ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29767—2013

信息安全技术　公钥基础设施 桥CA体系证书分级规范

Information security techniques—Public key infrastructure—Bridge Certification Authority leveled certificate specification

2013-09-18 发布　　2014-05-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

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、中国科学院信息安全国家重点实验室。

本标准主要起草人:吴亚非、任金强、罗红斌、张凡、高能。

引　言

本标准对桥 CA 证书策略的安全保证级别规定了分级标准，将桥 CA 体系证书划分为四个应用级别和测试级共五个等级，并说明了对各级别的技术要求。四个应用级别是：初级、基本级、中级、高级，其安全级别逐次增高。测试级证书是用于交叉认证测试的证书。

本标准参照 RFC 3647，对各级别的证书策略做出了明确说明，用以指导设计者如何设计和实现相应级别的证书策略。每个级别针对九个方面的不同内容做出了要求，保证了证书策略从初级到高级，其安全程度随之递增，其适应的安全环境也随之更加严格。

信息安全技术　公钥基础设施
桥 CA 体系证书分级规范

1　范围

本标准规定了桥 CA 体系证书安全等级划分。

本标准适用于桥 CA 体系证书策略的设计与实现。桥 CA 系统的研制、开放、测试和产品采购也可参照使用。

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/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 20518—2006　信息安全技术　公钥基础设施数字证书格式

RFC 3647　互联网 X.509 公钥基础设施：证书策略和证书运行框架(Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework)

3　术语和定义

GB/T 16264.8—2005 界定的以及下列术语和定义适用于本文件。

3.1

公钥基础设施　public key infrastructure

支持公钥管理体制并提供鉴别、加密、完整性和不可否认性服务的基础设施。

3.2

交叉认证　cross certification

两个 CA 之间建立信任关系，以使它们可以互相信任和依赖任何一方发放的证书的过程。

3.3

交叉认证协议备忘　cross-certification memorandum of agreement

确定两个 CA 之间关系、规定了双方互通后享有的信任程度的协议。

3.4

证书策略　certificate policy

一组指定的规则，指出证书对具有公共安全要求的特定团体和/或应用的适用范围。

3.5

实体 CA　entity CA

要求帮助交叉认证的具体根 CA。

3.6

订户　subscriber

从 CA 接收数字证书的实体。

3.7

激活数据　activation data

用于操作密码模块所必需的、并且需要被保护的数据值。

3.8

符合性审计　compliance audits

定期对物理控制、密钥管理控制、鉴证执行等情况进行审查，以确定实际发生情况是否与预定的标准、要求一致，并根据审查结果采取行动。

4　缩略语

下列缩略语适用于本文件。

CA：证书认证机构（Certification Authority）

CARL：证书认证机构撤销列表（Certification Authority Revocation List）

CP：证书策略（Certificate Policy）

CPS：认证业务说明（Certification Practice Statement）

CRL：证书撤销列表（Certificate Revocation List）

OID：对象标识符（Object Identifier）

PKI：公钥基础设施（Public Key Infrastructure）

RA：注册机构（Registration Authority）

5　证书安全保证等级

5.1　概述

桥 CA 体系证书安全保证等级的分级是基于桥 CA 的证书策略要求，结构遵循 RFC 3647。根据证书策略，桥 CA 体系证书分为测试级和四个应用安全保证等级，四个应用安全保证等级包括初级、基本级、中级和高级。五个等级的证书都包括“导引”“信息发布与管理”“身份标识与鉴别”“证书生命周期操作要求”“认证机构设施、管理和操作控制”“技术安全控制”“证书、证书撤销列表和在线证书状态协议”“符合性审计和其他评估”“其他商务和法律问题”九个方面，主要根据该级证书所处的安全环境进行规范。不同级别的安全环境对证书安全的要求不同，环境越危险，所需证书的安全级别越高，反之亦然。本标准附录 A 对可审计事件在不同级别的要求进行了规范，附录 B 对各级别证书的不同证书策略要求作了总结。

5.2　测试级

5.2.1　导引

测试级证书应该拥有一个唯一的测试级证书策略 OID。

使用测试级证书策略的证书没有安全保护目标，只用于测试，不能被用于其他任何事务。

使用测试级证书策略的证书只能被用于实体 CA 与桥 CA 之间的交互测试中，不能被用于其他任何目的。此级证书策略不对安全做出任何保证。

5.2.2　信息发布与管理

无特殊要求。

5.2.3 身份标识与鉴别

测试级证书策略要求在备忘录中商定以下内容：

a) 测试级证书使用的主体名，具体要求依赖于具体的测试环境；

b) 申请证书时，测试级策略对申请者的身份鉴别方法，取决于具体的测试环境；

c) 测试级证书密钥更新时的身份鉴别方法，取决于具体的测试环境。

5.2.4 证书生命周期操作要求

测试级证书策略要求在备忘录中商定以下内容：

a) 申请证书时，申请者需要将证书公钥和其身份绑定后，安全递交给 CA。测试级证书策略要求这种绑定递交方法在备忘录中商定；

b) 在订户申请证书前对订户的要求；

c) 每隔一段时间，CA 系统都需要发布周期性的 CRL 和 CARL，在测试级证书策略中，发布 CRL 和 CARL 的周期应该在备忘录中商定。如果发现某个证书的私钥丢失或者安全性受到威胁，则 CA 系统在撤销该证书后的一定时间内应发布一次 CRL 或 CARL，这段时间的长度也需要在备忘录中商定。

