PKI 安全体系在手机智能卡中的应用*

张泽连,李代平,徐宏宁
(广东工业大学 计算机学院, 广东 广州 510006)

摘 要: 介绍 PKI 系统和智能卡系统的基本原理和安全技术, 重点研究 PKI 安全体系在手机智能卡中的应用。利用存储在卡中的 PKI 安全插件,为手机卡和 SP 应用之间提供身份认证、数字签名等服务支持,有效确保了手机智能卡在网络数据传输中的安全性、完整性。

关键词: PKI;智能卡;SP;数字证书;数字签名

中图分类号: TP316 **文献标识码**: A **文章编号**: 1674-7720(2011)01-0063-03

The application of the PKI security system in smart card

Zhang Zelian, Li Daiping, Xu Hongning
(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: This article introduced the basic principles and security technology of the public key infrastructure (PKI) system and the smart card system. It focused on the application of the PKI security system in smart card system. The system uses PKI security plug-in stored in SIM card to provide identity authentication, digital signatures and other infrastructure between the smart card and SP applications, which effectively ensure the security and integrity in network data transmission.

Key words: PKI; smart card; SP; digital certificate; digital signatures

随着移动技术的迅速发展以及手机卡的一卡多应用平台的建立,人们借助手机这种终端设备可以随时随地接入网络进行交易和数据交流, 因此用户的身份认证、传输数据的保密性、数据的完整性及交易的不可抵赖性等变得迫在眉睫。目前对互联网的安全研究已形成一套完整的解决方案,即广泛采取的 PKI。而内置于手机的智能卡,属于内嵌式 CPU,具有独立的加密计算能力和一定的存储空间。本文介绍了 PKI 安全体系在手机智能卡中的应用方式和方法, 描述了基于 PKI 安全体系的证书管理、身份认证、数字签名和数据加解密。

1 PKI 概述

公共密钥基础设施 PKI (Public Key Infrastructure)是一种遵循既定标准的密钥管理平台,它能够为所有网络应用提供加密和数字签名等密码服务以及所必须的密钥和证书管理体系。在公共密钥系统中,PKI 体系涉及多个实体之间的协作过程:认证机构、注册机构、证书库、密钥管理、应用接口和用户等。主要基于非对称密码技术,即公开密钥密码技术。

* 基金项目:广州市越秀区自然科技基金资助项目(2008-GX-015)

公钥体制于 1976 年由 W.Diffie 和 M.Hellman 提出,其最大特点是采用两个密钥将加密和解密分开, 一个公钥作为加密密钥,另一个私钥为用户专有。用户要保障专用密钥的安全,公开密钥则可以发布出去。若以公钥作为加密密钥,以用户私钥作为解密密钥,可实现多个用户加密的信息只能由一个用户解读;反之,以用户专有的私钥作为加密密钥, 而以公钥作为解密密钥,则实现由一个用户加密的信息,可使多个用户解读。前者可用于保密通信,后者可用于数字签名。

2 手机智能卡

智能卡(Smart Card)是 IC 卡,相当于一个微型计算机, 具有计算机的基本组成部分:CPU (中央处理器)、ROM(只读存储器)、RAM(随机存储器)、COS(片内操作系统)和 EEPROM(电可擦除存储器)。本系统的智能卡是手机卡,具有随机数发生器和加密协处理器等,可以硬件实现 RSA 运算;具有 DES 和 SHA-1 等密码算法,可以在芯片内部产生密钥对, 并能在芯片上完成加解密运算。本系统将用户的私钥存放在智能卡存储器中,这样使用密协处理器运算执行 RSA 算法,完成加解密工作,

用户对手机智能卡的操作都是通过卡内的片上操作系统 COS 实现的。同时卡片还可以保存用户的公钥证书和信任 SP 证书。本系统采用开发完成的 UIM 卡,系统由 5 个模块组成,如图 1 所示。包括底层驱动、通信管理模块、命令处理模块、文件管理和安全模块。在此基础上可以开发一些上层的应用以及卡上虚拟机、小额支付、电子钱包、超级号簿、PKI 应用等功能。

