



中华人民共和国国家标准化指导性技术文件

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

Health informatics—Public Key Infrastructure (PKI)—
Part 2: Certificate profile

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

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 2 部分:证书轮廓
GB/Z 21716.2—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

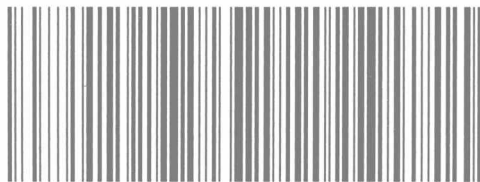
*

开本 880×1230 1/16 印张 2.25 字数 59 千字
2008 年 7 月第一版 2008 年 7 月第一次印刷

*

书号: 155066 · 1-32096 定价 26.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533



GB/Z 21716.2—2008

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 2 部分。

本部分参照 ISO 17090-2(DIS)《健康信息学 公钥基础设施(PKI) 第 2 部分:证书轮廓》制定,其主要技术内容与 ISO 17090-2(DIS)一致。相对原文而言,本部分仅进行了少量修改,包括:

- 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。

本部分主要起草人:董连续、任冠华、陈煌、刘碧松。

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 2 部分:证书轮廓

1 范围

本部分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。本部分还详述了公钥基础设施(PKI)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。

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 21716.1—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 21716.3—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
IETF/RFC 3280 Internet X.509 公钥基础设施证书和 CRL 轮廓
IETF/RFC 3281 针对机构的因特网属性证书轮廓
IETF/RFC 3739 Internet X.509 公钥基础设施合格证书轮廓

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
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	证书撤销列表	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、受托医疗保健提供者、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。

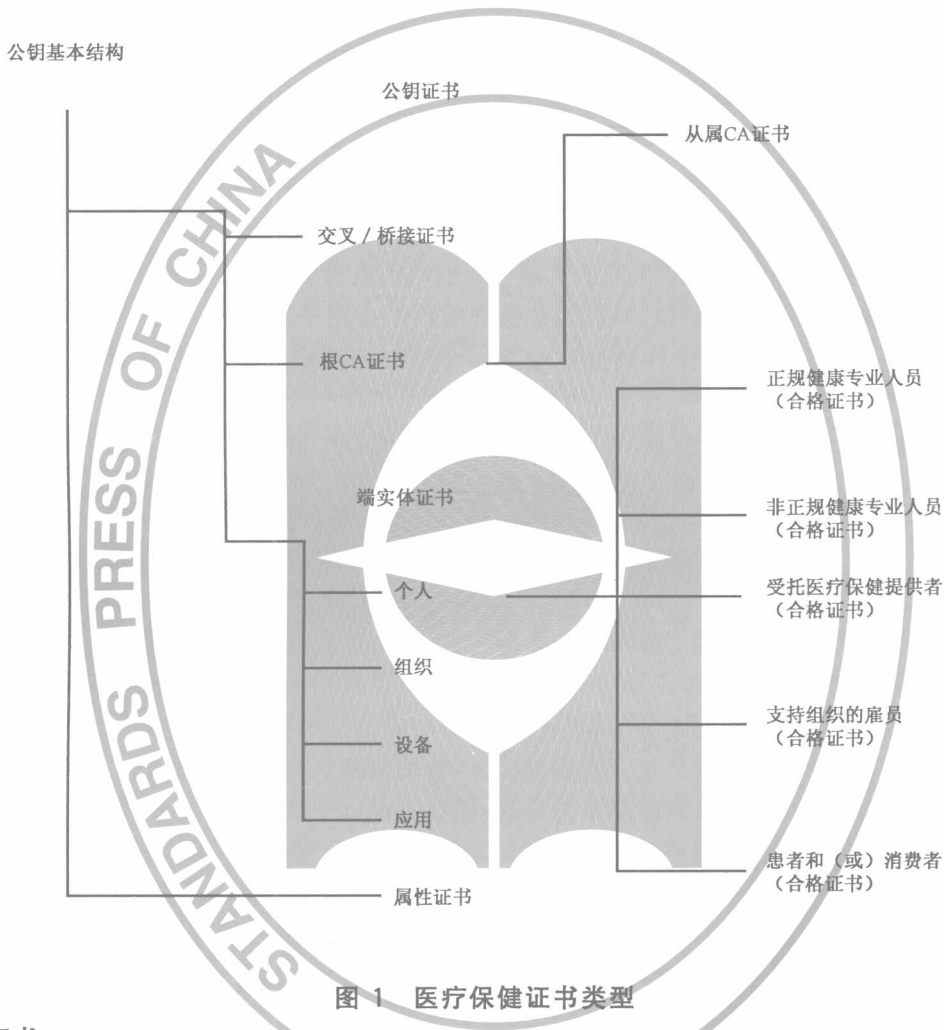


图 1 医疗保健证书类型

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。根证书被自我签名,并用于医疗保健 PKI 发行证书给包括从属 CA 在内的依赖方。基本约束域指示一个证书是否是 CA。

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。

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他需求。

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。他们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作为其个人。

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 2527 的要求,在本部分中对组织单元的名称进行了规定。

