邮件加密的第二道坎是公钥交换

(2021 年 4 月 6 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。这道坎如何迈过，留待下一篇博文详细讲。

第二道坎是公钥交换，如果邮件收发双方都过了第一道坎，都有了邮件证书，就必须相互之间先发送一封数字签名邮件来实现公钥交换，只有交换了公钥，发件人才能用收件人的公钥发送加密邮件给收件人。本文就讲讲如何轻松迈过这道坎。至于第三道坎，那就是密钥管理，这个坎也留给后面的文章细讲。

对于邮件加密的三道坎，为何笔者先讲第二道坎呢？因为公钥交换是 S/MIME 邮件加密的最关键和最繁琐的一步，如果没有这一步，即使大家都有邮件证书，也无法实现邮件加密。也正是由于这个繁琐的密钥交换机制导致了邮件加密无法普及应用。必须彻底解决公钥交换难题才能实现全自动邮件加密，才能普及邮件加密应用。

那么，该如何迈过邮件加密的第二道坎？先讲一个真实故事吧。笔者曾在一次国际会议上向坐在旁边的一位与会者(就叫他 Jason 吧)推荐使用密信 App，我让他直接使用密信 App 发送加密邮件给正在演讲的那位先生(就叫他 Andy 吧)，因为演讲人的 PPT 上公布了他的邮箱。Jason 说我没有同演讲人 Andy 交换过公钥哦，怎么发送加密邮件给他。我就告诉 Jason，使用密信 App 发送加密邮件不用事先交换公钥，他将信将疑地使用密信 App 给演讲人发送了加密邮件，并提示发送成功。演讲人回到观众席后也回复了加密邮件，是使用 Outlook 回复的。这就让 Jason 非常好奇，问我密信 App 是如何做到无需事先交换公钥的，我就同他讲了我们的解决方案，他现在成为了密信 App 的铁粉。本文就是要同读者分享一下我们是如何做到的。

密信技术的解决方案是创新地建设了全球公钥库。密信 App 作为一个邮件客户端软件，会自动收集用户同其他收件人邮件通信时使用的公钥，并自动同步到云端全球公钥库中，这样使得用户在输入收件人邮箱后，密信 App 可以自动从云端公钥库获取收件人的公钥，只有这样，才能实现用户无需事先同收件人交换公钥，“云”“地”一体，共同实现全自动邮件加密。

说回上面的故事，由于我以前给演讲人 Andy 发送过加密邮件，也就是说，我同演讲人交换过公钥，虽然他是用 Outlook 和使用自家 CA 签发的邮件证书，但是我使用密信 App 给他发加密邮件时，密信 App 就已经自动同步了他的公钥到密信全球公钥库中。所以，Jason 在使用密信 App 写邮件给演讲人时，密信 App 会自动连接云端公钥库而自动获得演讲人的公钥，从

而实现无需事先交换公钥就可以自动发送加密邮件。

还是眼见为实吧，如下图所示，用户在收件人栏输入密信客服邮箱后，双击邮箱就会弹出客服邮箱的加密证书信息，也就是说已经成功获取收件人的加密公钥，就可以点击“发送”给收件人发送加密邮件了。

当然，仅仅只是收集用户使用过的公钥是不够的，因为毕竟有公钥的用户目前还是非常少的，所以，密信技术建设了云密码基础设施，为用户提供了云 CA 服务和云密钥管理服务，自动为密信 App 用户免费签发邮件证书，并自动配置使用邮件证书，实现全自动邮件加密和数字签名。这样，凡是使用密信 App 作为邮件客户端的用户的公钥就不用收集了，在给用户签发邮件证书时直接写入公钥库即可。

相信读者从以上介绍就能了解为何密信技术能实现全自动邮件加密了，是因为我们建设了公钥库，并由密信 App 自动连接公钥库获取收件人的公钥。而目前大量的由各种管理信息系统自动发送的电子邮件都是明文邮件，如：银行给用户发送了大量的信用卡账单、对账单等重要的含有用户机密信息的邮件，但都是明文邮件，这是一个巨大的安全隐患。还有，各种电子政务系统也要给市民发送大量的办事结果通知邮件，包括我国日益普及的电子发票邮件，这些都是明文邮件。

那么，怎样保证这些由管理系统自动发送的含有大量机密信息的电子邮件的安全？当然是应该发送加密邮件给用户。但如何发送？密信技术提出了可行的解决方案，那就是免费开放我们的全球公钥库，让业务管理系统在给用户发送业务邮件时先调用密信公钥 API，免费获取收件人的公钥，就可以自动给用户发送加密邮件了。

密信技术之所以愿意免费开放加密公钥库给全球用户，包括政府机构、公共服务机构、金

融机构、企业和其他邮件客户端厂商，是因为密信技术有一个实现“邮件全加密”的梦想，希望能同各个邮件相关方一道共同推广邮件全自动加密的普及应用，共同保护全球用户的邮件机密信息安全，共同努力提升全球互联网安全，为互联网造福人类共同努力。

最后，给读者留一个思考题：如果某人既没有任何 CA 签发的邮件证书，也没有使用密信 App (没有密信 CA 自动签发的邮件证书)，也就是说，他/她根本就没有任何邮件证书。那么，使用密信 App 给这个人发加密邮件，密信 App 是如何获得这个人的公钥的？

这个思考题的答案是密信技术的技术秘密(已申请发明专利)，是密信技术全球独创的解决方案，也是我们敢叫我们的公钥库为“全球公钥库”的底气。笔者可以毫不夸张地讲，您想给任何邮箱发送加密邮件，密信 App 都能为您自动获得其公钥！欢迎免费 下载 密信 App，享受完全免费的全自动邮件加密服务！

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

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。