安全 Web Mail 中的关键技术

王鑫彦，单晓毅
（北京医药集团有限责任公司，北京 100078）

摘 要：基于公钥体系结构（PKI）原理，设计了结合CA安全证书的Web Mail安全系统，并将PKI技术融入到系统各组成部分。一方面，利用智能卡安全身份认证技术，提供了一种安全便捷的身份认证模式；另一方面，应用了动态页面关键信息提取技术，使得用户数据在客户端完成加解密操作，解决了公务邮件传输中的安全性和完整性问题。经过实验环境的原型验证，系统运转良好。

关键词：电子邮件；PKI；安全身份认证；关键信息加密
中图分类号：TP393.098 文献标识码：A

Key technologies of secure web mail

WANG Xin Yan, SHAN Xiao Yi
(Beijing Pharmaceutical Group Co.Ltd., Beijing 100078, China)

Abstract:Based on the principle of public key infrastructure(PKI), this paper designs a secure web mail system with CA certificate. PKI technology is integrated into each module of the system. It has two creative points: one is the secure and ease-of-use authentication mode, provided by the intelligent card secure authentication technology, the other is to resolve the security and integrality issue during business email transmission with the key information picking-up technology in dynamic page, and that lets end user's data encrypted and decrypted within client. Tested in the laboratory, the demonstration system works well and is being upgraded.

Key words:email; PKI; secure authantication; key information encryption

电子邮件作为互联网应用最广泛的信息交流工具，已深入普及到人们的日常生活和工作当中。于是电子邮件的安全性日益成为互联网行业和整个社会关注的问题，如何实现安全且易用的电子邮件系统，成为安全电子邮件应用的明确需求。

传统电子邮件技术是一种安全性较差的信息传输技术。目前，因特网用户所使用的绝大多数电子邮件系统中，基本没有采取任何措施来保证电子邮件在网络中安全传送。电子邮件的内容以明文的形式在网络中传递，使其面临着被截获、篡改、破坏的危险。

我国安全电子邮件应用的自主研究也在迅猛发展。服务提供商、产品厂商通过自己的努力，对安全电子邮件系统做出探索性的研制和推广，并配合相关法规和制度不断反馈和修订，但都尚未形成公开的或权威的标准。为了解决应用层邮件的安全问题，需要设计易用的企业级安全邮件系统，具有集中管理用户证书并进行后台自动数据安全处理的机制，同时做到灵活和易集成。

经过广泛的市场调研，基于非对称密钥加密理论，在传统电子邮件系统中引入公共密钥体系（PKI），通过CA安全认证、数字签名和信息加密技术（对称加密和非对称加密）可以为电子邮件用户提供以下安全服务：邮件发送方身份认证、邮件内容保密、邮件内容完整、邮件内容不可否认，从而实现安全易用的电子邮件系统[1]。

1 安全 Web Mail 系统总体设计

安全 Web Mail 系统总体分为4层，由基础层、平台层、应用层和客户层组成，提供统一的整体服务，如图1所示。底层是基础层，提供整体系统的后台基础服务，包括标准电子邮件服务系统及其管理用户信息的附属目录服务系统、CA证书服务系统。平台层位于基础层之上，包括Web服务器、应用服务器和数据库服务器，

符合 Internet3 层应用部署架构，为上层应用提供运行环境和数据存储空间，为客户端提供访问接入响应。应用层位于平台层之上，包含安全身份认证系统、网上证书受理系统、Web Mail 系统以及企业用户地址树、系统后台管理、单点登录接口等应用服务，实现证书受理、身份认证、信息加解密、用户管理和系统接口等各项安全 Web Mail 邮件功能。最上层是客户层，包括客户端浏览器及插件、用于安全认证的 USB 接口智能密钥棒。

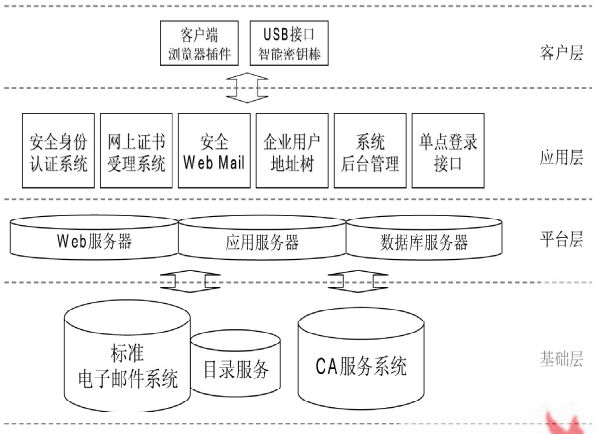

图 1 安全 Web Mail 系统分层模型

2 安全身份认证技术

2.1 身份认证安全设计

安全 Web Mail 邮件系统认证包括 4 个部分，即私钥签名、证书验证、证书检测、身份确认，主要完成对拥有证书的用户进行身份认证的功能。

每个用户拥有唯一一个密钥棒，其中存储代表用户身份的数字证书和私钥，用户登录系统时，在客户端 USB 口插入智能密钥棒，与远程身份认证服务器通讯，由认证服务器验证用户的数字签名完成对用户身份的认证，并得到用户的身份以及系统的授权信息[2-3]。采用智能密钥棒进行身份认证，很好地结合了 PKI 体系和智能卡设备，使 PKI 体系具有了“移动”特征[4]。

设计中采用 RSA + SHA1 作为安全 Web Mail 系统中身份认证的签名算法，采用 RSA 作为数字信封的非对称加密算法，采用国密标准的 SDBI 作为 HASH 算法[5]。

