文章编号:1001-9014(2005)01-0071-05

医疗信息安全体系架构设计

陈晓勐, 张建国
(中国科学院上海技术物理研究所医学影像实验室,上海 200083)

摘要:设计了基于公钥基础设施(PKI)的、并遵从医院管理规范和工作流程模式的证书认证(CA)系统和医学信息数字签字管理信息系统(DSMS).同时实现了与现有各种医院信息系统(如RIS,HIS和PACS)的接口与集成,并完成了对其系统信息的安全验证.由此保证了医学数字信息在院内使用的完整性、认可性和可鉴证性.

关 键 词:公钥基础设施;数字签字管理信息系统;证书认证
中图分类号:TP309.7;R81 **文献标识码**:A

DESIGN INFRASTRUCTURE OF SECURITY SYSTEM IN MEDICAL INFORMATION

CHEN Xiao-Meng, ZHANG Jian-Guo
(Shanghai Institute of Technical Physics, Chinese Academy of Sciences,
Laboratory of Medical Imaging, Shanghai 200083, China)

Abstract: Basing on PKI and obeying the criterion of hospital management and workflow patterns, certificate authority system and digital signature manage system were designed. The interface of CA and DSMS integrating with various hospital information systems (such as RIS, HIS and PACS) was realized and the security verification of system information was completed. Thus, the integrity, authorization and authentication of digital medical information being used in hospitals, were ensured.

Key words: public key infrastructure; digital signature management system; certificate authority

引言

本文所探讨的医疗信息安全是基于公共密钥架构(Public Key Infrastructure, PKI)的信息安全技术.PKI是一种新的安全技术,它由公开密钥密码技术、数字证书、证书发放机构(Certificate Authority, CA)和关于公开密钥的安全策略等基本成分共同组成的.PKI是利用公钥技术实现电子商务安全的一种体系,是一种基础设施,网络通讯、网上交易是利用它来保证安全的.从某种意义上讲,PKI包含了安全认证系统,即安全认证系统-CA/RA系统是PKI不可缺的组成部分.

PKI公钥基础设施是提供公钥加密和数字签名服务的系统或平台,目的是为了管理密钥和证书.一个机构通过采用PKI框架管理密钥和证书可以建立一个安全的网络环境.

1 基于PKI的医院数字信息安全处理架构设计

我们设计基于PKI的医院数字信息安全处理的具体架构如图1所示,它由数字证书系统(CA)、数字签字管理系统(DSMS)等组成.

按照医院行政、医务、技术人员责任划分和管理方式,建立医院信息操作和使用人员身份认证签发(CA)系统的信息数据模型,并使用关系型数据库予以实现,在该CA系统设计中将充分考虑不同人员对信息提交、查询权限分配原则,以使所发展起来的CA系统对医院其它信息系统在某种程度上有机密性和可认证性控制.

按照DICOM对不同种类医学信息实体(Entity)所规定的信息对象定义(IOD)模型研究设计医学信息数字签字管理系统,该系统主要存贮管理每一条

收稿日期:2004-03-16,修回日期:2004-09-24
Received date: 2004-03-16, revised date: 2004-09-24
基金项目:国家杰出青年科学基金(39925009)
作者简介:陈晓勐(1978-),男,山东招远人,硕博连读生,主要从事医疗网络信息安全.

