

零信 AI 邮探秘之六：用户自主

为什么即使是自动化也不应该替用户做决定

2026 年 9 月 21 日

自动化是现代软件变得越来越易用的主要原因之一。然而，自动完成工作与替用户做出决定之间存在一个根本区别。在电子邮件领域，这一区别尤其重要，因为证书、身份、私钥、信任关系、邮件数据以及 AI 服务都涉及可能产生不同的安全、隐私和通信结果的选择。因此，零信 AI 邮 App 的设计原则非常简单：自动化完成工作，但用户始终保持控制权。

这一原则贯穿零信 AI 邮 App 的所有设计，从 S/MIME 证书如何申请和选择，到发送邮件时使用哪一种身份；从密码学密钥如何备份和恢复，到选择哪一家 AI 服务商以及授予 AI 助手什么权限。目标并不是让用户手工配置一切，而是在自动完成重复性技术操作的同时，让重要的选择保持用户可见、明确，并且可以随时修改。

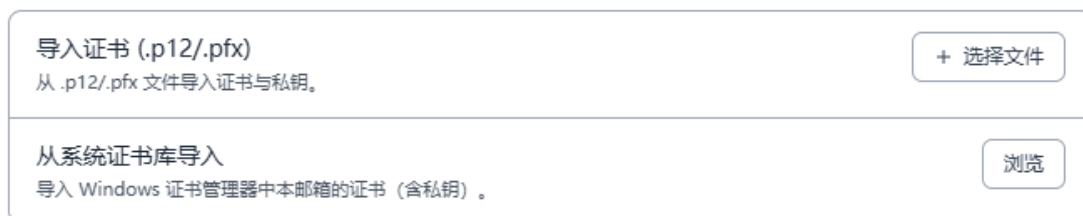
一、由用户发起的自动化证书管理，密码算法由用户自己选择

零信 AI 邮 App 提供免费的 S/MIME 证书并自动完成配置，但这一过程不会从用户登录了邮件账户就自动开始。用户必须主动打开“设置 - 证书”，并点击“自动申请证书”，才会开始自动申请证书。这一操作看似很小，却建立了一条重要的自主边界：自动化始于用户意图。

同样的原则也适用于密码算法。零信 AI 邮 App 不会自动创建一组固定的、多算法证书，而是让用户决定自己需要什么。用户可以申请 RSA 算法证书、SM2 算法证书，或者同时申请

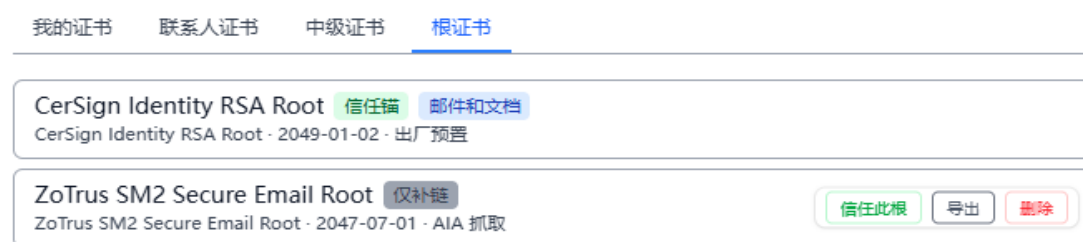
两种算法的证书。具体选择取决于用户的需求、兼容性要求以及所处的密码学环境。即使证书是免费的，零信 AI 邮 App 仍然把是否申请和使用这张证书由用户自主决定。

用户也可以导入自己已经从其他 CA 获得的邮件证书。现有证书可以从 PFX 文件或 Windows 证书存储中导入，用户可以决定哪张证书作为默认签名证书，以及哪张证书用于加密。通过零信 AI 邮 App 获得的免费证书，同样可以由用户删除或导出。



用户自主这一原则同样适用于零信 AI 邮 App 与 微软邮件客户端 Outlook 的互操作设计。早期方案是把零信 AI 邮 App 免费自动配置的邮件证书自动安装到 Windows 证书存储中，使 Outlook 无需额外设置即可解密零信 AI 邮 App 加密的邮件。最终方案则要求用户在需要这种互操作时自行手动导出并安装证书到 Windows 中。这个结果确实没有那么“自动”，但安全边界更加清晰：零信 AI 邮 App 不会在用户不知情、也未作出选择的情况下，悄悄把证书安装到用户的计算机中。

信任锚点遵循同样的规则。零信 AI 邮 App 已预置信任几家 CA 的根证书作为预定义信任配置的一部分，但不会仅仅因为一封签名邮件包含了由某个 CA 签发的证书，就自动信任这个原本并不受信任的根 CA 证书。如果用户收到一封数字签名邮件，而其证书链指向一个尚未被信任的 CA，用户可以点击“信任此根”。究竟信任哪一个 CA，仍然由用户自己决定。