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。

本部分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 3281(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。

IETF/RFC 3281 对 AC 语法进行了规定。

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 issuer 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)字段传递时间周期。在此周期内 AC 是有效的, 并以 GeneralizedTime 格式表示。

此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)可用来标识 AC 的发行方, 而用发行方的名称进行标识是不充分的。

扩展字段允许为 AC 附加新的字段。

GB/Z 21716.1 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 AC 可以包含对另一个具有附加特权 AC 的引用, 从而提供了实现特权角色的有效机制。

很多具有授权需求的环境要求采用针对某些操作特征的基于角色的特权(典型情况是有关基于标识的特权)。这样申请方可以向验证方提交证明申请方特定角色的证据(例如, “管理者”或“购买者”)。据此, 验证方也可以辨别出其优先程度或必须通过其他手段来发现的有关的声明角色, 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 3280 相一致。仅在与有关 IETF/RFC 3280 的已知问题建议方案相结合的情况下,方允许偏离 IETF/RFC 3280。
- c) 在个人标识方面,证书应符合 IETF/RFC 3739。仅在与已知问题建议方案相结合的情况下,方允许偏离 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/Z 21716.3 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 所标识的所有健康数字证书中的通用要素。这些要素是通用性的,使用它们可以构成不同种类的证书。

```

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)是指时间间隔,在此段时间内,CA 授权包含在证书内的信息是有效的。对于正规健康专业人员来说,CA 应保证证书的有效期限不超过其专业执照的有效期限。为了达到这一目标,CA 应该规定证书的有效性不超过专业执照的周期,或者先于专业执照终止日期可靠确定执照的更新,如果专业执照未被更新,则取消或终止证书。

关于时间格式的注释:

可识别编码规则(DER)允许格式化 UTC 时间和 Generalized 时间的几种方法。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。在年份大于或等于 2050 的情况下,应使用 Generalized 时间进行编码。为了保证对 UTC 时间编码进行一致地格式化,应使用“Z”格式对 UTC 时间进行编码,且不要忽略第二个字段,即使是“00”(即,格式应该是 YYMMDDHHMMSSZ)。在此种编码中,当 YY 大于或等于 50 时,则认为年字段 YY 等于 19YY;当 YY 小于 50 时,则认为 YY 等于 20YY。在采用 Generalized 时间时,应以“Z”格式对 UTC 时间进行编码,并应包括第二个字段(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。(IETF/RFC 3280 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 IETF/RFC 3280 的规定,建议不使用该字段)。

i) extensions(扩展)应表示一个或多个扩展的 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 3280 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 (1.2.840.10045.4.1);
- 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) sha256WithRSAEncryption 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。

6.3.3 有效性

有效日期应符合 IETF/RFC 3280 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)表示一个确切的时间,从那时起 CA 将维护和出版关于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/Z 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

存储于发行方名称字段的发行方名称应采用以下规定的修正和约束,与符合对象类别 Organizational Role(组织角色)的适当 ISO 名称结构相一致,位于一个组织或一个组织单元后面。

6.4 条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。

示例:国家名称=“CN”

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。

b) 地点名称:地点名称(localityName)用来至少存储一个地点名称数据。本规范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。

示例: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。即使能够正确地知晓证书的发行方和证书的用途,它所表示的名称也应该是提示性的。在通用名称字段值内包括管理证书策略的名称属进一步的要求。这是对使用 OID 策略的附加引用。

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采用以下定义的修正和约束,与符合对象类别 Organizational Role(组织角色)的适当 ISO 名称结构相一致,位于一个组织或一个组织单元后面。

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。

6.4 条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)用来至少存储一个地点名称数据。顶层为国家的两层地点名称被规定。其后是地理地点名称值。顶层要求列入由地理地点名称值随后的国家。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

IETF/RFC 3280 不赞成,但也允许在支持遗留实现的主体的可区分名中同时存在的电子邮件地址的属性。本指导性技术文件建议在主体名称字段不使用该电子邮件,而放在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。

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 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
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
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
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
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
^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。								

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	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	可选的
组织名称	必备的	必备的	可选的	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	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	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	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	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	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元素。										
^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 引言

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 3280 和 IETF/RFC 3739。

7.2 一般扩展

7.2.1 机构密钥标识符

此扩展应对用于验证证书签名的公钥进行标识。它使得区分由一个 CA 使用的独特的密钥可行(例如,当密钥更新发生时)。

仅使用 authorityKeyIdentifier(机构密钥标识符)扩展(字段)的密钥标识符。

这并不是严格的扩展。但如果使用,建议扩展应是必备的配置。

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 3280 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(digital-Signature)密钥的使用混合(见 6.1)。

此扩展是必备的。建议(按 IETF/RFC 3280 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为支持主体可区别名。

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 证书撤销列表分布点

IETF/RFC 3280 建议通过 CA 和应用支持 CRLDistributionPoints(证书撤销列表分布点)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 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、账单编号和患者标识符。见下述局部数据(REGIONAL-DATA)。

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

本指导性技术文件给定如下值:

```
{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,