5.2.5 认证机构设施、管理和操作控制

测试级证书策略要求在备忘录中商定以下内容：

a) CA 系统应产生并保存所有事件的安全审计日志，测试级证书策略要求该日志的保存期应在备忘录中商定；

b) 每隔一段时间，安全审计日志需要提供给管理者进行审查，测试级证书策略要求在备忘录中商定审查的周期以及审查的要求；

c) CA 系统需要对其自身的一些数据进行记录归档，测试级证书策略要求归档的内容及归档保存时间都在备忘录中商定；

d) CA 系统的物理安全要求；

e) 实体 CA 和桥 CA 的角色分配要求。

5.2.6 技术安全控制

订户所使用的密码设备和密钥管理应符合国家密码管理部门的相关要求。

CA 给订户发放的证书应使用密钥用途扩展项表明其密钥用途，给用户分别发放双证书：签名证书和加密证书。

桥 CA、实体 CA 和 RA 所使用的密码设备和密码算法应符合国家密码管理有关政策。

5.2.7 证书、证书撤销列表和在线证书状态协议

无特殊要求。

5.2.8 符合性审计和其他评估

对实行测试级证书策略的 CA 和 RA 的审计周期不做要求。

5.2.9 其他商务和法律问题

无特殊要求。

5.3 初级

5.3.1 导引

初级证书应该拥有一个唯一的初级策略 OID。

初级证书是所有应用级别中等级最低的证书，使用初级策略的证书的安全保护目标仅仅是在个人身份上提供最低等级的安全保证，例如保证签名消息的完整性。不应被用于任何组织的数据安全，如公司、团体等；不应被用于任何身份的标识与鉴别；也不应用于信息加密。

初级证书只能使用于极少出现恶意违法攻击行为的环境中，在该环境下的人员都是可以信赖的，其使用的程序也具有极高的安全等级。这种环境对其所使用的证书安全级别要求很低，只要求证书可以保证在个人身份上最低等级的安全。但初级证书不适合用于需要身份鉴别的事务中，除非根本无法得到更高级别的证书。

5.3.2 信息与发布管理

无特殊要求。

5.3.3 身份标识与鉴别

当初级证书使用了可选主体名扩展项且标志其为关键时，可以使用空主体名，否则证书应提供一个非空的主体名。

初级证书策略对主体名的具体内容不做具体要求，只要求其保证唯一性。例如用户可以使用一个大整数作主体名，只要该大整数在命名空间里是唯一的。

申请证书时，初级证书策略要求申请者提供个人身份证号码，申请人可以用他的电子邮件申请接收证书。

当订户需要密钥更新时，可以凭借现有私钥的签名来进行身份鉴别。

5.3.4 证书生命周期操作要求

申请证书时，申请者需要将证书公钥和其身份绑定后，递交给 CA。初级证书策略不对公钥和身份的绑定递交方法做具体要求。

初级证书策略对 CRL 和 CARL 的发布时间和频率不做要求。

5.3.5 认证机构设施、管理和操作控制

CA 系统应产生并保存表 A.1 中为初级证书策略规定的审计事件的安全审计日志，初级证书策略要求该日志的保存期不得短于 5 年。

每隔一段时间，安全审计日志需要提供给管理者进行审查，初级证书策略不对审查的周期做要求，只在管理者认为需要时进行审查。

CA 系统需要对其自身的一些数据进行记录归档，初级证书策略要求至少对以下事件进行记录归档：

a) 实体 CA 或桥 CA 的授权和鉴定；
b) CA 系统的 CPS；
c) 合同义务；
d) 系统和设备的配置；
e) 系统配置的修改和升级；
f) 收到的证书申请消息的内容；

g） 签发的所有证书；

h） CA 密钥的更新记录；

i） 所有的审计日志。

记录归档的保存期不得短于 5 年。

初级证书策略对 CA 系统的角色分配不做要求，对角色的认证也不做要求。

5.3.6 技术安全控制

订户所使用的密码设备和密钥管理应符合国家密码管理部门的相关要求。

CA 给订户发放的证书应使用密钥用途扩展项表明其密钥用途，给用户分别发放双证书：签名证书和加密证书。

桥 CA、实体 CA 和 RA 所使用的密码设备和密码算法应符合国家密码管理部门的要求。

如果订户的签名证书中所声明的安全保证级别为初级或者声明与桥 CA 的初级相对应，则证书对应的签名私钥可以进行备份和拷贝，但只能在用户的控制下进行。

实体 CA、桥 CA 和订户所使用的激活数据，都应使用一定的访问控制方法进行保护，其受保护的强度应与被其激活的私钥的保护强度相同。初级安全策略允许用户自行选择他使用的激活数据。

