

数字证书在社区卫生服务管理信息系统中的应用

郑 攀 王 晖

(北京市公共卫生信息中心 北京 100050)

〔摘要〕 随着医疗卫生行业信息化建设的推进,居民健康档案及处方信息等逐步电子化,但出现数据泄密、身份认证及医生签名的真实性等安全问题。结合北京市社区卫生信息系统试点安全建设项目的具体实施方案,介绍基于数字证书技术的电子签章系统在社区卫生行业中的具体应用。

〔关键词〕 健康档案;数字证书;电子签章;社区卫生信息系统

Application of Digital Certificates in the Community Health Service Information Management System ZHENG Pan, WANG Hui, Beijing Public Health Information Center, Beijing100050, China

〔Abstract〕 With the progress of informatization construction in medical health area, residents' health records and prescription information become electronization, but the safe problems also emerge, such as data leakage, identity authentication and the authenticity of the doctor signature, etc. Combined with the specific implementation plan of Beijing community health information system, the paper introduces the concrete application of electronic signature system based on digital certificate technology in community health area.

〔Keywords〕 Health record; Digital certificates; Electronic signature; Community health information system

1 背景

“人人享有基本医疗卫生服务”是中国共产党十七大确立的全面建设小康社会的新要求,社区卫生服务是实现“人人享有基本医疗卫生服务”目标的基础环节。在《卫生部关于规范城乡居民健康档案管理的指导意见》中,要求逐步建立电子健康档案信息系统。根据卫生部《健康档案基本架构与数据标准(试行)》(卫办发〔2009〕46号)、《基于健康档案的区域卫生信息平台建设指南(试行)》和相关服务规范的要求,逐步推进建立标准化电子

健康档案。鼓励以省或地级市为单位研究开发相关信息系统。电子健康档案信息系统要逐步与新型农村合作医疗、城镇职工和居民基本医疗保险信息系统以及传染病报告、免疫接种、妇幼保健和医院电子病历等信息系统互联互通,实现信息资源共享,建立起以居民健康档案为基础的区域卫生信息平台。随着医疗行业信息化的不断发展和各项政策的推进,社区卫生服务机构的各种医护信息数字化,已成为医疗行业信息化建设的必然趋势,同时为医生的查询管理及患者的就诊带来很大便利。

以电子处方和电子健康档案为信息基础的社区卫生服务信息系统承载大量涉及病人个人隐私、企业商业秘密和政府工作秘密的敏感信息,这些信息一旦被泄露并加以非法利用,轻则给居民带来严重影响,容易引起医患纠纷,重则引起社会恐慌。因

〔收稿日期〕 2010-09-15

〔作者简介〕 郑攀,网络工程师,发表论文多篇。

此, 如何确保电子处方及健康档案等信息的完整性、保密性、权责可控性及不可篡改性, 是社区卫生机构信息化建设亟待解决的问题。

2 影响安全的因素

2.1 数据泄密

由于行业的特殊性, 社区卫生服务机构的数据信息对于电子健康档案等信息的保密性、完整性, 开具电子处方的身份认证具有极高要求。电子处方和电子健康档案是在诊疗过程中医护人员录入信息通过网络传输到服务器进行储存的过程。由于电子健康档案承载着包括患者个人基本信息、生活习惯、既往病史、诊断治疗情况、家族病史、历次诊疗的电子病历与处方及体检情况等隐私信息, 如果档案信息被非法访问或在网络传输过程中被恶意窃取, 势必会对患者造成影响, 同时也影响社区卫生服务机构的形象, 甚至造成医患纠纷。

2.2 登录身份认证

大多数社区卫生服务信息系统都采用用户名 + 口令的登录方式, 此种登录方式存在很大弊端, 例如由于口令设置过于简单、长度过短、密码在后台数据库以明文显示等特点, 很容易被他人破解及非法利用, 从而更改档案信息等数据, 破坏健康档案的完整性。