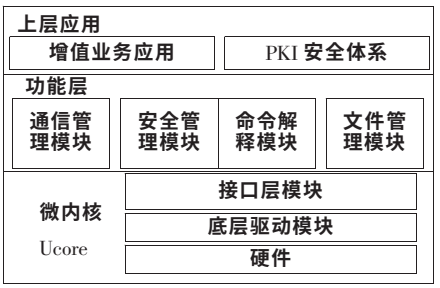

图 1 COS 系统结构模型图

由于不同厂家所生产的底层芯片不同,要求底层的相应驱动程序也不同,因此所采用的微内核结构,通过提取不同芯片驱动相同部分,实际应用时只需要将相应的底层驱动程序移植,具有良好的可移植性和可扩展性。通信管理模块负责实现与外部数据进行通信,对 I/O 输入缓冲区中接收到的数据采取奇偶校验、累加及分组长度检验等手段进行正确性判断,不进行信息内容的判断,接收经过安全管理、命令处理、文件管理处理后的信息,并按照标准 APDU 指令结构要求打包成完整的数据帧,发送到 I/O 的输出缓冲区;安全管理模块接受通信管理模块的调度,并向通信管理模块返回处理后的数据信息;将由通信管理模块接收到的数据进行安全验证;不做数据内容的验证;当安全验证不通过时,直接向通信管理模块返回数据;命令解释模块负责接受安全管理模块的调度,并向安全管理模块返回处理后的数据信息,即返回与命令相对应的响应代码,需要作数据内容上的鉴别,当数据内容鉴别不通过时,直接向通信模块返回数据;文件管理模块主要接受命令管理模块的调度,并执行命令,向命令解释模块返回数据。

3 基于手机智能卡的 PKI 安全体系

PKI 安全体系是手机卡安全模块的重要部分,基于目前越来越普及的手机应用体系上建立的 PKI 架构,担负着确保用户在使用手机交易时信息安全完整和确认身份的任务。智能卡作为数字存储介质,并且要支持多个数字证书组,通过运营商提供管理平台进行统一管理,让多个 SP(由网站提供的短信服务银行、企业等)为其应用开展基于 PKI 体系的身份认证、数字签名、签名认证、数字加密解密的基础设施支持。系统结构如图 2 所示。初始状态下,手机卡内置运营商的数字证书,即在手机和管理平台间建立信任关系;然后 SP 与运营商建立信任关系,允许使用运营商发布的手机智能卡开展基

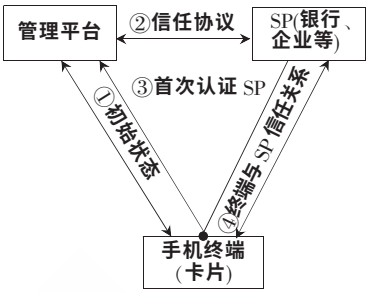

图 2 系统结构图

于 PKI 的基础服务;当终端与 SP 首次通信时,SP 身份则经过管理平台验证,验证通过即证明智能卡加载了 SP 证书并且生成该 SP 的个人证书/私钥,建立了与 SP 的信任关系;最后在 SP 与手机卡进行通信时,SP 提供身份信息给手机终端进行身份验证,智能卡验证通过后,即可进行加密解密、数字签名等。

3.1 管理平台

管理平台在本系统中只是运营商提供的一个中间管理模块,负责接收用户发送过来的消息和签名,分别提取消息和签名信息,然后从 SP 数据库查找有关信息进行身份验证。当验证 UIM 卡和 SP 为签署过协议的合法用户时,发出证书加载指令,最后生成消息,并用管理平台的私钥对消息进行签名,将消息发送给用户。管理平台可以管理 SP 信息及运营商的证书和私钥。

3.2 数字证书

在整个 PKI 体系中,证书的关系是最重要的构成要素。因此,在本系统中手机智能卡同样支持多个 SP 共享使用,并且是存储多个数字证书的介质。证书包括 SP 证书、个人证书以及私钥,这是用于个人与 SP 交互的凭证,证书存储在智能卡的文件管理模块中(安全存储区),而私钥在卡内生成,不能从卡中读取出来。SP 证书是由证书认证中心 CA 颁发给 SP 的数字证书,其格式都符合 x.509 证书 V3 版本格式。私钥是由 SP 保存,用来验证 SP 身份,SP 使用手机智能卡进行加密或者签名时,必须首先出示其身份信息,而智能卡验证通过后才能为 SP 提供加密或者数字签名等功能;个人证书/私钥是指 SP 或者 SP 信任的 CA 颁发给用户的证书,用户在访问 SP 前要进行身份认证和交易签名等功能。

在此系统,证书的管理只是限于管理员级别的,管理员可以加载证书、删除证书、更新证书、查看证书详细信息,而用户只能查看证书的内容。图 3 为证书样本。当查看证书的详细信息时,需要输入用户口令,口令校验正确才可以正常查看。当检测到 UIM 卡与终端已连接时,会自动将该 UIM 卡中的所有证书注册到终端中的证书存储区中,这样手机可以使用用户证书进行身份验证。当检测到有 UIM 卡拔掉时,会自动将 UIM 卡中的所有证书从系统的存储区中删除,在导入导出过程中,同样也需要验证用户合法性,这样可提高安全性。

