

零信 AI 邮探秘之十：生态建设

安全 + 密码：构建全球密码应用生态

2026 年 9 月 28 日

一个安全的数字世界并不是由某一个安全产品或某一种密码技术构建的，而是由身份、信任、密码技术、应用、基础设施和标准在用户已经使用的工作流程中协同工作而构建的。电子邮件是最典型的例子之一，但同样的原则也适用于聊天和文档。人们通过电子邮件和即时通讯（聊天）进行沟通，通过这些对话交换文档和签署文档，并希望由此产生的身份、签名、加密和验签能力能够在不同的应用和组织之间持续保持可信和互通兼容。

这也给整个行业提出了一个更广泛的问题：如果电子邮件、聊天和文档领域已经存在成熟的密码学技术，为什么这些能力仍然经常被孤立在不同的产品、平台和工作流程中？当前的挑战已经不再只是密码技术是否可用，而是如何让密码应用在全球数字生态中实现互操作、自动化，并真正具备实用性。

一、密码应用是一个生态问题

安全与密码通常被作为产品能力来呈现：部署安全网关、配置证书、启用加密、部署签名服务，或者增加一个加密聊天平台。然而，在真实的大规模应用环境中，数字信任并不局限于某一个应用。电子邮件涉及邮件平台、安全系统、证书颁发机构、客户端、身份和信任关系；聊天涉及用户、组织、消息应用、身份系统和通信基础设施；文档则会在电子邮件、聊天、业务系统、签名服务、存储系统以及可能使用完全不同应用的接收者之间流转。

S/MIME 已经为电子邮件提供了成熟的密码学模型：证书可以将身份与公钥绑定，数字签名可以提供完整性和签名者身份，加密则可以保护邮件内容。数字签名和加密同样为文档提供密码学基础，而安全即时通讯则可以直接对对话应用密码学保护。因此，挑战已经不再主要是技术是否存在，而是如何让这些能力在承载全球数字通信的现有基础设施和工作流程中真正发挥作用。

因此，密码应用自动化本质上是一个生态问题，而不仅仅是一个产品问题。真正需要解决的并不是应该替换哪个现有系统，而是如何让密码能力成为现有系统和工作流程中可靠的一部分，使信任、安全、通信、签名、加密和验签能够作为一个协调一致的过程运行。

二、每个参与者都已经擅长自己的领域

现有的数字生态中已经存在许多成熟的专业参与者，他们经过多年发展，分别在整个工作流程的某一环节形成了自己的能力。电子邮件平台负责邮件的传输和存储；聊天平台提供实时通信；安全厂商负责内容检测与保护；证书颁发机构在自身信任体系内验证身份并签发数字证书；文档平台提供文档签署和文档管理功能；邮件和聊天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。

密码应用要变得更容易部署，并不意味着这些角色需要消失。安全厂商不需要变成证书颁发机构，证书颁发机构也不需要变成电子邮件或聊天平台，文档服务也不需要因为密码学信任的重要性提高，就重新构建完整的身份基础设施。组织也不应该仅仅为了引入自动化密码能力，就必须替换现有的通信和安全基础设施。

真正缺少的是这些现有能力与日常应用之间的运行连接：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，并使这些能力能够直接进入用户已经用于沟通、交换文档和开展业务的工作流程的机制。

三、邮件安全急需密码应用自动化

邮件安全面临的问题已经无法仅通过加强安全防护手段来解决，需要一个专门的密码应用层来保障邮件安全。它的职责不是成为邮件服务器、聊天平台、文档管理系统、反恶意软件引擎、DLP 平台或 AI 模型，而是让密码学能够在这些现有工作流程中真正可用，并将密码学操作与数字通信已经运行于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、数字签名、签名验证、加密、解密、身份展示、时间戳以及证书生命周期管理。更深层的价值在于协调这些功能，使它们不再只是彼此孤立的管理任务。当密码学操作实现自动化并与应用工作流程连接后，信任就可以成为日常通信和文档处理的一部分，而不再是用户和管理员必须单独管理的一个项目。

数字证书已经存在。安全体系已经存在。消息应用已经存在。文档也已经存在。缺少的是让这些能力协同工作的自动化机制。单独拥有一张证书，并不能自动将可用的密码身份放入应用、保护相关密钥、为签名操作选择正确的证书、为指定接收者加密内容，或者管理随后的生命周期。