2.3 信息的抗抵赖

根据《中华人民共和国电子签名法》要求, 需建立符合该法“可靠电子签名”要求的电子签名、签章系统, 对所有业务中关键数据电文(如电子病历、处方等)进行电子签名, 形成符合法律要求的法律证据。以往的纸质处方可根据医生的笔迹判断处方出处, 随着社区卫生信息系统的建立, 如何能确保医生对处方信息的责任确定及处方信息不被修改, 是整个医疗卫生行业面临的问题。

3 数字证书在社区卫生服务管理系统中的实现方案

3.1 数字证书的含义与作用

数字证书是由权威机构——CA 证书授权 (Certificate Authority) 中心发行的, 能提供在 Internet 上进行身份验证的一种权威性电子文档, 人们可以在互联网交往中用它来证明自己的身份和识别对方的身份。数字证书在社区卫生服务信息系统中的作用表现在: 一方面用于对电子处方等数据文件进行电子签名, 从而确保信息内容的真实性及签名信息的不可否认性; 另一方面用于对居民健康档案等电子信息进行加密, 从而确保信息的机密性、完整性及不可篡改性。

3.2 北京市卫生局社区卫生服务管理信息系统建设项目简介

为进一步推进社区卫生服务管理的信息化建设, 建立覆盖北京市城乡的医疗预防保健网, 2008 年北京市卫生局启动了社区卫生服务管理信息系统建设项目, 该项目包括市区两级硬件及网络平台建设, 以及社区业务系统和社区财务系统的软件开发。目前, 北京市社区卫生服务信息系统建设试点阶段已结束, 包括北京市社区卫生服务信息系统市级平台、3 个试点区县的社区卫生管理中心的区平台、3 个试点区县的 9 个社区卫生服务中心以及下属的 45 个社区卫生服务站建设。

3.3 数字证书的实现方案 (图 1)

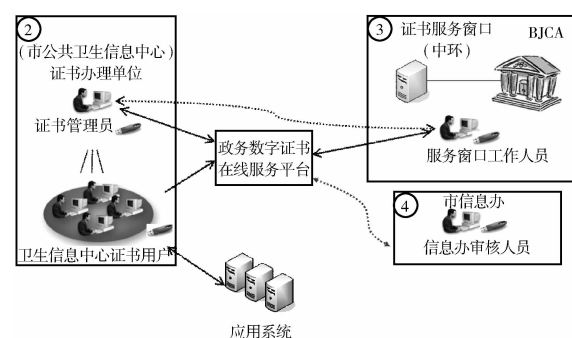


图 1 北京市社区卫生服务信息系统架构

3.3.1 政务数字证书在线服务平台 简称“证书服务平台”，是一个面向各证书应用单位（在此即为北京市公共卫生信息中心）和政务证书使用管理单位（市经信委）的数字证书管理系统，主要提供在线的证书业务及证书服务。目前，证书服务平台已可以承载绝大多数的政务数字证书业务，如证书申请、更新、吊销、USBKey 解锁、证书重签发及统计查询等。

3.3.2 证书办理单位 北京市公共卫生信息中心作为证书办理单位，负责为北京市公共卫生信息中心内部或其它单位（如有需要）办理政务证书。设专人担任证书管理员，负责证书管理和运维工作。证书管理员的日常工作包括：对北京市公共卫生信息中心内部的政务数字证书使用进行管理；申领证书；提交证书更新、吊销、重签发申请；处理 USBKey 解锁事宜；了解证书发放的基本数据。

