数字证书在电子病历中的应用

李斌[1]，朱朝华[2]

摘要：电子病历是医疗信息化发展的趋势，而要真正实现病历的电子化，首先要解决电子病历的真实可靠性问题，本文针对目前医院 CIS 的电子病历信息存在的安全和可信问题，把第三方权威认证机构基于数字证书的认证技术应用在医院 CIS 中，介绍了利用数字证书结合电子病历系统解决电子病历信息安全的作法，使电子病历具有真实性、可信性、安全性、合法性。

关键词：电子病历，数字证书，CIS，数字签名，身份认证，CA 认证技术

一、前言

电子病历是医疗信息化的一个重要的组成部分，是属于医院信息化水平的高级阶段，是建立在基本的医院信息管理系统（HIS）、临床信息系统（CIS），医生工作站、护士工作站等应用系统和相关数据库的基础之上，既是医院内部的一种诊疗过程记录，同时也是一种具有法律性质的文书，既然病历是一种法律性质的文书就要确保电子病历的真实性和安全性。

电子病历是由 CIS 中的医生工作站、护士工作站、PACS、LIS 和相关的医疗设备以及其他系统采集的信息，通过网络传输把信息保存在后台数据库上的数字电文，可见电子病历的数据采集、传输、存储都是由医院的 CIS 来完成。目前国内医院 CIS 的电子病历的数据采集、传输、存储都没有统一的规范和标准，而且 CIS 在医疗业务和信息技术上都是一个庞大复杂的管理系统，很多 CIS 只关注其功能的实现，对数据安全考虑较少，因此人们会对电子病历数据的安全性、真实性和合法性带来质疑。

本文把电子病历结合了数字证书进行应用，利用合法的第三方机构的 CA 认证来确保电子病历数据的真实性、安全性和合法性。

二、电子病历的安全隐患

1. 电子病历产生过程以及基本内容

电子病历信息是病人就诊的各个环节产生的，上一个环节信息是为下个环节服务的，有病人填写或病人主诉信息，再由医务人员输入 CIS，有医务人员对病人的诊疗信息，由医务人员自己录入 CIS，这些信息经医院的网络系统传输到 CIS 后台数据服务器进行存储。其中既有后台数据库方式存储，也有在服务器上以文件方式存储的。在数据库中，建立病历的描述结构，或者说电

子病历的数据模型，将这些信息按照类别及发生的时间顺序，有机地组织成一个整体，用于以后的调用、维护更新、归档。因此，电子病历是病人在医院就诊时的整个诊疗过程记录，其基本包含的内容有：

1) 患者信息：指患者个人信息，如：姓名、性别、年龄、婚姻状况、个人健康信息、过往病史、家庭状况等；
2) 医嘱信息：指医生对病人治疗过程和健康指导意见等；
3) 病程记录信息：指患者病情状况的连续性记录；
4) 检查检验信息：指病人在诊疗过程中所做的各项医学检查和检验的结果记录；
5) 影像检查信息：指病人在诊疗过程中所做的各项医学影像检查的影像资料和诊断结果记录；
6) 手术记录：指病人曾经所做的手术情况记录；
7) 护理信息：指患者接受护理的项目及护理情况和结果记录。

2. 电子病历安全的漏洞

从电子病历内容和产生过程可知，电子病历信息主要是由诊疗的各个医务人员录入信息通过网络传输到服务器进行存储，并且对每个环节实时性的要求都很高，不难看出电子病历存在如下安全问题：

◆ 系统登陆身份验证的问题

CIS 目前大多采用用户名密码方式来登陆系统，采用此种方式进行登陆系统存在着很大的弊端，比如密码设置过于简单、利用自己关切自己的数字（比如生日）来设置密码，密码存储在数据库中以明文的方式等，很容易被人盗取或破解，因此，CIS 系统登陆的身份验证需要解决是否有人使用他人的用户和口令进行病历信息输入和修改，是否有人越过 CIS 的身份验证进行病历信息输入和修改等等问题。