2.2 智能卡协调管理器

智能卡作为数字证书存储介质，遵循国际标准协议(PKCS11)。为了屏蔽各类智能卡的差异，简化应用系统的开发并增强系统的通用性，在原有各类智能卡接口函数的基础上，推出 CA 系统智能卡协调管理器，统一了各个类型智能卡的接口。

智能卡协调管理器主要分为 3 部分：上层应用调用的组件、Windows 智能卡资源管理接口和智能卡驱动程序。智能卡协调管理器就是中间调节作用的抽象层。智能卡协调管理器模型将智能卡厂商提供的应用接口与智能卡应用程序使用的接口隔离开。智能卡厂商提供的驱动程序发生变化或更新，对上层的智能卡应用程序没有影响。

3 动态页面关键信息提取技术

3.1 HTTP 数据的获取技术

IE 就是一个包含许多其他 COM 组件的较大 COM 组件，可以访问已经运行的 IE 实例，并从应用程序中获得对 IE 的控制。

对一个与其客户通信的 COM 对象来说，该对象必须支持一个或多个发出接口，支持发出接口的 COM 对象称作可连接对象。要想有资格成为可连接对象，就必须实现 Iconnection Point Container 接口。发出接口实际上由客户来执行，并通过连接点插入 COM 对象。每次启动新实例时，IE 都会加载浏览器帮助者对象（BHO）所指定的一个动态链接库（DLL），而此 DLL 能有效地与 IE 进行连接，获知 IE 正在激发的事件。对于 BHO 下的每个 CLSID，IE 在与浏览器相同的进程空间调用 CoCreateInstance，启动 BHO 实例。如果 BHO 注册了它的 CLSID 并执行了 IobjectWithSit 接口，那么 IE 就启动 BHO 并传递指向 IE 的 IwebBrowser 接口指针，通过该接口指针，就能控制和接收来自 IE 的事件。

3.2 Web 页面关键信息提取技术

关键信息标记语言是对 HTML 的扩充。HTML 脚本语言可以分为表现式语言和内容式语言。表现式语言主要完成显示功能，如表格的标记<table>、<tr>、<td>等；而内容式语言就是需要传递给用户的真实数据，如文本输入标记<textarea>。对 W3C 规定的标记语言的命名进行调整。例如，页面中的私钥密码输入：

<input type="password" name="abc1" size="14">

可以规定 type=password 的输入标记语言的名字，如果命名为一个特殊的标记，则表示它是关键信息，然后在对 HTML 进行解析时，发现了此特殊的标记，则按照此特殊标记应该做的操作进行处理。下面是关键信息标记语言的规则定义：

__KEY + 标记语言元素 +CONTENT + 对标记内容需要的操作

通过控制浏览器来获取所有的 HTTP 请求数据，并从数据中将关键信息分离出来，称为关键信息的自动解析。

4 安全 Web Mail 系统在实验环境中的实现

实验环境中，采用 4 台 x86 服务器作为功能服务器，利用商用软件平台产品，部署安全 Web Mail 应用软件，搭建实验系统。

若用 2 台 PC 作为客户端，利用 MS IE 浏览器进行功能测试，则如图 2 所示。

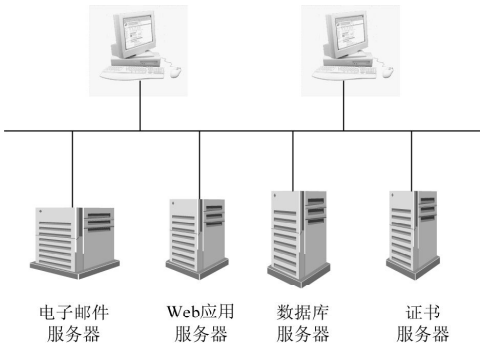

图 2 安全 Web Mail 系统实验环境

图 3 为安全 Web Mail 系统的登录访问界面，用户只需在客户端插入 USB 接口智能密钥棒，输入密钥保护口令，即可进行安全登录。

图 3 用户登录界面截图

图 4 为安全 Web Mail 系统的用户成功登录后的“发送邮件”页面。可以看到其中邮件内容采用了关键信息的加密操作。界面中除了公务邮箱管理外，也包含个人（普通）邮件管理、个人信息管理以及企业地址树等丰富的功能。

基于 PKI 的安全 Web Mail 系统作为信息安全产品的融合体，在用户使用方便的前提下，将身份认证、信息加密、访问控制等核心信息安全技术进行结合，为缺乏信息安全防护的系统提供了直接、高效的信息安全防护体系。

考虑技术应用范围的有限性，基于 PKI 的安全 Web Mail 技术研究也表现出许多不足，如尚未充分集成嵌入更紧密的电子邮件防病毒、防垃圾技术，应用系统接口比较复杂，密文信息处理得不够灵活等。所以，系统还有许多功能和技术需要进一步完善。本文的论述，希望能为促进我国推广自主知识产权的信息安全产品做出微薄贡献。

参考文献

[1] SCHNEIE B.E-Mail的安全[M].于文勇,朱志钢,译.北京：电子工业出版社，2003.

[2] RFC1421. Privacy Enhancement for Internet Electronic Mail : Part I : Message Encryption and Authentication Procedure, 1993.

[3] RFC1422. Privacy Enhancement for Internet Electronic Mail : Part II : Certificate-Based Key Management, 1993.

[4] HORSLEY R, POLK T. Planning for PKI: Best Practices Guide For Deploying Public Key Infrastructure, NewYork: Wiley, 2001.

[5] 周学广,刘艺.信息安全学[M].北京：机械工业出版社，2003.

图 4 用户登录后界面截图

（收稿日期：2009-03-31）