只有自动化实现端到端加密，才能真正保证电子邮件安全

目前全球市场上声称提供电子邮件端到端加密的厂商很多，各种五花八门的说辞让用户不知如何选择真正有效的端到端加密解决方案，本文就讲清楚什么才是真正的端到端加密，用户应该选择什么样的端到端加密才能真正保护自己的邮件机密信息安全。

一、 什么是端到端加密？为何电子邮件需要端到端加密？

端到端加密(End-to-End Encryption，简称 E2EE)就是信息从发送端一直到接收端都是加密的，比如常用的网站 HTTPS 传输加密，从用户浏览器发送到服务器端的信息就是通过 SSL 加密通道传输的，属于端到端加密。只有实现了端到端加密才能保证机密数据在传输过程中不会被非法窃取和非法篡改，才能保证机密信息在传输过程保持加密状态而保障机密信息传输安全。

电子邮件通信是发件人把信息从自己的电脑发送到收件人的电脑中的信息传输过程，同 HTTP 协议不同的是：电子邮件不是直接从发件人端发送给收件人端，而是通过双方的邮件服务器中转，这个特点注定了不能采用 HTTPS 加密一样的技术方案来实现端到端加密。也正是由于邮件是通过邮件服务器先保存后转发的这个特点决定了电子邮件需要端到端的加密，因为有第三方(邮件服务器)在接管这个传输过程，并且电子邮件会长期保存在邮件服务器中，除非用户自己彻底删除。

电子邮件端到端加密是指电子邮件在发送之前已经加密，以密文方式发送给收件人，这样，负责中转的邮件服务器也只能是以密文方式转发，也只能是以密文方式保存，只有这样才能保证电子邮件是真正的全程端到端加密的。

二、 实现电子邮件端到端加密有哪些技术方案？什么技术方案才是真正的电子邮件端到端加密？

我们先看看市场上流行的 TLS 邮件加密技术，这个技术当然是从 HTTPS 加密借鉴过来的，但是如上段文章所讲，邮件传送过程同 HTTP 传输过程是不同的，如下图所示，TLS 邮件加密技术是在邮件服务器上部署 SSL 证书实现 SSL IMAP 和 SSL SMTP 加密传输，电子邮件从张珊邮件客户端通过 TLS 加密通道把电子邮件发送到张珊的邮件服务器中，能保证传输安

全。张珊的邮件服务器把此邮件保存在张珊的邮箱中后把此邮件发送到收件人李诗的邮件服务器中，这个传输过程是否能实现 TLS 传输加密取决于李诗的邮件服务器是否支持 SSL SMTP 协议，如果支持，则能实现 TLS 传输加密，如果不支持，则只能明文传输，这就不是端到端加密了。所幸的是，目前大多数邮件提供商都已经支持 SSL SMTP 协议，所以电子邮件仍然可以加密方式达到李诗的邮件服务器，李诗则继续使用 TLS 传输加密从邮件服务器获取张珊发给他的电子邮件。

请注意：以上解决方案的邮件内容在用户端和邮件服务器端都是没有加密的明文邮件，电子邮件内容明文保存在邮件服务器中。TLS 邮件加密技术方案只解决了电子邮件的传输过程加密，并不解决电子邮件内容加密的难题。

再请看下图所示的，电子邮件在张珊电脑在发送之前就已经加密，无论邮件服务器是否支持 SSL STMP 协议都可以保证电子邮件以密文方式传输和密文保存在邮件服务器中，这就是端到端加密，中间负责转发和存储的邮件服务器也不能看到已加密的邮件内容，邮件服务提供商无法通过机读邮件内容而推送内容相关的广告，这就保护了邮件机密信息安全。

至于如何实现电子邮件在发送之前的加密，市场上采用的技术方案是五花八门，有把邮件内容变成 PDF 文件再加一个口令的，有把邮件内容变成所谓的加密信封保存把云端服务器中，收件人会收到一个在线解密的链接，必须连接云端服务器才能查看，等等。这些都是采用私有协议实现加解密，都不是可行的解决方案，只适用一个封闭系统使用，根本不适用于电子邮件这个通达全球的开放系统的基本要求。

目前市场上成熟的技术方案是采用密码技术实现电子邮件加密，主要有 S/MIME 加密、PGP 加密和 IBC 加密三种加密技术，后两种加密方式只注重了用数字证书加密，并且是用无可信身份信息的自签证书，没有注重发件人的可信身份认证。电子邮件属于不见面通信，不仅

需要加密，而且还需要证明发件人的可信身份，只有通过可信的第三方 CA 认证的可信认证身份，才能防止邮件身份欺诈，身份可信和加密两者都非常重要，这只有 S/MIME 技术做到了。S/MIME 不仅仅是笔者所爱，而且也是业界的绝大多数邮件加密解决方案采取的技术路线，也是常用的邮件客户端采用的解决方案，国际标准组织-CA/浏览器论坛已经成立了 S/MIME 邮件证书工作组，并制定了 S/MIME 证书基线标准，要求全球信任 CA 从 2023 年 9 月 1 日起必须遵循这个国际标准，这是全球业界对 S/MIME 加密技术的最大认可，使得 CA 机构首次有规可循地签发 S/MIME 邮件证书。

