ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35289—2017

信息安全技术
电子认证服务机构服务质量规范

Information security technology—
Specification on the service quality of certification authority

2017-12-29 发布　　2018-07-01 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:北京天威诚信电子商务服务有限公司、北京天诚安信科技股份有限公司、中国电子信息产业发展研究院。

本标准主要起草人:唐志红、刘旭、刘权、白波、刘艳丽、陈韶光、王亚静、金露、张海松。

信息安全技术
电子认证服务机构服务质量规范

1 范围

本标准规定了电子认证服务机构业务服务质量要求、保障服务质量要求及服务质量分级，明确了电子认证服务机构服务质量的具体指标要求。

本标准适用于提供电子认证服务的机构。

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 25056—2010 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 25069—2010 信息安全技术 术语

GB/T 35288—2017 信息安全技术 电子认证服务机构从业人员岗位技能规范

3 术语和定义

GB/T 25069—2010 中界定的以及下列术语和定义适用于本文件。

3.1

数字证书 digital certificate

由证书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、有效期以及一些扩展信息的数字文件。

3.2

电子认证 electronic authentication

采用电子技术检验用户真实性的操作。

3.3

电子签名 electronic signature

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

3.4

鉴证 authentication

辨别认定证书申请者提交材料的真伪，并对证书申请材料和申请者之间的关联性进行确定的活动。

3.5

可靠电子签名 reliable electronic signature

符合下列条件的电子签名：

a) 电子签名制作数据用于电子签名时，属于电子签名人专有；

b) 签署时电子签名制作数据仅由电子签名人控制；

c) 签署后对电子签名的任何改动能够被发现；

d) 签署后对数据电文内容和形式的任何改动能够被发现。

3.6

电子认证服务 electronic certification service

为电子签名相关各方提供真实性、可靠性验证的活动。

3.7

电子认证服务机构 certification authority

负责创建、分发证书并在必要时提供验证以证实用户身份的机构。

3.8

电子认证服务质量 electronic certification service quality

电子认证服务过程和结果满足明确的、隐含的要求所呈现的特征。

3.9

订户 subscriber

从电子认证服务机构接收证书的实体。

3.10

证书依赖方 certificate relying party

依赖于证书真实性的实体。

4 缩略语

下列缩略语适用于本文件。

CA	认证机构(Certification Authority)
CP	证书策略(Certificate Policy)
CPS	认证业务规则(Certification Practice Statement)
CRL	证书撤销列表(Certificate Revocation List)
FAQ	频繁提及的问题(Frequently Asked Questions)
KMC	密钥管理中心(Key Management Center)
PKI	公钥基础设施(Public Key Infrastructure)
RA	注册机构(Registration Authority)
USB KEY	采用 USB 接口的证书存储介质(Universal Serial Bus KEY)
OCSP	在线证书状态协议(Online Certificate Status Protocol)

5 电子认证服务综述

5.1 电子认证服务

5.1.1 综述

电子认证服务是指电子认证机构面向证书订户提供的认证服务。相关的服务内容包括:业务办理服务、技术支持服务、业务咨询服务、售后服务和司法支持服务等。

电子认证服务可分为 3 类:

a) 核心业务类:主要指业务办理服务,电子认证机构需面向证书订户提供;

b) 推荐业务类:主要指技术支持服务,建议电子认证机构面向证书订户提供,以提升其服务质量;

c) 可选业务类:包括业务咨询服务、售后服务和司法支持服务等,各电子认证机构根据自身情况

自行决定是否面向证书订户提供。

5.1.2 业务咨询服务

业务咨询服务是指向客户提供电子认证服务业务介绍、业务办理流程、证书应用和电子认证服务相关法律法规的解读，包括：

a) 业务介绍——内容应包括电子认证服务机构所能签发的业务种类、证书种类、适应范围等；
b) 业务办理流程——内容应包括证书订户在办理证书申请、撤销、更新等业务时所应遵循的流程和提交的各种资料；
c) 证书应用——内容应包括数字证书（本标准中也简称为“证书”）在应用系统中所能提供的功能和价值，操作方法等；
d) 电子签名法解读——应能提供电子签名法中对电子认证服务机构、证书订户、证书依赖方权利和责任的具体解读。