5.3.7 证书、证书撤销列表和在线证书状态协议

实体 CA 颁发的初级证书的扩展项应符合 GB/T 20518—2006 的规范。

5.3.8 符合性审计和其他评估

对实行初级证书策略的 CA 和 RA 的审计周期不做要求。

5.3.9 其他商务和法律问题

无特殊要求。

5.4 基本级

5.4.1 导引

基本级证书应拥有一个唯一的基本级证书策略 OID。

使用基本级策略的证书的安全保护目标是保护非重要数据的安全，例如公司的内部公开文件。其保护的数据可以为许多人所知，即使泄漏了，带来的后果和危害并不大。

使用基本级证书策略的证书可以在存在一些恶意违法攻击的环境中使用，但这些恶意行为不应该是环境中的主流现象。在这种环境中，数据受攻击的概率较低，即使被攻击了，带来的危害也并不高，因此，此种环境对证书的安全性要求相对较低，只要求其能保证在较弱攻击下的安全性。例如：此级证书可以用于访问私有信息的环境，在此环境中可能出现妄图非法访问这些信息的行为，但这种可能性并不高。基本级证书策略可假定用户都不大可能是恶意攻击者。

5.4.2 信息发布与管理

无特殊要求。

5.4.3 身份标识与鉴别

基本级证书应拥有一个非空的主体名，另外，如果可选主体名扩展被标记为非关键，则该扩展可以为空。

基本级证书策略对主体名的具体内容不做要求，只要保证唯一性。例如用户可以使用一个大整数作主体名，只要该大整数在命名空间里是唯一的。

申请证书时，基本级证书策略要求申请者证明其身份应满足下列要求：

a) 身份鉴别采用由申请者个人亲自到 RA 处进行鉴别的方法或者通过申请者机构人事负责人、或其他有关负责人的证明进行鉴别；

b) 若是非申请者亲自到场，则证明材料应有有关部门负责人的手写签名，此时可用邮寄方式递送身份鉴别材料，或由可信的数据库中获取；

c) 身份鉴别材料包括身份证、户籍证明、在所属单位任职证明。

基本级证书策略中，对订户的密钥更新时的身份鉴别分为两种情况：

a) 从订户最初申请证书起，每隔 7 年至少要重新鉴别一次其身份，鉴别过程与申请证书时的要求相同。即如果密钥更新时已 7 年未进行此种鉴别，则应进行一次这种身份鉴别。

b) 除第 a)种情况外，订户可以直接使用现有私钥的签名来进行身份鉴别。

5.4.4 证书生命周期操作要求

申请证书时，申请者需要将证书公钥和其身份绑定后，安全递交给 CA。这种绑定可以使用某种算法加密，且此种算法的强度至少达到 CA 发行证书时使用的算法强度，除此之外，基本级证书策略还允许使用某种物理或程序上的方法进行绑定，例如通过挂号信件邮寄软盘等。

基本级证书策略要求订户在申请证书前声明该订户将遵守使用证书和保护个人私钥的所有策略要求。

每隔一段时间，CA 系统都需要发布周期性的 CRL 和 CARL，在基本证书策略中，发布 CRL 和 CARL 的周期可以由系统自行斟酌决定。但是，如果发现某个证书的私钥丢失或者安全性受到威胁，则 CA 系统在撤销该证书后的 24 小时之内，应发布一次 CRL 或 CARL。