◆ 数据在网络中完整传输问题

医院 CIS 多数运行在医院内的局域网上，局域网上的 CIS 终端与服务器间的信息传输安全往往被忽视，因此，信息有可能被窃取并篡改，无法保障医务人员在 CIS 终端上输入和浏览的电子病历信息的正确性。

◆ 数据存储安全

电子病历信息多数是以明文的方式保存在后台数据库服务器上，而后台数据库服务器对于某些人是透明的。对于在数据库上的数据是否有人更改过，目前的医院 CIS 是没有这种机制来验证的，所以也无法保障医务人员在 CIS 终端上输入和浏览的电子病历信息的正确性。

◆ 对系统信息录入或修改的不可抵赖问题

电子病历的信息需要在CIS终端进行录入，而且对录入的信息要确实反映病人的真实情况，因此，确保录入信息的真实性显得非常重要，这需要每位信息的录入或修改人员对自己的操作行为负有高度的责任，即其行为不可抵赖。

◆ 电子病历的时间取证问题

要准确的把握病人的病情发展，需要对病人的诊断、医疗等的时间有个准确的把握，这就要求电子病历对实时性的要求很高。目前医院的CIS对电子病历的时间记录往往是取终端计算机的系统时间，而不是国家授时的时间，因此，时间的准确性的取证非常重要。

三、基于数字证书的CA认证技术

数字证书是标志网络用户身份信息的一系列数据，用来在网络通讯中识别通讯各方的身份，即要在网络上解决"我是谁"的问题，就如同现实中我们每一个人都要拥有一张证明个人身份的身份证或驾驶执照一样，以表明我们的身份或某种资格。

数字证书是由权威公正的第三方机构即 CA 中心签发的，以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性，签名信息的不可否认性，从而保障网络应用的安全性。简单的说我们可以使用数字证书来保证：信息除发送方和接收方外不被其他人窃取即使被窃取得到的也是不能读懂的乱码；信息在传输过程中不被篡改；发送方能够通过数字证书来确认接收方的身份；发送方对于自己发送的信息不能抵赖；信息存储的完整机密。

数字证书采用公钥密码体制，即每个实体都有一对互相匹配的密钥：公开密钥（公钥）和私有密钥（私钥）。每个用户拥有一把仅为本人所掌握的私钥，用它进行解密和签名；另外还拥有一把公钥并可以对外公开，用于加密和验证签名。

ＣＡ就是数字或电子证书认证中心，是一个负责数字证书发放和管理，同时为电子商务或电子政务系统等提供数字身份验证和安全可信支撑平台的第三方的权威机构。应用系统通过第三方认证机构提供的数字证书和安全支撑平台使应用系统具有可信性和合法性。这就是 CA 认证的意义。CA认证对应用系统主要提供以下功能：

1) 身份认证

通过安全应用支撑平台为应用系统提供安全认证的环境基础，利用为系统的用户、设备、机构、业务等颁发数字证书作为身份识别和认证的依据，在应用系统的登陆部分，实现用户与服务资源的双向认证，达到“一人一证、一机一证、每个机构一证、每个业务一证、持证上岗”的效果。

2） 数据签名

对数据的签名和验签，是将数据作为证据的一种最有效的方法。系统通过利用用户的签名私钥，对数据进行签名运算，并把运算结果作为一个字段存储在数据库中，这样数据就是经过这个用户签名的数据，具有法律效力，不能修改。当需要对数据进行验签时，系统只要再用用户的证书进行一次运算，就可以确定签名的有效性。对数据作签名验签可以确认数据单元的来源和完整性，并保护数据，防止被人伪造或篡改。

3） 数据的加解密

基于安全的整体规划考虑，数据在网络中传输时要确保机密数据不为第三方窃取。需要在机密数据的传输过程中进行加密处理，只能由接收方进行解密还原成明文，才能保证机密数据即使被第三方窃取也由于没有解密密钥而只能是一些无用的加密文件，这就是“取得到，但看不懂”。

