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。

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

1　范围

本标准规定了证书策略(CP)和认证业务声明(CPS)的概念,解释二者之间的区别,并规定了 CP 和 CPS 应共同遵守的文档标题框架,包括在标题中所应包含的信息类型。本标准提出的框架一般假设使用 GB/T 16264.8—2005 证书格式,但并不意味着此框架仅限于使用这种证书格式。此框架也可用于其他格式的证书。

本标准适用于 CP 和 CPS 的撰写和比较。本标准所给出的框架应作为一个灵活的工具来使用,用以指明在特定的 CP 或 CPS 中所应考虑的主题,而不是作为生成 CP 或 CPS 的固定公式。

本标准不适用于通用安全策略的定义,如组织安全策略、系统安全策略或数据标记策略。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 13000.1—1993　信息技术　通用多八位编码字符集(UCS)　第 1 部分:体系结构与基本多文种平面(idt ISO/IEC 10646-1:1993)

GB/T 16264.2—2008　信息技术　开放系统互连　目录　第 2 部分:模型(ISO/IEC 9594-2:2005,IDT)

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)

GB/T 16284.1—2008　信息技术　信报处理系统(MHS)　第 1 部分:系统和服务概述(ISO/IEC 10021-1:2003,IDT)

GB/T 19713—2005　信息技术　安全技术　公钥基础设施　在线证书状态协议

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

RFC 822:1982　ARPA 因特网文本消息格式标准(Standard For The Format of ARPA Internet Text Messages)

RFC 5280:2008　因特网 X.509 公钥基础设施证书和证书撤销列表轮廓(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)

3　术语和定义

GB/T 16264.8—2005 确立的以及下列术语和定义适用于本文件。

3.1

激活数据　activation data

用于操作密码模块所必需的,并且需要被保护的非密钥数据值(例如 PIN、口令或人工控制的密钥共享部分)。

3.2

鉴别　authentication

确定个人、组织或事物如其所声称的个人、组织或事物的过程。在 PKI 上下文中，鉴别指的是证实以某个特定名称申请或试图访问某事物的个人或组织确实为真实的个人或组织的过程。

3.3

认证业务声明　certification practice statement

证书认证机构在签发、管理、撤销或更新证书、密钥过程中所采纳的业务实践的通告。

注：在国内，认证业务声明也称为电子认证业务规则，CA 机构在开展电子认证业务前，需要将本机构的电子认证业务规则提交至国家工业及信息化部的相关部门进行备案。

3.4

CPS 摘要　CPS abstract

由一个 CA 公布的、关于其完整 CPS 的一个子集。

3.5

标识　identification

建立个人或组织的身份的过程，也就是指明某个人或组织是特定的个人或组织。在 PKI 上下文中，标识包含两个过程：

a) 确定某个人或组织的给定名称与真实世界中该个人或组织的身份相联系。

b) 确定在该名称之下申请或试图访问某事物的个人或组织确实为指定的个人或组织。寻求标识的人可能是证书申请者，或者是 PKI 系统中可信职位的申请者，或者是试图访问网络或应用软件的人(如 CA 管理员试图访问 CA 系统)。

3.6

签发证书认证机构　issuing certification authority

在特定的 CA 证书上下文中，签发 CA 是签发证书的 CA(见主体 CA)。

3.7

参与者　participant

在一个给定 PKI 中扮演某一角色的个人或组织，如订户、依赖方、CA、RA、证书制作机构、信息库服务提供者，或类似实体。

3.8

PKI 信息披露声明　PKI disclosure statement

关于 CP 或 CPS 的补充手段，用于公开证书策略和 CA/PKI 业务中的关键信息。PDS 是公开和强调信息的载体工具，这些信息通常在相关 CP 或 CPS 中作更详细描述。因此，PDS 并不能替代 CP 或 CPS。

3.9

策略限定符　policy qualifier

依赖于策略的信息，可能与 CP 标识符共同出现在 GB/T 16264.8—2005 证书中。该信息中可能包含指向适用 CPS 或依赖方协议的 URL 指针，也可能包含证书使用条款的文字(或引起文字出现的数字)。

3.10

注册机构　registration authority

具有下列一项或多项功能的实体：标识和鉴别证书申请者，同意或拒绝证书申请，在某些环境下主动吊销或挂起证书，处理订户吊销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书(即 RA 代表 CA 承担某些任务)。

注：在其他文档中可能使用本地注册机构(LRA)，是相同的概念。

3.11

依赖方　relying party

证书的接收者，他依赖于该证书和(或)可通过该证书所验证的数字签名。在本标准中，术语“证书使用者”与“依赖方”可互换使用。

3.12

依赖方协议　relying party agreement

证书认证机构与依赖方所签署的协议，通常规定了在验证数字签名或其他使用证书的过程中有关方所拥有的权利和义务。

3.13

条款集　set of provisions

关于业务实施和(或)策略声明的集合，覆盖了一定范围的标准主题，用于使用本框架中所描述的方法来表达 CP 或 CPS。

3.14

主体证书认证机构　subject certification authority

在特定的 CA 证书上下文中，主体 CA 指的是在证书中其公钥被认证的 CA(见签发 CA)。

3.15

订户　subscriber

被颁发给一张证书的证书主体。

3.16

订户协议　subscriber agreement

CA 与订户之间签署的协议，规定了双方在颁发和管理证书的过程中所拥有的权利和义务。

4　缩略语

ASN.1　抽象语法记法
B-to-B　企业到企业
CA　证书认证机构
CP　证书策略
CPS　认证业务声明
CRL　证书撤销列表
LRA　本地注册机构
OCSP　在线证书状态协议
OID　对象标识符
PDS　PKI 信息披露声明
PIN　个人识别数字
PKI　公钥基础设施
RA　注册机构
RPA　依赖方协议
RSA　由 R. Rirest、A. Sllalnlr 和 L. Adleman 共同发明的公钥算法
SSL　安全套接字
TLS　传输层安全
URI　统一资源标识符

5 概念

5.1 证书策略

当证书认证机构签发一张证书时，它就对证书使用者（依赖方）提供了一项声明：一个特定的公钥与一个特定实体（证书主体，通常也称作订户）的身份相绑定。但是，依赖方应该在何种程度上信任 CA 的声明，则需要由依赖方或者由控制、协调依赖方使用证书方式的实体来判断。不同的证书在颁发时遵循了不同的业务实践和程序，并且可能适用于不同的应用和（或）目的。

GB/T 16264.8—2005 标准将证书策略定义为“一套指定的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。”一个 GB/T 16264.8 证书可以指定一个特定的可用 CP，依赖方可以根据该 CP 来判断对于某个特定目的，是否信任该证书，以及公钥或该公钥所验证的数字签名。

CP 可分为两类。第一类 CP “指明证书对一个特定团体的适用性”。这些 CP 设置了证书使用要求和对团体成员的要求。举例见 B.1。

第二类 CP“指明了证书对于具有相同安全需求的某类应用的适用性”。这些 CP 指明了应用或证书使用方式的集合，并且说明这些应用或使用方式需要一定的安全级别，然后设置了适用于这些应用或使用方式的 PKI 要求。相对于依照相关的 CP 颁发的证书，此类 CP 常常设置适用于证书所提供的特定保证级别的特定要求。这些保证等级可对应于多种类型的证书，举例见 B.2。

