零信 AI 邮探秘之一：默认加密

普及 S/MIME 需采用自动化方式、不同的证书信任域与不同的产品策略

2026 年 9 月 14 日

大家都已经认识到电子邮件需要保护，因为电子邮件是明文的。但困难的是：究竟应该如何保护？市场上存在多种邮件加密式，包括 TLS 传输层加密、安全 Web 邮箱和加密门户、专有加密系统，以及针对特定应用场景设计的解决方案。这些方式都可以应对某些威胁或使用需求，但其中许多方案依赖特定的服务商、平台或封闭生态。S/MIME 则不同，它是一种成熟、基于标准的邮件加密和数字签名方案。如果邮件保护真正要成为人人都能使用的能力，就必须建立在不同产品、组织和用户之间都可以遵循的标准之上。这正是 S/MIME 能够走向普及的基础，而不是一个封闭的邮件加密解决方案。

一、S/MIME 已经准备就绪，真正的问题在于如何使用

S/MIME 并不是一种新出现的密码技术。几十年来，它一直是电子邮件标准体系的一部分，而它的两项核心用途也始终十分明确：加密用于保护邮件内容的机密性，数字签名则提供邮件发送者身份以及邮件在发送后是否被篡改的密码学证据。技术本身已经成熟，尚未实现规模化的，是组织和个人使用这项技术的方式。

传统的 S/MIME 使用体验清楚地暴露了这一点。用户或管理员需要获取邮件证书，将证书安装到邮件客户端，管理私钥，配置加密和签名，续期证书，替换过期证书，还要处理不同的证书颁发机构和信任环境。对于 PKI 管理员而言，这些操作单独看并不算特别困难；但将它们组合在一起，就足以阻碍 S/MIME 成为日常电子邮件中的常规能力。

因此，问题在于使用模式，而不是密码学本身。如果 S/MIME 要真正成为人人都能使用的实用能力，那么围绕它的使用方式就必须改变。用户不应该先成为证书管理员，才有资格对邮件进行加密或签名。

二、数字签名可以率先发挥作用

加密和数字签名解决的是不同问题，但两者都不可或缺。加密保护邮件内容本身，不过，要实现广泛的加密通信，发送方必须拥有收件方可用的证书公钥。数字签名的部署条件则不同：发送方可以在不等待每一位收件人都拥有 S/MIME 证书的情况下开始对邮件进行签名。因此，

数字签名是 S/MIME 最快能够产生实际价值的方式之一。

这种价值并不只是让数字签名存在于邮件内部，而是要让数字签名转化为人和系统都能使用的信息。在零信 AI 邮 App 中，密码学验证结果被转化为可见的身份信号。App 不再要求用户理解证书和签名细节，而是可以明确显示邮件已经完成数字签名，并以用户能够识别的方式呈现经过验证的发件人身份信息。密码学建立信任，而用户界面让这种信任变得可见。

同样的密码学验证结果，也可以被零信 S/MIME 自动化网关用作安全策略信号。有效的 S/MIME 签名和经过验证的身份，可以成为决定邮件如何处理或是否放行的判断依据，这会改变首次信任决策的速度。传统邮件安全系统可能需要先检查邮件内容、链接、附件或其他信号，才能判断一封邮件是否值得信任；而数字签名提供了一种可以立即验证的密码学信号，使系统能够在进行更深入的检查之前，先获得关于发送方身份的重要判断依据。

这并不意味着密码学身份会取代恶意软件检测、钓鱼分析、数据防泄漏或其他邮件安全控制，这些系统仍然按照其设计目标发挥作用。变化在于，安全架构可以先建立发送方信任判断中的一个重要部分，再根据需要继续执行内容和威胁检查。对于商业电子邮件入侵（BEC）和身份假冒攻击而言，这种更早获得的信号尤其有价值，因为它为用户和安全系统提供了比“看起来熟悉的发件人地址”更可靠的依据。

三、S/MIME 自动化让普及使用成为可能

消除 S/MIME 普及使用障碍的唯一可行方案就是自动化。

S/MIME 自动化应当覆盖那些通常会让证书管理变成行政负担的工作，包括申请证书、验证必要信息、签发和部署证书、配置签名与加密功能、续期和替换证书，以及维护证书与电子邮件身份之间的关联。用户应当负责作出有意义的决定，而软件则应当处理重复性的 PKI 密码学工作。

这一原则十分重要，因为自动化不应意味着剥夺用户的控制权。用户仍然拥有自己的数字身份和私钥；自动化消除的是使用和运维负担，而不是用户的控制权。

这一点在 Web PKI 的发展历程得到验证。SSL 证书自动化通过减少证书相关的手工工作，改变了 HTTPS 的实际可用性。S/MIME 也需要类似的使用与运维转型，尽管电子邮件有其自身不同的信任机制和部署要求。真正的任务并不是重新发明 S/MIME 密码学，而是在不要求用户理解底层复杂机制的前提下，让这套密码学真正可用。

