零信 AI 邮探秘之五：隐私保护

零信 AI 邮如何保护用户隐私

2026 年 9 月 20 日

隐私保护不应当是产品设计完成之后再添加的一项功能。对于零信 AI 邮而言，隐私保护正是这一平台诞生的原因之一。从一开始，公司的品牌名称零信（ZoTrus）源于“零信任”（Zero Trust），这也体现了零信 AI 邮将隐私保护视为基本安全边界的长期承诺，而不仅仅是隐私政策文件中的一项声明。

电子邮件已经成为日常生活、教育和商业活动不可或缺的基础设施，但其中也承载着身份信息、账单、合同、财务记录、机密讨论，以及个人和职业关系等大量敏感内容。因此，保护隐私不能只是在邮件传输过程中保障通信安全，还需要通过系统架构限制不必要的数据收集，让密码学控制权掌握在适当的主体手中，并在提供自动化便利的同时，避免将便利转化为集中式托管。

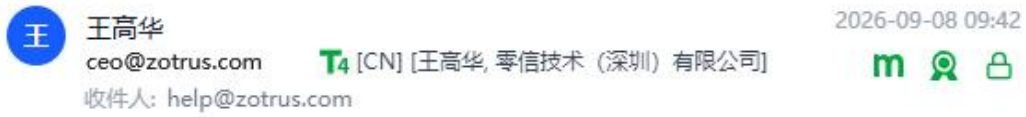
本文并不重复讲解零信 AI 邮的隐私保护条款，而是解释零信 AI 邮希望通过哪些架构设计和运营层面的决策，在实际运作中如何保护用户隐私。

一、让加密在用户端自动完成

传统上，各种通过电子邮件交换的信息都以可读内容的形式存储在邮件服务器上。TLS 传输加密技术只能保护邮件在电子邮件系统之间传输时的连接安全，但它本身并不能确保邮件抵达邮件服务器、备份系统或其他存储环境之后仍然保持加密状态。邮件以明文保存，任何不当获得相关邮箱或服务器访问权限的人或机器，都可读取其中的内容。

隐私问题并不止于邮件内容。对于许多邮件服务而言，机器读取用户邮件并展示定向广告已经成为重要的盈利模式；与此同时，越来越多的邮件数据和用户交互行为被用于人工智能训练，也带来了另一个重要问题：邮件服务提供商究竟应当能够访问、保留或重复利用多少用户的私人邮件信息？

零信 AI 邮的创建正是为了弥补这一空白，让 S/MIME 加密能够在用户端以实用、自动化的方式运行。其目标不是要求用户为每一封敏感邮件记住一套手动加密流程，而是将数字签名、加密、解密、证书处理和验证融入正常的邮件工作流程。



用户的邮件通过适当的公钥得到加密，生成的加密邮件以密文形式保留在用户的邮件服务器中。零信 AI 邮 不需要为了提供自动化加密而保留用户邮件的可读副本，加密由零信 AI 邮在用户本地设备自动化完成。自动化之所以重要，是因为如果加密保护完全依赖用户的手动操作和自律，其实际执行就很难保持一致。通过将 S/MIME 操作融入日常邮件体验，零信 AI 邮可以减少操作失误，同时保留用户对密钥的本地控制权。并且邮件以密态保存在用户的邮件服务器中，有效地阻止了除用户外的其他方阅读邮件隐私信息的可能。

二、有意不提供公钥交换服务

在早期阶段，零信 AI 邮曾将公钥交换视为推动电子邮件加密广泛应用的主要障碍之一。在传统的 S/MIME 工作流程中，发送方需要先取得收件方的公钥证书，才能发送加密邮件。这似乎意味着，系统需要一个证书目录服务，在邮件发送之前查询收件方的公钥证书。

然而，进一步评估发现，集中式公钥查询服务可能暴露有关通信关系的敏感元数据。一个记录“哪个发送方正在查询哪个收件方证书”的服务，可能推断出谁准备与谁通信、哪些组织彼此存在联系，或者用户在某一天正在联系哪些收件人。即使没有邮件正文，这些关系数据本身也可能属于隐私信息。

基于这一重要原因，零信 AI 邮决定不提供集中式公钥交换服务。这是一项面向隐私保护的架构决策：当技术问题可以通过普通的电子邮件交互解决时，就没有必要再建立一个能够观察用户通信行为的集中观察点。

实际上，这一所谓的“障碍”并不像最初看起来那样绝对。当用户发送一封经过数字签名的 S/MIME 邮件时，发送方的公钥证书可以随邮件一同发送。收件方收到签名邮件后，邮件客户端便可以提取该公钥证书并将其保存在本地。当收件方之后需要回复加密邮件时，就可以使用本地已有的证书，而不必事先通过第三方目录进行查询。

双方本来就要通过电子邮件进行正常通信的，通过签名邮件携带后续加密通信所需的公钥，使公钥交换成为正常通信的一部分，而不需要零信 AI 邮运营一个能够观察用户发信行为的公钥查询服务。

三、不托管私钥，但提供自动化密钥管理

用户的密码学密钥是与加密邮件相关的最敏感资产之一。私钥使用户能够解密受保护的通信，并继续访问历史加密邮件。无论谁控制了私钥，都可能实际获得访问原本应由加密保护的信息的能力。

因此，零信 AI 邮并不将自己定位为密钥托管服务商，不会为了实现邮件加密自动化而接管用户的密钥。零信 AI 邮的云服务可以提供证书自动化和可信 CA 连接，而不需要保留用户私钥，更不需要成为掌握用户解密权限的一方。

