ICS 35.030
CCS L 80

中国电子质盟冒理协会
CMm Oosty Manrment Ancletien Por Detrenles ndestry
COXF

团 体 标 准

T/CQAE 11034—2025

电子认证业务规则规范

Specification for Certification Practice Statement

2025-12-18发布 2026-01-18实施

中国电子质量管理协会 发布

目　　次

前　　言

本文件按照GB/T　1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由中国电子质量管理协会提出并归口。

本文件起草单位：国家工业信息安全发展研究中心、中国互联网络信息中心、杭州天谷信息科技有限公司、北京世纪速码信息科技有限公司、大陆云盾电子认证服务有限公司、广东省电子商务认证有限公司、华测电子认证有限责任公司、天津数字认证有限公司、中铁信弘远(北京)软件科技有限责任公司、内蒙古网信电子认证有限责任公司、中金金融认证中心有限公司、北京天威诚信电子商务服务有限公司、亚数信息科技(上海)有限公司、北京数字认证股份有限公司、上海市数字证书认证中心有限公司、数安时代科技股份有限公司、山西省数字证书认证中心(有限公司)、新疆数字证书认证中心(有限公司)、湖南省数字认证服务中心有限公司、深圳市电子商务安全证书管理有限公司、河南省信息化集团有限公司、安徽省电子认证管理中心有限责任公司、四川省数字证书认证管理中心有限公司、陕西省数字证书认证中心股份有限公司、浙江省数字安全证书管理有限公司、江西省数字证书有限公司、黑龙江省数字证书认证有限公司、卓望数码技术(深圳)有限公司、江苏省数据集团数字科技有限公司、北京国富安电子商务安全认证有限公司、湖北省数字证书认证管理中心有限公司、贵州省电子认证科技有限公司、福建省数字安全证书管理有限公司、东方中讯数字证书认证有限公司、联通智慧安全科技有限公司、吉林省安信电子认证服务有限公司、河北省电子认证有限公司、西部安全认证中心有限责任公司、江苏智慧数字认证有限公司、广西壮族自治区数字证书认证中心有限公司、东方新诚信数字认证中心有限公司、重庆程远未来电子商务服务有限公司、山东豸信认证服务有限公司、农信银资金清算中心有限责任公司、北京中认环宇信息安全技术有限公司、南京数字认证有限公司、天津市滨海数字认证有限公司、云南省数字证书认证中心有限公司、沃通电子认证服务有限公司、苏博云科数字认证有限公司、辽宁数字证书认证管理有限公司、山东省数字证书认证管理有限公司、颐信科技有限公司、江苏国密数字认证有限公司、海南省信安电子认证有限公司、中国电力科学研究院有限公司、泰尔认证中心有限公司、国汽(北京)智能网联汽车研究院有限公司、中汽数据（天津）有限公司、北京群盾科技有限公司、江苏公众数科数字科技有限公司。

本文件主要起草人：李慧颖、郭宏杰、蔡超、张镭、魏一才、兰磊、刘环宇、谭泳、肖磊、陈树乐、严硕、潘泽、李增冉、肖菲、舒剑、张黎、王谦、魏东宾、郭佳、冯永英、崔悦、饶伟、吕小菲、刘红日、李延昭、蔡京露、崔久强、沈传案、郑巍、瓦里别克·吐达洪、梁红贞、陈亚殊、李亚飞、李星、尹才敏、盛昀、方伟明、徐华、朱旭、袁胜、王杰勋、王小飞、余鹏、田勇、林文辉、文爱华、鲁华伟、孙静、吴志峰、王申、马圣东、葛岩、颜星、李海波、梅臻、董宝明、王超、张循、马羽、周建文、葛剑青、王刚、赵兵、杨贵忠、杨逢春、朱海威、万象、翟峰、孙圣男、方锐、赵万里、李彪、王志勇、魏建业、程亮。

电子认证业务规则规范

1 范围

本文件确立了电子认证业务规则(以下简称“CPS”） 的主要组成部分，规定了CPS 主要组成部分的具体内容和要求，描述了对应的证实方法。

本文件适用于电子认证服务机构(以下简称“CA”） 开 展CPS 的撰写与执行等过程，也适用于主管部门及其指定的支撑单位开展电子认证服务行业检查和评估。

本文件等同于相关证书策略，对应对象标识符(以下简称“OID”) 为：2.16.156.339.2.1.1.1、2.16.156.339.2.1.1.2、2.16.156.339.2.1.2.1、2.16.156.339.2.1.2.2,具体策略说明详见6.1.5.1。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GBT 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

GB/T 19713—2025 网络安全技术 公钥基础设施 在线证书状态协议

GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 25056—2018 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 37092—2018 信息安全技术 密码模块安全要求

GMT 0109—2021 基于云计算的电子签名服务技术要求

GMT 0120—2022 基于云计算的电子签名服务技术实施指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

加密 **encipherment encryption**

对数据进行密码变换以产生密文的过程。

[来源：GB/T 25069—2022,3.278]

3.2

密码模块 **cryptographic module**

实现密码运算功能，相对独立的软件、硬件、固件或这三者组合。

[来源：GB/T 25069—2022,3.379]

3.3

密码算法 **cryptographic algorithm**

描述密码处理过程的算法。

[来源：GB/T 25069—2022,3.380]

3.4

密钥 key

控制密码变换操作的符号序列。

[来源：GB/T 25069—2022,3.389]

注：在非对称密码算法中，密钥包括私钥和公钥。

3.5

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

[来源：GB/T 25069—2022,3.580]

注：属于《中华人民共和国电子签名法》中电子签名制作数据的一种实现形式。

3.6

公钥 public key

非对称密码算法中可公开的密钥。

[来源：GB/T 25069—2022,3.211]

注：属于《中华人民共和国电子签名法》中电子签名验证数据的一种实现形式。

3.7

RSA 算法 RSA algorithm

一种基于大整数因子分解问题的公钥密码算法。

[来源：GB/T 25069—2022,3.582]

3.8

SM2 算法 SM2 algorithm

由 GB/T 32918 定义的一种椭圆曲线公钥密码算法。

[来源：GB/T 25069—2022,3.583]

3.9

SM3 算法 SM3 algorithm

由 GB/T 32905 定义的一种密码杂凑算法。

[来源：GB/T 25069—2022,3.584]

3.10

公钥基础设施 public key infrastructure(PKI)

基于公钥密码技术，具有普适性，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务的基础设施。

[来源：GB/T 25069—2022,3.212]

3.11

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

[来源：GM/Z 4001—2013,2.113]

3.12

电子认证服务机构 certification service provider

取得电子认证服务许可证，为需要第三方认证的电子签名，签发电子签名认证证书并为有关各方提供真实性、可靠性验证的实体。

注：本文件中也称为认证机构，简称CA。

3.13

数字证书 digital certificate

也称公钥证书，由认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

[来源：GM/Z 4001—2013,2.115,有修改，删除了分类]

3.14

电子签名认证证书 electronic signature certificate

由依据《中华人民共和国电子签名法》设立的电子认证服务机构签发的，可证实电子签名人与电子签名制作数据有联系的数字证书。

注1:如无具体限定，本规范中的“证书”均指“电子签名认证证书”,本规范中的“密钥”“私钥”,均指电子签名认证证书所对应的“密钥”“私钥”。

注2:可证实电子认证服务机构与电子签名制作数据有联系的数字证书，称为根证书。

3.15

电子签名依赖方 electronic signature relying party

是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

注：本文件中简称依赖方。

3.16

订 户 subscriber

被颁发给一张证书的证书主体。[来源：GB/T 26855—2011,3.15]

注：在不同的阶段，也称为证书申请人、证书持有人。属于《中华人民共和国电子签名法》中电子签名人的一种类型。

3.17

对象标识符 object identifier(OID)

用于无歧义地标识对象的全局唯一值。

[来源： GB/T 25069—2022,3.138]

3.18

证书策略 certificate policy(CP)

指明证书对于具有普通安全需求的特定团体和/或应用类的适用性的规则集合。

[来源： GB/T 25069—2022,3.780]

3.19

证书策略对象标识符 CP OID

对某个证书策略进行唯一标识的OID。

3.20

证书链 certificate chain

证书链是一个用于证书验证的证书序列。

3.21

身份查验 entity authentication

证实某个实体就是所声称身份的过程。

3.22

激活数据 activation data

用于使密码模块进入可操作状态的数据。可为口令、生物特征等。

[来源：GB/T 25069—2022,3.267]

3.23

时间戳 time stamp(TS)

对时间和其他待签名数据进行签名得到的，用于表明数据时间属性的数据。

[来源： GB/T 25069—2022,3.541]

3.24

证书续期 certificate renewal

指在不改变订户信息的情况下，用一个新证书来代替旧证书的过程。

3.25

密钥更新 key re-key

用新密钥替换旧密钥的过程。

[来源： GB/T 25069—2022,3.400]