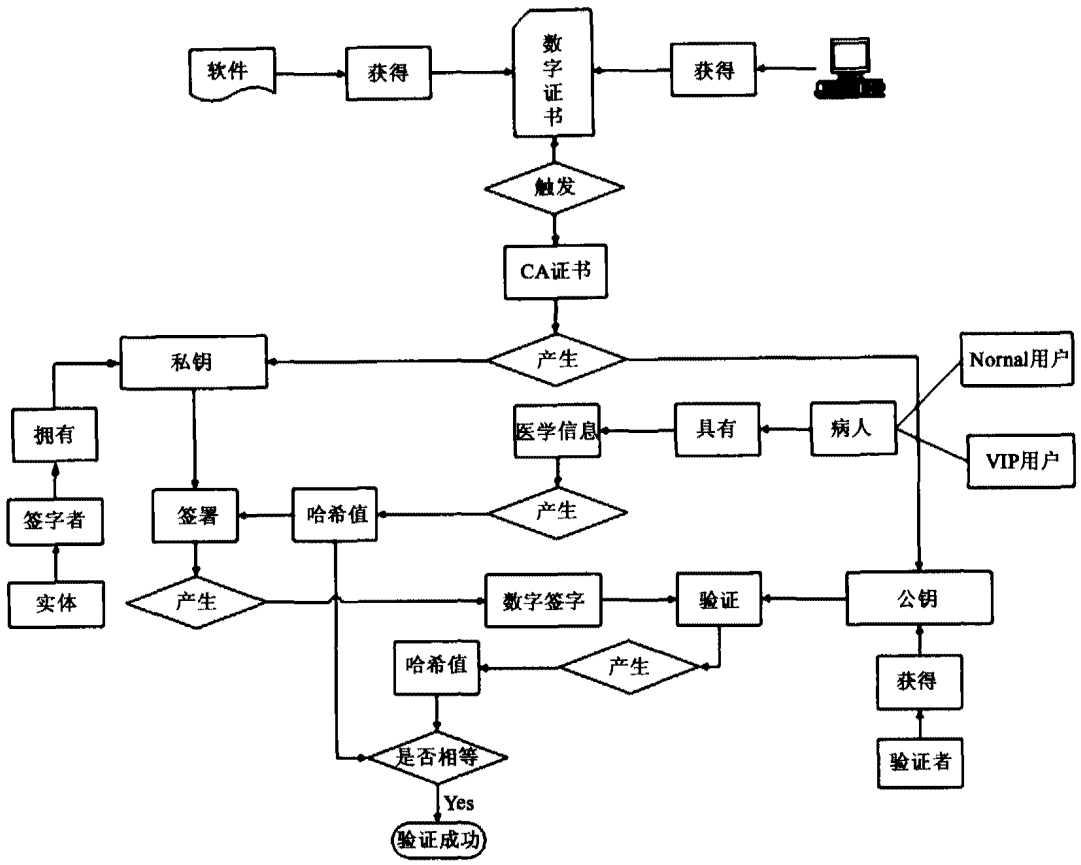

图1 基于PKI的医院数字信息安全处理架构

Fig. 1 Processing infrastructure of healthcare information security basing on PKI

医学信息的数字签字记录及相应的信息识别记录(与其它相应的信息系统共享此记录,并确保其唯一性).该系统将对广泛使用的数字签字过程所产生的哈希(HASH)值与对应的医学信息对象标识符进行存贮与管理.即原有的医学信息对象仍由原来的医学信息管理系统进行管理,而每个具有法律效能的医学诊断或治疗方案信息的数字签字由医院数字签字管理系统进行管理.

在不同计算机医疗工作站平台(UNIX/LINUX, WINDOWS 2000/XP)上使用,对不同种类的医学信息(文字,图像)产生数字签字的软件包.即对采集(产生)的医学数字信息计算其哈希值,并使用RSA公密钥匙加密算法及操作者(责任医生)的私密钥匙计算出该信息的数字签字(包括多重数字签字技术的实现及应用).将该软件包集成到各医学信息系统采集工作站(如RIS报告工作站或PACS图像采集工作站等),对每条具有法律效能的医学信息产生数字签字并传送至数字签字管理系统进行保管以备以后鉴证使用.

对不同种类数字医学信息进行完全验证的软件包,即该软件包可对通过网络输入(待验证)的医学数字信息(如放射门诊报告)计算其哈希值,同时从数字签字管理系统(DSMS)获取该信息相应的数字签字(利用共享信息的唯一标识记录),并根据该信息所附带的原始签字者的标记从CA系统获取原始签字者的公密钥匙,利用公密钥匙破解数字签字者的哈希值,并使其与计算机输入信息的哈希值相比较,以确定输入信息的真伪性.该软件包集成在DSMS之中,并通过网络系统与各种医学信息管理系统中的请求终端及CA系统相连接,通讯将采用TCP/IP协议并利用传输安全层SSL(即TSL)予以实现.