在证书中，CP 由唯一“对象标识符”（OID）表示。此 OID，或者至少是一个“树叉”，能够被注册。“树叉”就是 OID 数字序列的开始部分，并且分配给一个特定的组织。注册的过程要遵循 ISO/IEC 和 ITU 标准所指定的流程。注册 OID 或“树叉”的组织也要发布 CP 的文本定义，供依赖方审查。任何一个证书在颁发时都要声明与某一个 CP（或几个 CP，如果可能）相一致，这个声明显示在 GB/T 16264.8 证书的证书策略扩展项中。当 CA 在一个证书的证书策略扩展项中设置了多个 CP 时，则 CA 就确保该证书能够在任意所列 CP 下正当使用。

CP 也形成了一个审计、认可或以其他方式评估 CA 的基础。对每个 CA，都可根据认为其要实现的一个或多个 CP 或 CPS，对其进行评估。当一个 CA 为另一个 CA 签发一张 CA 证书时，签发 CA 必须对其所信任的主体 CA 的所有 CP 进行评估（这种评估也可以依据所涉及的证书策略进行）。然后，所有被评估的 CP 由签发 CA 在 CA 证书中指明。GB/T 16264.8 证书认证路径处理逻辑在定义好的信任模型中使用这些 CP 标识。

5.2 GB/T 16264.8 证书域

5.2.1 证书策略扩展项

证书策略扩展项中列举了证书认证机构声明该证书适用的 CP。附录 B 中给出了中国民用航空局（CAAC）所定义的普通 CP 和商业级 CP 的例子，在对常规员工所颁发的证书中可包含普通 CP 的对象标识符，通过专门分配机构发给员工的证书可同时包含普通 CP 和商业级 CP 的对象标识符。在证书中同时包含这两个对象标识符意味着该证书既可用于普通 CP，也可用于商业级 CP。在证书策略扩展项中还可以包括对每个 CP 的限定值，关于限定符的使用将在 5.2.5 中讨论。

在处理证书认证路径时，一个 CP 必须在路径中每个证书中都出现，包括 CA 证书和实体证书，才能被依赖方的应用所接受。

当证书策略扩展项被标记为“关键”时，除了与上述相同的目的，还有一项附加功能：即指明对该证书的使用被限定在所标识的策略之内，也就是说证书认证机构声明该证书必须仅仅用于所列 CP 的范围内。此扩展域意在保护证书认证机构，以免依赖方在适用 CP 条款所规定的目的和方式之外使用证

书，在造成损失时要求证书认证机构赔偿。

5.2.2 策略映射扩展项

策略映射扩展项仅用于 CA 证书。此项允许证书认证机构指明自己域内的某些策略能够被看作与主体 CA 域中某些其他的策略等同。

例如，假设为了促进互操作之目的，ACE 公司与 ABC 公司建立了一个协定，将彼此证书认证机构的公钥进行了交叉认证，以保护它们之间的业务往来。此外，假设两个公司都已经事先存在金融交易保护策略，分别称为 ace-e-commerce 和 abc-e-commerce。可以预见，简单地在两个域间产生交叉证书不能提供必要的互操作性，因为两家公司的应用程序被设置了各自的证书策略，雇员证书中也包含各自的证书策略。一个可能的解决方案是重新设置所有的金融应用程序承认任何一个策略，并重新签发所有的证书，使之在证书策略扩展项中带有两个策略。另一个解决方案是使用策略映射扩展项，这也许易于管理。如果这个域被包含在由 ACE 公司 CA 签发给 ABC 公司的 CA 的交叉证书中，则提供一项声明：ABC 公司的金融交易保护策略(abc-e-commerce)可看作等同于 ACE 公司的金融交易保护策略(ace-e-commerce)。通过包含在颁发给 ABC 公司的交叉证书中的此项声明，ACE 域内的依赖方应用(需要 ace-e-commerce 的对象标识符)，也能够接受、处理和依赖于 ABC 域内所颁发的证书(包含 abc-e-commerce 的对象标识符)。

5.2.3 策略限制扩展项

策略限制扩展项支持两个可选的功能。第一个是证书认证机构有能力要求在证书认证路径的所有后续证书中都需要包含显式 CP 指示。依赖方可以将证书认证路径的起始部分证书当作受信任域的一部分，也就是说，对于所有目的，证书认证机构被信任，因此在认证策略扩展项中不需要任何特定的证书策略。此类证书不需要 CP 的显式指示。但是，当在信任域中的证书认证机构，对信任域外进行认证时，就可以激活此要求，要求在证书认证路径的后续证书中必须出现特定 CP 的对象标识符。

策略限制扩展项的另一个可选功能是证书认证机构禁止证书认证路径中后续证书认证机构进行策略映射的能力。当对域外进行认证时，禁止策略映射功能的设置将有助于控制信任传递所造成的风险，例如，域 A 信任域 B，域 B 信任域 C，但是域 A 不希望被强迫信任域 C。

5.2.4 禁止任意策略扩展项

禁止任意策略扩展项指出了一项限制：自指定 CA 起，在所有后续证书中，任意策略(any-policy)不能视为其他证书策略的显式匹配。该扩展项只能用于 CA 证书，其主要目的在于控制风险，避免因在证书中包含任意策略而使得风险失控。

5.2.5 策略限定符

证书策略扩展项中，对每个 CP 标识符，都可有一个限定符域，用于表达依赖于此策略的额外信息。GB/T 16264.8—2005 标准中既没有规定使用此域的目的，也没有指定这个域的语法。策略限定符类型可以被任何组织注册。

在 RFC 5280 中定义了如下策略限定符类型：

——CPS 指针限定符，包含一个指向由 CA 发布的 CPS、CPS 摘要、RPA 或 PDS 的指针，这个指针为统一资源标识符(URI)格式。

——用户须知限定符，包含一个文本串，该串要在使用证书前显示给订户和依赖方。此文本串可以是一个 IA5 串或者是 BMP 串——GB 13000.1 八位元编码字符集的子集。CA 可以借助于一个过程，要求依赖者知道已公开或接受的适用术语和条件。

策略限定符能够被用来支持通用或者参数化 CP 的定义。除了基本 CP 所提供的，以每张证书为基

础，策略限定符类型能够被定义用来表达附加的特殊策略细节，以补充通用定义。

5.3 认证业务声明

CPS 包含证书生命周期的全部过程，如证书管理（包括发布和存档）、吊销、更新证书或密钥。认证业务声明可以由证书认证机构以公开声明的方式发布，内容包含各种细节，如其可信系统，其在运营操作和支持证书颁发中所采纳业务实践等，其详细程度可有所不同。

一些 PKI 可能不需要创建一个关于其业务实践的彻底而细致的声明。例如，CA 本身就是依赖方，已经知道其服务的本质和可信度。另一些情况下，PKI 只需提供很低保证级别的证书，如果发生泄密，被保护的应用程序只面临很小的风险。在这些情况下，建立 PKI 的组织可能只希望编写订户协议、依赖方协议或将二者结合在一起的协议，依不同 PKI 参与者的角色而定。在这种 PKI 中，该协议可能是 PKI 中唯一充当“业务声明”的文件。因此，该协议也可被视为 CPS，并以 CPS 命名。

