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。

3.1.4

医疗保健组织　healthcare organization

主要行为与健康服务或健康促进相关的官方注册组织。

示例：医院、医疗保健网站提供者和医疗保健研究院所。

注1：一般认为，医疗保健组织对其行为负有法律责任，但是不需要在卫生领域中注册具体的角色。

注2：按X.501所述，组织内部的一个部门称为一个组织单元。

3.1.5

非正规健康专业人员　non-regulated health professional

由医疗保健组织雇佣的、但不是正规健康专业人员的个人。

示例：负责安排预约的医疗接待员或帮助进行患者护理的护工。

注：当然，即使雇员没有被独立于雇主的组织对其专业能力进行的权威认定，也并不意味着这些雇员在提供服务方面是不专业的。

3.1.6

患者　patient

消费者　consumer

健康相关服务的接受者和健康信息系统中的参与者。

3.1.7

隐私权　privacy

防止因不正当或非法收集和使用个人数据而对个人的私生活或私事进行侵犯。

[GB/T 5271.8—2001]

3.1.8

正规健康专业人员　regulated health professional

由国家认证组织授权其具有提供特定健康服务资格的个人。

示例：内科医生、注册护士和药剂师。

注1：在不同的国家，针对不同的专业，注册或授权组织的类型是不同的。国家认证组织包括本地或区域政府机构、独立的专业协会和其他正式的国家公证处。它们的领域可能相互独立，也可能存在着交叉。

注2：在本定义中，国家认证组织并不一定是指国家控制的专业注册系统，它应是为了便于国际交流而建立的一个公认的健康专业注册组织的全国性目录。

3.1.9

受委托医疗保健提供者　sponsored healthcare provider

在其操作范围内并不是一个健康专业人员、但由医疗保健组织支持并在社区中开展活动的健康服务提供者。

示例：负责特殊群体中毒品和酒精教育的工作官员，发展中国家的健康援助人员。

3.1.10

支持组织　supporting organization

向医疗保健组织提供服务的经过官方注册的组织，但它不提供健康服务。

示例：健康基金组织(如保险机构、药品和其他物品的供应商)。

3.1.11

支持组织雇员　supporting organization employee

医疗保健组织或支持组织雇佣的个人。

示例：病历打字员、医疗保险索赔裁决人和药品订单登记办事员。

3.2　**安全服务术语**

3.2.1

访问控制　access control

一种保证手段，即数据处理系统的资源只能由被授权实体按授权方式进行访问。

[GB/T 5271.8—2001]

3.2.2

可确认性 accountability

可核查性

这样一种性质，它确保对一个实体的操作可以唯一地追踪到该实体。

[GB/T 9387.2—1995]

3.2.3

非对称密码算法 asymmetric cryptographic algorithm

在执行加密或与之相应的解密中用于加密和解密的密钥是不相同的算法。

[GB/T 18794.1—2002]

3.2.4

鉴别 authentication

通过将标识符与其鉴别码进行安全关联来可靠识别安全主体的过程。

注：也可参见“数据原发鉴别”和“对等实体鉴别”。

3.2.5

授权 authorization

授予权限，包括允许基于访问权的访问。

[GB/T 9387.2—1995]

3.2.6

可用性 availability

根据授权实体的请求可被访问与使用。

[GB/T 9387.2—1995]

3.2.7

密文 ciphertext

经加密处理而产生的数据，其语义内容是不可用的。

[GB/T 9387.2—1995]

3.2.8

保密性 confidentiality

机密性

这一性质使信息不泄漏给非授权的个人、实体或进程，不为其所用。

[GB/T 9387.2—1995]

3.2.9

密码学 cryptography

这门学科包含了对数据进行变换的原理、手段和方法，其目的是掩藏数据的内容，防止对它作了篡改而不被识破或非授权使用。

[GB/T 9387.2—1995]

3.2.10

密码算法 cryptographic algorithm

加密算法

密码 cipher

一种数据传输方法，用于隐藏其信息内容，防止被漏检修改和/或未经授权的使用。

3.2.11

数据完整性 data integrity

这一性质表明数据没有遭受以非授权方式所作的篡改或破坏。

[GB/T 9387.2—1995]

3.2.12

数据原发鉴别 data origin authentication

确认接受到的数据的来源是所要求的。

[GB/T 9387.2—1995]

3.2.13

解密 decipherment

解密处理 decryption

从密文中获取对应的原始数据的过程。

[GB/T 5271.8—2001]

注：可将密文再次加密，这种情况下单次解密不会产生原始明文。

3.2.14

数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元所作的密码变换(见3.2.9)，这种数据或变换使数据单元的接受者能够确认数据单元来源和数据单元的完整性，并保护数据，防止被人(例如接收者)进行伪造。

[GB/T 9387.2—1995]

3.2.15

加密 encipherment

加密处理 encryption

对数据进行密码变换(见3.2.9)以产生密文。

[GB/T 9387.2—1995]

3.2.16

标识 identification

以使数据处理系统能够识别实体的测试性能。

3.2.17

标识符 identifier

在用相应的鉴别码进行进一步确认之前，用于说明身份的信息片段。

[ENV 13608-1]

3.2.18

完整性 integrity

证明在传输过程中没有以任何方式对消息内容进行有意或偶然的改变。

[GB/T 9387.2—1995]

3.2.19

密钥 key

控制加密和解密操作的一序列符号。

[GB/T 9387.2—1995]

3.2.20

密钥管理 key management

在一种安全策略指导下密钥的产生、存储、分配、删除、归档及应用。

[GB/T 9387.2—1995]

3.2.21

抗抵赖 non-repudiation

提供可被任一方验证的数据完整性和来源(都是不可更改的)证据的服务。

[ASTM,19]

3.2.22

私有密钥　private key

私钥

在非对称密码算法中使用的并且其拥有者是受限制(通常只能由一个实体拥有)的密钥。

[GB/T 18794.1—2002]

3.2.23

公共密钥　public key

公钥

在非对称密码算法中使用的并且可以被公开的密钥。

[GB/T 18794.1—2002]

3.2.24

角色　role

与一项任务相关的行为集合。

3.2.25

安全性　security

可用性、保密性、完整性和可确认性的组合。

[ENV 13608-1]

3.2.26

安全策略　security policy

为保障计算机安全所采取的行动计划或方针。

[GB/T 5271.8—2001]

3.2.27

安全服务　security service

由参与通信的开放系统的层所提供的服务,它确保该系统或数据传送具有足够的安全性。

[GB/T 9387.2—1995]

3.2.28

对等实体鉴别　peer-entity authentication

确认有关的对等实体是所需的实体。

[GB/T 9387.2—1995]

3.3　公钥基础设施相关术语

3.3.1

属性机构　attribute authority;AA

通过发布属性证书来分配权限的机构。

3.3.2

属性证书　attribute certificate

由属性机构进行数字签名的数据结构,它将某些属性值与其持有者的标识绑定在一起。

3.3.3

授权机构证书　authority certificate

发给认证机构或属性机构的证书。

3.3.4

证书　certificate

公钥证书。

3.3.5

证书分发 certificate distribution

向安全主体发布和传输证书的行为。

3.3.6

证书扩展 certificate extension

X.509 证书的扩展域(简称为扩展),提供了将附加属性与用户或公钥关联起来和进行证书层次结构管理的方法。

注:证书扩展可以是必要的(即如果使用证书的系统遇到一个不能识别的必要扩展时,则必须拒绝该证书。),也可以是非必要的(即如果使用证书的系统不能识别扩展,则可以将其忽略)。

3.3.7

证书生成 certificate generation

创建证书的行为。

3.3.8

证书管理 certificate management

与证书相关的程序,即证书生成、证书分发、证书归档和撤销。

3.3.9

证书轮廓 certificate profile

关于证书类型的结构和许可内容的规定。

3.3.10

证书撤销 certificate revocation

即使证书没有过期,但由于证书不再可信,导致对证书与其持有方(或安全主体持有者)之间所有可靠链接进行删除的行为。

3.3.11

证书持有方 certificate holder

有效证书主体的实体。

3.3.12

证书验证 certificate verification

验证证书是否可信。

3.3.13

认证 certification

第三方作出保证数据处理系统的全部或部分符合安全要求的过程。

[GB/T 5271.8—2001]

3.3.14

认证机构 certification authority;CA

证书机构

证书认证机构

证书发行方 certificate issuer

负责创建和分配证书,受用户信任的权威机构。用户可以选择该机构为其创建密钥。

注1:术语"CA"中的机构并不特指政府机构,它只是说明该机构是可信任的。

注2:"证书发行方"可能是一个更合适的术语,但广泛使用的是"CA"。

[GB/T 16264.8—2005]

3.3.15

证书策略　certificate policy;CP

指定的一组规则,用于指出证书对具有通用安全需求的特定应用组和/或类的适用性。

[IETF/RFC 3647]

3.3.16

认证操作声明　certification practices statement;CPS

认证机构在发行证书方面的操作声明。

[IETF/RFC 3647]

