文章编号:1671 - 6833(2013)05 - 0100 - 04

居民健康卡加载数字证书的研究与实现

陈益洲[1], 王永峰[1], 郭仲勇[2], 马 飞[1], 冯海永[1]

(1. 河南省卫生厅 信息中心, 河南 郑州 450003; 2. 河南省数字证书有限责任公司, 河南 郑州 450046)

摘 要: 在居民健康卡(Residents Health Card)各项标准规范的基础上,提出了"一卡双芯片双界面"和"一卡单芯片双界面"模式,通过改造卡片操作系统 COS(Chip Operating System),在居民健康卡中创建第三方数字证书应用的容器,在芯片中生成 SM2(国家密码管理局指定的算法非对称算法)签名公私钥对并将其导入容器中,从芯片外将双数字证书(加密证书和签名证书)和 SM2 加密公私钥对导入容器中. 经过改造后的居民健康卡兼容目前卫生行业、金融行业和电子认证行业的相关标准,为居民健康卡持有人在网络空间中身份的合法化和数字签名应用奠定了基础.

关键词: 居民健康卡;网络信任体系;网络空间;隐私保护;数字签名

中图分类号: TP39 **文献标志码**: A doi:10.3969/j.issn.1671 - 6833.2013.05.022

0 引言

居民健康卡是卫生信息化发展中的一项全新的系统创新工程,是卫生信息化建设标志性成果,在医疗卫生服务活动中用于居民身份识别、个人基本健康信息存储、实现跨区域跨机构就医数据交换和费用结算的信息载体,是全体城乡居民唯一的、全国通用的居民健康卡[1],关乎百姓,关乎民生. 卫生部于 2011 年明确将河南省列为首个居民健康卡建设试点省份,我省与卫生部成立联合工作组,在卫生部带领和指导下共同推进居民健康卡项目实施和各项规范制定. 我省围绕居民健康卡发行及应用开展研究,探索出了一整套工作模式,尤其是在我国乃至全球个人证书的规模发放和多重应用上提供了前所未有的契机[2]. 目前,国内电子认证服务业整体规模仍较小,截止"十一五"末,全国有效数字证书持有量为 1 530 万张,其中个人证书仅为 790 万张,与全国拥有 4.5 亿网民相比相距甚远. 产业规模上不去,根本原因在于个人证书应用无法获得突破.

笔者提出在居民健康卡中植入第三方数字证书,通过数字认证技术实现虚拟和现实实体之间的绑定,解决了在网络空间中实体的身份认证和行为确认问题,是确定网络主体、认定网络行为的重要手段[3]. 笔者提出通过对居民健康卡 COS 进行改造,在卫生系统的容器中增加数字证书应用系统虚拟设备,在该设备中可创建多个应用,每个应用又可以划分成多个容器,在各个容器中植入数字证书和算法密钥. 在个性化过程中绑定公钥和居民真实身份,基于可靠签名及认证技术来保障健康卡在使用过程中的信息安全. 在确保居民健康卡保持其各项功能不减,标准规范、密钥体系、管理主体都不变的前提下,开展数字证书植入的技术改造和应用测试工作,目前已成功实现数字证书的植入和基于数字证书的各项密码运算功能. 推动医疗卫生行业居民健康卡的使用将为个人证书的规模发放和大规模应用提供了现实保障.

1 介质特性分析

1.1 居民健康卡

居民健康卡是采用安全级别较高的 CPU 卡,同时支持接触式和非接触式接口,接触部分符合 ISO7816 和《中国金融集成电路 IC 卡规范》,非接触部分支持 ISO14443—TYPE A 或 TYPE B 的双界面卡. 居民健康卡加载数字证书设计的关键内容有:接触式 CPU 卡、非接触式 CPU 卡、CPU 卡操作系统、算法模块和数字证书.

收稿日期:2013 - 04 - 30;**修订日期**:2013 - 06 - 19

基金项目:"十二五"国家科技支撑计划资助项目(2012BAH05F00)

作者简介:陈益洲(1966 -),男,河南光山人,高级工程师,主要从事区域卫生信息规划、应用技术及方法研究,E-mail:xnhcyz@163.com.

