邮件加密的第一道坎是申请证书

(2021 年 4 月 12 日)

邮件加密有三道坎，第一道坎是申请证书，这个很好理解，没有邮件证书就没法实现邮件加密，这是基础和基本条件。第二道坎是公钥交换，这道坎如何迈过，已在博文《邮件加密的第二道坎是公钥交换》讲清楚了，就是通过云端公钥库来实现全自动公钥交换。邮件加密的第三道坎是密钥管理，这个也已在博文《邮件加密的第三道坎是密钥管理》讲清楚了，就是通过云密钥管理服务来解决难题。

今天就讲一讲邮件加密的第一个拦路虎。1995 年 RSA 等公司提出了 S/MIME(安全/多用途互联网邮件扩展)协议 V1 版本，这是一个用数字签名和加密技术来解决电子邮件安全问题的解决方案，1998 年和 1999 年相继出台 V2/V3 版本并提交 IETF 形成系列 RFC 国际标准。从那时开始，邮件证书开始用于电子邮件数字签名和加密，用户必须向 CA 申请邮件证书，配置到邮件客户端中使用，这个流程已经走过了 21 年，基本上没有任何创新，唯一的改变的是：近几年随着 IE 浏览器退出市场，把证书申请过程中由用户在本地电脑生成密钥对和证书请求文件改为直接由 CA 给用户.pfx (.p12)格式证书，因为其他浏览器不支持本地电脑生成密钥对的操作流程。

让我们回到邮件加密需求的本源，反思一下繁琐的邮件证书申请过程，用户需要的是通过邮件加密来保障邮件机密信息安全，而不是邮件证书，邮件证书只是用于邮件加密的工具，而不是用户最终需要的产品，这个说法 CA 界朋友听起来可能难以接受，但是，想一想为何 S/MIME 邮件加密技术在 21 年后的今天还没有得到普及推广，明明大家都知道明文邮件不安全，为何就不去用 S/MIME 邮件加密技术来保护邮件安全？

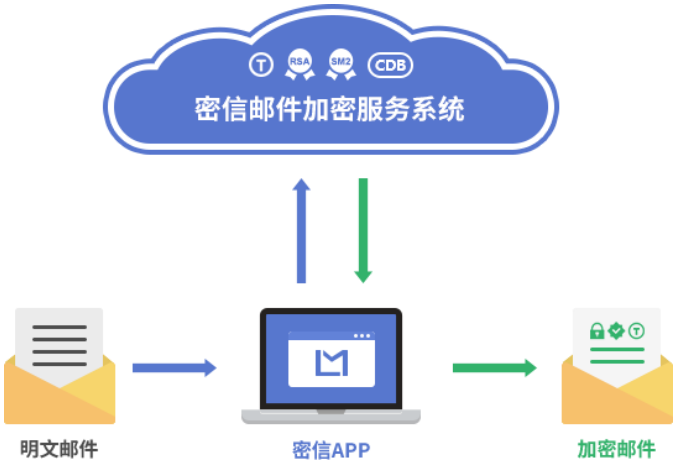
正是邮件加密的第一道坎-“申请证书”把用户拦在了高高的门槛外！更不用说拿到邮件证书后的许多坎了，拿到证书要发加密邮件必须事先同收件人交换公钥，证书过期又需要重新申请新的证书，还需要保管已经过期的邮件证书用于解密以前加密的邮件等等，这些繁琐的邮件加密实现过程从申请邮件证书开始，可以说就是一场永不停止的噩梦，人生都很不易，谁还会愿意为了邮件加密这点事去伤这么大的神哦！这就是为何 S/MIME 邮件加密标准已经诞生了 21 年，但还没有被普及应用的根本原因。

可是，人类必须进步，邮件必须加密，怎么办？密信技术除了彻底解决了公钥交换和密钥管理两大难题外，我们也彻底解决了申请证书的难题。由于用户需要的是邮件加密，所以，我

们把申请证书过程放到了后台，由邮件客户端软件-密信 App 来自动完成，用户只需设置好邮箱，登录自己邮箱就已经自动配置了邮件证书，就可以马上发送加密邮件了。也就是说，我们的邮件加密解决方案就没有让用户申请邮件证书这个环节，也就是无感地跨过了邮件加密第一道门槛。