四、安全 + 密码学：两种能力，一个工作流程

安全系统和密码学解决的是信任问题中的不同部分。安全系统负责发现威胁、检查内容、执行策略并响应可疑活动，而密码学提供可验证身份、完整性、机密性和可信签名等机制。如

果将两者视为相互竞争的层，就会产生一个没有必要的架构选择；实际上，它们完全可以在同一个工作流程中协同运行。

对于电子邮件而言，密码应用网关可以与现有的邮件安全网关协同工作，使每个系统都承担其最擅长的任务。收到加密邮件后，可以在适当的组织控制下进行解密，再交由现有安全体系检查，最后按照策略投递。发出的邮件则可以先经过安全检查，再进行数字签名，并在需要时为收件人加密。

同样的原则也适用于文档。业务系统生成的文档可以根据身份和策略进行签名和加密，然后返回业务工作流程。在电子邮件对话中，PDF 附件可以直接进行数字签名、添加时间戳、为一个或多个接收者加密并发送，而不需要创建一个独立的文档签署工作流程。密码学操作因此成为现有工作流程的一部分，而不是另一个孤立的目的地。

聊天则以另一种形式提出了同样的架构问题。如果参与者需要知道自己正在与谁通信，并且敏感消息需要端到端密码保护，那么一段对话所需要的不只是传输安全。密码应用层可以将可信身份、密钥管理和消息加密连接到聊天体验，同时让聊天平台本身继续专注于通信。

目标并不是为了检查而让安全系统看到更少的内容，也不是为了检查而削弱密码保护，而是让安全控制与密码保护作为同一应用基础设施中相互协调的组成部分共同工作。

五、一个密码学基础，三种应用形态

当我们从跨应用而不是单一产品类别的角度来看待这个问题时，一个共同的基础就会显现出来。邮件、聊天和文档是不同的数字应用形态，但它们需要许多相同的底层密码能力：可信身份、证书、密钥、签名、加密、解密、验签以及证书生命周期管理自动化。

因此，零信技术并不把邮件、聊天和文档看作三个彼此无关的应用，而是将它们视为建立在共同密码学基础和统一的密码应用自动化能力层之上的三种服务形态。零信 AI 邮将密码应用自动化带入电子邮件；零信聊将可信身份和加密通信延伸到聊天场景；零信签则将同一基础设施延伸到数字文档签名、加密、验签和时间戳。

这种模式的优势并不仅仅是技术复用。共同的技术基础可以使身份和密码能力在用户的通信从一种应用场景转移到另一种应用场景时保持一致。一封电子邮件可以建立可信身份；一段聊天可以使用这一身份进行可信通信；通过其中任何一种工作流程交换的文档，都可以使用基于证书的密码操作进行签名和加密。应用各不相同，但其信任和密码学基础可以保持协调一致。

六、电子邮件对话可以成为文档签署环境

文档签署尤其清楚地说明了为什么应用工作流程如此重要。在现有的电子文档签署服务中，文档需要被转移到一个专用电子签名平台：用户上传文档、创建签署事务、邀请参与者、完成签署，然后再将签署后的文档返回原来的邮件工作流程。这种模式可以发挥作用，但它会在文档原本出现的通信对话之外，再建立一套独立的文档工作流程。

零信签采用了不同的方法，将数字签名融入电子邮件工作流程。当文档已经作为电子邮件附件存在时，用户可以直接在电子邮件环境中使用可信身份数字证书进行签名。签署后的文档可以继续保留在同一对话中，根据需要为指定接收者加密，并可以在之后对生成的文档进行验证。

零信 AI 邮同时将密码学签署操作与不必要的文档传输分离开来。在云签名模式下，原始文档继续留在用户设备上，由零信 AI 邮 App 在本地生成密码学哈希值，并仅将哈希值发送到云签名服务。云签名服务使用其可信签名证书对该哈希值进行签名并返回签名数据，由零信 AI 邮 App 在本地完成签名过程。在这种模式下，云签名并不要求原始机密文档离开用户设备。

这体现了一个更广泛的原则：密码应用自动化应该跟随文档及其通信工作流程，而不是仅仅因为需要执行一次密码学操作，就迫使用户离开原有工作流程。

七、行业中缺少的角色：密码应用自动化提供商

当我们将这个问题视为一个生态问题时，一个独特的行业角色就会显现出来：密码应用自动化提供商（Cryptographic Application Automation Provider，简称 CAAP）。这一角色之所以存在，是因为行业中已经拥有证书颁发机构、安全厂商、电子邮件和聊天平台、文档服务、客户端以及密码学技术，但仅仅因为这些组件各自存在，并不会自动形成一个完整的运行工作流程。

