ICS 35.240.80
C 07

中华人民共和国国家标准化指导性技术文件

GB/Z 21716.3—2008

健康信息学　公钥基础设施(PKI)
第3部分:认证机构的策略管理

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

2008-04-11 发布

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

标准网
biaozhun.org

目　次

前　言

GB/Z 21716《健康信息学　公钥基础设施(PKI)》分为3个部分：

——第1部分：数字证书服务综述；

——第2部分：证书轮廓；

——第3部分：认证机构的策略管理。

本部分为GB/Z 21716的第3部分。

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

本部分由中国标准化研究院提出。

本部分由中国标准化研究院归口。

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

本部分主要起草人：陈煌、任冠华、董连续、刘碧松、尹岭、韵力宇。

引　言

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

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

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

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

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

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

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

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

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

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

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

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

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

健康信息学　公钥基础设施(PKI)
第3部分:认证机构的策略管理

1　范围

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

2　规范性引用文件

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

GB/T 19716—2005　信息技术　信息安全管理实用规则

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

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

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

3　术语和定义

GB/Z 21716.1给出的术语和定义适用于本部分。

4　缩略语

下列缩略语适用于本部分。

AA　属性机构　attribute authority

CA　认证机构　certification authority

CP　证书策略　certificate policy

CPS　认证操作声明　certification practice statement

CRL　证书撤销列表　certificate revocation list

OID　对象标识符　object identifier

PKC　公钥证书　public key certificate

PKI　公钥基础设施　public key infrastructure

RA　注册机构　registration authority

TTP　可信第三方　trusted third party

5　在医疗保健语境中数字证书策略管理的要求

5.1　概述

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

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

b) 对于参与进行个人健康信息的电子交换过程中所有人员、机构、应用软件、设备等，必须有专业角色安全可靠地与之绑定。做这种绑定是为实现对这些健康信息进行基于角色的访问控制打下基础。

c) （可选的）对于参与进行个人健康信息的电子交换过程中所有人员、机构、应用软件、设备等，应有相应的属性安全可靠地与之绑定。做这种绑定是为了进一步保障健康信息的安全通信。

完成上述目标是为了保证个人健康信息的完整性和保密性，并达到信任的使用数字证书来安全地进行通信的目的。

为此，每个发行用于医疗保健方面数字证书的CA应该为之提出一套促进实现上述目标的公开策略，并按照这个声明策略进行操作。

5.2 高层的保证要求

用于健康应用软件所需的安全服务在GB/Z 21716.1—2008中第6章有相关规定。对于其中每个安全服务（鉴别、完整性、机密性、数字签名、授权、访问控制等），需要有一个高层的保证。

5.3 基础设施可用性的高层要求

急诊服务是一个全天候的任务，要求具有能不受正常工作时间限制地随时进行证书获取、证书撤销、验证撤销状态等能力。与电子商务不同，医疗保健对任何电子证书都提出了高可用性要求，这样才能确保个人健康信息通信的安全性。

5.4 高层的信任要求

与电子商务不同（此时买方和消费者常常是电子交换中仅有的参与方，以及由此产生安全性和完整性），存储或传输个人健康信息的医疗保健应用在交换患者的信息时还要求经过患者（包括普通公众）的授信。如果大家认为个人健康信息的电子交换是不安全的，则医疗保健提供者或者患者都不会在此方面提供合作。

5.5 互联网兼容性的要求

本部分的目的之一是定义医疗保健数字证书的基本元素以支持跨国家和区域界限安全传输医疗保健信息，它基于众多的互联网标准以便有效的跨越这些边界。

5.6 便于评估和比较CP的要求

GB/Z 21716.1—2008的9.2中描述了使用数字证书来促进健康信息跨国的安全交换的相关步骤。如果医疗保健CP遵循统一的格式，则可以对不同来源的CP进行比较，这样就更进一步促进了上述步骤（如交叉识别和交叉认证）。

医疗保健CP是形成对CA信任的基础之一（受信任的CA支持一个或多个CP得到实施）。当信任标准超出本指导性技术文件的范围时，对医疗保健CA的信任的整个过程将通过格式一致性和本指导性技术文件所提出的最低标准而得到加速。

6 医疗保健CP和CPS的结构

6.1 CP的一般要求

当一个CA签发了一个证书时，它给了可依赖方一个声明表示已经给专门的证书持有者绑定了一个专门的公共密钥。不同的证书在签发时经历了不同的操作和程序，并适用于不同的应用产品和/或目的。

CA应负责对证书的签发、管理的各个方面，包括对注册过程的控制、证书中信息的确认以及对证书的制作、发放、撤销、暂停和更新等。CA还应负责确保CA服务和执行操作的各个方面都与对应CP的需求、表示、被担保人以及CA的CPS一致。

签发用于医疗保健的电子证书的CA在他们所提供服务方面应有相应的政策和程序。这些政策和程序应包括：

a) 在证书签发前注册潜在的证书持有者，包括符合 GB/Z 21716.2—2008 第 6 章的证书持有者角色；

b) 在证书签发前鉴别潜在证书持有者的身份；

c) 证书签发出去后，对证书的持有者的个人信息保密；

d) 把证书分发给证书持有者和有关名录；

e) 接受关于可能出现的私有密钥协议的信息；

f) 发布证书撤销列表(发布的频率，如何以及何地发布)；

g) 其他的密钥管理问题，包括密钥长度、密钥产生过程、证书的预期使用期限、重设密钥等；

h) 与其他 CA 的交叉证明；

i) 安全控制和审计。

为了实现这些功能，本基础设施中各 CA 都需要提供为其证书持有者和可依赖方提供一些基础服务。这些 CA 服务要在其 CP 中列出。

数字证书包含一个或多个经过注册的 CP OID，它标识了证书在签发时所遵循的 CP，并可用于判断一个用于特定目标的证书是否可信。其中注册过程遵循相关 ISO/IEC 和 ITU 标准所规定的程序。注册 OID 的一方也需要发布 CP 供证书持有者和可依赖方进行检验。

因为在 PKC 中建立信任时 CP 的重要性，所以 CP 不仅能被证书持有者也能被可依赖方所理解和参考是基本的要求。因此，证书持有者和可依赖方在证书签发后应能完全而可靠的访问到其 CP。

符合本部分规定的所有 CP 应满足下列需求：

a) 每个符合本部分规定的电子证书签发时，应至少包含一个经注册的 CP OID，它标识了证书在签发时所遵循的 CP；

b) CP 的结构应符合 IETF/RFC 3647；

c) CP 应能被证书持有者和可依赖方访问到。

虽然 CP 和 CPS 文档的本质是描述和控制 CP 及其实施，但是许多数字证书持有者特别是消费者发现这些文档难以理解。这些证书持有者和其他可依赖方可以通过从访问 CP 元素的简要声明中受益，其中用于此目的所需的重点、公示和 PKI 公示声明模型在本部分的第 8 章给出。

6.2 CPS 的一般要求

CPS 是对准确实施所提供的服务、证书生命周期管理详细过程等细节的完整描述，它一般比相关的 CP 要详细得多。

符合本部分规定的所有 CPS 应满足下列需求：

a) CPS 应符合 IETF/RFC 3647；

b) 拥有单个 CPS 的 CA 可以支持多个 CP(用于不同的应用目的和/或被不同团体的可依赖方使用)；

c) 所带 CPS 不完全相同的 CA 可以支持相同的 CP；

d) 一个 CA 可以选择让其 CPS 对证书持有者或可依赖方是不可访问的，或者选择让其 CPS 只是部分可访问。

6.3 CP 和 CPS 间的关系

CP 声明了在一个证书中放置了何种担保(包括证书使用上的限制以及可靠性的限制范围等)。CPS 声明了 CA 是如何建立该担保的。CP 可广泛应用到不止一个机构上，而 CPS 只能应用于单个 CA。CP 作为一种媒介提供服务，它形成了普通互操作标准和普通行业范围(或者可能是全球范围)担保标准的基础。但单个具体的 CP 不能单独形成不同 CA 间互操作性的基础。

