ICS 35.240.80
CCS C 07

中华人民共和国国家标准

GB/T 21716.2—XXXX/ISO 17090-2:2015
代替 GB/Z 21716.2—2008

健康信息学　公钥基础设施　第2部分：证书轮廓

Health informatics—Public Key Infrastructure—Part 2: Certificate profile

(ISO 17090-2:2015,MOD）

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件为GB/T 21716第2部分。GB/T 21716《健康信息学　公钥基础设施》分为5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；

——第 4 部分：医疗保健文档数字签名；

——第 5 部分：使用医疗保健 PKI 凭证进行身份验证。

本文件代替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》，与GB/Z 21716.2—2008相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了详细修改部分，见前言；

——增加了文件更新描述，见引言；

——更改了“本指导性技术文件”为“本文件”见全文；

——增加了更新的文献，见规范性引用文件；

——增加了一段,见“1　范围”；

——增加了一段，见 5.2.1 根 CA 证书；

——增加了一段，见 5.2.2 从属 CA 证书；

——更新了标准年代号，见 5.4.5 AC，6.1 证书的符合性，7.3.1 医疗保健角色属性；

——修改了语句表达，见 5.4.5 AC，7.1 概述，7.2.7 基本约束，见附录 A；

——增加了注，见 6.3.2 签名；

——修改了表内容，见表 3；

——更改了参考文献。

本文件修改采用ISO 17090-2：2015《健康信息学　公钥基础设施　第2部分：证书轮廓述》。

本文件与ISO 17090-2：2015的技术差异及其原因如下：

——根据 GB/T 1.1—2020 对“1　范围”进行修改。

——删除了引言中最后四段文字

——根据中国国情，将正文中示例包括的国家名称、单位名称等修改为中国的中文名称；

——不改变技术内容的编辑性修改。

本文件由中国标准化研究院提出并归口。

本文件起草单位：中国标准化研究院、中国人民解放军总医院、北京航空航天大学、上海中医药大学、深圳市卫生健康发展研究和数据管理中心、福建省中科标准科技有限责任公司、浙江大学、浙江师范大学、北京信息科技大学、厦门市众科佰联标准化服务有限公司、福建理工大学。

本文件主要起草人：。

本文件及其所代替文件的历次版本发布情况为：

——2008 年首次发布为 GB/T 21716.2—2008；

——本次为第一次修订。

引　言

为了降低费用和成本，医疗保健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它应用来进行交换。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。

医疗保健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。

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、操作的互操作性至关重要。

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它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，本文件的目的是为这些迅速发展的国际应用提供指导。

数字证书技术在某些方面仍在发展，而这些方面并非特定于医疗保健。重要的标准化工作以及在某些情况下的支持性立法正在进行中。另一方面，许多国家的医疗保健提供者已经在使用或计划使用数字证书。本文件旨在满足对这些快速发展的指导需求。

本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。

本文件的三个部分作为一个整体定义了在医疗保健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。

本文件的第1部分规定了医疗保健行业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。

本文件的第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 5280中规定的医疗保健轮廓。

本文件第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。

GB/T 21716的第4部分通过提供生成和验证数字签名及相关证书的最低要求和格式，支持数字签名的可互换性并防止不正确或非法的数字签名。

GB/T 21716的第5部分定义了基于GB/T 21716系列中定义的 PKI 验证实体凭证的程序要求，用于医疗保健信息系统（包括访问远程系统）。

健康信息学　公钥基础设施　第2部分：证书轮廓

1　范围

本文件规定了在单独组织内部、不同组织之间和跨越管辖界限时医疗保健信息交换所需要的证书轮廓。还详述了公钥基础设施数字证书在医疗行业中形成的应用，并侧重描述了其中与证书轮廓相关的医疗保健问题。

本文件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使用。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

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

GB/Z 21716.3　健康信息学　公钥基础设施　第3部分：认证机构的策略管理

IETF/RFC 5280　Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile（互联网Internet X.509 公钥基础设施证书和CRL轮廓）

1ETF / RFC 3281针对机构的因特网属性证书轮廓

1ETF / RFC 3739 Internet X. 509公钥基础设施合格证书轮廓

3　术语和定义

GB/T 21716.1界定的术语和定义适用于本文件。

4　缩略语

下列缩略语适用于本文件。

AA	属性机构	attribute authority
AC	属性证书	attribute certificate
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	证书吊销列表	certificate revocation list
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　医疗保健证书策略

5.1 医疗保健证书类型

标识证书应发行给：

——个人（正规健康专业人员、非正规健康专业人员、受托医疗保健供应者、支持组织的雇员、患者/消费者）；

——组织（医疗保健组织和支持组织）；

——设备；

——应用。

通过标识证书本身（证书的扩展部分）或关联的AC，应可以获取个人和组织的角色信息。不同种类的证书及其关联见图1。

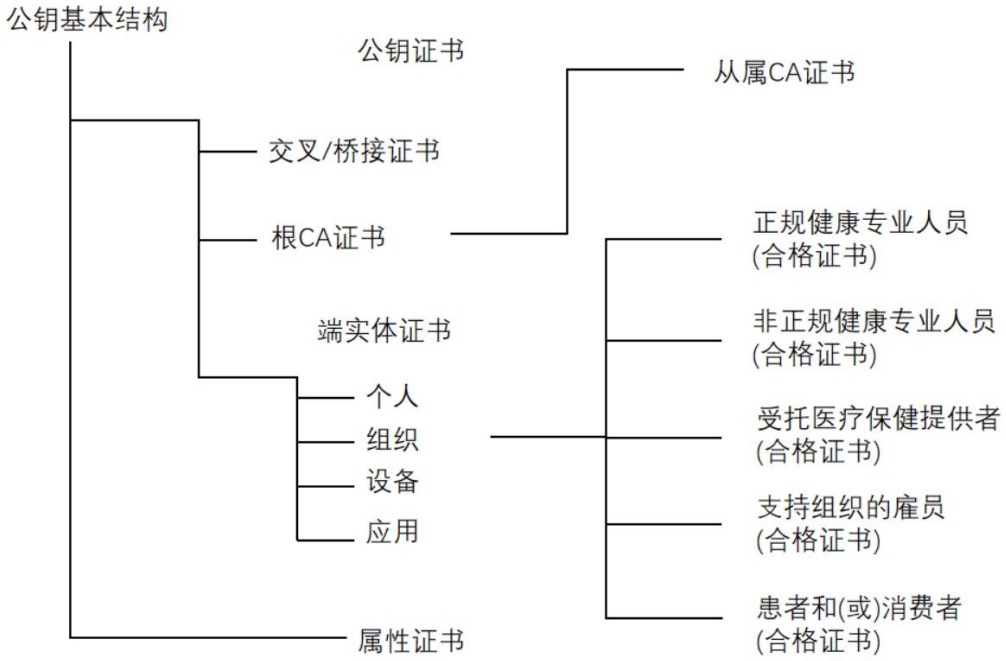

图1 医疗保健证书类型

5.2 CA 证书

5.2.1 根 CA 证书

当证书的主体本身是一个CA时，使用根CA证书，根CA证书自我签名，向依赖方（包括从属CA）颁发证书。基本约束字段指示证书是否是CA。根CA证书通过互联网浏览器和其他依赖PKI进行实体识别和身份验证的应用程序建立信任链。

5.2.2 从属 CA 证书

从属CA证书是对CA发行的，该CA完全通过另外的高层CA认证，而高层CA可对低层CA或端实体发行证书。从属 CA 证书与其他证书一起使用，由依赖 PKI 进行实体识别和身份验证的互联网浏览器和其他应用程序建立信任链。

