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 21716.1—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

**Health informatics—Public Key Infrastructure (PKI) —
Part 1: Overview of digital certificate services**

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1部分。

本部分是参照ISO 17090-1(DIS)《健康信息学　公钥基础设施(PKI) 第1部分：数字证书服务综述》而制定的。

本部分对ISO 17090-1(DIS)中的一些错误地方进行了改正，具体如下：

——原文在3.2.4中的注中指出要参见“数据原发鉴别”和“对等实体鉴别”，但是在原文中没有出现“对等实体鉴别”这个术语，因此本部分在3.2.28中增加了术语“对等实体鉴别”。

——原文在5.3的最后一段中指出“使用数字证书的剧本详见附录B。”但是本部分没有附录B，根据上下文内容判断应改为“使用数字证书的剧本详见附录A。”

——原文在8.3的第三段的最后一句话中指出“在这些情况中，按照IETF/RFC 3281和本指导性技术文件第2部分的6.3.3的第5条以及7.1.5的规定，……”，但是第2部分没有7.1.5，根据上下文内容判断应改为“在这些情况中，按照IETF/RFC 3281和本指导性技术文件第2部分的6.3.3的第5条以及7.2.5的规定，……”。

——原文在8.3的第六段的最后一句话中指出“因此，在本指导性技术文件第2部分的4.1中对PKC身份证书类型给出了称为HCRole的扩展。”但是根据上下文内容判断应改为“因此，在本指导性技术文件第2部分的5.1中对PKC身份证书类型给出了称为HCRole的扩展。”

——在原文中，参考文献3、8、9、17、18、20、21、23-30并没有标出引用位置，因此根据专家意见将其删除。

本部分的附录A为资料性附录。

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：任冠华、陈煌、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私密性和保密性。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)需要交换健康信息，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，确定了在健康信息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1部分:数字证书服务综述

1　范围

本部分定义了医疗保健数字证书的基本概念,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。本部分还给出了进行健康信息通信的主要利益相关方以及使用数字证书进行健康信息通信所需的主要安全服务。

本部分简述了配置医疗保健数字证书所需的公钥密码算法和基本构件,并进一步介绍了不同类型的数字证书(包括标识证书、用于可依赖方的关联属性证书、自签名认证机构(CA)证书)以及CA等级体系与桥接结构。

本部分适用于健康信息安全人员、专门从事健康信息应用软件的设计者和开发者的使用。

2　规范性引用文件

下列文件中的条款通过GB/Z 21716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/Z 21716.2—2008　健康信息学　公钥基础设施(PKI)　第2部分:证书轮廓

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

3　术语和定义

下列术语和定义适用于本部分。

3.1　医疗保健语境术语

3.1.1

应用　application

作为私有加密密钥持有方的、可标识的计算机运行软件程序。

注1:在本语境中,应用可以是医疗保健信息系统中使用的任一软件程序。它也包括那些在治疗或诊断中不直接使用的应用。

注2:在一定管辖范围内,可以包括正规医疗设备软件程序。

3.1.2

设备　device

作为私有加密密钥持有方的、可标识的计算机控制仪器或器械。

注1:设备包括能够满足上述定义的正规医疗设备。

注2:在本语境中,设备指健康信息系统中使用的任一设备。它也包括那些在治疗或诊断中不直接使用的设备。

3.1.3

医疗保健参与者　healthcare actor

参与与健康相关的通信并对安全服务所用数字证书有需求的正规健康专业人员、非正规健康专业人员、受委托医疗保健提供者、支持组织雇员、患者/消费者、医疗保健组织、设备或应用。