ICS 35.020
L 80

中华人民共和国国家标准

GB/T 26855—2011

信息安全技术　公钥基础设施 证书策略与认证业务声明框架

Information security technology—Public key infrastructure—Certificate policy and certification practice statement framework

2011-07-29 发布　　2011-11-01 实施

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

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息中心、吉大正元信息技术股份有限公司。

本标准主要起草人:刘海龙、李伟平、何长龙、于海波、李丹、罗红斌、龙毅宏、姜玉琳。

引　言

本标准凡涉及密码算法相关内容，按国家有关法规实施。

本标准中引用的 RSA 和 SHA-1 密码算法为举例性说明，具体使用时均须采用国家密码管理局批准的相应算法。

证书策略(CP)和认证业务声明(CPS)是公钥基础设施(PKI)建设中两份重要的文档。CP 是“一套指定的规则集，用以指明证书对具有相同安全需求的一个特定团体和(或者)应用类型的适用性”。依赖方可使用 CP 来帮助其决定一个证书(连同其中的绑定)是否足够可信、是否适用于特定的应用。CPS 是证书认证机构在颁发证书中所遵循的业务实践的声明。通常，CPS 也描述全部证书服务生命周期中的业务实践(如签发、管理、吊销、更新证书或密钥)，并且 CPS 提供其他业务、法律和技术方面的细节。

RFC3647 是由因特网工程任务组(IETF)制定的关于 CP 和 CPS 的框架标准，在国际上得到了广泛的认可。本标准是根据 RFC3647 制定的，主体框架与 RFC3647 一致，主要做了两方面修改：其一将与国内密码政策不符的部分进行了修改或删除；其二是将不必要的解释性文字删除，使标准更加简洁。此外，还将原标准中部分前后不一致的地方进行了改正。

销售信息、贸易秘密和在非公开协议下从第三方得到的信息。特别地，此子项说明：

——被认为是保密信息的范围；

——被认为在保密信息范围之外的信息类型；

——接收到保密信息的参与者防止其泄漏、避免使用和发布给第三方的责任。

6.9.4 个人隐私保密

该子项与参与者，尤其是CA、RA和信息库需要采取的保护措施相关，这些措施用来保护证书申请者、订户和其他参与者的个人身份私有信息。特别地，在适用法律范围之内，该子项包括：

——根据有关法律或政策的需要，指定并公开适用于参与者活动的隐私方案；

——PKI中认为或者不认为是隐私的信息；

——收到参与者的隐私信息保证其安全、避免使用和泄漏给第三方的责任；

——在使用或者公开其隐私信息时，通知个人或获得个人同意的相应要求；

——在个人或政府事务或其他任何法律事务中，参与者依据司法或管理程序授权或必须公开隐私信息的条件。

6.9.5 知识产权

该子项说明知识版权问题，如版权、专利、商标、商业秘密等。这些内容可能出现在某些参与者的CP、CPS、证书、名称和密钥中(或在其中声明)，也可能是发给或来自参与者的许可证中的主体。

6.9.6 陈述与担保

该子项包括CP或CPS对各种实体所作的陈述和担保。例如，一个作为合同的CPS可能包含CA的担保：保证其所颁发证书中的信息是准确的。或者CPS包含一个较有限的担保：在认真执行了某种身份鉴别过程后，就CA所掌握的信息而言，证书中的信息是真实的。该子项还可以要求在某些协议中要包含陈述和担保条款，如订户或依赖方协议。例如，某个CP可以包含一项要求：所有的CA要使用订户协议，在该协议中包含CA的一项担保，确保证书中的信息是正确的。CA、RA、订户、依赖方和其他参与者都可制定自己的陈述和担保。

6.9.7 担保免责

该子项包含对有可能存在其他协议中的明示担保责任的否定描述，也包含对由于适用法律引起的隐含担保责任的描述，如商品的可买卖性或适用于特殊目的担保。在CP或CPS中可以直接使用这些担保免责规定，或者包含一项要求，规定担保免责条款要出现在相关协议当中，如订户或依赖方协议。

6.9.8 有限责任

该子项包含CP或CPS中的陪付责任限制，或者出现在与CP或CPS相关的协议中的赔付责任限制，如订户或依赖方协议。这些限制可分为两类：遭受的损失中哪些是可补偿的，和遭受损失可补偿的总量，也就是上限。通常，合同中包含拒绝对某些损失的赔偿，如意外损失、后续性损失和惩罚性损失。经常地，合同中也包含限制一方或另一方赔偿到一确切的数量，或者到一个基准数量，如供应商在合同下所得到的支付。