6.4 适用性

本部分适用于 CP 和 CPS 用在 GB/Z 21716.2—2008 第 4 章所规范的签发医疗保健证书的方面。

7 医疗保健CP的最小要求

7.1 一般要求

符合本部分规范的CP应满足本章中的以下所有要求。本章中各条标题下括号中的数字对应的是IETF/RFC 3647中的章条号。

7.2 发布和存储责任

7.2.1 存储库

(2.1)

保留在RA或CA存储库中关于证书持有者的信息应是：

a) 保持当前日期并更新日期(变化被验证的一天之内甚至更早，根据具体情况而定)；

b) 按照GB/T 19716—2005的规范，或经认可的授权，或执照许可规范进行管理。

7.2.2 证书信息的发布

(2.2)

所有发布用于卫生领域电子证书的CA应让他们的证书持有者和可依赖方获得下列内容：

a) 代表该CA或由该CA维护的有效网址的URL，且该网址包含着该CA的证书策略；

b) 按照其证书策略来签发或更新每个证书；

c) 在该策略下每个证书的当前状态；

d) CA进行合格认定或发布许可时所遵循的准则，其中这些认定或许可应用在不同的权限中。

被CA授权的代表电子签名的CP文件的电子拷贝应可由下列情况获得：

a) 放在所有可依赖方都可访问的网址上，或者

b) 通过电子邮件请求得到。

由于CPS详细描述了一个CA服务和密钥生命周期管理程序的具体实施，而且比CP更详细，因此它所包含的信息应保持更高的保密性以保证CA的安全。

7.2.3 发布的频率

(2.3)

每当信息被修改后，CA就应发布信息。

7.2.4 对存储库的访问控制

(2.4)

已发布的信息(如政策、实践、证书)以及这些证书的当前状态应是只读的。

7.3 标识和鉴别

7.3.1 初始注册

7.3.1.1 名称类型

(3.1.1)

用于在该策略下所发布证书的主题名称应符合GB/Z 21716.2。

7.3.1.2 名称应有含义

(3.1.2)

证书的有效使用需要有相关的特定名称显示在证书上且能被可依赖方所理解和使用。这些证书中所使用的名称应能标识出证书持有者以便他们能以有含义的方式被分配，见7.3.1.3。

对于证书持有者是正规健康专业人员、非正规健康专业人员、受委托医疗保健提供者、支持组织雇员或患者/消费者的情况，其名称应符合7.3.2所鉴别的名称。

7.3.1.3 匿名或假名

(3.1.3)

名称应有含义的要求(见7.3.1.2)，并不排除在发给患者/消费者的证书中使用假名。

7.3.1.4 对各种名称形式进行解释的规则

(3.1.4)

CP 应有一个可对名称进行申请、辩论、决议的程序，以及应有一个协定以便能对当发起名称申请辩论时所用的名称形式进行解释。

7.3.1.5 名称的唯一性

(3.1.5)

证书中列出的主体识别名对于 CA 的不同证书持有者都应是无歧义的和唯一的。

如有必要，在识别名中(如 IETF RFC 3280 所述)包含识别名属性“序列号”可以用来保障唯一性。如有可能，建议该序列号是有含义的(如正规健康专业人员的执照号)。参见本部分的 7.3.1.2。

7.3.1.6 商标的识别、鉴别和角色

(3.1.6)

CA 不应在明知商标不属于证书的主题范围的情况下发布包含该商标的证书。

7.3.2 初始身份确认

7.3.2.1 私钥拥有权的证明方法

(3.2.1)

在 CA 没有生成密钥对的情况下，密钥持有者需要其对私钥的所有权进行证明(如通过密钥持有者提交证书签名请求(CSR)的方法)。也可要求密钥持有者定期对发自 CA 的质询进行签名。

7.3.2.2 组织身份的鉴别

(3.2.2)

医疗保健组织、支持组织或代表组织或设备利益的个人应通过提交与其国家、省/市/自治区相对应的文件来向 RA 证明其真实性和医疗保健角色。CA、RA 以及(如果合适的话)AA 应验证上述信息，以及进行该请求的代表的真实性，并授权该代表在活动时使用该组织的名称。

7.3.2.3 个人身份的鉴别

(3.2.3)

包括正规健康专业人员、非正规健康专业人员、受委托医疗保健提供者、支持组织雇员以及患者/消费者在内的个人应在发行证书前向 RA 鉴别其身份。本部分建议应提供与签发护照给个人时所需的相同证明以及实施与之一样严格的程序。

正规健康专业人员，为了鉴别他们的医疗保健执照、角色以及医疗专业(如果有的话)，应向 RA 提供由相关专业协调或认可团体在其权限内为该人员建立的专业证书等证明。

非正规健康专业人员，为了确立其职业关系并鉴别其医疗保健角色，应向 RA 提供由其委托健康组织或委托(正规)健康专业人员给出的委托关系或雇佣关系的证明。

受委托医疗保健提供者，为了确立他们在其医疗保健社区中的活动以及鉴别其医疗保健角色，应向 RA 提供由其委托健康组织或委托(正规)健康专业人员给出的委托关系或雇佣关系的证明。

支持组织雇员，为了确立其职业关系并鉴别其医疗保健角色，应向 RA 提供由其支持健康组织给出的雇佣关系的证明。

7.3.2.4 未经验证的证书预订者信息

(3.2.4)

未经验证的证书预订者信息应符合 IETF/RFC 3647:2003 中 3.2.4 的规定。

7.3.2.5 授权机构的确认

(3.2.5)

授权机构的确认应符合 IETF/RFC 3647:2003 中 3.2.5 的规定。

7.3.2.6 互操作的标准

(3.2.6)

互操作的准则应符合 IETF/RFC 3647:2003 中 3.2.6 以及 GB/Z 21716.2 的规定。

7.3.3 重建密钥请求的标识和鉴别

7.3.3.1 日常重建密钥的标识和鉴别

(3.3.1)

7.3.3.1.1 CA 日常重建密钥

应基于在创建时原始记录所用的原始文件来实施 CA 证书的日常重建密钥或重新发布证书。

7.3.3.1.2 RA 日常重建密钥

应基于在创建原始记录时所用的原始文件来实施 RA 证书的日常重建密钥或重新发布证书。

7.3.3.1.3 证书持有者日常重建密钥

应通过重新引用在创建原始记录时所用的原始文件或记录(包括相信当前还未过期的有效密钥)来实施证书持有者信息的日常重建密钥或重新发布证书。

如果原始文件已失效或被废弃,可以使用其替代文件。

7.3.3.2 在撤销后重建密钥

(3.3.2)

7.3.3.2.1 在撤销后 CA 重建密钥

在证书被撤销后对信息重建密钥时,应要求再次提供用于最初给 CA 授权的原始信息。

7.3.3.2.2 在撤销后 RA 重建密钥

在证书被撤销后对信息重建密钥时,应要求再次提供用于最初给 RA 授权的原始信息。

7.3.3.2.3 在撤销后证书持有者重建密钥

进行证书持有者信息的日常重建密钥时,应提供原始记录被创建时的原始文件,或者引用所使用的原始记录。如果原始文件已失效或被遗弃,可以使用其替代文件。

7.3.4 用于撤销请求的标识和鉴别

(3.4)