5.3 交叉/桥接证书

在因特网环境中，期望跨界和跨辖区的医疗行业信任顶层CA是不可行的。替代方法是在每个医疗行业领域建立信任孤岛，这些“信任孤岛”是基于信任特定CA的专业、权限、位置或地区的。而后，每个“信任孤岛”的中枢根CA可以交叉地验证另外的根。在这些情形中，一组CA可以达成在其策略和相关规范声明中具体化的标准的最小集合。如果达成了标准的最小集合，依赖方可以接受自己本领域外的证书，这对于跨越国家和省份管理机构传输信息是非常有效的。

交叉/桥接证书是不同CA领域交叉验证的证书类型。这种证书支持公钥应用的大范围开展，例如医疗行业中安全电子邮件和其它需求。

5.4 端实体证书

端实体证书对包括个人、组织、应用或设备的实体发行。之所以被称为端实体，是因为没有依赖于此证书的更深一层的实体存在。

5.4.1 个人标识证书

个人标识证书是为证明目的而对个人发行的端实体证书的特定种类。人们公认以下五种类型的医疗保健参与者可视为个人：

a) 正规健康专业人员

证书持有者是健康专业人员。他/她为了履行其职业范围内的工作，需要有关政府机构给予许可和注册。此类证书可以是资格证书。

b) 非正规健康专业人员

证书持有者是健康专业人员，但他/她不属于有关政府机构给予许可和注册的人员。此类证书可以是资格证书。

c) 受托医疗保健提供者

证书持有者是在医疗保健社区活动的个人，并且由一个受限医疗保健组织或专业人员主管。此类证书可以是资格证书。

d) 支持组织的雇员

证书持有者是一个受雇于某医疗保健组织或支持组织的个人。此类证书可以是资格证书。

e) 患者/消费者

证书持有者是可能接受、正在接受或已经接受正规或非正规健康专业人员服务的个人。此类证书可以是资格证书。

5.4.2 组织标识证书

与医疗行业密切相关的组织可以持有用于识别自身和加密目的的证书。根据IETF/RFC 3647，这一部分对组织单位名称进行了规定。

5.4.3 设备标识证书

设备可以是计算机服务器、医疗设备（例如X光机）、重症信号监视设备或需要单独识别和验证的假体设备。

5.4.4 应用证书

应用程序是需要单独识别和验证的计算机信息系统，例如医院的患者管理系统。

本文件主要是关于提供者的，但也认识到在医疗保健自行管理方面患者/消费者将更加需要数字证书可提供的安全服务。

5.4.5 AC

AC是属性的数字签名集合或证明集合。AC是类似于PKC的构造，主要区别是AC不包括公钥。AC可以包括特定组成员、角色、安全清除和其他有关AC持有者的信息，此类信息不可以用于访问控制。AC应符合IETF/RFC 5755（针对机构的因特网属性证书轮廓）的有关规定。

在医疗保健行业的环境中，AC可以充当传送机构信息的重要角色。机构信息完全不同于可包括在PKC中的关于医疗保健或执照的信息。角色和执照暗示机构水平，而其本身并非机构信息。应注意到对AC的详细规范仍在发展中，而且还应注意AC的详细规范需要在软件工业中更广泛地加以实现。

AC的语法在IETF/RFC 5755中指定。

AC采用下列组件：

version(版本号)用于区分AC的不同版本。如果objectDigestInfo呈现或issucr被标识等同于baseCertificateID，则其版本应该是 v2。

Owner（拥有者）字段传递AC持有者的标识。此字段要求采用特定PKC的发行者名称和序列号，也可选择使用一般名称,但禁用对象摘要。通过一般名称本身识别持有者时,GeneralNames的使用具有危险，此时公钥对名称与公钥的绑定不够充分,使得拥有者标识认证过程局限于AC的使用。此外,GeneralNames的某些选项（例如：IPAddress）不适用于命名是角色而不是个人实体的AC持有者。一般名称的形式应该限制为被识别的名称、RFC 822(电子邮件)地址和(对角色名称的)对象标识符。

issuer（发行方）字段传递发行证书的AA的标识。要求使用发行商名称和特定的PKC序列号，一般名称的使用随意。

signature(签名)标识了用于数字化签名于AC的加密算法。

serialNumber(序列号)是唯一在其提供方范围内标识AC的序列号。

attrCertValidityPeriod（属性证书有效期限）字段表示AC被视为有效的时间段，以GeneralizedTime 格式表示。

Attributes（属性）字段包含需验证的证书持有者的属性（如特权）。

issuerUniqueID（发行方唯一ID）可用于标识 AC 的发行方，当用发行方的名称进行标识不充分的情况下。

extensions扩展字段允许向AC添加新字段。

GB/Z 21716.1—2008中8.3对医疗领域中AC的使用进行了详细的规定。

5.4.6 角色证书

用户的AC可以包含对另一个具有附加特权AC的引用。这为实现特权角色提供了一种有效的机制。

许多具有授权要求的环境要求在其操作的某些方面使用基于角色的特权（典型情况是有关基于标识的特权）。因此，申请方可以向验证方提供证明仅申请方具有特定角色的证据（例如“管理者”或“购买者”）。验证方也可以辨别出其优先程度或者通过其他方式发现有关的声明角色，以便做出通过或失败的授权决定。

以下各项内容均是可行的：

——任何 AA 可以定义任何角色的编号；

——角色本身和角色的成份可以由不同 AA 分别进行定义和管理；

——为给定角色所设定的特权可以放置在一个或多个 AC 之中；

——也可以将角色的成份仅设定为一个与角色相关的特权子集；

——角色的成份可以被代表；

——可以为角色和成份设定任何适当的生命周期。

设定一个实体包含一个属性，该属性用于断言其实体具有的角色。这种证书具有指向另一个定义角色的AC的扩展段（即，角色证书规定作为持有者的角色，且包括设定该角色的特权的列表）。实体证书的发行方可以与角色证书的发行方无关，可以完全单独管理（终止、取消等等）这些设定。

不是所有GeneralName（通用名称）均适用于角色名称。最好是选用对象标识符和可区分名。

6 一般证书要求

6.1 证书的符合性

以下要求适用于本部分所规定的全部证书：

a) 证书应属于 X.509 第 3 版规定的证书；

b) 证书应与 IETF/RFC 5280 相一致。仅在与 IETF/RFC 5280 有关的已知问题建议方案相结合的情况下，方允许偏离 IETF/RFC 5280；

c) 在个人标识方面，证书应符合 IETF/RFC 3739 的规定。仅在与已知问题的建议方案相结合的情况下，才允许偏离 IETF/RFC 3739；

d) 签名字段应标明所采用的签名算法；

e) 证书公钥应根据所采用的算法决定最小密钥长度字段。密钥的大小应符合 GB/TZ 21716.3—2008 中 7.6.1.5 的规定。

f) 数字加密密钥的使用不应与抗抵赖和数字签名的使用相混合。（见 7.2.3）

以下内容描述了图1所标识的所有医疗保健数字证书中的通用要素。这些要素是通用性的，使用他们可以构建不同种类的证书。

Certificate ： ： = SIGNED { SEQUENCE }		
Version	**[0]**	**Version DEFAULT v1**
SerialNumber		**CertificateSerialNumber**
Signature		**AlgorithmIdentifier**
Issuer		**Name**
Validity		**Validity**
Subject		**Name**
SubjectPublicKeyInfo		**SubjectPublicKeyInfo**
IssuerUniqueIdentifier	**[1]**	**IMPLICIT UniqueIdentifier OPTIONAL**
SubjectUniqueIdentifier	**[2]**	**IMPLICIT UniqueIdentifier OPTIONAL**
Extensions	**[3]**	**Extensions MANDATORY**

version（版本）是编码证书的版本。证书版本应是v3

6.2 各类证书的通用字段

a) serialNumber（序列号）是由 CA 为每个证书设定的一个整数，唯一标识每个证书。
相对特定 CA 发行的全部证书而言，每个 serialNumber 均是唯一的（即，发行商名称和序列号可标识唯一证书）。

b) signature（签名）包含 CA 为证书签名所使用的算法的算法标识符；

c) issuer（发行方）标识实体名称，该实体已签名并发行了证书。此字段应采用适当的 ISO 名称结构，并符合组织或组织单元中组织/角色的对象类别；

d) validity（有效性）是指 CA 授权证书中包含的信息有效的时间间隔，对于正规健康专业人员，CA 应确保证书的有效期不超过专业执照的有效期。为此，CA 应将证书有效期设置为不超过

