邮件加密，任重道远

笔者第一次使用电子邮件大概是在 1995 年，当时是使用 Eudora 邮件客户端软件，通过拨号到香港电信接入到互联网，使用香港 NetVigator 提供的邮箱发送电子邮件，再后来是注册了 Hotmail 邮箱、Yahoo 邮箱和 MSN 邮箱。从那时到现在，30 年来笔者一直是以电子邮件办公，所以对电子邮件通信是情有独钟。虽然现在即时通讯和社交媒体很普及，但是全球范围内各种正式的通信仍然是以电子邮件为主，其霸主地位从未被撼动过。电子邮件等同于纸质信件，是可以永久保存在邮箱中供以后查阅的，这是一个非常珍贵的资产，不像聊天聊完就没有了，也不像在社交媒体上发的是公开信息，电子邮件是你的私信。

笔者在 2004 年代理销售 GeoTrust 电子邮件证书时学会了用电子邮件证书来加密电子邮件，之后就沉迷于 S/MIME 邮件加密而不可自拔。在多年的使用加密电子邮件体验中，深深感到电子邮件加密的不方便，也正是由于太不方便使用使得电子邮件加密到现在仍然还没有普及。

但是，现在几乎所有电子邮件服务都已经迁移到云端，而电子邮件是明文传输和明文存储的，明文电子邮件显然已经无法让用户放心使用了。而互联网第一大流量 http 流量已经实现了强制 https 加密和接近普及 https 加密，有力保障了 http 流量的零信任安全。而对于邮件流量安全，虽然美国政府发布的“联邦零信任战略”在强调 https 加密的同时也强调了邮件加密的重要性，但是由于目前市场上没有用户体验很好的邮件加密解决方案而无法给出能落地实施的具体方案。

目前市场上有各种不同的电子邮件加密解决方案，本文特对各种方案做一个总结，以便大家对电子邮件加密有一个比较全面的了解。

1. 邮件客户端加密

电子邮件在发明时是明文的，包括邮件传输是明文的，邮件明文存放在邮件服务器中。随着电子邮件的普及应用，就出现 S/MIME 加密电子邮件标准，也就出现了 CA 机构签发电子邮件证书，邮件客户端支持用邮件证书加密电子邮件。大家常用的邮件客户端如 Outlook，雷鸟和苹果邮件等都是支持 S/MIME 标准实现邮件加密的。

市场上也有支持 PGP 邮件加密的解决方案，也有支持 IBC 邮件加密的解决方案，这两个解决方案只是注重了加密，并没有注重发件人身份认证。而笔者认为电子邮件不仅需要加密，

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，两者都非常重要，这只有 S/MIME 解决方案做到了。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/浏览器论坛还专门成立了 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。所以，零信技术电子邮件加密解决方案就是采用 S/MIME 标准的解决方案，本文也只讲 S/MIME 加密和数字签名解决方案。

邮件客户端采用 S/MIME 技术实现电子邮件加密的主要普及应用障碍有三个：

(1) **必须向 CA 机构申请电子邮件证书**

申请证书过程非常繁琐，而拿到证书后还需要费力在各种邮件客户端中配置好证书，每年还需续期证书，自己管理好证书私钥等等。

(2) **必须先同收件人交换公钥**

发件人必须发送一个数字签名邮件给收件人，收件人回复一个数字签名邮件才完成公钥交换，才能开始发送加密邮件，也就是说对方也必须有电子邮件证书并且在客户端软件配置好才能使用。

(3) **必须自己管理好加密密钥**

这个太重要的了，包括管理好已过期的证书私钥。笔者早期的已加密邮件现在有许多都打不开了，因为用于加密的证书私钥找不到了或者忘了保护口令。这是用户使用邮件加密的一个痛，有时急用的重要的邮件找到了但打不开。

正是这三大应用门槛阻碍了 S/MIME 加密技术的普及应用，使得这个在 1998 年就已经制定了 RFC 2311 国际标准的先进技术在 26 年后的今天还没有得到普及应用，人们还在无奈地忍受明文邮件的不安全，因为太难用了，非专业人士搞不定这么复杂的加密技术。

2. 邮件传输 TLS 加密

邮件发送协议 SMTP 和接收协议 POP3/IMAP 在设计时都是明文传输的，所以业界的第一个行动是实现 SMTP/IMAP 协议的 TLS 加密，借鉴 HTTPS 加密，采用 SSL 证书实现收发电子邮件的传输加密，也就是说，SMTP 邮件服务器和 IMAP 邮件服务器都必须部署 SSL 证书实现邮件传输加密，以保障用户从邮件客户端发送电子邮件到邮件服务器时使用了加密通道，从发件人邮件服务器发送到收件人邮件服务器采用加密通道传输，收件人从邮件服务器取回邮件也

