ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31508—2015

信息安全技术　公钥基础设施 数字证书策略分类分级规范

Information security techniques—Public key infrastructure—Digital certificate policies classification and grading specification

2015-05-15 发布　　2016-01-01 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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:中国科学院数据与通信保护研究教育中心、北京数字证书认证中心有限公司、中国科学院软件所。

本标准主要起草人:荆继武、高能、林璟锵、王展、马存庆、向继、王跃武、夏鲁宁、查达仁、王平建、王琼霄、詹榜华、连一峰。

引　言

使用电子认证服务进行电子交易的实体主要关心两个问题：一是交易对象的合法公钥是什么；二是交易对象的数字证书的安全性能否用于本交易。为了体现第二方面的信息，数字证书中包含了一个由电子认证服务机构提供的证书策略标识，它表明了证书持有者（公钥所对应的用户）的安全属性。数字证书的依赖方可以通过阅读相应的证书策略文档来评估证书的安全程度，以便正确使用或依赖该证书（如：仅用于测试的，或者仅用于访问网络，或者可用于金融交易并有 10 万元担保）。因此，证书策略的实施是数字证书实际应用中不可缺少的一部分，也是提供分层次可靠的电子认证服务的基础之一。

目前，我国的电子认证服务机构签发的数字证书均未包含证书策略的内容，即在证书中没有说明公钥可以应用在什么场景，适用于什么样的安全需求。这导致了证书的使用者对于证书的用途十分茫然，限制了数字证书的广泛应用。另外，由于缺乏数字证书使用范围或质量的标准，各电子认证服务机构证书签发的安全措施（如：证书签发过程中的身份鉴别、物理设备安全、责任和赔付等）也存在较大差距。这种不一致导致了证书依赖方的许多困惑，阻碍了数字证书的跨区域跨行业应用，限制了应用程序直接获得证书的安全信息，对证书进行自动地验证。而标准化的证书策略能够使用户清晰地认识到证书的质量和安全通途，方便应用系统的开发设计。因此，对证书策略进行规范和标准化，是推进电子商务、电子政务系统之间互联互通的重要一步。

通过证书策略的标准化，设计数字证书策略的分级分类规范，可以为电子认证服务市场规划出分级的、多层次的服务质量体系，为不同应用系统实现适度的安全服务，从而促进电子认证服务机构之间的良性竞争，提升服务质量，推动电子认证服务市场的有序发展。另外，随着证书策略的分级分类逐步的实施，也可以促进电子认证服务机构评估和许可工作的规范化，即审查电子认证服务机构是否真正地按照其证书策略要求的规范来运营，是否提供相应的安全保障，这也是构建证书策略分级分类体系的重要意义。

信息安全技术　公钥基础设施
数字证书策略分类分级规范

1　范围

本标准通过分类分级的方式，规范了用于商业交易、设备和公众服务领域的电子认证服务中的8种数字证书策略。

本标准适用于我国电子商务和公众服务中所涉及的数字证书。

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 20518—2006　信息安全技术　公钥基础设施　数字证书格式

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

GB/T 29241—2012　信息安全技术　公钥基础设施　PKI互操作性评估准则

3　术语和定义

下列术语和定义适用于本文件。

3.1

证书签发机构　certification authority

负责签发证书和维护证书状态的实体。

3.2

订户注册机构　registration authority

负责订户的标识和鉴别，批准或拒绝订户的证书申请、撤销申请和挂起申请，发起证书的撤销和挂起的实体。

3.3

电子认证服务机构　certification service provider

依据《电子签名法》和《电子认证服务管理办法》获得《电子认证服务许可证》向公众提供电子认证业务的机构，一般包含有证书签发机构和订户注册机构。

3.4

订户　subscriber

与电子认证服务机构签订协议，接受电子认证服务机构提供的服务的实体。订户应能对证书对应的私钥的使用负有法律责任。

3.5

依赖方　relying party

接受电子认证服务机构的依赖方协议，独立地判断证书的安全性是否满足其应用的安全需求，并验证证书和相应签名的实体。

3.6

证书主体　subject

证书中的“主体(subject)”项指明的、持有与证书中载明公钥相对应之私钥的实体。

注：证书主体可以是订户自己，也可以是订户全权控制的设备、账号、域名、IP 地址等。当订户是法人机构时，证书主体还可以是该法人机构的下属机构、下属职员、签约人和设备等。

3.7

证书申请者　certificate applicant

向电子认证服务机构申请证书的自然人或法人。

注：证书申请成功后，证书申请者即为订户。

3.8

证书申请递交人　certificate application deliverer

向电子认证服务机构递交证书申请的自然人，可以是订户或者订户的合法代表。

3.9

会话密钥　session key

在一次会话中有效的对消息进行加密的密钥。

3.10

OCSP 服务　OCSP service

在线的证书状态查询服务，该服务的主要对象是依赖方。

3.11

可辨识名　distinguished name

用于标识证书颁发机构和证书主体名称的序列，一般包括国家名称、省名、地理位置、机构名、机构单元名称和正式名称。

3.12

带外方式　out-of-band

指当前的通信方式之外的方式，如电子认证服务机构以网络方式提供证书申请与查询等服务，带外通讯方式包括但不限于报纸、电视、纸质文件、电话传真等。

3.13

激活数据　activation data

用于使密码模块进入可操作状态的数据，可以是口令、生物特征等。

3.14

依赖方协议　relying party agreement

电子认证服务机构在《电子认证业务规则》中或单独载明的与依赖方之间的协议，规定双方在证书使用和管理过程中所承担的责任和义务。

3.15

订户协议　subscriber agreement

电子认证服务机构与订户所签署的协议，规定了双方在证书使用和管理过程中所承担的责任和义务。

3.16

证书信任链　certificate chain

一个用于证书验证的有序证书序列，它包含一个终端订户证书和若干电子认证服务机构证书，证书信任链起始于根证书，终止于终端订户证书。

3.17

证书撤销列表　certificate revocation list

由电子认证服务机构维护的，包含由于各种原因(例如：私钥泄露、证书中的信息发生改变)在有效

期内被撤销的证书的列表。

3.18

对象标识符　object identifier

一串分段的数字，可以唯一地标识一个对象（例如：密码算法、证书策略等）。

3.19

公钥基础设施　public key infrastructure

一套由硬件、软件、人员、策略和流程构成的，用于生成、管理、分发、使用、存储和撤销数字证书的，利用公钥技术提供安全服务的基础设施。

3.20

证书策略　certificate policy

指定的一组规则，表明了证书在某特定范围内的、和（或）某些具有相同安全需求的应用内的适用程度。

3.21

电子认证业务规则　certificate practice statement

又称为认证业务声明，是电子认证服务机构对其签发、管理、撤销和更新证书的相关措施和实施行为的一份声明。

3.22

密码模块　cryptographic module

经国家密码管理部门批准使用的密码产品或密码系统，是指具有安全边界的用于进行密码相关的存储和计算操作的软件、固件或硬件组合。

4　缩略语

下列缩略语适用于本文件。

CA：证书签发机构（Certificate Authority）

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

DN：可辨识名（Distinguished Name）

IP：互联网协议（Internet Protocol）

LDAP：轻量级目录访问协议（Light-weight Directory Access Protocol）

OCSP：在线证书状态协议（Online Certificate Status Protocol）

OID：对象标识符（Object Identifier）

PKI：公钥基础设施（Public Key Infrastructure）

URL：统一资源定位符（Universal Resource Locator）

5　概述

电子认证服务机构可以根据需要签发符合一个或多个证书策略的证书。将本标准中的任何一个或多个证书策略包含在证书中，都应得到电子认证服务管理部门的许可。电子认证服务机构制定的《电子认证业务规则》，原则上不应与本证书策略内容冲突。电子认证服务机构无法执行本证书策略中某些条款具体要求的，应向电子认证服务管理部门提出申请，经电子认证服务管理部门审核后方可使用该《电子认证业务规则》。

电子认证活动的参与方包括电子认证服务机构、订户、依赖方以及其他参与者。本标准为数字证书签发和使用提供指导，为电子认证活动各参与方明确各自的权利和义务提供依据。本标准中证书策略

的适用对象包括：

- 电子认证服务机构：签发符合一个或多个策略要求的证书的电子认证服务机构，应按照本标准中证书策略的要求制定《电子认证业务规则》，并按照其《电子认证业务规则》运营；
- 订户：认定本标准中证书策略的规定可以满足其应用需求的订户，应当了解本标准中证书策略规定的订户权利和义务以及电子认证服务机构对其提供的保障；
- 依赖方：依赖方应依据本标准中证书策略的条款，确定在多大程度上信任符合本标准中证书策略的证书及其对应的电子签名。当依赖方使用符合某个证书策略的证书时，说明其已经了解相应证书策略内容并已确认该证书策略满足其安全需求。

本标准中证书策略符合 GB/T 26855—2011 的要求，各个证书策略的名称和对应 OID 如表 1 所示。

表 1　证书策略名称和 OID

类别	级别	OID
基线	基线	待申请
商业交易	商业交易普通级	待申请
	商业交易中级	待申请
	商业交易高级	待申请
设备	设备普通级	待申请
	设备可信级	待申请
公众服务	公众服务非实名级	待申请
	公众服务实名级	待申请

电子认证服务机构可根据应用的需要，将本标准中证书策略的 OID 包含在证书中。基线证书策略可应用于商业交易、设备和公众服务；商业交易普通级、商业交易中级和商业交易高级策略用于商业交易证书；设备普通级和设备可信级策略用于签发给设备的证书；公众服务非实名级和公众服务实名级策略用于提供和获取公共服务的证书。基线证书策略是进行电子认证业务的基本要求，三类证书策略都应该符合基线证书策略的要求；在同一类别的证书策略中，高等级的证书策略涵盖低等级证书策略的要求。

本标准中证书策略支持的应用如表 2 所示。

表 2　证书策略支持的应用

类别	级别	支持的证书应用
基线	基线	网络环境下的身份鉴别、网络安全登录、信息保护和通信密钥协商等基本应用以及当事人约定的其他应用
商业交易	商业交易普通级	身份鉴别、网络安全登录、信息保护和通信密钥协商等基本应用、小额度交易以及当事人约定的其他应用，其额度不超过电子认证服务管理部门所规定的商业交易普通级证书策略支持的交易额度
	商业交易中级	身份鉴别、网络安全登录、信息保护和通信密钥协商等基本应用、中等额度交易以及当事人约定的其他应用，其额度不超过电子认证服务管理部门所规定的商业交易中级证书策略支持的交易额度
	商业交易高级	身份鉴别、网络安全登录、信息保护和通信密钥协商等基本应用、大额交易以及当事人约定的其他应用，其额度不超过电子认证服务管理部门所规定的商业交易高级证书策略支持的交易额度

表 2（续）

类别	级别	支持的证书应用
设备	设备普通级	具有一般安全性要求的设备，如：安全邮件服务器、Web 服务器等
	设备可信级	安全性要求较高的设备，如：支持在线电子支付、大规模用户管理等敏感应用的服务器
公众服务	公众服务非实名级	需要匿名性的公众服务，如：电子投票。网络安全登录、信息保护和通信密钥协商等基本应用以及当事人约定的其他应用
	公众服务实名级	需要实名性的公众服务，如：电子报税。网络安全登录、信息保护和通信密钥协商等基本应用以及当事人约定的其他应用。签署需要承担法律责任但无经济责任的文书

符合本标准中证书策略的证书还可以用于其他用途，条件：依赖方根据自己的评估，有充分的理由信任该证书并确保该证书的使用不违反相关法律。订户或信赖方如果对电子认证服务机构有特殊要求，可以通过相关协议进行约定。