3.3.17

公钥证书　public key certificate;PKC

将身份与公钥绑定的 X.509 公钥证书。在客户端证明它拥有 PKC 中公钥对应的私钥后,可以使用身份来支持基于身份的访问控制决策。

[IETF/RFC 3280]

3.3.18

公钥基础设施　public key infrastructure;PKI

在密钥持有方和可依赖方二者的关系中使用的基础设施。它允许可依赖方将与密钥持有方相关的证书用于一个以上的应用,其中该应用使用依赖于公钥的安全服务。PKI 包括认证机构、证书数据结构、可依赖方获得证书撤销状态的当前信息的方法、认证策略和验证认证操作的方法。

3.3.19

资质证书　qualified certificate

主要目的是在公共抗抵赖服务中标识某人具有高级担保的证书。

注:决定一个证书是否应被认为是涉及法规的"资格证书"的有效机制不在本部分规定范围之内。

3.3.20

注册机构　registration authority;RA

负责标识和鉴别证书主体的实体,但其不签名或发行证书(即 RA 受委托代表 CA 执行特定的任务)。

[IETF/RFC 3647]

3.3.21

可依赖方　relying party

证书的接收方,它依靠证书和/或通过该证书验证的数字签名进行活动。

[IETF/RFC 3647]

3.3.22

第三方　third party

数据发送方和数据接收方之外的另一参与方。它被要求实施通信协议部分的安全功能。

3.3.23

可信第三方　trusted third party;TTP

对于安全协议而言被认为是可信第三方。

注:本术语被用于许多 ISO/IEC 国际标准和其他主要描述 CA 服务的文献中。然而,该定义是比较宽泛的,它包括诸如时戳和由第三方保存的契据之类的服务。

[ENV 13608-1]

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
ECG	心电图	electrocardiogram
EHR	电子健康记录	electronic health record
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 医疗保健语境

5.1 医疗保健证书持有方和可依赖方

为了便于描述数字证书需求，特对如下的参与者类别进行说明。但这并不意味着其他的类别和定义不适用于其他的语境。

此处关注的是健康通信中直接涉及并要求用于安全服务的 PKI 证书的医疗保健参与者。医疗保健参与者的定义见 3.1。表 1 给出了医疗保健参与者类别。

表 1 医疗保健参与者类别

个人	正规健康专业人员
	非正规健康专业人员
	患者/消费者
	受委托医疗保健提供者
	支持组织雇员
组织	医疗保健组织
	支持组织
其他实体	设备
	正规医疗服务
	应用

除了上述参与者外，大规模配置数字证书要求 CA 和 RA 必须是整个系统的一部分，并且这些组织应根据自身的权限成为重要的证书持有者。

一些医疗保健工作者与多个医疗保健组织有关。卫生行业中的一个基本要求就是通过一致性收费和证书多样性来避免重复或冗余注册。

在医疗保健语境中，RA 的职能是把参与者标识为一个有效的、执行给定角色的健康专业人员，或把消费者标识为对其信息具有所有权的个人。对于医生工作的支持人员（医疗接待员、收费员、文件管理员等）也需要一种注册方法。这些个人与诸如国家、省/市/自治区卫生行政部门负责的医院之类的机构无关。

5.2 参与者示例

5.2.1 正规健康专业人员

正规健康专业人员的例子如内科医生、牙医、注册护士和药剂师。不同的国家官方规定/认可的健康专业分类不同。在将来的国际标准化工作，一项重要的任务是创建一个关于健康专业分类的全球映

射，但是对于本指导性技术文件的目的而言，需假设只有非常宽泛的分类才能被国际认可。在本指导性技术文件第2部分中提出的数据结构允许同时使用一种宽泛的国际分类和一种更详细的、国家级或是地区级的分类，因为在某些国家，正规健康专业人员是由地方部门进行管理的。

5.2.2 非正规健康专业人员

非正规健康专业人员是由医疗保健组织雇佣的、不是正规健康专业人员的个人，它包括医疗秘书、档案助理、抄录员（即根据口述录音记录的人）、收费员和助理护士等。对于本部分，安全服务证书中包括雇员与医疗保健组织之间的关系是很重要的。对于健康专业人员，数字证书结构中包括其与健康专业人员注册机构的关系很重要，但其与诸如医生之间可能的雇佣关系或从属关系也很重要。

医疗保健雇员的角色或职业有许多类，本部分不提供分类方案。

注：雇员没有就其专业能力向雇主之外的组织进行注册并不意味着雇员在服务时不是专业人员。

5.2.3 患者/消费者

在大多数情况中，接受健康服务的个人称为患者，但在某些情形下，对于健康人而言，当考虑到其与医疗保健提供者之间的契约关系时，称其为健康服务的消费者更合适。在本语境中，只有当消费者也是健康信息系统的直接用户时才认为其是患者。

5.2.4 受委托医疗保健提供者

按照权限，医疗保健提供者中的某些类型人员不是正规的，但他们为社区提供服务，并由已注册的医疗保健组织对其专业角色进行认证和委托。例如，某些国家的助产士（由产科医生或其他医生保证）、不同类型的理疗医生、参与残疾人和老年人社区护理的各类人员（由全科医生或医院保证）。

5.2.5 支持组织雇员

支持组织雇员是指为支持组织工作的、且不是正规或非正规健康专业人员的个人。

5.2.6 医疗保健组织

主要参与健康服务或健康促进相关的官方注册组织。例如医疗保健提供者、医疗保健资助团体（保险公司或政府公共卫生资助部门）和医疗保健研究院所。

5.2.7 支持组织

支持组织为医疗保健组织提供服务，但不直接提供健康服务。

5.2.8 设备

设备是指诸如ECG设备、实验室自动化设备和为患者测量各种生理学参数的各种便携式诊断设备之类的装置。它也包括诸如电子邮件服务器、网络服务器和应用服务器之类的计算机设备。

5.2.9 应用

应用是指在单个机器和/或互联网中运行的计算机软件程序。在医疗保健语境中，依赖于数字证书的应用可能包括临床管理集成系统，EHR应用，急诊信息系统，影像系统，处方及药品管理系统。

5.3 医疗保健数字证书的适用性

本指导性技术文件既适用于一个辖区内的卫生行业，也适用于不同辖区之间的卫生行业。本指导性技术文件试图覆盖公共（政府）卫生机构、私营和公共医疗保健提供者（医院、社区健康以及全科医生的医疗活动）。本指导性技术文件还适用于医疗保险组织、健康教育机构以及与健康相关的活动（如家庭护理）。

本指导性技术文件的主要目的是为健康专业人员、医疗保健组织以及保险公司能够安全地交换健康信息确立一个框架，同时还试图为消费者提供安全访问自己健康信息的能力。在交易中使用CA和RA，可使医疗保健提供者、保险公司和消费者进行安全的信息交换，即使信息的完整性受损，也能很快地被发现。

在卫生领域中，数字证书适用于下列情况：

a) 安全电子邮件。

b) 利用数字证书，社区健康专业人员对医院信息系统中患者信息的访问请求。

c) 利用数字证书，医院信息系统内部的访问请求。其中系统应包括患者管理、临床管理、病理、医学影像、饮食以及其他相关的信息系统。

d) 账单应用：要求具有抗抵赖性、消息完整性、保密性和对患者、健康服务提供者和医疗保险公司的鉴别以及(在某些管辖权限中)防止欺骗。

e) 远程影像应用：要求将影像与患者身份进行可靠绑定，同时也要求对健康专业人员进行鉴别。

f) 远程访问控制应用：对验证真实性、保密性和完整性有特殊要求。

g) 电子处方应用：要求数字证书提供的所有安全服务对处方是否源自特定健康专业人员(源鉴别)以及是否为该患者开具的处方进行核查。为了保证在传输过程中没有错误，要求数字证书能提供完整性服务；为了保证审计能力，要求数字证书能提供抗抵赖服务。

h) 患者同意数字签名的文档。

i) 跨国界或跨辖区的转录服务。

j) 符合本地策略的其他系统。

本地策略可以排除一个或多个依赖于数字证书或以其他的方式使用数字证书的上述应用。

使用数字证书的剧本详见附录 A。

6 医疗保健应用中的安全服务需求

6.1 医疗保健特征

制定本指导性技术文件的原因是因为卫生行业对安全有特定的需求，需要进行特殊说明。医疗保健的具体特征如下：

a) 健康信息可重复使用，且其存在的时间同其所对应的个人的寿命一样长，甚至更长。这就要求能够长期保存数字签名以及一种能满足这种要求的时戳技术。

b) 健康消费者和健康服务提供者都对健康信息的使用非常重视。除非患者本人明确同意，否则其健康信息只有用于健康目的，而不能用于其他目的(如匿名患者数据用于培训和计划编制)。

c) 具有提高健康服务消费者对健康系统管理其信息能力的信心的需求。

d) 具有使健康专业人员和组织履行健康策略语境中安全义务的需求。

e) 具有确保使用数字证书的健康专业人员、贸易伙伴和可依赖方对保证患者信息的私密性和安全性具有信心的需求。

随着越来越多地使用电子信息系统代替纸质文件来存储个人健康信息，卫生领域中的安全性问题也变得越来越显著。卫生行业的首要关注点是保护患者的隐私和安全。特别是对于跨辖区传输的健康信息流，该关注点还要求符合相关的隐私法律法规。如果信息系统将由健康专业人员和患者/消费者使用，则它应是可信赖的。因此，对于健康信息系统而言，满足私密性和安全性的需求是非常严格的。

