一文搞懂 S/MIME 邮件加密 (一)

市场上的邮件加密解决方案五花八门，零信浏览器采用了基于 S/MIME 国际标准的技术路线。本文讲清楚 S/MIME 技术是如何实现电子邮件加密和数字签名的，以帮助用户理解 S/MIME 的魅力,并正确选择邮件加密解决方案。同时讲清楚零信浏览器是如何解决 S/MIME 技术的落地应用难题的，让用户见到 S/MIME 就 SMILE。

一、S/MIME 发展历史

要讲清楚什么是 S/MIME，得先讲清楚什么是 MIME，就像要想讲清楚什么是 HTTPS，必须先讲清楚什么是 HTTP 一样，这两个互联网最常用的协议中的 **S** 是英文 Secure(安全)的第一个字母，HTTP 是超文本明文传输协议，HTTPS 就是超文本加密传输协议。

MIME 是 Multipurpose Internet Mail Extensions (多用途互联网邮件扩展)的缩写，这一个扩展电子邮件格式的互联网标准，让仅支持英文 ASCII 字符的电子邮件可以发送 ASCII 以外的字符集的文本，并且可以以附件方式发送音频、视频、图像和应用程序等各种格式文件。具有 MIME 格式的电子邮件使用标准协议进行传输，如简单邮件传输协议(SMTP)、邮局协议(POP)和互联网邮件访问协议(IMAP)。尽管 MIME 格式主要是为 SMTP 设计，但其内容类型在其他通信协议中也都在使用，如 HTTP 协议，Web 服务器在任何 Web 传输的开头都会插入一个 MIME 标头字段，客户端使用内容类型或媒体类型标题为指示的数据类型选择适当的应用程序。

S/MIME 是 Secure/Multipurpose Internet Mail Extensions (安全/多用途互联网邮件扩展)的缩写，就是安全收发电子邮件，采用密码技术实现电子邮件的数字签名和加密。S/MIME 的第一个版本是由许多安全供应商于 1995 年开发的，但没有形成标准，1998 年发布了 S/MIME V2 版本，并提交 IETF 形成了 RFC 2311 和 RFC 2312 国际标准，前者建立了消息的标准，后者建立了证书处理的标准。这两个 RFC 标准共同提供了一个基于互联网标准的框架，所有相关厂商就可以遵循该框架来提供可互操作的消息安全解决方案，使得 S/MIME V2 版本成为了电子邮件安全标准。IETF 于 1999 年又提出了 S/MIME V3 版本-RFC 2632 (证书处理)、RFC 2633(消息规范)和 RFC 2634(增强安全服务)，在 V2 版本基础上增强了 S/MIME 功能。2004 年发布了

S/MIME V3.1 版本-RFC 3851(消息规范)，这是 RFC 2633 的升级版本，2010 年发布了 S/MIME 3.2 版本-RFC 5751(消息规范)，是 RFC 3851 的升级版本，2019 年发布了 S/MIME V4.0 版本-RFC 8551 (消息规范) 是 RFC 5751 的升级版本，这是最新的版本。这些标准规范都是基于加密消息语法标准(CMS，RFC 5652)，与 PKCS #7 大致相同。S/MIME V3 版本增强功能之一是“三重包装(triple-wrapping)”。三重包装的 S/MIME 邮件是先签名、再加密、再次签名，这样能保证加密后的邮件主体数据的完整性。而 S/MIME V4 版本主要是增加了 ECC 算法支持。

