零信 AI 邮探秘之八：生态建设

安全 + 密码：共同构建全球邮件安全生态

2026 年 9 月 23 日

一所学校最近发邮件提醒家长，要通过检查发件人域名来确认邮件是否确实来自学校。这是一种合理的防范措施，但它也暴露出一个更深层的问题：收件人在邮件中看到的信息，本身并不能证明邮件究竟是谁发送的。

如今，电子邮件已经拥有成熟的安全系统、受信任的域名、身份认证机制以及多层威胁检测能力，但收件人仍然经常需要自己做最后的判断。如果围绕电子邮件的基础设施已经如此成熟，为什么建立密码学信任仍然需要大量专业化工作？其中的缺口究竟在哪里？

1. 邮件安全是一个生态问题

邮件安全经常被描述成一个产品问题：部署一个网关、配置邮件证书、启用加密，然后工作就完成了。但在企业规模下，现实情况并非如此，因为电子邮件并不是一个单一应用，而是一整套服务、产品、身份、信任关系和专业系统组成的链条，这些系统经过数十年的演进，如今跨越组织和国家边界运行。

S/MIME 数十年来一直提供着底层的密码学模型：证书可以将身份与公钥绑定，数字签名可以提供完整性和发送者身份，加密则可以保护邮件内容。因此，真正的挑战并不在于技术是否存在，而在于如何让完整的证书生命周期在承载全球电子邮件的现有基础设施中切实可行，同时又不要求每一个参与者重新构建自己已经提供的功能。

因此，邮件安全首先是一个生态问题，而不仅仅是一个产品问题。真正需要回答的不是应该替换哪个现有系统，而是如何让密码学能力成为现有系统和工作流程中可靠的一部分，使安全、信任、邮件投递和密码学保护能够作为一个协调一致的过程运行。

2. 每个参与者都已经擅长自己的事情

现有的电子邮件生态已经拥有成熟的专业参与者，每一方都经过多年的发展，在整体流程中的某个环节形成了自己的能力。邮件平台负责邮件投递和存储；安全厂商负责邮件检测和防护；CA 机构在各自的信任体系中负责身份鉴证和证书签发；邮件客户端提供用户体验；云平台和 AI 平台则提供应用、基础设施和分析能力。

这些角色都不可或缺，电子邮件密码学才会变得更容易部署。安全厂商不需要变成 CA 机构，CA 机构也不需要变成邮件安全平台。邮件服务商不需要重建自己的信息基础设施，AI 服务也不需要因为密码学日益成为可信通信的重要组成部分，就变成一个密码学系统。

目前缺少的是这些既有能力与日常电子邮件之间的运行连接：一种能够自动化获取证书和信任，将其与密钥及密码学操作连接起来，并把这些能力带入用户和组织已经依赖的邮件工作

流程中的机制。

3. 当加密成为安全问题时

邮件安全的核心存在一个架构上的张力。安全系统需要获得足够的邮件访问能力，以便进行检测、分类和策略执行；而消息级加密的设计目的，恰恰是确保只有经过授权的接收者才能访问受保护的内容。这两个目标都合理，但如果组织希望它们协同运行，就不能把它们视为彼此独立的功能。

因此，邮件加密技术反而可能降低安全系统保护邮件所需要的可见性。这并不是反对加密，而是一个系统协同问题；随着组织增加更多安全检测、策略执行和自动化分析层，这一问题会变得更加突出。

实际可行的架构必须允许安全检测与密码学保护在受控的工作流程中共存。对于入站邮件，可以在适当的组织控制下进行解密，由现有安全栈完成检测，然后按照策略投递；对于出站邮件，则可以先完成安全检测，再对邮件进行数字签名，并在需要时为收件人加密。在两个方向上，目标都是保留两套系统各自的优势，而不是迫使一种能力牺牲另一种能力。

因此，目标既不是让安全系统看到更少的内容，也不是为了检测而削弱密码学保护，而是让密码学保护与安全检测作为同一套邮件基础设施中相互协调的组成部分共同工作。

4. 缺失的能力：密码应用自动化

这正是密码应用层应该发挥作用的地方。它的任务不是成为邮件服务器、反恶意软件引擎、DLP 平台或 AI 模型；相反，它的目的在于让密码学能够真正应用于这些现有工作流程，并将密码学操作与电子邮件已经运行其中的应用和基础设施连接起来。

