2026，乘势而上，赢战市场

2026 年 1 月 4 日

2026 年注定是一个不平凡的一年，因为 3 月 15 日将正式终结已经持续了 **32** 年之久的以年为 SSL 证书签发周期的历史，改为 200 天签发周期，并于 2029 年 3 月 15 日改为 47 天，这是 2026 年全球互联网安全的大事之一，笔者为此定义 2026 年为“**HTTPS 加密自动化元年**”。

第二件大事是：3 月 1 日起，代码签名证书有效期缩短为一年零 3 个月(450 天)，这将正式终结已经持续了 **30** 年之久的可以签发多年有效期代码签名证书的历史，这是 2026 年全球软件安全的大事之一，笔者为此定义 2026 年为“**代码签名自动化元年**”。

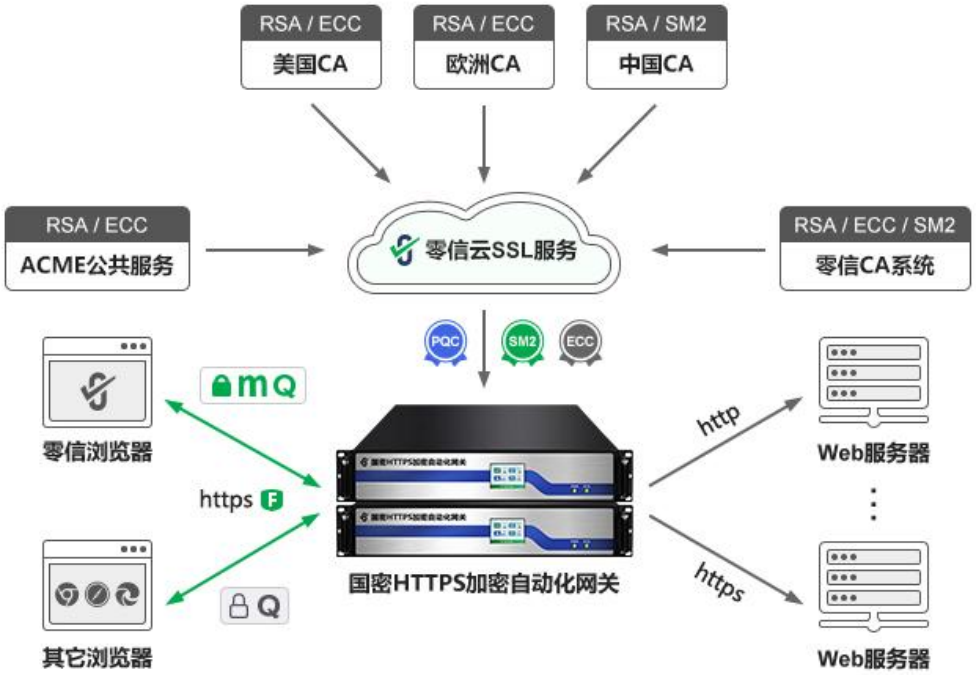
这两件大事意味着什么？意味着必须实现数字证书应用自动化。零信技术从 2021 年成立那天开始布局证书应用自动化，历时 4 年于 2025 年 12 月完美完成同时支持商用密码和后量子密码的 HTTPS 加密自动化管理解决方案，以迎接 2026 年 HTTPS 加密自动化元年的到来。零信技术 2026 年的战略目标是乘势而上，赢得 HTTPS 加密自动化市场和代码签名自动化市场。

一、 网站安全解决方案已完成全部研发，2026 年赢战市场

零信技术网站安全解决方案就是 HTTPS 加密自动化解决方案，HTTPS 加密确保了浏览器/APP、网站、API 和服务之间的安全通信，SSL 证书是实现 HTTPS 加密的核心组件。当笔者还在忙于 CA 运营时，其核心业务当然是销售 SSL 证书。但是，成立零信技术时，笔者已经认识到用户需要的是实现 HTTPS 加密，而不是 SSL 证书，同时认识到 SSL 证书自动化已经成为不可阻挡的发展趋势，因为万物互联都需要实现 HTTPS 加密，人工申请和部署 SSL 证书是不可能实现安全的万物互联。笔者从 SSL 证书自动化管理的发起者-Let’s Encrypt 的成长过程明确看到了 SSL 证书自动化的威力，Let’s Encrypt (让我们加密)这个名字本身就已经点题—用户需要 HTTPS 加密，而不是 SSL 证书！需要的是自动化实现 HTTPS 加密，而不是自动化管理 SSL 证书。

