零信技术，打通数字证书与密码应用之间的鸿沟

从证书管理自动化到密码应用自动化

2026 年 11 月 9 日

数字证书已经存在数十年。证书颁发机构（CA）负责签发证书，公钥基础设施（PKI）为数字信任提供基础，RSA、ECC 和 SM2 等密码技术也已得到广泛应用。与此同时，后量子密码技术正在逐步走向实际部署。然而，对于许多个人和组织而言，在日常应用中使用数字证书仍然十分复杂。

拥有证书并不意味着懂得如何使用证书。用户仍可能需要了解申请证书、证书格式、安装证书、配置应用、管理私钥，并手动执行密码应用。组织面临的挑战更大。它们需要管理大量证书，将密码能力集成到现有业务系统中，维护安全基础设施，并持续跟进不断演进的密码标准和合规要求。

问题的根本并不在于缺少数字证书或密码技术，而在于拥有密码资源与在实际应用中有效使用这些资源之间存在鸿沟。数字证书奠定了信任基础。但真正缺失的是这种信任难以便捷、持续地融入日常应用。

一、证书与应用之间的鸿沟究竟在哪里？

证书与应用之间的鸿沟并非由单一技术问题造成，而是涉及多个相互关联的挑战。总结起来，共有四道难以逾越的鸿沟。

1. 证书管理鸿沟

数字证书是一个具有完整的生命周期的产品，包括：

(1) 证书申请与身份认证

(2) 证书签发与部署

(3) 证书续期与更换

(4) 证书吊销

(5) 证书和私钥管理

随着证书有效期不断缩短、证书数量增加以及密码算法的不断演进，人工管理变得越来越困难，效率也越来越低。缺少自动化会使证书管理成为沉重的运维负担。

©2026 零信技术（深圳）有限公司

2. 密码应用鸿沟

即使用户拥有了有效的数字证书，应用也未必能够自动使用这些证书。例如：

(1) 邮件客户端需要进行非常复杂的人工配置，才能对邮件进行数字签名和加密

(2) 文档应用需要集成数字签名、签名验证、加密和解密功能，也需要各种人工配置。

(3) Web 服务需要正确部署和维护证书，才能正确建立 HTTPS 连接。

拥有证书并不意味着就具备了可实际使用的密码能力。

3. 基础设施集成鸿沟

大中型组织通常已经部署了企业 CA、HSM、身份管理系统、安全网关和业务应用。然而，这些系统可能各自独立运行，缺少能够协调证书管理与密码运算的自动化机制。

将密码能力集成到现有业务环境中，可能需要投入大量开发、部署和维护资源。

4. 易用鸿沟

密码技术具有很强的专业性，但普通用户不应该为了享受数字信任带来的好处而必须成为密码专家。用户希望邮件能够自动完成签名和加密，文档能够便捷地进行签名和验证，网站能够自动建立 HTTPS 安全连接，而不必亲自管理证书。

密码技术应该自然融入应用工作流程，而不应成为额外施加给用户的技术任务。

二、零信技术解决方案：从证书管理自动化到密码应用自动化

零信技术正是为解决这一鸿沟而成立。我们的解决思路建立在两项相辅相成的能力之上：

1. 证书管理自动化

证书管理自动化解决的是如何获取、部署、维护和管理数字证书的整个生命周期。它将以下关键证书管理操作实现自动化：

(1) 证书申请与签发流程

(2) 证书部署

(3) 证书续期与更换

(4) 证书生命周期管理

©2026 零信技术（深圳）有限公司

(5) 与现有基础设施集成

RFC 8555 定义的 ACME（自动化证书管理环境）标准是实现证书管理自动化的一项重要标准化机制。但证书管理自动化并不局限于 ACME。不同的应用环境可能需要采用不同的集成方式和管理机制。