专业执照的期限，或者在执照到期日之前确认专业执照的续期，如果专业执照未被更新，则撤销或暂停证书。

关于时间格式的注释：

可识别编码规则（DER）允许使用多种方法来格式化 UTCTime 和 GeneralizedTime。所有使用相同格式使签名验证问题最小化的实现均是重要的。如果年份大于或等于 2050 年，则应使用 GeneralizedTime 来编码时间。为了确保 UTCTime 编码格式一致，UTCTime 应使用“Z”格式进行编码，并且不要忽略第二个字段，即使是 00（即，格式应是 YYMMDDHHMMSSZ）。当这样编码时，当 YY 大于或等于 50 时，年份字段 YY 应解释为 19YY；当 YY 小于 50 时，应解释为 20YY。当使用 GeneralizedTime 时，应以“Z”格式对 UTCTime 编码，并应包含第二个字段（即，格式应是 YYYYMMDDHHMMSSZ）。

e) **subject**（主体）标识在主体公钥字段所发现的公钥相关联的实体的名称；

f) **subjectPublicKeyInfo**（主体公钥信息）用于携带公钥，并标识该公钥所采用的算法；

g) **issuerUniqueIdentifier**（发行方唯一标识符）是用于唯一标识发行方的选择性位串。（RFC 5280 标准建议不使用该字段）；

h) **subjectUniqueIdentifier**（主体唯一标识符）是用于唯一标识主体的选择性位串。（同意 RFC 5280 的规定，建议不使用该字段）；

i) **extensions**（扩展）应表示的一个或多个扩展的 SEQUENCE（次序）。

通过 X.509 所定义的标准签名数据类型的方式将证书的签名附加给证书数据类型。

6.3 通用字段规范

6.3.1 概述

下列条款规定了对基本证书字段中信息内容的要求。对这些内容，IETF/RFC 5280 或 IETF/RFC 3279未进行规定。

6.3.2 签名

建议在签名字段中包含下列其中的一项值：

a) md5WithRSAEncryption (1.2.840.113549.1.1.4)；

b) sha1WithRSAEncryption (1.2.840.113549.1.1.5)；

c) dsa-with-sha1 (1.2.840.10040.4.3)；

d) md2WithRSAEncryption (1.2.840.113549.1.1.2)；

e) ecdsa-with-SHA1 (1.2.840.10045.2.1)；

f) ecdsa-with-SHA224 (1.2.840.10045.4.3.1)；

g) ecdsa-with-SHA256 (1.2.840.10045.4.3.2)；

h) ecdsa-with-SHA384 (1.2.840.10045.4.3.3)；

i) ecdsa-with-SHA512 (1.2.840.10045.4.3.4) ；

j) d-RSASSA-PSS (1.2.840.113549.1.1.10)；

k) sha256WthRSAEncryption 1.2.840.113549.1.1.11；

l) sha384WithRSAEncryption 1.2.840.113549.1.1.12；

m) sha512WithRSAEncryption 1.2.840.113549.1.1.13。

注：包括 MD2、MD5 和 SHA1 hash算法 [列表项a到e]，以便向后兼容旧系统。这些hash算法已被当代系统中更新、更强大的算法所取代 [参见列表项f至m]。

6.3.3 有效性

有效日期应符合IETF/RFC 5280的规定。按照GB/Z 21716.3 2008中7.6.3.2 的规定，本部分对健康证书有效期规定了适度的约束。

证书的 notBefore time（有效期起始时间）表示 CA 将从何时开始维护并发布有关证书状态的准确信息。

6.3.4 主体公钥信息

应标识算法标识符，例如：

a) RSA
pkcs-1 OBJECT IDENTIFIER ：：= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) 1 }
rsaEncryption OBJECT IDENTIFIER ：：= { pkcs-1 1}

b) Diffie-Hellman
支持Diffie-Hellman OID的轮廓是通过ANSI X9.42 [X9.42] 定义的。
dhpublicnumber OBJECT IDENTIFIER ：：= { iso(1) member-body(2)
us(840) ansi-x942(10046) number-type(2) 1 }

c) DSA
本轮廓支持的 DSA OID 为：
id-dsa ID ：：= { iso(1) member-body(2) us(840) x9-57(10040)
x9cm(4) 1 }

d) Elliptic Curve
Ecdsa [1, 2,840,10045,2,1]}
引用GB/T 21716.3 2008中7.6.1.5对密钥大小的规定。

6.3.5 发行方名称字段

存储在发行者名称字段中的发行者名称，应符合下述规定的修改和限制。与适当的ISO名称结构保持一致，该名称结构依据对象类别Organizational Role（组织角色），位于某个组织或组织单元之下。

第6.4为各类证书规定了发行方名称字段的内容。

a) 国家名称：国家名称（**countryName**）应包括 ISO 双字符国家标识符。在医疗保健领域必须能分辨出用来请求访问个人健康信息所提供的证书的起源国家，所以此字段是必备的。不同国家有不同保护客户/消费者隐私方面的法律和法规，分辨出请求起源的国家将有助于做出是否批准请求的决定。

示例：国家名称=“CN”

b) 地点名称：地点名称（**localityName**）可用于存储至少一个地点名称数据。本文件将规定地点名称的两层应用。顶层是指列入地理地点名称值后面的国家。在证书发行方名称内，可以省略高层地点名称，仅使用地理地点名称。

示例：地点名称=“北京”

c) 组织名称：组织名称（**organizationName**）字段应包括组织注册名称的全称，组织名称是指端实体情况下的受托医疗保健组织和 CA 证书情况下的 CA 的组织名称。

示例：组织名称=“北京市卫生局”

d) 组织单元名称：如果存在组织单元，组织单元名称（**organizationalUnitName**）用于存储特定组织下属的组织单元/科室。通过纳入多于一个的字段值，可以在若干层次中规定组织单元。在存在组织单元的情况下，应该以在 CA 范围内避免名称多义性的方法选择组织单元名称。
组织单元名称=“安贞医院放射科”

e) 通用名称：本字段用于描述被普遍认知的主体的名称。在为用户提交证书时，此字段通常与通用名称（commonName）主体一同通过标准化软件组件来使用。所呈现的名称应具有信息性，便于理解证书发行者和证书的用途。还建议在通用名称（commonName）字段值中包含管理证书策略的名称。

示例：通用名称=“患者健康信息策略”

6.3.6 主体名称字段

存储于主体名称字段的主体名称应符合下述定义的修改和限制，与适当的ISO名称结构保持一致，该名称结构依据对象类别Organizational Role（组织角色），位于某个组织或组织单元之下。

医疗保健执行者的资格和头衔应反映在证书扩展（HCRole字段）中。

第6.4规定了每种证书类型的主体名称的内容。附加的建议和指南见ISO TS 21091。

a) 国家名称：国家名称（countryName）应包含 ISO 双字符国家标识符。

示例：国家名称=“CN”