那么，密信技术是如何实现为密信 App 用户全自动配置邮件证书的呢？当然首先需要有云 CA 服务，这是密信云密码基础设施的重要组成部分之一，其次就是要有云密钥管理服务，再就是必须有云公钥库。最后就是必须有邮件客户端软件来连接云密码服务实现自动为用户配置邮件证书。这就是为何密信技术必须研发邮件客户端软件的原因，因为目前市场上没有一个邮件客户端软件能自动为用户申请和配置邮件证书。

用户只需下载安装密信 App，设置自己的邮箱账户，密信 App 就会自动连接云 CA 系统和云密钥管理系统获取绑定用户邮箱的加密证书和签名证书，并自动配置好用于邮件加解密，并把用户的加密公钥提交到云公钥库，让其他密信 App 用户能自动获取其公钥，自动发送加密邮件给该用户。对用户来讲，使用密信 App 作为邮件收发的客户端软件根本就没有要求用户去 CA 申请证书这一步！全部由密信 App 连同密信云密码基础设施一道自动完成，邮件加密的第一道坎就这么轻松地迈过去了！



行文到此，本文就可以结束了。但是，笔者还想给读者多分享一些技术细节。目前，全球各大 CA 签发给用户的邮件证书都是单证书(同时含加密和数字签名用途)，这个解决方案的好处是用户只需管理一张证书。但是，如果采用云密码服务来解决邮件加密难题的话，单证书就有问题了，因为加密只需要证书的加密用途，不需要签名用途，按照最少化原则，只需要把加密证书密钥托管在云密钥管理系统即可。

所以，密信技术把传统的一张邮件证书拆分为两张证书(一张签名证书和一张加密证书)，加密证书密钥在云端生成并安全加密托管在云端，用户在完成邮箱控制权验证后就可以自动从云端取到加密密钥和加密证书来自动解密已加密邮件，使得用户无需费时费力申请和导入邮件

证书，完美实现全自动邮件加解密。而签名证书由于有用户的身份信息，用户的签名行为具有法律效力，所以，密信技术把签名证书设计为用户在本地设备上生成密钥，并在本地设备上加密保存密钥。这就是为何密信 App 用户看到在不同设备上的签名证书的序列号是不一样的原因。

密信技术把传统的一张邮件证书拆分成两张证书，并根据签名和加密的两个不同用途采用不同的密钥管理方式，完美地解决了 S/MIME 邮件加密服务的易用性问题，同时继承了 S/MIME 邮件签名的不可假冒、不可伪造和不可抵赖的特点，使得 S/MIME 邮件加密技术真正能实现零门槛无缝使用，用户无需关心证书是怎么来的和证书在哪，只需像平常一样写好邮件点击发送即可，实现全自动发送加密邮件和自动解密已加密邮件。

最后，再给大家分享多一点，本文话题是申请证书，密信 App 不仅支持由密信云 CA 签发的邮件证书的全自动申请和配置使用，默认自动配置的邮件证书是完全免费的；而且还支持自动申请和配置由其他CA签发的邮件证书，密信邮件加密服务入门版就是自动配置全球知名CA-Sectigo 的邮件证书，我们称之为 Vp 邮件证书，这是收费服务。为何需要自动配置这张证书？因为此证书是全球信任的邮件证书，用此证书发送的签名邮件，常用的邮件客户端软件，如 Outlook、雷鸟和苹果邮件，会显示数字签名可信。也就是说，免费自动配置的邮件证书仅密信信任，而自动配置的收费的 Vp 邮件证书则是全球信任。密信 App 不仅解决了自家 CA 自动为用户配置邮件证书的难题，同时也实现了其他家 CA 也能自动为用户配置邮件证书。密信技术采用了同其他邮件客户端一样的 S/MIME 邮件加密技术，实现了邮件加密和数字签名的互通加解密。

好了，最后总结一下，邮件加密有三道坎，密信技术通过建设了云密码基础设施，并研发了邮件客户端软件-密信 App，云地两端紧密结合，创新地完美地帮助用户顺利轻松迈过了这三道坎，使得用户可以使用密信 App 可以像处理明文邮件一样轻松发送加密邮件和解密已加密邮件。只有这样，才能让邮件加密得到普及应用，才能让电子邮件安全地造福人类的生活和工作。

----------END----------

ceo@mesign.com

想联系我讨论此话题？请使用 密信 App（ - ）扫码发加密邮件给我，我一定会回复您的加密邮件。