型通过四个级别表达：T1 对应 MV（Mailbox Validated，邮箱认证），用于确认对邮箱的控制权；T2 对应 IV（Individual Validated，个人认证），用于证明个人身份；T3 对应 OV（Organization Validated，单位认证），用于证明单位身份；T4 对应 SV（Sponsor Validated，单位员工认证），将单位身份与员工身份结合起来。实际呈现时，这一层级可以让收件人看到发件人的姓名、组织名称，或者两者。

如下图所示，零信 AI 邮会在发件人邮箱地址旁展示 “**T4** [CN] [王高华, 零信技术（深圳）有限公司]”的发件人可信身份信息。真正产生价值的并不是这个视觉标签，而是其背后的身份认证和数字签名。这个区别非常重要：可信身份应该让普通用户容易理解，但不能让人误以为一个 UI 标签本身就能够创造信任。



关键在于，身份认证与加密并不是相互竞争的功能，而是协同工作的。数字签名可以提供可验证的身份信号，而 S/MIME 加密保护邮件内容。如上图所示，在邮件 UI 的右边展示了此邮件已采用国密算法实现了数字签名和加密。也就是说，零信 AI 邮将身份认证（数字签名）和加密两者放入同一个工作流，让密码学身份不再隐藏在证书管理界面之后。

传统邮件安全控制会分析内容、行为、信誉和其他信号来识别可疑邮件。密码学身份解决的是不同的问题：它为收件人提供一个与发件人数字签名证书绑定的、可验证的身份信号。零信 AI 邮并不取代过滤或其他安全控制，而是在其基础上增加一层密码学身份，使可信通信对正在阅读邮件的人更加明确。

3. 让每个人都能使用完整密码学能力，会改变 S/MIME 的普及逻辑

个人市场存在一个企业部署通常无法解决的问题：成本与复杂度相互强化。如果完整的 S/MIME 能力意味着付费证书、人工配置和专业知识，那么它的采用自然会集中在拥有专职 IT 资源的组织中。但如果 S/MIME 的目标是成为互联网通信的一项普通属性，其门槛就必须非常低。

因此，零信 AI 邮对**免费版**的定位不同于传统意义上其他产品的“免费版”或“基础版”。它是一个完整密码学功能版本，而不是功能受限版本。加密、解密、数字签名、验签、证书管理和身份展示都属于完整的密码学工作流。它与其他版本的区别，在于身份认证级别和信任范围，而不是底层 S/MIME 功能是否可用。

免费版使用 T1 / MV 邮箱认证身份，免费自动配置的邮件证书仅零信生态信任。MV 证书是高度自动化的：它建立的是对邮箱控制权的验证，而不是通过人工流程试图建立个人或组织身份。从这个意义上说，它类似于 HTTPS 中 DV 证书所回答的问题：验证一个明确的控制权问题，而不试图证明超出该问题范围的更多身份信息。这样，零信 AI 邮可以在不让身份验证本身成为使用障碍的情况下，提供完整的 S/MIME 使用体验。

可信身份版是零信 AI 邮的收费服务，是在相同密码学基础上，为需要更强身份证明的用户提供更高等级的身份认证。T2 / IV 可以建立个人身份，T3 / OV 可以建立单位身份，T4 / SV 可以建立与单位相关联的员工身份。其目的并不只是再签发一张证书，而是让经过认证的身份真正能够被使用，并在邮件对话中被看见。

全球生态版面向的是另一类需求：更广泛的邮件生态中的互操作性与识别度。在需要全球范围识别的场景中，它采用国际认可的公共 CA 全球生态信任；在适合的可信身份路径中，也可以同时使用零信生态信任。产品类型同时区分标准版和增强版，体现全球邮箱互操作性与全球可信身份之间的差异。

零信 AI 邮提供的这三个服务版本体现了一个重要的架构原则：密码学能力与信任范围

是两个不同维度。同样的 S/MIME 操作，可以承载不同程度的身份保证，也可以使用不同的信任域。将这两个维度分离后，零信 AI 邮就可以让完整密码学能力更广泛地被使用，同时允许用户在需要时选择更强的身份或更广的信任范围。

对于个人和中小企业而言，这一设计改变了 S/MIME 的普及逻辑。S/MIME 可以先作为一种应用能力被体验，再随着通信需求增长而扩展。广泛普及并不要求所有用户拥有完全相同的证书和信任域；真正需要的是，让密码学工作流对每一个用户都一样可用。

4. 邮件客户端正在成为一种密码学应用软件

当 S/MIME 在个人层面真正变得可用，邮件客户端需要承担的角色也会发生变化。传统客户端主要是通信界面，而密码学邮件应用则需要在同一个界面中管理身份、证书、密钥和密码学操作。应用不再只是“使用一张证书”，而是在把数字信任连接到日常通信。

