DOI: 10.13657/j.cnki.gxkxyxb.2005.s1.044

数字签名在电子病历中的应用

Application of Digital Signature in Electronic Medical Record System

刘 茜

Liu Qian

(广西数字证书认证中心有限公司,广西南宁 530022)

(Guangxi Certificate Authority Center Ltd., Nanning, Guangxi 530022, China)

摘要:介绍数字签名的相关概念,以及电子病历中身份认证、数字签名与验证等数字签名技术的应用。数字签名技术的实施,可以有效解决电子病历的安全性、机密性和合法性等问题。

关键词:数字签名 电子病历 数字证书

中图法分类号:TP399 文献标识码:A 文章编号:1002-7378(2005)S0-0131-02

Abstract In this paper, the concept of Digital Signature of how to distinguish identity, Digital Signature and verifying identity by the technique of Digital Signature in the Electronic Medical Record System is introduced. With technique of Digital Signature, we can provide the security, the safeguard of patient's intimacy, the legitimacy etc. in the electronics medical record.

Key words digital signature, electronic medical record system, digital certificate

电子病历是医疗信息化的一部分,它不仅包括患者纸张病历的原有内容,而且反映患者整个的医疗过程,储存了患者全部的医疗信息,包括病史、各种检验检查和影像资料,是对个人医疗信息及其相关处理过程综合化的体现。

电子病历的最大优势在于超越传统病历的管理模式,提供电子存储、查询、统计、电子数据交换和互操作等功能,而这些功能中有些是传统病历无法达到的。

在我国,电子病历的推广应用也得到了相关部门的高度重视,卫生部曾强调"国内三甲以上的医院都需要实行信息化管理",而电子病历是医院实行信息化管理的一个重要组成部分。目前,电子病历的推广还面临一些新的问题,主要集中在访问控制、身份认证、信息机密性和信息抵赖性等方面,而利用电子签名技术则可以从根本上解决这些问题[1]。

目前,可以通过多种技术手段实现电子签名,但比较成熟的,使用方便的,具有可操作性的,在世界先进国家和我国普遍使用的电子签名技术是基于PKI(Public Key Infrastructure)的数字签名技术。本文介绍了数字签名的相关概念,以及数字鉴名技术在电子病历中的应用。

1 数字签名的相关概念[1]

数字签名采用规范化的程序和科学化的方法,用于鉴定签名人的身份以及对某项数据电文内容信息的认可,而且还能验证出文件的原文在传输过程中是否变动。

PKI是一个用公钥概念与技术来实施和提供安全服务的普遍适用的安全基础设施,它遵循标准的公钥加密技术,为电子商务、电子政务、网上银行和网上证券业,提供一整套安全保证的基础平台。用户利用PKI基础平台所提供的安全服务,能在网上实现安全地通信。PKI这种遵循标准的密钥管理平台,能够为所有网上应用,透明地提供加解密和数字签名等安全服务所需要的密钥和证书管理。

认证机构CA(Certificate Authority)是PKI的核心执行机构,是PKI的主要组成部分,一般简称为CA,在业界通常把它称为认证中心。它是一种具有权威性、可信任性和公正性的第三方机构。

收稿日期:2005-09-12

作者简介:刘 茜(1981-),女,广西全州人,助理工程师,主要从事PKI/CA数字证书认证服务工作。

PKI签名的核心元素是由 CA签发的数字证书。它所提供的 PKI服务就是认证、数据完整性、数据保密性和不可否认性。它的任务就是利用证书公钥和与之对应的私钥进行加 解密,并产生对数字电文的签名及验证签名。

2 数字签名技术在电子病历中的应用

电子病历文件进行数字签名、在网上传输的技术实现过程大致如下: 首先要在网上进行身份认证,然后再进行签名,最后是对签名的验证。

2.1 身份认证

PKI提供的服务首先是认证,即身份识别与鉴别,确认实体即为自己所声明的实体。认证的前提是甲乙双方都具有第三方 CA所签发的证书,认证分单向认证和双向认证[2]。

在电子病历中采用的是双向认证方式。双向认证是电子病历服务器和电子病历操作者 (医生、护士和系统管理员)在网上通信时,服务器不但要认证用户的身份,用户也要认证服务器的身份。医生、护士在通过 SSL方式登录应用系统时,系统会提示他们查看服务器证书,查看服务器证书可以验证服务器的真实性和有效性,然后系统会要求医生、护士出示自己的用户证书,当服务器验证了用户的证书真实性和有效性之后,则实现了双向认证。

2.2 数字签名与验证过程

网上通信的双方,在互相认证身份之后,即可发送签名的数据电文。数字签名的全过程分两大部分,即签名与验证。如图 1所示, A医生对数据进行签名,将原文用哈希算法求得数字摘要,用 A医生的签名私钥对数字摘要进行加密得到数字签名, A医生将原文与数字签名一起存储在服务器上,等待 B医生接收。B医生接收后需要验证签名, B医生使用 A医生的公钥解密数字签名,得出数字摘要,同时将 A医生的原文采用同样哈希算法又得一新的数字摘要,将两个数字摘要进行比较,如果二者匹配,说明经数字签名的电子文件传输成功。这一过程实现了签名无改动,签署的内容和形式无改动的要求,在实际应用中这些操作均是由程序处理。

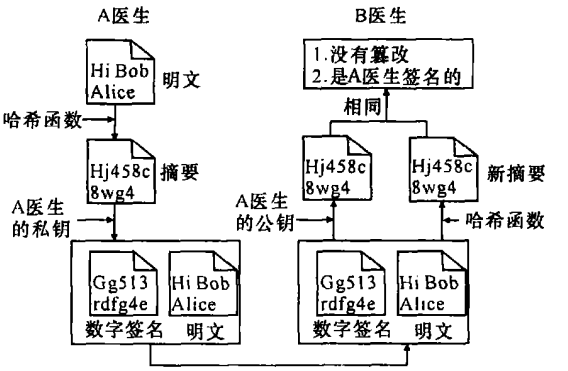

图 1 电子病历中的数字签名流程

3 结束语

电子病历中使用 PKI的数字签名技术有以下 3个特点[3]: (1)该电子文件是由签名者所签名,电子文件来源于该签名者。签署时电子签名的数据由电子签名人所控制; (2)被签名的电子文件确实是经签名者认可的,签名者使用自己的私钥进行签名,并得到验证,具有不可抵赖性; (3)电子文件在传输中没有被篡改,保持了数据的完整性。签署后对电子签名的任何改动都能够被发现。以上特点使电子病历实现了访问控制、身份认证、信息机密性和信息防抵赖性等要求,有效保证了电子病历的安全性、机密性和合法性等问题。

参考文献:

[1] 黄 彦.电子签名法律效力研究 [J].计算机安全, 2004, (12): 51-54.

[2] Eric Rescorla. SSL与 TLS[M].崔 凯译.北京: 中国电力出版社出版, 2002.

[3] 黄建初.《中华人民共和国电子签名法》释义及实用指南 [M].北京: 中国民主法制出版社, 2004.

(责任编辑: 韦廷宗)