7.3.4.1 CA

当一个 CA 按照医疗保健 CP 向另一个 CA 发出一个撤销请求时,该 CA 应:

a) 标识该证书;

b) 指明该证书被撤销的原因;

c) 用其私钥对该请求进行签名,加密该消息并将其发送给相关领域的 CA。

7.3.4.2 RA

当 RA 对于按照医疗保健 CP 签发的数字证书向证书权威机构发出一个撤销请求时,该 RA 应:

a) 对请求撤销的证书进行标识;

b) 指明该证书撤销的原因;

c) 用其私钥对该请求进行签名,加密该消息并将其发送给相关领域的 CA。

7.3.4.3 证书持有者

持有按医疗保健 CP 签发的数字证书的证书持有者,当向证书权威机构发出一个撤销请求时,该证书持有者应:

a) 对请求撤销的证书进行标识;

b) 指明该证书撤销的原因;

c) 向该相关领域 CA 安全地发送该撤销请求。

如果包含私钥的令牌出现丢失或被盗(并且该证书持有者因此而不能发起经过数字签名的撤销请求),该撤销请求应附有最初用于包含该证书的同等身份证据。

7.4 证书生命周期操作请求

7.4.1 证书申请

7.4.1.1 证书申请提交者

(4.1.1)

确定证书申请提交者的准则应按照 IETF/RFC 3647:2003 中的 4.1.1 的规定。

7.4.1.2 登记程序和职责

(4.1.2)

CA 可以将标识和鉴别功能委派给一个 RA,并由其负责。医疗保健组织 RA 的主要功能是在最初注册时验证证书持有者的身份及其医疗保健角色。RA 应使用与 CA 相同的一套鉴别方法和规则。RA 可以看做是单独授信、独立的特殊 CA。

为了保证证书及其中包含的公钥的真实性和完整性,证书持有者应让可信的发起者来创建他们的证书。由于 RA 是替 CA 执行鉴别功能,所以应授信他们去遵循 CA 的证书持有者鉴别策略并将正确证书持有者信息传递给 CA。同样,应授信 RA 以准确、及时的方式把证书撤销请求传递给 CA。

建议 RA 独立负责地代理 CA 进行相关活动。RA 应:

a) 如果 RA 实时履行其职责,则 RA 应保证其签名的私钥仅用于对证书请求、撤销请求以及证书持有者其他经鉴别的通信进行签名;

b) 向 CA 证明其已鉴别了证书持有者的身份;

c) 安全地传输和存储证书申请信息以及注册记录;

d) 按照 7.3.4.2 的规定(在适当的地方)发起撤销请求。

在配置了数字证书的卫生领域中的证书持有者,应接受证书并保证在证书申请中所表达信息的准确性,以及承认证书中所包含的所有信息都是正确的。

7.4.2 证书申请处理

7.4.2.1 执行标识和鉴别功能

(4.2.1)

执行标识和鉴别功能的准则应按照 IETF/RFC 3647:2003 中 4.2.1 的规定。

7.4.2.2 证书申请的批准或拒绝

(4.2.2)

批准或拒绝证书申请的准则应按照 IETF/RFC 3647:2003 中 4.2.2 的规定。

7.4.2.3 处理证书申请的时间

(4.2.3)

建议 CA 规定一个证书持有者在证书签发处理开始后必须完成其关键处理活动的最短时间期限。

7.4.3 证书签发

7.4.3.1 证书签发过程中 CA 的行为

(4.3.1)

证书重建密钥的程序应符合 IETF/RFC 3647:2003 中 4.7 的规定。

7.4.3.2 签发证书的 CA 给证书持有者的通知

(4.3.2)

当具有证书持有者识别名的证书被签发时,进行证书签发的 CA 应通知对应的每个证书持有者。

7.4.4 证书接受

7.4.4.1 构成证书接受的行为

(4.4.1)

在配置了数字证书的卫生领域中的证书持有者,应:

a) 阅读以简单语言清楚描述了证书持有者责任的 CP 或 PKI 公开文件；

b) 正式同意已签名的持有者协议中的相关义务。

7.4.4.2 CA 的证书发布

(4.4.2)

规定见 7.2.2。

7.4.4.3 CA 给其他实体的签发证书通知

(4.4.3)

CA 给其他实体的签发证书通知的准则应符合 IETF/RFC 3647:2003 中 4.4.3 的规定。

7.4.5 密钥对和证书的使用

7.4.5.1 证书持有者私钥和证书的使用

(4.5.1)

在配置了数字证书的卫生领域中的证书持有者，应：

a) 保护自己的私钥和密钥令牌(如果有的话)，并用合理的方法保护它们不被丢失、泄密、修改或非授权使用；

b) 尽各种可能去保护其私钥不被丢失、泄密或非授权使用；

c) 对于任何已出现的或怀疑出现的包括丢失、泄密在内的危及其私钥安全的情况，立即通知给 CA 和/或 RA；

d) 在医疗保健组织中，对于证书信息、角色或状态的任何修改，都应通知 RA 和/或 CA；

e) 使用符合 CP 的公钥对。

建议医疗保健数字证书的证书持有者还能证明其接受了适用于使用证书的健康信息功能的安全培训。

7.4.5.2 可依赖方公钥和证书的使用

(4.5.2)

只有在下列情况下，可依赖方才有权依赖于医疗保健证书：

a) 证书的使用目的适合于本策略；

b) 此种信赖是合理的，且在信赖时是忠实地以可依赖方所知的详情为依据的；

c) 可依赖方通过检查证书没有被撤销或被暂停来确认该证书当前的有效性；

d) 如果可能的话，可依赖方确认数字签名的当前有效性；

e) 对责任和担保的适当限制是众所周知的。

7.4.6 证书更新

(4.6)

签发方 CA 应确保证书更新的任何程序都与其 CP 相关的规定一致。

7.4.6.1 证书更新的环境

(4.6.1)

证书更新的具体环境应符合 IETF/RFC 3647:2003 中 4.6.1 的规定。

7.4.6.2 需要更新的相关方

(4.6.2)

确定需要更新准则的各相关方时应符合 IETF/RFC 3647:2003 中 4.6.2 的规定。

7.4.6.3 处理证书更新请求

(4.6.3)

处理证书更新请求的准则应符合 IETF/RFC 3647:2003 中 4.6.3 的规定。

7.4.6.4 通知证书更新对应的证书持有者

(4.6.4)

当更新带有证书持有者识别名的证书时，签发方 CA 应通知到每一个相关的证书持有者。

7.4.6.5 构成接受更新证书的行为

(4.6.5)

构成接受更新证书的行为应符合 7.4.4.1 中的规定。

7.4.6.6 CA 发布更新后的证书

(4.6.6)

规定见 7.2.2。

7.4.6.7 CA 给其他实体的发布更新的通知

(4.6.7)

规定见 7.4.4.3。

7.4.7 证书重建密钥

(4.7)

证书重建密钥的程序应符合 7.3.3 的规定。

7.4.8 证书修改

7.4.8.1 证书修改的环境

(4.8.1)

下列情况下,作为签发方的 CA 应修改证书:

a) 如果证书中的相关主题信息不再正确;

b) 如果证书持有者的组织关系改变,例如一个正规健康专业人员从某个特定的组织辞职;

c) 不管何种原因,只要证书持有者或者受委托医疗保健提供者的委托方提出请求。

如果意识到证书中的主题信息不正确,证书持有者、RA 以及委托方有责任通知 CA。

7.4.8.2 证书修改请求者

(4.8.2)

