

MEaaS，一个创新的云密码服务

(2021 年 3 月 18 日)

笔者相信许多读者对“**SaaS**”这个名词并不陌生，但考虑到可能有些非 IT 读者不了解，我先简单介绍一下 SaaS。**SaaS** 即 **Software as-a-Service** (软件即服务，通过网络提供软件服务)，SaaS 是随着互联网技术、云计算技术的发展和应用程序的成熟，在 21 世纪开始兴起的一种创新的软件应用模式。传统模式下，厂商通过卖软件许可将软件产品部署到企业内部多个客户端实现交付。SaaS 定义了一种新的交付方式，也使得软件进一步回归到服务本质。企业部署信息化软件的本质是为了自身的运营管理服务，软件的表象是一种业务流程的信息化，本质还是一种服务模式，SaaS 改变了传统软件服务的提供方式，减少本地部署所需的大量前期投入，进一步突出信息化软件的服务属性，已经逐渐成为了信息化软件市场的主流交付模式。

对于邮件加密来讲，传统模式下，软件厂商研发邮件客户端软件，支持 S/MIME 技术实现邮件加密和数字签名。用户免费或者收费方式把邮件客户端软件部署到企业内部多个客户端实现交付使用，同时用户还需要另外向 CA 厂商购买和申请邮件证书，并费力地给每个客户端配置使用邮件证书，还需要发件人同收件人交换公钥才能实现邮件加密，从而保障邮件内容的全程安全。

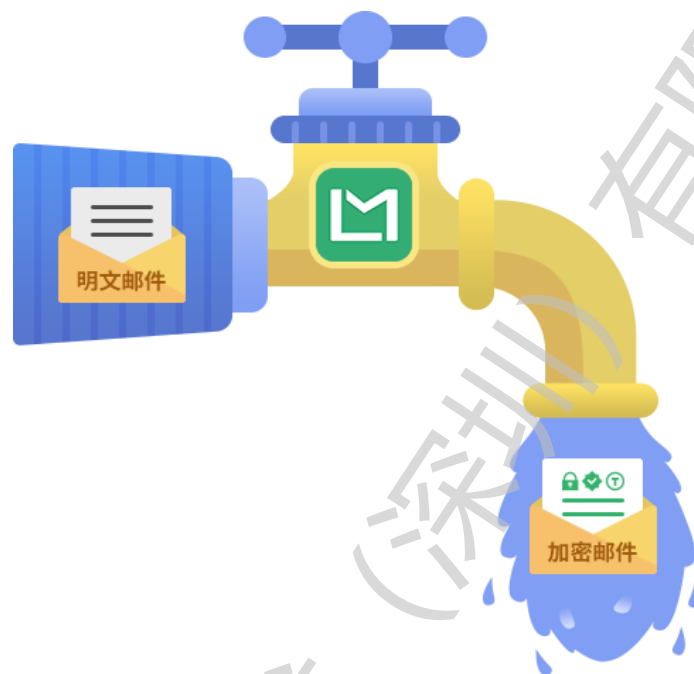
可以看出，传统的邮件加密解决方案是非常繁琐和很难实现的，这就导致了大家明明知道邮件是明文传输，不安全，需要加密。但是，由于 S/MIME 邮件加密技术太麻烦而不得不放弃邮件加密，任由不安全的明文邮件继续存在。笔者认为：这是“掩耳盗铃”或者说是“鸵鸟思维”。

当然，也有厂商试图去解决这个邮件加密难题，如 PGP 加密或 SM9 加密，不采用繁琐的 S/MIME 加密技术，不依赖于第三方 CA 签发的邮件证书来实现加密，用户可以自己制作一张加密证书来实现加密，但仍然逃不脱需要实现交换公钥的难题，并且并没有解决如何证明邮件发送者可信身份的问题。

密信技术通过多年的努力探索，找到了一个创新的解决方案，让邮件客户端软件回归到服务的本质。用户需要的加密邮件，是邮件加密服务，而不是需要邮件证书，也不需要一个不支持加密的邮件客户端软件。密信技术研发了加密邮件客户端软件，并建设了云密码基础设施，“云”“地”结合，使得用户无需向 CA 申请邮件证书和无需事先同收件人交换公钥，就可以自动发送加密邮件。这个解决邮件加密难题的思路同 SaaS 一样，所以，我们称之为“**MEaaS**”。

MEaaS 就是 **Mail Encryption as-a-Service**，邮件加密即服务，也就是密信技术为全球用

户提供的邮件加密服务。这是一个创新的云密码服务，使得非常复杂难用的 S/MIME 邮件加密技术变成了非常容易和非常好用的邮件加密技术，让用户发送加密邮件就像发送明文邮件一样容易，只有这样，才能真正普及邮件加密应用，才能真正保障电子邮件的全生命周期安全。密信技术使得邮件加密服务作为一个云服务(MEaaS)，就像自来水一样随时可用。





最后，我再详细讲一下 MEaaS 整个实现过程。用户只需下载和安装密信 App，并设置好自己的邮箱账户，剩下的事情都是由密信 App 来完成全部邮件加密工作。密信 App 会自动连接云密码基础设施的验证系统，自动完成邮箱控制权验证后自动向云 CA 系统和云密钥管理系统申请邮件证书，自动获取邮件加密证书和邮件签名证书，并自动配置可用于邮件加密和数字签名。而用户在密信 App 输入收件人邮箱后，密信 App 就会自动连接云公钥库获取收件人的加密公钥，使得用户无需事先同收件人交换公钥就能直接发送加密邮件，邮件发送时会自动附署发件人的数字签名以证明发件人的可信身份，并自动连接云时间戳服务获取时间戳签名以证明邮件发送时间可信和不可篡改。

整个过程看起来也许您会感觉有点复杂，但是就像自来水一样，您无需关心水是怎么来的，您只需打开水龙头，水就会来。您只需使用密信 App 写邮件，点击“发送”就能发送加密邮件！

MEaaS，一个创新的云密码服务，全球只有密信技术独家提供！欢迎 [下载](#) 密信 App 免费体验 **MEaaS**！

-----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。

© 2021 密信技术 (深圳) 有限公司