零信技术 HTTPS 加密自动化解决方案是一个满足我国特殊需求的双算法 SSL 证书自动化管理解决方案，是一个集商密 HTTPS 加密改造、SSL 证书自动化改造、后量子密码迁移于一体的创新解决方案，帮助用户一次微改造同时完成三个必须的技术改造。这是一个端云一体的解决方案，有两个必须的“端”：一是零信浏览器，这是一个同时支持商密算法和后量子密码算法的 HTTPS 加密客户端，完全免费，干净无广告，市场上已有的浏览器满足不了我国用户的

三个必须的技术改造需求。另一个“端”是零信 HTTPS 加密自动化网关，这是一个同时支持商密算法和后量子密码算法的、支持双算法 SSL 证书自动化管理的专用于 HTTPS 加密的新型网关，市场上已有的网关产品满足不了我国用户的三个必须的技术改造需求。而要想实现 SSL 证书自动化管理，还必须有零信云 SSL 服务系统，这是为零信 HTTPS 加密自动化网关提供双算法 SSL 证书签发服务的服务端，市场上已有的证书自动化服务端满足不了我国用户的三个必须的技术改造需求。国际上的自动化证书管理服务端只能提供国际算法 SSL 证书，也只能提供单一签发 CA 的证书自动化签发服务，我国不仅需要国际算法 SSL 证书同时更需要国密算法 SSL 证书，还同时需要支持多 CA 签发通道，这不仅是为了应对非常不确定的国际环境，而且也是为了为用户可靠提供 SSL 证书，因为单 CA 签发不能保证 SSL 证书的可靠供应。



这就是零信技术历时 4 年鼎力打造的 HTTPS 加密自动化解决方案，全球独一无二的完美解决我国商密 HTTPS 加密改造、证书自动化改造和后量子密码迁移难题的创新解决方案，这是一个自家生态拥有 HTTPS 加密所需的全套产品，包括上图没有列出的国密证书透明日志系统。全球独家率先同时支持两个混合 PQC 算法(SM2MLKEM768 和 X25519MLKEM768)和三个传统密码算法(SM2、RSA 和 ECC)，零信浏览器和零信 HTTPS 加密自动化网关优先采用 SM2MLKEM768 算法实现 HTTPS 加密，同时满足我国用户的商密合规改造和后量子密码迁移需求。

2026 年 3 月 15 日全球正式进入 SSL 证书自动化时代，零信技术已具备大规模实施 SSL 证书自动化改造和后量子密码迁移的生产能力、部署能力和服务能力。不仅可以为关键基础设

施运营单位快速提供 HTTPS 加密自动化网关产品，而且预计一月份为中小企业用户和个人用户上线完全免费的证书自动化服务，类似 Let's Encrypt 证书自动化服务，不同的是自动化签发 SM2+ECC 算法双证书，国密 SSL 证书所有国密浏览器信任，国际 SSL 证书所有浏览器信任，并完全开源 ACME 客户端软件，满足中小企业和个人用户单个或少量网站的证书自动化应用需求。

零信证书自动化(ACME)服务的免费版不限制网站数量和证书申请量，双算法(ECC+SM2) DV SSL 证书完全免费。对于需要 OV/EV SSL 证书自动化管理的用户，可选择专业版和增强版服务，双证书(国密 OV+国际 DV)低至每年 800 元，双证书(国密 EV+国际 DV)低至每年 1000 元。可选国际 OV/EV SSL 证书。

二、 应用安全、邮件安全、文档安全解决方案，2026 年全部交付

零信技术在完成了网站安全解决方案后就把研发力量转移到应用安全、邮件安全和文档安全解决方案的研发上，一样的理念—密码应用自动化，自动化实现代码签名、自动化实现邮件加密、自动化实现文档签名。

应用安全解决方案—代码签名云服务预计一月份上线，国内率先独家为软件开发者提供国内本地代码签名云签服务，云签服务所需的代码签名证书由微软 Windows 硬件合作伙伴中心指定的 6 家 CA 之两家甄选 CA-**Sectigo** 和 **SSL.com** 签发。同国外 CA 提供的代码云签服务最大的不同的是：不按签名代码数量收费，固定年费，不限制代码签名数量。当然，用户仍然可选购传统 USB Key 硬证书，但不同的是采用国产 USB Key，证书签发后用户无需等待 10 天从美国快递 USB Key，而是直接从深圳顺丰快递 24 小时内送达。

邮件安全解决方案—邮件加密服务预计第三季度上线，这是零信浏览器内置邮件客户端的解决方案，已经研发 3 年，在完成了网站安全和应用安全解决方案后将集中研发力量第二季度完成内测，第三季度全球开放。这是全球唯一免费自动化配置双算法电子邮件证书，自动化实现电子邮件加密、数字签名和时间戳的邮件安全解决方案，基础版完全免费，专业版提供邮件发送者可信身份认证服务，证明每一封邮件的可信身份，增强在线信任。

