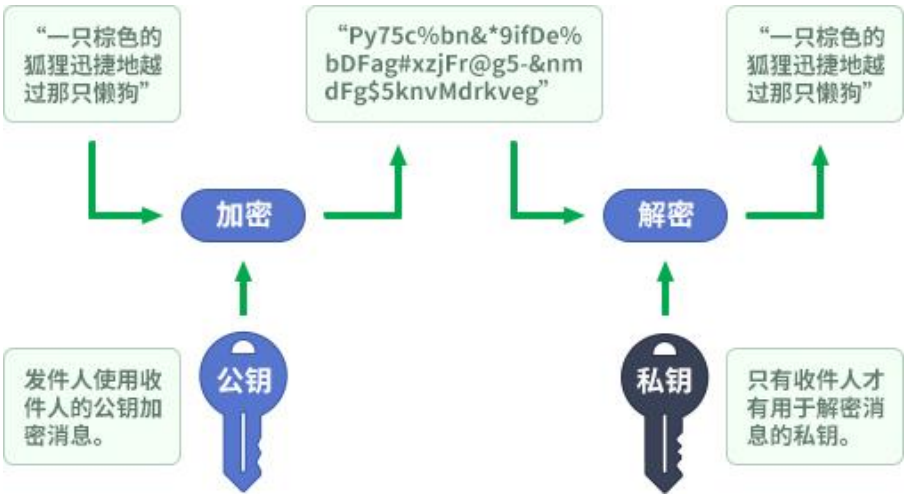
零信浏览器是如何实现公钥交换自动化的？

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公钥交换难题的，是如何实现公钥交换自动化的。

一、什么是公钥交换？为何公钥交换是一个难题？

PKI 技术的神奇之处就是公钥和私钥的设计，也就是俗称的“两把钥匙开一把锁”，因为“一把钥匙开一把锁”无法解决如何把钥匙给对方的难题。而两把钥匙的设计巧妙在于公钥是可以公开通过各种渠道获取的，私钥才是只能自己拥有的，公钥和私钥结合就可以实现加解密，而不用像一把钥匙那样必须把整个钥匙都给对方。如下图所示，先讲一下邮件加密的技术原理。发件人使用收件人的公钥加密信息，把明文信息变成密文，就可以安全地发给收件人了，无论双方的邮件服务器是否采用了 TLS 传输加密。收件人收到密文后用自己的私钥就可以解密已加密的消息。这就是非对称加密，不像对称加密那样双方共用一把钥匙。



问题来了，发件人应该如何拿到收件人的公钥呢？这就要求双方交换公钥，只有交换了公钥双方才能实现相互邮件加密。而传统的交换公钥是通过向收件人发送一封数字签名邮件实现的，对方也回复一封数字签名邮件就完成的公钥交换。这个过程看起来非常科学，也非常简单。其实，实现起来并不容易，试想一下，你有 100 个联系人，就得同这 100 个联系人交换公钥，

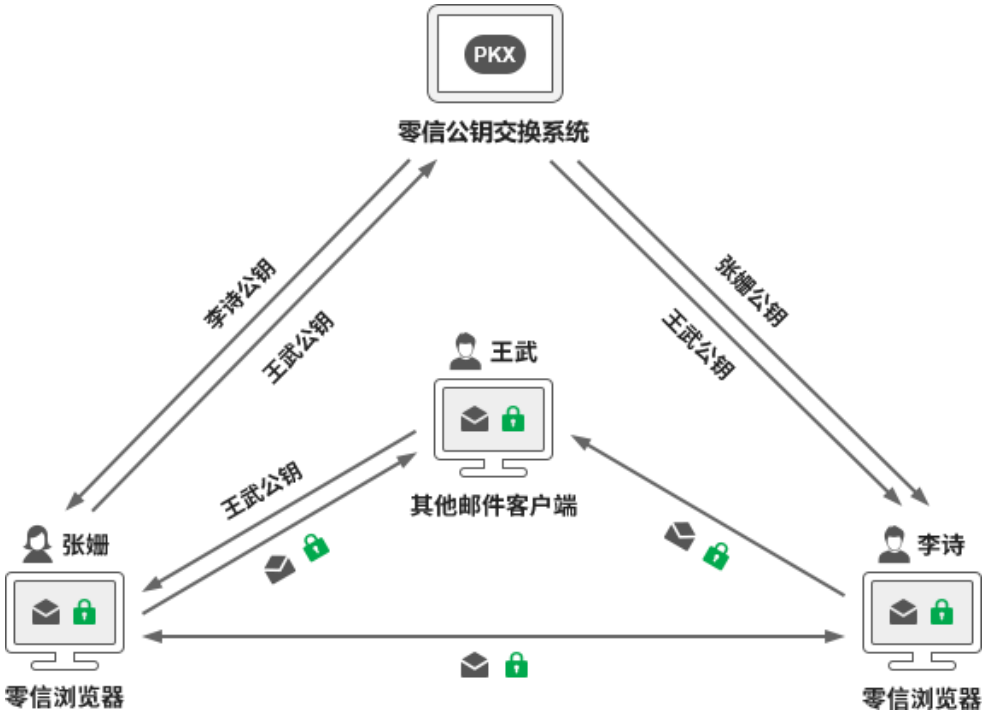
前提是这 100 个人也有邮件证书，如果收件人没有邮件证书就无法交换公钥，无法实现邮件加密。