5.1.3 业务办理服务

5.1.3.1 综述

业务办理服务是针对证书订户提供包括证书申请、证书签发、证书更新、密钥更新、证书变更、证书撤销和挂起、证书的有效性验证、密钥生成、备份和恢复、证书口令解锁、证书补办等在内的各种服务：

a) 证书申请——是指订户向电子认证服务机构提出申请，并按照相关要求提供身份证明材料；
b) 证书签发——指电子认证服务机构受理用户提出的证书申请，对申请材料的真实性进行鉴证，鉴证通过的，予以签发证书；
c) 证书更新——指订户使用的证书到期后如需继续使用，应向电子认证服务机构提出申请；电子认证服务机构审核订户提交的资料，完成证书更新的服务过程；
d) 证书密钥更新——指订户生成一对新密钥并申请为新公钥签发新证书的服务过程；
e) 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服务过程；
f) 证书的撤销和挂起——指在订户合同期满、丢失或私钥泄漏的情况下进行证书的撤销和挂起的服务过程；
g) 证书的有效性验证——指订户向电子认证服务机构申请验证证书是否有效；
h) 密钥的生成、备份和恢复——指加密证书私钥的生成、备份和恢复的过程；
i) 证书口令解锁——指订户由于某些原因导致忘记口令，应向电子认证服务机构提出申请；电子认证服务机构审核订户提交的资料，完成证书口令解锁的过程；
j) 证书补办——指订户由于证书丢失或损坏时申请证书补办的过程。

5.1.3.2 证书申请

证书申请服务要求电子认证服务机构应告知申请者需提交的材料，提供材料正确的则接收申请材料。

5.1.3.3 证书签发

电子认证服务机构或注册机构应执行严格的鉴证流程和准则，对申请材料进行真实性鉴证，并根据结果对申请者给予批准受理或者拒绝受理的答复。予以批准受理的则签发证书，证书签发服务要求电子认证服务机构验证注册机构签名和确认注册机构的权限，并签发证书。

5.1.3.4 证书更新

电子认证服务机构应明确告知证书订户需进行更新操作的情形、更新过程中对证书订户的要求、证

书更新的请求及受理方式、更新证书的签发及发布方式。

5.1.3.5 证书密钥更新

证书订户下载证书更新时，如需要对密钥对进行替换，电子认证服务机构应明确告知证书订户需进行更新操作的情形、更新过程中对证书订户的要求、证书更新的请求及受理方式、更新证书的签发及发布方式。

5.1.3.6 证书变更

证书变更是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。电子认证服务机构应明确告知证书订户需进行变更操作的情形、变更过程中对证书订户的要求、变更的请求及受理方式、变更证书的签发及发布方式。

5.1.3.7 证书的撤销和挂起

证书撤销和挂起服务过程中，电子认证服务机构应明确证书撤销和挂起的情形、请求撤销和挂起权限以及撤销和挂起请求的程序、处理流程、宽限期、处理时间、发布方式和依赖方检查证书撤销和挂起的要求。

5.1.3.8 证书的有效性验证

电子认证服务机构应明确证书有效性验证的操作特点，有效性验证服务可用性说明，服务不可用时适用策略，有效性验证服务其他可选特征。

5.1.3.9 密钥的生成、备份和恢复

通过电子认证服务机构或其他可信第三方进行的客户私钥生成、备份和恢复相关的策略和业务实践过程。包括客户私钥生成、备份、恢复和会话密钥封装和恢复过程。

5.1.3.10 证书补办

电子认证服务机构应提供证书补办服务，证书补办过程中，应当告知订户补办申请需提交的材料，电子认证服务机构对补办申请及其申请者身份进行审核，情况属实的予以办理。

5.1.3.11 证书口令解锁

证书口令解锁过程中，电子认证服务机构应当告知订户提交解锁申请需提交的材料，电子认证服务机构对口令解锁申请及其申请者身份进行审核，情况属实的予以办理。

5.1.4 技术支持服务

技术支持服务是指电子认证服务机构在提供电子认证服务时提供相关的技术支持，包括数字证书管理、数字证书使用、数字证书存储介质硬件设备使用、电子认证服务系统使用及各类数字证书应用(如证书登录、证书加密、数字签名和安全邮件等)等。