注：通常指证书与密钥同时更新。

3.26

密钥恢复 key recovery

将归档或备份的密钥恢复到可用状态的过程。

[来源： GB/T 25069—2022,3.405]

3.27

证书撤销列表 certificate revocation list(CRL)

由电子认证服务机构签发并发布的被撤销证书的列表。

[来源： GB/T 25069—2022,3.781,有修改，证书认证机构改为电子认证服务机构]

3.28

证书认证系统 CA system

对数字证书的申请、签发、发布、更新、撤销、验证等数字证书全生存周期进行管理和服务的系统。

[来源： GB/T 25069—2022,3.787,有修改，扩充了申请、验证和服务等内容]

注：也称电子认证服务系统，包括证书签发子系统、证书注册子系统等。

3.29

高等级电子签名认证证书 **enhanced electronic signature certificate**

适用于涉及生命健康、财产权益等高风险场景的电子签名认证证书。

3.30

基础级电子签名认证证书 **qualified electronic signature certificate**

适用于除高等级证书规定场景外的其他电子签名场景的证书。

4 缩略语

下列缩略语适用于本文件。

CA: 电子认证服务机构 (Certification Authority)

CPS: 电子认证业务规则(Certification Practice Statement)

CP: 证书策略 (Certification Policy)

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

DN: 甄别名称 (Distinguished Name)

LDAP: 轻量级目录访问协议(Lightweight Directory Access Protocol)

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

OID: 对象标识符 (Object Identifier)

RTO: 恢复时间目标 (Recovery Time Objective)

RPO: 恢复点目标 (Recovery Point Objective)

5 电子认证业务规则的主要组成部分

电子认证业务规则是电子认证服务机构对所提供的认证及相关业务的全面描述。电子认证业务规则由责任范围、作业操作规范和信息安全保障措施等组成，包括但不限于以下内容：

a) 概括性描述；
b) 信息发布与信息管理；
c) 身份标识与查验；
d) 证书生存周期操作要求；
e) 认证机构设施、管理和操作控制；
f) 认证系统技术安全控制；
g) 证书、证书撤销列表和在线证书状态协议；
h) 认证机构审计和其他评估；
i) 法律责任和其他业务条款。

电子认证业务规则文档结构见附录A。

6 主要组成部分的具体内容和要求

6.1 概括性描述

6.1.1 承诺

应在CPS中承诺：

a) 开展经营和服务活动时，遵守法律、行政法规，树立以人民为中心的服务理念，承担社会责任；
b) 与客户建立业务关系前，开展应用业务调研，建立应用接入业务风险评估及内部定责机制，严禁为存在违法违规风险的业务提供电子认证服务；
c) 使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务；
d) 接受政府和社会监督，对主管部门检查发现的问题及时整改，建立问题纠治长效机制，持续符合整改要求。

6.1.2 基本信息

应在CPS中提供一个概要性介绍，包括但不限于以下内容：

a) 机构名称；
b) 法定代表人；
c) 机构住所、经营场所的地址和联系方式；
d) 是否取得《电子认证服务许可证》等许可证书及其编号、发证机关和批准日期、有效期的起止时间；
e) 证书链及其包含证书的信息，包括但不限于：证书编号、颁发机构名称、密码算法、密钥长度、有效期、计划服务时间等。

6.1.3 文档名称与标识

应在CPS中说明版本号、发布日期、遵循的证书策略OID、历史版本信息等。CA 应为本机构发布的证书策略申请OID, 宜为本机构CPS申请OID。

6.1.4 电子认证活动参与者

应在CPS中说明电子认证活动参与者及其要求，参与者包括但不限于CA、订户、依赖方等。

6.1.5 证书应用

6.1.5.1 证书应用分类

应在CPS 中明确描述其颁发的用于电子签名用途的全部数字证书的类型、特点，以及其适用的具体应用场景。

按证书主体对象的类型和风险等级，电子签名认证证书可分为个人高等级电子签名认证证书、个人基础级电子签名认证证书、机构高等级电子签名认证证书、机构基础级电子签名认证证书四种类型。证书扩展项应包含主管部门制定发布的电子签名认证证书策略OID; 也可包含CA遵循的其他电子签名认证证书策略OID 。电子签名认证证书分类具体见表1。

表 1 电子签名认证证书类型

证书类型	主管部门 证书策略OID	其他 证书策略OID	含义
个人高等级电子签名认证证书	2.16.156.339.2.1.1.2	示例：X.X.XX.XX.X.X	适用于高风险业务、符合《电子签名法》的个人电子签名认证证书
个人基础级电子签名认证证书	2.16.156.339.2.1.1.1	示例：x.x.XX,XX.X.X	适用于低风险业务、符合《电子签名法》的个人电子签名认证证书
机构高等级电子签名认证证书	2.16.156.339.2.1.2.2	示例：x.x.XX.xX.X.X	适用于高风险业务、符合《电子签名法》的机构电子签名认证证书
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1	示例：X.x.xX,XX,X.X	适用于低风险业务、符合《电子签名法》的机构电子签名认证证书

应在CPS 中列出其颁发的其他数字证书的类型、安全级别、特点及其适用的场景，且需要明示其不适用于电子签名。

对于具有特殊用途或适用特定行业规范的证书，应在CPS 中额外声明其符合的相关规则要求。如：用于跨境互认领域电子签名认证证书，需要声明其符合相关跨境互认规则的要求。

6.1.5.2 证书应用限制

应在CPS 中明确描述限制的证书应用，列出禁止使用证书的场景，包括但不限于：

a) 涉及人身关系的，如婚姻、收养、继承等；

b) 涉及停止公共事业服务的，如停止供水、供热、供气等；

c) 法律、行政法规规定的其他不适用电子签名的应用场景或类型；

d) 国家法律法规禁止的活动。

涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

6.1.6 策略管理

6.1.6.1 策略管理机构

应在CPS 中声明设立了安全策略委员会，公示成员名单，明确工作职责并妥善保存安全策略委员会重大决议的相关文件和会议记录。安全策略委员会负责CPS 和CP 以及配套制度的维护，包括但不限于以下职责：

a) 确定维护CPS 和 CP 等 策略文档的职能分工，建立合理有效的修订和批准流程；

b) 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批；

c) 每年至少进行一次CPS 和 CP 全面评审，根据实际需要及时修订策略文档；

d) 每年组织运营风险评估并形成报告。

6.1.6.2 策略文档的批准程序

应在CPS中明确其批准程序，包括但不限于：

a) 起草小组的成立流程；
b) 安全策略委员会的审批流程；
c) 向主管机关的备案流程；
d) 发布流程。

6.1.7 定义和缩写

应在CPS 中明确其所使用的术语、定义及缩写。

6.2 信息发布与信息管理

应在CPS中明确：

a) 网站发布的内容，包括但不限于：
   1) CPS、CP的所有版本；
   2) 证书链；
   3) 证书信息、状态信息等查询服务；
   4) 详细的业务办理指南，包括但不限于服务网点地址、营业时间、联系电话等；
   5) 依赖方协议；
   6) 投诉处理政策及投诉方式，包括但不限于：投诉处理部门的地址、联系电话、电子邮件地址，以及内部监督部门名称。
b) 信息更新：信息发布内容如有变化，应在变化生效后1个工作日内更新；
c) 监管备案：应声明按照国家电子认证服务管理平台的要求进行了备案；
d) 证书信息对接：应完成与国家电子认证服务管理平台的技术对接，实现根据证书唯一编码、订户身份信息等维度查询本机构已签发证书列表的功能。

6.3 身份标识与查验

6.3.1 身份查验通用要求

6.3.1.1 通用要求

应在CPS中声明：

a) 在受理证书申请时，对订户和/或受托人进行告知、身份确认、意愿记录和协议签署；
b) 身份查验义务未委托给外部机构或个人(非属同一法人主体的机构视为外部机构)。

6.3.1.2 订户告知

6.3.1.2.1 告知内容

应在CPS 中明确订户申请证书时，告知以下内容：

a) 订户的权利和义务；
b) 服务收费的项目和标准；
c) 电子签名认证证书、电子签名的使用条件；
d) 信息安全保障措施；
e)CA 和订户的责任划分；
f) 订户签名私钥的存储方式及安全要求；

g) 订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

6.3.1.2.2 告知方式

应在CPS中明确告知方式：

a) 高等级证书采用面对面、电话、视频或主管部门认可的其他方式告知，并保留告知的记录；

b) 基础级证书采用高等级证书的告知方式，或采用强制阅读、短信、邮件等方式告知，并保留告知的记录。

6.3.2 初始身份确认

6.3.2.1 证明拥有私钥的方法

应在CPS 中明确：

a) 按照6.6.2.2规定的方式生成订户密钥对；

b) 通过数字签名的方式来确认证书订户拥有某个公钥对应的签名私钥。

6.3.2.2 个人身份的查验

6.3.2.2.1 个人身份信息有效性的确认

应在CPS中明确受理个人证书申请时，对个人身份信息的查验方式及内容：

a) 受理个人证书申请时，应要求订户出示其有效身份证件或有效身份证件信息，并明确有效证件类型仅限法律法规和国家有关文件规定的身份证件；

b) 应通过证件机读工具、权威数据库或主管部门认可的其他方式查验订户身份证件的真实性和有效性；

c) 当订户委托他人代为办理时，应查验订户本人签署的有效书面授权证明，要求受托人出示其有效身份证件或有效身份证件信息，并按照b)款方式查验订户和受托人的身份证件或身份资料。