6.2 卫生领域中的数字证书技术需求

6.2.1 概要

在健康信息与通信系统中，需要处理的大多数安全威胁是未授权访问，这些访问是通过窃取合法证书持有者的私钥后，假冒证书持有者的身份进行的。这样的未授权访问会导致健康信息被篡改、丢失或被复制。与安全标准(如 GB/T 19716)结合使用的数字证书能够有效降低这种未授权访问的风险。

数字证书提供了包含鉴别、完整性、保密性和数字签名等所有服务的策略、程序和技术的唯一组合。在医疗保健语境中，使用数字签名能使互不相识的医疗保健提供者和消费者运用电子手段，并通过信任链来安全放心地进行通信。

数字证书能够提供卫生行业特需的安全服务。这些服务及其在卫生行业中的应用将在下面进行详细描述。

6.2.2 鉴别

医疗保健是一项多学科联合的工作。当健康专业人员查阅包含个人健康信息的患者记录、会诊报告和其他文档时，需要依赖于其他医疗保健提供者的判断。当访问和更新这些文档和记录时，必须将包含在内的信息与其作者可靠关联起来。

非常重要的一点是既要使健康专业人员能够访问各种临床设备中敏感的个人健康信息，也要能防止未经授权的人访问或改变这些信息。对鉴别的进一步讨论见7.4。

6.2.3 完整性

当个人健康信息用于急救时，维护信息的完整性就成为了一个关乎生死的问题。尤其是对于某些类型的个人健康信息(如麻醉药品处方)完整性，应对其可能被破坏的情况给予高度关注。

6.2.4 保密性

在一般应用中，个人健康信息通常被认为是最机密的信息。与电子商务中传输的信息不同，个人健康信息的保密性是不能用金钱来衡量的，患者的隐私权一旦被取消，就不能再恢复。

6.2.5 数字签名

在审讯听证会、医疗渎职诉讼、专业人员纪律听证会和其他法庭或准法庭中，由于可将电子签名文档作为证据提交，因此在卫生领域中使用的数字签名以及用于确认其完整性的策略和操作最终会引起人们的高度关注。

即使证书已过期或已被撤销，仍可对医疗保健文档中的数字签名进行验证。在时戳到期前，该服务可以使用安全时戳技术来实现(参见IETF/RFC 3161)。因此建议使用IETF/RFC 3126作为长期的签名格式。

数字证书也支持基于授权和角色的访问控制服务(见6.2.6)。这些服务在医疗保健中非常重要，因为许多特殊性和情况要求根据所涉及的健康专业人员的角色和情形，来对个人健康信息的不同部分采用不同的访问级别。

6.2.6 授权

在医疗保健中，有必要只对那些为患者/消费者提供医疗保健的实体、或是已获得患者亲自同意的实体授予对个人健康信息访问的权利。

6.2.7 访问控制

在医疗保健中，有必要适当采取一些手段，来确保被授权实体只能根据授权目的/功能、以授权的方式访问数据处理系统的资源，这是因为未授权访问造成的后果可能是无法补救的。

当与合适的安全标准联合使用时，数字证书就能够明显降低未经授权而泄漏患者健康信息的风险。

本指导性技术文件的目的是定义数字证书发行和使用的通用元素，这些元素保证传输健康信息的信任链可以按照需求进行扩展，甚至可以超越辖区或国界。

6.3 分离加密和鉴别

将签名从加密功能中分离出来是卫生行业的一个特殊需求。之所以这样做的原因是因为在急救或其他特殊情况下，当了解患者的急救或特殊情况记录的健康专业人员不在场或无法联系时，被授权的健康专业人员需要访问这些消息。在健康信息安全性方面，一种通用的做法是鉴别时使用个人身份证书，加密时使用组织单元证书。

本指导性技术文件推荐在鉴别和加密(确保保密性)中使用独立的证书和关联密钥。本指导性技术文件使用独立的证书建立身份，使用与主体鉴别密钥关联在一起的关联密钥管理访问控制。

6.4 医疗保健数字证书安全管理框架

对于支持健康相关信息的安全传输和在国内或辖区内、甚至跨国界或跨辖区的数据访问的数字证书安全基础设施，需要通用安全管理策略框架的支持。为了对基础设施操作安全有一定的保障作用，需要制定用于对其进行管理的操作规范。

规定信息安全管理操作规范的标准已经存在并被普遍接受。GB/T 19716—2005、GB/T 19715.1和COBIT规范规定了安全风险标识以及适当控制风险管理的应用。

由数字证书配置提供的安全服务可以向签名者和验证者保证较弱的安全管理不会减弱电子签名的作用。上述标准中的操作规范对这些安全服务的约束作用很小甚至没有。

本指导性技术文件将引用 GB/T 19716—2005 来解决 IETF/RFC 3647 中提出的安全问题。

6.5 医疗保健数字证书发行和使用的策略需求

医疗保健数字证书发布和使用的策略需求和相关操作见本指导性技术文件第 3 部分。

7 公钥密码算法

7.1 对称密码算法与非对称密码算法

利用对称密码算法,可以使用密钥将纯文本加密为不可读的密文。这样的加密信息可以使用相同的密钥通过逆向密码算法对其进行解密。这种类型的密码系统广泛用于保证保密性,并称为对称密钥或密钥。

公钥密码算法是由 Whitfield Diffie 和 Martin Hellman 于 1976 年首先提出的。这种方法使用两种不同的密钥:一个是公钥,另一个是私钥。具有公钥的任何人都能够对消息进行加密,但不能对其解密;只有具有私钥的人才能够对消息进行解密。单独根据公钥的信息是不可能推导出私钥的,因此公钥可以公布而不需要考虑其保密性。

RSA 密码系统是非对称的。以三个发明者(Rivest、Shamir 和 Adelman)命名的 RSA 非对称算法使用广泛,它可以单独使用,也可以与其他对称密码系统联合使用。在这种混合系统中,非对称算法用于保护对称密码系统的密钥。

保证通信完整性可以实现对可依赖方的鉴别。通过实现这种鉴别以及实现授权和访问控制,非对称密码系统能够增加对称密码系统或虚拟专用网的价值。

某些公钥算法(如 RSA 算法)能用来恢复消息,因此适用于使用上述密码算法进行保密性保护的情况。这种算法也适用于相反的情况——即使用公钥对私钥加密的文本进行解密。这种原理不适用于保密性保护但可用于鉴别。只有私钥的持有者才能使用相应的私钥生成一个能够解密的密码。拥有私钥的某人可以利用这种特性来鉴别消息源。

7.2 数字证书

数字证书是一种软件数据结构,它将实体公钥、一个或多个与实体身份或实体公钥相关的属性以及其他信息绑定在一起,其中这些信息是按照 GB/T 16264.8 发布的 CA 私钥进行加密的,无法进行修改。一个标识实体的识别名是一个与身份相关的属性。

实体可以是一个人、一个组织单元、一个应用、一个服务器或一个硬件设备。数字证书的目的是提供某种级别的保密性。该级别的保密性中,公钥属于被标识的实体,并且该实体拥有对应的私钥。

保密性的级别是由对数字证书进行签名的 CA 利用其自身的私钥来实现的。通过对数字证书进行签名,CA 对数字证书中包含的信息承担责任,并为证书持有者提供某种级别的鉴别。

CA 发行证书,维护证书目录及其公钥,宣布证书作废并保证所有相关的可依赖方能够及时收到证书作废的通知。本指导性技术文件第 3 部分规定了证书的管理过程,也规定了 RA 的角色以及对 RA 角色执行者的相关约束。

7.3 数字签名

数字签名是指数据单元的附加数据或密码转换,它使数据单元的接收方可以检验数据单元的来源和完整性,避免被伪造,如符合 GB/T 9387.2 的接收方。

数字签名是通过使用发送方的私钥对即将发送的消息进行数学运算而生成的。因为私钥和公钥是配对的两个密钥,公钥绑定在数字证书的身份上,所以使用公钥提前验证发送方的身份是否具有某个级别的保密性是不可能的。保密性的级别是由对数字证书进行签名的 CA 利用其自身的私钥来实现的。通过对数字证书进行签名,CA 将对数字证书中包含的信息承担责任,并为证书持有者提供某种级别的鉴别。

所实现的保密性级别取决于CA的策略和操作以及可依赖方的密钥管理。

除提供鉴别发送方的保密性级别外，使用数字签名还能提供通信完整性的保密性级别。因为如果在源和目的地使用相同的方法生成数字签名，则可以获得相同的散列值。

7.4 保护私钥

证书并不是把密钥与身份绑定在一起，它只是将密钥与实体的识别名绑定在一起。实现私钥和实体的绑定需要采取特殊的步骤，从而确保只有指定的实体才能使用该私钥。因此在卫生行业内，合格的私钥管理对于合理配置数字证书很重要。如果私钥遭到泄密，则相关的数字证书将无法保护使用该公钥/私钥对进行通信和存储的信息。而且如果CA的私钥遭到泄密，则该CA所辖范围的安全性也将不复存在。