认证系统采用的是基于非对称和对称加密技术的数字信封的加密方式，即原文利用对称算法进行加密，得到原文的密文，在把对称算法的密钥利用非对称算法进行加密得到密钥密文，把原文密文和密钥密文加上公钥组成了数字信封进行机密传输，而用于加密和解密的私钥只能在存在数字证书中。

4） 可信时间戳

可信时间戳服务是数字签名功能与基于公共标准时间源的时间服务系统的结合，通过对目标数据加上可信时间源提供的时间标记，以确认系统所处理的数据在某一时间（之前）的存在性，并用数据签名来保证时间标记的完整性与真实性。可信时间戳服务为实现事务处理的抵赖性提供了时间证据基础。

当提交数据需要加盖时间戳时，可以通过使用认证系统中的时间戳服务系统，加盖有时间戳服务器签名的可信时间，并保留时间戳证据。这样对方就可以获得有时间戳标记的数据文件。

四、数字证书在电子病历中的应用

数字证书是网络上（或称为数字化的）实体身份证，可以用于出示给对方来表明自己的真实身份。围绕着数字证书中所包含的公钥和保存在“数字证书载体”（后面会具体描述，一种类似U盘的USB_KEY硬件介质，由使用者实体自己保管）中的私钥，利用这两者之间可以互相加密解密的功能，来实现身份认证、保密性及完整性等一系列安全服务技术。

这个实体可以是自然人、机构、岗位或服务器等硬件设备。具体到电子病历系统中，主要是指医护人员（医生、护士、药剂师等）、医院领导、系统管理人员和服务器设备等。在将来还可以扩展到患者（用于网上预约和查看结果）、他院相关人员（用于远程会诊）和上级领导部门（用于督察）。结合数字证书CA认证平台的电子病历系统的架构图如图1所示。

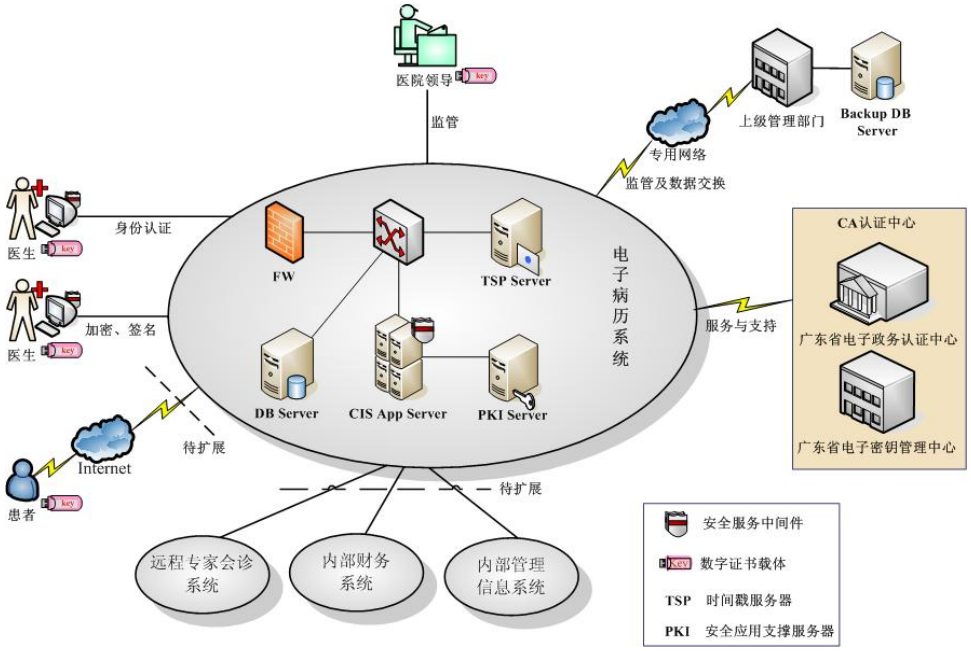

图 1 电子病历系统数字证书安全平台

如图所示，电子病历系统安全平台服务器端的核心为 PKI Server（安全应用支撑服务器）及安全服务中间件，PKI Server 是一个硬件密码设备，它提供了身份认证识别（证书鉴别）、数据加密解密、数字签名及验签等安全运算功能，以硬件方式为应用系统提供服务器端数据机密性、数据完整性、身份认证、防抵赖等服务，符合国密办《证书认证系统密码及其相关安全技术规范》，具有稳定、可靠、高效、易管理的特点。