5.4.5 认证机构设施、管理和操作控制

CA 系统应产生并保存表 A.1 中为基本级证书策略规定的审计事件的安全审计日志，基本级证书策略要求该日志的保存期不得短于 7 年。

每隔一段时间，安全审计日志需要提供给管理者进行审查，基本级证书策略不对审查的周期做要求，只在管理者认为需要时进行审查。

CA 系统需要对其自身的一些数据进行记录归档，基本级证书策略要求至少对以下事件进行记录归档：

a) 实体 CA 或桥 CA 的授权和鉴定；

b) CA 系统的 CPS；

c) 合同义务；

d) 系统和设备的配置；

e) 系统配置的修改和升级；

f) 收到的证书申请消息的内容；

g) 收到的证书撤销请求；

h) 订户申请证书时的身份证明材料；

i) 证书接受的相关文档；

j) 令牌接收的相关文档；

k) 签发的所有证书；

l) CA 密钥的更新记录；

m) 签发的所有 CRL 和 CARL；

n) 所有的审计日志；

o) 可以验证存档内容的其他数据或程序；

p) 审计员要求的其他文档。

记录归档的保存期不得短于 7 年。

基本级证书策略要求 CA 系统在物理安全上至少满足以下两个条件：

a) 确保对硬件系统的任何形式的访问都是经过允许的；

b) 确保任何保存敏感信息的存储介质(包括电子介质和纸介质)都被存放在一个安全的地点。

当实体 CA 或桥 CA 系统的物理设备处于无人使用的状态前，都应做一次安全检查，检查至少包括以下四种：

a) 针对不同的操作模式，设备都处于正确的状态中。例如：当一个硬件加密模块处于打开模式时，应放置于工作位置；当处于关闭模式时，应放置于一个安全保存地点。

b) 所有安全保存设施是否已经处于安全状态。例如：保险箱是否已设置密码保护。

c) 所有物理安全设备是否完好。例如：门锁是否完好。

d) 整个系统区域是否可以对抗非法访问。

基本级证书策略要求如果供电系统出现问题，实体 CA 或桥 CA 系统应有足够的备份能力，能够在断电前自动停止输入，结束任何挂起的任务，并记录当前的设备状态。

基本级证书策略要求实体 CA 或桥 CA 系统每隔一段时间应做一次全系统的备份，这种备份应能在系统发生故障时有效地恢复系统，系统的 CPS 应详细地描述此种备份。系统备份的周期不能长于一周，且应异地保存。系统备份应存储在具有与实体 CA 和桥 CA 的运行操作相适应的物理和过程控制的地点。

CA 系统的可信角色分为四种：超级管理员、系统管理员、系统审计员、系统操作员，基本级证书策略要求这四种角色都应有人担任，允许兼任，但不得同时兼任系统管理员和系统操作员。每个人在进行其对应角色的操作前都应向系统证明其身份。

5.4.6 技术安全控制

订户所使用的密码设备和密钥管理应符合国家密码管理部门的相关要求。

CA 给订户发放的证书应使用密钥用途扩展项表明其密钥用途，给用户分别发放双证书：签名证书和加密证书。

实体 CA、桥 CA 和 RA 所使用的密码设备和密码算法应符合国家密码管理有关政策。

如果订户的签名证书中所声明的安全保证级别为基本级或者声明与桥 CA 的基本级相对应，则证书对应的签名私钥可以进行备份和拷贝，但只能在用户的控制下进行。

实体 CA、桥 CA 和订户所使用的激活数据，都应使用一定的访问控制方法进行保护，其受保护的强度应与被其激活的私钥的保护强度相同。基本级安全策略允许用户自行选择其使用的激活数据。

5.4.7 证书、证书撤销列表和在线证书状态协议

实体 CA 颁发的基本级证书的扩展项应符合 GB/T 20518—2006 的规范。

5.4.8 符合性审计和其他评估

每隔一段时间，实体 CA、桥 CA 和 RA 都应接受一次符合性审计和评估，基本级证书策略要求每 2 年至少进行一次符合性审计和评估。

5.4.9 其他商务和法律问题

无特殊要求。

5.5 中级

5.5.1 导引

中级证书应拥有一个唯一的中级证书策略 OID。

使用中级策略的证书的安全保护目标是保护那些比较重要的数据，例如公司的普通商业秘密。这些数据只有较少的人才能接触，数据的泄漏也将会带来较大的损失和危害。

在使用中级策略证书的环境中，存在恶意违法攻击和危险的可能性都是中等程度的。但是，任何一份数据在这样的环境中都很有可能受到攻击。因此，此种环境对证书安全性的要求相对较高，要求证书在应用时假定会受到攻击，并仔细考虑好受到攻击的应对措施，证书的安全级别足以应付较高程度的攻击能力。例如：它可以用于一些有价值的事务交易中；可以使用于可能发生诈骗的环境中；也可以使用于对个人私有信息的访问环境，只要该环境中非法访问的可能性仅是中等程度的。

5.5.2 信息发布与管理

无特殊要求。

5.5.3 身份标识与鉴别

中级证书应拥有一个非空的主体名且遵循 X.500 的可辨别名的要求，另外，如果可选主体名扩展被标记为非关键的，则该扩展可以为空。

中级证书策略要求在桥 CA 颁发给实体 CA 的证书中，应使用名称限制来限制实体 CA 颁发的证书主体名的名字空间，这个名字空间应与实体 CA 所管理的范围相对应。