这包括证书申请与续期、证书选择、密钥保护、签名、加密、解密、身份展示以及生命周期管理，但更深层的价值在于协调这些功能，使它们不再是彼此孤立的管理任务。当这些操作实现自动化并与应用工作流程连接起来之后，密码学就可以成为日常邮件行为的一部分，而不再是需要用户和管理员单独管理的项目。

证书已经存在。安全栈也已经存在。现在缺少的是让它们协同工作的自动化，因为仅有证书，并不能自动地把可用的密码学身份部署到邮件客户端中，保护相关密钥，为邮件选择正确的证书，或管理随之而来的生命周期。

这与成为一家 CA 或安全厂商有着根本不同。其目的并不是取代任何一方，而是让它们的能力能够高效协同，同时让每一个参与者继续专注于自己最擅长的生态环节。

5. 安全 + 密码：两种能力，一个工作流程

安全与密码解决的是信任问题中的不同部分。安全系统负责检测威胁、检查内容、执行策略并响应可疑活动，而密码提供可验证身份、消息完整性和机密性的机制。如果把两者视为相互竞争的层，就会得到适得其反的效果；实际上，它们完全可以在同一个工作流程中协调运行。

因此，两者是互补关系，而不是竞争关系。密码应用网关可以与现有的邮件安全网关并行部署，各自执行自己最擅长的工作，同时组织可以保留现有的安全策略和检测能力，而不必仅仅为了引入 S/MIME 就建立一套平行的安全栈。

一个典型的入站流程可以是：加密邮件进入 → 密码应用网关 → 解密 → 现有安全栈检测 / 识别 / 执行策略 → 邮件客户端。对于出站邮件，流程可以是：邮件客户端 → 安全检测 → 密码应用网关 → 已签名和/或已加密邮件发出。如果不需要机密性，可以对邮件进行数字签名并关联可信身份；如果需要机密性，则可以在投递之前完成签名和加密。

这一架构也说明了协同的重要性。密码学身份并不能消除被攻陷的账户、被窃取的私钥或恶意内部人员，因为密码学本身无法消除所有攻击路径。它所改变的是：发送者身份和消息完整性可以通过密码学进行验证，而不再仅仅依赖可见的声明和基于内容的信号，从而为更广泛的安全模型增加一种独立的信任信号。

6. 缺失的产业角色：密码应用自动化提供商

当我们把问题视为一个生态问题时，一个独立的产业角色就变得清晰起来：密码应用自动化提供商（Cryptographic Application Automation Provider，CAAP）。之所以需要这一角色，是因为产业已经拥有 CA 机构、安全厂商、邮件平台、邮件客户端以及密码技术，但这些能力并不会因为各个组件都已经存在，就自动形成一个统一的运行工作流程。

CA 机构已经提供邮件证书和信任。安全厂商已经提供安全防护能力。邮件服务商已经提供邮件基础设施。邮件客户端已经提供用户发送和接收邮件的界面。现在缺少的是这样一种提供方：连接这些能力，并自动化密码应用生命周期，使基于证书的信任和密码学功能能够无缝参与日常邮件操作。

CAAP 可以连接证书服务、信任、密钥、密码学操作、邮件基础设施和安全工作流程，让每个参与者都能够发挥自己擅长的能力，而不必要求所有参与者都开发一套彼此重叠的功能。这是一个具有明确架构目的的集成与自动化角色，而不是试图把整个邮件安全栈重新集中到一起。

原则其实很简单：相关的每一家服务提供方都做好自己最擅长的事情。CAAP 让这些部分协同工作，使整个生态能够提供一种单个参与者很难高效独立提供的能力。

7. 国际标准让生态实现互操作

一个生态不仅需要各自独立的能力，还需要一种共同的方法，让这些能力能够协同工作；否则，每一个连接都会变成一项必须单独设计、实施和维护的专有集成。这正是国际标准的力量所在：标准提供共同规则，使独立开发的组件能够参与同一个技术流程。

RFC 8823 由 IETF 发布，在 ACME（RFC 8555）的基础上扩展了面向终端用户 S/MIME 证书的自动化机制。它定义了电子邮件标识符和基于电子邮件的挑战机制，并明确考虑了支持 ACME 的邮件用户代理（MUA）。在实际应用中，它为邮件应用参与自动化 S/MIME 证书流程提供了一条标准化路径，而不再把证书申请完全当作一个独立的人工流程。