2. 密码应用自动化

密码应用自动化解决的是另一个同样重要的问题：如何让应用真正自动使用数字证书和密码能力？它将密码运算集成到实际应用工作流程中，包括：

(1) 数字签名与验签

(2) 加密与解密

(3) 基于证书的身份识别

(4) 密码运算自动化

(5) 与现有应用和业务系统集成

证书管理自动化让证书能够被自动获取和管理；密码应用自动化则让证书真正自动应用于实际业务场景。这两项能力共同构成了零信技术的技术体系基础。

三、零信技术如何在实践中填补鸿沟的

零信技术历时 5 年多真正将证书管理自动化和密码应用自动化路落实到了三个实际应用领域：网站安全、邮件安全（包括基于电子邮件的聊天安全）和文档安全。

1. 网站安全：让 SSL 证书和 HTTPS 自动化

HTTPS 对保护网站与访问者之间的通信至关重要。然而，在多个网站和服务器上部署、维护 SSL 证书，给用户带来很大的运维压力。

零信技术提供 SSL 证书管理自动化和 HTTPS 加密自动化部署能力，以简化这一过程。主要能力包括：

(1) 基于 ACME 的证书自动申请、验证、部署与续期

(2) 支持 RSA、ECC、SM2 传统密码算法和混合 PQC 算法

(3) 双算法 SSL 证书的自动化部署

©2026 零信技术（深圳）有限公司

(4) 支持对接不同的 CA 服务和证书管理环境

(5) 将 HTTPS 加密自动化与网关安全能力相结合

(6) 零信 HTTPS 加密自动化网关内置 WAF 防护

零信 HTTPS 加密自动化网关将 SSL 证书自动化与网关安全防护相结合，帮助组织可以继续保持现有网站设施投资不变而更高效地部署和维护网站安全。**零信技术的目标是让 SSL 证书管理和网站防护成为 Web 基础设施中的自动化环节。**

2. 邮件安全：让邮件证书和 S/MIME 自动化

S/MIME 提供了邮件数字签名和加密的标准化机制。但在实际部署中，仍需要完成繁琐的证书申请、安装、配置和持续管理等工作。对于普通用户而言，这些步骤是普及应用邮件安全技术的最大障碍。对于组织而言，在现有邮件基础设施中管理 S/MIME 书和密码运算，则可能更加复杂。

零信技术通过零信 AI 邮解决这些问题，零信 AI 邮为邮件和聊天提供以下 S/MIME 自动化能力：

(1) S/MIME 证书自动申请及生命周期管理

(2) 对外发邮件自动进行数字签名和加密

(3) 自动验证已签名邮件

(4) 自动解密已加密邮件

(5) 基于证书识别和 UI 展示发件人身份

(6) 支持个人用户、中小企业及企业级应用环境。

零信 AI 邮提供两种实现路径：

(1) 零信邮 App：面向用户的应用软件，让个人和小型组织也能便捷使用 S/MIME 加密和数字签名，无需手动处理复杂的证书操作。

(2) 零信 S/MIME 自动化网关：面向大中型组织的解决方案，通过 SMTP 和 IMAP 代理能力与现有邮件基础设施集成，实现 S/MIME 操作自动化，同时支持证书和身份的集中管理。

通过将证书管理自动化与密码应用自动化相结合，零信 AI 邮让安全邮件通信和加密聊天成为日常邮件工作流程的一部分。**零信技术的目标是让每个人都能实际使用 S/MIME，让邮件安全变得简单、易用且自动化。**

©2026 零信技术（深圳）有限公司

3. 文档安全：让数字签名和加密融入工作流程

数字签名对于确认文档的真实性和完整性至关重要，文档加密也有助于防止敏感信息遭到未授权访问。然而，传统的文档签名和加密流程涉及不同的应用、手动选择证书、复杂配置以及额外的操作步骤。

零信技术将文档证书的自动化管理和基于证书的数字签名和密码操作融入文档工作流程。其能力包括：

(1) 文档证书自动申请及生命周期管理

(2) 对本地文档进行数字签名

(3) 对邮件附件进行数字签名

(4) 数字签名验签和身份展示

(5) 使用证书对文档加密与解密

(6) 自动附署时间戳签名

(7) 支持长期验证（LTV）

(8) 基于国际云签名联盟（CSC）标准的云签服务

零信技术云签服务的一项特色是无需将原始文档上传到云签服务平台，而是由零信邮 App 生成待签名文档的哈希值，并将其提交至云签服务系统进行签名，再返回给零信邮 App 在本地完成文档数字签名。这种方式在实现云端签名的同时，有助于保护文档隐私和商业机密信息。