应由下列一方或多方来提出修改证书的请求:

a) 证书持有者,其中证书以该证书持有者的名称签发的;

b) 代表设备或应用一方实施证书的个人或组织;

c) 证书持有者是整个健康专业人员的健康专业人员注册组织或发照组织;

d) 受委托医疗保健提供者的委托方;

e) 签发方 CA 的工作人员;

f) 与签发方 CA 相关的 RA 的工作人员。

7.4.8.3 处理证书修改请求

(4.8.3)

处理证书修改请求的准则应符合 IETF/RFC 3647:2003 中 4.8.3 的规定。

7.4.8.4 通知证书持有者有关修改证书的事宜

(4.8.4)

通知证书持有者有关修改证书发布的事宜应符合 7.4.3.2 中的规定。

7.4.8.5 构成接受修改后的证书的行为

(4.8.5)

构成接受修改后的证书的有关行为应符合 7.4.4.1 中的规定。

7.4.8.6 公布由 CA 修改的证书

(4.8.6)

公布由 CA 修改的证书其准则应符合 7.4.4.2 中的规定。

7.4.8.7 CA 通知其他实体有关修改证书的事宜

(4.8.7)

CA 通知其他实体有关修改证书的事宜时应符合 7.4.4.3 中的规定。

7.4.9 证书撤销和暂停

(4.9)

RA 能有助于处理证书撤销请求。在一些健康数字证书的具体实施中,RA 可用来发起或鉴别证书撤销请求。在适当的情况下,他们应把鉴别好的请求传递给合适的 CA。RA 本身可以发起一个撤销请求(例如,假设一个正规健康专业人员因为行为不当而被暂停工作,此时 RA 正好是其一个健康专业注册组织或发照组织)。不管怎样,此时 RA 有责任去鉴别该报告。如果(通过应用与 CA 所用过的相同标准)RA 认为该报告是可信的,该 RA 应安全的向 CA 发送一个含有证书标识信息的消息,并(此项为可选行为)陈述撤销该证书的理由。

建议在证书中定义的 CRL 分布点的地址应符合本部分 GB/Z 21716.2—2008 中 7.2.8 的规定。

7.4.9.1 撤销的环境

(4.9.1)

针对下列情况,签发方 CA 应撤销证书:

a) 证书持有者、雇主(对于非正规健康专业人员或支持组织雇员而言)或委托方(对于受委托医疗保健提供者而言)没有在本策略、各可用 CPS 或其他协议、法规和对于证书有强制性的法律下履行好义务;

b) 得知或有理由怀疑私钥的安全受到威胁;

c) 证书中的相关主题信息不再正确;

d) 证书持有者的组织关系发生改变,例如一个正规健康专业人员从某个特定的组织辞职;

e) 由于不符合本策略和/或任何可用的 CPS,CA 认为该证书未被正确的签发;

f) 不管何种原因,只要证书持有者或者受委托医疗保健提供者的委托方提出了请求。

如果意识到证书中的主题信息不正确,证书持有者、RA 以及委托方有责任通知 CA。

7.4.9.2 请求撤销者

(4.9.2)

应由下列一方或多方来提出撤销证书的请求:

a) 证书持有者,其中证书以该证书持有者的名称签发的;

b) 代表设备或应用一方实施证书的个人或组织;

c) 受委托医疗保健提供者的委托方;

d) 签发方 CA 的工作人员;

e) 与签发方 CA 相关的 RA 的工作人员。

7.4.9.3 请求撤销的程序

(4.9.3)

按照 7.3.4 的要求 CA 收到一个撤销请求时,该 CA 应:

a) 确认该请求撤销的实体是该要求被撤销的证书中所列的证书持有者;

b) 如果请求者是该证书持有者的代理,则该请求者有足够的权力进行撤销请求;

c) 验证请求撤销的理由,如果证明理由真实,则撤销该证书。

7.4.9.4 撤销请求的期限

(4.9.4)

在收到证书撤销的请求后应立即采取行动以给出相关结果。

7.4.9.5 CA必须处理撤销请求的时间期限

(4.9.5)

在收到请求后CA应立即发起撤销证书的相关行动。

7.4.9.6 为可依赖方检查撤销请求

(4.9.6)

无论何时只要可依赖方使用其他实体的公钥,可依赖方都应检查该CRL。应至少每天检查一次该CRL以便了解撤销的情况。

7.4.9.7 CRL的发布频率

(4.9.7)

无论何时只要CRL发生改变,关于撤销的通知应(在发布的当天)及时迅速地发出并更新。

7.4.9.8 CRL的最大有效期

(4.9.8)

CRL最大有效期的准则应符合IETF/RFC 3647:2003中4.9.8的规定。

7.4.9.9 检查在线撤销/状态的可用性

(4.9.9)

CA应使它的撤销/状态检查服务(如CRL或OCSP)对于匹配其可依赖方的业务时间是可用的。

7.4.9.10 对检查在线撤销的请求

(4.9.10)

在线撤销的检查(如通过OCSP)将要求证书持有者建立与在线证书状态检查服务器之间的安全通信,其中该在线证书状态检查服务器具有对响应进行的签名的能力。它可以是CA。通过这种方式,CA的真实性将得到验证。也有可能使用确认的权威机构或外界供应的目录而不是签发方CA。

7.4.9.11 其他公告撤销的有效形式

(4.9.11)

当包含着证书持有者识别名的证书被撤销时,发行方CA应通知所有相应的证书持有者(应向代表设备或应用证书一方的负责人或组织发出通知)。

7.4.9.12 鉴于密钥安全受到威胁时的特殊要求

(4.9.12)

在CA签发密钥时受到安全威胁的情况下,CA应立即将情况通知给共同签发交叉证书或从属CA证书的相关方。

7.4.9.13 暂停的环境

(4.9.13)

在一个卫生领域CP中,CA应支持暂停功能。下列经过标识的环境将表明证书暂停是需要的:

a) 怀疑私钥的安全受到威胁,此时在调查过程中暂停将发生;

b) 有关于证书的未澄清的信息;

c) 证书持有者请求暂停;

d) 在本地医疗保健数字证书领域范围的其他决定性环境。

7.4.9.14 请求暂停者

(4.9.14)

在CA支持暂停的地方,证书的暂停应由下列一个或多个来提出请求:

a) 证书签发时使用的是其名称的证书持有者;

b) 代表设备或应用一方实施证书的个人或组织;

c) 受委托医疗保健提供者的委托方;

d) 签发方CA的工作人员;

e) 与签发方 CA 相关的 RA 的工作人员；

f) 可依赖方。

7.4.9.15 暂停证书的程序

(4.9.15)

按照 7.4.9.14 和 7.4.9.15 的要求 CA 收到一个撤销请求时，该 CA 应：

a) 确认该请求者的身份，此时暂停请求声称是来自证书持有者、代表设备或应用一方实施证书的个人或组织，或者受委托医疗保健提供者的委托方的；

b) 确认该请求者的身份，此时暂停请求声称是来自代表设备或应用一方实施证书的个人或组织；

c) 如果请求者是证书持有者的委托方身份，则确认请求者有足够的权力要求暂停；

d) 验证请求暂停的理由，如果证明理由真实，则暂停该证书。

7.4.9.16 暂停期限

(4.9.16)

证书的暂停期应限制在相关调查(如验证信息)所需的时间范围上。建议暂停期不超过 10 个工作日。

7.4.9.17 证书暂停的通知

(4.9.17)