申请证书时，中级证书策略要求申请者采用下列方法证明其身份：

a) 身份鉴别时申请人应亲自到 RA 处，或由申请人所在当地可信的第三方鉴别机构鉴别申请人身份、提交由第三方鉴别机构鉴别人手写签名的申请人身份鉴别结果，同时提供由申请人所属机构人事负责人手写签名的申请人身份证实声明，以挂号信邮寄。这些身份鉴别材料的签署具有法律效应。

b) 身份鉴别材料应包括申请人身份证件、户籍证明、联系方式证明、在所属单位任职证明、个人银行账号证明。

申请者提供的材料应被仔细验证，检查其合法性。

中级证书策略中，对订户的密钥更新时的身份鉴别分为两种情况：

a) 从订户最初申请证书起，每隔 4 年至少要重新鉴别一次其身份，鉴别过程与申请证书时的要求相同。即如果密钥更新时已 4 年未进行此种鉴别，则应进行一次这种身份鉴别。

b) 除第 a)种情况外，订户可以直接使用现有私钥的签名来进行身份鉴别。

5.5.4 证书生命周期操作要求

申请证书时，申请者需要将证书公钥和其身份绑定后，安全递交给 CA。这种绑定可以使用某种算法加密，且此种算法的强度至少达到 CA 发行证书时使用的算法强度，除此之外，中级证书策略还允许使用某种物理或程序上的方法进行绑定，例如通过挂号信件邮寄软盘等。

中级证书策略要求订户在申请证书前签署一份声明文件，声明该订户将遵守使用证书和保护个人私钥的所有策略要求。

每隔一段时间，CA 系统都需要发布周期性的 CRL 和 CARL，在中级证书策略中，要求每天至少发布一次 CRL 和 CARL。但是，如果发现某个证书的私钥丢失或者安全性受到威胁，则 CA 系统在撤销该证书后的 18 小时之内，应发布一次 CRL 或 CARL。

5.5.5 认证机构设施、管理和操作控制

CA 系统应产生并保存表 A.1 中为中级证书策略规定的审计事件的安全审计日志，中级证书策略要求该日志的保存期不得短于 10 年。

每隔一段时间，安全审计日志需要提供给管理者进行审查，中级证书策略要求每 2 个月至少审查一次。审查中，自上次审查后产生的所有重要的安全审计事件都应仔细检查，并使用某种合理的方法搜寻任何恶意违法行为的迹象。

CA 系统需要对其自身的一些数据进行记录归档，中级证书策略要求至少对以下事件进行记录归档：

a) 实体 CA 或桥 CA 的授权和鉴定；
b) CA 系统的 CPS；
c) 合同义务；
d) 系统和设备的配置；
e) 系统配置的修改和升级；
f) 收到的证书申请消息的内容；
g) 收到的证书撤销请求；
h) 订户申请证书时的身份证明材料；
i) 证书接受的相关文档；
j) 令牌接收的相关文档；
k) 签发的所有证书；
l) CA 密钥的更新记录；
m) 签发的所有 CRL 和 CARL；
n) 所有的审计日志；
o) 可以验证存档内容的其他数据或程序；
p) 审计员要求的其他文档。

记录归档的保存期不得短于 10 年。

中级证书策略要求 CA 系统在物理安全上至少满足以下五个条件：

a) 确保对硬件系统的任何形式的访问都是经过允许的。
b) 确保任何保存敏感信息的存储介质(包括电子介质和纸介质)都被存放在一个安全的地点。
c) 在任何时候，系统都应保持对非法入侵的监控能力，方法可以使用人工监控或电子监控。
d) 系统应拥有一个访问日志，记录所有对系统的访问(一般数据库都有，重要操作要签名)。管理员应周期性的检查该日志内容。
e) 对于密码模块和计算机系统的所有物理访问，都要求至少有两人在场时方能进行。

当实体 CA 或桥 CA 系统的物理设备处于无人使用的状态前，都应做一次安全检查，检查至少包括以下四种：

a) 针对不同的操作模式，设备都处于正确的状态中。例如：当一个硬件加密模块处于打开模式时，它应该放置于工作位置；当处于关闭模式时，应该放置于一个安全保存地点。
b) 所有安全保存设施是否已经处于安全状态。例如：保险箱是否已设置密码保护。
c) 所有物理安全设备是否完好。例如：门锁是否完好。
d) 整个系统区域是否可以对抗非法访问。

中级证书策略要求如果供电系统出现问题，实体 CA 或桥 CA 系统应该有足够的备份能力，能够在断电前自动停止输入，结束任何挂起的任务，并记录当前的设备状态。

中级证书策略要求实体 CA 或桥 CA 系统每隔一段时间应做一次全系统的备份，这种备份应能在

系统发生故障时有效地恢复系统，系统的 CPS 应该详细地描述此种备份。系统备份的周期不能长于一周，且应该异地保存。系统备份应存储在具有与实体 CA 和桥 CA 的运行操作相适应的物理和过程控制的地点。

CA 系统的可信角色分为四种：超级管理员、系统管理员、系统审计员和系统操作员，中级证书策略要求这四种角色都应有人担任，允许兼任，但系统操作员不得同时兼任系统管理员或系统审计员。系统应能够鉴别使用者身份，以确保办事员没有兼任系统管理员或系统审计员。每个人在进行其对应角色的操作前都应向系统证明其身份。