私钥保护要求将管理过程和技术方法联合起来使用。不管选择什么技术，密钥保护都应按照符合GB/T 19716—2005的一个完整的信息安全管理框架内进行管理。

硬件令牌可以用来保护私钥，这时私钥被存储在可以执行密码计算的令牌中，而证书持有者通过使用密码、密码短语或生物测定可以对其进行访问。这是一种比较安全的私钥保护方法，因为在这种方法中，在令牌中可以植入复杂的鉴别算法，而且计算机没有与网络连接，所以无法通过互联网对其进行访问。特定类型的智能卡完全可以替代这种硬件令牌，也可以使用USB(Universal Serial Bus，通用串行总线)密钥或类似的硬件令牌。其中USB密钥或类似的硬件令牌只存储私钥，而加密逻辑存储在计算机中。

私钥也可以存储在软盘中，但这样做不太安全。私钥还可以存储在计算机工作站的硬盘中，这样做更不安全。因为这样做就有可能通过计算机工作站所连接的互联网对私钥进行访问。

为了访问存储在上述某个设备中的私钥，要求对证书持有者、其他设备或应用进行鉴别。这种鉴别在大多数情况下是利用密码、密码短语或生物测定进行的。鉴别有多种类型，其中大多数都是基于诸如个人地址、所掌握的知识、信息或所有物，例如要求在你所拥有的物理设备(如令牌)上使用(你所知道的)密码。建议使用一种以上类型的鉴别，即众所周知的双重鉴别，这样可以大大增加私钥的安全性。

本指导性技术文件给出了对多层安全的需求，说明了更高级的安全性需要用硬件令牌来保护私钥。对私钥管理的规定详见本指导性技术文件第3部分的7.6.2和7.6.3。

使用不安全的媒介(如互联网，此时发送方和接收方可以没有预先联系，也没有个人接触)进行跨辖区或跨国界传输个人健康信息意味着需要有鉴别相关方的方法，以确保传输和存储的信息能够保持完整性，同时保证信息在传输过程中没有被篡改，任一参与方不能对已发送或已接收信息的行为进行否认。这是对卫生行业中数字证书提供的安全服务的业务要求。

8 配置数字证书

8.1 必备组件

8.1.1 概要

PKI是由下述组件组成的基础设施。

8.1.2 CP

CP是一个已命名的规则集合，它指出证书对特定医疗保健社区的适用性和(或)具有通用安全需求的应用类。专门用于满足健康信息需求的、基于CP的证书，支持诸如授权、访问控制和信息完整性的服务。第6章中说明的健康信息系统的具体需求意味着数字证书用于卫生领域时需要进行专门规定。

8.1.3 CPS

CPS是关于CA通过发行证书来实施CP的操作说明。例如，当接收到卫生机构的请求时，CPS指出为向健康专业人员发行证书而要采取的行动。

8.1.4 CA

CA 是一个值得信赖的实体，它验证证书持有者的身份，并给证书持有者分配一个“识别名”。CA 也通过对数据进行签名来验证被标识证书持有者信息的正确性，此时也验证了名称或身份与公钥之间的绑定关系。这种绑定关系构成了证书持有者的数字签名。由于这些功能在本地层面上可以很好地执行，所以其中某些功能可以由 RA 完成(见 8.1.5)，如身份的验证和识别名的分配。

私钥可以存储在主体的计算机、软盘或诸如智能卡之类的其他媒介中。对密钥的访问通常是由证书持有者通过输入密码短语进行的。

本指导性技术文件认为卫生机构可以以不同的方式获得认证服务。某些认证服务是由其自身提供的，其他认证服务可由经过认证的私营组织进行。根据证书发行的目的，可以有多种认证。证书持有者也可以有多种证书。

根据国家对医疗保健数字证书的组织方法，CA 可以有若干个级别来向不同级别的实体(如组织内部的证书持有者、卫生行业整体或国内任何人)提供证书。

CA 应是一个公证处，该组织按照合理的管理和程序来提供所需的信任等级。这些管理和程序至少应符合 GB/T 19716—2005(或与其等效的标准)，如果可能的话，还应符合某个公认的数字证书担保方案，并适用于其操作权限。

8.1.5 RA

RA 是一个建立证书持有者的身份、并向 CA 注册其认证需求的实体。RA 也可以对存储在属性证书中的信息进行验证，从而获得证书持有者的角色、级别或就业状况。在这种情况中，验证诸如就业状况之类的属性的 RA(如政府医疗机构)与验证健康专业人员的操作资质的 RA(如健康专业人员注册委员会)有可能不同。

健康专业人员角色的标识可以由下列团体执行：

——国家、省/市/自治区卫生机构(包括相关的医院和健康组织)；

——医疗或健康专业人员注册委员会；

——医疗或健康专业人员团体，如培养外科医生、精神病医生、护士的院校；

——国立或私立医疗保险组织。

数字证书的用户可以信赖上述验证健康专业人员资格证书的一个或多个团体。注册程序参见本指导性技术文件第 3 部分的 6.1、7.2.1.2、7.3.1.2、7.3.2.2、7.3.3.2 和 7.3.4.2。

8.2 使用资质证书建立标识

资质证书是一种在数字签名服务中用于标识某人具有高级担保资质的证书类型。资质证书同电子签名的法律认同密切相关。本部分预先为使用资质证书作好准备，以对不断增加的、支持电子签名的健康和其他服务提供者的国家立法需求以及签名者和验证者的需求作出响应，从而使电子签名能被法律认同。

IETF 已经认识到了对资质证书的需求，并制定了 IETF/RFC 3739。该标准提出了资质证书的证书轮廓，其目的在于定义一个独立于本地法律需求的通用语法。IETF 使用资质证书轮廓来描述目的为对个人进行可靠标识的证书的格式。本部分使用 IETF 资质证书轮廓作为支持资质证书的框架。在本指导性技术文件的第 2 部分对资质证书轮廓进行了详细说明。

在医疗保健语境中，可以使用资质证书来对医疗保健提供者或消费者进行标识，从而使其具有在验证其电子签名时所必需的信用级别。本部分建议将资质证书用于正规健康专业人员和非正规健康专业人员。

8.3 使用身份证书建立专业和角色

本指导性技术文件认为在患者/消费者的眼中并不是所有的医生都是一样的。患者/消费者可以去找不同的医生来处理不同的健康问题。HIV/AIDS、传染病、精神健康都是一种需要人们分别处理的健康问题。因此，通常是根据健康专业人员的专业(如外科医生)和角色(如市中心综合医院急救部门的值班医生)来确定健康专业人员访问患者/消费者健康记录的具体部分。

首先需要重点关注的是，实体身份和公钥间的绑定与授权信息不具有相同的生存期，更不要说基本的医疗执照。例如，某人是一个行医40年的合格医生，但他可能只与某个医院签署了几个月的咨询医生合同。如果在PKC扩展中给出授权信息，则会导致缩短PKC的有效生存期。其次，PKC签发方对于授权信息通常不具有权威性。在这种情况中，PKC签发方尽管能够验证所涉及的人是一个医生，但很难对其在特定医院中担当的精神病咨询医生的角色进行验证。因此，PKC签发方还需要从权威部门获取授权信息，同时还可能由于某些信息无效而导致PKC生存期的缩短，造成需要增加宣告PKC无效、并发布一个替代品的管理行为。因此，常见的方法是把授权信息从PKC中分离出来。这就需要在软件产业中更广泛地实施属性证书规范(参见IETF/RFC 3281)。

IETF属性证书规范规定了如何使用公钥来验证数字签名或加密密钥管理操作，并指出并不是所有的请求和公开决策都是基于身份的。这样的访问控制决策也可以是基于规则、基于角色和基于等级的，因此还需要其他信息。例如，在访问控制决策中，作为特定类型专家的健康专业人员的信息比其身份更重要。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，支持这样的决策授权信息可以编入到PKC扩展部分或一个独立的属性证书中。

本指导性技术文件建议PKC应将证明身份作为其主要目的。在X.509证书中提供的证书持有者身份信息可以用来作为制定“是否为了某种目的而对服务器提出的请求的响应信息进行公开”的决策依据。X.509 PKC将客户端身份和公钥进行绑定。在证书持有者证明其有与PKC中包含的公钥相对应的私钥后，其身份可被用来支持基于身份的决策，以对请求和信息公开进行管理(见IETF/RFC 3281)。

作为包含主要身份证书中专业人员角色的各种属性的替代模型，负责分配这些角色的其他组织可以批准主要的CA，并发行一个使用与主要身份证书相同的密钥，但包括一个或若干个附加属性的二级密钥。

身份一旦得到证明，则可使用属性证书来管理信息。在这些信息中，与PKC绑定的信息比其他信息变化更快或更短暂。为此，本部分对属性证书进行了规定。然而，这种方法也存在许多难点。属性证书的使用仍在不断发展并需要在软件行业中得到更广泛的实施。而且，健康专业人员的专业信息(如精神病学、儿科学、泌尿学)也具有一定的寿命。此外，还需要一定的容量来记录患者/消费者角色信息。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。