此字段的配置应反映该国家的实际表达。

对于 CA、正规的和非正规的专业人员、负责医疗保健的提供方、支持组织雇员及组织来说，此字段均是必备的，因为在医疗保健领域分辨实体的起源国家是非常关键的，这种实体是由于访问个人健康信息的请求所提交的证书的主体。不同国家有着不同的保护客户/消费者政策方面的保密法律和法规，分辨请求来自哪个国家将辅助决定是否接受请求。

b) 地点名称：地点名称（localityName）可用于存储至少一个地点名称数据。本文件将规定地点名称的两层应用。顶层是指列入地理地点名称值后面的国家。在证书主体名称内，可以省略顶层地点名称，仅使用地理地点名称。

示例：地点名称=“北京”

c) 组织名称：组织名称（organizationName）字段应包括组织注册名称的全称，组织名称是指端实体情况下的受托医疗保健组织和 CA 证书情况下的 CA 的组织名称。

示例：组织名称=“北京安贞医院”

d) 组织/单元名称： 如果存在组织单元名称（organization/UnitName）字段，则该字段用于存储特定组织下属的组织单元/科室名称。通过纳入多于一个的字段值，可以在若干层次中规定组织单元。在存在组织单元的情况下，组织单元名称的选择方法应采用避免名称的多义性的方法。

在某些区域医疗保健实现中，例如，在日本，组织单元用于存储医疗保健角色。因为某些卖方的路由器/防火墙可以访问组织单元，而这种方法可用来施加批准或约束访问的规则，故这种方法在虚拟专业网实现中是有益的。这种方法还可以使依赖方直接从证书中读取角色信息。在组织/单元名称字段存在的情况下，该字段可以用来存储健康角色。

示例：组织单元名称=“北京安贞医院放射科”

示例：组织单元名称=“认可的内科医师”

e) 通用名称：此字段用于描述名称，通过该名称其主体通常可以被辨别。

示例：通用名称=“李国强”（人名）

对于作为证书主体的人和组织来说，此字段是必备的。在决定是否允许访问个人健康信息时，能够在健康系统中标识可以分辨某个人的通用信息是十分重要的。

f) 姓：此字段用于描述可用来分辨主体的姓。此字段可能存在。如果存在，它可以明显地标识主体，因为在医疗保健系统中可以分辨它。

示例：通用名称=“李”

g） 名：此字段用于描述通常可用来分辨主体的名。此字段可能存在。由于在医疗保健系统内部可以分辨它，所以它可以明确地标识主体。

示例：名= “国强”

h） e-mail：此字段的主要用途是记录主体的电子邮件地址。

示例：e-mail = donglx@health.com.cn

在主体区分名称中同时包含电子邮件地址属性以支持旧版实现的做法已被 IETF RFC 5280 弃用，但仍是允许的。本文件建议不要在主体名称字段中使用电子邮件，而是在subjectAltName（主体替换名称）字段中使用。

6.4 对各种医疗保健证书类型的要求

6.4.1 发行方字段

对各种医疗保健证书类型的发行方字段要求见表1。

表1 对各种医疗保健证书类型的发行方字段要求

证书要素	CA 证书		标识证书						属性证书
	认证机构证书 b	交叉/桥接证书	正规健康专业人员证书	非正规健康专业人员证书 c	消费者证书	组织证书	设备证书	应用证书	
发行方字段 a									
国家名称	必备的	必备的	必备的	必备的	必备的	必备的	必备的	必备的	可选的
地点名称	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的
组织名称	必备的	必备的	必备的	必备的	必备的	必备的	必备的	必备的	可选的
组织单元名称	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的
通用名称	必备的	必备的	必备的	必备的	必备的	必备的	必备的	必备的	不适用

[a] 本表引用在证书类型之间可以改变的发行方 ID 要素。

[b] 认证机构证书引用向端实体发行证书的要素。

[c] 非正规健康专业人员证书的值也适用于受托医疗保健提供者证书和支持医疗保健雇员证书。

6.4.2 主体字段

对各种医疗保健证书类型的主体字段要求见表2。

表2 对各种医疗保健证书类型的主体字段要求

证书要素	CA 证书		标识证书						属性证书
	认证机构证书 b	交叉/桥接证书	正规健康专业人员证书	非正规健康专业人员证书 c	消费者证书	组织证书	设备证书	应用证书	
主体字段 a									
国家名称	必备的	必备的	必备的	必备的	可选的	必备的	可选的	可选的	可选的
地点名称	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的
组织名称	必备的	必备的	可选的	可选的	可选的	必备的	可选的	可选的	可选的
组织单元名称	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的
通用名称	必备的	必备的	必备的	必备的	必备的	必备的	可选的	可选的	可选的

名	不适用	不适用	可选的	可选的	可选的	不适用	不适用	不适用	可选的
姓	不适用	不适用	可选的	可选的	可选的	不适用	不适用	不适用	可选的
电子邮件	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的

[a] 本表引用在证书类型之间可以改变的主体字段 ID 要素。

[b] 认证机构证书引用向端实体发行证书的要素。

[c] 非正规健康专业人员证书的值也适用于受托医疗保健提供者证书和支持医疗保健雇员证书。

7 证书扩展的使用

7.1 概述

关于在X.509第3版医疗保健证书中的实现应该具有证书扩展的一般要求如下。有关这些扩展的更详尽的信息见IETF/RFC 5280 和 IETF/RFC 3739。

7.2 一般扩展

7.2.1 机构密钥标识符

此扩展应标识用于验证证书签名的公钥。它使一个 CA 使用的不同密钥能够被区分（例如，当密钥更新时）。

仅使用**authorityKeyIdentifier**（机构密钥标识符）扩展中的密钥标识符（keyIdentifier）。

这是一个非关键扩展。如果使用，建议将该扩展配置为强制扩展。

7.2.2 主体密钥标识符

此扩展用于标识在证书的subjectPublicKeyInfo（主体公钥信息）字段保存的公钥。

IETF/RFC 5280包括如何从公钥中导出密钥标识符（keyIdentifier）的指南。

对于信赖医疗保健链内所有端实体证书和所有CA证书来说，此扩展是必备的和非关键的。

7.2.3 密钥使用

keyUsage（密钥使用）扩展应标识证书中有关公钥的基本密钥使用。加密和数字签名的单独密钥对的使用是受阻止的，且数据加密（**dataEncipherment**）密钥的使用不应与抗抵赖或数字签名（**digitalSignature**）密钥的使用混合（见6.1）。

此扩展是必备的。建议（按IETF/RFC 5280的规定）此扩展为关键扩展。

7.2.4 私钥使用期（privateKeyUsagePeriod）

建议不使用此扩展。

不存在此扩展时，缺省私钥使用期为证书的有效期。

7.2.5 证书策略

certificatePolicies（证书策略）扩展应包括GB/Z 21716.3规定的标准化证书CA策略的**objectidentifier**（对象标识符）。

此扩展为必备的和非关键的。

7.2.6 主体替换名称

建议将subjectAltName（主体替换名称）扩展表示在证书中。建议此扩展包含一项符合RFC 822的签署人电子邮件地址。如果此扩展包括目录名，则它应该以UTF8字符串开始，UTF8字符串提供国际字符集的目的支持主体可区别名。

此扩展为可选的和非关键的扩展。

7.2.7 基本约束

basicConstraints（基本约束）扩展含有一个布尔值，用于规定主体是否可作为CA活动，使用被认证的密钥签署数字证书。如此，也可对认证路径长度的约束进行规定。