6.3.2.2.2 个人高等级证书的实人查验

应在CPS中明确，对订户开展实人查验采用下列方式之一：

a) 面对面查验；

b) 远程人工面对面查验；

c) 生物特征验证：如活体人脸、指纹、声纹、掌纹等生物识别技术的应用；

d) 通过主管部门认可的其他方式。

应在CPS 中声明以可追溯的方式完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

6.3.2.2.3 个人基础级证书的实人查验

应在CPS 中明确，对订户开展实人查验采用下列方式之一：

a) 通过第6.3.2.2.2节规定的方式；

b) 电信运营商三要素：核对姓名、证件号码、手机号在电信运营商的一致性，并通过对应手机号的随机短信验证码核验；

c) 银行卡四要素：核对姓名、证件号码、银行卡号、银行预留手机号在银行的一致性，并通过预留手机号的随机短信验证码核验；

d) 由申请人持有的有效电子签名认证证书签名验证；

e) 通过主管部门认可的其他方式，如居民身份网络可信凭证、公民网络电子身份标识、国家网络身份认证系统、内地银行或支付机构对外提供的个人账户和身份信息对应关系验证等。

应在CPS 中声明完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

6.3.2.3 机构身份的查验

6.3.2.3.1 机构身份信息有效性的确认

应在CPS中明确受理机构证书申请时的身份信息查验方式及内容：

a) 机构有效证件的查验方式，并明确有效证件类型仅限法律法规和国家有关文件规定的证件；

b) 法定代表人或受托人的身份查验方式：

1)法定代表人或受托人身份证件信息查验方式参见6.3.2.2.1;

2)受托人办理时，应查验机构加盖公章的有效书面授权证明。

6.3.2.3.2 机构高等级证书的实人查验

应在CPS中明确，对订户开展实人查验采用下列方式之一：

a) 法定代表人实人查验，方法见6.3.2.2.2;

b) 受托人实人查验，方法见6.3.2.2.2,并通过机构对公账户随机金额打款验证或主管部门认可的其他方式。

应在CPS 中声明以可追溯的方式完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

6.3.2.3.3 机构基础级证书的实人查验

应在CPS中明确，对订户开展实人查验采用下列方式之一：

a) 法定代表人实人查验，方法见6.3.2.2.3;

b) 受托人实人查验，方法见6.3.2.2.3;

c) 由订户持有的同等级或者更高级的有效机构证书签名验证。

应在CPS中声明完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

6.3.3 订户意愿记录

6.3.3.1 订户意愿记录内容

CPS 中应明确订户意愿记录内容，包括但不限于：

a) 订户身份信息；

b)CA 的信息；

c) 签名私钥保存方及其保存义务；

d) 订户对电子签名的法律责任；

e) 订户对上述a) 至d) 项内容已充分知晓并同意的明确意愿表示。

6.3.3.2 个人高等级证书的意愿记录

应在CPS 中明确，订户意愿的确认采用下列方式之一：

a) 现场办理时，通过面对面确认或手抄提示语的方式，并采用录音录像或通过主管部门认可的其他方式记录订户意愿；

b) 远程办理时，通过音视频或通过主管部门认可的其他方式确认并记录订户意愿。

6.3.3.3 个人基础级证书的意愿记录

应在CPS 中明确，订户意愿的确认采用下列方式之一：

8） 与高等级证书相同的方式，见6.3.3.2;

b） 采用强制阅读、短信或邮件确认等电子方式。

应在CPS中声明保留完整、可追溯的订户意愿记录。

6.3.3.4 机构高等级证书的意愿记录

应在CPS 中明确，订户意愿的确认采用下列方式之一：

a) 法定代表人申请时，按照6.3.3.2的方式确认机构法定代表人的意愿；

b) 受托人申请时，查验加盖机构公章的授权文件，并按照6.3.3.2的方式确认受托人的意愿。

应在CPS中声明采用录音录像或通过主管部门认可的其他方式记录订户意愿。

6.3.3.5 机构基础级证书的意愿记录

应在CPS 中明确，订户意愿的确认采用下列方式之一：

a） 法定代表人申请时，按照6.3.3.3的方式确认机构法定代表人的意愿；

b） 受托人申请时，查验加盖机构公章的授权文件，并按照6.3.3.3的方式确认受托人的意愿。

应在CPS中声明保留完整、可追溯的订户意愿记录。

6.3.4 订户协议

应在CPS中明确订户协议包含6.3.1.2.1中规定的内容。

6.3.5 未验证的订户信息

应在CPS中明确：

a） 证书载明信息的查验方法、查验流程；

b） 证书中不能包含未经验证的订户信息。

6.3.6 互操作要求

应在CPS中明确互操作业务情形中CA的义务与责任。

6.3.7 命名

应在CPS中明确证书主体甄别名称(以下简称 “DN”) 的命名规则，包括但不限于：

a） 针对个人和机构等不同类型的证书，分别约定其命名规则；

b) 确保命名具有实际意义，且能追溯到唯一实体的方法：

1)个人证书，主体DN 项中包含订户姓名，在DN 项或扩展项中包含有效证件类型及其编号(或相关信息的映射，包括但不限于散列值、掩码等)；

2)机构证书，主体DN 项中包含机构名称，在DN 项或扩展项中包含组织机构的有效证件类型及其编号。

c） 对证书名称中商标权的处理策略和方式，妥善处理商标名及其风险；

d） 在不影响证书通用性的前提下，可在证书中增加自定义的其他内容；

e)DN 项结构定义符合GB/T 16264.8的要求，证书主体DN 项编码规则见表2。

表 2 证书主体 DN 项代码

代码	说明	示例
C	国家	CN
S	省份(可选)	北京
L	城市(可选)	北京
O	订户所在机构信息(可选)	xx公司
OU	订户所在机构部门信息(可选)	Xx部门
CN	订户名称(个人姓名或机构法定名称)	张三/xx公司

6.4 证书生存周期操作要求

6.4.1 通用要求

应在CPS中声明各方的责任，包括但不限于：

a) CA 承担建立、运营和维护注册通道的责任；

b)CA 承担与订户签订电子认证服务协议的责任；

c) 订户承担提供准确信息的责任；

d)CA 承担妥善记录并保存相关信息的责任。

6.4.2 证书申请

应在CPS中明确证书申请处理的流程与时限，包括：

a) 处理流程：按照6.3节规定，完成对订户的告知、身份确认、意愿记录、协议签署等动作，并依据既定准则批准或拒绝该申请；

b) 处理时限：明确自受理之日起完成证书申请处理的最长期限，因特殊情况确需超期的，应与订户协商确定处理时限。

6.4.3 证书签发

应在CPS中明确证书签发的相关要求，包括：

a) 签发过程：明确在证书签发过程中的行为，包括对申请信息的验证、证书的生成与签发等；

b) 结果通告：应明确规定证书申请处理完毕后向订户通告处理结果的方式，包括但不限于：

1)通过认证应用工具进行信息提示；

2)通过信函、站内信或电子邮件发送；

3)通过短信通知；

4) 通过电话通知；

5) 当面通知或通过实时视频等相当于面对面的方式通知；

6)通过主管部门认可的其他方式。

6.4.4 证书接受

应在CPS中明确证书交付、接受与拒绝的规则，包括：

a) 向订户交付证书的方式；

b) 订户接受证书或拒绝接受证书的步骤和条件；

c) 保存订户接受证书的记录，包括接受时间、方式、操作人等信息。

6.4.5 密钥对和证书的使用

应在CPS中明确：

a) 交付前的安全保护：在将密钥对交付订户保管之前，CA 应采取有效措施保障其安全性，包括但不限于：

1)保障签名私钥生成和传输过程的安全；

2)审核订户密钥是否符合国家或行业相关安全标准要求，对不符合要求的(如RSA 密钥长度小于2048位、使用MD5 、SHA-1 等不安全算法)应拒绝颁发证书。

b) 私钥管理服务要求：若CA 提供订户签名私钥管理服务，应明确相关管理与技术措施，并承诺：

1)未经订户书面授权，不得保存或委托他人保存其签名私钥；

2)机构证书签名私钥的使用，应设置法定代表人或受托人作为授权主体；

3)仅在获得订户明确授权的情况下使用其签名私钥；

4)签名私钥应以加密形式存储，且存储条件符合安全标准：

5)所有涉及签名私钥的操作应有完整、可追溯的记录。

c) 安全事件反馈：应建立便捷的外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失密或证书被盗用等异常惰况。