数字证书也可用于对诸如SAML(安全声明标记语言)之类的标准的安全声明进行签名。这样的安全声明包括对健康专业人员的专业和角色的声明。

8.4 使用属性证书进行授权和访问控制

IETF属性证书规范认为PKC中对授权信息的定位是不合适的。本部分认为人们希望身份证书可以具有多种用途，并减少保存在身份证书中的信息。本部分建议将次要角色、团体资格、安全许可保存在附加的属性证书中。

应注意的是授权信息明显不同于PKC中包含的健康角色或许可证信息。角色或许可证隐含着授权级别，但不一定是授权信息本身。本部分规定使用属性证书来支持传输基于角色的医疗保健提供者的信息。

在PKC发行的身份证书中隐含着一个角色，该证书在许多情况中并没有包括足够的信息来制定访问控制决策。例如，当代表外科医生院校的RA为医生发行PKC时，则表明该医生是一位外科医生。但通常这并不能表明授权该医生在其被聘为特殊医院急救部门的临时代理医生时可以接收患者到医院。

这些详细的授权信息更适合由与健康专业人员的公钥绑定在一起的属性证书来提供。一个健康专业人员可以有多个属性证书来体现其多个角色。一般来说这样的属性证书比身份证书寿命短。

IETF属性证书也规定，要以一种与PKC相类似的方式来保护授权信息，而属性证书可以提供这种保护。属性证书只是一个数字签名(或鉴定)属性集，具有与PKC相类似的结构。属性证书与PKC的主要区别是属性证书不包括公钥。它包括对与属性证书拥有者相关的团体资格、角色、安全许可和其他访问控制信息进行规定的属性。

对符合 IETF/RFC 3281 的属性证书中数据元素的规定见本指导性技术文件第 2 部分。因为目前属性证书规范仍处于不断完善的过程中，所以在本指导性技术文件的最新版本中对健康属性证书类型进行了更详细的规定。

涉及医疗保健文档签名的剧本参见附录 A.4.16。

9 互操作性要求

9.1 概述

本指导性技术文件尝试采用和增加 IETF 和其他现有的安全标准来支持跨国界或跨辖区的健康信息安全电子传输。互联网正逐渐成为支持这种传输的工具。

本指导性技术文件的目的之一是支持跨国界、跨区域和跨组织的健康信息安全传输，所以本指导性技术文件必须以互联网为基础来将其全球效果最大化。为此，本指导性技术文件将 IETF/RFC 3647 作为本指导性技术文件的组织框架，并可根据需要参考其他相关的 IETF/RFC。

通过参与国之间的相互承认机制可以实现跨国界的健康信息安全传输，每个国家应利用合适的复审策略、操作和程序来鉴定 CA。

医疗保健数字证书的发行和使用管理需要进一步的研究，但其不在本指导性技术文件讨论范围之内。本指导性技术文件建议跨国界的互操作性应通过一系列国家间的双边或多边协议来实现，这些协议应以本指导性技术文件第 3 部分中规定的最低需求为基础。最后，可依赖方需要 CA 制定程序以根据需要使基础设施具有所要求的担保级别。

9.2 配置跨辖区的医疗保健数字证书的选项

9.2.1 概述

以跨辖区(包括跨国界)为目的的数字证书配置存在的主要问题是信任。信任是许多参与方的办事方式，主要依赖于政策、操作，更深入地说，还要依赖由一个已建立的权威机构发行给证书持有者的数字证书的有效性。下面对配置医疗保健数字证书体系结构的选项进行说明。

9.2.2 选项 1——CA 的单层次体系

从技术角度看，本选项是最容易的。然而建立只有一个集中式 CA 的、全世界范围的保数字证书配置是不可能的。尽管在本剧本中注册是可以向下授权的，但是其管理方案仍不可行。

9.2.3 选项 2——可依赖方的信任管理

在本选项中，可依赖方的职责是决定是否信任所关注的发行 CA。本选项有内在缺陷，因为它要求信任决策完全由可依赖方决定，这样在某些情况中就可能让不能够作出正确决定的可依赖方承担不恰当的责任。

9.2.4 选项 3——交叉识别

交叉识别是一种互操作方案。利用该方案，一个数字证书域内的可依赖方可以使用另一个数字证书域内的授权信息来对后者域内的主体进行鉴别，反之亦然。比较典型的是，这样的授权信息可以从后者域范围内的正式许可或授权过程中产生，也可以从由代表可依赖方域的典型 CA 执行的正式审计过程中产生。从技术上来说，这种信息可以作为被可依赖方访问的证书域的值进行存储。

与交叉认证相比，是否信任国外数字证书域的责任在于应用或服务的可依赖方或持有者，而不是可依赖方直接信任的 CA。这种情况中不涉及两个域之间的合同或协议。

在交叉识别方案中，详细的 CP 或 CPS 的映射不是必需的。相反，根据正在使用的可依赖方决定是否为了某个目的而接受国外证书，这主要取决于证书是否是由一个值得信任的国外 CA 发行的。

如果 CA 已由一个正式的许可/鉴定组织进行过许可/鉴定或由一个值得信任的独立方进行过审计，则可认为该 CA 值得信任。而且，可依赖方应能够根据国外的 CP 或 CPS 中规定的政策单方面作出非正式判断。因此，本过程相对于交叉认证而言比较简单，特别是在政策和法律协调方面。本过程也可进行内部调整。

然而，交叉识别从程序上没有交叉认证严格，这样就给可依赖方增加了潜在的负担，而可依赖方可能并不清楚接受证书的整个后果(见参考文献16)。

总结：在交叉识别中，是否信任国外证书的决策主要取决于可依赖方而不是CA。

9.2.5 选项4——交叉认证

交叉认证使认证机构之间在信任决策方面达成一致。而技术协议强化了这种一致性并提供了互操作性。本模型的实现比选项1、选项2或选项3更难，但对用户而言更容易理解，因此也更容易获得用户的支持。这就意味着最终用户可以不需要承担作出信任决策的责任，因为它可以由最终用户的CA域中的CA来承担。

交叉认证是一种双向方式，它通过由两个典型CA执行复杂的程序把两个域(整体或部分)合并成一个更大的域。对于分级CA，典型CA通常是指根CA。然而，交叉认证也可以在任意两个CA之间进行。在后一种情况中，每个域只包括一个CA以及它的用户。为了实现交叉认证，要在应用层、策略层和技术层上相互兼容。此时，对于交叉认证涉及的CA域中的可依赖方，信息的传输是透明的，CA对信任决策负责。

交叉认证的过程要求每个典型CA策略的详细映射，这样做的结果将使包含在集体域中的每个CA域呈几何级数增长。这种增长是可测量的。但这种情况也存在一种风险，即第三个CA(CA-3)可以利用第二个CA(CA-2)进行交叉认证，但会发现第一个CA(CA-1)的策略不合适。在与这种情况相类似的情况中，CA-3不能排斥CA-1。因此，对于相对封闭的医疗保健模型以及开放但有界限的系统，交叉认证更适用。如果两个域属于两个相互工作关系比较密切的工作语境，则交叉认证最合适。例如，两个域(如电子邮件和财务应用)使用同一个应用和服务集(见参考文献16)。

总结：在交叉认证中，是否信任国外证书的决策取决于CA。

9.2.6 选项5——桥CA

桥CA模型依赖于潜在的CA域团体中的所有CA。这些域在通用的最小标准集方面达成了一致。这些最小标准并入到他们自己的CP和CPS中。在桥CA和交叉认证之间的不同之处是：对于单个CA，除了具有共享的最小标准外，还可以具有自己的本地需求。对于桥证书，那些不在本地CA域中的可依赖方并不要求这些本地需求。当CA具有相当数量的共同需求、并准备允许进行某些本地调整(如在同一个国家的州或省的卫生部门之间交叉认证的情况中)时，本模型是最好的工作模式。

在本模型中，组织可以建立自己的CA，然后决定该CA是否加入到一个桥CA中。

总结：在桥CA模型中，是否信任国外证书的决策取决于CA而不是可依赖方。

9.3 选项的用法

本部分认为不同辖区间的管理方案和政策存在着不同之处。因此，上述任一选项都是可以接受的。不管选择哪个选项，在其应用中使用本部分都是有利的。

为了便于使用，本指导性技术文件的第2部分规定了用于桥证书的框架以及用于CA的审计情况和审计人员鉴定的CA证书领域，这些都将有助于交叉识别。

附 录 A
（资料性附录）
使用医疗保健数字证书的剧本

A.1 简介

下述一组高级业务案例或“剧本”描述了支持具有广泛代表性的卫生行业的数字证书解决方案的核心业务和技术需求。

下面首先描述了与基本隐私和安全原则相关的一般需求和卫生行业的基本需求。每个剧本都给出了如下内容：

——对要求安全、私密电子通信的剧本或医疗保健情况的描述；

——通过数字证书解决方案实现的业务和技术需求。

A.2 剧本说明

A.3 中描述的医疗保健剧本对医疗保健中如何使用数字证书进行了说明。每一个剧本都是：

——由策略驱动：剧本旨在说明数字证书如何满足卫生行业的需求来实现国际、国内和本地的需求，从而确保为个人和社区提供的健康信息用于其本来的目的。

——可跨健康环境进行应用：对于分散在世界各地的各种医疗保健和需要积极配合提供无缝医疗保健的各种个人和组织而言，确保数字证书的所有实施都可以在不同的医疗保健环境（包括医院、社区服务、公共部门和私营部门）中进行操作是至关重要的。

