NEUSOFT 东软

软 件 创 造 客 户 价 值

SJY25电子邮件密码系统

安 全 快 递

技 术 白 皮 书

沈 阳 东 软 软 件 股 份 有 限 公 司

1　企业信息保护与邮件安全

今天，由于竞争的需要，企业纷纷采用非常灵活的经营策略，这就使得企业各分支机构的分布的地域十分广泛，可能跨越不同的省、市甚至不同的国家。与此同时，企业的总部又需要对各分支机构进行统一的管理。销售、物资、生产、财务、人事管理、研发中的技术交流甚至办公事务都需要通过因特网进行，这就需要采用相应的技术手段保证企业信息资产的安全。否则，企业会面临各种巨大的潜在威胁，可能造成严重后果和难以估计的损失。企业的信息资产包括各种企业核心机密、技术专利、销售数据、财务数据、物资及流向数据、市场信息等等。

目前，电子邮件是许多公司进行内部组织、管理与协调工作的重要工具，也是保持公司对外联系、为客户提供技术服务以及发布产品信息的重要手段。电子邮件已经成为一种重要的商业通信手段和沟通途径。

但是，明文的电子邮件是十分不安全的。电子邮件的投递过程，实质上是邮件在网络上被反复复制的过程。其投递路径是不确定的，途中会在许多地方留下拷贝，很容易被偷阅。电子邮件的误投现象也时有发生。误投的邮件可能导致极其重要的商业或技术信息的泄露。电子邮件的伪造现象在因特网上也很普遍。

由此可见，在国际互联网上通信，是很不安全的。在这种不安全的网络上实现安全的邮件传输，唯一办法的办法就是采用密码技术保证电子邮件传输的安全。

2 企业级加密邮件系统需求

电子邮件系统已经日益成为保证企业正常运营不可缺少的一种通信手段，应用的范围极为广泛，而且有许多基于邮件系统的办公软件，如 Notes 等。这就要求加密邮件系统能与现有的系统很好的兼容，而且具有操作简便，界面直观等特点，归纳起来，一个加密邮件系统应有如下特点：

1 加解密过程对用户透明

2 具有数据加密、数字签名、身份认证等功能

3 具有文件加密功能，方便用户进行敏感信息的本地存储。

4 采用的加密算法安全强度高，而且易于替换，方便地应用于不同安全等级的环境。

5 系统可扩展性好，界面直观。

3 SJY25 电子邮件密码系统概要

SJY25 电子邮件加密系统系统是一套基于 PKI 的电子邮件加密系统。可用于企事业单位、商业机构传送敏感信息（如各种财务报表，技术资料等等）。它包括 SecureExpress 及 SmartExpress 两个部件。通过采用标准格式的 RSA 私钥及 X509 标准的公钥证书，可以对电子邮件内容的保密性和完整性提供保护,并提供发方的不可否认性。SecureExpress 亦可用于本地文件和目录的加密存储。运行环境为 windows98 和标准的邮件客户端环境，如 MS Outlook Express、Netscape Communicator 等等。

4　SJY25 电子邮件密码系统功能特性

邮件保密

SJY25 电子邮件加密系统发送的邮件内容使用接收方的公钥加密，保证除了指定的接收方之外，任何其他第三方即使截获邮件，也不能获得任何有意义的信息。有效保证了通过 SJY25 电子邮件加密系统传送的商业合同、机密资料的保密性。

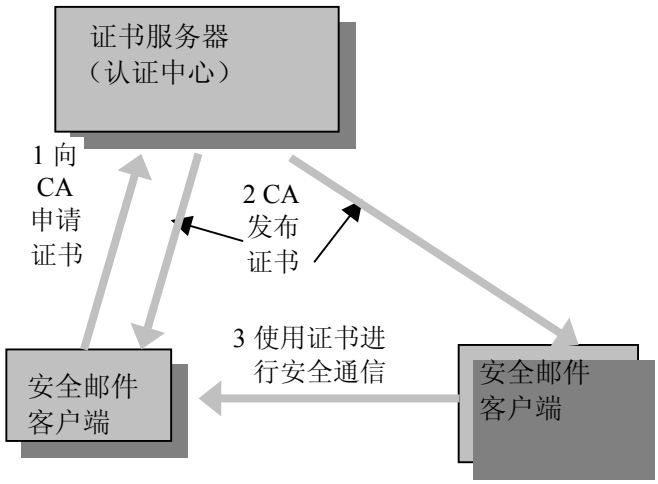
邮件内容的保真与保全

通过采用数字认证技术，SJY25 电子邮件加密系统自动验证接收的邮件的完整性，如果邮件内容与发送方的数字签名不符，系统会自动提示用户邮件内容与签名不符（签名错误），可以保证接收到的邮件内容的真实可靠。

