解读美国《联邦零信任战略》(三)：邮件安全

美国管理和预算办公室(OMB)在 2021 年 9 月 7 日发布了《联邦零信任战略》（Federal Zero Trust Strategy）草案并网上征求意见，以支持第 14028 号美国总统行政令《改善国家网络安全》，指导联邦政府机构的安全架构向基于零信任原则迁移。

其中关于加密电子邮件流量是这样写的：

> **3. Encrypting email traffic**
>
> It remains challenging today to easily and reliably encrypt an email all the way between any sender and any recipient. Unlike HTTP and DNS, there is not today a clear path forward for guaranteeing that Federal emails are encrypted in transit, particularly for emails with external parties.[12]
>
> **CISA will evaluate the viability of MTA-STS as a government-wide solution for encrypted email and make recommendations to OMB to inform future government-wide actions.**
>
> *3. 加密电子邮件流量*
> *在任何发件人和任何收件人之间轻松可靠地加密电子邮件仍然具有挑战性。与 HTTP 和 DNS 不同，目前还没有明确的技术路径来保证联邦电子邮件在传输过程中被加密，特别是对于与外部方的电子邮件。*
> *网络安全和基础设施安全局(CISA)将评估 MTA-STS 作为政府范围内加密电子邮件解决方案的可行性，并向 OMB 提出建议，以告知未来政府范围内的行动。*

既然是公开征求意见，笔者就给公开征求意见的邮箱发送了我的意见，明确指出 TLS 邮件加密方案(MTA-STS)不是一个最佳方案，最佳方案应该是端到端加密。在征求意见截止日之后，笔者收到了感谢回信，可以看出虽然是礼节式的回复，但仍然能体会到他们对实施电子邮件零信任安全的决心。

RE: [EXTERNAL] RE: Public comment on the Federal Zero Trust Strategy from ZoTrus

MO MBX OMB OFCIO <MBX.O[redacted]@OMB.eop.gov> 2021/9/23 (周四) 0:56

收件人 [redacted]@zotrus.com'

抄送 MBX O[redacted]

Hello,

We just wanted to acknowledge receipt, and to thank you for your comments, which we will consider before finalizing OMB's federal zero trust strategy. We really appreciate you taking the time to send us your feedback, and your interest in helping strengthen federal cybersecurity.

我们只是想确认已收到并感谢您的意见，这些意见将会被考虑并体现在最终发布的联邦零信任战略中。我们真的非常感谢您花时间发送您的建议方案，并且感谢您有兴趣帮助加强联邦政府网络安全。

大家再看看 2022 年 1 月 26 日发布的正式版本已经去掉了 MTA-STS 的内容，也可以理解为正式版本听取了笔者认为 TLS 加密不是一个好方案的建议，所以不再提及这个解决方案，而是在加密电子邮件流量的第三段说："CISA 将评估采用当前开放标准的可行性，以作为联邦政府范围内的加密电子邮件解决方案，并向 OMB 提出建议，为今后的政府行动提供信息。作为评估的一部分，CISA 应与 FedRAMP 合作召开会议和通过电子邮件咨询云服务提供商和其他电子邮件生态参与者。"

> CISA will evaluate the viability of current open standards as Government-wide solutions for encrypted email in transit and make recommendations to OMB to inform future Government-wide actions. As part of its evaluation, CISA should partner with FedRAMP to convene and consult with cloud service providers and other participants in the email ecosystem.