同样，由于详细的 CPS 可能包含其系统的敏感信息，CA 可能选择不公布全部 CPS，它可能只公布一个 CPS 摘要。CPS 摘要中可能只包含 CPS 中的部分规定，即 CA 认为与 PKI 参与者相关的部分（如各参与方的责任或证书生命周期的各阶段）。但 CPS 摘要中不会包含全部 CPS 中的敏感信息，这些信息可能会给一个攻击者带来一些关于 CA 操作的有用信息。在本文档中，当使用术语 CPS 时，包括详细的 CPS 和 CPS 摘要（除非另有声明）。

CPS 并不自动构成合同，也没有自动将 PKI 各参与方做自动的合同绑定。当一个文档具有订户或依赖方协议和 CPS 的双重目的时，该文档将可视为合同，并且与常规的订户或依赖方协议具有同等的效力。但是，大多数的 CPS 并不具有这样的双重目的。因此在多数情况下，只有当一个独立的文档在参与方之间创立了合同关系，并且该文档部分或全部地引用了 CPS 时，CPS 才具有合同效力。更进一步，如果某个 PKI 采用的是 CPS 摘要，该 CPS 摘要可以包含在任何适用的订户或依赖方协议当中。

5.4 证书策略与认证业务声明之间的关系

CP 和 CPS 所说明的是依赖方感兴趣的相同主题集合，如在何种程度上、为何种目的信任公钥证书。它们的主要不同在于其条款的针对对象不同。CP 列出了针对这些不同的主题 PKI 所采纳的要求和标准。换句话来讲，CP 的目的在于阐明各参与方必须要达到的要求。与之相应，CPS 则说明 CA 和其他参与者在给定的范围内所采取的过程和控制手段，如何满足 CP 中所提的要求。也就是说，CPS 的目的在于公开各参与方如何实现各自的功能和控制。

CP 和 CPS 的另一点不同在于两类文档所覆盖的范围。因为 CP 是关于要求的声明，所以可作为互操作 PKI 必须要满足的最小操作指南。这样，一个 CP 通常适用于多个 CA、多个组织或多个域。相反，CPS 只适用于单个 CA 或单个组织，通常不作为互操作的工具。只拥有一个 CPS 的 CA 可以支持多个 CP（应用于不同的目的或不同的依赖方团体）。同样，具有不同 CPS 的多个 CA，可以支持相同的 CP。例如，政府可以定义在政府范围内使用的 CP，用以处理保密的人力资源信息。该 CP 将是一个针对政府 PKI 系统范围内各参与方的共同要求的公开声明，并指明适用的应用类别。每个想在此 PKI 内运营 CA 的部门或机构，都将被要求撰写自己的 CPS 来支持此 CP，解释如何满足该 CP 中所提的要求。同时，部门或机构的 CPS 可以支持其他的证书策略。

CP 和 CPS 的第三点不同在于各自条款的详细程度。虽然不同 CPS 的详细程度可能不同，但 CPS 通常会比 CP 更详细。CPS 提供了满足 CP 要求的过程和控制的详细描述，而 CP 则更通用。

CP 和 CPS 的主要不同可总结如下：

——PKI 利用 CP 来提出各参与方必须满足的要求，单个 CA 或组织可用 CPS 来公开它是如何满足 CP 的要求，或如何实现其业务和控制的。

——通过交叉认证、单向认证或其他手段，CP 帮助实现互操作。因此，CP 要覆盖多个 CA。相反，CPS 是关于单个 CA 或组织的声明，其目的不在于实现互操作。

——CPS 通常比 CP 更详细，并且说明了 CA 如何满足一个或多个 CP 中的要求，CA 在这些 CP 下颁发证书。

除了在证书策略扩展项中标明适用 CP 的对象标识符，CA 可以在其颁发的证书中包含关于其 CPS 的引用。实现此目的的标准方式是采用 CP 策略限定符，如 5.2.5 所述。

5.5 CP、CPS 与协议以及其他文档之间的关系

在 PKI 的要求与业务实践的文档中，CP 和 CPS 扮演着核心角色，然而它们并不是 PKI 相关的全部文档。例如订户协议和依赖方协议，在订户和依赖方关于使用证书和密钥对的责任分配中，充当着重要的角色，其中规定了证书颁发、管理和使用的条款和条件。

订户协议、依赖方协议或者包括订户和依赖方两方面内容的协议，也可以作为一个 CPS。在其他的 PKI 中，订户或依赖方协议可通过引用而包括 CP 或 CPS 的部分或全部条款。当然在某些 PKI 中，可能从 CP 和/或 CPS 中提取适用于订户的条款，形成独立的订户协议，而不是通过引用来包括 CP 或 CPS。通过同样的方法，也可形成独立的依赖方协议。形成独立文档的好处在于便于消费者阅读。在某些法律环境下，订户或依赖方被认为是消费者，并受到相关条款的保护。在民法国家的法律体系下，通过引用实现的对 CP 或 CPS 的包含，被引用的 CP 或 CPS 条款可能不被当作对消费者的有效绑定。

CP 和 CPS 可通过引用包含到其他文档中，包括：

——互操作协议（包括 CA 间的交叉认证、单向认证或其他形式的互操作）；

——厂商协议（在该协议下 PKI 厂商同意满足 CP 或 CPS 中设置的标准）；

——PKI 信息披露声明（PDS）。

PDS 与 CPS 摘要具有类似的功能。它是相对较短的文档，只包含了 PKI 或 CA 的部分关键内容。但 PDS 与 CPS 摘要的不同点在于其旨在作为 PKI 全部信息的总结，而不仅仅是 CPS 的浓缩版。进一步而言，PDS 的目的在于提取 PKI 的信息，而不是保护包含在未发布 CPS 中的安全敏感信息，尽管 PDS 也可实现这方面的功能。

正如撰写者可以在一份协议或 PDS 中引用 CP 或 CPS，在 CP 或 CPS 中也可引用其他文档以确定要求。例如，在一个 CP 中可以通过引用一个外部文档来要求证书内容必须满足数字证书格式标准 GB/T 20518—2006。通过引用外部文档，可以在 CP 或 CPS 中加入详细的要求或说明而不必重新设置相关条款。另外，在 CP 或 CPS 中引用文档，也是区分公开信息和安全敏感信息的有效方法。例如，一个 PKI 系统要发布其 CP 或 CPS，但想对 CA 高安全区的构建参数保密，在这种情况下，就可在其 CP 或 CPS 中引用一个外部手册或文档，其中包含了详细的站点构建参数。

在 PKI 文档中，可在 CP 或 CPS 中引用的包括：

——安全策略；

——培训、操作、安装和用户手册；

——适用于 PKI 特定方面的标准文档（如描述 PKI 中所用硬件令牌的保护级别的标准或适用于站点构建的标准）；

——密钥管理方案；

——人力资源指南和雇佣手册（可能会涉及人员安全的某些方面）；

——电子邮件策略（可能会讨论订户和依赖方的责任）。

5.6 条款集说明

条款集是关于业务实践和（或）策略声明的集合，覆盖了一定范围的标准主题，用于使用本框架中所描述的方法来表达 CP 或 CPS，该描述要覆盖出现在第 7 章中的全部主题。这些条款集在第 6 章中有详细的解释。