本标准中证书策略不支持的应用如表 3 所示。

表 3　证书策略不支持的应用

类别	级别	不支持的证书应用
基线	基线	在违背相关法律法规规定的情况下使用
商业交易	商业交易普通级	● 在违背相关法律法规规定的情况下使用； ● 用于超过电子认证服务管理部门所规定的商业交易普通级证书策略支持的交易额度的交易
	商业交易中级	● 在违背相关法律法规规定的情况下使用； ● 用于超过电子认证服务管理部门所规定的商业交易中级证书策略支持的交易额度的交易
	商业交易高级	● 在违背相关法律法规规定的情况下使用； ● 用于超过电子认证服务管理部门所规定的商业交易高级证书策略支持的交易额度的交易
设备	设备普通级	● 在违背相关法律法规规定的情况下使用； ● 用于支撑金融交易等安全性敏感应用的设备； ● 设备以外的应用
	设备可信级	● 在违背相关法律法规规定的情况下使用； ● 用于设备以外的应用
公众服务	公众服务非实名级	● 在违背相关法律法规规定的情况下使用； ● 用于商业交易、需要实名性的公众服务
	公众服务实名级	● 在违背相关法律法规规定的情况下使用； ● 用于商业交易

仅符合本标准中证书策略要求的证书不适用于可能直接导致人员伤亡或者严重破坏环境的应用系统，例如：核设备的操作系统、航天器的导航或通信系统、航空管制系统或者武器控制系统等。在本标准中，未指明适用于特定策略的条款，适用于所有 8 种证书策略。

6 信息发布和证书资料库责任

6.1 证书资料库

电子认证服务机构应建立一个允许公众访问的在线资料库或者使用允许公众访问的在线第三方资料库，并将其签发的证书以及证书状态信息发布到该资料库上。

6.2 证书信息的发布

电子认证服务机构应将所签发的符合本标准中证书策略的证书及其状态信息发布到资料库上，同时还应发布以下文档的最新版本，允许订户或依赖方进行在线查询：

- 证书策略文档；
- 《电子认证业务规则》；
- 订户协议；
- 依赖方协议。

6.3 发布信息的时间或频率

电子认证服务机构的相关信息应在生效后及时发布。

本标准中证书策略和对应的《电子认证业务规则》的变更，应在审核通过之日起 10 天内发布。

电子认证机构应保证在吊销列表的下次更新时间之前更新吊销列表。对于终端订户的证书撤销列表，应至少每 24 h 签发一次，其中对于商业交易高级、设备可信级证书撤销列表，应至少每 12 h 签发一次。

电子认证服务机构证书的证书撤销列表应至少每年签发一次。当电子认证服务机构的证书需要撤销时签发证书撤销列表。

6.4 证书资料库的访问控制

电子认证服务机构不应使用技术手段来限制公众对以下信息的读取访问：证书策略、《电子认证业务规则》、证书和证书状态信息以及公开的订户协议和依赖方协议。

电子认证服务机构应执行控制措施来阻止对资料库的信息进行未经授权的添加、删除或修改。本标准中证书策略对于资料库访问控制的要求，如表 4 所示。

表 4 证书策略对资料库访问控制的要求

类别	级别	资料库的访问控制要求
基线	基线	应执行访问控制措施来阻止对资料库的信息进行未经授权的添加、删除或修改
商业交易	商业交易普通级	应执行访问控制措施来阻止对资料库的信息进行未经授权的添加、删除或修改
	商业交易中级	应采用访问控制和逻辑端口分割技术来阻止对资料库信息进行未经授权的添加、删除或修改
	商业交易高级	应采用访问控制和物理端口分割技术及通信加密保护技术来阻止对资料库信息进行未经授权的添加、删除或修改
设备	设备普通级	应采用访问控制和逻辑端口分割技术来阻止对资料库信息进行未经授权的添加、删除或修改
	设备可信级	应采用访问控制和物理端口分割技术及通信加密保护技术来阻止对资料库信息进行未经授权的添加、删除或修改

表 4（续）

类别	级别	资料库的访问控制要求
公众服务	公众服务非实名级	应采用访问控制和逻辑端口分割技术来阻止对资料库信息进行未经授权的添加、删除或修改
	公众服务实名级	应采用访问控制和物理端口分割技术及通信加密保护技术来阻止对资料库信息进行未经授权的添加、删除或修改

7 身份标识与鉴别

7.1 命名

7.1.1 名称类型

根据本标准中证书策略签发的证书应包含签发该证书的电子认证服务机构名称和证书主体的名称。出现在证书中“颁发者(issuer)”项的电子认证服务机构名称和出现在“主体”项的主体名称应采用GB/T 20518—2006 中的可辨识名(DN)。主体的唯一可辨识名中应含有订户的名称信息。

证书中出现的电子认证服务机构的名称，包括英文缩写名称，应使用电子认证服务管理部门批准的名称。

7.1.2 名称意义化的要求

证书中出现的证书主体名称应有实际意义。本标准中证书策略对主体名称意义的要求，如表 5 所示。

表 5 证书策略的名称意义化要求

类别	级别	主体名称要求
基线	基线	主体名称应有实际意义，包括：合法的机构名称、个人姓名、电子邮件地址、用户账号和电话号码等可以用于识别主体身份的名称
商业交易	商业交易普通级	主体名称应具有实际意义，例如：合法的机构名称或个人姓名、机构注册地址或个人家庭住址、电子邮件地址、电话号码等
	商业交易中级	主体名称应具有实际意义，例如：合法的机构名称或个人姓名、机构注册地址或个人家庭住址、电子邮件地址、电话号码等
	商业交易高级	主体名称应包含订户的地址、真实名称和其他辅助信息，这些信息可以确保联系到该主体
设备	设备普通级	主体名称应包含网络上可标识该设备的名称，如：合法域名或 IP 地址
	设备可信级	主体名称应包含订户的名称以及网络上可标识该设备的名称，如：合法域名或 IP 地址
公众服务	公众服务非实名级	主体名称可以为假名，但应在证书签发机构中保存有对应的真实身份信息
	公众服务实名级	主体名称应包含订户的地址、真实名称和其他辅助信息，这些信息可以确保联系到该主体

7.1.3 订户的匿名或假名

订户在证书中的名称可以是假名，但是电子认证服务机构应根据 7.2 的要求记录订户真实身份信息。本标准中证书策略对订户匿名或假名的要求，如表 6 所示。

表 6 证书策略对订户的匿名或假名的要求

类别	级别	订户假名的要求
基线	基线	主体名称可以是假名，但是在电子认证服务机构的数据库中，应根据 7.2 的要求记录订户真实身份信息
商业交易	商业交易普通级	主体名称可以是假名，但是在电子认证服务机构的数据库中，应根据 7.2 的要求记录订户真实身份信息
	商业交易中级	主体名称可以是假名，但是在电子认证服务机构的数据库中，应根据 7.2 的要求记录订户真实身份信息
	商业交易高级	主体名称应为户口簿或身份证载明的正式名称，不允许是假名
设备	设备普通级	主体名称可以是假名，但是在电子认证服务机构的数据库中，应根据 7.2 的要求记录订户真实身份信息
	设备可信级	主体名称应包含设备所有者在户口簿、身份证或组织机构代码证载明的正式名称，不允许是假名
公众服务	公众服务非实名级	主体名称可以为假名，但是在电子认证服务机构的数据库中，应根据 7.2 的要求记录订户真实身份信息
	公众服务实名级	主体名称应为户口簿或身份证载明的正式名称，不允许是假名

订户在证书中的名称不允许匿名。

7.1.4 不同名称格式的解释规则

商业交易高级、公众服务实名级的证书主体的机构名称或个人姓名应填写在 cn 域。

其他证书策略中对于不同名称格式的解释规则不作规定。

7.1.5 名称的唯一性

电子认证服务机构不应将主体名称相同的证书签发给不同的订户。电子认证服务机构应有统一的控制策略，保证每个证书主体拥有唯一的可辨识名。同一个订户可能拥有多个相同主体名称的证书。

7.1.6 商标的识别、鉴别和角色

证书申请中包含侵犯第三方知识产权的域名、商标、商号或服务标识的，订户应承担相应侵权责任。电子认证服务机构不对产权证明材料进行审查。出现产权争端时，电子认证服务机构有权拒绝或挂起引起争端的订户的证书申请。

7.2 初始申请证书的身份鉴别

7.2.1 证明拥有私钥的方法

证书申请者应证明持有与所要注册公钥相对应的私钥，证明的方法包括在证书请求消息中包含数字签名或其他与此相当的证明方法。对商业交易高级、设备可信级证书的申请，应该采用挑战响应的方法证明申请者拥有对应的私钥。

如果密钥对是电子认证服务机构为订户生成的,或者是由电子认证服务机构向其他第三方权威机构申请获得的,则不需要进行上述证明,但应测试密钥对的正确性。

7.2.2 机构身份的鉴别

当证书申请者是机构时,本标准中证书策略要求电子认证服务机构至少应对机构身份进行如表7中所要求的鉴别。

表7 证书策略中机构身份鉴别的要求

类别	级别	机构订户的鉴别
基线	基线	● 利用政府机构发放的合法性文件(如:工商营业执照、组织机构代码证)、权威第三方提供的身份证明或数据库服务,证明该机构的法人身份确实有效存在; ● 通过电话、邮政信函或类似方法确认该机构资料信息的真实性; ● 确认证书申请递交人得到了证书申请者的明确授权; ● 确认证书主体是由证书申请者全权控制,即证书申请者应表明其对该实体的控制能力
商业交易	商业交易普通级	● 利用政府机构发放的合法性文件(如:工商营业执照、组织机构代码证)、权威第三方提供的身份证明或数据库服务,证明该机构的法人身份确实有效存在; ● 通过电话、邮政信函或类似方法确认该机构资料信息的真实性; ● 确认证书申请递交人得到了证书申请者的明确授权; ● 确认证书主体是由证书申请者全权控制
	商业交易中级	● 利用政府机构发放的合法性文件(如:工商营业执照、组织机构代码证)、权威第三方提供的身份证明或数据库服务,证明该机构的法人身份确实有效存在; ● 通过电话、邮政信函或类似方法确认该机构资料信息的真实性; ● 确认证书申请递交人得到了证书申请者的明确授权; ● 确认证书主体是由证书申请者全权控制; ● 应检查机构订户的银行资信证明,1年内无不良信用记录
	商业交易高级	● 应检查由政府主管部门提供的机构合法性文件(如:工商营业执照、组织机构代码证); ● 通过实地考察,核实机构资料和信息的真实性; ● 应检查机构的授权代表所持有的书面授权书; ● 确认证书主体是由证书申请者全权控制; ● 应检查机构订户的银行资信证明,3年内无不良信用记录; ● 注册资本不低于100万,或年营业额高于500万
设备	设备普通级	● 利用政府机构发放的合法性文件(如:工商营业执照、组织机构代码证)、权威第三方提供的身份证明或数据库服务,证明该机构的法人身份确实有效存在; ● 通过电话、邮政信函或类似方法确认该机构资料信息的真实性; ● 证书申请递交人得到了证书申请者的明确授权; ● 确认证书主体是由证书申请者全权控制,检查由第三方提供的、该机构拥有对设备标识信息的控制权的证明,如:域名管理机构提供的域名注册记录,网络服务提供商提供的IP地址使用合同

表 7（续）

类别	级别	机构订户的鉴别
设备	设备可信级	● 利用政府机构发放的合法性文件（如：工商营业执照、组织机构代码证）、权威第三方提供的身份证明或数据库服务，证明该机构的法人身份确实有效存在； ● 通过电话、邮政信函或类似方法确认该机构资料信息的真实性； ● 证书申请递交人得到了证书申请者的明确授权； ● 确认证书主体是由证书申请者全权控制，检查由第三方提供的、该机构拥有对设备标识信息的控制权的证明，如：域名管理机构提供的域名注册记录，网络服务提供商提供的 IP 地址使用合同； ● 使用技术手段，确认证书申请者对设备具有全权控制能力； ● 设备通过了第三方权威机构的安全检测
公众服务	公众服务非实名级	不允许机构申请该策略证书
	公众服务实名级	● 利用政府机构发放的合法性文件（如：工商营业执照、组织机构代码证），证明该机构的法人身份确实有效存在； ● 通过电话、邮政信函或类似方法确认该机构资料信息的真实性； ● 确认证书申请递交人得到了证书申请者的书面授权； ● 确认证书主体是由证书申请者全权控制