身份认证

SJY25 电子邮件加密系统通过采用公钥证书和数字签名技术可以保证：接收者能够核实发送方的身份并验证发送者对报文的签名；发送者事后不能抵赖对邮件内容的签名；接收者也不能伪造对邮件内容的签名。SJY25 电子邮件加密系统的证书验证过程是系统自动完成的，在接到安全邮件时，系统会自动使用证书撤销列表（证书黑名单）验证对方证书的有效性。

5 SJY25 电子邮件密码系统工作流程



SJY25 电子邮件加密系统是一套基于 PKI 的邮件加密软件，因此用户系统中应已有相应的 CA 软件提供认证服务，我们建议使用 SRQ06 电子证书认证系统，它可以颁发 X509 标准的证书，与 SJY25 电子邮件加密系统无缝集成。用户也可使用已有的 CA 系统，但要求 CA 颁发的证书格式及私钥格式必须遵循 X509、PKCS＃10 等国际标准。

用户使用 CA 认证服务，进行安全的邮件传输的具体过程是：

- 用户使用 SJY25 电子邮件加密系统在本地工作站产生密钥对，私钥以加密的形式存储在本地硬盘上，同时生成证书请求。
- 用户通过邮件把请求发送到认证中心，
- 认证中心审核并验证请求的有效性之后，为用户签发证书。
- 用户证书、系统中的其它用户的证书及证书撤销列表（CRL）通过邮件发送给用户。
- 用户使用 SJY25 电子邮件加密系统配置好自己和其他用户的证书以及 CRL 之后，就可以进行安全加密的电子邮件通信了。

6　SJY25 电子邮件密码系统技术特点

操作的易用性

SJY25 电子邮件加密系统屏蔽了与加密、公钥认证、签名验证的有关的复杂过程，提供给用户一个直观明了的用户界面。用户只需轻点鼠标即可完成邮件的加密/解密、签名/验证操作，操作极为简便。

SJY25 电子邮件加密系统可以接受任何的文件和目录，并对其进行加密和签名，可以处理指定后缀的文件，对其进行解密，并释放其中的文件。文件或目录可以通过对话框指定或通过鼠标拖拽。

SJY25 电子邮件加密系统可以在资源管理器中以鼠标右键的方式被激活，发送指定的文件或目录。

SJY25 电子邮件加密系统可以在 Word 或 Excel 程序中以特定的菜单项的形式被激活，发送当前处理的文件。

SJY25 电子邮件密码系统的操作界面如下图所示：

指定多个收件人

用户可以同时向多个用户发送加密邮件。系统自动用各个接收者的证书及接收者的私钥生成安全邮件，并一次发送出去。

支持多种邮件客户端和多平台

SJY25 电子邮件加密系统可以与所有基于标准 MAPI 技术的邮件客户端兼容，如 MS Outlook Express、MS Outlook、Netscape Communicator、Lotus Notes 等等，系统可以运行于 window95/98/NT 平台。

自动发送与接收功能

SJY25 电子邮件加密系统的 SmartExpress 模块可以提供安全邮件的自动发送和接收功能。系统可以在本机建立发送的队列，并在用户设定的时间自动将信息发送出去。与此类似，系统可以按照一定的时间间隔自动接收安全邮件，在自动接收模式下可以根据信息的类型自动执行系统预先定义的外部程序，实现数据的自动接收和处理。基于这一特性可以建立离线式的信息自动收集系统。

文件和目录本地加密存储

用户可以把加密邮件的接收者设为自己，把 SJY25 电子邮件加密系统生成的加密包裹直接存储在本地硬盘上，同时删除原来的文件。解密包裹时，只需输入私钥口令即可解密出原来的数据。

沈 阳 东 软 软 件 股 份 有 限 公 司
地址：沈阳浑南高新技术产业开发区·东大软件园
传真：024-23784036　邮编：110179
网址：www.neusoft.com