电子认证服务过程中技术支持主要针对如下问题和故障，提供必要的支持方式：

a) 问题——主要指证书使用或者证书相关应用过程中的技术问题，如：证书不能签名等；

b) 故障——主要指电子认证服务系统不能正常运行或者停止服务，如：系统崩溃、宕机等。

电子认证服务过程中对技术问题或者技术故障可以分为如下 3 类：一般事件、严重事件和重大事件。

a) 一般事件——系统部分出现故障，不影响系统整体运行，不影响业务处理或客户提出的安全技术咨询、索取技术资料、技术支持等；

b) 严重事件——系统不能正常运转或不稳定，但不影响主要业务的故障；

c) 重大事件——系统停止服务或有严重错误，影响业务处理或对客户造成巨大损失而产生严重后果和不良影响的故障，如：系统崩溃、宕机等。

电子认证服务机构应对技术问题和技术故障参考上述描述进行分类，并制定相应处理流程和机制，以确保服务的及时性和连续性。

5.1.5 售后服务

售后服务主要是对用户在证书使用及证书相关应用中的意见、建议和投诉的处理，包括：

a) 回访——应制定回访计划和流程，记录用户意见和建议；

b) 投诉——应公布投诉接收方式、记录投诉内容、解决投诉问题；

c) 纠纷处理——应按照 CPS 承诺的方式、内容进行处理；

d) 客户满意度——应随机对客户进行抽查，记录客户对电子认证服务总体的满意度。

5.1.6 司法支持服务

是指电子认证服务机构为使用数字证书服务的用户提供的一种电子签名验证服务。

5.2 电子认证服务质量

5.2.1 综述

电子认证服务质量总体要求如下：

——电子认证服务应按照 GB/T 25056—2010 等标准和相关法规的要求执行；

——电子认证服务应能明确满足订户在业务办理和证书应用过程中的各种合法的明示需求；

——电子认证服务所应满足的隐含需求是指证书依赖方对证书可靠性的隐含需求。

5.2.2 电子认证服务业务质量

电子认证业务所涉及的各项服务及要求如下：

a) 业务咨询服务——应向客户提供电子认证服务业务介绍、业务办理流程、证书应用、电子签名法相关法律法规的解读等内容；

b) 业务办理服务——应对客户提供证书签发、证书更新、密钥更新、证书变更、证书的撤销和挂起、密钥的生成、备份和恢复、证书口令解锁、证书补办等业务办理服务；

c) 技术支持服务——指电子认证服务机构在提供电子认证服务时提供相关的技术支持，包括数字证书管理、数字证书使用、数字证书存储介质硬件设备使用、电子认证服务系统使用以及各类数字证书应用（如，证书登录、证书加密、数字签名和安全邮件等）等，并对出现的问题或故障进行及时的处理；

d) 售后服务——应对用户在证书使用及证书相关应用中的意见、建议、投诉和纠纷能够及时处理。

e) 司法支持服务——应对用户的取证申请及时受理，并将取证内容的结论形成报告提交用户。

5.2.3 电子认证服务保障质量

提供可靠电子签名的电子认证服务，还需要相应的服务保障，具体包括服务场所、服务组织机构、服务人员、服务设施、服务纪律、业务连续性等服务保障：

a) 服务场所——应提供电子认证服务需要的活动场所，包括数据机房、服务中心、办公场所等；

b) 服务组织机构——应设置承担、执行业务咨询服务、业务办理服务、技术支持、安全管理、质量管理的岗位；

c) 服务人员——应配备业务咨询人员、业务办理人员、技术支持人员和质量管理人员的工作角色，并明确具体工作职能；

d) 服务设施——应提供电子认证服务所使用的设备配置，应能实现快速接收客户问题与意见，并能对问题进行记录，将问题转给相关技术支持人员处理，以及将结果及时反馈给客户。如电话呼叫中心、Web 网站、邮件系统、即时通讯等；