是使用加密通道，保障明文电子邮件在传输过程中不会被非法窃取和非法篡改。

但是，这个 TLS 传输加密需要收发双方的电子邮件服务器都支持 TLS 传输加密，这使得电子邮件在没有部署 SSL 证书的一方仍然是明文传输的，仍然无法保障电子邮件在整个传输过程的全程加密传输。所以，这就有了国际标准 RFC 8461(MTA-STS，SMTP 严格传输安全)，这是强制实现全程 TLS 传输加密的标准，SMTP 服务器可以拒绝向未部署可信的 SSL 证书的邮件服务器发送电子邮件，以保障电子邮件的传输过程的全程加密。

这个技术对普通邮件用户是无感的，但是请注意，这个技术只是解决了明文电子邮件在传输中的安全，并不是像电子邮件客户端那样用邮件证书加密实现了端到端加密安全，如果电子邮件是以密文形式发送，则 SMTP 传输过程不采用 TLS 传输加密也能保证邮件的传输安全。而即使邮件通过 TLS 加密传输到邮件服务器，但仍然是明文存放在云端邮件服务器中，这仍然无法让用户放心，因为邮件服务提供商可以人为或机读用户的邮件内容，有些邮件服务提供商就是靠机读邮件内容并在邮件内容旁边展示广告来营利的。

3. Web 邮件加密

这类解决方案的领先者是瑞士的 ProtonMail, 支持邮件客户端方式和 Web 方式实现邮件加密，似乎用户反映也不错。笔者在这里必须指出的是：这个邮件加密服务的核心不足是一个不同角色的利益冲突问题。ProtonMail 既提供邮件内容托管服务又提供邮件加密服务，同时又替用户管理加密密钥，大家应该能发现这个所谓的绝对保护用户隐私的邮件加密服务的问题了吧。也就是说，ProtonMail 既拥有用户的加密邮件内容，又拥有能解密的密钥，这还能让用户放心认为已加密邮件是真的安全的吗？

4. 邮件网关加密

这是一个零改造现有邮件客户端的解决方案，对普通用户也是无感的，市场上有不少这样的解决方案。笔者曾试用过某个知名邮件安全大厂的解决方案，支持 S/MIME 邮件加密，但是需要用户自己向 CA 申请邮件证书，自己上传邮件证书(私钥)到管理后台，由网关来调用邮件证书实现邮件加解密。

这是一个类似于邮件客户端的解决方案，仍然存在邮件客户端在实现电子邮件加密中存在的三个主要应用障碍，笔者就不再重复讲这些问题了。

5. 零信技术邮件加密之路，艰难但使命必达

笔者从 2004 年开始实践电子邮件加密，到现在已有整整 20 年了，深深体会到邮件加密之路之艰难，特别是在国内电子邮件用户不断被微信取代后的今天，笔者仍然不忘初心，在重新创业后继续探索电子邮件加密之最优解决方案，即将发布的零信邮件安全服务将是笔者交出的最新答卷，敬请期待。

笔者 20 年的邮件加密实践过程可以分为三个阶段：

第一阶段：销售电子邮件证书，指导用户使用电子邮件客户端实现电子邮件加密。

这个阶段，笔者的心思主要是销售电子邮件证书，并为用户提供完全免费的一年期电子邮件证书。为用户提供详细的电子邮件证书使用指南，包括如何在各种常用的电子邮件客户端软件中配置邮件证书，如何发送数字签名邮件和加密邮件，收发双方如何交换公钥等等。这个阶段很累，唯一收获是深深了解了邮件加密之非常不好用，因为 CA 只管销售邮件证书，而邮件客户端厂商只能保证用户有了证书并配置好后能使用证书实现加密，两者的衔接和无缝用户体验根本就是空白。

第二阶段：研发电子邮件客户端，实现电子邮件加密自动化，但未完成。

也正是由于笔者深知使用电子邮件客户端和电子邮件证书实现电子邮件加密有多难，所以，笔者就决定研发电子邮件客户端软件(密信 APP)，这个邮件客户端不是普通的邮件客户端，是一个能自动化免费为用户配置电子邮件证书的客户端软件，能实现电子邮件无感自动加密，用户只需换用一个邮件客户端软件即可。这是全球首个类似于 HTTPS 加密自动化解决方案(ACME)的邮件加密自动化解决方案，很好地实现了 CA 机构与邮件客户端厂商的无缝对接，两者合二为一，实现自动化邮件加密。但很可惜的是，密信公司被收购后笔者不得不选择离开，这个自研邮件客户端项目在还没有完全完成的状态下已经被搁浅了。

