让 S/MIME 实现规模化组织部署

2026 年 9 月 11 日

今天的企业邮件环境已经拥有相当完善的安全检测层，它所缺少的是一个密码学应用层，能够持续地把身份、证书、密钥、签名、加密和验签整合进正常的邮件流程。但是，如何补缺？零信技术给出了不一样的答案。

1. 企业邮件安全体系中还缺少什么？

经过多年的发展，企业邮件安全已经成为一个成熟的防御体系。反垃圾邮件、恶意软件检测、钓鱼防护、数据防泄漏、内容检测，以及越来越多的 AI 辅助安全分析，已经成为现代邮件基础设施的重要组成部分。这些技术主要回答的是一个问题：一封邮件是否安全？邮件是否包含恶意内容、附件是否存在风险、内容是否违反策略，或者发送者的行为是否可疑。

然而，安全检测与密码学保护解决的是不同的问题。安全系统可以检查一封邮件，却并不因此赋予邮件可验证的数字身份、完整性保护或由收件人控制的内容加密。S/MIME 正是解决这一层问题的技术。通过数字证书和公钥密码学，它提供数字签名、可信身份和消息级加密。这些能力已经存在数十年，而且现代企业邮件客户端已经支持。

因此，问题并不是 S/MIME 是否成熟，而是为什么这些能力始终没有成为企业邮件基础设施中的常规组成部分。TLS 加密保护了邮件系统之间的通信通道，但它并不提供同等意义上的消息级保护。S/MIME 可以保护邮件消息本身，并携带可验证的发送者身份。对于需要更强身份保障、完整性和机密性的组织而言，真正需要的是一种实用的方法，让密码学邮件保护能够像基础设施一样运行。

2. 为什么 S/MIME 一直没有成为企业级能力？

S/MIME 一直没有成为主流邮件加密技术，并不是因为底层密码学不成熟。相关标准、PKI 基础设施、证书生态以及邮件客户端支持都已经存在多年。真正困难的是实施。

传统的 S/MIME 部署往往把每一个邮箱都当作一个独立的密码应用端点。需要为用户签发证书、完成身份验证、生成并保护密钥、在邮件客户端中配置证书，并持续管理续期、替换和吊销。当用户、部门、设备或业务关系发生变化时，相关的密码应用状态也必须随之变化。适用于几十用户的模式，当组织拥有数百、上千、数万甚至更多邮箱时，就会越来越难以管理。这还会带来经济上的严重负担。当每个邮箱都被当作一次独立的证书部署时，证书采购、生命

周期管理、管理和支持都会成为随着用户数量增长而持续增加的成本。仅适合于少量用户的模式，并不会自动成为覆盖整个组织的基础应用。

因此，要让 S/MIME 实现规模化应用，必须同时解决两个条件。**第一**，用户不应该被要求改变使用邮件的方式。如果每位员工都需要决定什么时候加密、管理证书或学习新的工作流程，系统最终依赖的就会是人的行为，而不是基础设施。而可规模化实施的模式应该是零用户改变：员工继续使用熟悉的邮件客户端，不改变工作流程，加密在后台自动完成。

第二，组织需要可持续的密码基础设施。证书申请、签发、部署、续期、替换和吊销不能继续作为一个个独立的邮箱项目来处理。HTTPS 提供了一个很好的先例。互联网之所以实现了 SSL 证书的广泛部署，并不是因为每一位用户都学会了证书管理，而是因为基础设施吸收了复杂性，并通过自动化完成部署和续期。

S/MIME 自动化的 ACME 标准的推进提供了一个很好的实施基础。RFC 8823 将 ACME 模型扩展到 S/MIME 证书，而 CA/浏览器论坛将 S/MIMEACME 纳入 S/MIME 证书 基线要求，为自动化提供了重要的标准化方向。但标准本身并不会自动形成企业级基础设施。剩下的挑战，是把证书自动化、证书、密钥保护、邮件流、信任关系和密码学应用结合起来，形成一个能够持续运行于组织级规模的系统。