e) 服务纪律——应在提供四大类服务时，满足电子认证服务业务要求，需具有的服务纪律，如服务态度、服务用语、保密意识等；

f) 业务连续性——为保障所提供的电子认证服务质量，需具备的系统可用性、业务持续运作、系统灾难恢复等保障能力。

6 电子认证服务业务质量要求

6.1 业务咨询服务要求

业务咨询服务应包括证书业务、证书应用业务及其他电子认证服务机构开展的相关业务的咨询。业务咨询服务具体要求如下：

a) 对证书业务的咨询应告知用户相应服务流程；

b) 对证书应用业务的咨询应提供相应的宣传手册；

c) 对电子签名法相关法律条文的咨询应能明确解答；

d) 应明确告知申请者和电子认证服务提供者的责任与义务。

6.2 业务办理服务要求

6.2.1 综述

业务办理服务流程应包括 10 个环节：证书申请、证书签发、证书更新、证书密钥更新、证书变更、证书的撤销和挂起、证书的有效性验证、密钥的生成、备份和恢复、证书补办、证书口令解锁。

6.2.2 证书申请

受理证书申请过程中电子认证服务机构或注册机构应满足以下要求：

a) 对证书申请信息进行注册；

b) 对接收到申请材料进行通知；

c) 对申请材料保密；

d) 明确申请人和电子认证服务提供者的责任与义务。

6.2.3 证书签发

6.2.3.1 证书申请处理过程中电子认证服务机构或注册机构应满足以下要求：

a) 明确描述处理证书申请的流程并发布，并告知申请者；

b) 有明确的申请受理时间期限；

c) 告知申请拒绝的理由。

6.2.3.2 证书签发过程中电子认证服务机构或注册机构应满足以下要求：

a) 电子认证服务机构验证注册机构签名和确认注册机构的权限、并签发证书；

b) 建立面向证书申请者的通告机制。

6.2.3.3 证书接收过程中电子认证服务机构或注册机构应满足以下要求：

a) 明确电子认证服务机构对证书的发布方式；

b) 对申请者接收证书的步骤、操作等的记录和审计；

c) 电子认证服务机构对其他实体(如注册机构、依赖方等)的通告。

6.2.4 证书更新

证书更新过程中电子认证服务机构或注册机构应满足以下要求：

a) 电子认证服务机构发布的证书即将到期，但证书策略允许继续使用相同的密钥对；

b) 应重新进行与原始签发证书相同的过程；

c) 通告订户和其他相关实体；

d) 发布更新证书。

6.2.5 证书密钥更新

证书密钥更新过程中电子认证服务机构或注册机构应满足以下要求：

a) 证书密钥更新的情形(如因私钥泄漏而撤销证书之后、或者证书到期并且密钥对的使用期也到期之后)符合 CPS；

b) 证书密钥更新过程满足 GB/T 25056；

c) 通告订户和其他相关实体；

d) 发布更新证书。

6.2.6 证书变更

证书变更过程中电子认证服务机构或注册机构应满足以下要求：

a) 证书变更的情形(如名称改变等而造成的实体身份改变)符合 CPS；

b) 应重新进行与原始签发证书相同的过程；

c) 通告订户和其他相关实体；

d) 发布更新证书。

6.2.7 证书补办

证书补办过程中电子认证服务机构或注册机构应满足以下要求：

a) 告知订户需提交的材料；

b) 对补办申请及其申请者身份进行审核，情况属实的予以办理；

c) 应重新进行与原始签发证书相同的过程；

d) 通告订户和其他相关实体；

e) 发布更新证书。

6.2.8 证书口令解锁

证书口令解锁过程中电子认证服务机构或注册机构应满足以下要求：

a) 因订户保存口令不当等原因导致的忘记证书口令；
b) 告知订户提交 USB Key 解锁申请材料；
c) 对口令解锁申请及其申请者身份进行审核，情况属实的予以办理。