为了让读者朋友全面了解电子邮件加密之难，大家可以再看看英国政府网站是怎么要求的:

How to secure email

You must:

- encrypt and authenticate email in transit by supporting Transport Layer Security (TLS) and Domain-based Message Authentication, Reporting and Conformance (DMARC) as a minimum
- use extra encryption if your data needs more protection
- make sure the recipient protects the data you send to them
- make email security invisible to end users as far as practically possible

如何保护电子邮件的安全性，您必须:

- *通过支持传输层安全(TLS)和 DMARC 标准作为最低要求来加密和验证传输中的电子邮件*
- *如果您的数据需要更多的保护，请使用其他加密手段*
- *确保收件人保护您发送给他们的数据*
- *尽可能不要为了邮件安全而改变最终用户的邮件使用习惯。*

我们从最后一条要求不改变用户的邮件使用习惯就不难理解为何英国政府网站对电子邮件安全的要求由以前要求采用 S/MIME 加密(如下图所示)改为了现在的采用 TLS 邮件加密了，因为目前市场上的 S/MIME 加密解决方案是效率很低的和用户体验也是很差的。

Transfer sensitive information

You should only use message-based encryption like PGP or S/MIME occasionally for transfer of sensitive information as it's inefficient and provides a poor user experience.

也就是说，为了用户体验，美国政府和英国政府都选择了不影响用户体验的 TLS 邮件传输加密，包括采用 MTA-STS。但是，TLS 邮件加密只能保证用户到自己的邮件服务器之间的传输加密，如果收件人邮件服务器没有采用 TLS 加密，则只是邮件发送端采用了链路加密但是在邮件服务器之间的传输和接收端都没有加密，这就是为何要求所有邮件服务都必须采用 TLS 加密(STS)。

英国政府网站还专门有一段文字强调用户体验- Make email security invisible to end users (让最终用户无感实现邮件安全)，尽量不要让最终用户为了邮件安全而必须采用非常复杂的技术措施。

Make email security invisible to end users

Email security should be invisible to the end user as far as possible. Users should have the option to mark sensitive information if needed but not have to make complex technical decisions about sending data.

那么，用户到底需要什么样的邮件加密解决方案？什么样的加密解决方案能让最终用户无感？笔者多年来一直在思考和实践这个难题。美国联邦零信任战略中的“加密电子邮件流量”的第一段是这样写的：“如今，在任何发件人和任何收件人之间轻松可靠地加密电子邮件仍然具有挑战性。与 HTTP 加密和 DNS 加密不同，目前还没有明确的技术途径来保证联邦政府电子邮件在传输过程中加密，尤其是与外部方发送的电子邮件。”这的确是事实，找到合适的电子邮件加密解决方案非常有挑战性。

第二段是这样写的：“然而，电子邮件仍然是联邦政府日常工作运作中重要的通信和认证方法。由于联邦政府机构发送和接收的电子邮件是由各种各样的邮件客户端软件和服务提供商来完成的，因此任何解决方案都必须基于开放标准。”这一段强调的是任何可行的解决方案必须是基于开放标准的。

However, email remains a critical method of communication and authentication in the operation of everyday life in the Federal Government. Since emails to, from, and within the Federal Government are sent and received by a tremendous diversity of clients and service providers, any solution will necessarily be based on open standards.