与此同时，如果撒手不管密码管理这个难题，让用户自行处理所有私钥备份、导出、迁移和恢复任务，这也是不负责任的方案。手动密钥管理很容易出错，尤其是在用户更换设备、重新安装操作系统、迁移邮件客户端，或者需要打开多年前加密的邮件时。

零信 AI 邮的解决方案是提供自动化密钥管理功能，但不将这些功能转化为密钥托管。相关证书和私钥材料被打包成加密备份档案，并自动存储在用户自己的邮箱中，而不是上传到零信 AI 邮的云端。邮箱负责提供存储和同步能力，而备份本身始终保持加密状态。

用户仍然需要负责保护用于解密备份档案的恢复密钥。零信 AI 邮会自动完成备份的创建、更新、存储和获取，但不会接管能够授予受保护材料访问权限的秘密信息的所有权。

四、不集中备份通讯录，但支持用户控制的自动同步

通讯录并不只是便利性数据，它可能揭示客户、供应商、同事、家庭成员、合作伙伴、职业关系以及组织结构。日历可以暴露会议、出行计划、项目安排和敏感的商业活动。邮件分类规则也可能透露用户如何对通信进行分类和排序。

许多互联网服务会因为集中式存储更便于多设备访问，而自动将用户的通讯录同步到服务商的云端。这种便利确实存在，但这种模式也可能在用户直接控制范围之外，持续收集个人关系数据。

零信 AI 邮不提供这种集中式通讯录备份服务，不同步用户通讯录到零信 AI 邮的云端。但如果不为用户提供邮件通讯录的自动同步服务也是不现实的，用户如果已经在一台设备上认真整理了联系人、日历和邮件分类规则，就不应当每换一台设备都重新完成这些工作。

因此，零信 AI 邮对通讯录、证书和私钥材料采用相同的、面向隐私保护的备份模式。通讯录、日历和邮件分类规则都被纳入自动化备份包，统一存储在用户自己的邮箱中，而不是存储在零信 AI 邮的云端。用户邮箱成为了用户控制的备份数据同步通道。

这个创新方案在隐私保护与可用性之间取得了最佳平衡。服务提供商不会拥有用户通讯录和关系图谱的独立云端副本，而用户仍然可以把通讯录迁移到另一台设备，并恢复自己的工作环境。自动化减少了重复劳动，同时不会在用户不知情的情况下扩大服务平台持有的个人信息规模。

五、将身份认证交由专业服务商处理

零信 AI 邮的收费服务，包括可信身份版和全球生态版，都依赖身份认证。这些服务可能需要关于个人、组织，或二者之间关系的经过认证的信息，以便让 S/MIME 证书能表达适当程度的可信身份。

身份认证是一项专业服务，涉及运营、监管、安全和数据保护等多方面要求。零信 AI 邮不打算自己建立一个广泛的身份认证业务，也不会直接收集大量身份凭证材料，而是遵循数据最小化原则，将身份认证过程交由专业服务商完成。

在这种模式下，专业身份认证服务商负责执行相应的身份核查，例如为 IV 认证需要进行个人身份鉴证。具体采用哪一家或哪几家服务商，可能因市场和服务安排而有所不同。零信 AI 邮已经针对全球客户评估适合的专业化多服务商方案。

零信 AI 邮不会因为用户需要完成身份认证，就保留不必要的身份核验材料或原始个人身份数据，例如身份证件号码。相反，零信 AI 邮只处理生成身份证书和提供相关服务所必需的身份信息，例如需要出现在身份证书中的经过验证的个人姓名和组织名称。

这种职责分离减少了零信 AI 邮自身需要收集和保留的敏感身份凭证材料，专业服务商负责身份认证，而零信 AI 邮则使用由此产生的、经过验证的身份属性，为邮件证书和可信身份体验提供相应支持。

六、隐私保护是一项架构承诺

本文所描述的隐私模型并不依赖某一项单独的功能，而是多项设计决策共同作用的结果：让 S/MIME 加密在用户端自动完成；避免运营可能暴露通信关系的集中式公钥交换服务；不接管用户私钥；在自动完成加密备份的同时，将恢复权限留给用户；避免在云端备份用户的通讯录及相关个人数据的副本；并在身份认证过程中使用专业服务商，同时对需要保留的信息实施数据最小化原则。

这些选择体现了自动化与所有权之间一贯而明确的区别。零信 AI 邮希望自动完成让 S/MIME 电子邮件变得实用所需的工作，但自动化不应当要求服务平台收集一切、观察一切，或控制每一个秘密。系统可以提供同步能力，而不必成为用户通讯录关系图谱的所有者；可以提供证书服务，而不必持有私钥；可以支持经过认证的身份，而不必保留身份认证过程中使用的每一份身份证明材料。

由此可见，对零信 AI 邮而言，隐私保护并不局限于帮助用户防止邮件内容被未经授权地访问。它还意味着减少不必要的数据收集，避免不必要的元数据暴露，保留用户对密钥的绝对

控制，并以这样的方式设计云端服务，使便利性不会自动演变为集中式托管。

下一代电子邮件安全将结合密码学、自动化与用户体验，让信任成为默认，并在整个邮件通信生命周期中得到验证。这正是零信 AI 邮致力推进的方向：让隐私属于个人或组织，并得到切实保护。

王高华

2026 年 9 月 20 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 290 篇(共 86 万 1 千多字)和英文 132 篇(18 万 4 千多单词)。