第三阶段：基于零信浏览器实现电子邮件加密自动化，迈出了坚实的一步。

笔者于 2021 年 6 月重新创业，脑子里仍然念念不忘一个德国用户对邮件加密自动化的喜爱，这个用户在使用了第二阶段研发的 APP 后称之为 Life Saver(救命神器)，彻底解决了繁琐的证书申请、配置邮件客户端、交换公钥和密钥管理难题，让他彻底从中解放出来。所以，笔者不忘初心，继续研究和探索邮件加密自动化解决方案。

在第二阶段研发邮件客户端软件时遇到的一个最大问题是无法说服用户更换邮件客户端软件，因为用户已经非常熟悉使用常用的邮件客户端软件，特别是大型组织多年来一直在使用特定邮件客户端办公，而邮件加密只是其中一个很小的功能，不可能因为这个功能不太好用就要求所有员工都换掉非常熟悉邮件客户端去使用一个陌生的邮件客户端。用户不仅非常熟悉常

用邮件客户端的使用，而且上面有所有人的通讯录、有日程管理、历史邮件等等，这些都是无法让用户为了邮件加密而舍弃的。

但是，第二阶段的探索值得高度肯定的是实现了邮件加密自动化，这是最受用户欢迎的主要原因。所以，笔者的第三阶段仍然坚持的技术路线是邮件加密自动化，自动化为用户免费配置电子邮件证书，自动化交换公钥，自动化实现邮件加密，自动化实现邮件证书密钥管理。而为了解决用户无法舍弃常用的邮件客户端问题，新的解决方案就要放弃让用户更换邮件客户端的想法，寻找新的解决方案。

所幸的是，笔者研发 HTTPS 加密自动化解决方案时研发和发布了零信浏览器，当初的出发点是为了让浏览器支持国密算法和国密 SSL 证书，用国密算法实现 HTTPS 加密。由于零信浏览器是目前市场上唯一一个完全免费的、支持国密算法和国密证书透明的国密浏览器，所以大受用户欢迎。零信浏览器不仅是一个原汁原味的同谷歌浏览器一样的基于开源 Chromium 的通用浏览器，而且是一个同时支持 RSA/ECC/SM2 三种密码算法实现自适应加密算法 HTTPS 加密的浏览器，同时还是一个全球率先实现的实时验证 PDF 文档数字签名和展示数字签名者可信身份的 PDF 阅读器。也就是说，无论用户是在乎零信浏览器的国密算法支持功能，还是在乎支持数字签名的 PDF 阅读器，反正用户爱上了零信浏览器，使得零信浏览器在全球市场的市场份额节节攀升，短短两年时间就已经覆盖了全球 130 多个国家和地区的用户。

据第三方统计数据，全球用户中使用浏览器登录 Web 邮箱的比例是使用邮件客户端用户的两倍，也就是说大多数用户喜欢直接用浏览器登录 Web 邮箱查看邮件，这就给我们指明了邮件加密解决方案的大方向—基于零信浏览器做文章，让用户在使用零信浏览器查看邮件时能自动解密已加密邮件、发送电子邮件时能自动加密电子邮件，这个功能的实现就解决了超过 50%以上用户的电子邮件加密自动化需求。而对于使用邮件客户端的用户的邮箱也是支持浏览器 Web 登录的，因为所有邮件服务提供商 100%都提供 Web 登录邮箱功能，也就是说，使用浏览器登录邮箱这是所有用户都有的经历和使用体验，是能全覆盖所有邮件用户的，用户需要做的无非是再多安装一个通用浏览器而已，用户实际上已经养成了安装使用多个浏览器的使用习惯。

零信技术这个不改变用户仍然可以使用熟悉的邮件客户端的使用习惯，只是需要多安装一个有优秀功能的浏览器，是一个用户为了邮件加密自动化可以接受的解决方案。并且我们的解决方案让 Windows 版本 Outlook 能自动解密用零信浏览器加密的电子邮件，最大程度做到了兼容 Outlook 的 S/MIME 加解密功能。

即将发布的零信浏览器升级版本(V2501)就是支持自动化实现电子邮件加密和解密的版本，用户只需使用零信浏览器登录邮箱，即可免费自动激活零信邮件安全服务，即可免费自动为用户配置双算法电子邮件证书-RSA 邮件证书和 SM2 邮件证书，双证书双算法自适应加密，用户

可选默认采用何种密码算法实现邮件加密。敬请期待和免费体验不一样的零信邮件加密自动化服务。

有诗为证：

求索加密二十载，即将圆梦新方案。
邮件加密自动化，只需零信浏览器。
邮件证书零配置，加密公钥零交换。
自动加密很流畅，自动解密也无感。

浏览网页超级快，阅读文档更是爽。
加密邮件新功能，省事省时更省钱。
一个通用浏览器，三个密码应用齐。
零信任安全上网，零信浏览器真酷！

王高华

2024 年 10 月 22 日于深圳

2024.10.22
00:27:17
+08'00'

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 185 篇(共 53 万 1 千多字)和英文 74 篇(9 万 4 千多单词)。