5.5.6 技术安全控制

订户所使用的密码设备和密钥管理应符合国家密码管理部门的相关要求。

CA 给订户发放的证书应使用密钥用途扩展表明其密钥用途，给用户分别发放双证书：签名证书和加密证书。

实体 CA、桥 CA 和 RA 所使用的密码设备和密码算法应符合国家密码管理有关政策。

如果订户的签名证书中所声明的安全保证级别为中级或者声明与桥 CA 的中级相对应，则证书对应的签名私钥可以进行备份和拷贝，但只能在用户的控制下进行。

实体 CA、桥 CA 和订户所使用的激活数据，都应使用一定的访问控制方法进行保护，其受保护的强度应该与被其激活的私钥的保护强度相同。中级安全策略允许用户自行选择他使用的激活数据。

5.5.7 证书、证书撤销列表和在线证书状态协议

实体 CA 颁发的中级证书的扩展项应符合桥 CA 体系证书及 CRL 格式规范中相应证书模板的设置。

5.5.8 符合性审计和其他评估

每隔一段时间，实体 CA、桥 CA 和 RA 都应接受一次符合性审计和评估，中级证书策略要求每 1 年至少进行一次符合性审计和评估。

5.5.9 其他商务和法律问题

无特殊要求。

5.6 高级

5.6.1 导引

高级证书应该拥有一个唯一的高级证书策略 OID。

使用高级证书策略的证书的安全保护目标是保护那些极其重要的数据的安全，如：公司重要数据。这些数据是极其关键和敏感的，只能被指定的少数人获知，数据的泄漏将带来致命和灾难性的后果。

使用高级证书策略的证书可以被使用于高度危险的环境中。在这些环境中，数据安全可能受到极大的威胁，或者安全被破坏后的代价是极其高昂的。因此，此种环境对证书安全级别的要求最高，要求证书在应用时假定会受到攻击，并应对各种攻击拥有应对的预案，证书的安全性应足以对付任何程度、任何可能的攻击行为。此级证书可以被用于价值极高的事务交易中，也可以被用于出现诈骗的可能性极高的环境中。

5.6.2 信息发布与管理

无特殊要求。

5.6.3 身份标识与鉴别

高级证书应拥有一个非空的主体名且遵循 X.500 的可辨别名的要求，另外，如果可选主体名扩展被标记为非关键的，则该扩展可以为空。

高级证书策略要求在桥 CA 颁发给实体 CA 的证书中，应该使用名称限制来限制实体 CA 颁发的证书主体名的名字空间，这个名字空间应与实体 CA 所管理的范围相对应。

申请证书时，高级证书策略要求申请者使用以下方法证明其身份：

a) 身份鉴别时，要求申请人应亲自前往 RA 处，或由申请人所在地可信的第三方鉴别申请人身份、提交由可信的第三方鉴别机构鉴别人手写签名的申请人身份鉴别结果、同时提供由申请人所属机构单位法人手写签名的申请人身份证实声明、送往 RA 处。这些身份鉴别材料的签署具有法律效应。

b) 身份鉴别材料须包括申请人身份证件、户籍证明、联系方式证明、在所属单位任职证明、个人银行账号证明。

高级证书策略中，对订户的密钥更新时的身份鉴别分为两种情况：

a) 从订户最初申请证书起，每隔 3 年至少要重新鉴别一次其身份，鉴别过程与申请证书时的要求相同。即如果密钥更新时已 3 年未进行此种鉴别，则应进行一次这种身份鉴别。

b) 除第 a)种情况外，订户可以直接使用现有私钥的签名来进行身份鉴别。

5.6.4 证书生命周期操作要求

申请证书时，申请者需要将证书公钥和其身份绑定后，安全递交给 CA。这种绑定应使用某种算法加密，且此种算法的强度至少达到 CA 发行证书时使用的算法强度。

高级证书策略要求订户在申请证书前签署一份声明文件，声明该订户将遵守使用证书和保护个人私钥的所有策略要求。

每隔一段时间，CA 系统都需要发布周期性的 CRL 和 CARL，在高级证书策略中，要求每天至少发布一次 CRL 和 CARL。但是，如果发现某个证书的私钥丢失或者安全性受到威胁，则 CA 系统在撤销该证书后的 6 小时之内，应发布一次 CRL 或 CARL。

5.6.5 认证机构设施、管理和操作控制

CA 系统应产生并保存表 A.1 中为高级证书策略规定的审计事件的安全审计日志，高级证书策略要求该日志的保存期不得短于 15 年。

每隔一段时间，安全审计日志需要提供给管理者进行审查，高级证书策略要求每 1 个月至少审查一次。审查中，自上次审查后产生的所有重要的安全审计事件都应仔细检查，并使用某种合理的方法搜寻任何恶意违法行为的迹象。