7.2.3 自然人身份的鉴别

当证书申请者是自然人的时候，本标准中证书策略要求电子认证服务机构至少应对其身份进行如表 8 中所要求的鉴别。

表 8 证书策略对自然人身份鉴别的要求

类别	级别	自然人订户的鉴别
基线	基线	● 利用政府机关发放的合法性文件（如：居民身份证）、权威第三方提供的身份证明或数据库服务，证明自然人的身份； ● 通过电话、邮政信函或类似方法确认个人信息的真实性以及代表进行证书申请的个人就是证书申请者本人或是得到了证书申请者的明确授权； ● 确认证书主体是由证书申请者全权控制
商业交易	商业交易普通级	● 利用政府机关发放的合法性文件（如：居民身份证）、权威第三方提供的身份证明或数据库服务，证明自然人的身份； ● 通过电话、邮政信函或与此类似的其他方式确认该个人身份信息的真实性以及代表进行证书申请的个人就是证书申请者本人或是得到了证书申请者的明确授权； ● 检查合法第三方提供的工作证明
	商业交易中级	● 利用政府机关发放的合法性文件（如：居民身份证）、权威第三方提供的身份证明或数据库服务，证明自然人的身份； ● 通过电话、邮政信函或与此类似的其他方式确认该个人身份信息的真实性以及代表进行证书申请的个人就是证书申请者本人或是得到了证书申请者的明确授权； ● 检查合法第三方提供的工作证明； ● 检查银行的资信证明，1 年内无不良信用记录

表 8（续）

类别	级别	自然人订户的鉴别
商业交易	商业交易高级	● 利用政府机关发放的合法性文件（如：居民身份证）证明自然人的身份，并利用第三方的数据库或致电第三方检查证书申请者身份的真伪； ● 通过电话、邮政信函或与此类似的其他方式确认该个人身份信息的真实性以及代表进行证书申请的个人就是证书申请者本人或是得到了证书申请者的明确授权； ● 检查银行的资信证明，3 年内无不良信用记录； ● 确保证书申请者拥有 40 万以上的资产或等同的支付能力
设备	设备普通级	检查由第三方提供的、该个人订户对设备控制权的证明，如：域名管理机构提供的域名注册记录，网络服务提供商提供的 IP 地址使用合同
	设备可信级	● 检查由第三方提供的，该个人订户拥有对设备的控制权的证明，如：域名管理机构提供的域名注册记录，网络服务提供商提供的 IP 地址使用合同； ● 应使用安全检查工具，检查该设备的安全状况
公众服务	公众服务非实名级	● 利用政府机关发放的合法性文件（如：居民身份证）、权威第三方提供的身份证明或数据库服务，证明自然人的身份； ● 确认至少两种可达的联系方式，如：电话、邮政信函、电子邮件等
	公众服务实名级	● 利用政府机关发放的合法性文件（如：居民身份证）、权威第三方提供的身份证明或数据库服务，证明自然人的身份； ● 确认至少两种可达的联系方式，如：电话、邮政信函、电子邮件等

7.2.4 未验证的订户信息

未验证的订户信息不应包含在证书中。

7.2.5 权力确认

当一个自然人的名称与一个机构名称相关联，可以合法代表机构行使职权时，电子认证服务机构应进行机构的身份鉴别和自然人的身份鉴别并确认该自然人具有这样的授权。

7.2.6 互操作规范

根据 GB/T 29241—2012，本标准对签发不同证书策略的电子认证服务机构互操作能力的要求，如表 9 所示。

表 9 证书策略中互操作规范的要求

类别	级别	互操作等级
基线	基线	一级
商业交易	商业交易普通级	二级
	商业交易中级	二级
	商业交易高级	三级

表 9（续）

类别	级别	互操作等级
设备	设备普通级	二级
	设备可信级	三级
公众服务	公众服务非实名级	二级
	公众服务实名级	二级

7.3 密钥更新请求的身份鉴别

7.3.1 常规密钥更新请求的身份鉴别

订户在证书有效期内、且证书未被撤销的情况下提出密钥更新请求，视为常规密钥更新请求。在常规密钥更新时，电子认证服务机构应对订户进行身份鉴别，鉴别的方法可以采用质询短语或者私钥签名的方式。质询短语是订户在申请证书时留下的用于身份鉴别的短语。利用质询短语进行鉴别时，订户应正确提供该短语的内容，并能正确提供部分其他登记信息。若采用私钥签名的方式进行鉴别，订户应使用现有私钥对更新请求进行签名，更新请求中应包含正确的部分登记信息。电子认证服务机构应对订户的签名和更新请求内包含的订户信息进行验证。

订户也可以选择初始证书申请流程进行常规密钥更新，按照要求提交证书申请所需的材料。

对商业交易普通级、商业交易中级、商业交易高级、设备普通级、设备可信级、公众服务非实名级和公众服务实名级策略的证书连续地进行三次常规密钥更新后，应按照初始证书申请流程获得新证书。

7.3.2 证书撤销后密钥更新请求的身份鉴别

订户在证书撤销后申请密钥更新时，应按照初始证书申请流程重新申请。

7.4 证书撤销请求的身份鉴别

电子认证服务机构应在订户协议中写明对证书撤销请求的鉴别方法。证书撤销申请人应满足下列条件之一：

- 提供申请证书时留下的质询短语，或者具有同等安全程度的方式；
- 使用拟被撤销的证书对应的私钥对撤销请求进行签名；
- 电子认证服务机构通过电话、传真、邮政信函或其他方式确认申请撤销的人确实是订户。

司法机关依法提出证书撤销，电子认证服务机构将直接以司法机关书面撤销请求文件作为依据，不再进行其他方式的鉴别。

8 证书生命周期操作要求

8.1 证书申请

8.1.1 证书申请递交人

下列人员可以递交证书申请：

- 能够独立承担民事责任的自然人或其授权代表；
- 独立法人机构的授权代表。

8.1.2 登记过程和责任

证书申请者在申请满足本标准中证书策略要求的证书时，应明确表示同意订户协议中的内容，并提供真实的信息，生成或委托电子认证服务机构为自己生成公私钥对。如果公私钥对由证书申请者自己生成，还应向电子认证服务机构提供相应的公钥，并证明其拥有公钥对应的私钥。

8.2 证书申请的处理

8.2.1 执行身份鉴别

电子认证服务机构应根据 7.2 的要求，对证书申请者及证书主体进行身份鉴别。

8.2.2 接受或拒绝证书申请

如果满足下列条件，电子认证服务机构将接受证书申请：

- 根据 7.2 的要求，成功地完成了证书申请的身份鉴别；
- 收到或确认能收到证书申请者应缴纳的费用。

如果发生下列情形之一，电子认证服务机构应拒绝证书申请：

- 不能完成证书申请的身份鉴别过程；
- 证书申请者不能提供电子认证服务机构应的补充文件或没有在指定的时间内响应电子认证服务机构的通知；
- 未收到或确认无法收到证书申请者应缴纳的费用；
- 电子认证服务机构认为批准该申请将会导致电子认证服务机构陷入法律纠纷。

8.2.3 处理证书申请的时限

收到证书申请后，电子认证服务机构应当在合理的时限内开始处理证书申请。

电子认证服务机构应在《电子认证业务规则》中对证书申请处理所需的时间给出明确规定，并按照规定操作。本标准中证书策略对证书申请处理时限的要求，如表 10 所示。

表 10 证书策略对处理证书申请时限的要求

类别	级别	处理证书申请的期限
基线	基线	不作规定
商业交易	商业交易普通级	不作规定
	商业交易中级	10 个工作日内
	商业交易高级	10 个工作日内
设备	设备普通级	10 个工作日内
	设备可信级	10 个工作日内
公众服务	公众服务非实名级	10 个工作日内
	公众服务实名级	10 个工作日内

8.3 证书签发

8.3.1 证书签发期间电子认证服务机构的行为

证书的产生和签发应在证书申请审核通过之后进行。电子认证服务机构产生和签发的证书中的内

容应来源于被审核通过的证书申请。

8.3.2 订户证书签发的通知

电子认证服务机构签发证书后，应及时通知证书申请者，并向证书申请者提供获得证书的方式，确保证书申请者能够通过公众易于获得的方式获得证书。

8.4 证书接受

8.4.1 证书接受行为

证书申请者按照订户协议中规定的方式确认已经接受证书，或者证书申请者在收到电子认证服务机构的证书签发通知后的规定时限内未对证书或证书内容提出合理的异议，则视为证书申请者已经接受证书。

8.4.2 电子认证服务机构发布证书

电子认证服务机构应将订户已经接受的证书发布到允许公众访问的证书资料库中。

8.5 密钥对和证书的使用

8.5.1 订户私钥和证书的使用

订户应在签订了订户协议并接受证书后才能使用证书对应的私钥。订户私钥的使用应符合证书中“密钥用途(KeyUsage)”扩展的要求。订户的私钥和证书的使用应符合订户协议的要求。

订户应保护其私钥免受未经授权的使用。证书到期或被撤销后，订户应停止使用私钥。

8.5.2 依赖方对公钥和证书的使用

依赖方信任证书的前提是同意依赖方协议中的条款。依赖方应根据证书使用的环境和条件判断证书是否可信任。如果依赖方应电子认证服务机构提供额外的保障，依赖方应在确认可以获得这些保障之后信任相应的证书。

在信任证书前，依赖方应独立的进行如下评估：

- 证书适用于当前应用场景，并确定证书的使用不违背本证书策略的要求；
- 证书的使用不违背证书中“密钥用途”扩展的规定；
- 证书及其证书信任链中所有电子认证服务机构证书的证书状态是合适的。当证书信任链中的某个证书有被撤销的情况时，依赖方有责任调查上述证书撤销前，订户证书对应私钥所做的签名是否可信任，并独立承担相应的风险。

依赖方还应利用合适的软件/硬件来执行数字签名验证或其他密码操作。

8.6 证书更新

8.6.1 证书更新的情况

若证书中的公钥和其他订户信息没有发生任何变化，订户可以通过证书更新获得新证书。过期证书也可以更新。

8.6.2 证书更新请求人

订户本人或授权代表、机构的授权代表可以请求证书更新。

8.6.3 证书更新请求的处理

电子认证服务机构对订户证书进行更新前，应确认证书更新请求是证书订户或订户授权代表提出的，可以通过以下两种方法之一进行鉴别：

- 提供申请证书时留下的质询短语，或者具有同等安全程度的方式，并能正确提供部分其他登记信息；
- 使用拟被更新的证书对应的私钥对更新请求进行签名。

用于初始证书申请时的鉴别方法也可以用于处理证书更新。

8.6.4 通知订户新证书签发

证书更新完成后，新证书的签发通知要求同8.3.2。

8.6.5 接受证书更新的行为

接受证书更新的行为要求同8.4.1。

8.6.6 电子认证服务机构对更新证书的发布

电子认证服务机构对更新证书的发布要求同8.4.2。

8.7 证书密钥更换

8.7.1 证书密钥更换的情况

当证书到期、密钥发生泄露或者其他应更换密钥的情况发生时，订户可以通过证书密钥更换获得一张包含新公钥、其他订户信息不变的新证书。

8.7.2 证书密钥更换请求人

订户本人或授权代表、机构的授权代表可以请求证书密钥更换。

8.7.3 证书密钥更换请求的处理

电子认证服务机构在对订户证书进行密钥更换前，应确认密钥更换请求是被更换证书的订户或订户授权的代表提出的，可以通过以下两种方法之一进行鉴别：

- 提供申请证书时留下的质询短语，或者具有同等安全程度的方式，并能正确提供部分其他登记信息；
- 使用拟进行密钥更换的证书对应的私钥对密钥更换请求进行签名。

初始证书申请的鉴别流程和方法也可以用于处理证书密钥更换。

如果订户证书对应的私钥发生泄露，电子认证服务机构应采用初始证书申请的鉴别流程来处理密钥更换请求。

8.7.4 订户密钥更换后新证书签发的通知

订户密钥更换后新证书签发的通知要求同8.3.2。

8.7.5 接受密钥更换后新证书的行为

接受密钥更换后新证书的行为要求同8.4.1。

8.7.6 电子认证服务机构对密钥更换后的证书发布

电子认证服务机构对密钥更换后的证书发布要求同8.4.2。

8.8 证书变更

8.8.1 证书变更的情况

当证书中包含的信息(除公钥外)发生变化时,订户可以通过证书变更获得新证书。证书变更视为初始证书申请。

8.8.2 证书变更请求人

证书变更请求人的要求同8.1.1。

8.8.3 证书变更请求的处理

电子认证服务机构应对申请证书变更的订户进行身份鉴别,具体要求同7.2。

8.8.4 订户新证书签发的通知

订户新证书签发的通知要求同8.3.2。

8.8.5 构成变更证书接受的行为

构成变更证书接受的行为要求同8.4.1。

8.8.6 电子认证服务机构对变更证书的发布

电子认证服务机构对变更证书的发布要求同8.4.2。

8.9 证书撤销与挂起

8.9.1 撤销证书的情况

仅当下列情况之一出现时,订户证书才应被撤销并发布在证书撤销列表中;如果订户基于其他情况申请不再使用该证书,则把证书标记为未激活:

- 订户或电子认证服务机构有理由相信或怀疑订户证书对应的私钥出现了安全问题;
- 有证据表明订户违反了证书策略、相应的《电子认证业务规则》和订户协议中的条款或相关法律法规;
- 订户协议终止;
- 电子认证服务机构有理由相信证书中或者证书申请中的信息是错误的。

8.9.2 证书撤销请求人

以下人员可以请求撤销证书:

- 个人证书订户或其授权代表;
- 机构证书订户的授权代表;
- 电子认证服务机构的授权代表;
- 司法机关等公共权力部门的授权代表。

8.9.3 证书撤销请求的处理流程

电子认证服务机构应根据7.4的要求,对证书撤销请求的身份鉴别。

8.9.4 撤销请求的宽限期

证书撤销请求应在发现应撤销证书的情形后的合理时间内提出。该宽限时间应当在《电子认证业务规则》中明确。本标准中证书策略对撤销请求宽限期的时间要求，如表 11 所示。

表 11 证书策略对撤销请求宽限期的时间要求

类别	级别	处理撤销请求的时间要求
基线	基线	电子认证服务机构应在《电子认证业务规则》中对证书撤销请求的宽限期做出明确规定
商业交易	商业交易普通级	电子认证服务机构应在《电子认证业务规则》规定：订户在发现应撤销证书时，应在当日内发起证书撤销请求
	商业交易中级	电子认证服务机构应在《电子认证业务规则》规定：订户在发现应撤销证书时，应在当日内发起证书撤销请求
	商业交易高级	电子认证服务机构应在《电子认证业务规则》规定：订户在发现应撤销证书时，应在当日内发起证书撤销请求
设备	设备普通级	电子认证服务机构应在《电子认证业务规则》规定：订户在发现应撤销证书时，应在当日内发起证书撤销请求
	设备可信级	电子认证服务机构应在《电子认证业务规则》规定：订户在发现应撤销证书时，应在当日内发起证书撤销请求
公众服务	公众服务非实名级	电子认证服务机构应在《电子认证业务规则》规定：订户在发现应撤销证书时，应在当日内发起证书撤销请求
	公众服务实名级	电子认证服务机构应在《电子认证业务规则》规定：订户在发现应撤销证书时，应在当日内发起证书撤销请求

8.9.5 电子认证服务机构处理撤销请求的时间要求

电子认证服务机构应在合理的时间内处理证书撤销请求，并在《电子认证业务规则》中对处理时间做出明确规定。本标准中证书策略对于处理撤销请求的时间要求，如表 12 所示。

表 12 证书策略对电子认证服务机构处理撤销请求的时间要求

类别	级别	处理撤销请求的时间要求
基线	基线	电子认证服务机构应在合理的时间内处理证书撤销请求，并在《电子认证业务规则》中对处理时间做出明确规定
商业交易	商业交易普通级	● 在正常工作时间内收到撤销请求，电子认证服务机构应在该工作日内完成撤销请求的处理； ● 在正常工作时间以外收到撤销请求，电子认证服务机构应在下一工作日完成撤销请求的处理
	商业交易中级	● 在正常工作时间内收到撤销请求，电子认证服务机构应在该工作日内完成撤销请求的处理； ● 在正常工作时间以外收到撤销请求，电子认证服务机构应在下一工作日完成撤销请求处理
	商业交易高级	电子认证服务机构收到撤销请求后应在当天完成撤销请求的处理

表 12（续）

类别	级别	处理撤销请求的时间要求
设备	设备普通级	● 在正常工作时间内收到撤销请求，电子认证服务机构应在该工作日内完成撤销请求的处理； ● 在正常工作时间以外收到撤销请求，电子认证服务机构应在下一工作日完成撤销请求的处理
	设备可信级	电子认证服务机构收到撤销请求后应当天完成撤销请求的处理
公众服务	公众服务非实名级	● 在正常工作时间内收到撤销请求，电子认证服务机构应在该工作日内完成撤销请求的处理； ● 在正常工作时间以外收到撤销请求，电子认证服务机构应在下一工作日完成撤销请求的处理
	公众服务实名级	● 在正常工作时间内收到撤销请求，电子认证服务机构应在该工作日内完成撤销请求的处理； ● 在正常工作时间以外收到撤销请求，电子认证服务机构应在下一工作日完成撤销请求的处理

8.9.6 依赖方进行撤销检查的要求

依赖方在信任证书前，应对证书信任链上所有证书的状态进行检查，获得证书状态的方法包括：

- 查询最新的证书撤销列表；
- 通过 Web 数据库查询证书状态；
- 通过 OCSP 方式查询。

依赖方还应对上述证书状态信息的有效性进行验证。

8.9.7 证书撤销列表签发频率

电子认证服务机构应定时签发证书撤销列表，对于电子认证服务机构证书的证书撤销列表，应至少每年签发一次，或者当电子认证服务机构的证书应撤销时签发证书撤销列表。本标准中证书策略对终端订户证书的证书撤销列表签发频率的要求如表 13 所示。

表 13 证书策略对证书撤销列表签发频率的要求

类别	级别	证书撤销列表签发频率要求
基线	基线	至少每 24 h 签发一次
商业交易	商业交易普通级	● 至少每 24 h 签发一次； ● 当由于密钥泄露或者怀疑被泄露而发生的证书撤销，电子认证服务机构应立即签发撤销列表
	商业交易中级	● 至少每 24 h 签发一次； ● 当由于密钥泄露或者怀疑被泄露而发生的证书撤销，电子认证服务机构应立即签发撤销列表
	商业交易高级	● 至少每 12 h 签发一次； ● 当由于密钥泄露或者怀疑被泄露而发生的证书撤销，电子认证服务机构应立即签发撤销列表

表 13（续）

类别	级别	证书撤销列表签发频率要求
设备	设备普通级	● 至少每 24 h 签发一次； ● 当由于密钥泄露或者怀疑被泄露而发生的证书撤销，电子认证服务机构应立即签发撤销列表
	设备可信级	● 至少每 12 h 签发一次； ● 当由于密钥泄露或者怀疑被泄露而发生的证书撤销，电子认证服务机构应立即签发撤销列表
公众服务	公众服务非实名级	● 至少每 24 h 签发一次； ● 当由于密钥泄露或者怀疑被泄露而发生的证书撤销，电子认证服务机构应立即签发撤销列表
	公众服务实名级	● 至少每 24 h 签发一次； ● 当由于密钥泄露或者怀疑被泄露而发生的证书撤销，电子认证服务机构应立即签发撤销列表

8.9.8 证书撤销列表发布的最长滞后时间

证书撤销列表生成后，应及时发布到资料库中。

8.9.9 证书状态在线检查的可用性

撤销信息或其他证书状态信息应通过 Web 数据库、LDAP 服务器或者 OCSP 服务在线获得。如果电子认证服务机构提供 LDAP 服务、Web 网站服务或者 OCSP 服务，并且允许依赖方进行在线查询，则电子认证服务机构应向依赖方提供相关的信息，告知依赖方如何访问合适的 LDAP 服务、Web 网站服务或 OCSP 服务。本标准中证书策略对证书状态在线检查方式的要求，如表 14 所示。

表 14 证书策略对证书状态在线检查的可用性的要求

类别	级别	证书状态在线检查的可用性的要求
基线	基线	应通过 LDAP 服务、Web 网站服务或者 OCSP 服务在线获得
商业交易	商业交易普通级	至少提供 Web 网站服务和 LDAP 服务中的任意一种
	商业交易中级	至少提供 Web 网站服务、LDAP 服务和 OCSP 服务中的任意两种
	商业交易高级	提供 Web 网站服务、LDAP 服务和 OCSP 服务
设备	设备普通级	至少提供 Web 网站服务、LDAP 服务和 OCSP 服务中的任意两种
	设备可信级	提供 Web 网站服务、LDAP 服务和 OCSP 服务
公众服务	公众服务非实名级	至少提供 Web 网站服务、LDAP 服务或者 OCSP 服务中的任意两种
	公众服务实名级	至少提供 Web 网站服务、LDAP 服务或者 OCSP 服务中的任意两种