当带有证书持有者识别名的证书被暂停时，签发方 CA 应通知到这些证书的所有持有者(通知应发给代表设备或应用证书一方的负责人或组织)。

7.4.10 证书状态服务

7.4.10.1 运行特征

(4.10.1)

运行特征的准则应符合 IETF/RFC 3647:2003 中 4.10.1 的规定。

7.4.10.2 服务的可用性

(4.10.2)

CA 应使它的状态检查服务对于匹配其可依赖方的业务时间是可用的。

7.4.10.3 操作特点

(4.10.3)

操作特点的准则应符合 IETF/RFC 3647:2003 中 4.10.3 的规定。

7.4.11 订阅的终止

(4.11)

订阅终止的准则应符合 IETF/RFC 3647:2003 中 4.10.11 的规定。

7.4.12 私钥的第三者保管

(4.12)

用于鉴别的私钥以及数字证书都不应由第三者保管，除非有法律的特殊要求。

7.5 物理控制

(5)

7.5.1 概述

物理、程序和人员上的安全控制应符合 GB/T 19716—2005(或其等效标准)的规定，或者符合经认可的规范或许可标准的规定。

7.5.2 物理控制

(5.1)

物理控制应符合 GB/T 19716—2005(或其等效标准)的规定。

7.5.3 过程控制

(5.2)

过程控制应符合 GB/T 19716—2005(或其等效标准)的规定。

7.5.4 人员控制

(5.3)

人员控制应符合 GB/T 19716—2005(或其等效标准)的规定。

7.5.5 安全审计日记记录程序

(5.4)

安全审计日记记录程序应符合 GB/T 19716—2005(或其等效标准)的规定。

7.5.6 记录归档

(5.5)

应按照 GB/T 19716—2005 的规定以及遵循当地法律、法规的要求对记录进行存档,并采取相应措施保存好这些存档记录。健康信息是可重用的信息,它存在的时间应该和要引用它的人寿命一样长(甚至比人的寿命更长)。这就特别要求对经过数字签名的记录要进行长期保存,而用于时间戳的重要角色以及长期的抗抵赖技术能支持实现这一点。

7.5.6.1 记录归档的类型

(5.5.1)

知道证书是如何以及为何产生的这在将来可能会很重要。卫生领域 RA 或它们的 CA 对于创建或撤销证书的请求应能对这些事件进行存档。

7.5.6.2 存档的保持时间

(5.5.2)

保存时间的准则应符合 IETF/RFC 3647:2003 中 5.5.2 的规定。健康信息是可重用的信息,它存在的时间应该和要引用它的人寿命一样长(甚至比人的寿命更长)。这就特别要求对经过数字签名的记录要进行长期保存。

7.5.7 密钥更换

(5.6)

为了使证书持有者能无缝的将一个公钥更换为另一个公钥,CA 应在更换日期前 30 天发布新的证书,并明确通知证书持有者从哪天开始他们将使用新证书。

7.5.8 安全威胁和灾难恢复

(5.7)

安全审计程序应符合 GB/T 19716—2005 的规定。

7.5.9 CA 终止

(5.8)

如果一个 CA 停止操作,则该 CA 应立即通知其证书持有者关于操作终止的情况,并安排发布最终的 CRL 以及保持该 CA 的密钥和信息。它也应通知所有与其一块进行交叉证明的 CA。

如果在较低担保级别下将一个 CA 的操作转移给另一 CA,则其操作将被转移的 CA 做签发的证书应通过该 CA 在转移之前所签发的 CRL 而被撤销。

如果一个 CA 终止,应进行相关安排以确保该 CA 的记录能被安全存档或处理。

7.6 技术方面的安全控制

(6)

7.6.1 密钥对的产生和安装

7.6.1.1 密钥对的产生

(6.1.1)

证书持有者的公/私钥对应由下列一方来产生:

a) CA；

b) 由 CA 指定的其他可信第三方；

c) 证书持有者依靠由 CA 认可的密钥管理功能或应用来产生。

如果密钥对由第三方产生，则应强制该第三方采用安全措施（如硬件令牌）来防止篡改密钥对以及对生成私钥产生安全威胁。

密钥的产生应以安全的方式来提供。

7.6.1.2 将私钥分发给证书持有者

(6.1.2)

如果私人才能解译的密钥不是由预期的证书持有者自己产生的，则它将既可以以符合 IETF/RFC 2511 标准规定的在线处理的形式分发给该证书持有者，也可以通过具有相同安全性的方式分发。CA 或可信第三方的密钥产生实体在其交付原始私钥时应能够证明在此过程中没有该私钥的任何拷贝，除非保留拷贝是为了符合 7.6.2.5 规定的密钥备份的目的。

7.6.1.3 将公钥分发给证书发行方

(6.1.3)

如果公共可解译的密钥不是由 CA 产生的，则它将既可以以符合 IETF/RFC 2511 规定的在线处理的形式分发给该 CA，也可以通过具有相同安全性的方式分发。

7.6.1.4 CA 将公钥分发给可依赖方

(6.1.4)

由于公钥是与 CA 签发证书绑定在一起的，因此应让可依赖方能够通过访问证书存储库而得到公钥。

7.6.1.5 密钥长度

(6.1.5)

密钥所能达到的最小长度依赖于其所使用的算法。如使用 RSA 算法，CA 证书的最小密钥长度应是 2 048 bit。如使用其他算法，为提供同等的安全性用于 CA 证书的最小密钥长度也应是 2 048 bit。如使用 RSA 算法或其等同技术，非 CA 证书的最小密钥长度应是 1 024 bit。使用其他算法的非 CA 证书的最小密钥长度也应是 1 024 bit 以提供同等的安全性。

7.6.1.6 公钥参数的产生和质量检查

(6.1.6)

公钥参数应由 CA 或可信第三方密钥生成组织来产生。它应由审计组织这种角色来验证其运作系统的参数质量。

7.6.1.7 按照 X.509 V3（密钥使用域）标准的密钥使用目的

(6.1.7)

鉴别和数字签名密钥应仅用于识别和/或抗抵赖的目的。用于加密的目的时应使用分开的密钥对。

7.6.2 私钥保护

(6.2)

7.6.2.1 概述

本部分建议应存在两个密钥对：一对用于加密以便 CA 能备份私钥，另一对为鉴别或数字签名密钥对以便使该密钥不能被第三者保存。

7.6.2.2 加密模块标准及控制

(6.2.1)

CA 签发的密钥应达到 US FIPS 140-2 中 level 2（或其等效标准）的要求。当一个医疗保健组织的 CA 并不交叉验证时（如一个小型医院），只要证书策略允许，那么满足 level 2 的要求就可以了。如果要活动国际组织间的信任，则该 CA 应达到 level 3 或更高的要求。

其他证书应达到 US FIPS 140-2 中 level 1(或其等效标准)或更高的要求。

加密模块工程控制应符合 GB/T 19716—2005(或其等效标准)的规定,或者符合其他经认可的规范或许可标准的规定。

7.6.2.3 私钥的(n out of m)多人控制

(6.2.2)

当证书持有者是医疗保健组织或支持组织时,私钥可以被分成由不同的人来控制的多个部分。

7.6.2.4 私钥的第三方保存

(6.2.3)

用于鉴别或数字签名的私钥应不能被第三方保存,除非法律上有特殊要求的。

7.6.2.5 私钥备份

(6.2.4)