电子病历系统实时性要求很高，同时系统对 PKI Server 的依赖程度也较高，为了避免由于偶发的机器故障而导致对系统业务应用的较大影响，可以通过配置两台或两台以上的 PKI Server 进行双机冗余，一旦出现故障时可以马上切换至备用设备。

安全服务中间件是基于 PKI 公钥基础设施构建安全应用的开发环境与运行支撑环境，遵循国密办《证书认证系统密码及其相关安全技术规范》，兼容 PKCS＃11、Windows CSP、JCE 等国际信息安全应用标准。能够屏蔽底层安全设备的硬件差异和复杂的密码实现逻辑，使用户只需在特定业务逻辑中嵌入所需安全功能，然后再进行简单的部署和配置，即可实现基于 PKI 的安全应用，可极大程度的降低应用系统的开发成本，提高开发效率。简单的说，它提供给电子病历等业务应用系统一整套二次开发接口函数，通过它可以很方便的调用密码设备（包括 PKI Server 和数字证书载体）实现各种认证功能。

TSP Server 指时间戳服务器，电子病历系统中产生的各种关键数据，在签名之前可以通过时间戳服务器获取当前的标准时间，并附加在签名之中，不可更改，提供准确的时间证据。

客户端用户需要配置“数字证书载体”（简称 USB KEY），其中存储了由 CA 中心颁布的数字证

书，同时也在保护区存储了代表个人数字签名的私钥。USB KEY 还包含了相关加密算法，配合载体内置的 CPU 运算芯片，可以实现数据的加密和签名等运算功能。USB KEY 通过 PIN 码保护其安全使用，三次尝试输入 PIN 码错误，KEY 将自动锁死，必须交还给 CA 中心进行解锁方能使用。

五、总结

医院 CIS 通过引入合法的第三方安全认证系统，结合数字证书进行应用可使电子病历受到系统的、连续的安全保护，意义主要有以下几点：

1. 电子病历的保密性。保证合法用户才能进入医院 CIS，医院 CIS 的信息在网络传输中和后台存储中不会给他人轻易盗取；
2. 电子病历的完整性。电子病历在医院 CIS 的整个操作过程中得到了有效的完整性验证，保证了医务人员在系统终端所看到的电子病历是正确的、真实的，保证了电子病历的存储过程完整性。
3. 电子病历的不可抵赖性。医务人员在 CIS 中对电子病历的任何操作和输入的电子病历信息都能得到有效证实，电子病历且可追溯、可查证，使电子病历具有不可抵赖性。
4. 电子病历的合法性。电子病历的整个产生全过程是受法律许可的第三方机构监控，并由第三方机构作公证，使电子病历和纸质病历一样受法律认可。

只有通过结合权威的第三方认证机构，把数字证书的应用真正灌输到电子病历系统中，才能彻底解决电子病历的真实可靠问题，真正实现病历从纸质化到电子化的转变，推动医疗信息化的发展。

［参考文献］

［1］广东省数字证书认证中心网站：www.gdca.com.cn

［2］信息周刊 2005 第十一期

［3］《全国卫生信息化发展纲要（2003-2010 年）》

1．李斌 广州医学院第二附属医院信息科助理工程师 510260

联系电话：13632277809 email：eric2778@tom.com

2．朱朝华 广东省数字证书认证中心 510030

联系电话：13925087512 email：zhuzh@gdca.com.cn ）