零信 AI 邮将证书生命周期从申请、验证、签发、部署、监控一直自动化到续期和替换。私钥在本地生成，并始终由用户控制；应用提交的是证书签名请求，而不是把私钥发送给证书服务。证书和私钥还可以加密后备份到用户自己的邮箱，以便在支持的设备之间进行恢复。因此，云端证书自动化与本地密码学控制被明确分开。

同样的模型适用于四项核心邮件操作：签名、加密、解密和验证。用户可以使用已有身份对邮件进行数字签名；在通过签名交换获得收件人公钥证书后自动加密邮件；使用本地私钥解密受保护邮件；并在验证发件人签名时显示对应的可信身份等级。目标不是让用户看到更多密码学细节，而是在隐藏运营复杂度的同时，让密码学结果更加清晰可见。

App 还需要能够连接用户已有的 S/MIME 历史。已经拥有 S/MIME 证书的用户，可以在条件允许时导入现有证书和私钥，包括用于解密过去已加密邮件的历史证书。因为密码学邮件并不是从安装新应用的那一天才开始的。一个真正自动化未来的应用，也必须尊重用户已经拥有的加密历史。

AI 又带来了另一层能力，但它不应与密码学信任混为一谈。零信 AI 邮的“AI, Your Key”模式允许用户选择 AI 服务提供商，并使用自己的 API Key。AI 可以帮助完成写作、翻译、摘要、任务提取，以及钓鱼或欺诈分析；而密码学功能仍然建立在 S/MIME、证书和数字签名之上。这是“AI for Productivity”和“AI for Security”：AI 可以增强生产力和安全分析，同时用户保留对 AI 连接方式的控制。

因此，零信 AI 邮更大的意义并不是简单地给另一个邮件客户端增加加密，而是把一个已经成熟的密码学标准连接到邮件真正发生的地方。Application Gap 存在于数字信任基础设施与日常通信之间。只有在客户端层面关闭这一缺口，S/MIME 才有可能同时覆盖个人、中小企业 和大型组织。

企业网关可以让 S/MIME 在组织内部实现规模化，而应用可以让它在组织之外真正变得易用。两者都是必要的，因为如果只有生态系统中的一侧能够使用可信且受保护的通信，就不可能完成互联网邮件的整体转型。

5. 让 S/MIME 成为普惠能力，就是让密码学赋能邮件通信

互联网安全的发展历史表明，真正的普及并不是要求每个用户理解更多技术，而是把复杂度转移到用户本来就依赖的系统中。HTTPS 为 Web 通信完成了这一转变。S/MIME 已经拥有进行类似转变所需要的密码学基础，但应用层必须让这些基础在个人层面和组织层面都真正可用。

这就是“让 S/MIME 成为普惠能力”的更深层含义。它并不只是意味着设计一款面向个人用户的应用，而是意味着让密码学身份、数字签名、加密和密钥控制成为普通人的通信环境的一部分。用户应该能够安全通信，而不必成为证书专家；同时，当一个身份经过验证时，用户应该能够看见，并理解这种验证究竟意味着什么。

免费版在这一模型中非常重要，因为完整的密码学能力并不一定要从商业门槛之后开始。用户可以先从零信生态信任中的自动化 MV 证书开始，随后根据通信需求升级到更强的身份验证或更广泛的全球信任。密码学基础保持不变，变化的是随用户需求而演进的信任范围。

这不仅关系到产品采用，也关系到互联网通信的基础设施。如果只有大型组织部署 S/MIME，那么互联网中相当大的一部分通信仍然处于密码学模型之外。个人和中小企业会与企业通信、彼此通信，并跨越不同组织边界。让所有邮箱真正可用 S/MIME，因此并不再是邮件安全的次要功能，而是实现广泛普及所必需的一部分基础设施。

AI 会让这一转变更加重要。未来的邮件应用不仅要保护和验证通信，还会帮助用户理解、处理和执行邮件内容。但智能通信不应意味着放弃控制。密码学密钥应继续由用户控制，而 AI 连接也应通过自带 API 密钥的模式由用户自行选择 AI 服务。

最终，让 S/MIME 成为普惠能力，就是消除“强密码学”与“日常易用性”之间那个错误的二

选一。技术已经存在，信任基础设施已经存在，邮件应用也已经存在。长期缺少的，只是让三者真正协同工作的连接层，并且是人人可用。

零信 AI 邮，让 S/MIME 成为普惠通信能力！

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 285 篇(共 84 万 4 千多字)和英文 127 篇(17 万 6 千多单词)。