6.9.9 赔偿

该子项包含一方对另一方遭受损失的赔偿条款，通常这种损失是由第一方的行为所导致的。赔偿条款可以出现在CP、CPS或其他协议当中。例如，在CP中可以要求在订户协议中包含一条规定，如果由于订户在申请证书过程中欺骗性的陈述其身份而使CA为其签发了不正确的证书，给CA造成损失，

订户有赔偿 CA 损失的责任。同样，在 CPS 中可以指出某一 CA 使用依赖方协议，在该协议下，如果依赖方在使用证书过程中没有正确检查吊销信息，或在 CA 允许的目的范围之外使用证书，从而使 CA 遭受损失，依赖方有赔偿 CA 损失的责任。

6.9.10 有效期限与终止

该子项包括 CP 或 CPS 有限的时间期限，以及文档、文档的某一部分或对某一特定参与者的适用性终止的条件。另外，在 CP 或 CPS 中可以要求某些期限和终止条款要出现在订户或依赖方协议中。特别地，这些条款包括：

——文档或协议的有效期限，也就是如果文档不提前终止，文档生效和失效的时间。

——终止规定，声明文档、文档的某一部分或对某一特定参与者的适用性停止有效的条件。

——文档终止的任何可能结果，例如协议的某些条款在协议终止后继续有效，如知识产权承认和保密条款。另外，终止可能涉及到各参与方返还保密信息到其拥有者的责任。

6.9.11 各参与者的个别通告与沟通

该子项讨论某一参与方与另一参与方进行通信时可以或必须遵循的方法，以使其通信过程在法律上有效。例如，一个 RA 想要告知 CA 它想终止与 CA 的协议。此子项的内容与公布和发布证书的功能不同，因为公布和发布证书是以与大范围的接受者之间的通信为目的，如所有的依赖方。此子项可建立通信机制并指明联系信息以便传递信息，比如发送经过数字签名的电子邮件到指定地址，随后是经过签名的电子邮件接收确认。

6.9.12 修订

有时需要修订某个 CP 或 CPS，有些变动并没有实质性地减少 CP 或其实施所提供的保证，这种改变将被策略管理员判定为对证书的可接受性没有重大影响，这样的变动不需要改变 CP 的 OID 或 CPS 的地址指针(URL)。另一方面，有些变动会从根本上改变对证书的接受(针对特殊目的)，这些变动需要改变相应 CP 的 OID 或 CPS 的地址指针。

该子项还可包含下列信息：

——CP、CPS 或其他文档必须或可以遵循的修正程序。当对 CP 或 CPS 修正时，变动过程可能包括通告机制(将建议的变更通知所有受影响的对象，如订户和依赖方)，评论期限，评论接收、审阅，并反映到文档的机制，和修正最终形成并生效的机制。

——当对 CP 或 CPS 进行修正时，需要变更 CP 的 OID 或 CPS 的 URL 的条件。

6.9.13 争议处理

该子项说明解决出自 CP、CPS 或其他协议的争端的程序，例如要求争端需要通过某个论坛解决，或者其他的争端解决机制。

6.9.14 管辖法律

该子项设置一项声明，说明在某个司法管辖域内的法律对 CP、CPS 或其他协议的解释和生效起作用。

6.9.15 与适用法律的符合性

该子项说明参与者所需遵守的适用法律，如与密码硬件和软件相关的法律，该法律可能还受控于给定司法管辖域下的出口控制法。CP 或 CPS 需要声明满足这些法律，或者声明这些规定在其他协议中给出。

6.9.16 一般条款

该子项包括综合规定，这里所总结的条款可以出现在CP、CPS或其他协议中：

——整体协议条款，通常标识出构成整个协议的全部文档，并声明该协议替代所有先前或同时期的、与相同主题相关的书面或口头解释。

——转让条款，通过某种方式限制一方的能力，如在该协议下将一方的权利转让给另一方的规定（如在将来接受费用的权利），或授权其某种义务。

——分割性条款，表达参与方在出现如下事件时的意图，即当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

——强制执行条款，可以声明在协议纠纷中有利的一方有权将代理费作为偿还要求的一部分，或者声明免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