1.1.1　接触式 CPU 卡

卡中的集成电路中央处理器 CPU、电可擦可编程只读存储器 EEPROM（Electrically-Erasable Programmable Read-Only Memory）、随机存储器 RAM 以及固化在只读存储器 ROM 中的卡片操作系统 COS.

EEPROM 是 CPU 卡用户访问的存储区，用于保存 CPU 卡的各种信息、密码、密钥、应用文件等.

ROM 用于存放 CPU 卡上的操作系统（COS 硬掩膜在 ROM 程序区），系统启动时从中读取数据，加载操作系统，管理整个 CPU 卡.

1.1.2　非接触式 CPU 卡

非接触式 CPU 卡是在接触式 CPU 卡的内部电路的基础上，增加了射频发射、接收及相关电路，符合 ISO/IEC 14443 通讯协议.

1.1.3　CPU 卡操作系统 COS

COS 是掩膜在 ROM 中的可执行代码，主要功能是控制外界对应用数据的存取，与接口设备通信及维护应用数据的保密性和完整性；对分区、文件等应用数据的管理；COS 中的内容是在卡的制造阶段定义的.

1.1.4　密码算法模块

算法模块支持国际通用密码算法和国家密码管理局指定的算法，带有 SM1/SSF33/SMS4/DES/AES 硬件加密引擎，支持 RSA/ECC/SM2 等非对称算法，支持 SHA-1/MD5/SM3 等杂凑算法等[4].

1.2　**数字证书**

数字证书是基于公钥基础设施 PKI（Public Key Infrastructure）技术，也可以称之为“网络身份证”，由权威公正的第三方机构 CA（Certificate Authority）签发的证书. 其作用类似于现实生活中的身份证，人们可以在网络交往中用它来识别对方的身份，建立彼此信任.

数字证书包含持有人身份、持有人公钥、签发者身份、序列号、有效期等信息，权威中心 CA 的数字签名证明了证书中各项信息的真实性和完整性.

PKI 通过数字证书实现用户的身份管理和公钥的可信发布. 数字认证技术和居民健康卡相结合，能有效地解决用户在应用系统中的强身份认证、隐私保护、可靠数字签名、证据留存等问题.

2　设计与实现

采用主流的单芯片双界面 CPU 卡，将居民健康卡应用、数字证书应用和金融应用等多应用共置于同一个芯片之中，应用分设，密钥管理体系相互独立，支持各自功能的实现.

卡片建立居民健康卡应用系统环境（WS）、数字证书应用系统环境（DCS）、金融接触式支付系统环境（PSE）或金融非接触支付环境（PPSE）. 居民健康卡、数字证书、金融的数据文件和密钥文件分别建立在各自环境下. 终端通过选择 WS 进入居民健康卡应用系统环境；选择 DCS 进入数字证书应用系统环境；选择 PSE、PPSE 进入金融支付系统环境. 此后依据《居民健康卡应用规范》、《智能 IC 卡及智能密码钥匙密码应用接口规范》和《中国金融集成电路（IC）卡规范》定义的流程对卡片进行操作. 卡片和终端在完成复位应答后，卡片当前目录应位于 MF 下. 多应用居民健康卡的卡片总体结构如图 1 示.

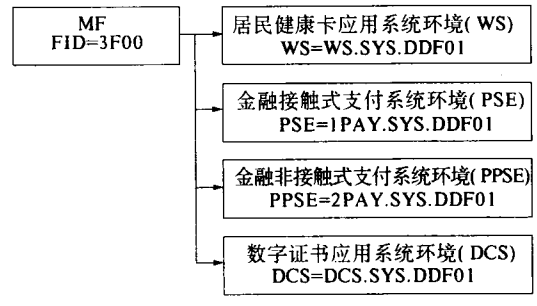

图 1　多应用居民健康卡卡片总体结构

Fig. 1　The overall structure of card application resident card health

2.1　**数字证书应用系统环境（DCS）**

按照《智能 IC 卡及智能密码钥匙密码应用接口规范》中的规定，通过将数字证书应用环境虚拟成设备，在设备中创建多个逻辑上独立的应用（如图 2 所示），每个应用由管理员 PIN、用户 PIN、文件（或多个文件）和容器（或多个容器）组成.