证书颁发机构提供证书和信任；安全厂商提供检测、检查和策略执行；电子邮件和聊天服务商提供通信基础设施；文档平台提供文档工作流程；客户端提供用户进行通信和工作的界面。缺少的角色，是将这些能力连接起来，并自动化密码应用的服务提供商，使基于证书的信任和密码学功能能够直接参与日常应用。

CAAP 可以连接证书服务、信任、密钥、密码学操作、应用基础设施和安全工作流程，使每个参与者都可以继续发挥自己的专长，而不需要所有参与者重复开发一套相互重叠的能力。它是一种具有明确架构目的的集成与自动化角色，而不是又一次试图整合整个安全或通信技术栈。

原则很简单：每个相关的参与者做好自己最擅长的事情。CAAP 让这些组成部分能够协同工作，使整个生态能够提供任何单一参与者都难以高效独立提供的密码能力。

八、标准让生态实现互操作

一个生态系统需要的不只是单独的能力，还需要共同的技术规则，让独立开发的组件能够彼此协同工作。因为如果没有共同标准，每一个连接都会变成一次专有集成，都必须单独进行设计、实施和维护。

IETF 发布的 RFC8823 将 ACME (RFC 8555) 扩展到终端用户 S/MIME 证书。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，它为电子邮件应用参与自动化 S/MIME 证书工作流程提供了一条标准化路径，而不是将证书申请完全作为一个独立的人工处理流程。

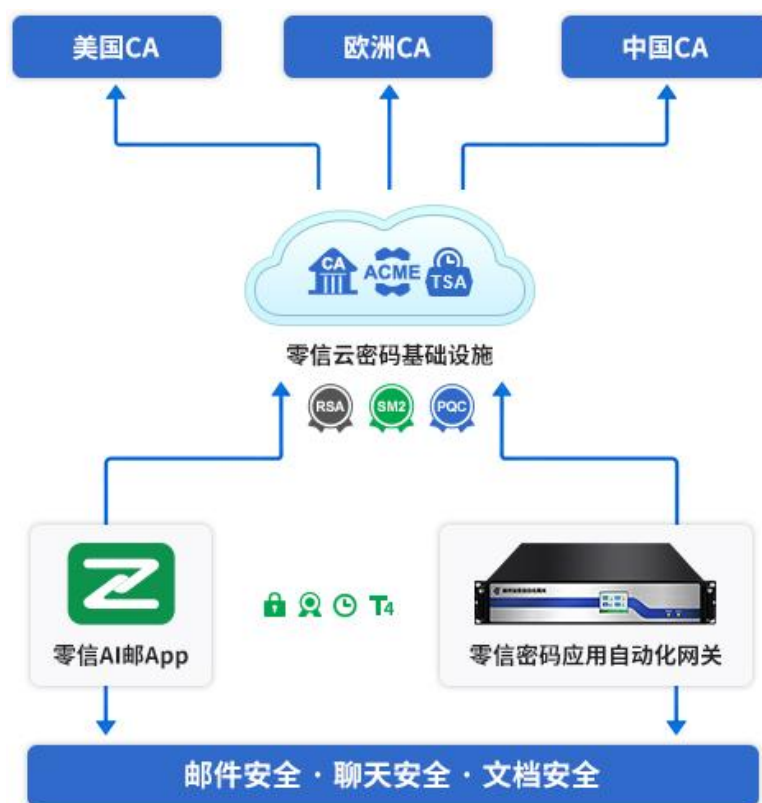
标准的意义并不止于电子邮件。在任何可信身份、证书、签名、加密和验证需要跨越应用边界的场景中，同样的生态原则都成立。云签名、文档验证、基于证书的身份以及安全消息通信，都可以从标准中受益，使不同提供商能够实现兼容的组件，而不必形成一个封闭的专有信任孤岛。

这就是标准对于全球密码应用生态的重要意义。依靠专有接口，行业可以生产功能强大的产品，却仍然难以高效地将它们连接起来。而通过开放标准，不同厂商可以实现兼容组件，围绕共同的技术基础构建集成，并让生态能够超越单一产品或单一提供商不断扩展。