CA证书应包括CA值为“真”的basicConstraints（基本约束）扩展。

关于此扩展是否是关键的和可选的见表3。

端实体证书（个体的正规健康专业人员、非正规医疗保健雇员、受托医疗保健提供者、支持医疗保健雇员、消费者、组织、应用和设备证书）不应将此扩展设定为“真”。

7.2.8 证书撤消列表分布点

IETF/RFC 5280建议通过CA和应用支持CRLDistributionPoints（证书撤消列表分布点）扩展。对于依赖CRL分布点的医疗保健实现来说，此扩展应标识在数字证书目录中的相关CRL（或CA证书的ARL）地址，并应作为必备的和非关键的扩展。

7.2.9 扩展密钥使用

ExtKeyUsage（扩展密钥使用）字段指出已验证的公钥可以用做的一个或多个用途，而对基本用途的添加或替换在密钥使用扩展字段指出。

此扩展为可选的和非关键的扩展。

7.2.10 机构信息访问

authorityInfoAccess（机构信息访问）扩展指出如何访问发行CA证书OCSP的应答器。此字段不规定CRL的地址。此字段由一系列的访问方法和访问地址组成。在该序列中的每个入口描述关于CA附加信息的格式和地址。访问方法规定信息的类型和格式，访问地址规定信息的地址。

此扩展是可选的、非关键的扩展。

7.2.11 主体信息访问

subjectInfoAccess（主体信息访问）指出如何访问主体CA证书和服务，例如，时间戳。此扩展是可选的、非关键的扩展。

7.3 专用主体目录属性

7.3.1 医疗保健角色属性

医疗保健角色（hcRole）属性允许对正规的和非正规的健康专业角色数据进行编码。因为实现此编码可在健康角色的认证中提供国际化的互操作性，故建议实现。这将允许多种证书发行，并使类别表的排列与此字段相关。提议此字段设有扩展机制，以允许采用国家或区域健康角色编码模式。

因为证书持有者的医疗保健角色是构成证书持有者标识的整体的组成部分，所以在标识证书中需要此字段。一旦经过验证，按照GB/Z 21716.1 2008中8.4 的规定，更多的信息更适合放置在AC中。

本部分允许对包括专业人员标识在内的局部数据的断言，例如，注册编号、帐单编号和患者标识符。见下述局部数据（REGIONAL-DATA）。详见下文中的“局部数据（REGIONAL-DATA）”部分。

```
hcRole ATTRIBUTE    : : =   {
    WITH SYNTAX                     HCActorData
    EQUALITY MATCHING RULE          hcActorMatch
    SUBSTRINGS MATCHING RULE        hcActorSubstringsMatch
    ID                              id-hcpki-at-healthcareactor}
```

对象标识符的赋值

本文件给定如下值：

```
{iso (1) standard (0) hcpki (17090)}
    id-hcpki    OBJECT IDENTIFIER   : : = 1.0.17090
id-hcpki-at OBJECT IDENTIFIER  : : = {id-hcpki 0 }
    id-hcpki-at OBJECT IDENTIFIER : : = 1.0.17090.0
id-hcpki-at-healthcareactor OBJECT IDENTIFIER  : : = {id-hcpki-at 1}
    id-hcpki-at-healthcareactor OBJECT IDENTIFIER : : = 1.0.17090.0.1
id-hcpki-cd OBJECT IDENTIFIER  : : = {id-hcpki 1}
    id-hcpki-cd OBJECT IDENTIFIER  : : = 1.0.17090.1
id-hcpki-is OBJECT IDENTIFIER  : : = {id-hcpki 2}
    id-hcpki-is OBJECT IDENTIFIER  : : = 1.0.17090.2
```

数据类型的定义：

```
HCActorData     : : = SET OF HCActor
HCActor : : = SEQUENCE {
        codedData   [0] CodedData OPTIONAL,
        RegionalHCActorData [1]
                            SEQUENCE OF RegionalData OPTIONAL }
CodedData : : = SET {
    codingSchemeReference   [0] OBJECT IDENTIFIER,
    ---- Contains the ISO coding scheme Reference
    ---- or local coding scheme reference achieving ISO or national registration.
    ---- The ISO coding scheme OID is id-hcpki-is (defined above).
    ---- At least ONE of the following SHALL be present:
    codeDataValue [1] UTF8String OPTIONAL,
    codeDataFreeText [2] DirectoryString OPTIONAL }
RegionalData : : = SEQUENCE {
    type    REGIONALDATA.&id({SupportedRegionalData}),
    value   REGIONALDATA.&Type({SupportedRegionalData}{@type})}
```

局部数据对象类别的定义：

```
REGIONALDATA    : : =   CLASS {
                                &Type,
                            &id OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX     {
        WITH SYNTAX &Type
                ID      &id }
```

所支持的局部数据对象类别集合的定义：

```
SupportedRegionalData REGIONALDATA : : =
```

```
    {coded,
            —expect additional regional/national objects to be defined}
```

代码信息对象的定义：

```
coded   : : = REGIONAL-DATA {
    WITH SYNTAX CodedRegionalData
                ID  id-hcpki-cd}
CodedRegionalData   : : = SEQUENCE {
    country [0] PrintableString (SIZE (2)),
        -- ISO3166 code of country of issuing authority.
    issuingAuthority    [1] DirectoryString,
        -- Identifier of issuing authority as Regional Entity.
        -- Could be implemented as a true identifier or a
        -- Directory lookup string (to be determined)
    hcMajorClassCode    [2] CodedData,
    hcMinorClassCode    [3] CodedData OPTIONAL
```

用于此字段的代码，例如 ASTM E1986-98 数据用户角色名称。

建议**HcActor**取自适当的国家编码模式。

对于正规健康专业人员证书和非正规健康专业人员证书来说，此扩展是必备的和非关键的扩展。在其它情况下，是可选的和非关键的扩展。

7.3.2 主体目录属性

建议将此扩展在个体标识证书中表示。在这种证书中，此扩展可以包含hcRole属性（见7.3.1）。另外，**subjectDirectoryAttributes**（主体目录属性）可以包括本文件未规定的其它属性。

应将此扩展标记为非关键的扩展。由于此证书用于认证和指定角色的用途，所以对于正规健康专业人员证书和非正规健康专业人员证书来说，此扩展是必备的。对于其它证书类型来说，此扩展的使用是可选的。

7.4 资格证书声明扩展

建议在正规健康专业人员证书和非正规健康专业人员证书中包含一项**qcStatement**（资格证书声明）。对于患者/消费者、受托医疗保健提供者、支持组织雇员的证书来说，可以包含一项**qcStatement**主体目录属性。在设备和应用证书中不应包含此**qcStatement**属性。有关的详细规定见IETF/RFC 3739。

建议符合性应用程序能够支持**qcStatements**扩展。

此扩展是可选的和非关键的扩展。

7.5 对每种医疗行业证书类型的要求

7.5.1 扩展字段

对每种医疗行业证书类型的扩展字段要求见表3。

表3 对各种医疗行业证书类型扩展字段的要求

证书要素	CA 证书		标识证书						属性证书
	认证机构证书	交叉/桥接证书	正规健康专业人员证书	非正规健康专业人员证书[C]	消费者证书	组织证书	设备证书	应用证书	

