零信浏览器是如何实现密钥管理自动化的？

邮件加密有三大难题：证书申请、交换公钥和密钥管理，本文讲清楚零信浏览器是如何解决密钥管理难题的，是如何实现密钥管理自动化的。

一、什么是密钥管理？需要管理什么？为何是一个难题？

密钥管理是指管理邮件加密用的私钥，公钥已经有了零信公钥交换系统来管理。那么，邮件加密的核心—私钥应该怎么管理呢？密钥管理包括密钥的生成、使用、保管和更新多个环节，并且只要已加密邮件还有保留的价值，就要一直保管好私钥，以便随时用于解密已加密邮件。所以，保障密钥安全是邮件加密的核心工作之一，也是邮件加密中最重要的工作。

传统方式的邮件密钥管理，就是全部由用户手工管理，用户向 CA 申请邮件证书时，本地电脑生成私钥和 CSR 文件，提交 CSR 给 CA 申请证书，拿到 CA 签发的公钥证书后手动或者自动合成为含有私钥和公钥的证书文件(.pfx/.p12)，并且必须为这个证书文件设置一个保护口令。用户需要保管好这个证书文件和证书保护口令，每次在各种邮件客户端导入使用证书时必须要输入这个保护口令，如果忘了保护口令就等于这张证书废了，所有用这张证书加密的邮件都再也打不开了。这就是密钥管理的重要性，管理不好急死人，因为有些邮件内容很重要，但是急用时打不开了，会后悔当初加密了。

也就是说，传统邮件加密需要用户自己保管好证书私钥文件和保护口令，需要同时在多台设备上备份证书文件，因为如果一台电脑系统坏了，密钥就彻底没有了！就再也无法解密已加密的邮件了。这就是密钥管理的难点和痛点，必须解决这个难题才能让用户放心使用邮件加密服务。

二、只有实现了密钥管理自动化才能实现普及邮件加密

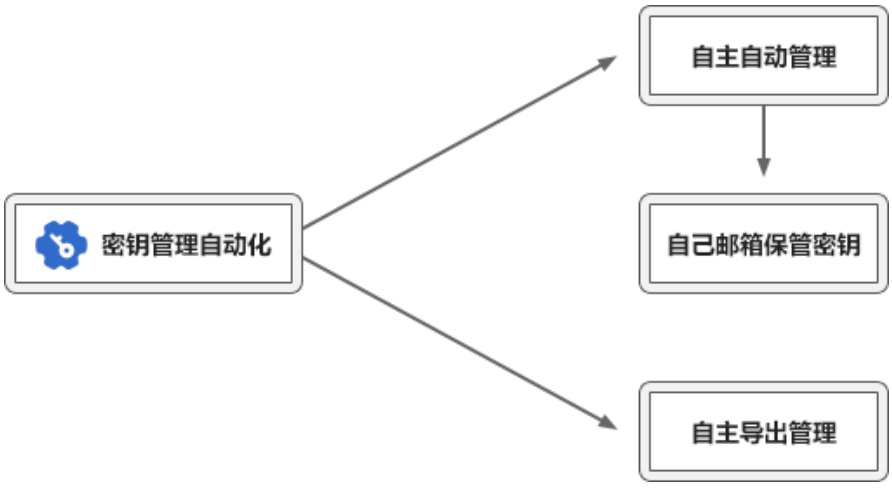
怎么解决密钥管理难题呢？用户在自己的电脑保管密钥，不仅管理难，而且万一电脑坏了，密钥也就没有了。唯一的出路还是要用云服务，因为我们可以假定云服务是一直可用的，在云上保管密钥是一个好主意，各大知名的云服务提供商都提供收费的密钥管理服务。

但是，零信浏览器并不打算为用户提供云密钥管理服务，因为零信技术推崇的产品理念是

零信任理念，保管用户的密钥不仅责任重大，而且有可能遭遇用户的信任危机，用户有可能不信任我们的密钥管理服务而弃用我们的服务，这是一个吃力不讨好的方案。但是，用户不想自己费力管理密钥，需要有密钥管理解决方案来解决密钥管理难题，怎么办？

零信浏览器创新地给出了解决方案—把用户的包含私钥密钥和公钥证书的证书文件(.pfx)作为一个邮件附件自动发送一封明文邮件到用户自己邮箱中保管，也就是实现了用户自己保管自己的密钥，并且是在云中保管，不会丢失，除非用户邮箱的邮件服务提供商破产倒闭了，这是大概率不可能的事情。之所以是明文邮件，当然是为了用户重装零信浏览器或者在新设备上安装零信浏览器时必须能明文获取到这封邮件并自动获得证书私钥而重新安装证书用于解密已加密邮件和用于发送加密邮件。

当然，为了保护密钥安全，这封明文邮件中保存的密钥文件必须有加密措施，这是一个采用私有算法实现的加密，此证书备份邮件仅用于零信浏览器，零信浏览器在备份 PFX 格式证书文件到用户邮箱时会自动创建一个名为 ZTBrowserOnly 的文件夹，并把密钥备份邮件保存在这个文件夹中，以便零信浏览器能快速自动获取用户密钥在新设备上使用。用户务必不能删除此文件夹和文件夹中的所有邮件，零信浏览器如果找不到这个文件夹或找不到密钥文件邮件，则会认为该用户没有邮件证书，会自动签发新的邮件证书并备份到这个文件夹中。如果以前有邮件证书并且有已加密邮件，则就无法实现自动解密已加密邮件了，除非用户自己已经备份了证书文件，并且可以导入使用。如果导入成功的话，零信浏览器仍然会重新自动备份密钥到用户邮箱中。



本着零信任安全理念，如果用户不想继续使用零信浏览器提供的邮件加密自动化服务，随时可以使用零信浏览器提供的一键导出所有证书(包括私钥)的功能，导出证书后就可以手动导入证书到其他支持 S/MIME 标准的邮件客户端中使用，就可以解密以前使用零信浏览器加密

的所有电子邮件，彻底解除用户担心被绑死使用的担忧，这也是其他采用封闭私有协议实现电子邮件加密所无法比拟的优势。

零信浏览器创新密钥管理方案既实现了密钥管理自动化，又解决了由第三方管理密钥的安全担心，同时解决了用户自己管理密钥有可能丢失的难题，是一个把用户邮箱作为密钥安全保管箱的创新方案，彻底搞定密钥管理自动化难题，是一个鱼和熊掌兼得的方案。只有搞定密钥管理自动化，才能真正实现邮件加密自动化，才能普及邮件加密应用。

三、邮件证书自动化、公钥交换自动化、密钥管理自动化，缺一不可，浑然天成，零信巨献

S/MIME 邮件加密技术之所以无法得到普及应用，就是因为这项技术很难落地应用，主要难在证书申请、交换公钥和密钥管理三个方面，而要解决这三个难题只有自动化一条路。零信浏览器的邮件证书自动化、公钥交换自动化和密钥管理自动化彻底解决了这三个难题，这是一个端云一体的创新解决方案，三者缺一不可，浑然天成，这是零信技术在邮件安全方面为全球邮件安全做出的巨献，一定会收到全球邮件用户的欢迎，大家齐努力共同打造一个零欺诈的安全邮件世界，让古老的去中心化的电子邮件服务继续更好地造福人类。

王高华

2024 年 11 月 7 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 189 篇(共 53 万 9 千多字)和英文 78 篇(9 万 9 千多单词)。