CA 系统需要对其自身的一些数据进行记录归档，高级证书策略要求至少对以下事件进行记录归档：

a) 实体 CA 或桥 CA 的授权和鉴定；

b) CA 系统的 CPS；

c) 合同义务；

d) 系统和设备的配置；

e) 系统配置的修改和升级；

f) 收到的证书申请消息的内容；

g) 收到的证书撤销请求；

h) 订户申请证书时的身份证明材料；

i） 证书接受的相关文档；
j） 令牌接收的相关文档；
k） 签发的所有证书；
l） CA 密钥的更新记录；
m） 签发的所有 CRL 和 CARL；
n） 所有的审计日志；
o） 可以验证存档内容的其他数据或程序；
p） 审计员要求的其他文档。

记录归档的保存期不得短于 15 年。

高级证书策略要求 CA 系统在物理安全上至少满足以下五个条件：

a） 确保对硬件系统的任何形式的访问都是经过允许的。
b） 确保任何保存敏感信息的存储介质（包括电子介质和纸介质）都被存放在一个安全的地点。
c） 在任何时候，系统都应保持对非法入侵的监控能力，方法可以使用人工监控或电子监控。
d） 系统应拥有一个访问日志，记录所有对系统的访问。重要操作应签名，并且只能查询不能修改。管理员应周期性的检查该日志内容。
e） 对于密码模块和计算机系统的所有物理访问，都要求至少有两人在场时方能进行。

当实体 CA 或桥 CA 系统的物理设备处于无人使用的状态前，都应做一次安全检查，检查至少包括以下四种：

a） 针对不同的操作模式，设备都处于正确的状态中。例如：当一个硬件加密模块处于打开模式时，它应该放置于工作位置；当处于关闭模式时，应该放置于一个安全保存地点。
b） 所有安全保存设施是否已经处于安全状态。例如：保险箱是否已设置密码保护。
c） 所有物理安全设备是否完好。例如：门锁是否完好。
d） 整个系统区域是否可以对抗非法访问。

高级证书策略要求如果供电系统出现问题，实体 CA 或桥 CA 系统应该有足够的备份能力，能够在断电前自动停止输入，结束任何挂起的任务，并记录当前的设备状态。

高级证书策略要求实体 CA 或桥 CA 系统每隔一段时间应做一次全系统的备份，这种备份应能在系统发生故障时有效地恢复系统，系统的 CPS 应该详细地描述此种备份。系统备份的周期不能长于一周，且应该异地保存。系统备份应存储在具有与实体 CA 和桥 CA 的运行操作相适应的物理和过程控制的地点。

CA 系统的可信角色分为四种：超级管理员、系统管理员、系统审计员和系统操作员，高级证书策略要求四种角色都应有人担任，但是不允许一人同时担任系统管理员、系统操作员和系统审计员中的两种角色。系统应能够鉴别使用者身份，以确保没有非法兼任的情况发生。每个人在进行其对应角色的操作前都应向系统证明其身份。

5.6.6 技术安全控制

订户所使用的密码设备和密钥管理应符合国家密码管理部门的相关要求。

CA 给订户发放的证书应使用密钥用途扩展项表明其密钥用途，给用户分别发放双证书：签名证书和加密证书。

实体 CA、桥 CA 和 RA 所使用的密码设备和密码算法应符合国家密码管理有关政策。

如果订户的签名证书中所声明的安全保证级别为高级或者声明与桥 CA 的高级相对应，则证书对应的签名私钥不允许进行备份和拷贝。

实体 CA、桥 CA 和订户所使用的激活数据，都应使用一定的访问控制方法进行保护，其受保护的强度应该与被其激活的私钥的保护强度相同。高级安全策略使用的激活数据或者来源于用户的人体生物