6.4.6 证书续期

应在CPS中明确证书续期(指在不改变订户主体信息的情况下，在原证书到期前，为订户签发新证书)的规则，包括：

a) 证书续期的情形；

b) 申请人为订户或其受托人；

c) 处理续期请求时的身份查验方式，若自申请人上次完成身份查验之日起至本次续期申请日未满三年，可使用有效的原证书进行电子签名验证的方式进行确认，否则，应按照6.3.2的规定重新进行身份查验；

j) 证书签发与接受的流程应符合6.4.3与6.4.4的规定。

6.4.7 证书密钥更新

应在CPS中明确证书密钥更新(指为订户生成新的密钥对并为其新公钥签发新证书)的规则，包括：

a) 证书密钥更新的情形；

b) 申请人为订户或其受托人；

c) 处理密钥更新请求时的身份确认方式，若自申请人上次完成身份查验之日起至本次更新申请日未满三年，可使用有效的原证书进行电子签名验证的方式进行确认，否则，应按照6.3.2的规定重新进行身份查验；

d) 证书签发与接受的流程应符合6.4.3与6.4.4的规定。

6.4.8 证书变更

应在CPS中明确证书变更(指改变证书中除订户公钥之外的信息而签发新证书的情形，例如：订户名称改变等)的规则，包括：

a) 证书变更的情形，如订户更名；

b) 申请人为订户或其受托人；

c) 按照6.3.2节的规定查验，若发起方不是证书订户，CA 应取得订户同意；

d) 证书签发与接受的流程应符合6.4.3和6.4.4节的规定。

6.4.9 证书撤销或冻结

应在CPS中明确证书撤销与证书冻结的相关规则，包括：

a) 制定证书撤销或冻结的审批流程；

b) 可请求撤销或冻结证书的实体，包括但不限于订户、受托人、依赖方或CA;

c) 请求处理：

1)应提供热线电话等便捷渠道，并记录影响证书或私钥安全的事件(如密钥遗失、泄露)；

2)应验证申请人的身份与权限，并做出是否受理的决定。

应在CPS 中声明保留处理流程的相关信息。

6.4.10 证书状态信息服务

应在CPS中明确：

a) 证书状态信息服务方式；

b) 证书状态信息服务响应时间；
c) 查询服务应为连续不间断服务，服务可用率不低于99%；
d) 提供备用查询机制。

6.4.11 停止使用认证服务

应在CPS中明确：
a) 停止订户服务的情形；
b) 处理停止服务请求的时限和方式，包括：
1)停止服务后应撤销证书、安全销毁订户签名私钥等；
2)用户数据的保存、销毁或转移政策。
c) 停止服务后可能涉及的责任延续条款；
d) 完整记录操作过程。

6.4.12 密钥托管与恢复

应在CPS中声明：
a) 根证书私钥不得托管给任何第三方机构或个人，应在自身控制的安全环境中保管；
b) 建立根证书密钥备份与恢复策略，对根证书密钥进行安全备份。

6.5 认证机构设施、管理和操作控制

6.5.1 物理控制

应在CPS中明确提供电子认证服务的技术设施及其控制措施，包括但不限于：
a) 基础设施：描述技术设施的地理位置，物理建筑、机房环境和网络通信设施的建设标准；
b) 分区管理与访问控制：
1)技术设施内部的安全区域划分，至少分为公共区、服务区、管理区和核心区，并规定每个区域的功能定位、 安全防护要求；
2)机房核心区和管理区的物理访问实施“双人共管”与“双因素认证”的强制访问控制策略，并记录访问信息。
c) 电力保障：声明保证电力应急的具体方式；
d) 门禁与监控：部署门禁、侵入检测、视频监控等安防系统，声明非公共区域(包括服务区、管理区、核心区)的视频监控记录和门禁访问记录的保存时间，上述记录在销毁前进行安全审计，形成的审计报告存档备查；
e) 灾备：对重要数据实施异地备份，声明异地备份位置及距离；
f) 环境保障措施：机房配备温湿度控制和防水措施，保持相对湿度在40%-60%范围内，保持温度在18-28℃范围内；
g) 消防措施：机房配备联动的火灾自动报警系统和配备自动灭火系统，包含温度和烟雾检测功能；定期进行消防安全检测；若机房配备了气体灭火系统，同时声明配备专用空气呼吸器或氧气呼吸器；
h) 设备管理：建立设备台账，设备台账包含每台设备的责任人、使用状态、维护周期和报废标准；定期进行设备盘点和核对，设备实际情况与设备台账相符；
i) 存储媒体管理：制定详细的存储媒体使用、报废管理规定，规定包含使用权限、报废标准、销毁方法和审批流程；完整记录存储媒体领用、归还、报废等情况。

6.5.2 操作过程控制

6.5.2.1 可信角色

应在CPS 中明确定义所有涉及证书认证系统操作、维护与管理的可信角色，明确其职责、任职要求、身份验证机制及最小人员配置。可信角色应包括但不限于：

a) 系统管理员：负责系统策略配置、用户与权限管理等；
b) 技术运维员：负责物理环境、网络、服务器及系统软件的日常监控与维护等；
c) 数据库管理员：负责数据库进行日常运维、性能优化及数据备份等；
d) 系统审计员：负责系统和网络日志的审计、管理、审计报告生成等；
e) 密钥管理员：负责根证书密钥材料管理、根证书密钥生存周期管理等；
f) 业务操作员：负责证书申请的受理、审核，订户的身份与意愿鉴证；
g) 客户档案管理员：负责客户证书相关档案资料的归档与保密等；
h) 运营审计员：负责对客户签发、客户服务等核心业务进行独立审计等；
i) 其他人员：对公司运营有重要影响的其他管理人员。

6.5.2.2 职责分离

应在CPS 中声明遵循职责分离原则，所有涉及关键操作(密钥管理、审计、鉴证、系统管理)的角色应实现双人操作或复核机制；涉及业务连续性相关操作(运维、鉴证、审计等)的角色按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作；禁止同一人员掌握可独立完成“发起、审批、执行、审计”全流程的任何组合，以下角色禁止相互兼任：

a) 系统管理员、技术运维员、数据库管理员、系统审计员之间不得兼任；
b) 同一证书业务的录入与审核环节不得由同一业务操作员完成；
c) 业务操作员、客户档案管理员、运营审计员之间不得兼任；
d) 密钥管理员不得与系统管理员、技术运维员兼任；
e) 密钥管理员不宜与除策略管理机构成员外的其他可信角色兼任。

6.5.3 人员控制

6.5.3.1 可信人员资格要求

应在CPS中明确所有可信角色的资格、经历与背景要求，包括但不限于：

a) 从业经历调查要求和无犯罪记录；
b) 具备履行岗位职责所必需的专业技能要求；
c) 签署具有法律约束力的保密协议，承诺不得私自保存、复制或泄露电子认证服务的所有秘密或敏感信息；
d) 签署劳动合同。

6.5.3.2 可信人员培训要求

应在CPS中明确建立覆盖所有可信角色的持续培训体系，并规定：

a) 岗前培训：所有可信人员上岗前须完成不少于20学时的培训并通过考核；
b) 持续培训：每年至少接受一次培训，每人每年培训时长不少于20学时，并通过考核；
c) 培训内容至少包括：
   1) 电子认证服务相关法律法规与标准；
   2) 岗位通用职责要求及各角色特定的工作要求；
   3) 内部管理政策、制度及流程等；

4)PKI 和密码技术基础知识；

5) CPS、CP;