二、发送邮件时，由用户选择展示何种身份

电子邮件身份并不仅仅是一个显示名称。一封有数字签名的 S/MIME 邮件携带了能够通过密码学验证的发送者可信身份信息，而不同的证书认证等级可以提供不同程度的身份保证。零信 AI 邮 App 遵循 CA/浏览器论坛定义的四类 S/MIME 证书认证类别：邮箱认证（MV）、个人认证（IV）、单位认证（OV）和单位员工认证（SV）。

最重要的是，用户可以选择在某一次具体通信中使用哪一个身份等级。如果用户认为邮箱认证已经足够，用户可以使用 MV 身份；如果需要经过认证的个人身份，可以使用 IV 身份；如果需要确认单位身份，或者确认个人与某一单位之间的关系，则可以使用 OV 或 SV 身份。用户也可以选择不对邮件进行签名和/或加密，而以普通明文邮件发送。最终采用什么通信方式、展示什么身份，由用户自主决定。



这一选择可以根据收件人和通信场景而变化。例如，在与一位从未见过面的收件人进行首次商务沟通时，OV 或 SV 身份所提供的身份信息，可能比仅有邮箱验证的身份更符合发件人的需求。当邮件在零信 AI 邮 App 中收到后，经过认证的身份会通过相应的信任级别图标显示出来。例如 T3 表示单位身份已经认证，T4 表示单位员工身份已经认证，同时显示已认证的单位名称。技术不会强迫用户在每一种情况下都展示可用的最高身份等级，而是让用户能够选择与当前通信相匹配的身份。

三、自动备份与恢复，但不接管用户的密钥

证书和密钥管理是实际部署 S/MIME 时最困难的部分之一。用户需要在更换设备、迁移邮件客户端、重新安装操作系统以及发生恢复事件时，持续保留证书和私钥。行业中的一种常见做法是将私钥材料同步备份到由服务商控制的云端。这种方式可以简化恢复手续，但也会让密码学控制权更加接近服务商。

零信 AI 邮 App 采用了不同的模式。证书和私钥材料被自动打包成加密备份文件，并存储在用户自己的邮箱中。恢复密钥由用户自己负责保管。当用户需要在另一台设备上恢复自己的密钥时，恢复密钥由用户提供，而不是由零信 AI 邮 App 持有。



这种设计把自动化与所有权分离开来。零信 AI 邮 App 自动完成创建、更新、存储和读取加密备份等重复性工作，而用户仍然控制用于解锁这些备份的恢复密钥。用户也可以随时主动发起同步，以恢复证书和密钥。如果历史加密邮件依赖之前使用过的密钥，App 一样会自动恢复相关证书和密钥材料，使旧的加密邮件继续保持可访问状态，但前提是相应的加密备份仍然存在。

同样的原则也适用于通讯录和日历。零信 AI 邮 App 不会把这些信息备份到零信 AI 邮 App 的云端，而是将通讯录、日历及相关用户设置打包成加密备份文件，存储在用户自己的邮箱中。是否允许另一台设备导入这些信息，仍然由用户决定。零信 AI 邮 App 提供同步机制，但不会因此成为用户个人数据的所有者。自动化是一种服务，而不是一种控制权转移：系统负责让自动恢复变得可行，用户自主决定何时恢复、恢复什么以及在哪个设备上恢复。

四、AI 服务商由用户选择，API 密钥由用户掌控

AI 助手正在成为电子邮件软件中的标准功能，但许多产品会把助手绑定到服务商自己的 AI 服务。用户可能并不清楚具体使用的是哪一个模型、请求在哪里处理，以及哪些凭据被用于授权这项服务。

零信 AI 邮 App 采取了不同的方法。用户自主选择 AI 服务商，自带配置该服务商的 API 密钥，并在本地管理 AI 助手。零信 AI 邮 App 提供的是 AI 集成工具，而不是把某一家 AI 厂商捆绑进产品。用户使用自己的 AI 服务，API 密钥保留在用户自己的电脑中。

通用

账户

外观

签名

规则

证书

网络

存储

备份

AI

关于

接入

DeepSeek

+

-

名称

DeepSeek

服务商预设

DeepSeek

OpenAI

Ollama

Custom

BASE URL

https://api.deepseek.com/v1

模型

deepseek-chat

这种模式也明确区分了 AI 密钥与密码学密钥。AI 密钥用于授权访问 AI 服务；密码学密钥则通过加密和数字签名保护电子邮件。两者不能相互替代。允许 AI 助手访问一封邮件，并不会因此产生对发送者的密码学信任；而拥有经过密码学验证的身份，也不会决定用户应该信任哪一家 AI 服务。

