商用 USB 加密系统的设计

Design of Cryptographic System Based on USB

张志强[1,2]　闫　飞[3]　娄洪伟[1]　隋永新[1]　杨怀江[1]

(1 中国科学院 长春光学精密机械与物理研究所应用光学国家重点实验室 吉林 长春 130033
2 中国科学院 研究生院 北京 100039　3 长春供电公司 吉林 长春 130033)

摘　要：为提高加密系统的可用性,提出了基于 USB 的加密系统设计,该系统上层接口符合微软的 CSP 标准,系统内部本身实现了证书解析和证书存储的功能;系统内部可以存储大量的证书,供使用者方便的选择通信对象;而且本系统也可以作为一种证书安全存储介质。对基于 CSP 的智能卡功能进行了扩充,方便了用户的使用和开发。

关键词：CSP　X.509　USB　智能卡　加密

开发基于智能卡的 CSP 能提供高可靠性和安全性的加密服务。为了方便在 Windows 上提供加密服务,Microsoft 提出了一套 CSP/Crypto API 的开发模式,它提供了一套加解密和签名认证的编程接口供应用程序开发人员调用,通过调用这套函数接口,应用程序可以利用软件或硬件为用户提供强大的加解密服务。近几年来,由于基于硬件的加密系统具有方便易用、灵活、高可靠性等优点,使得它已成为主流的安全介质。

PKI 技术以数字证书为媒介,通过对证书的使用和管理,可在网络信息交流中实现身份认证和并保证信息传输的安全性。本系统内部实现了对证书的解析功能,可以进行证书的导入和导出,导入的证书可以安全地存储在系统内部。

微软的 CSP 开发模式简化了系统的设计分析工作,但是在微软的 CSP 开发模式中,签名密钥和交换密钥的导入势必需要相应的证书支持,而相关证书要存储在 PC 机上,这会产生以下几个缺点:(1)大多基于 USB 加密系统是可以灵活地应用在每台 PC 机上,但将要进行通信的对象的证书却一般只能在自己的 PC 存储器中存储,这会使对系统的应用失去灵活性。(2)私有证书也是同样的存储在 PC 机上,将会降低系统的安全性。基于以上的考虑,本文在兼容 CSP 开发模式基础上,将证书的导入导出和证书解析功能(X.509),证书存储功能整合到系统内部,这样,公有证书的存储和解析方便了用户对通信对象的查找,方便了系统的应用;私有证书的安全存储可以提高系统的安全性,给私有证书的安全存储提供了保障。

1　引言

1.1　CSP 简介

CSP(Cryptographic Service Provider):密码服务提供者。一个 CSP 要实现一定的密码标准和算法,由 CSP 的体系结构所规定,CSP 的体系结构采用了策略与机制分开的思想,主要目的是为了为在 Windows 上开发提供密码服务产品的供应商提供一个标准体系,这样有两个好处,一是使提供密码服务者将主要的精力放在自己密码机制的实现上,而不必考虑那些上层的细节。二是为利用这些服务产品在 Windows 平台上开发基于安全的应用程序人员提供了一个标准,不必因为产品不同而要选择不同的 API 形式,使开发过程大大简化,并且以这种形式开发出来的应用程序是互相兼容的。

图 1 为本 CSP 的体系结构,应用程序开发者可以

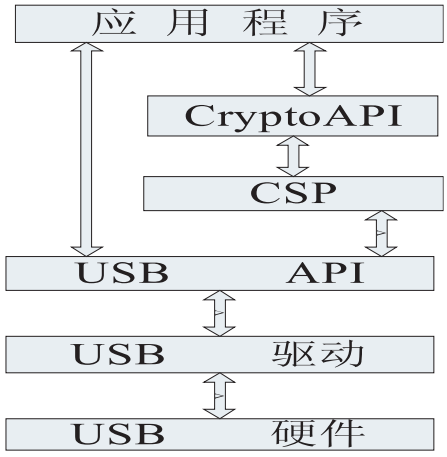

图 1　CSP 体系结构图

通过调用 Crypto API 来操作本系统，也可以以本系统自定义的 API 调用。

1.2　X.509

X.509 是广泛使用的证书格式之一。X.509 用户公钥证书由可信赖的证书权威机构（CA）创建。本加密系统内部有独立的证书公钥私钥提取功能，所以以自定义的 API 形式可以利用证书来更新自己的签名密钥和交换密钥，当然也可以利用公钥证书来获取对方的公钥，更重要的是内部实现了证书的存取功能，使得成为一种证书安全存储介质。