8.9.10 证书状态在线检查的要求

依赖方在信任证书前应检查该证书的状态。

8.9.11 密钥泄露的特殊要求

如果电子认证服务机构发现或有理由相信其私钥泄露，应立即上报电子认证服务管理部门，并尽可能及时通知所有订户、所有潜在的证书依赖方和其他参与方。

8.9.12 证书挂起的情况

订户证书的挂起，不作规定。

商业交易类、设备类、公众服务类证书策略要求电子认证服务机构证书不应被挂起。

8.10 证书状态服务

8.10.1 执行方法

证书状态可以通过 Web 网站服务、LDAP 服务提供的 CRL 或者 OCSP 服务在线查询获得。

8.10.2 服务可用性

证书状态服务应保证 7×24 不间断可用，不允许安排服务中断时间。

8.11 订购的终止

订户出现下列情形时意味着该订户的证书订购已经结束：

- 证书有效期满，并没有进行证书更新、证书变更或密钥更换；
- 证书有效期内证书被撤销，且没有进行证书更新、证书变更或密钥更换。

8.12 密钥托管和恢复

8.12.1 密钥托管和恢复的策略与实施

电子认证服务机构和订户的签名密钥都不应被托管。

电子认证服务机构可以为订户的加密密钥提供密钥恢复服务，提供密钥恢复服务的应在其《电子认证业务规则》中详细描述安全保障措施和服务流程。

电子认证服务机构也可以通过第三方权威机构为订户提供加密密钥托管和恢复服务，并在其《电子认证业务规则》中进行说明。

8.12.2 会话密钥封装和恢复的策略与实施

如果电子认证服务机构提供会话密钥封装和恢复服务，应在其《电子认证业务规则》中规定具体的实施流程。

9 设施、管理和运作控制

9.1 物理安全控制

9.1.1 场所位置和建筑

电子认证服务机构的所有操作应在受到物理保护的环境下进行。所采取的物理保护手段应能够保护敏感的信息和系统，防止并检测未经电子认证服务机构授权的访问、使用或披露。

电子认证服务机构应建立多级的物理安全防护区，并对不同安全级别的区域采取不同安全强度的物理防护措施。本标准中证书策略对区域分级控制的要求，如表 15 所示。

表 15　证书策略中场所位置和建筑的要求

类别	级别	区域分级控制
基线	基线	应建立多级的物理安全防护区，并对不同安全级别的区域采取不同安全强度的物理防护措施
商业交易	商业交易普通级	至少两个区域，核心区和非核心区，电子认证服务机构签名密钥的存储和使用设备需存放在安全级别较高的核心区，并进行电子屏蔽，保证非屏蔽时间每天少于 10 min
	商业交易中级	至少 3 个区域，核心区、控制区和服务区，电子认证服务机构密钥的存储和使用设备需放置在安全级别最高的核心区，并进行电子屏蔽，不允许任何时长的非屏蔽；发布签名命令的设备以及涉及隐私信息的资料或数据库需放置在安全级别次高的控制区
	商业交易高级	至少 4 个区域，核心区、控制区、支持区和接待区，电子认证服务机构密钥的存储和使用设备需放置在安全级别最高的核心区，并进行电子屏蔽，不允许任何时长的非屏蔽；发布签名命令的设备以及涉及隐私信息的资料或数据库需放置在安全级别次高的控制区；资料库、Web 服务器和监控等重要设备需放置在安全级别较高的支持区
设备	设备普通级	至少 3 个区域，核心区、控制区和服务区，电子认证服务机构密钥的存储和使用设备需放置在安全级别最高的核心区，并进行电子屏蔽，保证非屏蔽时间每天少于 10 min；发布签名命令的设备以及涉及隐私信息的资料或数据库需放置在安全级别次高的控制区
	设备可信级	至少 4 个区域，核心区、控制区、支持区和接待区，电子认证服务机构密钥的存储和使用设备需放置在安全级别最高的核心区，并进行电子屏蔽，不允许任何时长的非屏蔽；发布签名命令的设备以及涉及隐私信息的资料或数据库需放置在安全级别次高的控制区；资料库、Web 服务器和监控等重要设备需放置在安全级别较高的支持区
公众服务	公众服务非实名级	至少 3 个区域，核心区、控制区和服务区，电子认证服务机构密钥的存储和使用设备需放置在安全级别最高的核心区，并进行电子屏蔽，不允许任何时长的非屏蔽；发布签名命令的设备以及涉及隐私信息的资料或数据库需放置在安全级别次高的控制区
	公众服务实名级	至少 3 个区域，核心区、控制区和服务区，电子认证服务机构密钥的存储和使用设备需放置在安全级别最高的核心区，并进行电子屏蔽，不允许任何时长的非屏蔽；发布签名命令的设备以及涉及隐私信息的资料或数据库需放置在安全级别次高的控制区

9.1.2　物理访问

当人员从一个区域进入另一个区域或者进入安全级别较高的区域时，应通过相应的访问控制。

只有授权人员才能对电子认证服务机构的物理设备进行操作。本标准中证书策略对不同安全区域的具体访问控制要求如表 16 所示。

表 16　证书策略对不同安全区域的访问控制要求

区域名称	访问控制要求
核心区	两人或两人以上共同操作
控制区	两人或两人以上共同操作
支持区	单人双因素认证
服务区	电子门禁系统； 外来访客需验证身份后登记方可进入
接待区	电子门禁系统； 外来访客需验证身份后登记方可进入
非核心区	电子门禁系统； 外来访客需验证身份后登记方可进入

9.1.3　电力和空调

电子认证服务机构的安全设施应具有主、备电力供应系统，以确保持续不间断的电力供应。同时对于关键的安全设施，也应具有主、备空调系统来控制温度和湿度。

9.1.4　防水措施

电子认证服务机构的安全设施应安装在具有防水设备的场所，并制定相应的流程，以防止洪水或者其他由于暴露在有水的环境对系统造成的损害。

9.1.5　火灾预防与保护

电子认证服务机构的设备机房应提供火灾自动报警系统和应急处理装置，并制定有相应的处理流程，以防止明火或者烟雾对电子认证系统造成损害或不利影响。

签发商业交易高级和设备可信级策略证书的电子认证服务机构的核心区需配备气体灭火装置。

9.1.6　介质存储

电子认证服务机构应保证存储介质不会被意外破坏（如：水，火和电磁干扰），不被未经授权的物理访问。

9.1.7　废弃物处理

电子认证服务机构应制定废弃物处理流程，对不再使用的敏感介质、文件和其他废弃物，应以安全的方式销毁，销毁方法包括但不限于以下形式：

- 纸质的敏感信息应通过粉碎、焚烧或其他不可恢复的方法处理；
- 信息系统的存储介质和废弃的密码设备等应根据制造商的指南将其物理销毁。

9.1.8　异地备份

电子认证服务机构应对关键数据和其他包括审计数据在内的敏感信息提供安全的异地备份。本标准中证书策略对异地备份的要求，如表 17 所示。

表 17　证书策略中对异地备份的要求

类别	级别	异地备份要求
基线	基线	● 备份中心应设在不同的地级行政单位； ● 备份中心与生产中心直线距离在 10 km 以上
商业交易	商业交易普通级	● 备份中心应设在不同的地级行政单位； ● 备份中心与生产中心直线距离在 10 km 以上
	商业交易中级	● 备份中心应设在不同的地级行政单位； ● 备份中心与生产中心直线距离在 10 km 以上
	商业交易高级	● 备份中心应设在不同的地级行政单位； ● 备份中心与生产中心直线距离在 50 km 以上
设备	设备普通级	● 备份中心应设在不同的地级行政单位； ● 备份中心与生产中心直线距离在 10 km 以上
	设备可信级	● 备份中心应设在不同的地级行政单位； ● 备份中心与生产中心直线距离在 50 km 以上
公众服务	公众服务非实名级	● 备份中心应设在不同的地级行政单位； ● 备份中心与生产中心直线距离在 50 km 以上
	公众服务实名级	● 备份中心应设在不同的地级行政单位； ● 备份中心与生产中心直线距离在 50 km 以上

9.2　流程控制

9.2.1　关键岗位

关键岗位包括应访问、操作或者管理认证和密码设备的岗位。

服务于关键岗位的员工被认为是可信人员。参与关键岗位操作的第三方服务人员和顾问等应被认定为“等同可信人员”。成为可信人员应符合本标准中证书策略关于人员的要求。

9.2.2　每项任务需要的人数

电子认证服务机构应该建立、维护和执行严格的控制流程，进行职责分离，确保敏感操作由多名可信人员参与才能完成。例如：对于设备的物理访问和逻辑访问应进行职责分离。

特别敏感的操作应有多名可信人员共同参与，如：访问和管理电子认证服务机构的硬件密码设备和相关的密钥材料等。

本标准中敏感操作包括但不限于：

- 访问资料库中严格控制的区域；
- 生成、签发和销毁电子认证服务机构证书；
- 电子认证服务系统的维护。

本标准中证书策略对敏感操作参与人数的要求，如表 18 所示。

表 18　证书策略中敏感操作参与人数的要求

类别	级别	人数要求
基线	基线	至少 2 名
商业交易	商业交易普通级	至少 2 名
	商业交易中级	至少 2 名
	商业交易高级	至少 3 名
设备	设备普通级	至少 2 名
	设备可信级	至少 3 名
公众服务	公众服务非实名级	至少 2 名
	公众服务实名级	至少 2 名

9.2.3　岗位的标识和鉴别

在执行下述操作前，电子认证服务机构应对服务于关键岗位的人员进行身份鉴别：

- 为可信人员分配用于访问物理设备、设施的权限，并发放实现上述权限所需的门禁卡、钥匙等；
- 为其发放电子凭证，用于访问特定的信息系统和电子认证服务系统。

身份的鉴别应包括：行使人事职能或者安全管理的可信人员应对被调查人的身份进行当面的核查，并要求被调查人提供有效身份证件。更进一步的背景调查应按照 9.3.2 的要求进行。

9.2.4　需要职责分离的岗位

同一个人员不应同时服务于以下任何两个或两个以上的岗位。应进行职责分离的岗位包括但不限于：

- 证书申请信息的验证；
- 证书申请、撤销请求、更新请求、信息变更的批准、拒绝或其他；
- 签发或撤销证书，以及对资料库中严格控制区域的访问；
- 订户信息或者订户请求的保管；
- 生成、签发和销毁电子认证服务机构证书；
- 电子认证服务系统的维护。

9.3　人员控制

9.3.1　资历和安全要求

电子认证服务机构应要求可信人员提供有关教育背景、资格证书以及相关从业经历的证明。如果需要，也应要求可信人员提供无犯罪证明。

9.3.2　背景审查流程

电子认证服务机构应制定并执行严格的背景审查流程，对担当关键岗位的人员进行审查，并定期进行复审。本标准中证书策略对背景审查流程的要求，如表 19 所示。

表 19　证书策略中背景审查流程的要求

类别	级别	背景审查流程要求
基线	基线	背景调查中，有下列行为的被审查人不应通过审查： ● 被审查人提供虚假信息； ● 有犯罪记录
商业交易	商业交易普通级	背景调查中，有下列行为的被审查人不应通过审查： ● 被审查人提供虚假信息； ● 有犯罪记录
	商业交易中级	背景调查中，有下列行为的被审查人不应通过审查： ● 被审查人提供虚假信息； ● 有犯罪记录； ● 有不良财务记录
	商业交易高级	背景调查中，有下列行为的被审查人不应通过审查： ● 被审查人提供虚假信息； ● 有犯罪记录； ● 有不良财务记录。 被审查人应提供推荐信
设备	设备普通级	背景调查中，有下列行为的被审查人不应通过审查： ● 被审查人提供虚假信息； ● 有犯罪记录
	设备可信级	背景调查中，有下列行为的被审查人不应通过审查： ● 被审查人提供虚假信息； ● 有犯罪记录； ● 有不良财务记录。 被审查人应提供推荐信
公众服务	公众服务非实名级	背景调查中，有下列行为的被审查人不应通过审查： ● 被审查人提供虚假信息； ● 有犯罪记录； ● 有不良财务记录。 被审查人应提供推荐信
	公众服务实名级	背景调查中，有下列行为的被审查人不应通过审查： ● 被审查人提供虚假信息； ● 有犯罪记录； ● 有不良财务记录。 被审查人应提供推荐信

9.3.3　培训要求

电子认证服务机构应对其人员进行培训，培训内容与人员对应职责相关，包括：使用、操作和维护电子认证服务系统过程中涉及的职责、安全机制（例如：灾难恢复的方法、业务连续性要求）以及电子认证服务系统的软硬件操作规范等。

电子认证服务机构应定期对培训内容进行审查。

9.3.4 培训周期要求

电子认证服务机构应定期对相关人员进行培训。

当《电子认证业务规则》有重大的内容更新或电子认证服务机构系统有重大的升级改动时，电子认证服务机构应及时对相关人员进行培训。本标准中证书策略对培训周期的要求，如表 20 所示。

表 20 证书策略中对培训周期的要求

类别	级别	培训周期要求
基线	基线	● 至少每年培训一次； ● 重大的内容更新或电子认证服务机构系统有重大的升级改动，应进行培训
商业交易	商业交易普通级	● 至少每年培训一次； ● 重大的内容更新或电子认证服务机构系统有重大的升级改动，应进行培训
	商业交易中级	● 至少每年培训一次； ● 重大的内容更新或电子认证服务机构系统有重大的升级改动，应进行培训
	商业交易高级	● 至少每半年培训一次； ● 重大的内容更新或电子认证服务机构系统有重大的升级改动，应进行培训
设备	设备普通级	● 至少每年培训一次； ● 重大的内容更新或电子认证服务机构系统有重大的升级改动，应进行培训
	设备可信级	● 至少每半年培训一次； ● 重大的内容更新或电子认证服务机构系统有重大的升级改动，应进行培训
公众服务	公众服务非实名级	● 至少每年培训一次； ● 重大的内容更新或电子认证服务机构系统有重大的升级改动，应进行培训
	公众服务实名级	● 至少每年培训一次； ● 重大的内容更新或电子认证服务机构系统有重大的升级改动，应进行培训

9.3.5 未授权行为的处罚

电子认证服务机构应建立、维护和实施相应的管理办法，对相关人员的未授权行为，如：对电子认证服务系统和资料库等进行的未经授权访问，进行处罚，未授权行为出现的次数和严重程度不同，处罚的力度也应不同。