——独立于技术：开发医疗保健行业数字证书标准的一个主要目的是在不考虑供应商、硬件、运行的操作系统或应用的情况下，确保在提供者、消费者、保险公司和其他相关方之间能够安全传递信息。

——满足当前和新生的隐私要求：如果要使电子健康应用被广泛使用，则必须使提供者和患者对其信任。为了实现这种信任就必须解决隐私和安全问题。

——简单易用：数字证书的安全服务不应妨碍授权给医疗保健组织或专业人员的职能。如果安全系统的日常运作过于烦琐，医生将会设法不使用它，或不完全遵守管理程序。如果出现这种情况，则会产生破坏安全的重大风险。

A.3 医疗保健剧本中的服务示例

表 A.1 给出了健康服务和剧本。

表 A.1 健康服务和剧本

服务	剧本序列号															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
鉴别	×		×	×	×	×	×	×	×	×	×	×	×	×	×	
保密性	×		×			×	×	×	×	×	×		×			
完整性		×		×	×		×	×						×		
数字签名		×		×	×			×			×	×	×	×	×	×

关键剧本

1——急救部门对记录的访问；
2——临时服务（急救援助）；
3——招收新成员；
4——远程影像；
5——自动发给医生的结果报告；
6——带有医生消息的结果报告；
7——医患间讨论治疗方案；
8——患者护理注册总结；
9——患者向药剂师咨询；
10——医患间的消息交流；
11——远程访问临床信息系统；
12——急救访问；
13——远程转录；
14——电子处方；
15——鉴别医嘱；
16——医疗保健数字签名的潜在应用。

A.4 剧本描述

A.4.1 急救部门对记录的访问

剧 本 描 述：来自另一国的患者被送入到急救部门(ED)。患者无法连贯回答问题，其病史也无法可靠地获得。他/她的钱包内有医疗保险卡，通过该卡可获得确切的身份。

没有数字证书：根据医疗保险卡中的信息，在场的 ED 医生尝试向医疗保险提供者进行国际呼叫。由于时差，要求医生在行政部门开始工作时再打电话回来。医生对病人的症状进行处理。此时是否会造成患者治疗措施的不连续性就不得而知了。

具有数字证书：根据医疗保险卡中的信息，在场的 ED 医生通过互联网访问患者的医疗保险提供者网站，提交确认其当前角色为 ED 医生的数字证书。医疗保险提供者的网络服务通过验证电子签名和检查数字证书没有过期或没有被撤销来确认电子令牌。因为令牌有效且符合现行标准，所以医疗保险提供者的网络服务接受该令牌，从而获得患者的健康信息也是理所当然的。审计记录访问文件包括创建日期、时间、主治医生的全名和行医执照号码以及 ED 设施的标识。医生了解了患者的病史、过敏史以及产生不良反应的药物(患者最近在处方中做了修改)。患者经过治疗后，ED 医生发送一个有数字签名的、加密的 ED 访问医疗保险提供者记录的副本，医疗保险提供者将该副本放入到患者的电子健康记录中，以说明患者的症状以及对患者的诊断、治疗和处理。

A.4.2 临时服务(急救援助)

剧 本 描 述：大地震给大城市市区造成了极大的破坏。当地医院和诊所本身也被破坏，并且造成大量的人员伤亡。国家的医疗资源无力应对这种情况，需要接受国际提供的援助。

没有数字证书：无法立即核实提供医疗帮助的专业人员的资格证和执业许可证，也不能保证先前提供的援助在事后被确定。

具有数字证书：通过查看健康专业人员附带的数字证书，可以马上对他们提供的援助进行确认。因为援助信息已经利用那些提供帮助的人员的私钥进行了数字签名，因此无法否定援助信息。

A.4.3 成员登记

剧 本 描 述：在去另一国家停留 6 至 12 个月的准备中，一家之主要对医疗保险进行安排。

准成员 Charles 先生希望参加医疗保险计划。他访问包含成员报名表的保险公司主页，填写完表格后将其发送到登记部门的邮箱。表格经确认后将进行医学审查。医学审查指安排准成员进行体检，并通过邮件通知准成员。该准成员接受体检，医生根据体检结果确定其是否可以将其接受为成员。医生通报医学审查的结果并将该信息传送到成员登记部门。成员登记部门发给 Charles 先生一份合同，遵照合同每月要从其账户中扣除保险费用。成员登记部门接受新成员并将获得其照片身份健康卡的说明。作为成员登记过程的一部分，该准成员必须出示其驾驶证或其他经过公认的照片身份。在 Charles 先生收到他的新照片身份健康卡的同时，也会收到从医疗保险计划中下载数字证书的说明。

没有数字证书：新成员无法向医生可靠表明自己的身份，医生也无法向患者表明自己的身份。尽管在二者之间有许多对发送的消息进行加密的其他方法，但这些方法不可能同时实现可靠性和保密性。

具有数字证书：使用新发行的数字证书，Charles 先生能够通过 web 访问成员服务，包括他自己的部分个人健康数据，并能够同他的医生交换安全电子邮件。数字签名证书也使

Charles 先生具有了直接授权其他提供者(比如在外出旅行找了另一个医疗保健提供者)访问其健康记录的能力。

A.4.4 远程影像

剧 本 描 述：远程影像内科专家在计算机上观看血管造影片系列并创建一个分析报告来对其进行解释。专家的工作负担很繁重(每天 10～15 个病例),他们更愿意在家进行工作。在家中,医生通过互联网访问影像传输服务器,使用自己的数字证书证明自己,然后下载图像。当在自己的工作站上观看图像时,医生还通过互联网访问医疗机构的临床信息系统来查看患者的其他医疗信息。医生有信心认为图像是正确的,因为应用具有一个完整性校验功能(通过使用验证消息完整性的散列算法而实现的)。医生把他/她在图像中看到的结果写入到医学影像报告中,并选择远程对其报告进行电子签名。

没有数字证书：医生无法让医院用与数字证书相同的信任级别来对他/她进行鉴别。就医院而言,这意味着如果他们接受了就存在把图像下载给一个骗子的风险因素。通过电子传输医生的意见和结果也面临着同样的风险。医生也不能保证所下载的图像没有遇到传输错误或被蓄意篡改。

具有数字证书：医生通过鉴别来使医院认为他/她具有法院可接受的信任级别。医生可以相信下载的图像是正确的,他/她将不会根据一个错误的图像作出结论。医院也可以根据医生的数字签名来验证其发送的报告。

A.4.5 自动发给医生的结果报告

剧 本 描 述：星期二,患者去实验室抽血。当结果出来后系统会自动生成一个消息给医生,告诉他/她结果已出来了。星期三,医生使用他/她的健康工作证 ID 和密码登录到医疗机构的网站,查看等待处理的信息,并将其放入到自己的公文箱中。他/她找到关于“胆固醇检查”主题的消息。该消息告诉医生:患者的胆固醇值是 220,可将该患者归为中等风险类中。医生同患者讨论检查结果,建议患者与脂肪管理组联系,了解如何通过饮食和锻炼来降低胆固醇。医生还建议患者在 6 个月内再进行一次胆固醇检查并去医院看病。患者要求医生把结果加入到患者在互联网上的电子病历中。患者网址包括若干个关于补充资料的链接。一个链接指向关于胆固醇检查本身的信息,第二个链接指向脂肪管理组预约安排功能,另一个链接指向根据当前临床报告制定的个人饮食建议,这是通过分析患者的各种数据(如年龄)而制定的。饮食建议包含对行为变化支持方案的链接,该方案帮助患者在接下来的 6 个月里创建和跟踪他/她的饮食情况。

没有数字证书：实验室不能确定医生是否已接收到消息。无法保证消息是否被阅读或修改。

具有数字证书：数字签名可以向医生确保消息确实来自于实验室,给患者处理胆固醇问题的链接也是有效的。消息的数字签名确认消息将证明医生确实已收到了消息。

A.4.6 带有医生消息的结果报告

剧 本 描 述：在例行的医生手术访问中,医生为他/她的患者预约了血细胞计数(CBC)检查。在向患者询问过他/她的选择后,医生在定制界面上选择了一个选项框,该选项框指出医生在查看结果后要对结果进行评论,然后将带有评论的结果通过互联网发给患者。返回的结果中大部分是正常的,只有一个结果稍高。医生知道这对患者无关紧要,因此他/她针对那个结果写了一个便笺,并把它附到结果记录中。