一个 CP 能够被表达成单独的条款集。

一个 CPS 能够被表达成单独的条款集，每项说明如何满足一个或者多个证书策略的要求，或者作为条款集的一个有组织的集合。例如，CPS 能够被表达成如下内容的组合：

a) CPS 支持的证书策略的列表；

b) 对在 a)中的每个 CP，都有一个条款集，包含关于此 CP 中所未规定的，或留给 CA 做决定的细节声明，该声明用以说明此 CPS 如何满足特定 CP 的要求；

c) 一个条款集，包含关于 CA 认证业务实践的声明，不对应专门 CP。

在 b)和 c)中提供的声明可以增加或者细化适用 CP 的规定，但是不能与该 CP 中的规定冲突。而策略机构可以允许出现不满足 CP 要求的例外，因为 CA 在其 CPS 公布了某种补偿措施，使 CA 可以提供与该 CP 完全一致的保证。

本标准定义了条款集的内容框架，包括如下 9 个部分：

	内容标题
1	引言
2	发布和信息库责任
3	标识与鉴别
4	证书生命周期操作要求
5	设施、管理和操作控制
6	技术安全控制
7	证书、CRL 和 OCSP
8	一致性审计和其他评估
9	业务和法律事务

PKI 可以使用此简易框架来撰写简单的 CP 或 CPS，此外，CA 还可以利用此框架来撰写订户协议、依赖方协议或包括订户和依赖方的其他协议。如果 CA 利用此简易框架来构建一个协议，可以将第 1 部分作为引言，在第 2～8 部分设置各参与方的职责，第 9 部分来详述业务和法律问题。本框架及 6.9 业务和法律问题所列主题顺序，与典型的软件或其他技术协定的主题顺序是相同(或者相近)的。因此，PKI 可以创建一套具有相同结构和主题顺序的核心文档(CP、CPS、订户协议和依赖方协议)，从而简化在这些文档和其他 PKI 相关文档之间的比较和映射。

除了订户协议和依赖方协议，对于其他协议，本简易框架也是有用的。例如，当 CA 想将部分服务外包给 RA 或证书制造机构时，可以利用此框架作为一个检验清单，来撰写 RA 协议或外包协议。同样，两个 CA 也可利用此框架来起草交叉认证、单向交叉认证或其他互操作协议。

本框架的主要部分(如上所述)能够满足简单 CP、CPS、订户协议和依赖方协议的起草者的要求。不仅如此，本框架是可以扩展的，也能够满足复杂 CP 和 CPS 撰写者的要求。特别地，上述每一项都可以进一步分解为子项，每个子项又由多个元素组成。第 6 章提供了对上述每一项及其子项的详细描述，CP 和 CPS 的起草者能够在子项之下再增加新的子项，以满足其特殊 PKI 的要求。

6 条款集内容

6.0 说明

本章对 5.6 条所介绍的简易框架的内容进行扩展，本章所列主题是详细 CP 或 CPS 的候选主题。

尽管此处给出很多主题，但 CP 和 CPS 没有必要对每一个主题包含一个具体的声明。确切而言，对于特定的 CP 或 CPS 不需要或不能公开的项、子项或元素，可以声明“无规定”。在这个意义上，主题列

表可以被看成是 CP 或 CPS 撰写者要考虑的主题一览表。

CP 和 CPS 中应包含每一个项和子项，尽管只是“无规定”。这种撰写方式可避免无意的主题遗漏，在进行策略映射时，有助于比较不同的 CP 或者 CPS。

在一个 CP 当中，可以留下某些项、子项和/或元素而不做声明，规定所需的信息将在策略限定符中或策略限定符所指定的文档中说明。这种 CP 可看作是参数化定义方式，条款集应该引用或者定义所需的策略限定符类型，并且应该指定任何可用的缺省值。

CP 或 CPS 的标题列表见附录 A。

6.1 引言

6.1.0 本项说明

此项标识和介绍条款集，并指明该文档(CP 或 CPS)的目标实体和应用的类别。

6.1.1 概述

该子项对当前撰写文档提供一个概要性介绍，对当前 CP 或 CPS 所适用的 PKI 提供一个大纲。例如，可以设定 PKI 中证书所提供的不同保证等级。根据特定 PKI 的复杂性和范围，可以使用图表的表达方式。

6.1.2 文档名称与标识

该子项提供关于文档的任何适用名称或标识符，包括 ASN.1 对象标识符。文档的名称可能是政府用于安全电子邮件的策略。

6.1.3 PKI 参与者

该子项描述扮演 PKI 中参与者角色的不同实体的身份或类型，它们是：

——证书认证机构，也就是颁发证书的实体。就其所签发的证书而言，一个 CA 是签发 CA；就签发给其的 CA 证书而言，一个 CA 是主体 CA。CA 可以组织成层状结构，一个组织的 CA 为其下属组织运营的 CA 颁发证书，如分支、分公司或大组织下的部门。

——注册机构，也就是为最终用户证书申请者建立注册过程的实体，对证书申请者进行标识和鉴别，发起或传递证书吊销请求，代表 CA 批准更新证书或更新密钥的申请。大组织的下属组织能够扮演 RA 的角色，服务于整个组织，但 RA 也可以独立于 CA 之外。

——订户，即从 CA 接收证书的实体，包括自己拥有 CA 的组织的雇员、银行或证券经纪的客户、拥有电子商务网站的组织、参与 B-to-B 交换的组织、从 CA(为公开用户颁发证书)处接收证书的公众成员。

——依赖方，依赖方的实例包括自己拥有 CA 的组织的雇员(他们接收到其他雇员发来的签名电子邮件)、由电子商务网站购买商品和服务的人、参与 B-to-B 交换的组织(接收到其他组织发来的订单)、与订户(接收了公共 CA 颁发的证书)发生业务往来的个人或组织。依赖方可以是，也可以不是一个给定 PKI 的订户。

——其他参与者，如证书制造机构、信息库服务提供者，以及其他提供 PKI 相关服务的实体。

6.1.4 证书应用

该子项包括：

——所颁发证书适用的证书应用列表或类型，如电子邮件、零售交易、合同、旅游订单；

——所颁发证书限制的证书应用列表或类型。

在 CP 或 CPS 描述不同保证等级的情况下，该子项能够描述对不同保证等级适用或不适用的应用或应用类别。

6.1.5 策略管理

该子项包括负责起草、注册、维护和更新当前 CP 或 CPS 的组织的名称和邮件地址，还包括联系人的姓名、电子邮件地址、电话号码和传真号码。作为一种替代方案，可不指定真实人，在文档中可以定义一个称谓或角色、一个电子邮件别名或其他通用的联系信息。在某些情况下，组织可以声明其联系人，单独或与其他人一起，能够回答关于文档的问题。

进一步，当一个正式或非正式策略机构来负责决定是否允许某一 CA 在一个 PKI 内运营或与之互操作时，则可能会期望它来批准 CA 的 CPS 与策略机构的 CP 相适应。如果是这样，该子项要包括作此决定的实体的名称、电子邮件地址、电话号码、传真号码，以及其他常用信息。在这种情况下，该子项还包括作此决定的过程。

6.1.6 定义和缩写

该子项包括文档中所使用术语的定义一览表，还包括首字母缩略语及其含义一览表。

6.2 发布和信息库责任

此项包括任何针对下列内容的规定：

——运营 PKI 信息库的实体或实体群的标识，如证书认证机构、证书制造机构，或独立信息库服务提供者；

——PKI 参与者发布其业务实践、证书和证书的当前状态的职责，这些责任可能包括应用不同机制使 CP 或 CPS 对公众可用的，标识出存在的但对公众不可用的项、子项和元素，例如：安全控制、清除程序和因为敏感而需要保密的商业信息；