四、费用不应成为另一道 S/MIME 普及应用的门槛

使用复杂性并不是唯一障碍。S/MIME 证书成本同样可能阻碍 S/MIME 的普及应用，尤其是对于个人用户和小型组织而言，因为它们通常没有足够的理由按每个邮箱分别购买和管理 S/MIME 证书。

因此，面向个人用户和中小企业的解决方案需要采用低门槛的证书模式。零信 AI 邮 App 的方案是在零信生态内自动配置免费的 S/MIME MV 证书；而对于需要更高身份保证等级或更广泛外部信任的用户，则可以选用使用收费服务自动配置的更高身份级别证书和全球信任的证书。

关键并不在于每一张证书都必须免费，而在于证书成本和密码应用复杂性不应阻止普通用户开始使用 S/MIME 技术。

然而，当部署规模进入企业级时，问题就会发生变化。一个拥有数千甚至数万个邮箱的组织，不可能把每一位员工的证书都当作一笔需要单独开支的费用，这就需要能够融入自身邮件环境的证书基础设施。

这正是企业模式采用零信 S/MIME 自动化网关及组织级证书基础设施的原因。网关内置企业 CA 系统，采用定制的组织专用子 CA，实现在组织自身的信任域内，自动完成所有员工 S/MIME 证书的签发和生命周期管理。在这种模式下，企业不再需要花钱为每个员工邮箱采购邮件证书，而是拥有了一套能够在组织规模上自主运行的 S/MIME 自动化基础设施。

五、同一项原则，两种产品策略

让 S/MIME 人人可用，并不意味着必须开发一个产品，再要求所有用户采用同一种部署模式。个人用户、中小企业和大型企业具有根本不同的应用需求。

对于个人用户和较小型组织，零信 AI 邮 App 将 S/MIME 自动化直接集成到邮件客户端中。用户可以连接现有邮箱账户，自动申请新证书或导入旧证书，并在日常邮件使用过程中完成邮件签名和加密。其目标是让密码学层尽可能不再成为需要用户管理的日常任务。

对于大型组织，零信 S/MIME 自动化网关将 S/MIME 自动化从用户现有的邮件客户端和邮件基础设施中分离出来。它可以与现有邮件服务器和邮件安全网关协同工作，并负责邮件数字签名、加密、解密、证书生命周期管理以及可信身份处理。硬件网关增加了大规模部署所需的组织级证书基础设施；对于不需要内置企业 CA 的组织，则可以采用更轻量的软件部署模式。

这两种模式并不是对 S/MIME 的不同理解，而是同一理念的两种实现方式：S/MIME 证书相关操作应当成为基础设施能力，而不应成为用户的日常工作。App 将这一原则应用于每个

邮箱层面，Gateway 则将其应用于每个组织级别。

六、不同策略让 S/MIME 人人可用

任何认真讨论普及电子邮件加密的文章，都必须承认一个重要限制：S/MIME 加密要求发送方拥有收件方的证书公钥。这意味着，仅仅通过自动化证书签发，并不能让加密通信在一夜之间普及。证书覆盖范围仍然需要逐步扩展到不同组织、合作伙伴、客户以及更广泛的互联网环境。

数字签名可以更快地发挥作用。组织可以先对外发邮件进行数字签名，让收件人看到经过验证的身份，同时继续扩大加密所需的证书覆盖范围。因此，这两项能力可以相互强化：数字签名能够立即提供有用的发送方身份真实性和邮件完整性信号；随着越来越多的收件人能够通过免费证书和收费证书建立加密通信，邮件加密则逐步扩大机密性保护的范围。

因此，S/MIME 自动化不应仅仅被理解为证书管理，它更是一种应用模式，目的是将已经成熟的密码学转化为普通用户能够使用的日常通信能力。App 让个人用户和中小企业能够实际使用这种能力，网关则让企业能够以可部署、可扩展的方式采用它。证书自动化消除了运营摩擦，合适的证书模式减少了不必要的采用障碍，数字签名提供即时的信任信号，而随着证书覆盖范围不断扩大，普及加密才能真正实现保护邮件内容的机密性。

“**默认加密**”并不意味着每一位用户都必须使用同一种证书类型、同一个证书信任域或同一种证书产品。它意味着，每一位用户都应当拥有一条切实可行的 S/MIME 自动化实现路径，而不必先成为密码技术专家。密码学早已存在，真正的工程实施挑战，是让使用它成为一种自然、普遍的日常行为。

王高华

2026 年 9 月 14 日于深圳