利用CA和DSMS系统构造"电子信封",主要是将"虚拟信封"和"数字信封"概念相融合并进一步引申,即每个"电子信封"是由所要传送信息的整体内容决定的,该信封将包含病人的基本信息、各种医学数据(文字,曲线和图像)相应的数字签字和公密钥匙、以及目的地的信息.具体的构造的方法是:构造一数据结构用于存贮所传送的各种医学信息的数字签字、相应签字者的公密钥匙、病人的基本信息

及接受者的信息.传送方将这一数据结构使用接收方的公密钥匙进行加密处理(使用RSA公密钥匙加密算法)产生电子信封,将加密产生的电子信封嵌入需要传送的数字信息对象(DICOM信息对象或XML文件)的文件头之中,然后使用传送方的私密钥匙对这些嵌入了电子信封的信息对象分别进行加密处理(RSA私密钥匙加密算法).通过网络将这些信息对象传送到接收方.接收方使用传送方的公密钥匙(RSA公密钥匙解密算法)解密各个信息对象,并取出各信息对象中的电子信封,再使用接收方的私密钥匙打开其中一个信封(因信封相同),利用信封中的数字签字和签字者的公密钥匙取出所传信息(多种)的哈希值(多个),并将这些哈希值分别与所接收到的医学信息哈希值(接收后计算出来的)进行比较,得到最终鉴证.信封中所包含的数字签字和公密钥匙分别来自传送方的DSMS和CA系统,以上操作都通过所涉及的软件程序在传送方和接收方自动完成.

2 数字签名验证和加密解密

在医疗信息系统中,实施数字签字的主要实体应该主要是医生和产生图像文件的机器.医生数字签字主要是针对病人图像的诊断信息进行签字,在实际应用中才有其价值,对整个DICOM文件进行数字签字是毫无意义的,所以医生进行数字签字,是对DICOM文件中的部分信息进行数字签字,而这些诊断信息在RIS和HIS系统又是以XML文件形式存在,所以工作站上的签字模块除了要对DICOM文件进行签字处理,还要结合RIS和HIS系统对XML形式的病人诊断同时进行数字签字.

2.1 计算机(机器)数字签字和加密

机器产生数字签字的主要目的是验证图像的来源,检查医疗图像在发送图像工作站和PACS服务器交互操作中是否被恶性地更改,所以机器的数字签字主要针对病人图像等信息.在可以向PACS服务器发送图像的网关工作站上和PACS服务器上,分别部署CA签发给该机器的PKCS12数字证书(包含该机器的私钥和公钥)和CA系统的cer数字证书(只包含CA系统的公钥).当网关工作站从CT、MR、CR医疗仪器设备取得图像向服务器发送图像前,先提取DICOM图像信息,进行数字摘要的计算,然后提取本机数字证书的私有钥匙对该数字摘要进行数字签字,最后进行DICOM头文件数字签名标准化处理,把数字签名和该机器的数字证书等签字信息存入DICOM头文件中.当PACS服务器收到工作站的DICOM文件后,先提取工作站发送过来的图像信息和发送方机器的数字证书,然后从本地提取CA系统X.509标准的数字证书的公钥,验证发送方机器数字证书的有效性,验证通过后,使用该机器数字证书的公钥验证DICOM文件数字签名的有效性,验证通过后再进行影像存档处理,如果验证失败,向DSMS发送验证失败警告,接下来由DSMS进行处理.

这个安全机制只能保证PACS服务器只对拥有CA系统签发的数字证书的机器进行数字签字的图像进行存储和归档,而不能保证发送工作站和PACS服务器之间图像信息不被截取.而对于一些VIP病人的图像信息,这样的安全机制不够的.所以为了确保双方身份认证和数据完整性校验,可以采用SSL(Secure Sockets Layer)数据流加密协议.由于DICOM通讯协议是建立在TCP/IP socket通讯基础之上,所以在建立Socket通讯之前,首先建立SSL握手过程.在握手过程中,客户端和服务器产生一个共享的会话密钥,并且可以验证彼此的身份.这个过程通过交换一系列的消息来完成.

数字签字的用途只是保证了数据的完整性和同一性,而并没有对数据的私密性进行处理.在医疗影像系统中,如果通过影像工作站和PACS服务器或PACS web服务器之间建立SSL安全连接,只能确保数据传输中的完整性,当病人的图像信息,医生的诊断信息以及其它相关信息(比如病人的姓名)通过HTTPS或SSL + DICOM方式下载到客户端后,便无法对医疗信息进行安全控制了,因此对病人的数据信息进行加密处理也是非常重要的,而且必要的.加密方式一般可分为非对称和对称加密两种,非对称加密技术虽然最安全,但是加解密过程过于缓慢,在实际应用中使用非对称加密对大量数据是不太可能的,所以在应用中一般采用非对称和对称相结合的方式对数据进行加密处理.对称加解密过程中,由于只使用一把钥匙,所以钥匙在加解密双方的传输变得尤为重要.