通过将文档签名融入邮件工作流程，并支持本地文档密码操作，零信技术让数字签名在日常工作中更加便捷易用。**零信技术的目标是让文档签名、加密和验证自然融入文档处理流程。**

四、从个人到组织：密码应用自动化的两种实现路径

不同用户对密码能力的部署有不同需求。个人和小型组织需要配置简单、易于使用的应用。大中型组织则需要集中管理、与现有基础设施集成，并对密码运算进行统一管控。

零信技术通过两种相辅相成的实现路径满足这些需求。

(1) 基于 App 的自动化

对于个人和规模较小的组织，零信邮 App 等应用软件可提供开箱即用的证书管理自动化和密码应用自动化能力。用户无需了解底层的证书管理和密码处理过程，即可执行邮件和文档

©2026 零信技术（深圳）有限公司

密码应用操作。

(2) 基于网关的自动化

对于大中型组织，零信技术网关方案可将证书管理自动化和密码应用自动化能力集成到现有基础设施中。网关无需组织替换现有业务应用和网安设施，而是与现有系统协同工作，实现证书管理和密码应用自动化。

相关产品包括：零信 HTTPS 加密自动化网关、S/MIME 自动化网关、文档密码应用自动化网关、企业密钥管理系统（EKMS）、企业时间戳服务系统、企业即时通讯加密网关等，这种方式使组织能够在保留现有业务流程和基础设施投资的同时，引入密码应用自动化。

两种部署路径各不相同，但目标始终一致：让证书管理和密码应用实现自动化。

五、面向密码技术的持续演进

密码技术仍在持续演进，RSA 和 ECC 为现代数字安全奠定了基础，SM2 则是我国的强制合规应用需求。与此同时，后量子密码技术的发展也对面向未来的密码基础设施提出了新的要求。支持多种算法只是挑战的一部分。随着密码标准和安全要求不断变化，应用和基础设施也必须具备相应的适应能力。

零信技术通过支持多种密码算法，并适应不断变化的应用需求，践行密码敏捷性理念。主要技术方向包括：

(1) 支持 RSA、ECC 和 SM2 密码算法

(2) 支持国际密码标准和国密标准

(3) 面向后量子密码做好准备

(4) 混合密码机制

(5) 具备适应能力的证书管理和密码应用工作流程

密码敏捷不仅仅意味着支持更多算法，更重要的是让实际应用能够管理和适应密码技术的演进。零信技术认为，密码应用自动化是让未来密码技术真正落地并普及应用的关键。

六、零信技术的愿景：让密码技术易用、自动并真正落地

数字世界已经通过数字证书、CA、PKI 和标准化密码技术建立了密码信任的基础。但这些

©2026 零信技术（深圳）有限公司

基础不应只是彼此孤立的技术资源。它们应当能够无缝融入人们日常使用的应用之中。这正是零信技术致力于将证书管理与实际密码应用连接起来的原因。

零信技术的愿景围绕三个原则展开：

(1) 让密码技术触手可及：让普通用户和组织无需具备专业技术知识，零门槛使用专业的密码能力。

(2) 让密码应用自动化：实现证书管理和密码应用自动化，让数字签名、加密、解密和验签自然融入应用工作流程。

(3) 让数字信任清晰可见和可操作：帮助用户和系统识别可信身份、验证数字签名，并了解通信和文档背后的安全保护。

数字证书是基础，自动化让证书真正发挥作用，应用则让数字信任成为现实。**零信技术，以密码技术构建信任，以自动化实现安全，以人工智能提升效率**。零信技术致力于让每个人都能使用密码应用自动化，填补数字证书与依赖证书的应用之间的鸿沟。

王高华

2026 年 11 月 9 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 301 篇（共 91 万 3 千多字）和英文 142 篇（20 万 6 千多单词）。

©2026 零信技术（深圳）有限公司