6)安全管理策略和机制；

7) 订户身份查验和审核策略和流程；

8) 电子认证服务运营体系构成；

9) 电子认证服务技术体系构成；

10)灾难恢复和业务连续性管理。

6.5.4 审计日志程序

应在CPS中明确审计日志的记录、保存与审计要求：

a) **记录范围：应持续、完整地记录关键操作与事件，包括但不限于：**

1)根证书密钥操作：包括密钥生成、备份、存储、恢复、归档、销毁，以及密码设备的启用、停用、转移和销毁等；

2)系统访问行为：包括所有对系统的访问企图，包括成功的和失败的登录、退出、权限使用行为等；

3)系统操作与变更：包括对系统的各种关键查询、修改、删除等操作，系统组件的安装、升级、维修，人员，以及敏感信息的获取与取阅等；

4)网络安全事件：包括防火墙、路由器、入侵检测安全设备记录的告警信息，以及针对被攻击事件识别与相应处理过程、结果等；

5)证书生存周期关键过程：包括记录证书申请、审核、签发、更新、变更、撤销、冻结、恢复等操作，CRL 的签发与发布等，所有操作的通过或拒绝结果均应明确记录；

6)机房门禁控制等物理环境事件：包括业务人员、安全运维人员、外部人员等在不同安全区域的进出记录等。

b) 记录内容：每个事件记录应包含时间、类型、内容、操作人、作用对象及结果。对系统的关键操作应由操作人员进行电子签名；

c) 保存期限：系统日志应至少保存至相关证书失效后五年，并实施严格的访问控制以防篡改或删除；

d) 日志审计内容：核实系统和操作人员的合规性包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件；

e) 审计周期：应至少每季度对系统日志进行一次审计，形成审计报告，并基于结果采取改进措施。

6.5.5 记录归档

应在CPS中明确记录归档的范围、期限与保护措施：

a) 归档范围：

1) 证书申请材料和订户意愿记录；

2)所有审计日志；

3) 密码设备全生存周期管理记录；

4) 密码设备的日常操作与使用记录；

5)根证书或密钥生存周期管理相关的全部记录；

6) 证书认证系统运行日志；

7) 已识别的安全事件及处置记录；

8) 证书认证系统关键操作日志；

9) 电子认证服务过程中其他操作记录。

b) 保存期限：订户相关档案、系统日志和审计记录至少保存至证书失效后五年；

c) 保护措施：对电子归档记录采取技术手段保障其完整性，并存储在安全的物理与数字环境中，建立备份机制；

d) 设立专门的档案管理机构统一管理归档记录，明确管理职责、操作规范和安全要求。

6.5.6 电子认证服务机构根证书密钥更替

应在CPS 中声明CA 根证书密钥更替的流程与情形，包括但不限于：

a) 密钥更替程序：

1)密钥生成：在颁发或更换根证书时，在安全可靠的环境中生成新密钥对，具体见6.6.2;

2)根证书发布：将新的CA 公钥证书发布给证书订户和依赖方；

3)旧密钥处理：在完成签名密钥更替后，应按GB/T 25056—2018中8.2.4.3规定的方式，销毁旧私钥及其备份，并保留相关操作记录。

b) 密钥更替的时间：

1)紧急更替：发现密钥泄露或存在安全隐患，应立即启动密钥更替程序；

2)到期更替：宜在密钥到期前二年完成密钥更替。

6.5.7 损害和灾难恢复

应在CPS中明确损害与灾难恢复的预案与流程，包括：

a) 业务连续性目标：承诺并公布灾难恢复的恢复时间目标 (RTO) 和恢复点目标(RPO)；

b) 恢复流程：

1)证书库的恢复过程：包括重建安全运行环境的流程，生成受影响并被撤销的证书列表，对订户密钥的处理方式，以及重新向订户提供实体公钥证书的要求和流程；

2)根密钥损害的恢复过程：包括重建安全环境的流程，为订户重新签发公钥证书，向订户提供新的公钥证书的流程；

3)其他关键资产恢复过程：包括对CA 物理设施、计算资源、网络环境、软件或数据，以及其他密钥数据的恢复方案。

c) 根私钥应急处理：建立根私钥泄露的应急流程，流程需明确应急响应时间要求、责任人员、处置步骤和上报机制，每年进行一次应急演练；

d) 事件报告：见6.5.9;

e) 定期验证：定期验证备份的设备、数据可用性，包括备份恢复测试和功能验证，每年至少进行一次灾难恢复演练。

6.5.8 电子认证服务机构终止

联络应在CPS中明确规定因技术性原因或商业原因需要终止服务时的流程和通告机制，包括但不限于：

a) 起草并发布CA 终止声明，至少提前九十日通知与证书订户、依赖方等相关实体，至少提前六十日向主管部门报告；

b) 具有资质的电子认证服务业务承接单位，并签署承接协议，明确约定承接机构的工作范围与责任；

c) 向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；

d) 停止证书状态服务并归档相关数据；

e) 停止其他电子认证相关服务并归档相关数据；

f) 停止密码设备并归档相关密钥数据；

g) 及时撤销或冻结业务管理员和业务操作员的操作权限；

h) 对所有存档文件记录进行整理和封存；
i) 对所有敏感文档和数据进行安全处理和封存；
j) 清除主机和密码硬件设备中的敏感数据；
k) 其他涉及CA 运营的数据、密钥安全的操作；
l) 如果有与订户电子签名认证证书签发、管理相关的外部合作机构，应在CPS 中明确描述合作机构终止服务和通告相关的过程。

6.5.9 重大事项报告

应在CPS中明确重大事件的报告流程，包括事件发生后向公司管理层、上级机构和主管部门报告的程序、时限与内容。重大事件包括但不限于：

a) **证书认证系统迁移或改造：包括系统软件、网络、部署的重大改变。符合以下任意之一：**
1)机房迁移，或机房内服务区、管理区或核心区划设范围改变；
2)变更电子签名认证证书签发逻辑；
3)新增远程证书注册子系统；
4)新增、更改或者删除用于签发电子签名认证证书的证书链；
5)其他对电子认证服务安全、用户资料安全有影响的改变。

b) 重大安全事故：包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形。符合以下任意之一：
1)证书签发及验证服务连续停机时间超过24h;
2) 发生根证书密钥等关键数据泄露；
3)持续或较大范围未经授权的私钥访问记录或其他异常活动；
4)系统日志持续或较大范围显示异常操作(如非授权时间或网络地址访问敏感功能)。

c) 订户信息泄露事件：包括订户身份信息、证书申请资料等敏感数据被泄露等。符合以下任意之一：
1)个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；
2)数据丢失导致无法恢复证书状态信息。

d) 合规性事件：包括不符合相关法律法规、标准或监管要求的情形。符合以下任意之一：
1)涉及电子认证服务的司法判定；
2)收到行政部门违规通知或处罚决定。

e) 人力资源类事件：包括一个月内核心管理层集体离职、大规模劳动纠纷、重大职场安全事件等。符合以下任意之一：
1)涉及2名及以上管理层人员或10%以上可信人员的离职；
2)劳动纠纷参与人数超过员工总数10%,且经法院或仲裁机构生效裁决确认由CA 承担法律责任。

6.6 认证系统技术安全控制

6.6.1 技术安全管理制度要求

应在CPS 中声明已建立并实施覆盖密钥管理、系统开发、网络防护等领域的技术安全管理制度，并定期接受安全策略委员会的评审，频率不低于每年一次。

6.6.2 密钥对的生成和安装

6.6.2.1 根证书密钥对的生成和安装

应在CPS 中明确根证书密钥对的生成与安装要求，包括：

a) 根证书密钥对应在物理隔离的安全环境中，采用通过国家密码管理部门认可的硬件密码设备

生成；

b) 生成、备份、恢复、销毁过程应实施M 选N 多人控制机制，M 不少于5,N 不少于M/2， 操作应在安全策略委员会授权下进行，并通过录音录像方式全程记录，保存期限不少于操作完成后十年。

6.6.2.2 订户密钥对的生成和交付

应在CPS 中明确订户签名密钥对的生成、交付及控制方式，并符合以下要求之一：

a) 由订户持有的符合国家安全标准的密码模块产生和存储；

b) 由CA 产生、保存，并提供技术措施确保订户对签名私钥的独占控制权；

c) 采用通过主管部门认可的其他创新性保护方案。

应在CPS 中声明完整记录所有与订户签名私钥相关的操作日志，包括时间、方式、操作人员等信息，保存期限不少于证书失效后五年。

6.6.3 私钥保护和密码模块工程控制

6.6.3.1 CA 私钥保护和密码模块工程控制

应在CPS中声明根证书私钥保护符合的要求，包括但不限于：

a) 根证书私钥保护使用通过国家密码主管部门认可的密码产品，符合GB/T 37092—2018第5章的要求；

b) 根证书私钥实施严格的分割保护机制，实现单人无法获取完整私钥；

c) 根证书私钥备份由密钥管理员分别保存在有防盗措施的安全场所。

6.6.3.2 订户私钥保护和密码模块工程控制

应在CPS 中声明订户签名私钥保护符合下列要求之一：

a) 订户签名私钥由订户持有：协议中要求订户采取预防措施防止私钥及其激活数据的丢失、泄露、更改或未经授权的使用；

b) CA 受订户委托保管订户签名私钥，明确以下内容：

1) 采用的电子签名模式；

2)采用的安全控制措施，并定期进行安全评估；

3) 每次签名私钥调用必须获得订户的明确授权，授权记录应完整保存；

4)向订户提供关于签名私钥及激活数据安全使用的指导与建议；

5)电子签名模式和控制措施应符合相关标准或采用经主管部门认可的其他方式。

6.6.4 密钥对管理的其他方面

6.6.4.1 公钥归档

应在CPS 中声明对公钥证书进行定期归档及其最大间隔。

6.6.4.2 证书操作期和密钥对使用期限

应在CPS 中声明：

a) 无论是订户证书还是CA 证书，证书到期后，签名私钥不可用于电子签名；

b) 根证书密钥对、订户证书密钥对及其他各类密钥的最长有效期。

6.6.5 激活数据

应在CPS中明确激活数据从生成、传输、使用、保管到销毁各环节的安全控制措施，包括但不限于：

a)CA、 证书订户妥善保管各自的激活数据，并采用安全的技术措施传输激活数据；

b) 激活数据宜采用多种方式，并具有足够的复杂度。

6.6.6 计算机安全控制

应在CPS 中明确建立并实施符合GB/T 25056—2018中8.2要求的计算机安全控制体系，包括但不限于：

a) 至少每半年检查一次系统升级补丁，记录系统升级审批及实施过程；
b) 对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划：
c) 对所有服务器和操作终端安装杀毒软件；
d) 病毒库更新间隔；
e) 病毒扫描时间间隔。