图 3 数字证书

3.3 数据加密解密

加密操作使用接收方的 RSA 公钥把消息转化成密文，而解密操作使用接收方对应的 RSA 私钥将密文恢复成消息。加密原语在公钥的控制下从消息代表产生出密文代表，解密原语在对应私钥的控制下从密文代表中恢复消息代表。为了加强密钥计算的安全性和数据的保密性，在进行运算前需要对原始报文按照一定格式进行编码，实际运算是对编码后数据的运算。

3.3.1 数据加密具体实现步骤

(1)首先将接收方的公钥和待加密消息进行计算，生成密文，长度也通过计算而得，是一个长度为 k 的八位组串(k 表示和数模 n 以八位组为计量单位的长度)。

(2)根据编码规则进行编码从而形成编码消息。

(3)将编码消息经过一些转换和对加密原语的处理形成密文。

(4)最后将所得信息密文送给接收方，接收方再进行解密。

3.3.2 数据解密具体实现步骤

(1)首先对发送方所传来的密文进行长度检查，如果长度不符则终止运算。

(2)将 RSA 私钥和密文代表代入解密原语，经过一系列运算得出编码信息。

(3) 根据一定的规则分离编码信息最后得出所发送的消息，即数据解密和数据加密过程其实是具有一定运算规则的一个互逆运算过程。

3.4 数字签名和验证

数字签名是建立在公钥体制基础上的一种服务，其主要功能是保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。数字签名运算利用签名者的 RSA 私钥产生一个签名，而签名验证运算利用签名者对应的 RSA 公钥验证消息上的签名，为了验证用这种方案产生的签名，验证者必须拥有消息本身。数字签名算法是用户私钥解密的操作，验证数字签名是用户公钥加密的操作。为了非对称密钥计算的安全性和数字签名的安全性，在进行运算前需要对原始报文按照一定格式进行编码，实际运算是对编码以后数据的运算。数字签名是加密过程，数字签名验证是解密过程。

3.4.1 数字签名生成具体过程步骤

(1) 将签名者的私钥和待签名的信息利用 RSA 算法算出签名。

(2)对消息进行 EMSA-PKCS1-v1_5(编码方案)编码运算产生编码消息 EM。

(3)将编码消息 EM 转换成一个整数消息代表 m，再将 SP 签名原语作用于签名者私钥和整数消息代表形成签名代表 s。

(4)最后将签名代表 s 转换成签名 S，并输出。

3.4.2 签名验证具体实现步骤

(1)检查由数字签名产生的签名 S 的长度，长度不符则输出无效签名。

(2)再转换成签名代表 s，并将验证原语作用于 RSA 公钥和签名代表 s 产生整数消息代表 m。

(3)再将产生的消息代表 m 转换成编码消息。EM 在对消息 M 进行 EMSA-PKCS1-v1_5 编码运算，产生另外一个编码消息 EM1。

(4)比较编码消息 EM 和编码消息 EM1。相同有效，不同则无效。

本文成功对手机智能卡的安全部分进行了延伸，将公钥基础设施 PKI 安全体系应用在手机智能卡上，提高了安全性。该卡片已经应用于生产，在中国电信 3G 网络安全交易中具有重要的作用。

参考文献

[1] 曾自强，邹俊伟. 基于 PKI-SIM 技术的网上购物系统. 中国科技论文在线，http://www.paper.edu.cn.

[2] 黄成，汪海航. 智能卡在 WPKI 中的应用研究[J]. 计算机技术与发展，2007(12)：154-160.

[3] 段斌. 数字签名的智能卡实现[J]. 湘潭大学自然科学学报，2001(3)：102-109.

[4] 俞刚. 智能卡-PKI 私钥的安全载体[J]. 计算机与数字工程，2008(11)107-110.

[5] 关振胜. 公约基础设施 PKI 及其应用[M]. 北京：电子工业出版社，2008.

(收稿日期：2010-08-04)

作者简介：

张泽连，女，1986年生，硕士研究生，主要研究方向：智能卡芯片操作系统。

李代平，男，1955年生，教授，硕士生导师，主要研究方向：软件工程与并行计算。

徐宏宁，男，1984年生，硕士研究生，主要研究方向：智能卡芯片操作系统。