网关程序从医疗仪器取得图像并做完机器数字签字后,自动产生固定长度的对称加密钥匙(通常采用DES算法或更安全的TripleDES算法),从DICOM文件中提取图像信息进行对称加密处理,与PACS服务器建立SSL安全连接,把所有加密过的DICOM发送到PACS服务器上,随后再与DSMS系统建立SSL连接,把加密钥匙,加密算法,图像标识

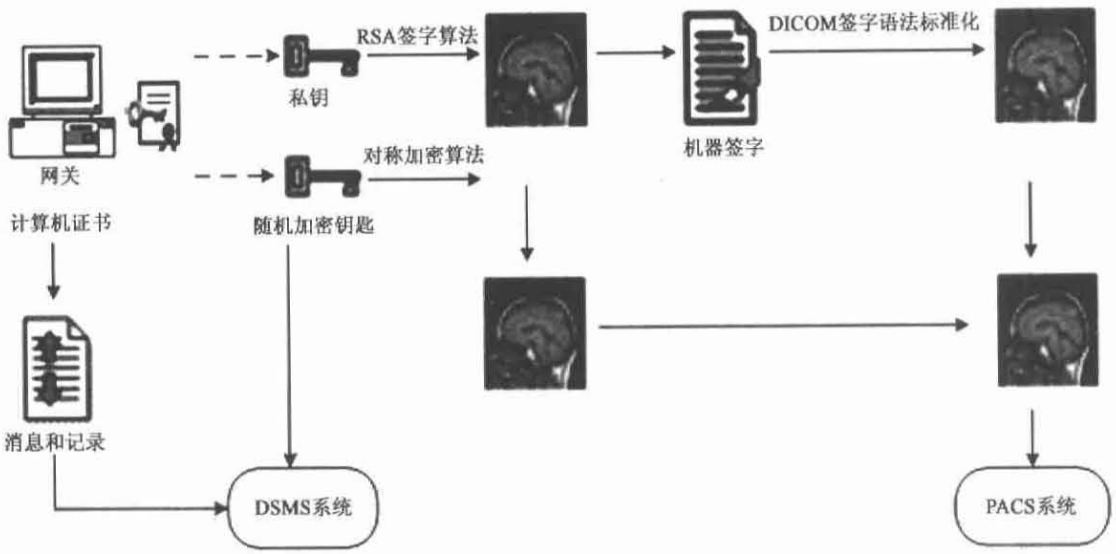

图2 网关签字和加密处理的流程图
Fig. 2 Digital signature and encryption processing in the gateway

以及数字签字等信息发送给 DSMS 系统. 对称加密钥匙如果隐藏在 DICOM 文件中,无法控制图像的查看权限和适应医院内部多点诊断的要求. 但是这种方式很适合远程医疗安全加密,这将在后面数字信封中作具体说明. 整个网关图像发送过程可以确定图像的来源,保障图像传输途中不被获取以及显示工作站不能轻易读取 DICOM 文件信息.

以下是网关机器在后台作签字和加密处理的流程图:

2.2 医生的签字和加密

通过 CA 系统以 PKCS12 证书形式把签字私钥发放给具有签字权限的医生,私钥存储在医生手中的加密外设中,如 IC 卡,U 盘等. 在医疗影像工作站的医生获取外部设备上的私钥后,对 DICOM 文件内的部分信息(例如 structure report 等)进行 RSA 算法的数字签字,然后按照 DICOM 3.0 的 Supplement41 数字签字的补充标准,把数字签字的基本信息加入 DICOM 头文件中,标准化处理,然后把图像发送到 PACS 服务器,覆盖原有 DICOM 文件的同时将 XML 形式的诊断报告加密处理后提交给 RIS 系统的 web 服务器. 完成这些操作后,提交信息给 DSMS,报告数字签名完成. 数字签字管理系统记录下签字人 ID 标识,图像标识信息,签字时间等,以备以后验证使用.