一般扩展									
authorityKeyIdentifier[a]（机构秘钥标识符）	必备的[a]	必备的[a]	必备的[a]	必备的[a]	必备的[a]	必备的[a]	必备的	必备的[a]	可选的
subjectKeyIdentifier（主体秘钥标识符）	必备的	必备的	必备的	必备的	必备的	必备的	必备的	必备的	可选的
keyUsage（秘钥使用）	必备的	必备的	必备的	必备的	必备的	必备的	必备的	必备的	可选的
privateKeyUsagePeriod（秘钥使用期限）	缺省的	缺省的	可选的	可选的	可选的	可选的	可选的	可选的	可选的
certificatePolicies（证书策略）	必备的	必备的	必备的	必备的	必备的	必备的	必备的	必备的	可选的
subjectAltName（主体替代名称）	缺省的	缺省的	可选的	可选的	可选的	可选的	可选的	可选的	可选的
subjectDirectoryAttributes（主体目录属性）	缺省的	缺省的	可选的	可选的	可选的	缺省的	缺省的	缺省的	可选的
basicConstraints（基本约束）	必备的和强制的	必备的和强制的	可选的	可选的	可选的	可选的	可选的	可选的	可选的
CRLDistributionPoints（CRL 分布点）	必备的	必备的	必备的	必备的	必备的	必备的	必备的的	必备的	可选的
ExtKeyUsage（扩展秘钥使用）	可选的	可选的	可选的	可选的	可选的	可选的	可选的	缺省的	可选的
其他扩展									
机构信息访问	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的	可选的
qcStatements extension（Qc 声明扩展）	缺省的	缺省的	必备的[c]	必备的[c]	必备的[c]	缺省的	缺省的	缺省的	可选的
Hcrole（Hc 角色）	缺省的	缺省的	可选的	可选的	可选的	可选的	可选的	缺省的	缺省的

[a] 建议此字段为必填项。

[b] 非正规健康专业人员证书的值也适用于受托医疗保健提供者证书和支持性医疗保健雇员证书。

[c] 在使用资格证书对应的辖区内，“必备的”受法律支持。

附 录 A
（资料性）
证书轮廓示例

A.1 概述

为了说明各类证书的细节，特给出下列基本性详细示例。这些示例不是规范性的。其规范性代码和文本见本部分的正文。

A.2 示例1：消费者证书轮廓

注：以下示例仅仅是说明性的，并不试图声明英国国家健康服务(NHS)证书将来所采用的格式。

Bill Smith的NHS 编号 为368964278，证书发行日期为2001年8月1日，证书终止日期为2006年8月1日。

Version		(2 – decimal code for version 3 certificates)
SerialNumber		(unique CA generated decimal number)
Signature		(sha-1WithRSAEncryption {1，2，840，113549，1，1，5})
Issuer		
	countryName	(UK)
	localityName	(London)
	organizationName	(Dept. of Health)
	organizationalUnit	(National Health Service)
	commonName	(Patient Certificate v1)
	serialNumber	{serialNumber of the issuer})
Validity		(validity period coded as UTCTime： not before 010801000000z not after 060801000000z)
Subject		
	countryName	(UK)
	localityName	(London)
	organizationName	(NHS)
	organizationalUnit	(Patient Registration)
	commonName	(Smith， Bill)
	surName	(Smith)
	givenName	(William)
	e-mail	(bSmith@uknet.com)
subjectPublicKeyInfo		
	algorithm	(public RSA key， 1024 bit {1，2，840，113549，1，1，1})
	subjectPublicKey	(Subject's PUBLIC KEY)
Extensions		
authorityKeyIdentifier		(unique identifier of CA public key)
subjectKeyIdentifier		(unique identifier of subject public key)
keyUsage		(digitalSignature)
certificatePolicies		
policyIdentifier		OBJECT IDENTIFIER ：：= *Policy-OID-for-Patient-Certificate-v1*
	cRLDistributionPoints	(http：//crl.location.nhs.uk)
authorityInformationAccess		(http：ocspserver.nhs.uk/OCSP_SERVER：5555)
subjectDirectoryAttributes		

hcRole OBJECT IDENTIFIER ：： = *id-hcpki-at-healthcareactor*
hcActorData SET OF {
codedData CodedData ：： = {
codingSchemeReference OBJECT IDENTIFIER ：： = *id-hcpki*，
codeDataValue UTF8String ：： = *the-code-for-patient*，
codeDataFreeText DirectoryString ：： = *optional-data }*
regionalHCData Sequence of RegionalData ：： = {
type OBJECT IDENTIFIER ：： = OID-for-this-regional-encoding，
country PrintableString (SIZE (2) ：： = ISO-country-code-for-UK，
issuingAuthority DirectoryString ：： = (c=UK， National Health Service，
ou=patients)，
hcMajorClassCode CodedData ：： = {
codingSchemeReference OBJECT IDENTIFIER ：： =
Coding-Scheme-for-Type-OID，
codeDataValue UTF8String ：： = Type-OID-for-patient，
codeDataFreeText UTF8String ：： = “patient ID 368964278”}} }

A.3 示例 2：非正规健康专业人员证书轮廓

注：以下示例仅仅是说明性的，并不试图声明加利福尼亚州将来发行健康证书所采用的格式。

Bill Smith为被认可的医疗打字员（Certified Medical Transcriptionist，CMT）。CMT由医疗打字员美国协会发行。

Version		(2 – decimal code for version 3 certificates)
SerialNumber		(unique CA generated decimal number)
Signature		(sha-1WithRSAEncryption {1，2，840，113549，1，1，5})
Issuer		
	countryName	(US)
	localityName	(California)
	organizationName	(Name-of-CA-for-California-Health-Care)
	commonName	(Name-of-CA-for-California-Health-Care)
Validity		(validity period coded as UTCTime)
Subject		
	countryName	(US)
	localityName	(California)
	organizationName	(CertHolderOrganization)
	commonName	(Smith， Betty)
	surname	(Smith)
	givenName	(Betty)
subjectPublicKeyInfo		
	algorithm	(public RSA key， 1024 bit {1，2，840，113549，1，1，1})
	subjectPublicKey	(Subject’s PUBLIC KEY)
Extensions		
authorityKeyIdentifier		(unique identifier of CA public key)
subjectKeyIdentifier		(unique identifier of subject public key)

keyUsage (digitalSignature or non-repudiation or keyEncipherment)
certificatePolicies (appropriate policy OID)
cRLDistributionPoints (CRL X.500 entry location)
subjectDirectoryAttributes
(**hcRole** OBJECT IDENTIFIER ：： = id-hcpki-at-healthcareactor
hcActorData SET OF {
codedData CodedData ：： = {
codingSchemeReference OBJECT IDENTIFIER ：： = *id-hcpki*，
地点名称 (加利福尼亚)
组织名称 (证书持有者组织)
通用名称 (Smith， Betty)
姓 (Smith)
名 (Betty)
主体公钥信息
算法 (公共 RSA 密钥，1024 位{1，2，840，113549，1，1，1})
主体公钥 (主体公钥)
扩展
机构公钥标识符 (CA 公钥唯一标识符)
主体公钥标识符 (主体公钥唯一标识符)
公钥使用 (数字签名或防抵赖或密钥加密术)
证书策略 (适当策略的 OID)
cRL 分布指针 (CRL X.500 入口地址)
主体目录属性
codeDataValue UTF8String ：： = *the-code-for-transcriptionist-role*，
codeDataFreeText DirectoryString ：： = *optional-data}*
regionalHCData Sequence of RegionalData ：： = {
type OBJECT IDENTIFIER ：： = OID-for-this-regional-encoding，
country PrintableString (SIZE (2) ：： = ISO-country-code-for-USA，
issuingAuthority DirectoryString ：： = (C=US，
OU= American Association of Medical Transcriptionists)，
nameAsIssued DirectoryString ：： = (CN= Elizabeth Smith)
hcMajorClassCode CodedData ：： = {
codingSchemeReference OBJECT IDENTIFIER ：： = ASTM-Coding-Scheme-for-Type，
codeDataValue UTF8String ：： = ASTM-Type-OID-for-transcriptionist}
codeDataFreeText UTF8String ：： = “license number 1234567”} })

A.4 示例 3：正规健康专业人员证书轮廓

注：以下示例仅仅是说明性的，并不试图声明加利福尼亚州将来发行健康证书所采用的格式。.