当天晚些时候,患者的电子信箱收到一个通知,告诉其有一个来自于医生的消息正在一个安全网站上等待阅览。他/她点击内置的 URL,输入自己的病历号和密码,浏览实验室的结果和来自于医生的消息。网站已自动确定这是 CBC 结果,并给出

了健康百科全书中业余人士对 CBC 及其结果进行描述的那部分内容的链接。

没有数字证书：在没有能力来鉴别电子邮件是否来自于实验室或医生，或确保电子邮件是以安全加密的形式传输的情况下，患者通过邮局接收结果，注意到一个结果值偏高，然后打电话给医生以进一步了解情况。此时医生正为另一个患者诊治，不能打扰，而验血的患者正好有一个重要会议需要参加，因此无法对话。最终他们联系上了，但是患者焦虑了许多天，医生也打了许多次电话给患者。

具有数字证书：结果以一种经过验证的和安全的方式快速传送给患者。患者能够阅读电子邮件中医生对结果的解释，并可以访问网站了解更多的信息，这样患者不需要与医生进行电话交流就可以很快地消除焦虑。

A.4.7 医患间讨论治疗方案

剧 本 描 述：参加了医疗保险计划的成员对他/她的治疗方案有疑问。他/她登录医生的网站，使用可信赖的数字证书通过鉴别，然后填写信息表，点击“发送”来开始对话：

C 大夫，您好

昨天你告诉我要更换伤口的包扎，但是我记不起你要我多长时间更换一次。你说只要正常就不需要更换，但是我不记得你是否说过每个星期更换一次还是其他什么。另外，我忘了问你伤疤得多长时间可以没有？

在两个小时内，呼叫中心的咨询护士查阅了患者的消息，并确定它并不紧急，应由患者原来的护理组成员来对该消息作出响应。不久后，在患者原来的护理医生的计算机屏幕上出现了患者的消息，他/她给患者发送一个响应消息，并对消息进行数字签名。第二天早上，患者再次登录医生的网站，阅读该信息：

XXX，你好

在接下来的几周中，只有当包扎变得潮湿时才需要马上更换，否则只需要 4～5 天更换一次即可。然后，我们将再见一次面，决定下一步该怎么做。至于疤痕，我想你将会留下一点疤痕，但它不会太大——只是一条很小的线状疤痕。

没有数字证书：没有可靠的认证技术就意味着医生工作的医疗保健组织不能够验证 XXX（患者的名字）就是发送电子邮件的那个人，它有可能是要求免费咨询的其他人。患者也不能够确定来自于医生的答复是否就是来自于医生，也不能够确定交换的信息是否被中途截取并被第三方阅读过。

具有数字证书：医疗保险组织和医生能够相信他们是同某一医疗保险计划的一个已知和有效的成员进行安全通信。患者也能相信医生已经处理了请求，并且也确实是医生给其作出了答复。

A.4.8 患者护理注册总结

剧 本 描 述：糖尿病的风险注册系统汇总了来自于医疗保健组织的各种临床信息系统中关于糖尿病患者的临床数据。嵌入到注册系统中的临床指南能够生成关于患者的病情、病史、可能产生的危险和下一步治疗措施的总结报告。这个总结报告经医生审查后通过组织网站提交给患者。患者使用医疗保健组织 CA 发行的数字证书对网址进行鉴别。当患者浏览总结报告时，嵌入在报告中的超文本链接可以使患者很容易地浏览到相关的培训信息（如培训课程表、检验说明和患者培训等），并向临床医生提出约见请求或发送一个消息。该系统可以保证患者能够阅读报告。

没有数字证书：对于患者，没有足够的信心相信这个网站就是真正的糖尿病风险注册系统的网站，也无法相信同注册系统的通信是保密的。对于注册系统，也不能确定患者已访问了网站并接收到信息。

具有数字证书：数字证书能够使患者和注册系统相互进行鉴别以及进行保密通信，注册系统能确

定患者已访问了网站并接收到信息。

A.4.9 患者向药剂师咨询

剧 本 描 述：一位医疗保险计划成员的七岁女儿患有哮喘。儿科医生最近为她开了色甘酸钠，但是该成员无法判断吸氧器什么时候是空的，什么时候是满的。他/她到医疗保健组织的网站上寻找这方面的资料，但是仍然感到困惑，因此向在线的药剂师发送一个询问，咨询如何能知道吸氧器是空的。

在线的药剂师通过对医疗保健数字证书目录（该成员的数字证书存储的地方）具有访问权的电子邮件发送一个加密信息，该信息使用专门为这类问题设计的模板生成，并且信息中附有个人电话和电话号码以便进一步咨询。

没有数字证书：对于药剂师，无法鉴别医疗保险计划成员是否达到所要求的信任级别。也许可以发送一个安全消息，但无法进行鉴别。

具有数字证书：药剂师可以对成员进行鉴别并发送一个加密信息。成员也能够相信信息是来自于药剂师。

A.4.10 不针对具体诊断的医患间的消息交流

剧 本 描 述：患者得了皮疹来看皮肤科医生，医生为患者开了一剂护肤面霜。皮肤科大夫告诉患者如果皮疹在三个星期内仍然没有消去，患者就必须告诉医生，以便医生为患者开另一种不同的药物。

三个星期后，皮疹看上去仍然和以前一样多，因此患者登录医疗组的网址，使用医疗保健数字证书来对自己进行鉴别。患者向医生发送一个安全的、非正式的消息：

我已经使用护肤面霜三个星期了，但是不见任何好转，我现在该怎么办？

医生开了一个新处方，告诉患者可以到药房购买或在线定购新的护肤面霜。

当患者在安全的网站上看到来自于皮肤科医生的消息时，他/她只需要简单点击在线药房区，定购护肤面霜，并让药房将其送到患者的家中。

没有数字证书：医生不能鉴别患者是否具有足够高级别的信任度，从而不能通过电子邮件给出治疗疾病的建议。

具有数字证书：医生和患者能够对对方及药剂师进行鉴别。保密消息能够进行交换，并可以向药剂师定购新类型的护肤面霜。所有参与方都相信他们发送过自称已发送的消息。

A.4.11 远程访问临床信息系统

剧 本 描 述：医生接入到单位临床信息系统的结果管理功能。他/她使用系统功能来：

——审查检验结果；

——通过自动生成信件或电子邮件向患者通报他们的结果，包括医生的个人意见；

——安排更多的检验；

——制定新的药物治疗；

——改变药物剂量。

通过电话、信件或单位的保密网站为患者所建新邮箱的电子邮件来通知患者。

系统将浏览过的检验标记为：

——已签署（已阅）；

——已通知患者；

——如何通知；

——如何见效。

没有数字证书：不能鉴别医生的身份具有可接受的信任级别，这样将使上述交换不能进行。

具有数字证书：这些行为和消息的源及接收的抗抵赖性、完整性和保密性是由使用组织的数字证书的临床信息系统和网址提供的。

A.4.12 急救访问

剧 本 描 述：ED医生对陷于半昏迷状态的患者进行治疗。患者思维混乱，无法解释所发生的事情。尽管造成这种情况的潜在原因有很多，但很可能是由于滥用药物的交互作用或并发症，或是由于治疗精神紊乱的药物造成的。当患者有生命危险时，了解治疗史（包括可能使用的娱乐性毒品）以及所有的治疗药物非常重要。例如在北美，在常规治疗中不能看到美沙酮处方，因为美沙酮是受州法律保护的药物滥用计划中的一部分。医生利用“特例”程序，使自己能够访问患者所有的处方和药物信息（包括受限制的信息）。该系统采用数字证书鉴别和医生数字证书的内容来创建一个受限制数据急救访问的记录。

ED医生看到患者有服用可卡因和冰毒的历史，并曾服用过锂。他/她按照所推荐的协议，确保以最快捷的方式进行诊断和治疗。为了IT安全部门和/或安全委员会进行跟踪调查，应创建一个完整的急救访问日志报告。

没有数字证书：按照患者文件中的安全级别，非治疗医生无法访问数据。这种情况可能造成生命危险。如果医生不需要数字证书就能够访问记录，则以访问医生的身份访问记录时不可能具有任何级别的保密性。

具有数字证书：医生可以使用自己的数字证书使自己通过系统的鉴别，从而获得所需的患者信息。而且，对于未授权患者的访问，将留下审计索引，用于今后的调查。

A.4.13 远程转录

剧 本 描 述：通过与美国维吉尼亚的ABC转录服务处电话联系，医生口述一份关于一名患者的会诊记录，其中转录服务处与患者目前就诊的加拿大医院有协议。口述录音可以由印度的转包医疗转录员访问和转录，然后该转录员将其提交给ABC转录服务处的安全网站。当服务处的QA（质量评价）审查员对口述录音文档进行访问、审查和批准后，将该文档再次提交给公司的安全网站，并以可用的电子邮件通知Swanson医院的转录主管人。他/她将该文档提交到医院的安全网址，然后通知医生可以对文档进行查阅了。医生对文档进行访问、查阅和鉴定后，将该文档添加到患者的电子病历中。