3.3.3 证书服务窗口 政务证书服务中心是负责为北京市各级国家机关提供统一的政务数字证书办理服务的机构，在试点项目中具体由北京数字证书认证中心（以下简称 BJCA）承担证书服务中心的技术支持、系统维护和用户服务等工作。BJCA 在中环广场设置政务证书服务窗口，作为集中办理政务数字证书业务的窗口，为北京市公共卫生信息中心提供服务。证书服务窗口主要办理如下证书业务事宜：协助北京市公共卫生信息中心证书管理员提交证书申请；组织制作和发放政务数字证书；协助北京市公共卫生信息中心证书管理员进行证书更新、吊销、重签发、USBKey 解锁等操作；解答所有关于证书服务平台的操作和使用问题；与证书管理员及时沟通，解决证书办理和使用中的各类问题，保障政务证书的无障碍使用。另外市经信委负责本市电子政务数字证书的使用管理工作，监管 BJCA 所提供的证书服务。

3.4 电子签章系统实现方案

3.4.1 使用对象 电子签章系统客户端结合成熟的组件技术、PKI 技术、图像处理技术以及智能卡技术，按照一系列的标准体系，以电子形式对电子文档签名并加盖签章。该系统使用对象是社区卫生

中心和社区卫生站的医生和护士，护士通过社区卫生信息服务系统平台为病人建立公民健康档案，医生开处方和相关药品。通过加盖电子公章实现责任认定，从形式上符合实际签章的传统习惯。

3.4.2 电子签章系统管理端 通常称为服务器端，提供电子签章制作生成系统，本系统除了支持电子印章制作外，还实现电子印章的完整生命周期管理，电子签章系统管理端可以签发在线和离线版两种客户端，其中在线版包含印章授权、证书 CRL 验证、过期验证、签章控制及日志审计等功能，在制作生成客户端签章的时候，会自动为客户端初始化一个 URL 地址，客户端会自动连接该 URL 进行相关验证工作，离线版则包含印章授权、日志审计等功能。

3.4.3 电子签章系统框架结构（图 2） 电子签章（签名）系统在可信电子签名和签名验证的基础上，将印章图片和证书密钥绑定成电子印章，实现不规则的电子签名以可视化的数字化签章形式出现，即确保了文档发布者的可信性及文档内容的正确性，又能以签章图片形式满足传统纸质化办公的工作习惯，并防止了印章图片被非法盗用，使各类文档文件的权威性和可信性得到保证。

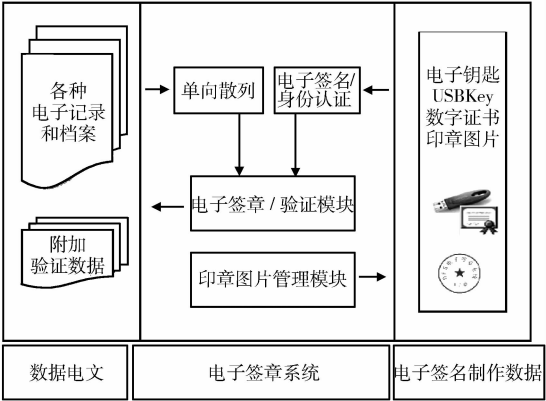


图 2 电子签章系统结构

3.4.4 网络环境拓扑图（图 3） 电子签章系统的部署方式为在试点社区中心平台部署 1 台电子签章管理系统服务器，社区卫生服务中心和社区卫生服务站各终端部署电子签章客户端，用于医生护士加盖电子签章。

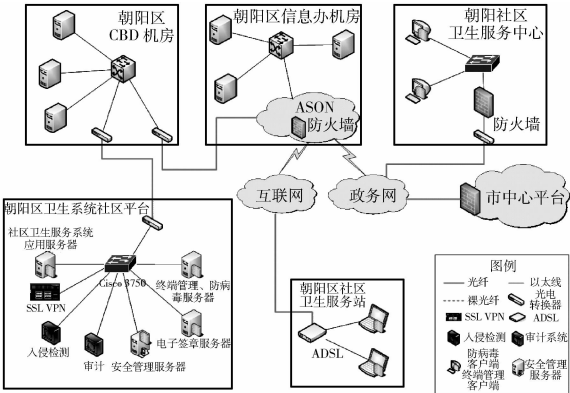


图 3 网络环境拓扑图

3.4.5 电子签章及验证过程（图 4） 在技术路线上，电子签章（签名）系统以基于数字证书的电子签名技术为手段，采用国际标准、国家认可的签名算法，实现对内容进行签名和验证，确保各种网上事故的相关责任能够有效认定，防止恶意抵赖，满足用户对于重要信息的完整性和不可否认性的需要，进而构建起各个信息化应用系统中的责任机制和督查机制。

