HTTPS 加密自动化和邮件加密自动化

零信技术已经完成 HTTPS 加密自动化相关的所有产品的研发和已经开始小规模生产和部署应用，本文给读者朋友讲一讲下一个即将发布的爆款—邮件加密自动化，并讲一讲这两个自动化之间的关系。

一、 什么是 HTTPS 加密自动化？零信技术主要做了哪些工作？

HTTPS 加密自动化源自 ACME 国际标准(自动化证书管理环境)，实现了自动化为网站域名申请 SSL 证书和部署 SSL 证书，彻底把网站管理员从人工手动申请和部署 SSL 证书解放出来，大大加速了 HTTPS 加密的普及应用。

但是，自动化证书管理的目的是为了自动化实现 HTTPS 加密，由于基于 RSA 密码体系的 HTTPS 加密解决方案经过了三十多年的快速发展已经非常成熟，只剩下自动化申请和部署 SSL 证书这一块当时没有实现了，所以，ACME 就出来了。但是，对于一些比较老的系统是无法安装 ACME 客户端软件的，也有些系统由于太重要了，管理员是不愿意动这些服务器去安装 ACME 客户端软件的，也许还有不信任这些第三方软件的考虑。

虽然 Cloudflare、亚马逊等云服务提供商基于这个标准把证书自动化管理拓展到了云服务中，但是仍然是依赖于非常成熟的 RSA 密码应用体系-只需申请和部署 SSL 证书即可，对于还不成熟的 SM2 密码应用体系是无法使用的，因为用户要实现的最终目的是 HTTPS 加密自动化，而 HTTPS 加密就不仅仅是 SSL 证书一个产品，而是一个生态应用。

零信技术也正是已经认识到了国际标准的局限性，认识到了用户的最终需求是要实现 HTTPS 加密自动化，所以，在参考 ACME 国际标准研发了国密 ACME 客户端软件后决定弃用这个解决方案，因为我国大量的 Web 服务器软件不是 Nginx，无法安装国密 ACME 客户端软件，甚至不想也不能安装第三方客户端软件。这就有了现在大家看到的零信国密 HTTPS 加密自动化网关和零信国密 HTTPS 加密自动化云服务，这是一个原 Web 服务器零改造的创新解决方案，一个用户无需关心 SSL 证书为何物的方案，因为 SSL 证书是最终实现 HTTPS 加密的中间产品，用户所需要的是实现 HTTPS 加密自动化，特别是国密 HTTPS 加密自动化。

而要实现 HTTPS 加密自动化，仅有网关仍然是不够的，还需要一个 PKI/CA 云服务—零信云 SSL 服务系统，为网关提供双算法 SSL 证书的自动化申请和签发下发服务，签发国密 SSL 证书时需要国密证书透明日志服务，这也是零信技术目前独家提供的服务，还需要有浏览器支

持国密算法实现国密 HTTPS 加密，这就是零信浏览器，一个完全免费的、干净无广告的、支持国密算法、支持国密证书透明的、严格验证 SSL 证书有效性的通用浏览器。

这就是零信技术为了实现 HTTPS 加密自动化而打造的两个国密算法密码应用生态—国密证书透明生态和国密证书自动化管理生态，两个生态产品保证了能可靠地为用户提供 HTTPS 加密自动化服务，满足用户国密合规和全球信任的网站安全应用需求，一站式为用户提供 HTTPS 加密自动化和 WAF 防护自动化服务。

二、 什么是邮件加密自动化？为何这个自动化也非常重要？

HTTPS 加密自动化已经基本上达到了其顶峰应用，实现了 90%以上网站的 HTTPS 加密都是自动化完成的，下一个证书自动化应用重点是邮件加密自动化。因为电子邮件是第一个最早的互联网应用，比 HTTP 应用早很多年，而这个有了五十多年历史的最古老的互联网应用到现在还是明文方式工作，这的确是不可接受的事实，相信这段明文邮件历史一定会被改写！零信技术决定做这个改变世界的大事！

电子邮件加密协议 S/MIME 实际上只比 HTTP 加密协议 HTTPS 晚两年，但是 HTTPS 加密获得了普及应用，其根本原因还是实现了自动化，这就给电子邮件加密指明了方向，也只有自动化实现电子邮件加密才能最终实现普及电子邮件加密应用。但是，这个自动化无法像 HTTPS 加密自动化一样仅仅是自动化提供邮件证书即可，还需要邮件客户端支持。

正如 HTTPS 加密自动化的推动者是浏览器厂商一样，邮件加密自动化的推动者也只能是邮件客户端厂商，因为 CA 机构只能签发邮件证书，没有能力或者根本就没有想到要去开发邮件客户端来实现邮件证书自动化管理。笔者早在 2017 年就决定干这个邮件加密自动化，决定自己开发一个邮件客户端来实现邮件证书自动化和邮件加密自动化，但是可惜只开了个头就无法继续而导致这个项目停了。

2021 年 6 月笔者重新创业，就确定了要继续研发邮件加密自动化解决方案，在这三年里已经完成了云密码基础设施的建设，完成了 HTTPS 加密自动化相关产品的研发和生产，邮件加密自动化相关产品的研发工作也已经接近尾声，一个彻底解决邮件加密这个世纪难题的创新方案即将横空问世。