建议证书持有者把私钥备份在可能的地方,例如把私钥存储在软件令牌中。

私有鉴别或数字签名密钥应在证书持有者的完全控制下被备份。应按照经过鉴别的程序来进行备份。应在不低于原始拷贝所需级别的保护下进行密钥的备份。

除非法律有特殊要求,CA 未经证书持有者事先同意不可将私有解密密钥泄露给任何其他相关方。除此以外,CA 可以提供密钥备份服务以用于加密数据的数据恢复。在这种情况下,因为非正规健康专业人员或支持组织雇员为了从事其作为雇员的业务而接收证书,所以为了数据恢复的目的,CA 可将私有解密密钥透露给非正规健康专业人员或支持组织雇员的雇主,这种安排应在证书发行之前得到认可。

7.6.2.6 私钥存档

(6.2.5)

当 CA 经过证书持有者同意后备份了一个私钥时,该私钥应保留一段时间,且该时间应至少和在 CA 权限范围内个人健康记录的托管保存时间一样长。

7.6.2.7 从加密模块中转出密钥以及密钥转入加密模块

(6.2.6)

如果私有解密密钥不是在实体的加密模块中生成的,则它应按照 IETF/RFC 2511 的规定(或经由同等安全的方式)加入到安全模块中。

7.6.2.8 在加密模块上的私钥存储

(6.2.7)

如果私有解密密钥不是在实体的加密模块中生成的,则它应按照 IETF/RFC 2511 的规定(或经由同等安全的方式)加入到安全模块中。

7.6.2.9 激活私钥的方法

(6.2.8)

对于在卫生领域 CP 下发行的数字证书,只有证书持有者才能激活私钥。证书持有者应被鉴别后提供给加密模块或提供给在激活私钥前保护私钥的应用。该鉴别可以通过密码、密码短语、个人身份号码或生物测定。当取消激活时,私钥应仅以加密的形式保留。

7.6.2.10 取消激活私钥的方法

(6.2.9)

当密钥取消激活时,它们应在内存被释放之前从内存中清除掉。而存储密钥的任何磁盘空间应在该空间被释放给操作系统前被重写。加密模块应在密钥的不活动预置期后自动取消激活该私钥。

7.6.2.11 销毁私钥的方法

(6.2.10)

当一个密钥不再使用时,在计算机内存以及共享磁盘空间中该密钥的所有备份应通过多次重写来安全销毁。私钥销毁的过程应在 CPS 或公开可见的文本中描述。

7.6.2.12 加密模块等级

(6.2.11)

CA 签发的密钥应达到 US FIPS 140-2 中 level 2(或其等效标准)的要求。

其他证书应达到 US FIPS 140-2 中 level 1(或其等效标准)的要求。

7.6.3 密钥管理的其他方面

(6.3)

7.6.3.1 公钥存档

(6.3.1)

应与可信第三方一起对公钥证书和 CRL 进行存档以便允许将来对签名进行验证。CA 应负责确保公钥证书和 CRL 已存档。

7.6.3.2 证书操作周期和密钥对使用周期

(6.3.2)

对于正规健康专业人员,CA 应确保证书的有效期不会超过专业执照的有效期。为了实现该目标,CA 应或者设置证书的有效期限不超过专业执照的有效期,或者准确地确认该专业执照在执照到期前已得到更新,如果该专业执照没有得到更新,则 CA 应撤销或暂停该证书。

非 CA 的公钥和私钥使用应不超过 3 年,过了该期限后应发行新的密钥对。属性证书可以有较短的有效期,具体依业务需求而定。

CA 公钥和私钥的使用应不超过 10 年,过了该期限后应发行新的密钥对。

7.6.3.3 CA 的私钥使用上的限制

CA 应确保其用于证书签发的私钥只能用于签发证书或签发证书撤销列表。CA 应确保签发给其工作人员的私钥只能用于访问和操作 CA 应用的唯一目的。

7.6.4 激活数据

(6.4)

激活数据(注:处于激活状态的数据)应是唯一的、不可预知的,并以安全的形式传递给证书持有者。

7.6.5 计算机安全控制

(6.5)

计算机安全控制应符合 GB/T 19716—2005(或其等效标准)的规定,或者符合其他经认可的规范或许可准则的规定,而且还应涵盖下列文件内容:

a) IETF/RFC 3647 中 6.5.1 指定的计算机安全技术要求;

b) IETF/RFC 3647 中 6.5.2 计算机安全级别。

7.6.6 生命周期技术控制

(6.6)

生命周期技术控制应符合 GB/T 19716—2005(或其等效标准)的规定,或者符合其他经认可的规范或许可准则的规定,而且还应涵盖下列文件内容:

a) IETF/RFC 3647 中 6.6.1 系统开发控制;

b) IETF/RFC 3647 中 6.6.2 安全管理控制;

c) IETF/RFC 3647 中 6.6.3 生命周期安全控制。

7.6.7 网络安全控制

(6.7)

网络安全控制应符合 GB/T 19716—2005(或其等效标准)的规定,或者符合其他经认可的规范或许可准则的规定。

7.6.8 时间戳

(6.8)

用于时间戳的准则应符合 IETF/RFC 3647:2003 中 6.8 的规定。

7.7 证书、CRL 和 OCSP 轮廓

(7)

证书、CRL 和 OCSP 轮廓(如果合适的话)应符合 GB/Z 21716.2—2008 的规定。

7.8 符合性审计

(8)

符合性审计是许多数字签名互操作模型的一个基本构件(例如可参见 GB/Z 21716.1—2008 的 9.2.4)。

7.8.1 CA 符合性审计的频率

(8.1)

CA 依照卫生领域 CP 发行的证书应使所有可依赖方都确信该证书完全符合该策略的要求。CA 符合性审计应由有资格的独立第三方以少于一年的时间为间隔实行。

7.8.2 审计员的身份/资格

(8.2)

审计员应是受到相关专业团体(如通过 ISO 9000 认证)承认并满足其扩展需求的有资格的信息系统审计员。审计员应拥有足够的数字证书经验。如果有该方面正式的认可团体,审查员应满足该团体的要求。

7.8.3 审计员与被审计方的关系

(8.3)

审计员应属于一个与 CA 分离的组织而完全独立于被审计方。审计员应不牵涉被审计方的任何经济利益。

7.8.4 审计所涵盖的主题

(8.4)

诸如证书持有者注册、证书注册、密钥安全威胁报告以及证书撤销等事件都应被审计。审计通常应涵盖审计与 CP 的符合性以及与关联 CPS 的符合性。

为了给 RA 的可信性提供担保并给雇员行为内部审计提供信息,每个 RA 的所有行为都应是可审计的。应为各事件生成符合相关策略的审计记录和审计跟踪。

7.8.5 其结果会造成缺陷的行为

(8.5)

7.8.5.1 概述

如果在一次审计中发现了不正规之处,CA 应对其进行纠正。如果 CA 对于此次审计并没有成功采取合适的措施,则该 CA 的主管团体可以:

a) 指出该不正规之处,但允许该 CA 继续运作直到下一次审计;或者

b) 允许该 CA 在撤销证书之前先不管问题的正确与否而继续运作最多 30 天;或者

c) 撤销该 CA 的证书。

考虑采取上述行动的任何决定时应以该不正规之处的严重性为基础。然而,该 CA 还不能被关闭,因为这导致各种服务的中断。

7.8.5.2 严重失败的归类

当 CA 的认可团体(此处这种认可处于涉及 CA 运作的权限范围内)判定一个 CA 不能遵守 CPS 的实质章节时,这种情况被归为一种严重失败。例如,某一 CA 的检测曾经削减了一些花费多的程序而导致其证书受到安全威胁则应将其归为一个严重失败。