即使双方交换了公钥，为了密钥安全，邮件证书最长只能是两年有效期，也就是说，每两年又要同这 100 个联系人重新交换公钥。完成交换公钥后还需要按照邮件客户端的要求配置到收件人通信录中，以便邮件客户端能调取公钥发送加密邮件。

二、 只有实现了公钥交换自动化才能实现普及邮件加密

以上人工手动交换公钥的方式是效率最低的交换方式。如果张珊有 100 个联系人，需要交换 100 次，1 亿邮件用户就要交换 100 亿次。但是，如果有一个第三方的公钥管理数据库提供公钥管理服务，每个人只需给公钥数据库提交一次自己的公钥即可，需要某个人的公钥时由邮件客户端直接从公钥数据库获取即可，这就省去了事先交换公钥的操作。这就是提高公钥交换效率的解决方案，零信技术已经建设了公钥交换系统免费为所有零信浏览器用户提供公钥交换自动化服务。

笔者在博文《零信浏览器是如何实现邮件证书自动化管理的？》讲解了零信浏览器是如何自动化为用户配置邮件证书的，所有为用户签发的邮件证书公钥都自动写入公钥交换库，这样零信浏览器用户之间发送加密邮件就无需事先交换公钥。如下图所示，张珊直接从公钥交换系统获得李诗的公钥就可以直接给李诗发送加密邮件给李诗，而无需事先同李诗交换公钥。李诗也是从公钥交换系统获得张珊的公钥而直接给张珊发送加密邮件。



但这还不够，如果零信浏览器用户张珊需要向其他支持 S/MIME 的邮件客户端的用户王武发送加密邮件怎么办？当然，需要张珊和王武采用传统的手动发送一封数字签名邮件方式交换公钥，这样，张珊就可以发加密邮件给王武了。同时，零信浏览器会自动提交王武的公钥到零信公钥交换数据库，这样所有零信浏览器用户，如李诗，就不再需要同王武交换公钥了，李诗可以从公钥交换系统自动获取王武的公钥，自动发送加密邮件给王武而无需事先同王武交换公钥，这就大大提高了传统的手动交换公钥机制的交换效率。

也就是说，随着零信浏览器用户的不断增加，用户需要手动同其他非零信浏览器用户交换公钥的几率就越来越小。但是，鉴于目前拥有邮件证书的用户仍然是少数，如果零信浏览器用户需要给一个没有邮件证书的用户发送加密邮件怎么办？或者说，零信浏览器用户不知道收件人是否有邮件证书，也不想手动发送一个数字签名邮件给收件人交换公钥，怎么办？零信浏览器有一个默认的无需手动交换公钥的机制，用户不用关心收件人是否有邮件证书，也无需问收件人是否有邮件证书，也无需手动交换公钥，可以直接给任何人发送加密邮件。一旦零信浏览器无法从公钥交换数据库获取到收件人的公钥，则临时自动为收件人生成一个密钥对(私钥和公钥)，用这个临时公钥加密邮件自动发送加密邮件给收件人，零信浏览器同时自动以发件人的名义给收件人发送一封明文邮件，告诉收件人如何才能解密发件人给他/她发送的加密邮件。收件人只需下载安装零信浏览器，启用邮件加密自动化服务，即可使用零信浏览器登录自己的邮箱查看已经自动解密的加密邮件了。

这就是零信浏览器提供的公钥交换自动化服务，让用户无需关心收件人是否有邮件证书，也无需事先同收件人交换公钥，可以直接使用零信浏览器给所有邮件用户发送加密邮件，收件人一定能解密阅读加密邮件，并且是由收件人自己使用零信浏览器免费自动配置的邮件证书本地自主解密，而不是云服务模式解密阅读。

有了零信公钥交换系统的支持，零信浏览器就可以在发送加密邮件时把收件人的所有公钥都加到收件人密钥列表中，包括零信浏览器自动配置的邮件证书和其他 CA 签发的邮件证书，这样就可以保证收件人使用任何设备的任何邮件客户端都可以解密这封加密邮件，做到了加密邮件的最大兼容支持。

三、 零信浏览器提供的邮件证书自动化加上公钥交换自动化，为普及邮件加密扫除了技术障碍

用户只需下载使用零信浏览器免费提供的邮件加密自动化服务，就可免费自动申请和配置 4 张电子邮件证书和 2 张电子邮戳证书，这些证书可用于邮件加密服务。而要想实现邮件加密，

还得有收件人的公钥，这就是零信浏览器免费提供的第二个自动化服务—公钥交换自动化服务。有了这两个自动化服务，用户就可以像平时发送明文邮件一样向所有邮件用户发送加密邮件了，用户无需关心如何向 CA 申请证书，也无需关心同所有收件人交换公钥，无感地收发加密邮件，所有邮件都实现了端到端加密，并以密文形式存放在云端邮件服务器中，切实保障电子邮件的在途安全和在云安全。

零信技术免费提供的邮件证书自动化和公钥证书自动化，使得全球用户可以零成本地无感地向任何邮件用户发送加密邮件，为普及邮件加密扫除了技术障碍，剩下的工作就是大家都用起来，切实保护个人邮件机密信息安全和单位邮件商业秘密安全。

王高华

2024 年 11 月 4 日于深圳

2024.11.04
15:58:52
+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 188 篇(共 53 万 7 千多字)和英文 77 篇(9 万 8 千多单词)。