John Stuart Woolley aka Tink Woolley的执照由加利福尼亚州医疗执照委员会颁发，执照编号20A4073，执照状态码 17（“01”为“活动和现行），发行日期为2000年3月22日， 截止日期为 2002年3月21日。

Version (2 – decimal code for version 3 certificates)

SerialNumber (unique number)
Signature (sha-1WithRSAEncryption {1，2，840，113549，1，1，5})
Issuer
countryName (US=United States of America)
localityName (California)
organizationName (Name-of-CA-for-California-Health-Care)
commonName (Name-of-CA-for-California-Health-Care)
Validity (validity period coded as UTCTime)
Subject
countryName (US=United States of America)
localityName (California)
organizationName (CertHolderOrganization)
commonName (Woolley， Tink)
surname (Woolley)
givenName (John Stuart)
subjectPublicKeyInfo
algorithm (public RSA key， 1024 bit {1，2，840，113549，1，1，1})
subjectPublicKey (Subject's PUBLIC KEY)
Extensions
authorityKeyIdentifier (unique identifier of CA public key)
subjectKeyIdentifier (unique identifier of subject public key)
keyUsage (digitalSignature or non-repudiation or keyEncipherment)
certificatePolicies (appropriate policy OID)
cRLDistributionPoints (CRL X.500 entry location)
subjectDirectoryAttributes
(**hcRole** OBJECT IDENTIFIER :: = id-hcpki-at-healthcareactor
hcActorData SET OF {
codedData CodedData :: = {
codingSchemeReference OBJECT IDENTIFIER :: = *id-hcpki*，
codeDataValue UTF8String :: = *the-code-for-physician-role*，
codeDataFreeText DirectoryString :: = *optional-data}*
regionalHCData Sequence of RegionalData :: = {
type OBJECT IDENTIFIER :: = OID-for-this-regional-encoding，
country PrintableString (SIZE (2) :: = ISO-country-code-for-USA，
issuingAuthority DirectoryString :: = (C=US， L=CA， OU=California Medical License Board)，
nameAsIssued DirectoryString :: = (CN= John Stuart Woolley)
hcMajorClassCode CodedData :: = {
codingSchemeReference OBJECT IDENTIFIER :: =
ASTM-Coding-Scheme-for-Type-OID，
codeDataValue UTF8String :: = ASTM-Type-OID-for-physician}
codeDataFreeText UTF8String :: = "license number 20A4073"}
hcMinorClassCode CodedData :: = {
codingSchemeReference OBJECT IDENTIFIER :: =

ASTM-Coding-Scheme-for-License-Status-OID，

codeDataValue UTF8String ：：= "*unrestricted*"，

codeDataFreeText UTF8String ：：= “unrestricted”} }）

在上述示例中，应注意的是执照编号和执照状态属区域性的数据。对这种区域性数据可选择使用，是否纳入这种数据须留待CA发行时再行决定。

A.5 示例 4：受托医疗保健提供方证书轮廓

注：以下示例仅仅是说明性的，并不试图声明加利福尼亚州将来发行健康证书所采用的格式。

Julie LeClerk为安大略省的助产士。

Version (2 – decimal code for version 3 certificates)
SerialNumber (unique number)
Signature (sha-1WithRSAEncryption {1，2，840，113549，1，1，5})
Issuer
countryName (CA=Canada)
localityName (Ontario)
organizationName (Name-of-CA-for-Ontario-Health-Care)
commonName (Name-of-CA-for-Ontario-Health-Care)
Validity (validity period coded as UTCTime)
Subject
countryName (CA=Canada)
localityName (Ontario)
organizationName (CertHolderOrganization)
commonName (LeClerk， Julie)
surname (LeClerk)
givenName (Julie)
subjectPublicKeyInfo
algorithm (public RSA key， 1024 bit {1，2，840，113549，1，1，1})
subjectPublicKey (Subject’s PUBLIC KEY)
Extensions
authorityKeyIdentifier (unique identifier of CA public key)
subjectKeyIdentifier (unique identifier of subject public key)
keyUsage (digitalSignature or non-repudiation or keyEncipherment)
certificatePolicies (appropriate policy OID)
cRLDistributionPoints (CRL X.500 entry location)
subjectDirectoryAttributes
(**hcRole** OBJECT IDENTIFIER ：：= id-hcpki-at-healthcareactor
hcActorData SET OF {
codedData CodedData ：：= {
codingSchemeReference OBJECT IDENTIFIER ：：= *id-hcpki*，
codeDataValue UTF8String ：：= *the-code-for-midwife-role*，
codeDataFreeText DirectoryString ：：= *optional-data}*
regionalHCData Sequence of RegionalData ：：= {
type OBJECT IDENTIFIER ：：= OID-for-this-regional-encoding，

country PrintableString (SIZE (2) ：：= ISO-country-code-for-Canada，

issuingAuthority DirectoryString ：：= (C=CA， OU= Name-of-CA-for-Ontario-Health-Care)，

hcMajorClassCode CodedData ：：={

codingSchemeReference OBJECT IDENTIFIER ：：= *ISO-Role-Coding-Scheme*，

codeDataValue UTF8String ：：= *the-code-for-midwife-role* }

codeDataFreeText UTF8String ：：= “*optional printable data*”}})

A.6 示例5：支持组织雇员证书轮廓

注：以下示例仅仅是说明性的，并不试图声明加利福尼亚州将来发行健康证书所采用的格式。

Sally R Jones为帐目管理员，受雇于美国健康系统。

Version	(2 – decimal code for version 3 certificates)	
SerialNumber	(unique number)	
Signature	(sha-1WithRSAEncryption {1,2,840,113549,1,1,5})	
Issuer		
	countryName	(US=United States of America)
	localityName	(California)
	organizationName	(Name-of-CA-for-California-Health-Care)
	commonName	(Name-of-CA-for-California-Health-Care)
Validity		(validity period coded as UTCTime)
Subject		
	countryName	(US=United States of America)
	localityName	(California)
	organizationName	(American Health Systems)
	commonName	(Jones， Sally R.)
	surname	(Jones)
	givenName	(Sally R.)
subjectPublicKeyInfo		
	algorithm	(public RSA key， 1024 bit {1，2，840，113549，1，1，1})
	subjectPublicKey	(Subject’s PUBLIC KEY)
Extensions		
authorityKeyIdentifier		(unique identifier of CA public key)
subjectKeyIdentifier		(unique identifier of subject public key)
keyUsage		(digitalSignature or non-repudiation or keyEncipherment)
certificatePolicies		(appropriate policy OID)
cRLDistributionPoints		(CRL X.500 entry location)
subjectDirectoryAttributes		

(**hcRole** OBJECT IDENTIFIER ：：= id-hcpki-at-healthcareactor

hcActorData SET OF {

codedData CodedData ：：={

codingSchemeReference OBJECT IDENTIFIER ：：= *id-hcpki*，

codeDataValue UTF8String ：：= *the-code-for-file-clerk-role*，

codeDataFreeText DirectoryString ：：= CN=Sally R. Jones*}*

regionalHCData Sequence of RegionalData ::= {
type OBJECT IDENTIFIER ::= OID-for-this-regional-encoding，
country PrintableString (SIZE (2) ::= ISO-country-code-for-USA，
issuingAuthority DirectoryString ::= (C=US， OU= American Health Systems)，
hcMajorClassCode CodedData ::= {
codingSchemeReference OBJECT IDENTIFIER ::= ASTM-Coding-Scheme-for-Type，
codeDataValue UTF8String ::= ASTM-Type-OID-for-file-clerk} } })

应注意到，本示例不同于示例3（正规健康专业人员），它没有执照编号和执照状态编码。这是允许的，因为对这种区域性数据可选择使用，是否纳入这种数据须留待CA发行时再行决定。