标准定义路径，自动化让这条路径真正可用。

九、零信 AI 邮：打造可运行的密码应用自动化生态

零信 AI 邮将自身定位为密码应用自动化提供商，其架构展示了当密码能力跨越多种应用形态并实现连接时，这一模式可以呈现出怎样的形态。零信 AI 邮 App 将 S/MIME 自动化带入电子邮件工作流程；零信聊将可信身份和加密通信延伸到聊天；零信签将数字签名、加密、验签和时间戳带入文档工作流程；零信密码应用自动化网关则将密码应用自动化延伸到组织基础设施和业务系统。



重要的并不是零信 AI 邮必须拥有每一个组件，而是完整的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基础设施中进行管理；电子邮件可以进行签名和加密；聊天消息可以通过可信身份和加密得到保护；文档可以进行数字签名、附署时间戳、加密和验签；这些能力可以参与正常的应用工作流程，而不是停留在彼此分离的管理流程中。

从这个意义上说，零信 AI 邮并不是要成为另一个电子邮件平台、另一个聊天平台、另一个文档签署平台、另一套安全技术栈，或者另一个 CA。它正在实现密码应用自动化提供商这一角色，并通过标准展示如何将现有能力连接起来，使整个行业看到的不是一组孤立的技术，而是一种密码应用能够彼此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，是因为当存在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身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，而是让更多参与者更容易加入生态。

十、从一个可运行的实践走向全球密码应用生态

一个成功的生态不应该依赖某一家厂商。零信 AI 邮的目标不是再建立一个面向电子邮件、聊天或文档安全的专有孤岛，而是建立一个更加开放的模式，让更多参与者能够实施、集成和

扩展。

其他密码应用自动化提供商可以提供自己的实现和服务；电子邮件客户端可以增加自动化 S/MIME 支持；聊天平台可以集成可信身份和基于标准的加密；文档和业务平台可以集成数字签名、加密、时间戳和验签；证书颁发机构可以提供证书和信任服务，并具备自动化证书管理能力；安全厂商则可以将密码工作流程与现有的检查和策略能力结合起来。

因此，生态可以通过专业化分工而不是整合来发展。一家公司可以提供身份和信任，另一家公司提供安全检查，另一家公司提供通信基础设施，另一家公司提供文档服务，还有另一家公司提供密码应用自动化。真正的价值来自让这些能力实现互操作并能够协同运行。



零信 AI 邮的目标是构建一个全球密码应用生态，在这个生态中，邮件、聊天和文档不再是彼此孤立的应用孤岛。可信身份可以在需要的地方使用；密码学密钥可以保持在适当的控制之下；签名可以证明是谁签署的；加密可以控制谁能够阅读；时间戳可以证明签名何时存在；验签则可以在数字信息的整个生命周期中持续进行。

十一、安全 + 密码学：面向互联的可信数字世界

未来的数字信任不会通过在安全与密码学之间二选一来实现，也不会通过要求每一个应用都成为密码应用平台来实现。它将通过连接现有能力，并自动化那些在日常工作流程中仍然过

于复杂的密码学操作来实现。

邮件、聊天和文档代表了数字通信和业务活动中的三种重要形态。它们各自拥有不同的用户体验和基础设施，但都可以从相同的密码底层原则中受益，包括可信身份、密码保护和自动化证书生命周期管理。密码应用自动化的作用，就是让这些原则变得真正可用，而不要求每一家应用提供商、安全厂商、证书颁发机构或组织重新构建完整的密码学技术栈。

因此，零信 AI 邮的目标显然不只是邮件安全。电子邮件是起点，因为 S/MIME 已经提供了成熟的、基于标准的基础。聊天和文档则将同一密码应用模型延伸到其他通信和业务工作流程。下一步，是让这些能力更容易被其他参与者集成，使密码应用能够成为更广泛全球数字基础设施的一部分。

目标不是让零信 AI 邮成为这个生态本身，而是帮助构建一个行业各方能够参与其中、贡献自身专业能力，并将密码学的实际应用范围扩展到邮件、聊天和文档的全球生态。安全提供防护。密码学提供信任。应用自动化将二者连接到人们进行通信、签署、交换和开展数字行动的工作流程中。三者结合，可以将已经成熟的密码学技术转化为面向全球数字世界的实用、可互操作能力。

王高华

2026 年 9 月 28 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 299 篇（共 90 万 3 千多字）和英文 140 篇（共 20 万 2 千多单词）。