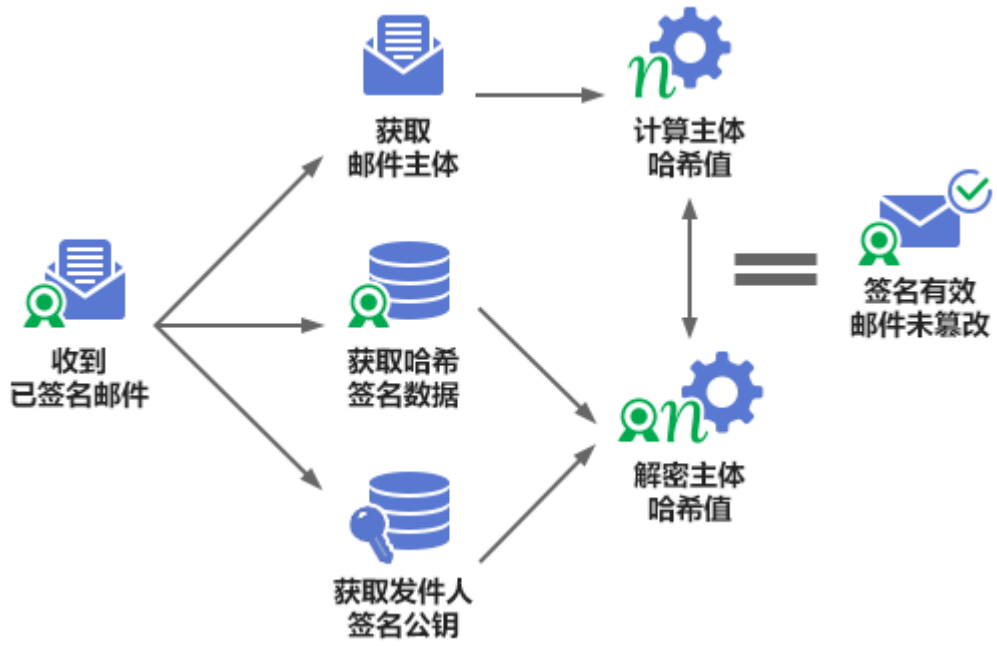
二、S/MIME 数字签名

数字签名是 S/MIME 第一个主要功能。顾名思义，数字签名是纸质文档上传统手写签名的数字对应物。与手写签名一样，电子邮件 S/MIME 数字签名提供以下安全功能：

- **身份验证**：数字签名用于验证身份，回答“你是谁”，证明实体的唯一性。由于明文 SMTP 电子邮件中没有身份验证，因此无法知道真正是谁发送了邮件。数字签名中的身份验证解决了这个难题，它让收件人确信电子邮件的确是由声称的发件人发送的。
- **不可否认性**：数字签名的唯一性可防止签名者否认该签名。此功能称为不可否认性，数字签名提供的身份验证提供了强制执行不可否认性的手段，在某些领域越来越多地被认可为具有法律约束力，类似于纸质手写签名的不可否认，解决了明文 SMTP 电子邮件发送无法提供不可否认性的难题。
- **数据完整性**：数字签名提供的另一项安全保证是数据完整性。借助数据完整性，当数字签名电子邮件的收件人验证数字签名时，收件人可以确信收到的电子邮件在传输过程中没有被篡改。因为数字签名后，在传输过程中对邮件的任何篡改都会使数字签名无效。通过这种方式，数字签名提供了纸质手写签名无法提供的保证，因为纸质手写签名在签名后可能会有不被发现的篡改。

如下图所示为 S/MIME 数字签名邮件的发送流程图，由电子邮件客户端软件采用 SHA-2 或 SM3 算法计算邮件主体的哈希值，再用发件人的私钥签名哈希值，再把这个哈希值作为数字签名附加到邮件主体中，再加上邮件头就可以发送已数字签名的电子邮件了。

如下图所示为 S/MIME 数字签名的验证流程图，收件人收到已签名邮件后，分别获取邮件主体、签名数据和发件人签名证书(公钥)，并使用发件人的公钥解密哈希签名数据得出邮件主体哈希值，再计算邮件主体的哈希值，比较这两个哈希值是否相同，如果相同，则签名有效，表明邮件未被篡改，邮件客户端会显示签名者身份信息。



这就是 S/MIME 数字签名的签名和验签过程，用户需要有 S/MIME 邮件证书才能完成电子邮件的数字签名，邮件客户端也必须支持 S/MIME 标准来验证数字签名。

尽管 S/MIME 数字签名提供了数据完整性，但它并不能保证机密性。仅有数字签名的邮件是以明文形式发送的，其他人可以阅读。即使是 Base64 编码的不透明方式签名，只能起到一定程度的混淆作用，但它仍然属于明文。为了保证电子邮件内容的机密性，必须使用 S/MIME 加密。