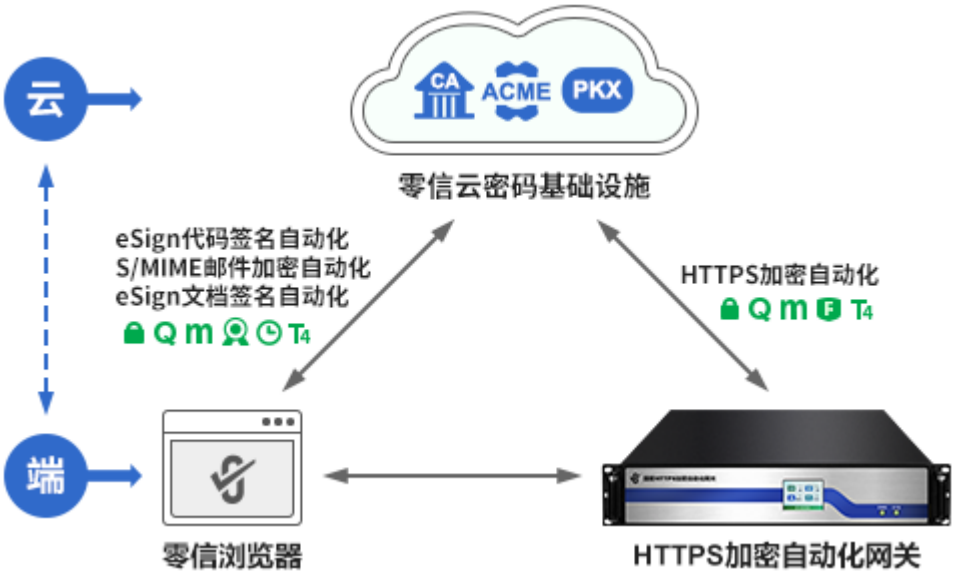
文档安全解决方案—文档签名服务预计第四季度上线，这是继零信浏览器内置 PDF 阅读器实时验证文档数字签名和展示签名者可信身份之后的完整文档安全服务，免费为用户自动化配置双算法文档签名证书，提供免费文档签名服务。专业版则提供全球信任的电子签名服务和提供签名者可信身份认证服务，证明每一个文档的可信身份，增强在线信任。同时，基于加密电子邮件服务免费提供电子合同签署服务，待签署的和已完成签署的合同文件以加密邮件方式保存在用户自己的邮箱中，彻底颠覆目前全球常用的已签署合同文件保存在电子合同签署服务提供商手中的不安全方式。

三、 零信技术，密码应用自动化领导者

保障全球互联网安全的主要密码产品是四种数字证书，SSL 证书保障客户端(浏览器/APP)到服务端的通信传输安全，代码签名证书保障用户端和服务端运行的软件安全，邮件证书保障电子邮件通信安全，文档证书保障文档安全。

但是传统的密码应用与用户的实际应用需求是脱节的，需要用户向 CA 申请证书，再费力配置到各种应用软件系统中去使用，CA 只管发证书，而应用软件系统开发商只管使用证书，中间的衔接工作交给了用户人工手动处理，这就是密码应用的瓶颈，导致了 1977 年发明的 RSA 密码算法到现在 50 年了还没有得到普及应用。而新的情况是这个还没有普及应用的密码算法再过 4 年就要被弃用了，因为这个算法在量子计算面前是不安全的算法。所以，为了防止“先收集后解密”安全威胁，现在就必须启用后量子密码算法，唯一的解决方案是遵循密码敏捷原则，实现各种证书应用自动化，也即是密码应用自动化。

零信技术已经完成了 SSL 证书应用自动化解决方案研发和规模化生产能力建设，多项技术指标全球唯一和全球领先。而代码签名证书应用自动化也即将推出，邮件证书应用自动化和文档签名证书自动化都将在 2026 年完成研发并推向市场。



零信技术在 2026 年将为用户提供更多的先进的 HTTPS 加密自动化管理解决方案和相关产品与服务，同用户一道共同迎接 HTTPS 加密自动化元年的到来，帮助用户一次技改同时搞定商密改造、证书自动化改造和后量子密码迁移，切入保障用户宝贵的数据资源在现在和量子时代的持续安全。

王高华

2026 年 1 月 4 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 247 篇(共 73 万 1 千多字)和英文 107 篇(15 万 2 千多单词)。