在此之前如果 CA 在其权限范围内已经过认可，则建议立即取消该认可。

7.8.5.3 主要失败的归类

一个 CA 不能成功遵守 CPS 的重要元素(这些元素被认为时担保程序的一部分)时，应被归为主要失败。例如，某一 CA 的识别没有包含足够的业务连续性措施应被归为主要失败。

如果同时有更多的事件影响该 CA 或者该 CA 没能在几天内纠正该符合性问题，则应强制将该问题扩大为严重失败。

7.8.5.4 局部失败的归类

任何对 CPS 符合性的破坏(其中，这些 CPS 符合性被看做是担保程序的一部分，它虽然不会变成主要失败但已能影响该 CA 运作的完整性)应归为局部失败。例如，安全策略和程序的过期应被归为局部失败。

如果又发现更多的此类失败或者该 CA 没有在 30 日内纠正这些符合性问题，则应强制将该问题扩大为主要失败。

7.8.5.5 次要失败的归类

一些符合性的失败虽尚不能归为局部失败，但它对 CA 运作的完整性从整体上有一定的削弱作用，这样的失败应归为次要失败。例如，管理上的失误(如记账不正确)应归为次要失败。

如果发现了更多的本来失败或者该 CA 在下一次安排的审计之前还未纠正该符合性问题，则应强制将该问题扩大为局部失败。

7.8.6 审计结果的通信

(8.6)

应将所有 CA 和 RA 被审计员发现有缺陷的情况立即通知给各证书持有者和可信赖方。

7.9 其他业务和法律问题

(8)

7.9.1 费用

(9.1)

费用应符合 IETF/RFC 3647:2003 中 9.1 的规定。

7.9.2 金融责任

(9.2)

金融责任应符合 IETF/RFC 3647:2003 中 9.2 的规定。

7.9.3 业务信息的保密性

(9.3)

业务信息保密性应符合 IETF/RFC 3647:2003 中 9.2 的规定。

7.9.4 个人信息的保密性

(9.4)

7.9.4.1 保密性设计

(9.4.1)

保密性设计应符合 IETF/RFC 3647:2003 中 9.4.1 的规定。

7.9.4.2 经过保密性处理的信息

(9.4.2)

下列信息应进行保密性处理并维持其保密性：

a) 证书持有者的个人信息以及注册权威机构收集的用于标识目的个人信息，但不包括证书本身(例如，个人标识、背景证明、家庭地址、详细联系方式)。其中一些信息经过证书持有者同意后可以包含在该证书持有者的目录列表中；

b) 私钥。

CA 应对与证书持有者的证书被撤销或暂停的根本原因相关的信息进行保密。

7.9.4.3 不应认为是私有的信息

(9.4.3)

下列信息不应被看做是私有的或者保密的信息：

a) 公钥；

b) 正规或非正规健康专业人员的角色；

c) 医疗保健专业。

7.9.4.4 保护保密信息的责任

(9.4.4)

保密信息应仅在证书持有者的明确同意下或在 CA 或 RA 所在国家的法律要求下才能发布。

7.9.4.5 通知和同意使用私有信息

(9.4.5)

通知或同意使用私有信息应符合 IETF/RFC 3647:2003 中 9.4.5 的规定。

7.9.4.6 按照法律或者管理程序公开信息

(9.4.6)

保密信息应只有在 CA 或 RA 所在国家的法律下根据合法法庭的命令要求才能公开。

7.9.4.7 其他发布信息的环境——在证书持有者的要求下公开

(9.4.7)

保密信息应根据经过鉴别的(带有证书持有者数字签名的)电子邮件或来自证书持有者手写的授权书的要求公开给由该证书持有者指定的一方。

在没有来自证书持有者手写授权书的情况下，保密信息只有根据在 CA 或 RA 所在国家的法律下根据合法法庭的命令要求才能公开。

7.9.5 知识产权

(9.5)

涉及知识产权时应符合 IETF/RFC 3647:2003 中 9.5 的规定。

7.9.6 表述和担保

(9.6)

7.9.6.1 概述

7.9.6.2 所列情况中的扩展责任是医疗保健的各领域中 CA 运作的整个策略的一部分。这些领域都服从于国家法规和国际协议。因此产生了对 CA 责任和 RA 责任的需求。属性机构责任(如果需要用上的话)应包含前面的责任或者进行明确的描述。

7.9.6.2 CA 的表述和担保

(9.6.1)

当一个发行方 CA 发布一个证书时，它要证明它已发行了一个证书给某个证书持有者，并且证书中所表述的信息经验证符合该 CA 的 CP。从证书持有者所访问的存储库中发布该证书时，应继续发布这样的证明。

CA 应给每个证书持有者提供关于该持有者在该 CP 下的权利和责任的通知书。该通知书可以是证书持有者协议的形式，且应包含该证书的使用说明、关于密钥保护和用于证书持有者与 CA 或 LRA 之间通信(包括服务交付中发生改变或策略发生改变的通信)程序的证书持有者责任。CA 应提醒证书持有者关于处理可疑密钥安全威胁、重新申请证书或密钥、取消服务以及解决争议的各项程序。

CA 发行用于卫生领域的数字证书时应承担且不限于以下责任：

a) CA 应对密钥分发过程中私钥所受到的安全威胁负责。

b) CA 应对带有相关数字签名的个人身份与其他认可信息之间的错误绑定负责，除非它能证实

附上了带有证明文件的策略和过程以用于标识和鉴别。该责任应扩展到 CA 已知道或怀疑、或者应已经知道或怀疑该绑定是错误的情形。

c) CA 应对没有根据其撤销策略来撤销证书负责。

d) CA 应对以其撤销策略中没有指定过的理由而撤销证书负责。

7.9.6.3 RA 的表述和担保

(9.6.2)

用于卫生领域的 RA 注册潜在的证书持有者的责任应包括且不限于以下内容：

a) RA 应对带有相关数字签名的个人身份与其他认可信息之间的错误绑定负责，除非它能证实附上了带有证明文件的策略和过程以用于标识和鉴别。该责任应扩展到 RA 已知道或怀疑、或者应该已经知道或怀疑该绑定所产生的主题信息是错误的情形。

b) RA 应对没有根据其撤销策略来撤销证书负责。

c) RA 应对以其撤销策略中没有指定过的理由而撤销证书负责。

7.9.6.4 证书持有者的表述和担保

(9.6.3)

卫生领域 PKI 中的证书持有者应：

a) 确保在证书申请中表述的准确性，以及通过接受证书来承认该证书中的所有信息是真实的；

b) 保护他们的私钥和密钥令牌(如果有的话)，并采取所有合理的方法来保护它们不被遗失、泄密、篡改和未经授权的使用；

c) 尽可能防止对其私钥的遗失、泄密和非授权使用；

d) 对于任何实际的或可疑的遗失、泄密或其他对其私钥的安全威胁都立即通报给 CA 和/或 RA；

e) 对于证书信息、在医疗保健组织中的角色或状态发生了任何改变都通报给 CA 和/或 RA；

f) 使用符合 CP 的密钥对；

g) 通过签署证书持有者协议正式同意这些义务。

建议医疗保健 PKI 中的证书持有者也要证明其接受了适用于使用证书的健康信息功能的安全培训。

7.9.6.5 可依赖方的表述和担保

(9.6.4)

只有在下列情况下卫生领域 PKI 的可依赖方才有权力依赖于一个卫生领域的证书：

a) 该证书的使用目的正好是在本策略之下的；

b) 该依赖是合理的，且在依赖时所诚实依据的所有环境都要让可依赖方知晓；

c) 可依赖方通过检查该证书没有被撤销或暂停而确认了该证书当前的有效性；

d) 如果需要的话，可依赖方确认了数字签名当前的有效性；

e) 可用的义务和担保限制都得到认同。

7.9.7 担保的拒绝

(9.7)