——信息发布的时间和频率；

——对发布信息的访问控制，包括 CP、CPS、证书、证书状态和 CRL。

6.3 标识与鉴别

6.3.0 本项说明

此项描述在颁发证书之前对最终用户证书申请者的身份和(或)其他属性进行审核的过程。对于期望成为 CA、RA 或其他 PKI 运营机构的实体，此项设置鉴别其身份的过程和接受准则。此项还描述如何鉴别密钥更新请求者和吊销请求者。另外，此项还说明命名规则，包括在某些名称中对商标权的承认问题。

6.3.1 命名

该子项包括下列关于订户命名和身份标识的问题：

——分配给主体的名称类型，如 X.500 甄别名、RFC-822 名称、X.400 名称；

——名称是否一定要有意义；

——订户是否能够使用匿名或假名，如果可以，订户可以使用或将被分配给什么样的名称；

——理解不同名称形式的规则，如 X.500 标准和 RFC-822；

——名称是否需要唯一；

——对商标的识别、鉴别及其角色。

6.3.2 初始身份确认

对于每种主体类型(CA、RA、订户或其他参与者)初始注册中的标识和鉴别过程,该子项包含下列元素:

——主体是否以及怎样证明持有与注册公钥相对应的私钥,如在证书请求消息中包含数字签名。

——对订户或参与者[CA、RA、订户(当给组织或由一个组织控制的设备颁发证书时)]的组织身份进行标识和鉴别的要求,如咨询提供组织身份识别服务的数据库,或检查组织的成立文件。

——对于个人订户或代表组织订户的个人进行标识和鉴别的要求,包括:

- 所需文档的类型和(或)身份证号码;
- CA 或 RA 如何基于其所提供的身份文档来鉴别组织或个人的身份;
- 个人是否需要抵达 CA 或 RA 的现场;
- 如何鉴别一个人确实是组织的代表人,如通过察看经过签署的授权文件或公司标识徽章。

——在初始注册中没有验证的订户信息列表。

——对机构的验证涉及确定一个人是否具有特定的权力或许可,包括代表组织获取证书的许可。

——当一个 CA 申请要在一个 PKI 下操作或与之互操作时,该子项包含一个 PKI、CA 或策略机构决定该 CA 是否适合此操作或互操作的准则。这些互操作可能是交叉认证、单向交叉认证或其他形式的互操作。

6.3.3 密钥更新请求的标识与鉴别

针对于密钥更新中对每个实体(CA、RA、订户或其他参与者)标识和鉴别过程,该子项说明下列元素:

——正常密钥更新中对标识和鉴别的要求,如使用当前有效密钥对包含新密钥的密钥更新请求进行签名;

——证书被吊销后密钥更新中对标识和鉴别的要求,如使用原始身份验证相同的流程。

6.3.4 吊销请求的标识与鉴别

该子项描述对每个主体类型(CA、RA、订户或其他参与者)吊销请求的标识和鉴别过程。例如,吊销请求由与被吊销公钥对应的私钥签名,以及请求经 RA 数字签署。

6.4 证书生命周期操作要求

6.4.0 本项说明

此项说明在证书生命周期方面对签发 CA、主体 CA、RA、订户或其他参与者的要求。在每个子项之内,对签发 CA、主体 CA、RA、订户或其他参与者可能需要给予分别考虑。

6.4.1 证书申请

该子项用于说明关于主体申请证书时的要求:

——谁能够提交证书申请,如证书主体或 RA。

——主体在提交证书申请时所使用的注册过程,以及在此过程中各方的责任。例如,主体在哪里产生密钥对,并发送一个证书请求到 RA。RA 验证该请求,并对其签名,然后将其发送给 CA。为了接收证书申请,CA 或 RA 负有建立注册过程的责任。同样,证书申请者负有在其证书申请中提供准确信息的责任。

6.4.2 证书申请处理

该子项用于描述处理证书申请的过程。例如，为了验证证书申请，签发 CA 或 RA 可能要执行标识和鉴别流程，根据这些步骤，CA 或 RA 将可能依照某些准则或者批准或者拒绝该证书申请。最后，该子项要设置 CA 或 RA 必须受理并处理证书申请的时间期限。

6.4.3 证书签发

该子项用于描述下列与证书签发相关的元素：

——在证书签发过程中 CA 的行为，如 CA 验证 RA 签名和确认 RA 的权限，并生成证书的过程；

——CA 签发证书时对订户的通告机制，如 CA 用电子邮件将证书发送给订户或 RA，或者用电子邮件将允许订户到某网站下载证书的信息告知用户。

6.4.4 证书接受

该子项说明下列内容：

——申请者正式接受证书的行为。这种行为可以包括表示接受的确认性步骤、暗示接受的操作、否定证书或其内容失败。例如，如果 CA 在一定时间内没有收到订户的任何通知，即可认为订户接受了证书；订户可能发送一个经过签名的消息，明示已接受证书；订户可能发送一个经过签名的消息拒绝该证书，在消息中有拒绝的理由并指向证书中的某些字段，而对有关字段的指认是不正确或不完整的。

——CA 对证书的发布，例如 CA 可以将证书发布到 X.500 或 LDAP 信息库。

——CA 在颁发证书时对其他实体的通告，例如，CA 可能发送证书到 RA。

6.4.5 密钥对和证书的使用

该子项用于描述与密钥对和证书使用相关的责任，包括：

——与订户使用其私钥和证书相关的订户责任。例如，订户可能被要求只能在恰当的应用范围内使用私钥和证书，这些应用在 CP 中设置，并且与有关的证书内容相一致（如密钥用途字段）。私钥和证书的使用要遵从于订户协议的规定，订户只有在接受了相关证书之后才能使用其私钥，并且在证书到期或被吊销之后，订户必须停止使用私钥。

——与使用订户公钥和证书相关的依赖方责任。例如，依赖方只能在恰当的应用范围内依赖于证书，这些应用在 CP 中设置，并且与有关的证书内容相一致（如密钥用途扩展）。成功地完成公钥操作依赖于证书的条件，有责任使用 CP/CPS 中所要求或允许的一种机制来检查证书状态，和同意依赖方协议中的有关规定依赖于证书的条件。