6.2.9 证书的撤销和挂起

证书变更过程中电子认证服务机构或注册机构应满足以下要求：

a) 证书撤销和挂起情形(例如订户合同期满、密码令牌丢失或怀疑私钥泄漏)符合 CPS；
b) 明确证书撤销和挂起流程；
c) 明确订户可用的宽限期；
d) 明确撤销和挂起请求处理期限；
e) 如果使用 CRL，明确 CRL 发布频率；
f) 如果使用 CRL，明确发布到证书库中的最长延迟；
g) 明确在线证书状态查询的可用性和方法；
h) 明确证书挂起的最长时间或期限；
i) 发布撤销或挂起信息。

6.2.10 证书的有效性验证

证书的有效性验证过程中电子认证服务机构应满足以下要求：

a) 明确证书的有效性验证的操作流程和特点；
b) 明确服务的可用性，以及服务不可用时的适用策略；
c) 如果有效性验证服务还有其他可选特征，需要明确。

6.2.11 密钥的生成、备份和恢复

密钥的生成、备份和恢复过程中电子认证服务机构应满足以下要求：

a) 密钥生成、备份和恢复的情形符合 CPS；
b) 密钥生成、备份和恢复过程满足 GB/T 25056；
c) 明确与私钥生成、备份和恢复相关的策略；
d) 明确会话密钥封装和恢复相关策略。

6.3 技术支持服务要求

技术支持服务具体要求如下：

a) 技术支持服务内容应解决证书使用问题和电子认证服务系统故障两大方面问题；
b) 技术支持服务内容应明确对一般事件、严重事件、重大事件的处理流程和响应时间；
c) 技术支持服务形式应至少包括：电话支持、远程协助支持、现场支持等；
d) 技术支持响应时间应以最大程度不影响客户使用为准则。

6.4 售后服务要求

售后服务主要是对客户证书使用情况的回访、接收客户投诉、客户纠纷处理以及客户满意度调查。

具体要求如下：

a） 应制定详细的客户证书使用情况回访计划，计划中应明确回访的目的、时间和形式；

b） 应及时接收客户投诉并解决相关问题；

c） 应及时处理与客户的纠纷；

d） 应定期对客户进行随机抽查，记录客户对电子认证服务总体的满意度。

6.5 司法支持服务要求

电子认证服务机构应按照申请完成对下述内容的验证：

a） 对用户要求取证的证书的有效性与真实性进行验证；

b） 对用户要求取证的电子数据进行验证；

c） 对取证过程进行见证，并对电子签名的法律符合性进行评定；

d） 将上述取证内容的结论形成专业的报告，以满足用户的行政审计、诉讼支撑等需求。

7 电子认证服务保障质量要求

7.1 服务场所要求

电子认证服务机构提供电子认证服务应具有固定的经营场所和满足电子认证服务要求的物理环境，应满足《电子认证服务管理办法》和 GB/T 25056—2010 等法律法规和规范的要求。

7.2 服务组织机构及服务人员要求

电子认证服务机构服务组织机构及服务人员要求应满足 GB/T 35288—2017 等规范和国家相关法律法规的要求。

7.3 服务设施要求

服务设施配置应实现快速接收客户问题与意见，并能对问题记录，将问题转给相关售后服务和技术支持人员处理，以及将结果及时反馈给客户，可通过呼叫中心、网站平台、电子邮件、即时通信工具等方式。