6.6.7 生存周期安全控制

应在CPS中声明建立并实施符合GB/T 25056—2018中第10、11、12章要求的生存周期安全控制体系。

6.6.8 网络安全控制

应在CPS中明确建立并实施符合GB/T 25056—2018中5.3.8要求的网络安全控制体系，包括但不限于：

a) 网络结构满足GB/T 25056—2018附录A 中规定形式的一种；
b) 对所有Web 服务配置防火墙、Web 应用防火墙、入侵检测系统和内容过滤等网络安全防护措施；
c) 建立并维护网络拓扑图，包含所有网络设备、连接关系和安全边界，定期更新，与机房实际情况保持一致；
d) 网络访问控制：
   1) 建立针对证书签发子系统及数据库的访问白名单机制，仅授权证书注册子系统的必要功能模块及必要的管理设备进行访问；
   2) 建立针对证书注册子系统和数据库的访问白名单机制。
e) 网络监控：
   1) 定期对系统日志进行分析；
   2) 分析内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

6.6.9 时间戳

若部署时间戳服务，应在CPS 中明确时间戳服务的使用范围、方式、保障机制及相关技术标准。

6.7 证书、证书撤销列表和在线证书状态协议

6.7.1 证书

应在CPS中明确电子签名认证证书的格式，格式应符合GB/T 20518的要求，包括但不限于：

a) 支持的数字证书格式版本号；
b) 密码算法对象标识符；
c) CA 和订户的名称；
d) 证书策略对象标识符，其中必须包含主管部门制定的相应等级证书策略OID（见6.1.5.1），可包含CA 制定或遵循的证书策略OID;
e) 证书序列号；
f) 证书有效期；
g) 订户的电子签名验证数据；
h) CA 的电子签名。

宜在CPS中明确电子签名认证证书中包含证书用途、建立的流程、签名私钥的保存方式、相关的法律符合性等内容，便于订户及依赖方了解证书内容。

6.7.2 证书撤销列表

应在CPS中明确证书撤销列表 (CRL) 的格式符合GB/T 20518—2018中5.3的要求。

6.7.3 在线证书状态协议

应在CPS中明确在线证书状态服务符合GB/T 19713—2025中第7章的要求。

6.8 认证机构审计及相关评估

6.8.1 审计评估制度

应在CPS 中声明制定了审计评估制度，制度内容包括但不限于：

a) 审计评估的类型，至少包括认证业务审计和全面符合性评估；
b) 执行审计评估的频率，或是引发评估事件的条件；
c) 参与执行审计评估人员的专业背景；若由外部机构执行审计，规定对外部机构的要求；
d) 审计评估所涵盖的主题和评估的方法。

6.8.2 认证业务审计

应在CPS 中明确认证业务审计方式，包括但不限于：

a) 审计周期；
b) 审计内容包括但不限于证书申请、续期、密钥变更、更新、撤销、冻结等业务中订户告知、身份查验、意愿记录、协议签署、资料保存的合规性；
c) 审计采用全面审计或抽样审计方式，采用抽样方式的，明确审计抽样率；
d) 对于审计发现的问题，通知相关部门和人员及时整改，并跟踪整改落实情况。

6.8.3 全面符合性评估

应在CPS中声明符合性评估方式，包括但不限于：

a) 评估周期不少于每年一次；
b) 评估内容包括但不限于：年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况等；
c) 审计采用抽样方式的，抽样率不低于6.8.2.c 的要求；
d) 对于审计发现的问题，通知被审计部门及时整改，并跟踪整改落实情况；
e) 在1月底前将上一年度符合性评估报告报送主管部门。

6.9 法律责任和其他业务条款

6.9.1 费用

应在CPS中声明开展了服务成本核算，制定价格策略，并公布各项服务收费标准，收费标准可包括：

a) 证书颁发或更新费用；
b) 证书访问费用；
c) 撤销证书的费用；
d) 状态信息访问费用；
e) 电子签名的费用；
f) 签名验证的费用；
g) 签名验证报告的费用；

h） 其他服务的费用。

应在CPS 中明确收费标准的公布方式。可在CPS 中明确退款规定的公布方式。

6.9.2 财务责任

应在CPS 中明确赔付专项备用资金或其他资金保障方式，资金保障额度不低于上一年度营业收入1.5%,声明资金来源以及管理方式。

6.9.3 业务信息保密

应在CPS 中明确保密信息和非保密信息的范围。

6.9.4 个人隐私保护

应在CPS 中明确保护个人隐私信息的措施，具体措施参照GB/T 35273的规定。

6.9.5 知识产权

应在CPS 中明确电子认证业务开展中的知识产权情况，如著作权、专利、商标等。

6.9.6 陈述和担保

应在CPS 中明确CA、 订户、依赖方在从事电子认证活动中应作的陈述和担保。

6.9.7 担保免责

应在CPS中明确担保免责内容，包括但不限于：

a) 担保责任的否定描述；
b) 隐含担保责任的描述；
c) 担保免责条款的适用规定。

6.9.8 偿付责任规则

应在CPS中声明制定偿付责任规则，内容包括但不限于：

a) 财务赔偿范围应涵盖CA 在履行其服务职责时可能面临的各种风险，包括但不限于技术故障、人为错误、安全漏洞等；
b) 明确界定不同情形下的赔付计算方式；
c) 设立赔付监督机制。

6.9.9 赔偿

应在CPS中明确赔偿的申请、审核、审批和支付流程，明确各环节时限。

6.9.10 有效期和终止

应在CPS中明确CPS的有效期，以及文档全部或部分终止或对某一特定参与者的适用性终止的条件。

6.9.11 对参与者的个别通告与沟通

应在CPS 中明确电子认证活动中某一参与方与另一参与方进行通信时使用的方法，以使其通信过程在法律上有效。

6.9.12 修订和发布

应在CPS 中明确规则修订的条件，以及修订后的通告机制和周期。

6.9.13 争议处理与举证

应在CPS中明确：

a) 与 CP/CPS、 电子认证服务相关的争议解决机制，包括争议的受理范围、处理流程、协商时限、调解规则，以及诉讼、仲裁等法定争议解决方式的管辖规则与适用条件；

b) 举证制度和能力体系覆盖证书全生存周期，包括但不限于：

1)证书签发环节，身份验证记录、材料审查记录、告知记录、意愿确认记录等；

2)签名环节，签名请求验证、签名操作日志、时间戳记录等；

3)验证签名环节，验证请求记录、验证结果记录、异常情况处理记录等：

4) 提供举证材料的时间承诺。

6.9.14 管辖法律

应在CPS中明确各类活动的适用管辖。

6.9.15 与适用法律的符合性

应在CPS中明确电子认证服务的相关参与者需遵守适用的法律法规，在中华人民共和国境内适用的法律法规包括但不限于《中华人民共和国电子签名法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》《电子认证服务密码管理办法》。