五、AI 可以访问哪些邮件内容，由用户自己决定

选择 AI 服务商只是用户自主的一部分。更重要的问题是：AI 助手究竟被允许读取什么。为此，零信 AI 邮 App 提供多个级别的邮件访问权限，让用户决定 AI 助手可以使用多少邮件信息。

在限制最严格的级别，用户可以完全关闭 AI 服务的邮件访问权限。下一个级别只允许访问当前邮件，而且只有当用户明确选择将邮件内容加入 AI 请求时，AI 才能获得访问权限。还有是否把邮件内嵌图片发动给 AI、是否发送附件内容（不是发送原文件）给 AI 等设置。这形成了一条按次授权的边界：用户决定某一封具体邮件何时可以提供给 AI 助手。

权限与隐私

只在你主动发起时发送，没有后台调用。

邮件访问权限

☐ 不允许 AI 读取任何邮件

☒ 仅当前邮件，每次由我带上（推荐）

☐ 允许 AI 检索邮箱
每次最多检索 4 次、读 24 封，侧栏可核查。

☒ 允许 AI 访问和操作日历与任务
提取待办、创建日程，可一键撤销。

☐ 把邮件内嵌图片发送给 AI
需要视觉模型，最多 4 张。

☐ 发送附件内容
Word、PDF 等附件在本地提取成文字随信，不上传原文件。

☐ 允许发送 S/MIME 加密邮件的解密明文
解密后的明文会离开本机，请谨慎。

对于更加复杂的任务，用户可以允许 AI 助手搜索邮箱。在这种模式下，助手可以在必要时检索历史邮件，同时 App 会在侧边栏的审计卡片中记录搜索和读取活动。因此，用户可以查看助手做过什么，而不是把 AI 的访问当成一个不可见的后台过程。

零信 AI 邮 App 还把访问加密邮件作为一个独立的用户决定。用户可以设置是否允许将加密邮件提供给 AI 助手。这一点很重要，因为加密邮件代表着用户已经通过密码学控制主动保护的信息。因此，对这些内容的 AI 访问应该由用户明确决定，而不是在启用 AI 功能之后自动获得。

AI 助手还可以处理日历和任务，包括从邮件中提取行动事项，并创建日历事件或提醒。助手创建的操作可以通过一次操作撤销。因此，自动化与可逆性是配套的：助手可以完成有用的工作，但用户始终保留查看和撤销这些工作的能力。

六、我的客户端，我做主

上面的例子涵盖了最重要的用户自主决定，但这一原则并不局限于证书、身份、密钥和 AI。零信 AI 邮 App 是一个完整的电子邮件客户端，覆盖邮件、日历、任务、笔记、联系人和 AI 助手，同时提供 S/MIME 证书自动化和密码学邮件操作。

用户可以选择使用哪一家 CA 的证书、使用哪一种算法、哪张证书作为默认证书、信任哪些 CA 根证书、发送时展示哪一种身份等级、连接哪一家 AI 服务商，以及授予 AI 助手什么级别的访问权限。甚至体验 App 本身的一些元素，例如外观和背景颜色，也可以进行自定义。这些设置看起来似乎与密码学没有直接关系，但它们共同体现了同一个产品理念：客户端应该适应用户，而不是在用户不知情的情况下替用户做出具有重要结果的决定。

在软件越来越多地融合云服务、密码学和 AI 的时代，这一点尤其重要。便利性往往来自从界面中移除决策，但安全和隐私有时恰恰依赖于让正确的决定保持可见。零信 AI 邮 App 的做法，是把重复性或技术复杂的操作自动化，同时把具有重要结果的选择留给拥有账户、数据、身份和密码学控制权的人。

零信 AI 邮 App 的用户自主模型可以概括为一个简单的区别：自动化应该减少工作，而不是减少所有权。用户自主决定何时启动证书自动化，选择使用哪些算法和证书，决定接受哪些信任锚点，决定展示哪一种身份，决定加密密钥如何备份和恢复，选择连接哪一家 AI 服务商，并决定 AI 助手可以访问哪些邮件数据。零信 AI 邮 App 提供让这些选择真正可行所需的工具和自动化能力，同时把这些底层决定留在用户手中。

在 AI 时代，这一区别变得越来越重要。最有用的软件并不一定要替用户做出所有决定。它可以自动完成日常工作，同时让用户始终知情、保持控制，并能够改变或撤销重要决定。这就是“我的客户端，我做主”。

王高华

2026 年 9 月 21 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 291 篇(共 86 万 8 千多字)和英文 133 篇(18 万 6 千多单词)。