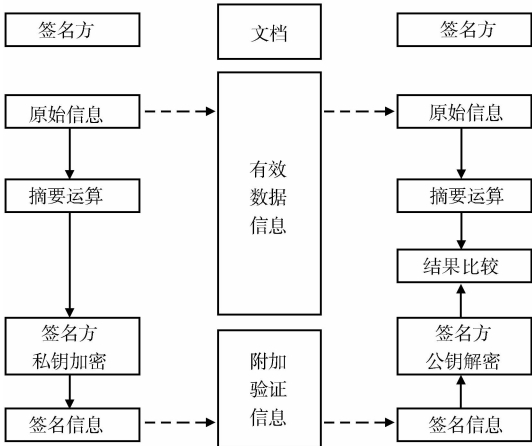


图 4 电子签章及验证过程

3.4.6 电子签章使用流程 第 1 步：医护人员录入公民健康档案，填写公民的基本信息及健康相关的信息，在保存录入信息时，对必填信息进行签章。在该环节进行签章，能够保证录入的准确性，确保录入人对其录入信息负责，能够划清责任。第 2 步：医生在完成诊断后，要为病人填写健康情况，

此次填写会自动新增到公民健康档案中。医生为病人看病的职业行为，是负有责任的，那么就需要保证医生对自己职业行为的记录保留合法有效，此环节就需要加盖电子签章，跟传统纸质文档签字一样，达到责任认定的效力。第 3 步：医生在完成诊断后，要根据诊断情况，为病人对症下药，这也是一个职业行为，在该环节引入电子签章，能够对医生进行有效的监督，同时能够防止在纠纷的时候没有依据，电子签章就是一个合法的证据来源，记录了当时的真实情况。电子签章系统效果，见图 5。

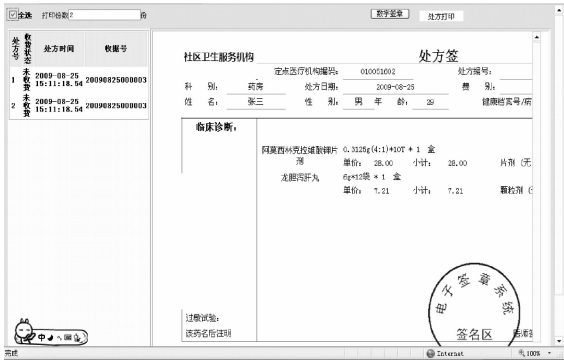


图 5 电子签章系统效果

随着北京市社区卫生服务信息系统中数字证书的应用，在医生诊断开具处方环节集成电子签章系统（包含数字证书），实现了医生在对病人进行诊断后，对开具的处方进行电子化签章，能够确保医生对病人处方的责任的认定，有效防止恶意抵赖和建立督查机制。

参考文献

1 张元, 李久琳, 胡锦涛. 数字证书在医院信息化中应用现状 [J]. 中国卫生事业管理, 2009, (7): 451.
2 李斌, 朱朝华. 数字证书在电子病历中的应用 [J]. 现代计算机 (专业版) 杂志, 2007, (7): 74.
3 梁志伟, 吕玉波, 罗方坚, 等. 医院电子签名和信息加密系统解决方案与应用 [J]. 医学信息, 2007, 20 (6): 901 - 906.
4 卫生部. 医院信息系统基本功能规范 [S]. 2002.
5 卫生部. 健康档案基本架构与数据标准 (试行) [S]. 2009.