邮件加密自动化不只是邮件证书自动化，也是一个生态应用体系，不仅要能签发双算法邮件证书，而且还需要有邮件客户端支持自动化申请和使用邮件证书来实现电子邮件加密和数字签名，零信技术已经完成的云密码基础设施可以实现自动化签发邮件证书，就差一个邮件客户端来自动化对接云邮件证书自动化签发系统，自动化为每一个电子邮箱配置邮件证书，自动化

实现电子邮件加解密和数字签名。零信技术还计划自动化为用户配置时间戳签名证书，自动化为每一封发出的电子邮件盖上可信电子邮戳，以确保每一封邮件的发送时间可信，弥补国际标准在这一块的空缺。

三、 HTTPS 加密自动化与邮件加密自动化两者的关系是什么？

HTTPS 加密自动化的实现，可以用于实现电子邮件传输通道加密自动化，因为邮件发送协议 SMTP 和邮件接收协议 IMAP 都已经支持 SSL 证书实现 SSL SMTP 加密邮件发送通道和 SSL IMAP 加密接收通道，这两个通道的加密一样需要 SSL 证书，也就是一样需要 SSL 证书自动化管理。也就是说，用于实现 HTTPS 加密自动化的 SSL 证书自动化管理一样可以实现邮件加密自动化的电子邮件传输加密自动化。

这是目前电子邮件安全全球市场中普遍采用的 TLS 传输加密解决方案，能解决电子邮件从发送方发出到接收方接收到邮件的全程加密，但这取决于收发双方的邮件服务器都支持 TLS 传输加密，如果有一方不支持，则无法实现全程加密传输。所幸的是，目前 90%以上的电子邮件服务已经迁移到云上，而这些云服务提供商提供的电子邮件服务都是支持 TLS 传输加密的，这个 TLS 传输加密所用的 SSL 证书就可以采用目前的 ACME 技术实现 SSL 证书的自动化申请和部署。

但是，这个解决方案的缺陷在于电子邮件从发出到接收方收到都是明文邮件，并且也是明文方式存放在云端邮件服务器中，这只是实现了端到端的邮件传输加密，可以有效防止电子邮件内容被非法篡改和窃取，但是并不能防止邮件内容在邮件服务器存放的安全，因为是明文存放。目前许多电子邮件服务提供商，特别是免费邮件服务提供商，可能由于找不到盈利模式而只能靠读取用户邮件内容给用户推送相关的广告而获利，这也许是业界巨头没有动力去推动加密电子邮件的主要原因之一。

为了保障电子邮件的安全，最终的解决方案一定是端到端加密解决方案，即电子邮件内容本身先加密再发送，这样不仅能保证电子邮件在传输过程的安全，也能保证电子邮件在云端存储的安全，因为是密文保存在邮件服务器中。而这个端到端的邮件加密解决方案必须用邮件证书来实现加密和数字签名，再结合 TLS 传输加密，就可以真正保障电子邮件的全生命周期安

全。因为仅有加密电子邮件无法保障邮件内容在传输过程中被非法篡改和使得加密失败，导致收件人无法正常收到加密邮件，即使能收到也无法正常解密。这就是 HTTPS 加密自动化与邮件加密自动化的紧密关系，借助 SSL 证书自动化来保障邮件传输安全，再加上电子邮件端到端加解密自动化，就可以完美地完成电子邮件加密自动化的伟大使命。

四、 邮件加密自动化是下一个热点，全球互联网将迎来第二个密码应用高峰

电子邮件是第一个互联网应用，第二大互联网流量，虽然有许多是垃圾邮件导致的废流量，但是如果解决了电子邮件加密自动化难题，也就是自动解决了垃圾邮件和恶意攻击邮件泛滥难题，因为电子邮件加密自动化将实现每一封电子邮件都有可信身份的数字签名和加密，只要邮件服务器拒绝接收没有数字签名和加密的电子邮件，也就杜绝了垃圾邮件。而如果再把微信公众号文章发布的商用模式应用到成熟的邮件列表订阅上，那就有了可行的邮件营销解决方案，这就是有可能颠覆目前的微信公众号的新的不受打扰的加密的信息发布和获取方式。

邮件加密自动化一定是下一个密码应用热点，也必将大受全球用户的欢迎，因为电子邮件不仅仅是通信工具，也是所有互联网服务的落地通知工具，是个人生活和工作的所有互联网数据的集中保存地，即使在社交媒体日益盛行的今天，全球互联网用户不仅没有减少电子邮件的使用，反而使得电子邮件使用频率越来越高，其信息保存和汇聚功能越来越重要。

但是，互联网用户已经深感明文邮件对保护个人隐私信息和商业机密信息的严重不足，业界一直在探索各种邮件加密解决方案，谁能拿出好的解决方案，谁将能赢得用户的喜爱，就能在全球市场赢得邮件加密领导地位。唯一的正确方向就是自动化，自动化用电子邮件证书实现邮件加密，保障电子邮件的全生命周期安全。零信技术将拿出不同的创新解决方案，为全球用户提供不一样的全球信任和国密合规的电子邮件加密自动化服务，敬请期待。

有诗为证：

自动化，已深得所有行业共识。
证书自动化，保网页流量安全，
也正在保障邮件流量传输安全，
即将保障邮件端到端加密安全。

王高华

2024 年 9 月 29 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 179 篇(共 51 万多字)和英文 69 篇(8 万 6 千多单词)。。