没有数字证书：对于转录员、QA审查员或医生，是不可能将自己鉴别到进行互操作所需的信任级别。

具有数字证书：所有被授权方的鉴别和记录的保密性都能够得到保证。而且，以后没有人能够否认进行过通信。

A.4.14 电子处方

剧 本 描 述：预约结束后，医生为患者写了一个电子处方。电子处方系统验证所开的药品是否符合处方规则中患者不知道的药物过敏情况、是否与患者使用的其他药品有配伍禁忌、验证所开药品的数量是否在最佳操作准则内。医生对处方进行数字签名，然后使患者选择的药房能够看到该处方。药房拿到处方后，对医生的医疗资格证和数字签名进行验证，填写并将电子处方归档。在患者来到药房的时候，处方已经准备完毕，并正在等待患者来拿药。

没有数字证书：无法对医生进行鉴别，医生也可以在以后否认其发送过电子处方。

具有数字证书：药房可以验证医生的身份和资格证以及他/她开出的药方。医生在以后不能否认他/她开过电子处方。

A.4.15 鉴别医生医嘱

剧 本 描 述：患者来到医生的办公室，抱怨几个月一直上腹疼痛。患者认为是由于食物和抗酸

药导致了疼痛，这种疼痛是慢性的，而且是周期性发作。经过初步检查后，医生怀疑是胃溃疡病，决定为病人安排门诊上消化道内窥镜检查。通过办公室的计算机，医生可以访问移动诊疗中心的日程安排申请，发现早上有一个合适的检查时间。然后，医生完成为患者进行内窥镜检查的预约申请并对其进行数字签名。

没有数字证书：诊疗中心不能够鉴别医生是否具有足够高的信任级别，因此医生需要打电话给诊疗中心进行预约，这需要相当长的时间。

具有数字证书：医生能够向诊疗中心证明自己并进行预约，诊疗中心也相信是该医生提出的预约，以后他/她将无法否认他/她没有进行过预约。

A.4.16 医疗保健数字签名的潜在应用

剧 本 描 述：下列不完全列表包括要求正规健康专业人员进行签名的文档类别。这种签名需求在立法和管理程序中进行了规定。

a) 用于以下情况的医疗证书：
   1) 所提供的医疗服务(医生或医院的收入、税收)；
   2) 工伤；
   3) 旷课；
   4) 事假(产假，家人生病请假)；
   5) 取消保险的疾病；
   6) 无知情同意能力(智障，如老年痴呆症)；
   7) 紧急医疗援助；
   8) 死亡；
   9) 出生。
b) 治疗处方：
   1) 药物；
   2) 物理疗法。
c) 用于以下情况的索赔申请文档：
   1) 药物；
   2) 矫形装置等。
d) 用于以下情况的体检证明：
   1) 事故；
   2) 保险；
   3) 工作申请；
   4) 对第三方、综合补助、收入支持的帮助；
   5) 残疾人的停车执照；
   6) 社会救济金；
   7) 进入疗养院或回家休息。
e) 对专家或医院护理和实验室药品的请求文档：
   1) 放射科；
   2) 临床实验室；
   3) 病理解剖；
   4) 治疗安排；
   5) 住院治疗：入院、延期、出院。
f) 收集符合临床知识库(肿瘤学等)规则的标准临床数据集。

下一步还有一些要求签名的文档分类，其中包括：

1） 健康卡的发行；
2） 门诊发票的接收；
3） 外科手术台运送证明；
4） 个人门诊医药发票；
5） 集体住院发票；
6） 门诊发票的声明；
7） 普通门诊康复服务声明；
8） 氧治疗康复声明；
9） 每月化验门诊声明；
10） 血液制品及衍生物的声明；
11） 声明表格的总结列表。

没有数字证书：如果这些文档的签名是法律或管理部门要求的，则由被授权人员打印并签署纸面文档，然后由邮局发送出去。

具有数字证书：在大多数情况中，对文档进行签名的健康专业人员的身份并不是决定因素，他/她的角色才是决定因素。可以使用通用的声明来对角色进行简单的定义，其中声明可以是长期有效的（如X是医生），也可以是短期有效的（如X是医学研究所Y的主治医生，X是医学研究所Y的新成员，等等）

医生的角色被看作是一个属性，该属性具有独立于签名功能等的生存期。属性证书与角色证书是相同的。属性证书是由负责角色（如医生职称注册员，对该领域中应用的角色负责的医疗保健研究所）的组织发行的。

文档可附加一个或多个角色属性。发送者或作者使用自己的数字密钥对所有的文档和属性证书进行签名。在比利时，用于签名的公钥和私钥以及证书将发行给每一个国家公民。这项工作目前正在进行中。

可以有一个以上的签名证书和密钥的发行方，但是并不是每个角色都要求具有自己的签名证书。每个角色都要求具有自己的角色证书。因此角色是通过角色证书的附件而不是签名来表示的。签名的技术作用是将文档及附加的证书（完整性方面）绑定在一起，这对于标识/鉴别发送方/作者是必要的。

当遇到特殊的道德规则时，签名应用应对签名者提出警告。例如，一个医生可以是为患者治病的医生，在其他时间里也可以是另一名患者的保险医生（例如，当医生为保险公司工作时，在该医生通过人机界面请求询问其即将使用的医疗信息时，则不允许他/她同时作为治疗医生进行访问）。

参 考 文 献

[1] GB/T 5271.8—2001 信息技术 词汇 第8部分:安全(ISO/IEC 2382-8:1998,IDT)

[2] GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构(idt ISO 7498-2:1989)

[3] GB/T 16262.1—2006 信息技术 抽象语法记法一(ASN.1) 第1部分:基本记法规范(ISO/IEC 8824-1:2002,IDT)

[4] GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架(ISO/IEC 9594-8:2001,IDT)

[5] GB/T 18794.1—2002 信息技术 开放系统互连 开放系统安全框架 第1部分:概述(ISO/IEC 10181-1:1996,IDT)

[6] GB/T 19715.1—2005 信息技术 信息技术安全管理指南 第1部分:信息技术安全概念和模型(ISO/IEC TR 13335-1:1996,IDT)

[7] GB/T 19716—2005 信息技术 信息安全管理实用规则(ISO/IEC 17799:2000,MOD)

[8] ISO/IEC 14516 Information technology—Security techniques—Guidelines for the use and management of Trusted Third Party services

[9] ISO/IEC 15945 Information technology—Security techniques—Specification of TTP services to support the application digital signatures

[10] ENV 13608-1 Health informatics—Security for healthcare communication—Concepts and terminology

[11] IETF/RFC 3126 Electronic Signature Formats for long term electronic signatures

[12] IETF/RFC 3161 Internet X.509 Public Key Infrastructure Time—Stamp Protocol (TSP)

[13] IETF/RFC 3280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[14] IETF/RFC 3281 An Internet Attribute Certificate Profile for Authorization

[15] IETF/RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[16] IETF/RFC 3739 Internet X.509 Public Key Infrastructure Qualified Certificates Profile

[17] ANKNEY, R, CertCo. Privilege Management Infrastructure, v0.4, August 24, 1999.

[18] APEC Telecommunications Working Group, Business Facilitation Steering Group, Electronic Authentication Task Group, PKI Interoperability Expert Group. Achieving PKI Interoperability, September, 1999.

[19] ASTM Draft Standard, Standard Guide for Model Certification Practice Statement for Healthcare. January 2000.

[20] BERND B, ROGER-FRANCE F. A Systemic Approach for Secure Health Information Systems, International Journal of Medical Informatics (2001), 51-78.

[21] Canadian Institute for Health Information. Model Digital Signature and Confidentiality Certificate Policies, June 30, 2001. http://secure.cihi.ca./cihiweb/dispPage.jsp? cw page=infostand pki e.

[22] COBIT (Control Objectives for Information and Related Technologies) specification produced by the Information Systems Audit and Control Foundation.

[23] DRUMMOND Group. The Healthkey Program, PKI in Healthcare: Recommendations and Guidelines for Community-based Testing, May 2000.

[24] EESSI European Electronic Signature Standardization Initiative (EESSI), Final Report of the EESSI Expert Team 20th July 1999.

[25] FEGHHI, J, FEGHHI, J. and WILLIAMS, P. Digital Certificates—Applied Internet Security, Addison-Wesley 1998.

[26] Government of Canada. Criteria for Cross Certification, 2000.

[27] KLEIN, G, LINDSTROM, V, NORR, A, RIBBEGARD, G. and TORLOF, P. Technical Aspects of PKI, January 2000.

[28] KLEIN, G, LINDSTROM, V, NORR, A, RIBBEGARD, G, SONNERGREN, E and TORLOF, P Infrastructure for Trust in Health Informatics, January 2000.

[29] Standards Australia. Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia SAA MP75.

[30] WILSON, S. Audit Based Public Key Infrastructure, Price Waterhouse Coopers White Paper, November 2000.

中 华 人 民 共 和 国
国家标准化指导性技术文件
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 21716.1—2008
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.25 字数 58 千字
2008年7月第一版 2008年7月第一次印刷
*
书号:155066·1-32229 定价 26.00 元

GB/Z 21716.1-2008