3. 硬件网关改变了部署模式

零信技术的解决方案是把 S/MIME 的部署单元从单个邮箱转变为整个组织。零信 S/MIME 自动化网关 不只是又一个邮件功能网关，而是一个专用的密码基础设施，旨在让 S/MIME 成为组织级密码服务。

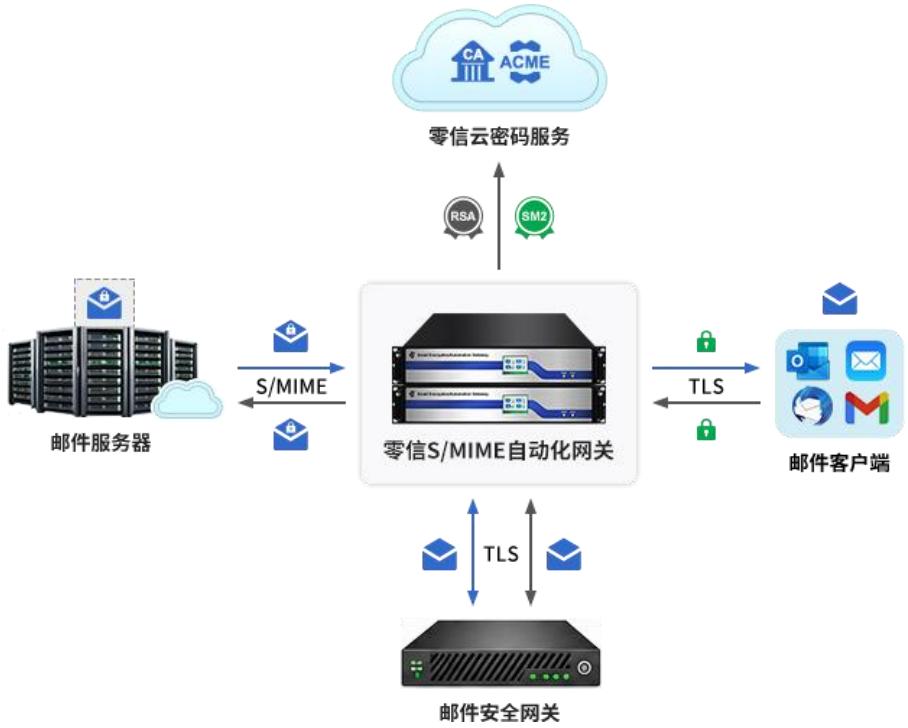
网关集成 企业 CA 和组织级 子 CA，并通过集成 HSM 保护 子 CA 私钥。这样，组织可以在网关环境中建立组织级信任与证书基础设施。证书申请、签发、部署、续期、替换和吊销，可以从分散在各个邮箱和管理员之间的操作，转变为集中管理的证书生命周期。
由此形成的是一种根本不同的运行模式：组织不再管理数千个相互独立的证书项目，而是把邮箱作为组织级密码基础设施所管理的端点。

一个网关，一套组织级信任基础设施，覆盖数千到数百万个邮箱。

借助零信生态信任，组织可以实现组织级规模部署，没有 S/MIME 证书签发数量限制。当外部通信需要全球信任的公共 CA 信任时，可以使用 全球信任生态。这两个信任域服务于不同的通信和信任需求，同时仍然可以属于同一套密码网关架构。

网关不要求组织替换现有的邮件安全系统，而是协调工作各司其职。入站 S/MIME 邮件可

以在受控的密码学边界内完成解密和验签，然后进入现有的安全检测流程；出站邮件则可以先经过现有安全控制，再由网关自动完成数字签名和加密。这样，组织可以继续保留反垃圾邮件、恶意软件检测、钓鱼防护、DLP、内容检测和合规系统，同时增加消息级密码学保护。