2　系统结构设计

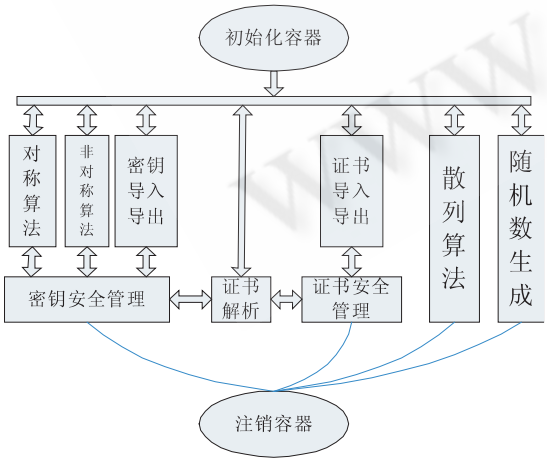

图 2　系统结构图

图 2 为本系统的总体结构图，分为（1）密钥安全管理模块；包括系统工作时在内存区的临时密钥和 RSA 公私钥对，也包括永久密钥对的安全存储管理。RSA 公私钥对可以来自上层的导入操作或者是上面向下层发送的对某一个证书的解析操作。（2）证书安全管理模块实现了对证书的安全保存功能，将导入的证书以更安全的方式存储在 FLASH 上，也可以导出公钥证书，私钥证书以密文形式存储，私钥的解析是受到口令的约束的。私钥证书可以以密文的形式导出，这时系统可以看作是安全存储介质。（3）证书解析模块，在固件内部实现，对固件内部保存的证书解析出公钥或私钥，并传递给密钥安全管理模块，以方便各加密算法的调用或密钥的导入和导出。（4）实现了公钥的导出功能和公钥、私钥的导入功能，不提供私钥的导出功能，此部分的导入导出格式符合微软的 CSP 定义的标准。（5）RSA 算法的密钥长度为 1024 位，用 DSP 的汇编语言编写，RSA 的签名速度可以达到每秒钟 7 次。（6）会话密钥可以以两种方式生成，口令方式和随机生成，由于本系统集成了随机数发生器，所以由随机数生成的密钥的随机性比较好。（7）对称加密算法有 SCB2 算法、DES 算法、3DES 算法（密钥长度可变），分别实现了 CFB/OFB/CBC/ECB 加密方式，给用户以较多的选择。SCB2 加密速度为 15Mbps；散列算法分别实现了 MD5 和 SHA1 算法，MD5 的散列速度为 7Mbps，SHA1 的速度为 29Mbps。

2.1　上层 SPI 设计

本子系统的实现形式为一个动态链接库文件，此部分是由已由微软定义了行为的若干个函数组成的。本系统的主要功能为接受源于上面应用程序，并经过操作系统传下来的参数，判别输入的合法性，进行相应操作，并向下面传递相应的命令。此部分的重点是使输入和输出具有 CSP 规定的标准。

本系统的设计原则是和安全性无关的操作都尽量在 PC 中实现，加密系统中有很多部分是为加密操作进行定制的过程，选定了加密算法后，对算法的密钥长度进行选择，选择加密长度，填充值，反馈长度等信息。这些内容都交由 PC 完成，以结构体的形式保存在 PC 中，这样 PC 中的密钥结构体将含有大量的信息，而在固件中就只是含有和密钥相关的信息。

这样,在密钥参数定制和提取、散列对象参数定制和提取、CSP 参数定制和提取等这些相关函数都不需要固件的支持,而在进行加密等操作时,传下的 USB 包中含有一定的控制命令和信息,供固件进行识别和应用。

2.2 下层固件设计

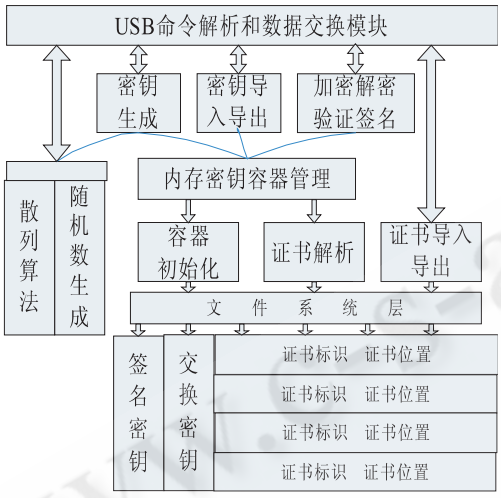

图 3　下层结构图

如图所示,USB 模块主要负责和上层进行命令、信息、数据的交换。每个 USB 包中的前 64 个字节为命令信息,包后面的内容为数据内容;密钥生成模块可以以两种方式生成会话密钥,基于口令(对口令进行散列)生成和利用随机数生成;密钥导入导出模块,不能导出私有密钥,导出格式符合微软提供的格式;容器初始化、证书解析、证书导入导出这三个模块都是和固件内部 FLASH 存储器相关的,容器初始化负责将 RSA 密钥对导入到内存,当然由于安全关系将有一次口令输入,证书解析模块负责对本人的证书解析功能和对方的公钥证书解析功能,解析本人证书同样要有一次口令的输入。

FLASH 部分由三部分组成,第一部分存储各个密钥容器名和容器体的起始地址。第二部分为容器体部分,内容如上图所示,(上图文件系统层下面的内容即为第二部分的示意图)。容器中含有签名密钥对和交换密钥对,之后为证书标识和证书在 FLASH 中的存储位置,这部分包括公有证书和私有证书。第三部分为各个证书的存储位置,具体的引用由第二部分的证书地址标识。和安全相关的即为第二部分内容的私钥的存储,这些内容的存储都是以密文的形式进行存储的,由容器所有者根据口令进行操作。

本系统内部可以存储多个容器和多达上千个证书,每个容器对象都可以有多个公有证书和私有证书,这样容器可以方便的选择通信对象。利用有效的散列算法可以快速的查找证书。

3 总结

本文主要对支持 CSP 的基于 USB 加密系统的设计进行了分析。对基于微软的 CSP 开发模式进行了功能上的扩充,方便了应用程序开发者,提高了系统的应用灵活性。基于此功能开发出的应用程序,可以被应用于诸如个人金融、证券、保险等行业和领域,应用前景十分广阔。

参考文献

1 赵为强,谢吉华. 使用 Microsoft CryptoAPI 开发基于 USB 电子钥匙的 CSP. 计算机安全,2003,(11):93-96.
2 王波,伍洲凯. 智能卡文件系统. 安徽建筑工业学院学报,2004,(4):12.
3 冉春玉,汪学舜, 吕恢艳. 加密服务提供(CSP)的实现与开发. 武汉理工大学学报,2003,(10):25.