邮件加密的第三道坎是密钥管理

(2021 年 4 月 9 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。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。

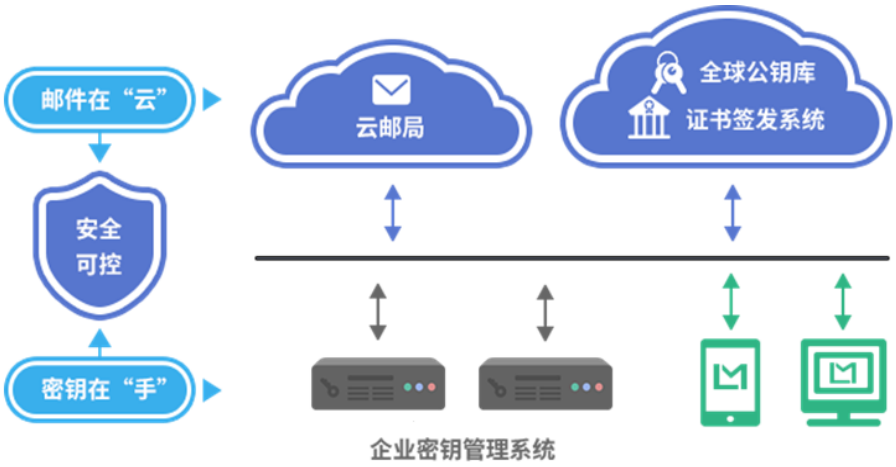
邮件加密的第三道坎是密钥管理，为何说这是一道坎呢？熟悉邮件加密的读者一定知道，目前的邮件加密是用户向 CA 申请邮件证书，由用户自己管理证书密钥，需要手动导入证书到各种邮件客户端和各种终端设备上使用，非常繁琐。如果证书到期了，又要申请新的邮件证书，而为了解密以前加密的邮件，则需要保管好已经过期的邮件证书。笔者在 15 年前就开始使用邮件证书加密邮件，现在由于各种原因无法找到以前的邮件证书了，导致即使以前的邮件都还在邮件服务器上，但是由于找不到加密证书而无法解密这些老邮件了，这就是邮件加密的烦恼，对于某个无法解密的重要邮件，甚至有些后悔当时不该加密此邮件！这就是邮件加密的一道坎 – 密钥管理，必须想办法迈过！

怎么迈？笔者想到了云服务，使用百度中文搜索“云密钥管理”，或使用谷歌英文搜索“cloud key management”，都能搜索出各大著名的云服务提供商提供的云密钥管理服务。密信技术在调研了这些云密钥管理服务后，决定建设了自己的云密钥管理系统，让用户可以随时使用邮件客户端软件-密信 App 自动获取绑定用户邮箱的加密密钥，实现随时随地使用任何设备都能解密已加密邮件，彻底解决由用户自己管理密钥时遭遇的困境。只有这样，才是解决了密钥管理难题，让用户无需费力配置邮件证书到现有的各种邮件客户端中使用，无需费力管理加密密钥，无需担心密钥丢失而无法解密已加密邮件。也只有这样，才能使得发送加密邮件和发送明文邮件一样轻松，才能真正普及邮件加密应用。

也就是说，密信技术的全自动邮件加密的实现是云密钥管理服务的成功落地应用，“云”“地”一体，让用户轻松迈过了邮件加密的第三道坎！笔者坚信：云密钥管理服务，一定会成为一个非常重要的云服务，因为为了保护各种云数据的安全，需要对数据进行加密和数字签名，而这些都离不开云密钥管理服务。

一个国外用户用了一个很形象的单词来表达他对密信解决方案的赞许 - “**lifesaver**”，查英文字典是这样解释的：a thing that saves one from serious difficulty. 如：a microwave oven could be a lifesaver this Christmas。可以形象地翻译为：这简直是在拯救生命哦。因为目前市场上其他家的邮件加密解决方案很难用，非要把人搞死还不一定能搞定，所以这个用户才说密信 App 是在救命！

而对于政府机构、金融机构或大企业，如果希望自己掌控加密密钥，不使用云密钥管理服务，密信技术也有解决方案，可以本地部署密信企业密钥管理系统，自己本地管理密钥。这样，密信 App 就会自动连接本地密钥管理系统去获取用户密钥，而不会连接密信云密钥管理系统，从而满足用户的本地自己管理密钥的需求，实现“邮件在云”“密钥在手”的邮件安全管理新模式。



总之，要想实现全自动邮件加密，必须使用密钥管理服务。密信技术免费为密信 App 全球用户提供云密钥管理服务，具有“**按需获取，随时可用**”、“**免费使用，普及加密**”、“**云地一体，解决难题**”等许多优势特点。而对于希望自己管理密钥的用户，密信技术也提供了可本地快速部署的企业密钥管理系统，让用户本地管理密钥，实现“邮件在云，密钥在手”，从而放心地使用云邮箱服务。

----------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。