RFC 8823 的意义并不在于创造另一种证书技术，而在于建立一种共同的技术语言，使邮件应用、证书自动化服务和信任提供方能够参与自动化，并让不同厂商可以实现相互兼容的组件，而不必针对每一种合作关系分别协商一套专有协议。

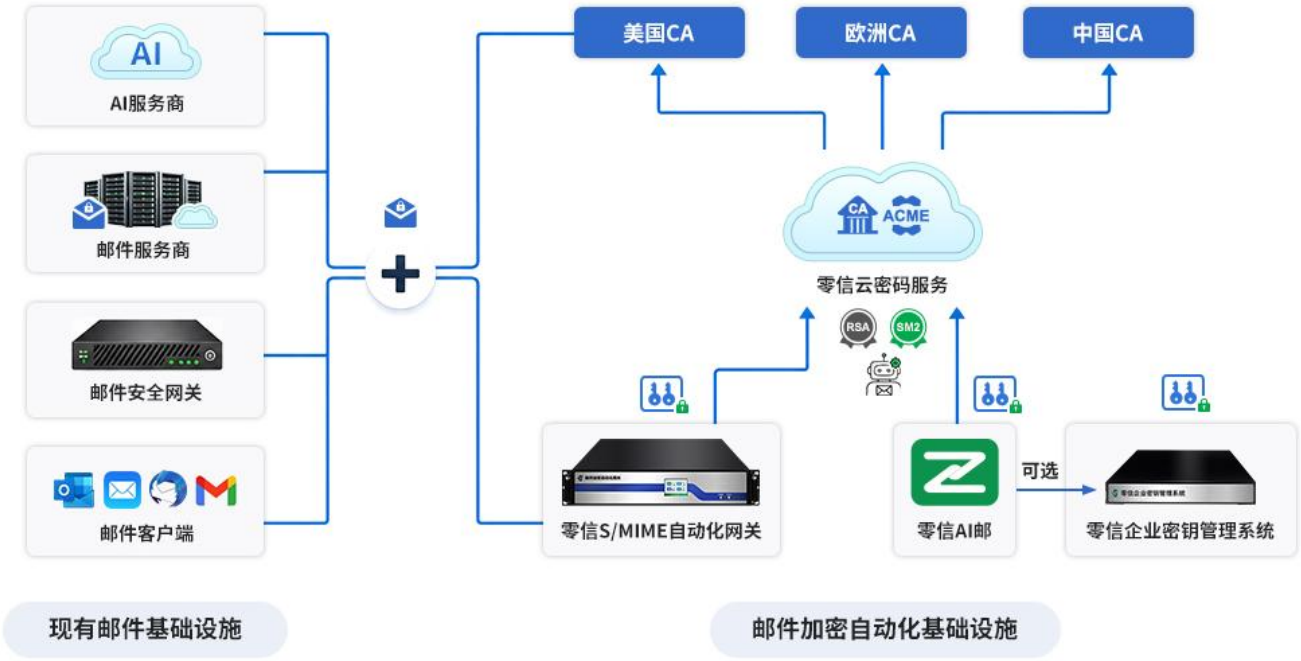
这正是国际标准对生态的重要意义。依赖专有接口，产业可以生产能力很强的产品，却仍然可能难以高效连接；采用开放标准后，不同厂商可以实现兼容的组件，围绕同一技术基础建

立集成，并让生态不断扩展，而不受限于单一产品或单一提供方。

标准定义路径，自动化让这条路径真正可用。

8. 零信 AI 邮：将标准变成可运行的生态

零信 AI 邮定位为密码应用自动化提供商，其系统设计目标是展示当各种安全组件实现端到端连接后，这一模式可以如何运行。零信 AI 邮 App 将 S/MIME 自动化带入用户工作流程，而零信 S/MIME 自动化网关则把密码应用自动化延伸到组织安全基础设施；证书自动化服务和密码基础设施将证书签发及生命周期操作与这些应用连接起来，由此形成一个完整实现，使主要功能能够作为一个协调一致的过程运行。



重要的并不是零信 AI 邮必须拥有每一个组成部分，而是完整工作流程可以真正运行起来：身份和证书可以通过自动化流程获得；密钥和密码学操作可以在适当的应用软件和基础设施中进行管理；邮件则可以在日常操作中自动完成签名、验签、加密、解密和可信身份展示，而不再是一系列彼此分离的管理流程。