医生在影像工作站读取 DICOM 文件图像信息前,先必须提供由 CA 签发的个人证书并与 DSMS 系统建立 SSL 安全连接,DSMS 验证用户的身份和权限后,将图像信息解密的对称钥匙传递给显示工作站. 图像解密完成后, DICOM 图像才能被解密到工作站供医生诊断. 当需要验证该图像的数字签字时,首先提取 DICOM 头文件信息,其中包括签字对象信息、对象信息的 hash 值和签字者的公钥等相关信息. 验证者接着就可以根据 RSA 签字算法对该图像进行验证,验证的结果、验证人 ID 标识、图像信息唯一标识和验证时间等信息同时提交给 DSMS. 医生诊断结束关闭程序后,工作站程序将自动删除解密后的本地 DICOM 图像. 在某些情况下,可能还需要对病人 DICOM 文件中的 Structure Report 信息和 RIS 系统中的 XML 诊断报告同步加密处理. DICOM 文件的诊断信息加密处理过程与上面提到的机器对图像信息加密基本相同,只是在医生诊断报告数字签字完成后再对信息进行加密,同时在程序后台 DICOM2XML 转换过程中,按照 W3C 组织的 XML SECURITY 标准同时进行相应的转换处理,确保 RIS 和 PACS 信息的一致性. 而解密报告信息是在验证医生数字签字验证之前完成.

3 数字信封(Digital Envelop)

随着远程医疗系统的发展,医院之间信息交换的安全变得尤为重要. 在医院双方都有自己的子 CA 系统情况下,可以把各自医院的 CA 证书拿到第三方去签字认证,两家医院由此建立了信任关系. 电子信封主要包括各种医学数据(文字,曲线和图像),主要是以 XML 和 DICOM 文件形式存在,数字签字

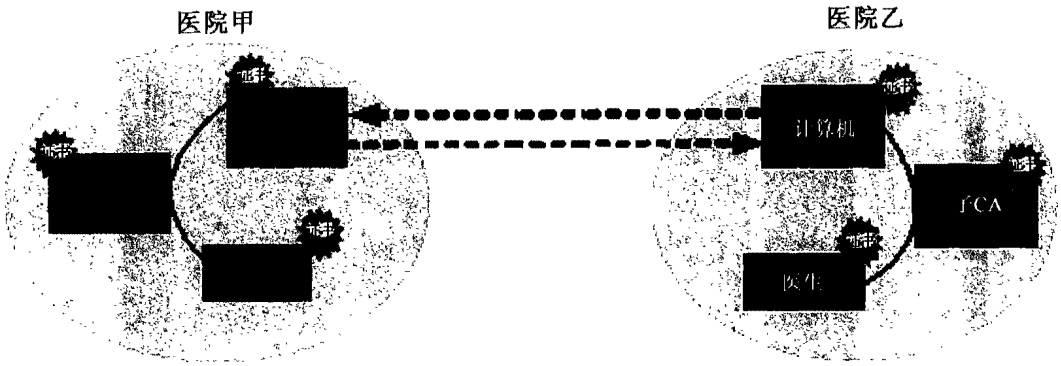

图 3　医院间信息交换图
Fig. 3　Exchange Information in Hospitals

以及其它一些相关信息都可以标准化地存储在 XML 和 DICOM 文件中,而用来加密的对称钥匙,可以通过非对称加密方式保存在文件. 发送方提取接收方机器公钥证书中的公钥,对加密钥匙进行 RSA 非对称加密,并把加密的钥匙和算法等相关信息嵌入到 DICOM 和 XML 文件中,接收方从 Internet 收到电子信封后,通过自己接收方机器的私钥可以进行解密处理. 解密后的 DICOM 和 XML 文件就可以用于远程医疗诊断.

有时候可能出现某些信息只能某个医生阅读的情况,或者接收方医院没有 CA 系统的情况下,这就需要利用接收方医院医生的公钥证书对加密钥匙进行非对称加密了.

4　结语

由于我国医院的信息安全性研究和技术实现几乎是空白,几乎所有的医院信息系统都没有信息安全措施(大都使用系统的 Password 方法)和使用信息安全鉴证技术来保证医学信息系统的真实性、完整性和可靠性及其相应的法律严肃性. 任何责任报告的认证仍然使用手签纸张报告完成,为了在医院实现无纸化,建立医院的数字证书系统(CA)和数字签字管理系统(DSMS)是十分重要的.

REFERENCES

[1] Huang K H. *PACS Basic Principles and Applications*[M]. USA: A John Wiley & Sons, Inc., Publication, 1999.

[2] Zhang J, Chen X. Developing security architecture for both in-house healthcare information Systems and electronic patient record[J], *SPIE*, 2003, **5033**: 392—403.

[3] William Stallings. *Cryptography and Network Security Principles and Practice* [M]. US: Prentice Hall, 2001: 123—197.