三、S/MIME 加密

S/MIME 加密是为了解决 SMTP 明文传输电子邮件的安全问题，任何人都有可能在电子邮件传输过程中非法获取电子邮件内容和非法篡改邮件内容，也可以在电子邮件服务器上查看明文邮件，特别是现在所有电子邮件都在云端。这些问题由 S/MIME 加密技术来解决。加密是一种信息变换的方式，使信息在恢复为可读且可理解的形式之前无法被阅读或理解。电子邮件 S/MIME 加密提供以下安全功能：

- **机密性**：电子邮件 S/MIME 加密用于保护电子邮件内容。只有预期的收件人才能查看内容，并且内容保持保密，任何其他可能接收或查看邮件的人都无法解密。S/MIME 加密可在邮件传输和存储过程中提供保密性。
- **数据完整性**：与数字签名一样，邮件加密也提供数据完整性保证，由于无法解密而保证了其完整性。

如下图所示为 S/MIME 加密邮件的流程图，电子邮件客户端软件必须首先获取收件人的公钥，再生成一次性对称会话密钥，并使用会话密钥对邮件主体进行加密，再用收件人公钥加密会话密钥，并把加密的会话密钥包含在加密邮件主体中，再加上邮件头等信息就可以发出已加密邮件。

如下图所示为 S/MIME 解密邮件的流程图，收件人收到已加密邮件后，分别获取加密邮件主体和已加密的会话密钥，用收件人私钥解密已加密的会话密钥，再用已解密的会话密钥来解密已加密的邮件主体，这样，收件人就可以查看已解密的邮件内容了。

这就是 S/MIME 的加密和解密过程，加密发送方必须通过一定的渠道获得邮件接收方的公钥，通常做法是收发双方各发送一封数字签名邮件而完成公钥交换。而接收方需要拥有 S/MIME 邮件证书私钥才能完成电子邮件的解密。

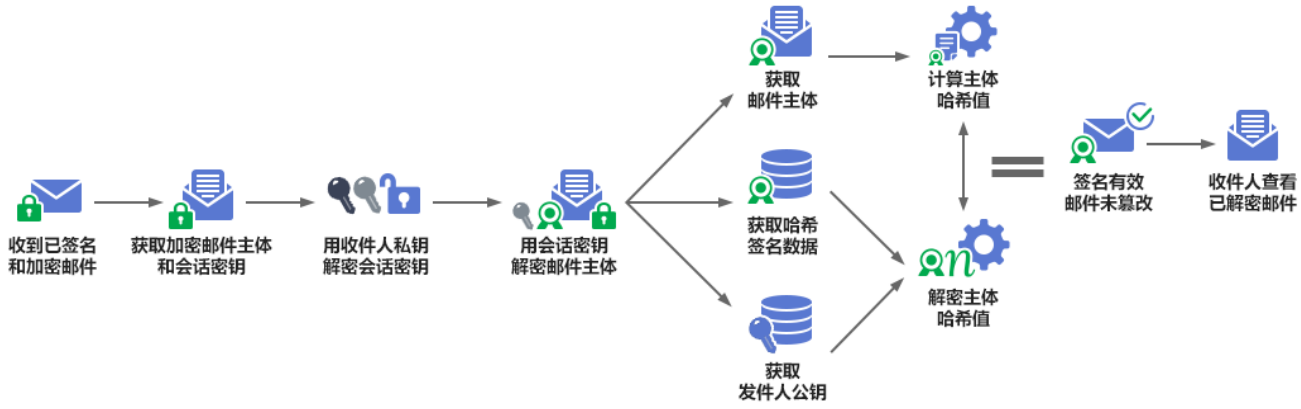
尽管 S/MIME 加密提供了机密性保证，但它不会以任何方式验证邮件发送者的身份。没有数字签名的加密邮件与没有加密的明文邮件一样容易被假冒发送者身份，并且邮件加密也不能提供不可否认性。尽管邮件加密也提供了数据完整性，但加密邮件只能显示消息自发送以来未被篡改，并不提供谁发送了邮件的身份信息。为了证明邮件发送者的可信身份，必须同时使用 S/MIME 数字签名。

