为什么邮件加密比网站 HTTPS 更难普及？

2026 年 8 月 14 日

Let's Encrypt 于 2015 年正式推出，通过 ACME（自动化证书管理环境）协议，让 SSL 证书的申请、验证和续订实现了全自动。短短十年间，全球 HTTPS 加密普及率从不到 50%跃升至超过 95%。浏览器对 HTTP 站点强制显示红色“不安全”警告，更是在用户侧形成了强大的倒逼机制。

与此同时，S/MIME 邮件加密技术在 1995 年就已诞生，其首个正式标准 RFC 2311 于 1998 年确立，比 ACME 协议的 RFC 8555（2019 年）早了整整 21 年。然而二十多年过去了，邮件加密的普及率仍然低得惊人,一项覆盖 27 年、涉及 8100 多万封邮件的研究显示，仅 5.46%的用户用过加密，加密邮件占比仅 0.06%。

同样是加密，为什么邮件比 HTTPS 难了这么多？

一、HTTPS 是如何成功普及的？

HTTPS 的普及，是一场由“自动化”和“UI 警示”双轮驱动的革命。

自动化层面：Let's Encrypt 和 ACME 协议让 SSL 证书实现了自动申请、自动验证、自动续期。网站管理员不再需要手动向 CA 提交资料、域名验证、等待审核、下载证书、手动安装。这一切都变成了后台的自动化流程。

UI 警示层面：Chrome、Edge、Firefox 等主流浏览器对 HTTP 站点强制显示“不安全”红色警告。当用户看到“不安全”三个字，出于信息安全顾虑，90%以上会直接关闭页面。这种直观的视觉警示，让“不加密”变得不可接受。

这套组合拳的效果立竿见影：**技术层面让加密变得零门槛，用户层面让“不加密”变得不可接受。**

二、S/MIME 加密普及的三大门槛

反观邮件加密，S/MIME 虽然早在 1998 年就成为标准，但普及率始终上不去。主要有三大门槛：

门槛一：证书申请和配置极其复杂。用户需要向 CA 机构申请 S/MIME 证书、验证身份、下载证书、手动配置到邮件客户端中。这一套流程足以让 99.99%的用户望而却步。

门槛二：公钥交换困难。发送加密邮件前，收发双方需要事先交换公钥证书。这相当于在

加密通信之前还需要一个“加密的准备工作”，大大增加了使用门槛。

门槛三：密钥管理繁琐。证书有有效期，到期需要续期；更换设备需要重新配置；私钥丢失则所有加密邮件无法解密，这些管理负担让普通用户难以承受。

三、为什么邮件加密比 HTTPS 更难自动化？

HTTPS 和 S/MIME 虽然都依赖 PKI（公钥基础设施），但自动化的难度完全不在一个量级：

主体不同。 SSL 证书只需在**服务器端**配置一次，一个证书服务于一个网站的所有用户。而 S/MIME 证书涉及**每一个邮件用户**，普及难度呈指数级上升。

生态不同。网站有统一的 Web 服务器生态（Nginx、Apache 等），ACME 协议可以标准化对接。邮件则涉及无数客户端和设备（Outlook、Thunderbird、Apple Mail、Gmail 网页版），互操作性极差。

意识不同。用户对“邮件是明文的”缺乏感知。二十多年来，人们习惯了在邮件里讨论合同、传递财务报表、交换身份信息，却很少有人意识到这些内容在网络上是“裸奔”的。

四、UI 警示：HTTPS 普及的“临门一脚”

HTTPS 普及过程中，最关键的推动力未必是技术本身，而是**浏览器 UI 的“不安全”警告**。当用户在地址栏看到“不安全”三个红色大字，第一反应是警觉和回避。这种直观的视觉警示，让“加密”从一个技术选项变成了用户期待的默认配置。网站所有者为了不让用户流失，不得不尽快部署 SSL 证书。