6.4.6 证书更新

该子项用于描述下列与证书更新相关的元素。证书更新的意思是在不改变证书中订户或其他参与方的公钥或其他任何信息的情况下，为订户签发一张新证书：

——进行证书更新的条件，如证书已到期，但策略允许继续使用相同的密钥对；

——谁可以请求更新，如订户、RA 或 CA 可以自动更新订户证书；

——为签发新证书，CA 或 RA 处理更新请求的过程，如使用令牌，比如口令，来重新鉴别订户，或使用与原始签发证书相同的过程；

——颁发新证书给订户时的通告；

——接受更新证书的行为；

——CA 对更新证书的发布；

——CA 在颁发证书时对其他实体的通告。

6.4.7 证书密钥更新

针对订户或其他参与者生成一对新密钥并申请为新公钥签发一个新证书，该子项描述下列元素：

——证书密钥更新的条件，如因私钥泄漏而吊销证书之后，或者证书到期并且密钥对的使用期也到期之后；

——谁可以请求证书密钥更新，如订户；

——为签发新证书，CA 或 RA 处理密钥更新请求的过程；

——颁发新证书给订户时的通告；

——接受密钥更新证书的行为；

——CA 对密钥更新证书的发布；

——CA 在颁发证书时对其他实体的通告。

6.4.8 证书变更

该子项描述的下列元素，针对于因为改变证书中除订户公钥之外的信息而签发新证书的情形：

——证书变更的条件，如名称改变、角色改变、因重组而造成的 DN 改变；

——谁可以请求证书变更，如订户、人力资源部门或 RA；

——为签发新证书，CA 或 RA 处理证书变更请求的过程，如采用与原始证书签发相同的过程；

——颁发新证书给订户时的通告；

——接受变更证书的行为；

——CA 对变更证书的发布；

——CA 在颁发证书时对其他实体的通告。

6.4.9 证书吊销和挂起

该子项说明下列内容：

——证书挂起的条件和证书必须吊销的条件，例如订户雇佣期满、密码令牌丢失或怀疑私钥泄漏；

——谁可以请求吊销证书，例如对最终用户证书而言，订户、RA 或 CA；

——证书吊销请求的流程，如由 RA 签署的消息、由订户签署的消息或由 RA 电话通知；

——订户可用的宽限期，订户必须在此时间内提出吊销请求；

——CA 必须处理吊销请求的时间；

——为检查其所依赖证书的状态，依赖方可以或必须使用的检查机制；

——如果使用 CRL，其发布频率是多少；

——如果使用 CRL，产生 CRL 并将其发布到信息库的最大延迟是多少（也就是在生成 CRL 之后，再将其发布到信息库中所用的处理和通信相关最长延迟）；

——在线证书状态查询的可用性，例如 OCSP 和可提交状态查询的 Web 网站；

——依赖方执行在线吊销状态查询的要求；

——吊销信息的其他可用传播途径；

——当因为私钥泄漏而造成证书吊销或挂起时，上述规定的不同之处（与其他原因造成吊销或挂起相对）；

——证书挂起的条件；

——谁可以请求证书挂起，例如对于最终用户证书而言，订户、人力资源部门、订户的上级，或者 RA；

——请求证书挂起的过程，如由订户或 RA 签署的消息，或由 RA 电话请求；

——证书挂起的最长时间。

6.4.10 证书状态服务

该子项说明依赖方可用的证书状态查询服务，包括：

——证书状态查询服务的操作特点；

——这些服务的可用性，以及服务不可用时的适用策略；

——这些服务的其他可选特征。

6.4.11 订购结束

该子项说明订户结束订购 CA 的服务时所使用的过程，包括：

——结束订购时的证书吊销（依赖于结束订购是因为证书到期，还是因为服务终止，可能会有所不同）。

6.4.12 密钥托管与恢复

该子项包含下列元素，说明与私钥托管和恢复相关的策略和业务实践（通过 CA 或其他可信第三方）：

——包含密钥托管和恢复的策略及实践的文档标识，或此类策略和实践一览表；

——包含会话密钥封装和恢复的策略及实践的文档标识，或此类策略和实践一览表。

6.5 设施、管理和操作控制

6.5.0 本项说明

此项描述非技术安全控制（即物理、过程和人员控制），签发 CA 使用这些控制手段来安全地实现密钥生成、主体鉴别、证书签发、证书吊销、审计和归档等功能。

此项也用于定义信息库、主体 CA、RA、订户和其他参与者的非技术安全控制，主体 CA、RA、订户和其他参与者的这些非技术控制手段可能会相同、相近或非常不同。

对证书的可信而言，这些非技术安全控制很重要，因为缺乏安全控制可能会使 CA 在创建证书或 CRL 时混入错误信息，或者 CA 的私钥泄漏。

在每个子项当中，通常对每个实体类型都要给予分别考虑，即签发 CA、信息库、主体 CA、RA、订户和其他参与者。

6.5.1 物理控制

该子项当中，描述了针对放置实体系统的机房设施的物理控制，可以包括下列主题：

——场所区域和建筑，如对高安全区的建筑要求，使用带锁的房间、屏蔽室、保险柜、橱柜；

——物理访问，也就是从场所的一个区域到另一个区域或进入安全区的访问控制机制，如将 CA 的运营安置在有门卫把守或安全警报的安全计算机机房内，从一个区域到另一个区域的移动需要使用令牌、生物识别设备和（或）访问控制列表；

——电力和空调；

——水患防治；

——火灾预防和保护；

——介质存储，例如需要在不同的场所利用备份介质进行存储，该场所在物理上是安全的，能够防止水灾和火灾的破坏；

——废物处理；

——异地备份。

6.5.2 过程控制

该子项中，描述定义可信角色的要求，以及各个角色的责任。可信角色包括系统管理员、安全官员和系统审计员等。

对于规划出每项任务，要声明完成该项任务所需的每个角色人员数，还可以定义对每个角色的标识和鉴别要求。

此项还可能包括按照角色而定义的责任分离，这些角色不能由相同的人承担。

6.5.3 人员控制

该子项说明下列内容：

——对于充当可信角色或其他重要角色的人员，其需要具备的资格、经历和无过失证明要求，例如对这些职位的候选者所需具备的信任证明、工作经历和官方凭证。

——在雇佣充当可信角色或其他重要角色的人员时所需背景审查程序，这些角色可能要求调查其犯罪记录、档案，以及参加者需要持有为雇佣特定人员而制作的附加凭证。

——雇佣人员后对每个角色的培训要求和过程。

——在完成原始培训后对每个角色的再培训周期和过程。

——在不同角色间的工作轮换周期和顺序。

——对下列行为的处罚：未授权行为、未授予的权力使用和对系统的未授权使用，从而破坏全体人员过程的可追踪性。

——对独立合约人而非实体内部雇员的控制，包括：

- 对缔约人员的责任要求；
- 合同要求，包括对由缔约人员行为造成的损失的赔偿；
- 对缔约人员的审计和监控；
- 对缔约人员的其他控制。

——对全体人员在初始培训、再培训和其他过程中使用的文档。

6.5.4 审计日志程序

该子项用于描述事件日志和审计系统，实现该系统的目的在于维护一个安全的环境。包括下列元素：

——记录事件的类型，如证书生命周期操作、对系统的访问企图和对系统的请求。

——处理或归档日志的周期，如每星期、在报警或异常事件之后，或审计日志已满时。

——审计日志的保存期。

——审计日志保护：

- 谁可以浏览审计日志，如只能是审计管理员；
- 对审计日志更改的保护，如要求没有人能够更改或删除审计记录或者只有审计管理员才能够删除审计文件；
- 对审计日志删除的保护。

——审计日志备份程序。

——审计日志收集系统是在实体的内部还是外部。

——是否对触发事件的主体进行通告。

——脆弱性评估，如审计数据的运行工具破坏系统安全性的潜在可能。

6.5.5 记录归档

该子项用于描述通用的记录归档(或记录保留)策略,包括:

——归档记录的类型,例如所有审计数据、证书申请信息、支持证书申请的文档。

——档案的保存期。

——档案的保护:

- 谁可以浏览档案,如要求只有审计管理员才能浏览;
- 对档案更改的保护,如将数据保存在只能一次写入的介质中;
- 对档案删除的保护;
- 对档案保存介质老化的保护,如要求周期性地将数据保存到新的介质;
- 对硬件、操作系统和其他软件废止的保护,如将硬件、操作系统和(或)其他软件作为归档的一部分,以能够在后期访问和使用归档数据。

——档案备份程序。

——对记录加盖时间戳的要求。

——档案收集系统是内部还是外部。

——获得和验证档案信息的程序,如由两个人分别来保留归档数据的两个拷贝,并且为了确保档案信息的准确,需要对这两个拷贝进行比较。

6.5.6 CA 密钥更替

该子项描述 CA 产生新密钥,并将新的公钥提供给 CA 用户的过程。此过程可以与产生当前密钥的过程相同,而且可以用旧密钥为新密钥签发证书。

6.5.7 损害和灾难恢复

该子项描述与密钥损害或灾难事件相关的通告和恢复过程要求,对下列内容需要分别考虑:

——适用事件和损害的列表,以及对事件的报告和处理过程。

——对计算资源、软件和(或)数据被破坏或怀疑被破坏的恢复过程,此过程包括如何重建一个安全环境,哪些证书要吊销,实体的密钥是否被吊销,如何将新的实体公钥提供给用户,以及如何为主体重新发证。

——对实体私钥损害的恢复过程,此过程包括如何重建一个安全环境,如何将新的实体公钥提供给用户,以及如何为主体重新发证。

——自然或其他灾难后实体的业务连续性能力,此能力包括远程热备站点对运营的恢复,也可以包括在灾难发生后到重建安全环境前,或者在原始站点,或者在远程站点保护其设施的程序。例如,防止从遭地震破坏的站点偷窃敏感信息的程序。

6.5.8 CA 或 RA 终止

该子项描述与 CA 或 RA 终止和终止通告相关的过程的要求,包括 CA 或 RA 档案记录管理者的身份问题。

6.6 技术安全控制

6.6.0 本项说明

该项用于定义签发 CA 为保护其密钥和激活数据(如 PIN 码、口令字或手持密钥共享)而采取的安全措施。该项也用于对信息库、主体 CA、订户和其他参与者进行限制,以保护他们的私钥、私钥激活数

据和关键安全参数。安全密钥管理十分重要，以确保所有的秘密密钥、私钥和激活数据都在保护之中，并且只被授权的人员使用。

该项也描述签发 CA 使用的其他技术安全控制，用以安全地实现密钥生成、用户鉴别、证书注册、证书吊销、审计和归档等功能。安全控制包含生命周期安全控制(包括软件开发环境安全，可信的软件开发方法论)和操作安全控制。

该项还可用来定义其他的用于信息库、主体 CA、RA、订户和其他参与者的技术安全控制。

6.6.1 密钥对的生成和安装

对于签发 CA、信息库、主体 CA、RA 和订户，都需要考虑密钥对的生成和安装。对其中的每类实体，都需要回答下列问题：

a) 由谁来生成实体的公、私钥对？是订户、RA 还是 CA。进一步，密钥对的生成是如何实现的？由硬件还是软件生成？

b) 私钥是如何安全地提供给实体的？可能的方法包括实体自生成从而自动拥有、用物理的方式将私钥传递给实体、邮寄保存私钥的令牌，或是通过 SSL 会话传递。

c) 如何将实体公钥安全地提供给证书认证机构？可通过在线 SSL 会话或经 RA 签署的消息。

d) 对于签发 CA，如何将 CA 公钥安全地提供给潜在的依赖方？可能的方式包括用人工将公钥发送给依赖方、用物理方式邮寄一份拷贝给依赖方，或通过 SSL 会话传递。

e) 密钥长度是多少？如 RSA 的模长是 1 024 比特、DSA 的大素数是 1 024 比特。

f) 由谁来生成公钥参数？在生成密钥时是否对参数的质量进行检查？

g) 密钥的使用目的是什么？或者密钥的使用目的限制在什么范围内？对于 GB/T 16264.8—2005 证书，这些目的需要映射到第三版证书的密钥用途标志位。

6.6.2 私钥保护和密码模块工程控制

对于签发 CA、信息库、主体 CA、RA 和订户，都要考虑私钥保护和密码模块的要求。对其中的每个实体类型，都可能要回答下列问题：

a) 如果有，对用来产生密钥的模块需要哪些标准？密码模块可以由硬件、软件、固件或其组合构成。例如，被基础设施认证的密钥是否需要由符合国家有关密码标准的模块产生？如果是，模块需要达到的级别是多少？是否存在与密码模块相关的其他工程或控制，如密码模块边界的标定、输入/输出、角色和服务、有限状态机、物理安全、软件安全、操作系统安全、算法一致性、电磁兼容性和自检测等。

b) 私钥是否由 M 选 N 多人控制？如果是，N 和 M 是多少(两人控制是一个特殊的例子，其中 $N=M=2$)？

c) 私钥是否被托管？如果是，谁是托管机构，密钥以什么形式托管(如明文、密文、分割密钥)，并且托管系统的安全控制如何？

d) 私钥是否备份？如果是，谁是备份机构，私钥以什么形式备份(如明文、密文、分割密钥)，并且备份系统的安全控制如何？

e) 密钥是否归档？如果是，谁是归档机构，私钥以什么形式归档(如明文、密文、分割密钥)，并且归档系统的安全控制如何？

f) 在什么条件下私钥可以从密码模块导入或导出？谁能够执行此类操作？在导入/导出时私钥的形式怎样(如明文、密文、分割密钥)？

g) 私钥如何被保存在模块中(如明文、密文、分割密钥)？

h) 谁能激活(使用)私钥？为激活私钥必须执行哪些操作(例如登录、上电、提供 PIN、插入令牌/钥匙、自动等)？一旦密钥被激活，密钥是活动无限长的时间、只活动一次，还是活动于一个定

义的时间段？

i） 谁能够冻结私钥以及如何做？冻结私钥的方式包括退出、切断电源、移开令牌/钥匙、自动冻结或者有效期届满。

j） 谁能够销毁私钥以及如何做？销毁密钥的方式包括交出令牌、销毁令牌或者重写密钥。

k） 给出密码模块在下列方面的指标：密码模块边界的标定、输入/输出、角色和服务、有限状态机、物理安全、软件安全、操作系统安全、算法一致性、电磁兼容性和自检测。指标可以以与某标准兼容的方式给出，如符合国家有关标准。

6.6.3 密钥对管理的其他方面

对于签发CA、信息库、主体CA、RA、订户和其他参与者，还要考虑密钥管理的其他方面。对其中的每个实体类型，都需要回答下列问题：

a） 公钥是否归档？如果归档，谁是归档机构以及归档系统的安全控制如何？进一步，还需将什么软件和硬件作为档案的一部分一同保存，以能够在日后使用公钥？

注：该子项并不限于要求或描述对归档数据使用数字签名，还包括当档案需要防止篡改时其数字签名的完整性控制。数字签名并不提供对篡改的保护，或保护数据的完整性，它们仅仅验证数据的完整性。并且，归档期可能会长于密码分析期，在该时期内利用公钥能够验证应用于归档数据的任何数字签名。

b） 颁发给订户的证书的操作期是多少？订户密钥对的使用期或生命期又是多少？

6.6.4 激活数据

激活数据指的是用以操作私钥或包含私钥的密码模块所需的数据值，如PIN、口令字或私钥的一部分（使用某种密钥分割方案），而不是整个私钥。对激活数据的保护是为了防止对私钥的非授权使用，签发CA、主体CA、RA和订户都需要考虑保护激活数据。这些考虑可能需要说明激活数据的整个生命周期，从产生到归档和销毁。对每个实体类型（签发CA、信息库、主体CA、RA、订户和其他参与者），所有问题（6.6.1～6.6.3）都要回答，只是关于激活数据而不是关于密钥。