7.4 服务纪律要求

电子认证服务机构提供电子认证服务，应有严格的纪律要求，应至少满足以下要求：

a） 电子认证服务机构业务办理人员须严格依据 CPS 流程对证书订户身份进行鉴证，确保订户身份的可靠性和证书申请行为的真实性；

b） 电子认证服务机构应设定专用服务投诉电话，严格记录投诉原因、内容和处理结果，并备案归档；

c） 电子认证服务机构从业人员应遵守国家的保密法规，尊重客户的保密要求，不对外泄露客户提交的资料；

d） 当客户的认证要求与政策、法律、法规相悖时，应向客户耐心解释，争取客户理解，做到有理有节。遇有客户提出不合理要求时，应向客户委婉说明，不得盲从客户，更不应与客户发生争吵；

e） 电子认证服务机构客户服务人员应对客户的咨询、业务办理、投诉等，要及时、耐心、准确地给予解答。

7.5 业务连续性要求

7.5.1 系统可用性要求

系统高可用性是指以容错和防错的基础设施支持持续的应用处理。应至少满足以下要求：

a) 明确信息发布的时间和频率；
b) 明确对发布信息的访问控制，包括 CP、CPS、证书、OCSP 和 CRL；
c) 明确受理并处理证书申请的时间期限；
d) 明确证书订户的证书撤销和挂起的宽限期；
e) 明确处理撤销请求的时间；
f) 明确 CRL 发布频率；
g) 明确产生 CRL 并将其发布到证书库的最大延迟；
h) 明确证书挂起的最长时间。

7.5.2 业务持续运作要求

业务持续运作是指开展电子认证业务的人员培训、数据日常备份、系统维护、审计等内容的持续服务要求。应至少满足以下要求：

a) 明确人员在完成原始培训后的再培训周期和过程；
b) 明确不同岗位的工作轮换周期和顺序；
c) 明确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；
d) 明确审计日志保存期；
e) 明确档案保存期。

7.5.3 系统灾难恢复要求

系统灾难恢复是指通过可靠的系统恢复和数据保护应对灾难发生，如防止计划外停机。应至少满足以下要求：

a) 明确灾难事件的定义和划分；
b) 制定不同等级的灾难事件预案；
c) 如果异步数据备份，明确数据备份时间周期；
d) 明确不同灾难事件情况下系统恢复最长时间。

8 电子认证服务质量分级

8.1 服务质量评价指标体系

8.1.1 综述

服务质量基于服务流程进行综合评价。参考以下电子认证服务的 6 个流程：业务咨询服务、业务办理服务、技术支持服务、售后服务、司法支持服务和服务保障，其中，业务咨询服务、业务办理服务、技术支持服务、售后服务和司法支持服务属于业务服务指标。依据电子认证服务要求，划分为 6 个一级指标、13 个二级指标，如表 1 所示。

表 1　服务质量分级评价指标

总指标	一级指标	二级指标
电子认证服务质量总指标	业务咨询服务质量指标	
	业务办理服务质量指标	电子认证服务信息公示指标
		业务办理事项告知指标
		业务办理周期指标
		数字证书有效性服务指标
		鉴证质量指标
	技术支持服务质量指标	
	售后服务质量指标	客户投诉指标
		客户回访指标
		客户纠纷指标
		客户满意度指标
	司法支持服务质量指标	
	服务保障质量指标	服务态度指标
		服务设施指标
		服务纪律指标
		业务连续性保障指标

6 个一级指标及 13 个二级指标共 19 个指标按照 0 分(差)、1 分(一般)、3 分(良)、5 分(优)进行不同服务质量的定义和衡量。分值高的一级需在满足上一级分值要求的基础上,满足本分值要求。

8.1.2　业务咨询服务质量指标

业务咨询服务是指向用户提供电子认证服务业务介绍、业务办理流程、证书应用和电子认证服务相关法律法规的解读。该指标直接反映了认证机构对客户证书应用的负责态度。业务咨询服务质量指标评价如表 2 所示。

表 2　业务咨询服务质量指标评价

序号	业务咨询服务质量指标主要内容	分值
1	1)　能够提供业务咨询服务的基本内容,包括业务介绍、业务办理流程、证书应用和电子认证服务相关法律法规解读	1 分
2	1)　能够提供业务咨询服务的全部内容; 2)　有规范的文档化管理; 3)　具有一定的方案咨询能力; 4)　具备专门的咨询团队,具备 3 年以上从业的咨询人员	3 分
3	1)　能提供与证书应用相关的解决方案咨询服务; 2)　能够提供部署 CA 的运营管理咨询服务; 3)　能够提供证书应用的法律风险分析咨询服务; 4)　具备文档化的业务咨询流程和内容管理; 5)　具备专门的具有 3 年以上从业经历的 3 人以上的咨询团队	5 分