——不可抗力条款，通常用于出现超出受影响方控制事件的发生时，免除一方或多方对合同的执行责任。通常，免除执行的时间与事件所造成的延迟时间相当。此条款也可包括协议终止的环境和条件。构成不可抗力的事件包括战争、恐怖袭击、罢工、自然灾害、供应商或卖方执行失败、因特网或其他基础设施的瘫痪。不可抗力条款的起草应与框架的其他部分相一致，并达到适用的服务级别协议。例如，业务连续性和灾难恢复的责任和能力可以将某些事件置于组织的可控范围之内，如在停电时启用备份电源的义务。

6.9.17 其他条款

针对PKI参与者，又不属于本框架的项或子项的任何附加责任和规定，都在此描述。

附 录 A
（规范性附录）
条款集框架

本附录包含条款集的标题列表，可作为全部标题的一览表或 CP、CPS 编写者的标准模板。此标题列表有助于：

a） 在进行交叉认证或其他形式的互操作时，比较两个证书策略（为实现策略映射）。

b） 将 CPS 与 CP 进行比较，来确认 CPS 忠实地实现了策略。

c） 比较两个 CPS。

条款集标题列表如下：

1 引言
1.1 概述
1.2 文档名称与标识
1.3 PKI 参与者
1.3.1 证书认证机构
1.3.2 注册机构
1.3.3 订户
1.3.4 依赖方
1.3.5 其他参与者
1.4 证书应用
1.4.1 适合的证书应用
1.4.2 限制的证书应用
1.5 策略管理
1.5.1 策略文档管理机构
1.5.2 联系人
1.5.3 决定 CPS 符合策略的人员
1.5.4 CPS 批准流程
1.6 定义和缩写
2 发布与信息库责任
2.1 信息库
2.2 认证信息的发布
2.3 发布的时间或频率
2.4 信息库访问控制
3 标识与鉴别
3.1 命名
3.1.1 名称类型
3.1.2 对名称意义化的要求
3.1.3 订户的匿名或伪名
3.1.4 解释不同名称形式的规则
3.1.5 名称的唯一性
3.1.6 商标的识别、鉴别和角色
3.2 初始身份确认

附 录 B
（资料性附录）
证 书 策 略

B.1 适用于特定团体的证书策略

假定中国民用航空局(CAAC)联合各航空公司共同运营一个 PKI，定义在航空领域内使用的 CP，可以定义两个 CP：CAAC 普通 CP 和 CAAC 商业级 CP。

CAAC 普通 CP 能够被业内人员用来保护日常的信息(如电子邮件)，和在通常的信息检索中鉴别浏览器到服务器间的连接。密钥对可以通过低成本的、基于软件的系统(如商业浏览器)来产生、存储和管理。在这种策略下，证书可以被自动签发给任何在 CAAC 公共目录中列出的员工或者任何成员航空公司，只要该公司提交了一个签名的证书申请表给组织内的网络管理员。

CAAC 商业级 CP 可用于保护金融交易或者绑定航空公司间的合同交换。在这个策略下，CAAC 可能要求被认证的密钥对需要在经过认可的密码硬件令牌中生成和存储，证书和令牌可能通过专门的分配机构发放给航空公司的雇员。作为颁发令牌和证书的条件，这些被授权的个体可能被要求向公共的安全部门登记，出示有效的身份证件，并且签署一份订户协议书，该协议书要求其保护令牌并仅用于指定的目的。

B.2 适用于共同安全需求的证书策略

对于在电子政务中使用的 PKI，可由其策略管理机构(PMA)定义证书策略。针对签名证书和加密证书，可以定义 8 个证书策略：4 个策略用于数字签名证书，另 4 个策略用于加密证书。对每种类型的应用，都可定义 4 个保证等级：初级、基本级、中级和高级。在定义证书策略时，应根据应用对签名和加密的不同安全要求进行分类，分别提供初级、基本级、中级和高级的保证级别。从初级到高级，安全要求逐渐增加，从而保证级别也不断增加。

参 考 文 献

[1] Chokhani,S. and W. Ford. Internet X.509 Public Key Infrastructure,Certificate Policy and Certification Practices Statement Framework. RFC 3647,November 2003.

[2] European Telecommunications Standards Institute. Policy Requirements for Certification Authorities Issuing Qualified Certificates. ETSI TS 101 456,Version 1.1.1,December 2000.

[3] Government of Canada PKI Policy Management Authority. Digital Signature and Confidentiality Certificate Policies for the Government of Canada Public Key Infrastructure,v.3.02,April 1999.

[4] Identrus,LLC,Identrus Identity Certificate Policy IP-IPC Version 1.7,March 2001.

[5] American Bar Association,Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce,1996.

[6] American Bar Association. PKI Assessment Guidelines,v0.30,Public Draft For Comment,June 2001.