6.9.16 一般条款

应在CPS 中声明的一般条款，包括但不限于：

a) 标识出构成CPS 的全部文档，并声明该CPS 替代所有先前或同时期的相关文档；

b) 订户协议及依赖方协议中标明对应的CPS 版本。

6.9.17 其他条款

CPS可包括未在上述说明的其他相关内容条款。

7 证实方法

7.1 证实方式

可通过以下方式进行验证：

a) 材料检查：对CA 公布的CPS、CP 与本文件要求进行对比，并与CA 的内控制度、运行记录等材料进行符合性检查；

b) 现场检查：现场勘察、访谈、业务模拟，能够证实CA 的相关人员、环境、系统、管理制度真实存在，能够证实CA 的运行情况与相关材料相符。

7.2 检查方法

7.2.1 电子认证业务规则内容完整性的检查

通过材料检查，验证CPS包含第5章规定的内容。

7.2.2 概括性描述的检查

7.2.2.1 承诺的检查

通过材料检查，验证CPS包含6.1.1规定的内容。

7.2.2.2 基本信息的检查

通过材料检查，验证CPS包含6.1.2规定的内容。

7.2.2.3 文档名称与标识的检查

通过材料检查，验证CPS包含6.1.3规定的内容。

如果CA 发布了CP，通过文本对比和权威OID数据库查询，检查该机构是否为CP申请了OID。

7.2.2.4 电子认证活动参与者的检查

通过材料检查，验证CPS包含6.1.4规定的内容。

7.2.2.5 证书应用的检查

通过现场检查，验证CA 发布的电子签名认证证书是否包含主管部门的证书策略OID。

通过现场检查，验证CA是否按应用对签发的数字证书进行分类，并且符合6.1.5的规定。

7.2.2.6 策略管理的检查

通过材料审查，验证CA建立策略管理机构，并履行6.1.6.1规定的职责。

通过材料审查，验证CA按6.1.6.2规定的流程批准及备案CPS。

7.2.2.7 定义与缩写的检查

通过材料检查，验证CPS包含6.1.7规定的术语、定义与缩写，并与本文件保持一致。

7.2.3 信息发布与信息管理的检查

通过现场检查，验证CA在官网发布6.2规定的内容，并完成与国家电子认证服务管理平台的备案和对接。

7.2.4 身份标志与查验的检查

7.2.4.1 身份查验通用要求的检查

通过材料审查，验证CPS 包含6.3.1规定的内容。

通过现场办理证书和抽样证书资料的方式，检查CA未将订户告知、身份、意愿记录、协议签订等相关义务委托外部机构或个人。

7.2.4.2 订户告知的检查

通过查验7.2.4.1节获取的证书和资料，验证CA按照6.3.12.2要求的方式向订户告知了6.3.1.2.1规定的内容，并进行了记录。

7.2.4.3 初始身份确认的检查

7.2.4.3.1 证明拥有私钥的方法的检查

通过查验7.2.4.1节办理证书的过程，验证CA提供可靠的技术手段和其他必要措施，实施或监督实施用户私钥的生成，并通过数字签名的方式确认订户拥有公钥对应的签名私钥。