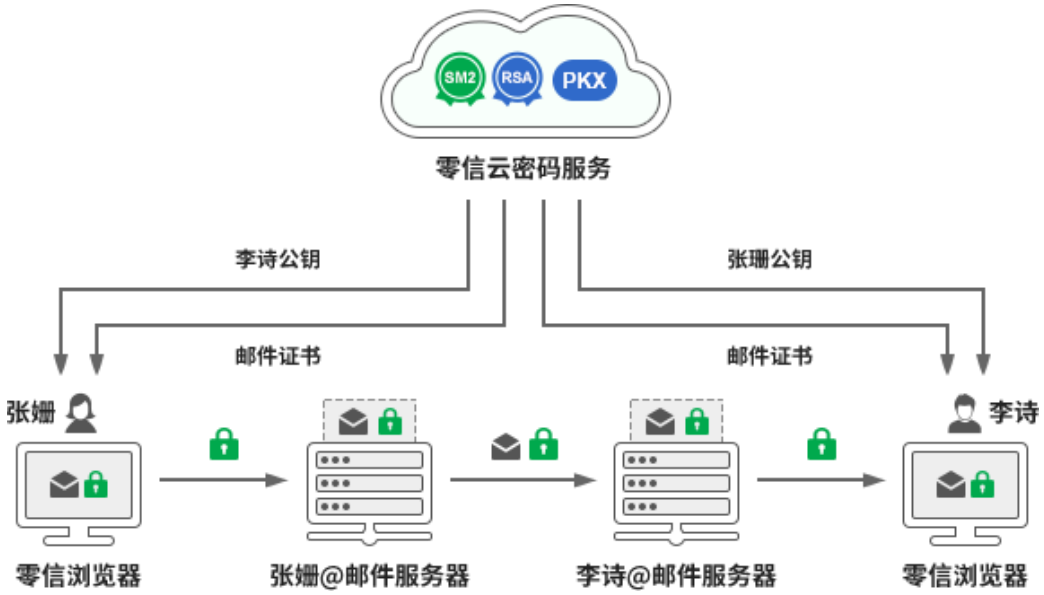
那么，电子邮件加密的开放标准是哪一个呢？当然只有 S/MIME 国际标准，这是在 1998 年就已经制定了的 RFC 2311 国际标准，目前所有常用的电子邮件客户端软件都支持这个标准，所有全球信任的 CA 机构都在签发基于这个标准的电子邮件证书，国际标准组织-CA/浏览器论坛的 S/MIME 证书工作组在 2023 年 1 月 1 日发布了《签发和管理公共信任的 S/MIME 邮件证

书的基线要求》，这是全球第一个规范全球 CA 签发电子邮件证书的国际标准，当然也是明确地肯定了 S/MIME 技术标准的国际地位，电子邮件加密就是基于 S/MIME 国际标准，我国的电子邮件安全标准也是采用 S/MIME 标准的。

但是，为何这个基于 S/MIME 标准技术的加密方案在 S/MIME 标准诞生后的 26 年后还是没有得到普及应用呢？就是因为英国政府网站所讲的用户体验太差而导致的，非常难用，用户不仅要费力去向 CA 申请邮件证书，而且还要同收件人交换公钥才能实现相互加密，同时还要费力管理加密密钥，一旦密钥丢失或忘记了密钥保护口令而就永久无法解密已加密的邮件，这个痛苦笔者是深深领教了，后悔当初还不如不加密！

既然用邮件证书实现邮件加密这么痛苦，那是否有不痛苦的解决方案呢？电子邮件作为互联网第二大流量，承载了大量的机密信息交换和有大量的个人隐私信息和商业机密信息存储在云端，这些机密信息都是明文传输和明文存储，很不安全！全球业界通过努力已经把互联网第一大流量 http 流量逐渐变成了 https 加密流量，有效地保障了全球互联网的主要信息流量的传输安全。虽然 TLS/SSL 证书也可以保障邮件传输安全，但是邮件传输过程同 HTTPS 加密不一样，邮件系统是一个连接全球的分布式去中心化的系统，是需要邮件收发双方甚至多方都必须一致采取统一行动才能完全实现邮件传输加密的。而即使大家都实现了 TLS 传输加密，但是邮件内容仍然是明文存储在云端邮件服务器中，仍然是不安全的。

怎么办？零信技术的创新解决方案是端云一体的解决方案，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 S/MIME 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，完全遵循国际标准和国密标准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。



零信技术邮件加密自动化解决方案完美地解决了美国联邦零信任战略中邮件加密的技术难题，而且也解决了英国政府关于邮件安全的用户无感要求，这一个创新解决方案一定会得到全球用户的认可。零信技术愿同全球邮件用户一道共同努力，让互联网的第二大流量也能实现端到端全加密，保证电子邮件在途和在云的全程安全，让伟大的电子邮件继续为人类提供更加安全的通信服务。

王高华

2024 年 10 月 14 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 183 篇(共 52 万 4 千多字)和英文 72 篇(9 万多单词)。