四、S/MIME 数字签名和加密

正是因为 S/MIME 数字签名只解决了邮件内容的完整性问题和邮件发送者的可信身份问题，而 S/MIME 加密也只解决了邮件内容的机密性问题，所以，要想真正保证邮件安全，必须同时实现 S/MIME 数字签名和加密，只有这样才能同时解决电子邮件的机密性、完整性、不可否认性和身份验证等四大令人痛苦的邮件安全难题(**PAIN**，Privacy / Authentication / Integrity / Nonrepudiation)。

如下图所示为同时发送 S/MIME 数字签名和加密邮件的流程图，由电子邮件客户端软件计算邮件主体的哈希值，再用发件人的私钥签名哈希值，再把这个哈希值作为数字签名附加到邮件主体中，这就是完成了数字签名。接着获取收件人的公钥，生成一次性对称会话密钥，并使用会话密钥对已签名的邮件主体进行加密，再用收件人公钥加密会话密钥，并把加密的会话密钥包含在已签名和加密的邮件主体中，再加上邮件头等信息就可以发出已数字签名和加密的邮件。

如下图所示为验证 S/MIME 数字签名和解密已加密和数字签名邮件的流程图，收件人收到已加密和数字签名邮件后，分别获取加密邮件主体和会话密钥，并用收件人私钥解密已加密的会话密钥，再用已解密的会话密钥来解密已加密和已签名的邮件主体，这就完成了解密过程。再分别获取邮件主体、邮件主体哈希签名数据和发件人公钥，使用发件人的公钥解密哈希签名数据得出邮件主体哈希值，再计算邮件主体的哈希值，比较这两个哈希值是否相同，如果相同，则签名有效，表明邮件未被篡改。这样，收件人就可以查看已解密的邮件内容了，邮件客户端会显示签名者身份信息。



这里就不再讲三重包装的 S/MIME 邮件加密和数字签名实现过程了，同上面的基本原理一致，需要最后再增加一次数字签名和再验证一次，增强保护加密邮件的邮件主体数 据的完整性。

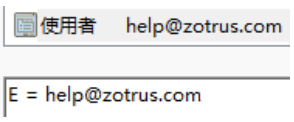
五、 S/MIME 邮件证书和 S/MIME 邮件客户端

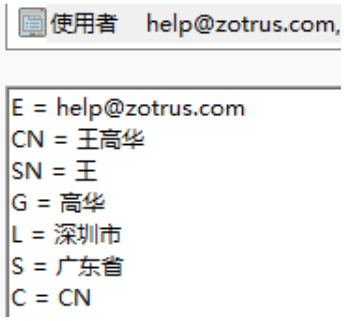
S/MIME 邮件数字签名和加密离不开数字证书，也就是 S/MIME 证书，或简称为邮件证书或电子邮件证书。电子邮件证书同 SSL 证书一样也必须是由第三方 CA 机构在完成了邮箱控制验证和证书申请者身份鉴证后签发，也必须同 SSL 证书一样有一个证书签发标准，也必须同 SSL 证书一样有浏览器信任机制的邮件客户端信任机制，只有这样才是一个完整的 PKI 应用生态，才能真正实现密码保障电子邮件的全生命周期安全。

1. S/MIME 邮件证书

S/MIME 邮件证书同 SSL 证书一样，也是标准的 X.509 V3 数字证书，同 SSL 证书绑定域名不同的是邮件证书绑定电子邮件地址，所以，同签发 SSL 证书必须验证绑定的域名控制权一样，签发邮件证书必须验证绑定的邮件地址，使用的验证方法就是向申请邮件证书的邮箱发送一封带有验证码的电子邮件，这个验证过程同 SSL 证书的邮箱验证也是一样的，只有验证了用户的邮箱控制权 CA 系统才能签发邮件证书。