A.7 示例 6：组织证书轮廓

注：以下示例仅仅是说明性的，并不试图声明加利福尼亚州将来发行健康组织证书所采用的格式。

Version		(2 – decimal code for version 3 certificates)
SerialNumber		(unique number)
Signature		(sha-1WithRSAEncryption {1，2，840，113549，1，1，5})
Issuer		
	countryName	(US=United States of America)
	localityName	(California)
	organizationName	(California Hospital Authority)
	commonName	(Health Digital Certificate policy v01)
Validity		(validity period coded as UTCTime)
Subject		
	countryName	(US = United States of America)
	localityName	(Region = California)
	organizationName	(Midtown Hospital)
subjectPublicKeyInfo		
	algorithm	(public RSA key， 1024 bit {1，2，840，113549，1，1，1})
	subjectPublicKey	(Subject’s PUBLIC KEY)
Extensions		
authorityKeyIdentifier		(unique identifier of CA public key)
subjectKeyIdentifier		(unique identifier of subject public key)
keyUsage		(digitalSignature or non-repudiation or keyEncipherment)
certificatePolicies		(appropriate policy OID)
cRLDistributionPoints		(CRL X.500 entry location)

A.8 示例 7：AC 轮廓

注：以下示例仅仅是说明性的，并不试图声明加利福尼亚州将来发行健康证书所采用的格式。

Version	(3)
SerialNumber	(unique number)
Signature	(sha-1WithRSAEncryption {1，2，840，113549，1，1，5})
baseCertificateID	339393322281
entityName	Dr Benjamin Casey

Optional		
AttCertValidity		Period
Attributes		Surgeryrecordaccess，
Issuer		
	countryName	(US= United States of America)
	localityName	(California)
	organizationName	(California Hospital Authority)
	commonName	(CA - / policy v01)
Validity		(validity period coded as UTCTime)
Subject		
	countryName	(US= United States of America)
	localityName	(Region = California)
	organizationName	(Midtown Hospital)
	commonName	(Midtown Secure Server 01)
subjectPublicKeyInfo		
	algorithm	(public RSA key， 1024 bit {1，2，840，113549，1，1，1})
	subjectPublicKey	(Subject’s PUBLIC KEY)
Extensions		
authorityKeyIdentifier		(unique identifier of CA public key)
subjectKeyIdentifier		(unique identifier of subject public key)
keyUsage		(digitalSignature or non-repudiation or keyEncipherment)
certificatePolicies		(appropriate policy OID)
cRLDistributionPoints		(CRL X.500 entry location)

A.9 示例 8：CA 证书轮廓

注：以下示例仅仅是说明性的，并不试图声明加利福尼亚州将来发行健康证书所采用的格式。

Version	(2 – decimal code for version 3 certificates)	
SerialNumber	(unique number)	
Signature	(sha-1WithRSAEncryption {1，2，840，113549，1，1，5})	
Issuer		
	countryName	(US=United States of America)
	localityName	(Ex. Region California)
	organizationName	(Ex. California Hospitals Authority)
	commonName	(Ex. CA – Health PKI US-CT/ policy v01)
Validity		(validity period coded as UTCTime)
Subject		
	countryName	(US=United States of America)
	localityName	(Ex. Region California)
	organizationName	(Ex. El Cerrito Health Authority)
	commonName	(Ex. CalifHA PKI US CT/ policy V.03)
subjectPublicKeyInfo		
	algorithm	(public RSA key， 1024 bit {1，2，840，113549，1，1，1})
	subjectPublicKey	(Subject’s PUBLIC KEY)

Extensions	
authorityKeyIdentifier	(unique identifier of CA public key)
subjectKeyIdentifier	(unique identifier of subject public key)
keyUsage	(CRL and certificate signing)
certificatePolicies	(appropriate policy OID)
basicConstraints	(CA = true)
cRLDistributionPoints	(CRL X.500 entry location)

A.10 示例 9：桥接证书轮廓

注：以下示例仅仅是说明性的，并不试图声明加利福尼亚州将来发行健康证书所采用的格式。

Version	(2 – decimal code for version 3 certificates)
SerialNumber	(unique number)
Signature	(sha-1WithRSAEncryption {1，2，840，113549，1，1，5})
Issuer	
countryName	(US=United States of America)
localityName	(Region California)
organizationName	(California Hospitals Authority)
commonName	(CA – Health PKI US-CT/ policy v01)
Validity	(validity period coded as UTCTime)
Subject	
countryName	(US=United States of America)
localityName	(Region Washington)
organizationName	(Washington Health Authority)
commonName	(CalifHA PKI US CT/ policy V.03)
subjectPublicKeyInfo	
algorithm	(public RSA key， 1024 bit {1，2，840，113549，1，1，1})
subjectPublicKey	(Subject’s PUBLIC KEY)
Extensions	
authorityKeyIdentifier	(unique identifier of CA public key)
subjectKeyIdentifier	(unique identifier of subject public key)
keyUsage	(CRL and certificate signing)
certificatePolicies	(appropriate policy OID)
basicConstraints	(CA = true)
cRLDistributionPoints	(CRL X.500 entry location)

参 考 文 献

[1] ISO/IEC 2382, Information technology — Vocabulary

[2] ISO 7498 2, Information processing systems — Open Systems Interconnection — Basic Reference Model— Part 2: Security Architecture

[3] ISO/IEC 8824 1, Information technology — Abstract Syntax Notation One (ASN.1) — Part 1: Specification of basic notation

[4] ISO/IEC 9594 8, Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks
[5] ISO/IEC 10181 1, Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview
[6] ISO/IEC TR 14516, Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services
[7] ISO/IEC 15945, Information technology — Security techniques — Specification of TTP services to support the application of digital signatures
[8] IETF/RFC 2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols
[9] IETF/RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[10] IETF/RFC 3739, Internet X.509 Public Key Infrastructure Qualified Certificates Profile
[11] U.S. government standard FIPS-140-2, level 1 and level 2
[12] ENV 13608 1, Health informatics — Security for healthcare communication — Concepts and terminology
[13] ANKNEY, R., CertCo. Privilege Management Infrastructure, v0.4, August 24, 1999
[14] APEC Telecommunications Working Group, Business Facilitation Steering Group Electronic Authentication Task Group PKI Interoperability Expert Group, Achieving PKI Interoperability, September 1999
[15] BERND, B. and ROGER-FRANCE, F., A Systemic Approach for Secure Health Information Systems, International Journal of Medical Informatics, pp. 51 78, 2001
[16] CANADIAN INSTITUTE FOR HEALTH INFORMATION. Model Digital Signature and Confidentiality Certificate Policies, June 30, 2001
[17] Drummond Group, The Healthkey Program, PKI in Healthcare: Recommendations and Guidelines for Community-Based Testing, May 2000
[18] EESSI (European Electronic Signature Standardization Initiative), Final Report of the EESSI Expert Team 20th July 1999
[19] FEGHHI, J. and WILLIAMS, P., Digital Certificates — Applied Internet Security, Addison-Wesley, 1998
[20] Government of Canada. Criteria for Cross Certification, 2000
[21] KLEIN, G., LINDSTROM, V., NORR, A., RIBBEGARD, G. and TORLOF, P., Technical Aspects of PKI, January 2000
[22] KLEIN, G., LINDSTROM, V., NORR, A., RIBBEGARD, G., SONNERGREN, E. and TORLOF, P., Infrastructure for Trust in Health Informatics, January 2000
[23] SAA MP75 (Standards Australia), Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia, 1996
[24] WILSON S. Audit Based Public Key Infrastructure, Price Waterhouse Coopers White Paper, November 2000