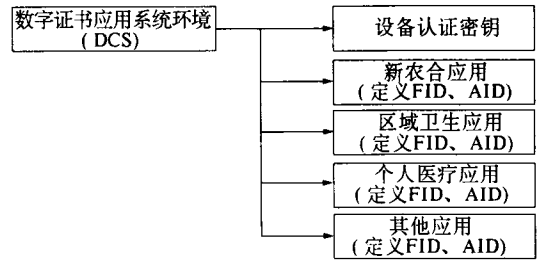

图 2　数字证书应用系统环境结构

Fig. 2　Environment structure of the application of digital certificate

每个容器中可以包含加密公钥、加密私钥、加密数字证书、签名公钥、签名私钥、签名数字证书、会话密钥等组成如图3所示.

签名密钥对由内部产生,加密密钥对由密钥管理系统产生并安全导入,会话密钥可由内部产生或由外部产生并安全导入[5].

加密密钥对用于保护会话密钥,签名密钥对用于数字签名和验证,会话密钥对用于数据加解密和MAC运算.

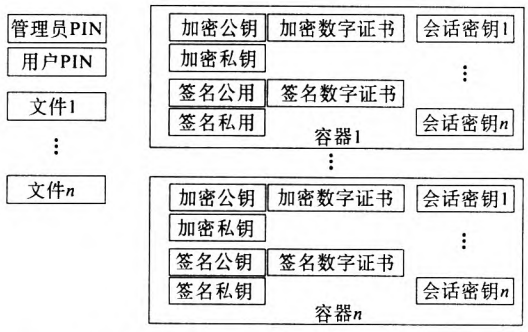

图3 居民健康卡加载数字证书应用逻辑结构图

Fig.3 Residents health card loading digital certificate application logic structure diagram

2.2 居民健康卡数字证书生成及植入

第三方CA获得用户资料,制作生成居民数字证书.在居民健康卡制卡环节灌制居民信息到居民健康卡的同时,自动将该用户证书一并植入卡中,一次完成全部信息及证书的灌入[6].证书植入流程如图4所示.

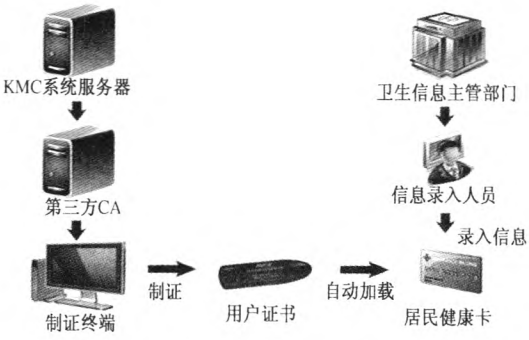

图4 数字证书植入健康卡流程

Fig.4 Digital certificate into the health card process

2.3 终端SAM卡数字证书的植入与认证

终端SAM证书:由发卡机构、审核结算机构将终端设备、SAM卡等信息,发送给第三方CA生成SAM卡数字证书,再由相应部门植入证书.

发卡机构身份验证:结算机构终端通过根公钥索引定位根公钥,用根公钥验证发卡机构的发卡证书并得到发卡机构的公钥值.

3 居民健康卡的应用

居民健康卡数字证书应用,包括居民日常看病就诊、医务人员及管理人员日常办公应用等,涉及安全身份认证、数字签名、安全数据交换[7].患者日常就医流程如图5.

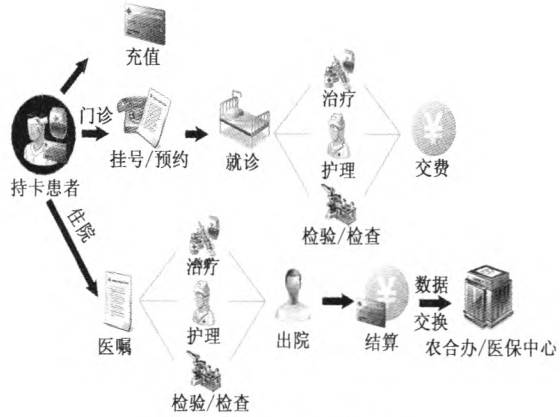

图5 患者就医流程

Fig.5 Patient medical treatment process

通过使用患者和医务人员居民健康卡中的电子身份证书对充值、挂号、缴费、结算记录进行签名并保存,为日后责任认定提供法律保障,有效防止行为抵赖.患者和医务人员安全身份认证过程如图6所示.