邮件证书同 SSL 证书一样按照身份验证的严格程度分为四类：MV 邮件证书、IV 邮件证书、OV 邮件证书和 SV 邮件证书，身份认证规则和验证内容分别类似于 SSL 证书的四类：DV SSL 证书、IV SSL 证书、OV SSL 证书和 EV SSL 证书，但稍有不同的是 SV 邮件证书，这类证书等同于 IV+OV 证书，也就是既验证个人身份(IV)又同时验证单位身份(OV)。而 MV 邮件证书就只是验证邮箱，不验证用户身份。这 4 种邮件证书的主题信息如下图所示，依次为 MV/IV/OV/SV 邮件证书。





邮件证书同 SSL 证书一样，也有证书签发管理国际标准-由 CA/浏览器论坛制定的《公共可信 S/MIME 证书签发和管理基线要求》，用于规范全球信任 CA 签发 S/MIME 邮件证书，同时也就规范了 S/MIME 邮件客户端如何验证邮件证书，有了此标准就是使得 S/MIME 技术有了完整的产业链标准，包括 S/MIME 协议标准和 S/MIME 证书标准，这是其他任何邮件加密技术都没有实现的开放生态，使得 CA 机构和邮件客户端开发商都可以依据标准来实现电子邮件加解密的兼容互认。

2. S/MIME 邮件客户端

要实现电子邮件加密，当然离不开邮件客户端的支持。既然已经有了 S/MIME 标准，那所有邮件客户端只需按照 S/MIME 标准支持邮件加解密，实现邮件数字签名和验证签名即可，这些客户端统称为 S/MIME 邮件客户端。目前支持 S/MIME 标准的邮件客户端有微软 Outlook、Mozilla 雷鸟、苹果邮件、华为邮件等，最好用的就是 Outlook 了，只要把 S/MIME 邮件证书安装到 Windows 证书存储处，Outlook 能自动配置使用，自动解密已加密邮件。手机端 APP 比较好用的就是苹果邮件了，需要手动安装和配置 S/MIME 邮件证书，配置过程比较复杂。

也正是由于用户需要先向 CA 申请 S/MIME 邮件证书再配置到邮件客户端中使用，这两个不同产业虽然都是遵循 S/MIME 标准，但是各自为政，没有很好的配合做好无缝对接，导致了一个非常优秀的邮件加密技术无法普及应用。

六、 S/MIME 标准是电子邮件加密的唯一通用标准

前面四个部分讲清楚的S/MIME标准的工作原理，电子邮件数字签名和加密是相辅相成的，为解决 SMTP 电子邮件的安全问题提供了全面的解决方案。第五部分简单讲解了 S/MIME 证书和 S/MIME 客户端，这些都是 S/MIME 加密技术生态的重要组成部分，数字证书、邮件数字签名和加密是 S/MIME 的核心功能，PKI 公钥机制使得 S/MIME 数字签名和邮件加密变得可

行，而数字证书通过公钥和私钥密钥对使得使用数字签名和加密成为可能。

S/MIME 标准实现的是真正的端到端加密，从电子邮件在邮件客户端中生成时就已经加密，以密文形式从用户端发送到邮件服务器，以密文方式存储在邮件服务器中，并以密文方式发给收件人。而市场上的 TLS 邮件加密，实际上只能保证电子邮件从用户端发送到邮件服务器的传输过程是通过类似于 HTTPS 加密的方式实现了电子邮件传输通道的加密，并没有加密电子邮件本身。严格来讲，不属于电子邮件加密技术。但是，IMAP 和 SMTP 支持了 TLS 加密后，能有效保证电子邮箱的账户安全，确保了用户名和口令是通过加密通道传输到邮件服务器上完成登录验证的，这个对于电子邮件安全也非常重要，所以，几乎所有电子邮件服务提供商都已经默认提供 IMAP 和 SMTP 的 TLS 加密。

除了基于国际标准的 S/MIME 邮件加密解决方案外的其他电子邮件加密解决方案都是采用私有协议实现，不具备广泛的通用性和多厂家的兼容互通，同时由于封闭而无法得知是否真正安全(即使是开源)，一旦使用只能锁定这一家服务提供商，笔者不认为这些解决方案是好方案，所以，零信技术坚持走 S/MIME 标准技术路线。

未完待续。。。。。

王高华

2025 年 2 月 17 日于深圳