S/MIME 技术的核心是由第三方 CA 在严格按照国际标准验证用户身份后签发电子邮件证书，用户需要把邮件证书配置到邮件客户端中使用才可以实现电子邮件加密和数字签名，实现电子邮件在发出之前就已经用证书加密，这才是真正可靠的端到端加密。常用的电子邮件客户端如微软 Outlook、Mozilla 雷鸟、苹果邮件、华为邮件等都支持 S/MIME 技术实现电子邮件端到端加密。

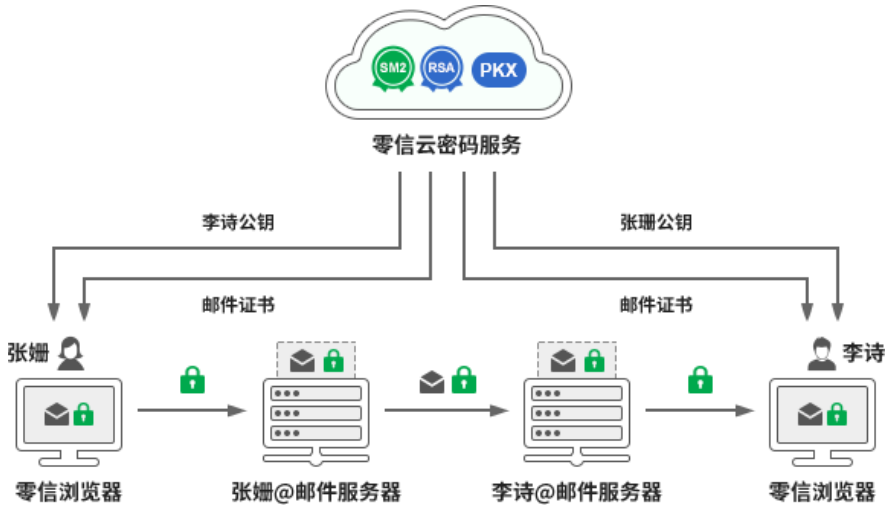
三、 零信技术自动化实现电子邮件端到端加密，有力保障电子邮件全生命周期安全

虽然大家都认可采用 S/MIME 技术实现端到端加密是保护电子邮件安全的唯一可靠技术，但是目前真正使用 S/MIME 技术来加密日常邮件通信的用户还是非常少的，因为这个技术的使用门槛太高，不仅需要用户向 CA 申请邮件证书，还需要手动配置证书到常用的邮件客户端中使用，还需要收件人也有邮件证书，并且双方必须事先交换公钥证书，同时还需要自己管理加密密钥(不能丢失)和定期更新邮件证书。这些都是普及使用 S/MIME 技术实现电子邮件加密的技术障碍，不解决这些易用问题就无法普及应用这个技术来普及电子邮件加密。

HTTPS 加密之所以已经在全球普及应用，其秘诀在于自动化，自动化申请和配置 SSL 证书实现 HTTPS 加密。零信技术电子邮件加密解决方案同 HTTPS 加密解决方案一样，也是走自动化路线，自动化为用户申请和配置电子邮件证书，自动化交换公钥证书，自动化管理加密密钥，只有自动化才能实现普及电子邮件加密的宏伟目标。

要实现自动化，当然也一定是端云一体解决方案，这个端就是零信浏览器，一个内置邮件客户端的基于谷歌 Chromium 内核的高性能通用浏览器，用户使用零信浏览器登录邮箱后，零信浏览器会自动连接零信云密码服务系统，自动化为用户完成电子邮件证书申请、电子邮箱验证、电子邮件证书签发和配置使用。同时，在使用零信浏览器发送加密电子邮件时自动连接零信云密码服务系统提供的公钥交换服务，自动获取收件人的公钥证书，无需事先同收件人交换公钥就可以发送加密邮件。端云一体，彻底解决电子邮件加密所遭遇的各种技术难题，让用户

可以无感地像发送明文邮件一样发送加密邮件，实现端到端电子邮件加密，电子邮件内容也是密文保存在邮件服务器上，完美地实现了电子邮件的全生命周期安全。



零信技术同样采用了 S/MIME 技术来实现电子邮件加密，实现了与全球所有支持 S/MIME 标准的邮件客户端之间的电子邮件加解密的兼容互通。不同的是：零信技术是自动化实现的，完美地解决了 S/MIME 技术使用的各种不方便和高门槛，使得用户可以无感地享受先进的 S/MIME 技术带给用户的电子邮件安全保障，也只有做到自动化实现电子邮件加密，才能普及电子邮件加密，真正保障全球邮件用户的电子邮件在途安全和在云安全，也就是保障全生命周期安全。

有诗为证：

端到端邮件加密，保证邮件信息安全。
零信技术端到端，自动化零门槛实现。
唯有加密零门槛，才能普及邮件加密。
邮件加密定普及，保障全球邮件安全。

王高华

2024 年 10 月 11 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 182 篇(共 52 万 1 千多字)和英文 71 篇(8 万 8 千多单词)。