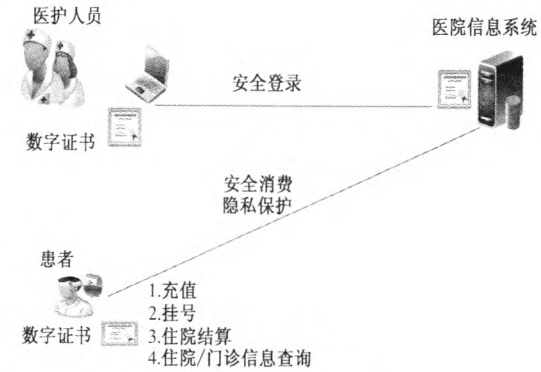

图6 安全身份认证

Fig.6 The security identity authentication

4 结论

采用单芯片双界面CPU卡,在不对居民健康卡现有标准构成影响的前提下,通过对居民健康卡芯片操作系统COS进行改造,在居民健康卡中植入数字证书和算法,既赋予了居民健康卡新的功能,更好地用于惠民工程,又保证了在网络信任体系下卫生系统的真实可信性和合法有效性.在兼容全国范围跨区域应用的同时[8],再进一步实现在卫生系统外的其它行业中"互信互认、一证

多用、一卡多用”的增值服务[9],进而逐步实现“一证通用、一卡通用”.

参考文献:

[1] 郝惠英, 王才有. 医院信息安全体系设计方法[J]. 中国数字医学,2010,5(3):61-63.

[2] 王存库,郝惠英,潘晓平,等. 卫生业务条线信息化建设思路及居民健康卡应用探讨[J]. 中国卫生信息管理杂志,2012,9(5):67-69.

[3] 郭珉江,胡红濮,谢莉琴,等. 电子认证服务在区域卫生信息化中的应用需求研究[J]. 中国数字医学,2012,7(10):32-35.

[4] 卫生部. 居民健康卡技术规范[M]. 2011(卫办发[2011]60号).

[5] 国家密码管理局. GM/T 0016—2012 智能密码钥匙密码应用接口规范[S]. 北京:中国标准出版社,2008.

[6] 石光, 王才有. 中美医疗卫生体制改革论坛综述[J]. 中国卫生政策研究 2011,4(6):61-66.

[7] JR/T 0025—2010,中国金融集成电路IC卡规范[S].

[8] 国家密码管理局电子认证服务密码管理办法[M]. 2009.

[9] GM/T 0015—2012. 基于SM2密码算法的数字证书格式规范[S].

The Research and Implementation of Residents Health Card Loading Digital Certificate

CHEN Yi-zhou[1], WANG Yong-feng[1], GUO Zhong-yong[2], MA Fei[1], FENG Hai-yong[1]

(1. Henan Provincial Department of Health Information Center, Zhengzhou 450003, China; 2. Henan Digital Certificate Co., LTD, Zhengzhou 450046, China)

Abstract: In this paper, we propose two application models: the dual-core chip card with dual interface and the single-core card with dual interface. These models are based on the specifications of the Residents Health Card. Through the transformation of the card Operating System COS(Chip Operating System), the capacitance of the third-party residential health card is created. We can get the SM2 (It is the asymmetric algorithms that is specified by the State Encryption Administration) signature public-private key pair in the chip and import it into the container. The dual digital certificate (encryption certificate and signature certificate) can be imported outside the chip. And the SM2 key pair, encryption key pair can be imported too. These models are compatible with the standards of medical industry, financial industry and electronic certification industry. Research result of this paper lays a good foundation for the legalization of residential health card holder's identity in internet.

Key words: residents health card; network trust system; cyberspace; privacy protection; digital signature