ICS 35.240.80
C 07

中华人民共和国国家标准化指导性技术文件

GB/Z 21716.3—2008

健康信息学　公钥基础设施(PKI)
第3部分:认证机构的策略管理

Health informatics—Public key infrastructure(PKI)—
Part 3: Policy management of certification authority

2008-04-11 发布

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/Z 21716《健康信息学　公钥基础设施(PKI)》分为3个部分：

——第1部分：数字证书服务综述；

——第2部分：证书轮廓；

——第3部分：认证机构的策略管理。

本部分为GB/Z 21716的第3部分。

本部分是参照ISO 17090-3/DIS：2006《健康信息学　公钥基础设施(PKI)　第3部分：认证机构的策略管理》而制定的。

本部分由中国标准化研究院提出。

本部分由中国标准化研究院归口。

本部分起草单位：中国标准化研究院、中国人民解放军总医院、中国人民武装警察部队指挥学院。

本部分主要起草人：陈煌、任冠华、董连续、刘碧松、尹岭、韵力宇。

引　言

为了降低费用和成本，卫生行业正面临着从纸质处理向自动化电子处理转变的挑战。新的医疗保健模式增加了对专业医疗保健提供者之间和突破传统机构界限来共享患者信息的需求。

一般来说，每个公民的健康信息都可以通过电子邮件、远程数据库访问、电子数据交换以及其他应用来进行交换。互联网提供了经济且便于访问的信息交换方式，但它也是一个不安全的媒介，这就要求采取一定的措施来保护信息的保密性和保密性。未经授权的访问，无论是有意的还是无意的，都会增加对健康信息安全的威胁。医疗保健系统有必要使用可靠信息安全服务来降低未经授权访问的风险。

卫生行业如何以一种经济实用的方式来对互联网中传输的数据进行适当的保护？针对这个问题，目前人们正在尝试利用公钥基础设施(PKI)和数字证书技术来应对这一挑战。

正确配置数字证书要求将技术、策略和管理过程绑定在一起，利用“公钥密码算法”来保护信息，利用“证书”来确认个人或实体的身份，从而实现在不安全的环境中对敏感数据的安全交换。在卫生领域中，这种技术使用鉴别、加密和数字签名等方法来保证对个人健康记录的安全访问和传输，以满足临床和管理方面的需要。通过数字证书配置所提供的服务(包括加密、信息完整性和数字签名)能够解决很多安全问题。为此，世界上许多组织已经开始使用数字证书。比较典型的一种情况就是将数字证书与一个公认的信息安全标准联合使用。

如果健康应用需要在不同组织或不同辖区之间(如为同一个患者提供服务的医院和社区医生之间)交换信息，则数字证书技术及其支撑策略、程序、操作的互操作性是最重要的。

实现不同数字证书实施之间的互操作性需要建立一个信任框架。在这个框架下，负责保护个人信息权利的各方要依赖于具体的策略和操作，甚至还要依赖于由其他已有机构发行的数字证书的有效性。

许多国家正在采用数字证书来支持国内的安全通信。如果标准的制定活动仅仅局限于国家内部，则不同国家之间的认证机构(CA)和注册机构(RA)在策略和程序上将产生不一致甚至矛盾的地方。

数字证书有很多方面并不专门用于医疗保健，它们目前仍处于发展阶段。此外，一些重要的标准化工作以及立法支持工作也正在进行当中。另一方面，很多国家的医疗保健提供者正在使用或准备使用数字证书。因此，本指导性技术文件的目的是为这些迅速发展的国际应用提供指导。

本指导性技术文件描述了一般性技术、操作以及策略方面的需求，以便能够使用数字证书来保护健康信息在领域内部、不同领域之间以及不同辖区之间进行交换。本指导性技术文件的最终目的是要建立一个能够实现全球互操作的平台。本指导性技术文件主要支持使用数字证书的跨国通信，但也为配置国家性或区域性的医疗保健数字证书提供指导。互联网作为传输媒介正越来越多地被用于在医疗保健组织间传递健康数据，它也是实现跨国通信的唯一选择。

本指导性技术文件的三个部分作为一个整体定义了在卫生行业中如何使用数字证书提供安全服务，包括鉴别、保密性、数据完整性以及支持数字签名质量的技术能力。

本指导性技术文件第1部分规定了卫生领域中使用数字证书的基本概念，并给出了使用数字证书进行健康信息安全通信所需的互操作方案。

本指导性技术文件第2部分给出了基于国际标准X.509的数字证书的健康专用轮廓以及用于不同证书类型的IETF/RFC 3280中规定的医疗保健轮廓。

本指导性技术文件第3部分用于解决与实施和使用医疗保健数字证书相关的管理问题，规定了证书策略(CP)的结构和最低要求以及关联认证操作声明的结构。该部分以IETF/RFC 3647的相关建议为基础，确定了在健康跨国通信的安全策略中所需的原则，还规定了健康方面所需的最低级别的安全性。

健康信息学　公钥基础设施(PKI)
第3部分:认证机构的策略管理

1　范围

本部分为在医疗保健过程中包括配置使用数字证书在内的证书管理问题提供了指南。它规定了证书策略的结构和最低要求,包括认证实施声明的结构等。它还给出了为实现跨国界通信所需的医疗保健安全策略的基本原则,以及专门针对医疗保健方面的安全要求的最小级别。

2　规范性引用文件

下列文件中的条款通过GB/Z 21716—2008的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 19716—2005　信息技术　信息安全管理实用规则

GB/Z 21716.1—2008　健康信息学　公钥基础设施(PKI)　第1部分:数字证书服务综述

GB/Z 21716.2—2008　健康信息学　公钥基础设施(PKI)　第2部分:证书轮廓

IETF/RFC 3647:2003　Internet X.509公钥基础设施证书策略和认证实施框架

3　术语和定义

GB/Z 21716.1给出的术语和定义适用于本部分。

4　缩略语

下列缩略语适用于本部分。

AA　属性机构　attribute authority

CA　认证机构　certification authority

CP　证书策略　certificate policy

CPS　认证操作声明　certification practice statement

CRL　证书撤销列表　certificate revocation list

OID　对象标识符　object identifier

PKC　公钥证书　public key certificate

PKI　公钥基础设施　public key infrastructure

RA　注册机构　registration authority

TTP　可信第三方　trusted third party

5　在医疗保健语境中数字证书策略管理的要求

5.1　概述

在医疗保健语境中部署数字证书必须实现下列目标,以便有效保障个人健康信息通信的安全性:

a)　对于参与进行个人健康信息的电子交换过程中所有人员、机构、应用软件、设备等,必须与唯一的和容易区分的名称安全可靠地绑定。