对于网关部署架构而言，目标并不是声称邮件在所有内部处理步骤中始终保持加密。真正的目标是：邮件进入云端第三方负责运维的邮件服务器，始终以密文方式存储，并不意味着 S/MIME 加密保护就必须自动消失。在组织受控的解密边界之外，消息可以继续保持密码学保护；在这一受控环境内部，现有安全系统可以访问执行检测和策略控制所需的明文内容。因此，密码学保护成为邮件基础设施的一部分，而不是一个孤立的邮件客户端功能。

这一点非常重要，因为 S/MIME 自动化并不只是自动签发 S/MIME 证书。证书只是企业密码学系统中的一个组成部分。一个可规模化的架构还必须管理身份、证书生命周期、私钥保护、邮件流、信任关系、密码学操作以及安全策略。

一旦经过密码学验证的身份成为企业邮件基础设施的一部分，它还可以成为安全决策的输入。系统不仅可以评估邮件内容、附件和行为信号，还可以判断邮件是否携带有效的密码学可信身份、数字签名是否有效，以及发送者对应的身份认证级别。

这也是 AI 可以发挥更大作用、同时又不取代现有安全控制的地方。AI 可以分析语言、行为、链接、附件和其他信号，以识别可疑通信。可信身份提供的是另一类信号：邮件中所声明的发送者，是否能够通过密码学方式与一个经过验证的身份建立关联。这样，AI 就可以同时基于“这封邮件看起来是什么样”和“发送者能够证明自己是谁”来进行判断。

这一点需要明确区分。AI 不会创造密码学信任，可信身份也不会取代基于 AI 的检测。

但两者结合，可以为邮件安全决策提供更强的基础，把行为和内容分析与可验证的身份信号结合起来。密码学改变信任边界，AI 则可以更有效地利用这一边界内可获得的信任信息。

从这个角度看，真正发生变化的并不只是邮件是否加密。密码学改变了信任建立的位置，以及信任信息可以如何被使用。TLS 保护邮件服务器之间的连接，S/MIME 保护消息。两者并不冲突，而是可以成为同一企业安全架构中的互补组成部分。

4. 邮件已经准备好走完 Web 已经完成的加密转型

HTTPS 的发展历史证明了一个重要原则：广泛的加密并不是因为用户学会了更多密码学知识才实现的，而是因为基础设施吸收了复杂性。今天，用户访问网站时不需要理解证书如何签发、密钥如何生成或 HTTPS 连接如何建立。这些操作已经成为信息基础设施的一部分。

邮件也需要经历类似的转型。邮件仍然是世界上最重要的数字通信形式之一，承载着商业信息、金融数据、知识产权、个人信息以及其他敏感内容。如果 HTTPS 能够让加密成为 Web 的默认属性，那么邮件也应该能够让消息级密码学保护成为邮件基础设施的一部分。

实现这一目标所需的技术组件已经基本就位。公钥密码学已经成熟。S/MIME 是一个长期存在的邮件安全标准。企业邮件客户端支持所需能力，PKI 和 CA 提供身份与信任基础设施。ACME 则为 S/MIME 证书自动化提供了标准化基础。

真正缺少的不是另一种加密算法，也不是另一个邮件安全检测产品，而是一种能够把这些组件结合起来、并持续运行于企业规模的基础设施模式。这一模式必须解决长期限制 S/MIME 的两个问题：用户不应该改变正常的邮件使用方式；随着邮箱数量增长，组织也不应该承担成比例增加的证书管理和运营负担。

一旦密码学成为邮件基础设施的一部分，加密就不再需要成为用户主动执行的操作。它可以成为邮件系统本身的一项默认能力。

这正是 S/MIME 需要完成的转型。问题已经不再是邮件能否被加密。技术几十年前就已经回答了这个问题。真正的问题是：加密能否变得足够简单、足够可规模化、也足够可持续，从而成为默认的基础设施能力。

Web 已经完成了这一转型。现在，邮件也一定能完成同样的转型。

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 284 篇(共 83 万 9 千多字)和英文 126 篇(17 万 4 千多单词)。