6.6.5 计算机安全控制

该子项用来描述计算机安全控制，例如使用可信计算基的概念、自主访问控制、标签、强制访问控制、对象重用、审计、标识与鉴别、可信路径、安全测试和渗透测试，也可以说明产品的安全保证。

可以要求计算机系统需要达到一定的安全级别，分级标准可以基于国家颁布的计算机信息系统安全等级保护要求中对PKI公钥基础设施的技术要求、可信系统评估标准、加拿大可信产品评估准则、欧洲信息技术安全评估准则或信息技术安全评估通用准则。该子项也能说明对下列事宜的要求：产品评估分析、测试、描述、产品认证，和/或与产品认可相关的活动。

6.6.6 生命周期技术控制

该子项描述系统开发控制和安全管理控制。

系统开发控制包括：开发环境安全、开发人员安全、产品维护期的配置管理安全、软件工程实施、软件开发方法论、模块化、层次化、使用容错设计和实现技术（如防御性编程），以及开发工具安全。

安全管理控制包括执行工具和程序来保证操作系统和网络符合设置的安全，这些工具和程序包含检查安全软件、固件和硬件的完整性来确保它们正确运行。

该子项还可以说明生命周期安全等级，例如基于可信软件开发方法学级别Ⅳ和Ⅴ、独立的生命周期安全控制审计和能力成熟度模型。

6.6.7 网络安全控制

该子项说明与网络安全相关的控制，如防火墙等。

6.6.8 时间戳

该子项说明与不同数据使用时间戳相关的要求或业务实践，还可声明时间戳应用是否需要使用可信时间源。

6.7 证书、CRL 和 OCSP

6.7.0 本项说明

该项用于说明证书格式、CRL 和(或)OCSP 格式，包括描述、版本号和扩展项的使用。

6.7.1 证书

该子项说明下列主题(也可能通过引用一个独立的规范定义，如 RFC5280)：

——支持的版本号；

——所使用的证书扩展项及其关键性；

——密码算法对象标识符；

——CA、RA 和订户所使用的名称形式；

——所使用的名称限制及其形式；

——证书策略对象标识符；

——策略约束扩展项的使用；

——策略限定符的语法和语义；

——对关键证书策略扩展项的处理规则。

6.7.2 CRL

该子项说明下列主题(也可能通过引用一个独立的规范定义，如 RFC5280)：

——CRL 支持的版本号；

——CRL 和 CRL 入口扩展项及其关键性。

6.7.3 OCSP

该子项说明下列主题：

——OCSP 版本号；

——所使用的 OCSP 扩展项及其关键性。

该子项也可通过引用一个独立的规范(如 GB/T 19713—2005)来说明。

6.8 一致性审计和其他评估

该项说明下列问题：

——评估所涵盖的主题和(或)评估的方法列表。

——依照某一 CP 或 CPS，对每个实体进行一致性审计或其他评估的频率，或者是引发评估事件的条件。可能的情况如每年一次的年审，作为允许实体运行的一个运营前条件的评估，或一个疑似或真实安全泄密后的调查。

——关于执行审计或其他评估的人员的身份和资质。

——评估者与被评估实体之间的关系，包括评估者的独立程度。

——对评估中出现的不足所采取的措施，例如暂停运营直到错误得到改正，吊销被评估实体的证书，变换人员，触发特殊调查或增加后续一致性评估频率，宣布被评估实体的损失等。

——谁有权察看审计结果(如被评估实体、其他参与者、公众),由谁提供(评估者或被评估实体),它们之间如何通信。

6.9 业务和法律事务

6.9.0 本项说明

该项涵盖了一般性的商务和法律问题。本框架的 9.1 和 9.2 讨论不同服务的费用问题,和各参与方为了保证资源维持运营,针对参与方的诉讼、争议的审判和解决提供支付所需要承担的财务责任。该项的其余内容通常与法律问题相关。

自本框架的 9.3 开始,其标题顺序与典型的软件许可协议或其他技术协议的标题顺序相同或相近。因此,本框架不仅适用于 CP 和 CPS,还可用于其他 PKI 相关的协议,尤其是订户协议和依赖方协议。如此安排顺序旨在帮助律师审阅 CP、CPS 和依据本框架而编写的文档。

关于此项中的许多法律子项,CP 或 CPS 的撰写者可以将其包含在文档的限定条件中,使其直接作用于订户或依赖方。例如,在一个 CP 或 CPS 中可以设定订户和依赖方的责任范围。当 CP 或 CPS 本身作为一个合同或作为合同的一部分时,限定条件中所包含的内容就变得很有意义。

但在其他情况下,CP 或 CPS 并不作为合同或合同的一部分。相反地,可设定通过另外的文档使 CP 或 CPS 的条款或条件作用于有关方,这些文档可能包括相关的协议,如订户协议或依赖方协议。在这种情况下,CP 的撰写者可能会编写一个 CP,要求其某些法律规定和条件要出现(或不出现)在这些相关协议当中。例如,一个 CP 可能包含一个子项,声明某些责任限制条款必须出现在 CA 订户协议和依赖方协议中。再比如,一个 CP 可包括一个子项,禁止使用包含与该 CP 规定不符的 CA 责任限制的订户或依赖方协议。CPS 的撰写者可以利用法律子项来公布某些限定条件出现在 CA 所使用的相关订户、依赖方或其他协议中。例如,在一个 CPS 中可以说明 CA 使用相关的订户或依赖方协议以适用于某特定条款来限定责任。

6.9.1 费用

该子项包括 CA、信息库拥有者或 RA 收取费用的条款,如:

——证书颁发或更新费用;

——证书访问费用;

——吊销或状态信息访问费用;

——其他服务的费用,如对相关 CP 或 CPS 提供访问服务;

——退款规定。

6.9.2 财务责任

该子项包括与 CA、RA 和其他提供认证服务的参与者的可用资源相关的要求或公开声明,这些资源是其运营 PKI 的责任的必要支撑,并且在其运营发生错误并造成损失时提供赔付和解决办法。这些规定包括:

——该参与者对其他参与者所负有的责任保险范围声明;

——该参与者利用其他资源来支持其运营和对潜在责任进行赔付的声明,可以以 PKI 正常运营和处理可能意外事件所需的最少财产级别的方式表达,如组织收支平衡表上的财产、保证书、信用证明、在某种条件下要求赔偿的权力契约;

——该参与者拥有对使用其 PKI 的其他参与者提供首方责任险或担保保护的程序的声明。

6.9.3 业务信息保密

该子项包括与各参与方在进行相互通信时对保密商业信息问题进行处理的相关规定,如商业计划、

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.

GB/T 26855—2011

中 华 人 民 共 和 国
国 家 标 准
**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**
GB/T 26855—2011
*
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.gb168.cn
服务热线:010-68522006
2011 年 11 月第一版
*
书号:155066·1-43762

GB/T 26855-2011