但邮件客户端在这个问题上一直缺位。传统邮件客户端（Outlook、Thunderbird、Apple Mail 等）对未加密邮件**没有任何视觉警示**。用户收了一辈子明文邮件，从未收到过任何“不安全”的提醒，自然也就没有动力去改变。

五、零信 AI 邮：自动化加密 + 看得见的安全

零信 AI 邮的设计理念，正是同时解决“自动化”和“可视化”两大问题：

1. 自动化层面

借鉴 ACME 协议的成功经验，实现了邮件证书的全自动管理：

- **自动化证书管理**：基于 RFC8823 标准，用户在设置点击“申请证书”后，系统自动完成证书申请和配置一张 RSA S/MIME 证书。有国密合规需求的用户可按需申请 SM2 算法 S/MIME 证书。密钥在本地生成，私钥永不离开用户设备。

- **自动化公钥交换：**发送加密邮件时，系统自动查询证书目录服务获取收件人公钥证书，收发双方无需事先交换公钥。
- **自动化密钥管理：**密钥在本地生成和保存，支持一键加密导出/导入备份/恢复到用户自己邮箱中，用户自主管理。

2. 可视化层面

零信 AI 邮借鉴浏览器的“不安全”警示机制，在邮件客户端中实现了创新的 UI 展示：

- **有数字签名和加密但仅验证邮箱：**显示签名和加密标识、**T1 认证标识**。**个人认证（IV）：**显示 **T2 认证标识**、已认证的姓名。**单位认证（OV）：**显示 **T3 认证标识**、已认证的单位名称。**单位员工认证（SV）：**显示 **T4 认证标识**、已认证的发件人姓名和所属单位名称。
- **未加密邮件显示“不安全”：**凡是没有数字签名的邮件，都会显示一个**警告惊叹号标识**和一个**黑色开锁图标**，表示此邮件没有数字签名和没有加密，提醒用户注意发件人身份是否可信。

- **邮件地址不一致提醒：**如果邮件头中的发件人地址同证书中绑定的地址不一致，会在发件人地址后面增加一个**警告惊叹号标识**。**邮件被篡改警告：**如果数字签名验证有问题，会显示“**数字签名有问题，邮件内容已被篡改，请勿相信邮件内容！**”。**签名证书已过期：**显示黄色签名图标，会显示“签名者证书已过期”
- **加密状态一目了然：**点击加密锁标识，显示“邮件已加密”；点击数字签名标识，显示“签名有效，内容未被篡改，证书链受信任”。

这套 UI 体系的逻辑非常清晰：**没有加密和签名的邮件，用户一眼就能看到“不安全”；有加密和签名的邮件，用户一眼就能看到发件人的可信身份级别**。就像浏览器用“不安全”三个字倒逼网站部署 HTTPS 一样，零信 AI 邮用直观的视觉标识让邮件安全变得“看得见”。

让每一封不安全邮件都无所遁形，让每一封安全邮件都身份分明。

六、普及邮件加密，也急需自动化

HTTPS 的普及证明了一条真理：**加密的普及，不能靠用户的自发学习，而要靠技术的自动化和“不加密”的不可接受。**

今天 HTTPS 的成就，就是明天 S/MIME 可以到达的地方。零信 AI 邮的目标，就是**让邮件加密像 HTTPS 一样，成为默认、无感的基础设施。**技术层面实现全自动，用户层面让“不安全”一目了然。

当每一封未加密的邮件都显示“不安全”警告，当每一封已加密的邮件都清晰展示发件人的可信身份，邮件加密的普及就不再是一个技术问题，而是一个时间问题。

免费自动化配置 S/MIME 邮件证书，自动化实现端到端邮件加密，让普及电子邮件加密不再有门槛，普惠保障全球电子邮件安全。

浏览器普及了 HTTPS，零信 AI 邮将普及 S/MIME。两条路，同一个答案：自动化。

王高华

2026 年 8 月 14 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 280 篇(共 83 万 1 千多字)和英文 122 篇(16 万 9 千多单词)。