从这个意义上说，零信 AI 邮并不是要成为另一个邮件平台、另一套安全栈或另一家 CA。它是在实现密码应用自动化提供方这一角色，即 CAAP，并通过开放标准展示现有能力如何连接起来，使整个产业看到的不是一组孤立的技术，而是一种这些技术可以协同工作的实际模式。

零信 AI 邮之所以端到端地构建这一模式，是因为当生态拥有一个能够展示完整路径、为集成提供基础，并让其他参与者看到自己的能力可以在哪里接入的实际实现时，生态会更容易建立。因此，构建第一个完整模型的目的并不是封闭生态，而是让其他参与者更容易加入生态。

9. 从一个可运行的模型走向开放的产业生态

一个成功的生态不应该依赖单一厂商，因为目标不是在电子邮件内部再建立一座封闭的专有孤岛，而是建立一种更多参与者都可以实施、集成和扩展的模式。当这一模式得到验证后，下一

步自然就是邀请更多参与者使用相同的标准作为共同技术基础，共同建设这一生态。

其他 CAAP 可以提供自己的实现和服务，其他邮件客户端厂商可以增加对 ACME 和 RFC 8823 的支持。其他密码技术提供商可以开发 S/MIME 自动化网关。CA 机构可以继续通过 ACME 为 S/MIME 证书提供证书和信任服务，而安全厂商则可以将密码学工作流程与现有的检测和策略能力集成，使生态通过专业化而不是集中化不断发展。

这正是开放标准的力量：生态可以通过参与而不是依赖单一专有架构不断成长。随着更多独立参与者实现技术兼容，可实现的集成数量会增加，部署选择会更加多样化，组织也可以越来越容易地保障邮件安全，而不必依赖一家提供商提供所有组件。

因此，零信 AI 邮的角色并不是拥有这个生态，而是帮助搭建舞台，证明这些部分可以协同工作，并邀请更广泛的产业参与其中。第一个完整实现是对这一模式的证明；更大的目标，是让整个产业都可以在这一模式之上继续建设和发展。

10. 诚邀共同建设邮件安全的未来

S/MIME 不必永远是一项只有那些拥有足够资源、能够手工管理证书、密钥、邮件客户端和密码学基础设施的组织才能使用的专业能力。技术已经存在，标准已经存在，产业也已经拥有支持邮件安全所需的大部分专业能力；现在需要做的是连接这些能力，自动化其中的协同工作，并让这一模式能够在全球规模上真正落地。

这需要整个产业的协作。邮件客户端厂商可以让密码学成为用户体验的一部分；CA 机构可以借助 ACME 能力提供身份和信任；安全厂商可以通过引入信任信号，增强检测、检查和防护能力；密码技术提供商可以构建安全的密码学基础设施；邮件和云平台可以在自身平台内提供邮件加密自动化服务；而密码应用自动化提供方则可以连接这些能力，并将它们转化为可

运行的工作流程。

零信 AI 邮已经构建了一个端到端的实现，用于展示这一生态如何在实践中运行，并遵循相关标准、连接产业中已经存在的各种角色。下一步的目标将超越任何单一产品或公司：邀请更多参与者实施这些标准、连接各自的能力、开发兼容的产品和服务，并共同实现全球所有个人用户、中小企业和大型组织的电子邮件安全密码应用自动化。

目标不是让零信 AI 邮成为这个生态，而是建设一个整个产业都能够参与其中的生态，让每个参与者贡献自己的专业能力，并共同扩大邮件安全的实际应用范围。

归根结底，这不仅关乎一个产品、一家公司或一个市场，而是要完成这样一次技术革命：让 S/MIME 从一项技术上已经成熟的能力，真正成为全球电子邮件基础设施中广泛可用的一部分，使强大的密码学身份、完整性和机密性保护能够在任何使用电子邮件的地方得到普及应用。

只有整个产业共同努力，才能让 S/MIME 从一项经过验证的技术，真正成为电子邮件普遍可用的能力，让安全、可信的电子邮件成为全球每个人和每个组织都能够切实享有的现实。

王高华

2026 年 9 月 23 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 293 篇(共 87 万 7 千多字)和英文 135 篇(19 万 1 千多单词)。