9.3.6 独立合约人的要求

当满足如下条件时，电子认证服务机构应允许独立合约人或者顾问成为“等同可信人员”：

- 没有合适的雇员能够担当这个岗位的职责；
- 独立合约人或者顾问与雇员具有同等的可信度。

另外，应访问电子认证服务机构的安全设施的独立合约人和顾问，应由电子认证机构的可信人员陪同。

9.3.7 提供给员工的文档

为保障电子认证服务机构运营的规范和安全，电子认证服务机构应确保所有员工能够获得完成工作职责所需的文档，这些文档包括：岗位职责、业务操作说明和电子认证服务机构安全管理的相关规范等。

9.4 审计日志处理流程

9.4.1 应纳入审计记录的事件类型

电子认证服务机构应对审计事件进行记录并审计。所有电子或手工生成的日志都应当包括事件信息、时间和引发事件的实体身份。电子认证服务机构应在《电子认证业务规则》中描述其记录的事件类型。

纳入审计的事件类型包括：

- 对电子认证服务系统的操作事件；
- 证书生命周期事件；
- 可信人员的操作事件；
- 不符合规程的事件。

9.4.2 日志处理周期

电子认证服务机构应对日志进行定期处理，以便发现重要的安全和操作事件。对日志的处理包括：

- 检查日志的完整性；
- 查看日志中的所有记录；
- 分析重要事件的原因并形成总结文档；
- 针对日志中安全记录的事件采取行动，并通过文档记录上述行动。

本标准中证书策略对日志处理周期的要求如表 21 所示。

表 21 证书策略对日志处理周期的要求

类别	级别	日志处理周期要求
基线	基线	定期处理
商业交易	商业交易普通级	至少每周
	商业交易中级	至少每两天
	商业交易高级	至少每天
设备	设备普通级	至少每两天
	设备可信级	至少每天
公众服务	公众服务非实名级	至少每两天
	公众服务实名级	至少每两天

9.4.3 审计日志的保存期限

审计日志被处理后，在日志生成所在地保存时间不应少于3年。

9.4.4 审计日志的保护

电子认证服务机构应确保审计日志不被未经授权的访问、复制、修改和删除。

9.4.5 审计日志的备份

审计日志应定期进行备份。本标准中证书策略对日志备份周期要求，如表22所示。

表22 证书策略对审计日志备份周期的要求

类别	级别	日志备份周期要求
基线	基线	定期备份
商业交易	商业交易普通级	至少每月
	商业交易中级	至少每两周
	商业交易高级	至少每周
设备	设备普通级	至少每两周
	设备可信级	至少每周
公众服务	公众服务非实名级	至少每两周
	公众服务实名级	至少每两周

9.4.6 审计日志收集系统(内部或外部)

基线证书策略对审计日志收集系统不作规定。

商业交易类、设备类、公众服务类证书策略要求电子认证服务机构应建立统一的审计日志收集系统，并由专人负责管理。

9.4.7 脆弱性评估

通过对日志中记录的事件进行审查，对系统的脆弱性进行评估。这种评估应定期执行，并形成脆弱性评估报告。本标准中证书策略对脆弱性评估的周期的要求，如表23所示。

表23 证书策略对脆弱性评估周期的要求

类别	级别	脆弱性评估周期要求
基线	基线	定期执行
商业交易	商业交易普通级	至少每年
	商业交易中级	至少每半年
	商业交易高级	至少每3个月
设备	设备普通级	至少每半年
	设备可信级	至少每3个月
公众服务	公众服务非实名级	至少每半年
	公众服务实名级	至少每半年

9.5 记录归档

9.5.1 归档的记录类型

电子认证服务机构至少应归档以下记录：

- 所有在 9.4 涉及的审计数据；
- 证书申请的相关信息；
- 证书生命周期的相关信息。

9.5.2 归档记录的保存期限

电子认证服务机构的归档记录应至少保存 5 年。

9.5.3 归档记录的保护

电子认证服务机构应采取安全措施，保证未经授权的用户不会浏览、修改和删除电子认证服务机构的归档记录。

商业交易类、设备类、公众服务类证书策略要求归档记录应采用加密或物理方式进行保护。若采用电子方式进行归档，应采用只读介质。

9.5.4 归档记录的备份流程

电子认证服务机构应对电子和纸质归档记录定期进行异地备份。本标准中证书策略对异地备份周期的要求，如表 24 所示。

表 24 证书策略对归档记录备份流程的要求

类别	级别	归档记录异地备份的周期
基线	基线	定期进行
商业交易	商业交易普通级	至少每月
	商业交易中级	至少每两周
	商业交易高级	至少每周
设备	设备普通级	至少每两周
	设备可信级	至少每周
公众服务	公众服务非实名级	至少每两周
	公众服务实名级	至少每两周

9.5.5 归档记录的时间标记要求

电子认证服务机构的归档记录应包含记录产生的时间和日期信息。

9.5.6 归档记录收集系统(内部或外部)

电子认证服务机构应该设立内部的档案管理专门机构，统一管理归档记录及其备份。

9.5.7 访问和检验归档记录的流程

只有经授权的可信人员才能访问归档记录。所有归档记录的调用查阅应当记录在案。调用查阅后重新归档时,需验证其完整性。

9.6 电子认证服务机构密钥的更替

电子认证服务机构根密钥的更替,应上报电子认证服务管理部门,并在其监督下重新生成新的密钥。更替完成后应将自签名证书交电子认证服务管理部门备案,并按照 10.1.4 的要求将电子认证服务机构公钥传递给依赖方。

9.7 事故和灾难恢复

9.7.1 事故处理流程

电子认证服务机构应该针对事故的性质制定和实施灾难恢复流程。重大事故需立即上报电子认证服务管理部门。

9.7.2 计算资源、软件和/或数据遭到破坏

电子认证服务机构的计算资源、软件和/或数据等遭到破坏后,电子认证服务机构应采取相应的业务恢复措施。

9.7.3 电子认证服务机构私钥泄露的处理流程

一旦电子认证服务机构的密钥泄露应被撤销,应立即上报电子认证服务管理部门,并尽可能地通知潜在的依赖方。

9.7.4 灾难发生后的业务连续性

电子认证服务机构应明确灾难发生后的业务恢复时间,用于保证灾难发生后的业务连续性。本标准中证书策略对灾后业务恢复时间要求,如表 25 所示。

表 25 证书策略对灾后业务恢复时间的要求

类别	级别	灾后业务恢复时间要求
基线	基线	应明确灾后业务恢复时间
商业交易	商业交易普通级	72 h 内
	商业交易中级	36 h 内
	商业交易高级	24 h 内
设备	设备普通级	36 h 内
	设备可信级	24 h 内
公众服务	公众服务非实名级	36 h 内
	公众服务实名级	36 h 内

9.8 电子认证服务的终止

电子认证服务机构应制定服务终止计划，并在《电子认证业务规则》中公开。

10 技术安全控制

10.1 密钥对的生成和安装

10.1.1 密钥对的生成

10.1.1.1 电子认证服务机构的密钥的生成

电子认证服务机构用于签发证书和证书状态信息的密钥（含根密钥）应由专门的硬件设备生成，生成密钥的系统应能保护私钥不被丢失、泄露、修改和未经授权的访问。

电子认证服务机构的根密钥生成应上报电子认证服务管理部门，在电子认证服务管理部门或相关主管部门的监督下生成，并将自签名证书交电子认证服务管理部门备案。

10.1.1.2 订户密钥的生成

订户的密钥对应由订户、电子认证服务机构或电子认证服务机构委托的机构生成，生成密钥的系统应能保护私钥不被丢失、泄露、修改和未经授权的访问。

由电子认证服务机构或其委托的机构生成的订户密钥的传递要符合 10.1.2 的要求。

商业交易中级、商业交易高级、设备可信级、公众服务非实名级和公众服务实名级证书策略要求证书的签名密钥应在密码硬件设备中生成。

10.1.2 递交私钥给订户

如果订户自己生成密钥对，则不应进行私钥传递。

电子认证服务机构或其委托机构代替订户生成私钥，应确保将订户私钥安全地递交给订户。如果密钥对在电子认证服务机构提供的硬件令牌中生成，分发这些令牌应采取合理的方式提供物理安全防护措施，防止令牌中的私钥丢失、泄露、修改和未经授权访问。

10.1.3 递交公钥给证书签发机构

订户将自己生成的公钥递给证书签发机构时，应保证公钥的完整性，并证明其拥有公钥对应的私钥。

10.1.4 传送电子认证服务机构公钥给依赖方

电子认证服务机构应当通过安全的途径发布自签名证书或由电子认证服务管理部门发布自签名证书。发布方法包括但不限于：

- 将自签名证书下载到令牌中，通过安全的渠道传递给依赖方；
- 通过安全的带外方式发布自签名证书或自签名证书的杂凑函数值；
- 将自签名证书上载到可信的 Web 站点；
- 由电子认证服务管理部门对合法 CA 的公钥进行签名并发布。

本标准中证书策略对电子认证服务机构公钥发布的要求，如表 26 所示。

表 26　证书策略对电子认证服务机构公钥发布的要求

类别	级别	电子认证服务机构公钥发布要求
基线	基线	上述发布方法中的任意一种
商业交易	商业交易普通级	上述发布方法中的任意两种
	商业交易中级	电子认证服务管理部门认可的新闻媒体和第三方网站上发布自签名证书或其杂凑函数值
	商业交易高级	电子认证服务管理部门认可的新闻媒体和第三方网站上发布自签名证书或其杂凑函数值，并在营业场所提供含自签名证书杂凑函数值的纸质证明文件
设备	设备普通级	电子认证服务管理部门认可的新闻媒体和第三方网站上发布自签名证书或其杂凑函数值
	设备可信级	电子认证服务管理部门认可的新闻媒体和第三方网站上发布自签名证书或其杂凑函数值，并在营业场所提供含自签名证书杂凑函数值的纸质证明文件
公众服务	公众服务非实名级	电子认证服务管理部门认可的新闻媒体和第三方网站上发布自签名证书或其杂凑函数值
	公众服务实名级	电子认证服务管理部门认可的新闻媒体和第三方网站上发布自签名证书或其杂凑函数值

10.1.5　密钥长度

本标准中证书策略对电子认证服务机构的根密钥长度安全性的要求，如表 27 所示。

表 27　证书策略对电子认证服务机构根密钥长度安全性的要求

类别	级别	电子认证服务机构根密钥长度要求
基线	基线	安全强度不低于 2 048 bit 的 RSA 密钥
商业交易	商业交易普通级	安全强度不低于 2 048 bit 的 RSA 密钥
	商业交易中级	安全强度不低于 2 048 bit 的 RSA 密钥
	商业交易高级	安全强度不低于 4 096 bit 的 RSA 密钥
设备	设备普通级	安全强度不低于 2 048 bit 的 RSA 密钥
	设备可信级	安全强度不低于 4 096 bit 的 RSA 密钥
公众服务	公众服务非实名级	安全强度不低于 2 048 bit 的 RSA 密钥
	公众服务实名级	安全强度不低于 2 048 bit 的 RSA 密钥

本标准中证书策略对电子认证服务机构的签名密钥长度安全性的要求，如表 28 所示。

表 28　证书策略对电子认证服务机构签名密钥长度安全性的要求

类别	级别	电子认证服务机构签名密钥长度要求
基线	基线	安全强度不低于 2 048 bit 的 RSA 密钥
商业交易	商业交易普通级	安全强度不低于 2 048 bit 的 RSA 密钥
	商业交易中级	安全强度不低于 2 048 bit 的 RSA 密钥
	商业交易高级	安全强度不低于 2 048 bit 的 RSA 密钥
设备	设备普通级	安全强度不低于 2 048 bit 的 RSA 密钥
	设备可信级	安全强度不低于 2 048 bit 的 RSA 密钥
公众服务	公众服务非实名级	安全强度不低于 2 048 bit 的 RSA 密钥
	公众服务实名级	安全强度不低于 2 048 bit 的 RSA 密钥