特征，或者满足所使用的密码模块的策略要求。

5.6.7 证书、证书撤销列表和在线证书状态协议

实体 CA 颁发的高级证书的扩展项应符合桥 CA 体系证书及 CRL 格式规范中相应证书模板的设置。

5.6.8 符合性审计和其他评估

每隔一段时间，实体 CA、桥 CA 和 RA 都应接受一次符合性审计和评估，高级证书策略要求每半年至少进行一次符合性审计和评估。

5.6.9 其他商务和法律问题

无特殊要求。

附 录 A
（规范性附录）
可审计事件安全要求级别划分

表 A.1 对可审计事件在不同级别的要求进行了规范。

表 A.1 审计事件表

可审计的事件	初级	基本级	中级	高级
安全性审计				
审计参数的任何变动，如：审计频率、审计的事件类型等		×	×	×
任何试图删除或改动审计日志的行为		×	×	×
身份鉴别和认证				
成功或失败扮演一个角色的企图		×	×	×
改变最大认证数值的企图		×	×	×
在使用者登录时不成功认证的最大数目		×	×	×
一个管理员将因使用者未成功认证达到最大数值而被锁住的该用户账号解锁的企图		×	×	×
一个管理员改变认证方式（如：从口令认证改为生物认证）的企图		×	×	×
密钥生成				
只要实体 CA 或桥 CA 产生了密钥时（在单一通讯会话中或单次使用对称密钥时不要求强制执行）	×	×	×	×
私钥装载和存储				
私钥内容的装载	×	×	×	×
在实体 CA 或桥 CA 中用于密钥恢复时对证书主体私钥的访问	×	×	×	×
可信公钥的介入、删除和存储				
所有对可信公钥的变更，包括可信公钥的增加和删除	×	×	×	×
私钥的出口				
私钥的出口（不包括在单次会话或单个消息中私钥的使用）	×	×	×	×
证书注册				
所有证书申请	×	×	×	×
证书撤销				
所有证书撤销请求		×	×	×
证书状态变更批准				
批准或拒绝证书状态变更请求		×	×	×
实体 CA 或桥 CA 设置				
任何与安全性有关的实体 CA 或桥 CA 的设置		×	×	×
使用者账号管理				

表 A.1（续）

可审计的事件	初级	基本级	中级	高级
增加或删除角色或使用者	×	×	×	×
一个使用者账号的访问控制方式或一个角色更改时	×	×	×	×
证书格式管理				
证书格式的所有变更	×	×	×	×
证书撤销格式管理				
证书撤销格式的所有变更		×	×	×
证书撤销列表格式管理				
证书撤销列表格式的所有变更		×	×	×
其他各种事件				
操作系统的安装		×	×	×
实体 CA 或桥 CA 的安装		×	×	×
密码模块的安装			×	×
密码模块的移出			×	×
密码模块的销毁		×	×	×
系统启动		×	×	×
实体 CA 或桥 CA(应用)系统的登录		×	×	×
收到硬件/软件			×	×
设置口令的企图		×	×	×
更改口令的企图		×	×	×
实体 CA 或桥 CA 内部数据库备份		×	×	×
实体 CA 或桥 CA 内部数据库的恢复		×	×	×
文件处理(如:产生、重新命名、转移)			×	×
将任何材料放入资料库(目录器)			×	×
实体 CA 或桥 CA 内部数据库的访问			×	×
所有证书失密的通知请求		×	×	×
用证书装载 Tokens			×	×
Tokens 运输			×	×
Tokens 的清零		×	×	×
实体 CA 桥 CA 的密钥更新	×	×	×	×
CA 服务器设置的变更				
硬件		×	×	×
软件		×	×	×
操作系统		×	×	×
补丁		×	×	×

表 A.1（续）

可审计的事件	初级	基本级	中级	高级
安全轮廓			×	×
物理访问/场所安全				
个人访问实体 CA 或桥 CA 机房			×	×
访问实体 CA 或桥 CA 服务器			×	×
物理安全已知的或怀疑的侵害		×	×	×
非正常性				
软件错误条件		×	×	×
软件完整性检测失败		×	×	×
不适当消息的接收			×	×
被错误传输的消息			×	×
怀疑或证实的网络攻击		×	×	×
设备失效	×	×	×	×
电力过多消耗或损耗			×	×
不间断电力供应的失效			×	×
明显或显著的网络服务或访问失效			×	×
证书策略的违反	×	×	×	×
认证实施声明的违反	×	×	×	×
重新设置操作系统时钟		×	×	×
注：“×”表示可审计事件在相应级别进行了规范。				

附 录 B
（规范性附录）
证书级别划分

表 B.1 对证书级别划分进行了总结。

表 B.1 证书级别划分

级别内容	测试级	初级	基本级	中级	高级
导引	+	++	+++	++++	+++++
信息发布与管理	+	+	+	+	+
身份标识与鉴别	+	++	+++	++++	++++
证书生命周期操作要求	+	+	++	+++	++++
认证机构设施、管理和操作控制	+	++	+++	++++	+++++
技术安全控制	+	++	++	+++	++++
证书、证书撤销列表和在线证书状态协议	+	++	++	+++	+++
符合性审计和其他评估	+	+	++	+++	+++
其他商务和法律问题	+	+	+	+	+
注：“+”表示对证书策略的要求，“+”数量的增加表示证书策略要求的提高。					

参 考 文 献

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

[2] RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile.April,2002.

[3] X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA). September,2002.

[4] Booz,Allen,Hamilton.Federal Bridge Certification Authority (FBCA) and the XXXX For cross certification at a Rudimentary Level of Assurance.March,2003.

[5] Booz,Allen,Hamilton.Federal Bridge Certification Authority (FBCA) and the XXXX For cross certification at a Basic Level of Assurance.March,2003.

[6] Booz,Allen,Hamilton.Federal Bridge Certification Authority (FBCA) and the XXXX For cross certification at a Medium Level of Assurance.March,2003.

[7] Booz,Allen,Hamilton.Federal Bridge Certification Authority (FBCA) and the XXXX For cross certification at a High Level of Assurance.March,2003.

[8] Certificate Issuing and Management Components Family of Protection Profiles Version 1.0. October,2001.