担保的拒绝应符合 IETF/RFC 3647:2003 中 9.7 的规定。

7.9.8 责任限制

(9.8)

7.9.8.1 CA 的责任限制

用于卫生领域的 CA 发行数字证书的责任可在就 CA 而言的下列疏忽行为上受到限制：

a) 一个 CA 可以在证书持有者遗失私钥方面没有责任；

b) 一个 CA 可以在证书持有者生成的密钥方面没有责任，除非该持有者是完全按照一个医疗保

健 CP 来生成该证书的；

c) 一个 CA 可以在私钥本身造成的安全威胁方面没有责任，除非能证明该密钥是在 CA 受到安全威胁的，或者在该密钥生成过程中没有附上策略和程序的证明文件，从而导致私钥更易受安全威胁或实际泄露的影响；

d) 一个 CA 可以在伪造的签名方面没有责任，除非是由于没有附上医疗保健 CP 的策略和程序的证明文件而导致的伪造，或者有迹象显示该 CA 同意了该伪造；

e) 一个 CA 可以在可依赖方所承受的以及由于 CA 没有完全符合本策略的条款所造成的直接伤害的程度上负有有限的责任。

7.9.8.2 RA 的责任限制

用于卫生领域的 RA 注册潜在证书持有者的责任可限制在就 RA 而言的疏忽行为上。

7.9.8.3 证书持有者的责任限制

用于卫生领域的证书持有者的责任可限制在就证书持有者而言的疏忽行为上。

7.9.9 赔偿

(9.9)

赔偿(如果有的话)应符合 IETF/RFC 3647:2003 中 9.9 的规定。

7.9.10 期限和终止

(9.10)

期限和终止应符合 IETF/RFC 3647:2003 中 9.10 的规定。

7.9.11 个人通知及参与方之间的通信

(9.11)

个人通知及参与方之间的通信应符合 IETF/RFC 3647:2003 中 9.11 的规定。

7.9.12 修改

(9.12)

7.9.12.1 修改的程序

(9.12.1)

CP、CPS 以及其他相关的修改应经过 CA 管理团体的同意。

7.9.12.2 通告机制和期限

(9.12.2)

在对 CP 进行任何改动之前，该 CA 的管理团体应通知所有与该 CA 进行直接交叉验证的 CA 并征求意见。

7.9.12.3 OID 必须被修改的环境

(9.12.3)

OID 必须被修改的环境应符合 IETF/RFC 3647:2003 中 9.12.3 的规定。

7.9.13 解决争议的程序

(9.13)

解决争议的程序应符合 IETF/RFC 3647:2003 中 9.13 的规定。

7.9.14 管理方面的法律

(9.14)

在卫生领域中配置数字证书应遵守本地法律以及国际法的要求并符合 GB/T 19716—2005(或其等效标准)的规定，或者符合经认可的规范或许可的规定。

7.9.15 与适用法律的一致性

(9.15)

与适用法律的一致性应符合 IETF/RFC 3647:2003 中 9.15 的规定。

7.9.16 其他规定

(9.16)

7.9.16.1 总体协议

(9.16.1)

总体协议应符合 IETF/RFC 3647:2003 中 9.16.1 的规定。

7.9.16.2 指派

(9.16.2)

如果 CA 或 RA 与另一个组织合并,则新的组织应保持原有责任继续履行原来的协议。

7.9.16.3 分离

(9.16.3)

医疗保健 CP 应规定清楚该 CP 的某个章节是否应判定为不正确或无效的,而其他章节应仍然保持有效直至该 CP 被更新。

7.9.16.4 强制执行

(9.16.4)

强制执行方面应符合 IETF/RFC 3647:2003 中 9.16.4 的规定。

8 PKI 公开声明模型

8.1 概述

设计 PKI 公开声明模型是为了让发行证书的 CA 将之用于补偿公开文件以及 CP 和/或 CPS 所需强调或公开的要素的通告。一个 PKI 公开声明可帮助 CA 对调整请求和可依赖方的顾虑进行应答。尽管 CP 和 CPS 文件是描述和管理 CP 和证书实践的实质文件,然而很多数字证书持有者,特别是消费者,发现这些文件难以理解。

建议使用 PKI 公开声明。

表 1 给出了 PKI 公开声明的结构的例子,用以阐明应公开的信息。

8.2 PKI 公开声明的结构

PKI 公开声明应包含一个部分来标明各个声明类型。PKI 公开证明的各个部分包含了描述性的声明,这些声明可以包括有关 CP/CPS 章节的超链接。

表 1 PKI 公开声明模型

声明类型	声明描述	CP 要求
CA 联系信息	名称、地点以及 CA 的相关联系信息	无
CP 信息和注册	经注册的 CP 对象标识符(OID)	经注册的 CP 对象标识符(OID) CP 和 CPS 的发布(见 7.2.6)
证书的担保级别、确认过程和使用	描述 CA 所发行的证书的担保的级别,相应的确认程序以及证书使用方面的限制	证书使用方面的任何限制
依赖限制	依赖限制,如果有的话	证书使用方面的任何限制(例如,如果证书只能用在电子签名,则在证书方面的依赖限制支持抗抵赖)
证书持有者的职责	描述证书持有者的职责	证书持有者的职责根据 7.2.1.3 的定义

表 1（续）

声明类型	声明描述	CP 要求
可依赖方的职责	扩展到可依赖方有责任检查证书状态，并“适当地依赖”证书	可依赖方的职责根据 7.2.1.4 的定义
有限的授权以及责任的放弃/限制	责任的授权、放弃、限制各方面的摘要，以及任何合适的授权或保险程序	责任的限制（见 7.2.2）
适当的协议、CPS、证书	对适当的协议、CPS、CP 以及其他相关文件的标识和引用	被应用的有资格的 CP
保密性策略	对适当的保密性法律及策略的描述和引用	在本策略下 CA 被要求遵守国家保密性法规的要求
赔偿策略	对适当的赔偿策略的描述和引用	无
适当的法律、投诉和争议的解决	法律的选择声明，投诉程序和争议解决机制	投诉的程序和争议的解决， 适当的法律系统
CA 审计	描述审计过程和审计机构	验证该 CA 是否与其 CP 一致
交叉验证	描述交叉验证以及与该 CA 进行交叉验证的其他 CA 的标识	管理交叉验证的相关策略
CA 和存储库执照以及信任标记	任何政府的执照、印章程序的摘要	无

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(ISO 7498-2:1989,IDT)

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

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

[9] IETF/RFC 2510 Internet X.509 Certificate Management Protocol

[10] IETF/RFC 2511 Internet X.509 Certificate Request Message Format

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

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

[13] U.S. government standard FIPS-140-2, level 1 and level 2

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

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

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

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

[18] BERND, B, ROGER—FRANCE, F A Systemic Approach for Secure Health Information Systems, International Journal of Medical Informatics ,2001:51-78

[19] 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.

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

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

[22] FEGHHI, J, FEGHHI, J and WILLIAMS, P Digital Certificates—Applied Internet Secu-

rity, Addison—Wesley 1998.

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

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

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

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

[27] 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3部分:认证机构的策略管理
GB/Z 21716.3—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 字数 53 千字
2008年7月第一版 2008年7月第一次印刷
*
书号:155066·1-32105 定价 24.00 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 21716.3-2008