本标准中证书策略对于订户的密钥长度安全性的要求，如表 29 所示。

表 29　证书策略对订户密钥长度安全性的要求

类别	级别	订户密钥长度要求
基线	基线	安全强度不低于 1 024 bit 的 RSA 密钥
商业交易	商业交易普通级	安全强度不低于 2 048 bit 的 RSA 密钥
	商业交易中级	安全强度不低于 2 048 bit 的 RSA 密钥
	商业交易高级	安全强度不低于 2 048 bit 的 RSA 密钥
设备	设备普通级	安全强度不低于 2 048 bit 的 RSA 密钥
	设备可信级	安全强度不低于 2 048 bit 的 RSA 密钥
公众服务	公众服务非实名级	安全强度不低于 2 048 bit 的 RSA 密钥
	公众服务实名级	安全强度不低于 2 048 bit 的 RSA 密钥

10.1.6　公钥参数的生成和质量检查

公钥参数应使用国家密码主管部门批准的方式生成和选取，并遵守相应的生成规范和标准。

10.1.7　密钥用途

密钥用途应与证书中“密钥用途”扩展内容一致。

签发商业交易中级、商业交易高级、设备可信级、公众服务非实名级和公众服务实名级策略证书的电子认证服务机构根密钥不应直接用于签发订户证书。

10.2　私钥保护和密码模块的工程控制

10.2.1　密码模块标准和控制

订户应按照与电子认证服务机构签订的相关协议要求选用密码模块，并妥善保管私钥。

电子认证服务机构所使用的密码模块，应通过国家密码主管部门的专门检测。

本标准中证书策略对电子认证服务机构所使用的密码模块的要求，如表 30 所示。

表 30　证书策略对密码模块的要求

类别	级别	密码模块要求
基线	基线	应通过国家密码主管部门的专门检测
商业交易	商业交易普通级	● 应通过国家密码主管部门的专门检测； ● 采用基于角色鉴别的访问控制； ● 具有开启证据； ● 使用不透明的覆盖物或封壳保护
	商业交易中级	● 应通过国家密码主管部门的专门检测； ● 采用基于角色鉴别的访问控制； ● 具有开启证据； ● 使用不透明的覆盖物或封壳保护； ● 具有开启响应和置零电路
	商业交易高级	● 应通过国家密码主管部门的专门检测； ● 关键安全参数的输入输出端口和接口与其他端口和接口物理隔离或者通过可信通道逻辑隔离； ● 密码模块采用基于身份鉴别的双因素访问控制； ● 密码模块具有开启证据； ● 使用不透明的覆盖物或封壳保护； ● 具有开启响应和置零电路； ● 密码模块具有温度和电压失效检测和保护电路
设备	设备普通级	● 应通过国家密码主管部门的专门检测； ● 密码模块采用基于身份鉴别的访问控制； ● 具有开启证据； ● 使用不透明的覆盖物或封壳保护； ● 具有开启响应和置零电路
	设备可信级	● 应通过国家密码主管部门的专门检测； ● 关键安全参数的输入输出端口和接口与其他端口和接口物理隔离或者通过可信通道逻辑隔离； ● 密码模块采用基于身份鉴别的双因素访问控制； ● 密码模块具有开启证据； ● 使用不透明的覆盖物或封壳保护； ● 具有开启响应和置零电路； ● 密码模块具有温度和电压失效检测和保护电路
公众服务	公众服务非实名级	● 应通过国家密码主管部门的专门检测； ● 密码模块采用基于身份鉴别的访问控制； ● 具有开启证据； ● 使用不透明的覆盖物或封壳保护； ● 具有开启响应和置零电路
	公众服务实名级	● 应通过国家密码主管部门的专门检测； ● 密码模块采用基于身份鉴别的访问控制； ● 具有开启证据； ● 使用不透明的覆盖物或封壳保护； ● 具有开启响应和置零电路

10.2.2 私钥多人控制

对于电子认证服务机构的私钥的敏感操作，包括私钥激活、备份和恢复等，应采用多人控制策略，针对同一私钥的多人控制策略中的门限值应该是一致的。本标准中证书策略对电子认证服务机构私钥多人控制的要求，如表31所示。

表31 证书策略对私钥多人控制的要求

类别	级别	私钥多人控制要求
基线	基线	应采用多人控制策略，针对同一私钥的多人控制策略中的门限值应该是一致的
商业交易	商业交易普通级	私钥激活、备份和恢复，应至少2人共同控制。有权参与控制的总人数不应超过5人
	商业交易中级	私钥激活、备份和恢复，应至少3人共同控制。有权参与控制的总人数不应超过7人
	商业交易高级	私钥激活、备份和恢复，应至少3人共同控制。有权参与控制的总人数不应超过6人
设备	设备普通级	私钥激活、备份和恢复，应至少3人共同控制。有权参与控制的总人数不应超过7人
	设备可信级	私钥激活、备份和恢复，应至少3人共同控制。有权参与控制的总人数不应超过6人
公众服务	公众服务非实名级	私钥激活、备份和恢复，应至少3人共同控制。有权参与控制的总人数不应超过7人
	公众服务实名级	私钥激活、备份和恢复，应至少3人共同控制。有权参与控制的总人数不应超过7人

10.2.3 私钥托管

电子认证服务机构的私钥和订户的签名私钥不应托管。订户密钥的托管应参照8.12的要求。

10.2.4 私钥备份

10.2.4.1 电子认证服务机构私钥的备份

本标准中证书策略对电子认证服务机构私钥的备份要求，如表32所示。

表32 证书策略对电子认证服务机构私钥备份的要求

类别	级别	电子认证服务机构私钥备份要求
基线	基线	电子认证服务机构私钥的备份应由多人控制，并放置在同样安全的场所
商业交易	商业交易普通级	电子认证服务机构私钥的应进行备份，并放置在同等安全程度的场所。电子认证服务机构私钥的备份应由多人控制，要求参照10.2.2
	商业交易中级	电子认证服务机构私钥的应进行备份，并放置在同等安全程度的场所。电子认证服务机构私钥的备份应由多人控制，要求参照10.2.2
	商业交易高级	电子认证服务机构私钥的应进行备份，并放置在同等安全程度的场所。电子认证服务机构私钥的备份应由多人控制，要求参照10.2.2。至少有一个备份在异地

表 32（续）

类别	级别	电子认证服务机构私钥备份要求
设备	设备普通级	电子认证服务机构私钥的应进行备份，并放置在同等安全程度的场所。电子认证服务机构私钥的备份应由多人控制，要求参照 10.2.2
	设备可信级	电子认证服务机构私钥的应进行备份，并放置在同等安全程度的场所。电子认证服务机构私钥的备份应由多人控制，要求参照 10.2.2。至少有一个备份在异地
公众服务	公众服务非实名级	电子认证服务机构私钥的应进行备份，并放置在同等安全程度的场所。电子认证服务机构私钥的备份应由多人控制，要求参照 10.2.2
	公众服务实名级	电子认证服务机构私钥的应进行备份，并放置在同等安全程度的场所。电子认证服务机构私钥的备份应由多人控制，要求参照 10.2.2

10.2.4.2 订户私钥备份

本标准中证书策略对于订户私钥备份的要求，如表 33 所示。

表 33 证书策略对订户私钥备份的要求

类别	级别	订户私钥备份要求
基线	基线	如果电子认证服务机构对订户私钥提供备份和恢复服务，则应采用物理或密码学手段对备份的私钥进行保护
商业交易	商业交易普通级	允许私钥备份，但备份私钥应在订户的控制之下。订户的密钥备份应有物理或密码学手段的保护，在密码模块之外不允许明文存在
	商业交易中级	允许私钥备份，但备份私钥应在订户的控制之下。订户的密钥备份和恢复应有物理或密码学手段的保护，在密码模块之外不允许明文存在
	商业交易高级	不允许私钥备份
设备	设备普通级	允许私钥备份，但备份私钥应在订户的控制之下。订户的密钥备份和恢复应有物理或密码学手段的保护，在密码模块之外不允许明文存在
	设备可信级	不允许私钥备份
公众服务	公众服务非实名级	允许私钥备份，但备份私钥应在订户的控制之下。订户的密钥备份和恢复应有物理或密码学手段的保护，在密码模块之外不允许明文存在
	公众服务实名级	允许私钥备份，但备份私钥应在订户的控制之下。订户的密钥备份和恢复应有物理或密码学手段的保护，在密码模块之外不允许明文存在

10.2.5 私钥归档

电子认证服务机构的签名私钥在失效后应与密码模块一起进行归档，不应被再次使用。归档的具体要求参见 9.5。

对于订户私钥的归档不作规定。

10.2.6 私钥导入或导出密码模块

私钥应在密码模块中产生，在不同模块之间传输密钥时，应采用物理的或者密码学手段进行保护，

防止私钥被丢失、偷窃、修改、泄露或者未经授权的使用。本标准中证书策略对私钥导入和导出的要求，如表 34 所示。

表 34　证书策略对私钥导入或导出密码模块的要求

类别	级别	私钥导入、导出要求
基线	基线	密码模块之间传输加密的私钥
商业交易	商业交易普通级	密码模块之间传输加密的私钥
	商业交易中级	密码模块之间传输加密的私钥
	商业交易高级	密码模块之间传输加密的私钥，加密的私钥不在任何介质和第三方设备上出现
设备	设备普通级	密码模块之间传输加密的私钥
	设备可信级	密码模块之间传输加密的私钥，加密的私钥不在任何介质和第三方设备上出现
公众服务	公众服务非实名级	密码模块之间传输加密的私钥
	公众服务实名级	密码模块之间传输加密的私钥

10.2.7　密码模块中的私钥保存

电子认证服务机构及其重要组件的私钥应在密码模块中加密保存。

10.2.8　激活私钥的方法

各参与方应对其私钥的激活数据进行保护，防止丢失、偷窃、修改、泄露或者未经授权的使用。

电子认证服务机构私钥应按照 10.2.2 的要求进行激活。

本标准中证书策略对订户私钥激活方式的要求，如表 35 所示。

表 35　证书策略对私钥激活方法的要求

类别	级别	私钥激活方式要求
基线	基线	订户私钥的激活应采用身份鉴别的方式，可接受的鉴别方式包括：口令和生物特征识别等
商业交易	商业交易普通级	订户应对其工作站进行物理防护，防止未经授权的使用。订户应按照 10.4.1 的要求，在激活私钥之前使用口令或者同等强度的方式进行鉴别，例如：操作私钥需要的口令，操作系统登录口令、屏幕保护口令等
	商业交易中级	订户应对其工作站进行物理防护，防止未经授权的使用。订户应按照 10.4.1 的要求，在激活私钥之前使用口令或者同等强度的方式进行鉴别，例如：操作私钥需要的口令，操作系统登录口令、屏幕保护口令等。未激活状态的私钥应以加密形式保存
	商业交易高级	订户应对其工作站进行物理防护，防止未经授权的使用。订户应按照 10.4.1 的要求，在激活私钥之前进行双因素鉴别。未激活状态的私钥应以加密形式保存

表 35（续）

类别	级别	私钥激活方式要求
设备	设备普通级	管理员应对设备进行物理防护，防止未经授权的使用。在激活私钥之前，应按照 10.4.1 的要求，使用口令或者同等强度的方式进行鉴别，例如：操作私钥需要的口令，操作系统登录口令、屏幕保护口令等。未激活状态的私钥应以加密形式保存
	设备可信级	管理员应对设备进行物理防护，防止未经授权的使用。在激活私钥之前，应按照 10.4.1 的要求，进行双因素鉴别。未激活状态的私钥应以加密形式保存
公众服务	公众服务非实名级	订户应对其工作站进行物理防护，防止未经授权的使用。订户应按照 10.4.1 的要求，在激活私钥之前使用口令或者同等强度的方式进行鉴别，例如：操作私钥需要的口令，操作系统登录口令、屏幕保护口令等。解除激活状态的私钥应以加密形式保存
	公众服务实名级	订户应对其工作站进行物理防护，防止未经授权的使用。订户应按照 10.4.1 的要求，在激活私钥之前使用口令或者同等强度的方式进行鉴别，例如：操作私钥需要的口令，操作系统登录口令、屏幕保护口令等。解除激活状态的私钥应以加密形式保存

