零信 AI 邮探秘之三：身份可视

身份认证如何重新定义电子邮件信任

2026 年 9 月 17 日

生成式 AI 正在让电子邮件通信变得更加智能和高效，帮助用户起草邮件、总结信息并自动化处理工作流程。然而，更高的智能并不会自动带来更高的信任。随着 AI 生成的通信内容越来越逼真，也越来越容易大规模生产，电子邮件安全面临一个根本性挑战：收件人和邮件安全系统如何有把握地判断，一封邮件背后究竟是谁？

商业电子邮件入侵（BEC）清楚地暴露了这一挑战。不同于依赖恶意软件或技术漏洞的传统攻击，许多 BEC 攻击的成功关键在于利用信任。攻击者冒充单位领导、企业高管、供应商、客户和业务伙伴，诱使收件人将虚假身份当作真实身份。AI 并没有改变这种威胁的本质，但显著提升了攻击者制造具有说服力、看起来像正常商务往来的通信内容的能力。

多年来，电子邮件安全主要依靠邮件检查、威胁情报、信誉分析和行为监控来检测可疑内容。这些能力仍然不可或缺，但它们存在一个根本局限：它们试图在邮件已经生成之后，判断这封邮件看起来是否可疑。随着攻击者越来越擅长使用 AI 生成逼真的邮件内容，行业需要一种更坚实的基础，用来确认发件人身份本身是否值得信任。

一、以密码学身份突破检测瓶颈

基于内容的检测存在一个核心弱点：许多 BEC 攻击并不包含明显的技术指标。一封欺诈邮件可能使用恰当的语言，符合特定业务场景，并模仿某位受信任人士的沟通风格。因此，核心问题不仅在于邮件包含什么内容，还在于邮件背后的身份是否真实。

数字签名通过将通信内容与受密码学保护的身份关联起来，提供了这一缺失的信任层。借助 S/MIME，电子邮件系统可以将发件人身份与数字证书关联，使收件人能够验证邮件是否由相应身份证书数字签名，以及邮件内容是否曾被篡改。

IT 行业从来不缺少构建可信电子邮件所需的密码学基础。真正的挑战在于，如何将这一基础转化为能够在日常通信规模下运行的实用能力。证书申请、部署、续期和密钥管理长期以来带来的极高的运维复杂度，严重限制了其普及应用。

自动化将改变这一模式：它将证书生命周期管理和签名操作整合进现有的电子邮件工作流程。当这些过程对用户而言足够透明、对组织而言易于管理时，密码学身份就能从一种专业化的安全能力，转变为实用的通信标准。

二、让已认证的身份在电子邮件中可见

尽管 S/MIME 证书包含有价值的身份信息，但这些信息过去通常隐藏在技术性的证书字段中。证书颁发机构和身份鉴证流程所建立的信任确实存在，但普通用户在判断是否信任一封邮件时，很少能够看到或理解这些信息。

HTTPS 的成功提供了一个重要启示。安全浏览之所以得到广泛采用，并不只是因为加密技术已经存在；它之所以能够普及，原因之一是浏览器在用户作出判断的关键位置，将信任展示了出来。浏览器界面把复杂的证书验证转化为简单易懂的安全体验。

电子邮件也需要经历类似的转变。零信 AI 邮通过将基于 S/MIME 证书的身份保证转化为邮件使用过程中的可见信任信息，来应对这一挑战。零信 AI 邮 App 不要求收件人手动检查证书主题信息，而是直接在邮件界面中展示已认证的可信身份信息，使用户不仅能够了解数字签名是否有效，还能了解发件人身份背后的可信保证级别。

根据 CA/浏览器论坛国际标准组织定义的 S/MIME 身份可信保证级别，每封已数字签名的电子邮件包括了邮箱认证（MV）或个人认证（IV）或单位认证（OV）或单位员工认证（SV），这些可信身份就可以成为有实际意义的信任信号，而不再只是隐藏的技术元数据。

图 1：零信 AI 邮 App 在邮件 UI 展示已认证的可信身份信息，使收件人能够查看发件人的身份信任级别及其关联的组织信息。

三、从人可见的信任到机器可见的安全

验证邮件可信身份所创造的价值并不止于提升用户认知，因为同样的信任信息还可以成为企业邮件安全系统能够采取行动的信号。零信 AI 邮通过密码学网关架构，将身份可视性从应用层延伸至邮件安全基础设施。

零信 AI 邮 App 让人能够看到每封邮件的可信身份，而**零信 S/MIME 自动化网关**则让邮件安全系统能够识别可信身份。网关可以评估入站邮件所关联的已验证身份，并将相关信息纳入自动化安全策略。组织可以将身份保证信息作为额外因素，用于决定一封通信是否可以放行、需要监控，或应接受进一步的安全控制。

这改变了可信数字身份在电子邮件安全中的角色。身份不再只是展示给用户看的信息，也成为安全系统可以评估并据此采取行动的安全信号。人可见的信任帮助用户作出更好的判断，而机器可见的信任则使组织能够基于经过验证的发件人信息，自动执行安全策略。

四、建立基于可信身份的电子邮件安全生命周期

完整的基于身份的电子邮件安全模型，需要让已认证身份贯穿整个邮件通信生命周期。在发送邮件时，邮件客户端（如零信 AI 邮 App）和企业网关系统（如零信 S/MIME 自动化网关）使用适当的可信身份证书，例如 IV、OV 或 SV 证书，为邮件实施与邮箱对应的发件人的可信身份相关联的数字签名。

当邮件到达收件人一侧时，邮件客户端和网关可以验证这些数字签名，识别相应的可信身份级别，App 展示可信身份信息，收件人和网关都可以根据该身份作出安全决策。这些能力共同构成了完整的密码学信任生命周期：在通信开始之前建立发件人身份，使用与身份绑定的证书对邮件进行数字签名，使收件人能够理解通信背后的信任级别，并让企业系统能够执行基于可信身份的安全策略。

不同于主要依赖检测可疑内容的方法，这一模型通过受密码学保护并经过可信第三方认证的身份来建立信任，从而为 BEC 等基于身份的攻击提供更直接的快速防御。

五、电子邮件安全的未来以可信身份为中心

电子邮件安全的未来不会仅仅由更智能的检测技术所定义，还将取决于能否在邮件欺骗发生之前建立可信通信。

随着经过身份认证的可信身份的电子邮件日益普及，许多依赖身份假冒的欺诈手段将失去其赖以存在的基础。所以，现在就开始普及应用实际上已无门槛的电子邮件数字签名技术，将一定能彻底消灭邮件欺诈和 BEC 攻击。加密对于保护通信机密性仍然不可或缺，而数字签名和验证身份则为判断通信参与者是谁提供了技术基础。

下一代电子邮件安全将把密码学、自动化和用户体验结合起来，使信任不再只是被默认接受，而是在整个通信生命周期中得到验证。这正是零信 AI 邮致力于推进的方向：让可信身份可视和可操作。

王高华

2026 年 9 月 17 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 288 篇(共 85 万 2 千多字)和英文 130 篇(18 万多单词)。