7.2.4.3.2 个人身份查验的检查

通过查验7.2.4.1节获取的个人证书和资料，验证CA按6.3.2.2规定的要求实施个人订户身份的查验，并保存查验过程和结果的资料。

7.2.4.3.3 机构身份查验的检查

通过查验7.2.4.1节获取的证书和资料，验证CA按6.3.2.3规定的要求实施机构身份的查验，并保存查验过程和结果的资料。

7.2.4.4 订户意愿记录的检查

通过查验7.2.4.1节获取的证书和资料，验证CA 按6.3.3规定的要求，记录订户办理电子认证服务的意愿。

7.2.4.5 订户协议的检查

通过查验7.2.4.1节获取的证书和资料，验证CA 按6.3.4规定的要求，与订户签订协议。

7.2.4.6 未验证的订户信息的检查

通过查验7.2.4.1节获取的证书和资料，验证CA按6.3.5规定的要求查验证书载明信息。

7.2.4.7 命名的检查

通过文本比对，验证CPS 按6.3.7规定的要求说明证书主体DN的命名规则。

通过查验7.2.4.1节获取的证书和资料，验证CA 签发的电子签名认证证书符合6.3.7规定的要求。

7.2.5 证书生存周期操作要求的检查

7.2.5.1 通用要求的检查

通过文本比对，验证CPS按6.4.1规定的要求撰写证书申请的流程和各方责任。

7.2.5.2 证书申请的检查

通过文本比对，验证CPS按6.4.2规定的要求撰写证书申请处理的过程。

通过现场检查，验证CA按6.4.2规定的要求处理证书申请。

7.2.5.3 证书签发的检查

通过文本比对，验证CPS按6.4.3规定的要求撰写证书签发的过程。

通过现场检查，验证CA对接国家电子认证服务管理平台。

通过查验7.2.4.1节获取的证书和资料，验证CA按6.4.3规定的要求处理签发申请并告知订户。

7.2.5.4 证书接受的检查

通过文本比对，验证CPS按6.4.4规定的要求撰写证书接受的过程。

通过查验7.2.4.1节获取的证书和资料，验证CA按6.4.4规定的要求交付证书并记录。

7.2.5.5 密钥对和证书的使用的检查

通过文本比对，验证CPS按6.4.5规定的要求撰写电子认证活动参与者在密钥对和证书使用中的权利和义务，并说明本机构保护订户签名私钥的措施。

通过现场检查，验证CA按6.4.5规定的要求保护订户签名私钥。

7.2.5.6 证书续期的检查

通过文本比对，验证CPS按6.4.6规定的要求撰写证书续期的过程。

通过现场检查，验证CA按6.4.6规定的要求响应续期申请。

7.2.5.7 证书密钥更新的检查

通过文本比对，验证CPS 按6.4.7规定的要求撰写证书密钥更新的过程。

通过现场检查，验证CA按6.4.7规定的要求响应证书密钥更新的申请。

7.2.5.8 证书变更的检查

通过文本比对，验证CPS按6.4.8规定的要求撰写证书变更的条件和过程。

通过现场检查，验证CA 按6.4.8规定的要求响应证书变更的申请。

7.2.5.9 证书撤销或冻结的检查

通过文本比对，验证CPS 按6.4.9规定的要求撰写证书撤销与冻结的规则，验证CA制定非订户发起的撤销请求的审批制度。

通过现场检查，验证CA按6.4.9规定的要求响应证书撤销或冻结的申请，并在证书安全性受到威胁时，实施相应的操作。

7.2.5.10 证书状态信息服务的检查

通过文本比对，验证CPS按6.4.10规定的要求公开证书状态信息服务的情况。

通过现场检查，验证CA按6.4.10规定的要求提供证书状态信息服务。

7.2.5.11 停止使用认证服务的检查

通过文本比对，验证CPS 按6.4.11规定的要求明确订户停止使用电子认证服务的流程及后续处理方式。

7.2.5.12 密钥托管与恢复的检查

通过现场检查，验证CA按6.4.12规定的要求保护根证书密钥。

7.2.6 物理控制的验证

7.2.6.1 物理控制概述的验证

通过文本比对，验证CPS 按6.5.1规定的要求明确其采用的控制措施及其遵守的法律法规和技术标准。

7.2.6.2 物理控制的检查

通过文本比对，验证CPS按6.5.1规定的要求明确技术设施情况和控制措施。

通过现场检查，验证CA按6.5.1规定的要求实施物理控制。

7.2.6.3 操作过程控制的检查

7.2.6.3.1 可信角色的检查

通过文本比对，验证CPS 按6.5.2.1规定的要求明确可信角色的设置。

通过现场检查，验证CA具备相应角色的人员。

7.2.6.3.2 职责分离的检查

通过文本比对，验证CPS 按6.5.2.2规定的要求明确各岗位的设置。

通过现场检查，验证CA 实际人员符合相应的职责分离要求。

7.2.6.4 操作过程控制的检查

7.2.6.4.1 可信人员资格要求的检查

通过文本比对，验证CA在CPS和管理制度中按6.5.3.1规定的要求明确可信人员资格要求和核实流程。

通过现场检查，验证CA实际人员满足相应要求。

7.2.6.4.2 可信人员培训要求的检查

通过文本比对，验证CA 在CPS 和管理制度中按6.5.3.2规定的要求明确可信人员培训的要求。

通过现场检查，验证CA 按相应要求开展培训和考核。

7.2.6.5 审计日志程序的检查

通过文本比对，验证CPS 按6.5.4规定的要求明确日志记录和审计的范围和程序。

通过现场检查，验证CA 按相应要求实施。

7.2.6.6 记录归档的检查

通过文本比对，验证CPS 按6.5.5规定的要求明确相关记录归档的范围和程序。

通过现场检查，验证CA按相应要求开展记录归档。

7.2.6.7 电子认证服务机构密钥更替的检查

通过文本比对，验证CPS按6.5.6规定的要求明确本机构密钥更替的程序。

通过现场检查，验证CA 按相应要求开展密钥更替。

7.2.6.8 损坏和灾难恢复的检查

通过文本比对，验证CA制定电子认证服务的连续性计划与灾难恢复应急预案，验证CA 按6.5.7规定的要求明确本机构应对损害和灾难的程序。

7.2.6.9 电子认证服务机构终止的检查

通过文本比对，验证CA 按6.5.8规定的要求明确本机构终止服务的程序。

7.2.6.10 重大事项报告的检查

通过文本比对，验证CA在CPS或其他管理制度中按6.5.9规定的要求明确本机构重大事项报告的范围和程序。

通过现场检查，验证CA 按相应要求开展重大事项报告。

7.2.7 认证系统技术安全控制的验证

7.2.7.1 技术安全控制制度要求

通过文本比对，验证CA按6.6.1规定的要求建立本机构技术安全控制制度。

7.2.7.2 密钥对的生成和安装的检查

7.2.7.2.1 根证书密钥对的生成和安装的检查

通过文本比对，验证CA建立本机构密钥对全生存周期管理机制，在CPS中按6.6.2.1规定的要求明确本机构密钥对生成和安装要求。

通过现场检查，验证CA 按相应要求开展本机构密钥对生成和安装。

7.2.7.2.2 订户密钥对的生成和交付的检查

通过文本比对，验证CA 建立订户密钥对全生存周期管理机制，在CPS中按6.6.2.2规定的要求明确订户密钥对生成和交付要求。

通过现场检查，验证CA按相应要求开展订户密钥对生成和交付。

7.2.7.3 密钥对管理的其他方面的检查

7.2.7.3.1 公钥归档的检查

通过文本比对，验证CA 在CPS 或其他管理制度中按6,6.4.1规定的要求明确本机构公钥归档的机制、时间和程序。

通过现场检查，验证CA 按相应要求开展公钥归档。

7.2.7.3.2 证书操作符合密钥对使用期限的检查

通过文本比对，验证CPS 按6.6.4.2规定的要求明确密钥的使用期限及到期后的使用限制。

通过现场检查，验证CA 按相应要求销毁到期的签名私钥。

7.2.7.4 激活数据的检查

通过文本比对，验证CPS 按6.6.5规定的要求明确激活数据的安全控制措施。

通过现场检查，验 证CA 按相应要求保护激活数据。

7.2.7.5 计算机安全的检查

通过现场检查，验 证CPS 按6.6.6规定的要求实施计算机安全控制。

7.2.7.6 生存周期安全控制的检查

通过现场检查，验证CPS 按6.6.7规定的要求实施证书生存周期安全控制。

7.2.7.7 网络安全的检查

通过现场检查，验证CPS按6.6.8规定的要求实施网络安全控制。

7.2.7.8 时间戳的检查

通过文本比对，验证CPS按6.6.9规定的要求明确时间戳服务的相关情况。

通过现场检查，验证CA真实提供时间戳服务，且符合CPS中声明的情况。

7.2.8 证书、证书撤销列表和在线证书状态协议的检查

7.2.8.1 证书的检查

通过文本比对，验证CPS 按6.7.1规定的要求明确本机构签发的电子签名认证证书的格式。

通过现场检查，验证CA 生成的证书符合相关要求。

7.2.8.2 证书撤销列表的检查

通过文本比对，验证CPS按6.7.2规定的要求明确本机构证书撤销列表的格式。

通过现场检查，验证CA 发布的证书撤销列表符合相关要求。

7.2.8.3 在线证书状态协议的检查

通过文本比对，验证CPS 按6.7.3规定的要求明确本机构在线证书状态的协议。

通过现场检查，验证CA提供的在线证书状态服务符合相关要求。

7.2.9 认证机构审计和其他评估的检查

通过现场检查，验证CA按6.8规定的要求建立并实施定期审计或评估机制。

7.2.10 法律责任和其他业务条款的检查

7.2.10.1 费用的检查

通过文本比对，验证CPS 按6.9.1规定的要求声明本机构收费标准的公布方式。

通过现场检查，验证CA按相应方式公布收费标准。

7.2.10.2 财务责任的检查

通过文本比对，验证CPS按6.9.2规定的要求明确本机构财务赔偿责任的范围和资金来源。

7.2.10.3 业务信息保密的检查

通过文本比对，验证CPS按6.9.3规定的要求明确本机构保密信息的范围和非保密信息的范围。

7.2.10.4 个人隐私保护的检查

通过文本比对，验证CPS 按6.9.4规定的要求明确本机构个人隐私保护措施。

7.2.10.5 知识产权的检查

通过文本比对，验证CPS按6.9.5规定的要求明确本机构知识产权保护相关问题。

7.2.10.6 陈述和担保的检查

通过文本比对，验证CPS按6.9.6规定的要求明确电子认证服务各参与方应作的陈述和担保。

7.2.10.7 担保免责的检查

通过文本比对，验证CPS按6.9.7规定的要求明确本机构担保免责条款。

7.2.10.8 偿付责任的检查

通过文本比对，验证CPS按6.9.8规定的要求明确本机构偿付责任规则。

7.2.10.9 赔偿的检查

通过文本比对，验证CPS按6.9.9规定的要求公开本机构赔偿的业务流程。

7.2.10.10 有效期和终止的检查

通过文本比对，验证CPS按6.9.10规定的要求明确CPS的有效期和适用性。

7.2.10.11 对参与者个别通告与沟通的检查

通过文本比对，验证CPS按6.9.11规定的要求明确本机构与相关方通信时使用的方法。

7.2.10.12 修订和发布的检查

通过文本比对，验证CPS 按6.9.12规定的要求明确CPS的修订条件及发布机制和周期。

通过现场检查，验证CA按相关要求修订和发布CPS。

7.2.10.13 争议处理的检查

通过文本比对，验证CPS按6.9.13规定的要求明确本机构关于CPS的争端解决程序。

通过现场检查，验证CA:

a) 真实提供电子签名验证服务；
b) 公示电子签名验证服务标准、流程和价格；
c) 建立举证制度和能力体系。

7.2.10.14 管辖法律的检查

通过文本比对，验证CPS按6.9.14规定的要求明确电子认证服务的司法管辖区。

7.2.10.15 与适用法律的符合性的检查

通过文本比对，验证CPS按6.9.15规定的要求明确电子认证服务的相关参与者应遵守适用的法律法规。

7.2.10.16 一般条款的检查

通过文本比对，验证CA按6.9.16规定的要求，在订户协议和依赖方协议中明确CPS的版本。

附 录 A
（资料性）
电子认证业务规则文档结构

一般情况下， 一个典型的电子认证业务规则文档结构见示例。

示例：

1概括性描述
1.1承诺
1.2基本信息
1.3文档名称与标识
1.4电子认证活动参与者
1.5证书应用
1.6策略管理
1.7定义和缩写
2信息发布与信息管理
3身份标识与查验
3.1身份查验通用要求
3.2初始身份确认
3.3订户意愿记录
3.4订户协议
3.5未验证的订户信息
3.6互操作要求
3.7命名
4证书生存周期操作要求
4.1通用要求
4.2证书申请
4.3证书签发
4.4证书接受
4.5密钥对和证书的使用
4.6证书续期
4.7证书密钥更新
4.8证书变更
4.9证书撤销或冻结
4.10证书状态信息服务
4.11停止使用认证服务
4.12密钥托管与恢复
5认证机构设施、管理和操作控制
5.1物理控制
5.2操作过程控制
5.3人员控制
5.4审计日志程序
5.5记录归档
5.6电子认证服务机构根证书密钥更替
5.7损害和灾难恢复
5.8电子认证服务机构终止
5.9重大事项报告
6认证系统技术安全控制
6.1技术安全管理制度要求
6.2密钥对的生成和安装
6.3私钥保护和密码模块工程控制
6.4密钥对管理的其他方面
6.5激活数据
6.6计算机安全控制
6.7生存周期安全控制
6.8网络安全控制

参 考 文 献

[1]GB/T 16262.1—2025 信息技术抽象语法记法一(ASN.1) 第1部分：基本记法规范

[2]GB/T 17969.1—2015 信息技术开放系统互联 OSI 登记机构的操作规程第1部分： 一般规程和国际对象标识符树的顶级弧

[3]GB/T 25069—2022 信息安全技术术语

[4]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

[5]GB/T 33560—2017 信息安全技术密码应用标识规范

[6]GB/T 35275—2017 信息安全技术 SM2密码算法加密签名消息语法规范

[7]GB/T 35276—2017 信息安全技术 SM2 密码算法使用规范

[8]GM/Z 4001—2013 密码术语

[9] 《电子认证服务管理办法》(2015年4月29日中华人民共和国工业和信息化部令第29号《工业和信息化部关于修改部分规章的决定》修订)

[10]《中华人民共和国网络安全法》(2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过，根据2025年10月28日第十四届全国人民代表大会常务委员会第十八次会议《关于修改《中华人民共和国网络安全法〉的决定》修正)

[11]《电子认证服务密码管理办法》(2009年10月28日国家密码管理局公告第17号公布，根据2017年12月1日《国家密码管理局关于废止和修改部分管理规定的决定》修正)

[12]《中华人民共和国电子签名法》(2019年4月23日第十三届全国人民代表大会常务委员会第十次会议修正)

[13]《中华人民共和国数据安全法》(中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于2021年6月10日通过)

[14]《商用密码管理条例》(2023年4月14日国务院第4次常务会议修订通过)

CQAE

T/CQAE 11034-2025

中国电子质量管理协会
团体标准
电子认证业务规则规范
T/CQAE 11034—2025

*

中国电子质量管理协会 编制
中国电子质量管理协会 发行

电话：(010)68209757　传真：(010)68209757
地址：北京市海淀区万寿路27号8号楼8层
邮编：100036
网 址：www.cqae.org.cn

*

开 本：880×12301/16　　印张：2 $\frac{1}{2}$ 字数：60千字
2026年3月第一版2026年3月第一次印刷