10.2.9 解除私钥激活状态的方法

电子认证服务机构的私钥在激活后就持续有效，断电将自动解除激活状态。

订户解除私钥激活状态的方式由其自行决定，例如退出、切断电源、移开令牌和自动锁定等。

电子认证服务机构应为商业交易高级、设备可信级策略证书订户提供以下解除私钥激活状态的方法：

- 退出；
- 切断电源；
- 移开令牌；
- 超时自动锁定；
- 进行签名操作后立即锁定。

电子认证服务机构应为商业交易普通级、商业交易中级、设备普通级、公众服务非实名级和公众服务实名级证书策略的证书订户至少提供上述私钥激活状态解除方式中的两种。

10.2.10 销毁私钥的方法

当私钥需要被销毁的时候，应按照密码模块给出的说明完成密钥的销毁。

10.2.11 密码模块安全要求

密码模块应符合国家密码主管部门的相关规定。

10.3 密钥对管理的其他方面

10.3.1 公钥归档

具体要求参见 9.5。

10.3.2 证书操作期和密钥对使用期限

证书操作周期起始于证书被激活,终止于证书过期或者被撤销。订户密钥对的使用周期与证书的操作周期是相同的,仅用于解密的私钥和用于签名验证的公钥还可能在操作周期后被使用。电子认证服务机构所签发的证书的操作周期不应超过电子认证服务机构的密钥对的使用周期。

本标准中证书策略对电子认证服务机构的根证书有效期的要求,如表 36 所示。

表 36 证书策略对电子认证服务机构根证书有效期的要求

类别	级别	电子认证服务机构根证书有效期
基线	基线	不超过 50 年
商业交易	商业交易普通级	不超过 30 年
	商业交易中级	不超过 30 年
	商业交易高级	不超过 50 年
设备	设备普通级	不超过 30 年
	设备可信级	不超过 50 年
公众服务	公众服务非实名级	不超过 30 年
	公众服务实名级	不超过 30 年

本标准中证书策略对签发订户证书的电子认证服务机构证书有效期的要求,如表 37 所示。

表 37 证书策略对签发订户证书的电子认证服务机构证书有效期的要求

类别	级别	签发订户证书的电子认证服务机构证书有效期
基线	基线	不超过 10 年
商业交易	商业交易普通级	不超过 10 年
	商业交易中级	不超过 10 年
	商业交易高级	不超过 10 年
设备	设备普通级	不超过 10 年
	设备可信级	不超过 10 年
公众服务	公众服务非实名级	不超过 10 年
	公众服务实名级	不超过 10 年

本标准中证书策略对订户证书有效期的要求,如表 38 所示。

表 38 证书策略对订户证书有效期的要求

类别	级别	订户证书有效期要求
基线	基线	不超过 5 年
商业交易	商业交易普通级	不超过 5 年
	商业交易中级	不超过 3 年
	商业交易高级	不超过 2 年

表 38（续）

类别	级别	订户证书有效期要求
设备	设备普通级	不超过 2 年
	设备可信级	不超过 1 年
公众服务	公众服务非实名级	不超过 3 年
	公众服务实名级	不超过 3 年

10.4 激活数据

10.4.1 激活数据的生成和安装

生成和安装私钥激活数据，应采取防护措施来防止私钥丢失、被窃、被篡改、未经授权的披露或者被未经授权的使用。

本标准中证书策略对订户的激活数据的要求，如表 39 所示。

表 39 证书策略对订户激活数据的要求

类别	级别	订户激活数据要求
基线	基线	应采取防护措施来防止私钥丢失、被窃、被篡改、未经授权的披露或者被未经授权的使用
商业交易	商业交易普通级	订户应使用口令作为激活数据，订户选择的口令应不易被猜测或抵抗字典攻击
	商业交易中级	订户应使用口令作为激活数据，订户选择的口令应不易被猜测或抵抗字典攻击
	商业交易高级	订户应使用双因素方式激活私钥
设备	设备普通级	设备管理员应使用口令作为激活数据，订户选择的口令应不易被猜测或抵抗字典攻击
	设备可信级	设备管理员应使用双因素方式激活私钥
公众服务	公众服务非实名级	订户应使用口令作为激活数据，订户选择的口令应不易被猜测或抵抗字典攻击
	公众服务实名级	订户应使用口令作为激活数据，订户选择的口令应不易被猜测或抵抗字典攻击

电子认证服务机构私钥激活数据的生成和安装，应符合 10.2.2 对于多人控制的要求。

10.4.2 激活数据的保护

各参与方应采取相应的措施保护私钥的激活数据，免受丢失、被窃、篡改、未经授权的披露或者未经授权使用。

商业交易类、设备类、公众服务类证书策略要求电子认证服务机构私钥的秘密分享者不应复制、披露、告知第三方其分享的秘密或对秘密进行未经授权的访问，也不应向第三方透露任何秘密分享者的身份。

10.4.3 激活数据的其他方面

10.4.3.1 激活数据的传递

商业交易类、设备类、公众服务类证书策略要求私钥的激活数据进行传送时，各参与方应保护它们在传送过程中免于丢失、偷窃、修改、未经授权的披露或使用。

10.4.3.2 激活数据的销毁

商业交易类、设备类、公众服务类证书策略要求电子认证服务机构保证其私钥的激活数据在销毁的过程中免于丢失、偷窃、未经授权的披露或使用。当超过 9.5.2 要求的记录保留期限后，电子认证服务机构应通过覆盖原有记录或者物理销毁的方式来销毁激活数据。

10.5 计算机安全控制

电子认证服务机构应使用可信的系统来运行软件和存放数据文件，应确保软件和数据不会受到未经授权的访问。

电子认证服务系统应与其他系统进行隔离，只允许已经定义的应用进程对电子认证服务系统进行访问。

为保护电子认证服务机构的网络免受现有攻击的威胁，未使用的端口和服务应全部关闭。

10.6 电子认证服务系统生命周期技术控制

10.6.1 系统开发控制

电子认证服务系统在开发时需要如下的系统开发控制：

- 电子认证服务软件和硬件在开发时应有正式的文档化的开发流程支持，购买的商用软件或硬件除外；
- 电子认证服务机构需要的其他专门的软件和硬件的开发环境是可控的，并有正式的文档化的开发流程支持，购买的商用软件或硬件除外；
- 电子认证服务机构使用的软件和硬件应仅服务于电子认证。系统不应包含其他不用于提供电子认证服务的任何应用程序和硬件；
- 任何软件或硬件的升级应保持一致并且有专人负责。

10.6.2 安全管理控制

电子认证服务系统运行之前，应验证软件是未被篡改的。

电子认证服务机构应定期的对其电子认证服务软件的安全性进行检查。

电子认证服务系统的升级和配置都应文档化。

本标准中证书策略对于软件完整性验证的要求，如表 40 所示。

表 40 证书策略对电子认证服务软件完整性验证的要求

类别	级别	电子认证服务软件完整性验证要求
基线	基线	要求对软件进行安全性检查
商业交易	商业交易普通级	软件安装前验证软件的完整性
	商业交易中级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每两天进行一次完整性校验

表 40（续）

类别	级别	电子认证服务软件完整性验证要求
商业交易	商业交易高级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每天进行一次完整性校验
设备	设备普通级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每两天进行一次完整性校验
	设备可信级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每天进行一次完整性校验
公众服务	公众服务非实名级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每两天进行一次完整性校验
	公众服务实名级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每两天进行一次完整性校验

10.7 网络的安全控制

电子认证服务机构应配备网络防火墙、过滤路由等设备，以阻止非法访问。

电子认证服务机构内部网络上传输的敏感信息应进行加密和完整性保护。

本标准中证书策略对电子认证机构和注册机构在线状态的要求，如表 41 所示。

表 41 证书策略对网络安全控制的要求

类别	级别	电子认证服务机构	注册机构
基线	基线	不作要求	不作要求
商业交易	商业交易普通级	不作要求	不作要求
	商业交易中级	可以短时在线	不作要求
	商业交易高级	不允许在线	不允许在线
设备	设备普通级	可以短时在线	不作要求
	设备可信级	不允许在线	不允许在线
公众服务	公众服务非实名级	可以短时在线	不作要求
	公众服务实名级	可以短时在线	不作要求

10.8 时间标记

证书、证书撤销列表、日志和其他关键信息应包含准确的时间和日期信息。

11 证书、证书撤销列表和在线证书状态协议

11.1 证书

11.1.1 版本号

符合本标准中证书策略要求的电子认证服务机构应签发 GB/T 20518—2006 中规范的 V3 版本证书。

11.1.2 证书扩展

电子认证服务机构可以根据应用的需要在证书中包含自定义的私有扩展。证书中的私有扩展应标记为“非关键”扩展。

11.1.3 算法对象标识符

符合本标准中证书策略的证书中应使用国家密码主管部门允许的算法的对象标识符。

11.1.4 命名形式

命名形式同 7.1 的要求。

11.1.5 证书策略对象标识符

符合本标准中证书策略的证书中应包含相应的对象标识符。

11.1.6 关键证书扩展项的处理规则

如果证书中标记为“关键”的扩展项不能被识别，则应拒绝处理该证书。

11.2 证书撤销列表

基线证书策略要求电子认证服务机构支持签发 V1 版本或 V1 版本以上的证书撤销列表。

商业交易类、设备类、公众服务类证书策略要求电子认证服务机构应支持签发 V2 版本的证书撤销列表。

12 合规性审计和相关评估

12.1 评估的频率和情况

电子认证服务机构应接受电子认证服务管理部门组织的定期合规性审计。

根据审计结果，需要整改后复审的，电子认证服务机构应接受复审。

电子认证服务管理部门认为电子认证服务机构运营存在问题，需要审计的，电子认证服务机构应接受审计。

本标准中证书策略对内部审计周期的要求，如表 42 所示。

表 42　证书策略对内部审计周期的要求

类别	级别	内部审计周期要求
基线	基线	每年
商业交易	商业交易普通级	每年
	商业交易中级	每半年
	商业交易高级	每 3 个月
设备	设备普通级	每半年
	设备可信级	每 3 个月
公众服务	公众服务非实名级	每半年
	公众服务实名级	每半年

12.2　评估者的身份/资质

进行合规性审计和评估的机构，应是电子认证服务管理部门认可的机构。

参与电子认证服务机构评估的人员应证明其具备计算机安全方面的相关专业知识，在信息安全和 PKI 审计评估方面有丰富的经验。

12.3　评估者与被评估者的关系

评估者和电子认证服务机构之间应是相互独立的，没有任何利益关系。

12.4　对不足采取的措施

电子认证服务机构完成内部评估后，评估人员应列出所有问题条目的详细清单，由评估人员和被评估对象共同讨论有关问题，并将结果书面通知电子认证服务机构，进行后续处理。

外部评估完成后，电子认证服务机构应根据评估的结果检查缺失和不足，根据提出的整改要求，提交修改和预防措施以及整改计划书，并接受对整改计划的审查，以及对整改情况的再次评估。

对于整改计划不完善或者限期整改后不能达到要求的电子认证服务机构，电子认证服务管理部门有权终止其签发本标准中策略证书的服务。

12.5　评估结果的传达

审计评估机构在完成评估后，应在 15 d 内向电子认证服务管理部门提交评估结果。电子认证服务管理部门根据需要发布评估结果。

中 华 人 民 共 和 国
国 家 标 准
**信息安全技术 公钥基础设施
数字证书策略分类分级规范**
GB/T 31508—2015
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2015 年 5 月第一版
*
书号:155066·1-51451

GB/T 31508-2015