8.1.3 业务办理服务质量指标

8.1.3.1 电子认证服务信息公示指标

该指标依据《电子签名法》《电子认证服务管理办法》等法律法规要求，对需要公示的信息进行指标化。

需要公示的信息有：

a) 机构名称和法定代表人；

b) 机构住所和联系办法；

c) 《电子认证服务许可证》编号；

d) 发证机关和发证日期；

e) 《电子认证服务许可证》有效期的起止时间；

f) 电子认证服务从业机构的投诉受理电话；

g) 电子认证服务监管机构的投诉受理电话。

电子认证服务信息公示指标主要是对公示的信息进行抽查，具体计分如表 3 所示。

表 3 电子认证服务信息公示指标

序号	电子认证服务信息公示指标主要内容	分值
1	信息公示缺 1 项以上	1 分
2	信息公示不全面，缺 1 项	3 分
3	在互联网上信息公示全面，无遗漏	5 分

8.1.3.2 业务办理事项告知指标

证书业务办理事项告知服务是指客户在申请证书过程中获取到的相关告知事项，包括密钥对产生、加密密钥管理、证书应用范围、法律责任等 CPS 规定的需要告知事项。

业务办理过程中主要的告知事项有：

a) 数字证书和电子签名的使用条件；

b) 服务收费的项目和标准；

c) 保存和使用证书持有人信息的权限和责任；

d) 电子认证服务机构的责任范围；

e) 证书持有人的责任范围；

f) 其他需要事先告知的事项。

业务办理事项告知指标是通过对客户的抽查统计而得，公式如下：

业务办理事项告知不全率＝没告知或告知不全的抽样调查客户/总抽样调查客户×100%；

业务办理事项告知指标评价如表 4 所示。

表 4 业务办理事项告知指标评价表

序号	业务办理事项告知指标主要内容	分值
1	业务办理事项告知不全率 ＞10%	1 分
2	5%＜业务办理事项告知不全率≤10%	3 分
3	其他	5 分

8.1.3.3 业务办理周期指标

业务办理周期是指接收到客户的申请材料工作日起，发送客户申请的数字证书工作日止。客观上反映了业务办理的服务效率。

业务办理周期指标评价如表 5 所示。

表 5 业务办理周期指标评价

序号	业务办理周期指标主要内容	分值
1	其他	1 分
2	≤7 个工作日	3 分
3	≤3 个工作日	5 分

8.1.3.4 数字证书有效性服务指标

数字证书的有效性对数字证书的安全使用影响重大，其有效性查验服务指标反映了 CRL 的更新频率、OCSP 服务水平等。

数字证书有效性服务指标评价如表 6 所示。

表 6 业务办理周期指标评价

序号	数字证书有效性服务指标主要内容	分值
1	能够向客户提供数字证书有效性验证服务； 能够遵循 CPS 对 CRL 进行定期更新； 在网站上提供明显的下载提示	1 分
2	能够提供在线、离线的证书有效性查验服务	3 分
3	能够提供基于用户需求的定制的数字证书有效性查验服务，如：接口、插件、软件等	5 分

8.1.3.5 鉴证服务质量指标

鉴证服务质量是电子认证服务的关键环节，其质量确保了数字证书的安全使用。

鉴证服务质量指标评价如表 7 所示。

表 7 鉴证服务质量指标评价

序号	鉴证服务质量指标主要内容	分值
1	能够对客户提交的申请材料的真实性进行鉴别； 能够对客户的身份与提交的材料关联关系进行验证	1 分
2	有文档化的鉴证流程定义和管理； 有规范化的处理流程； 能够遵守安全规定对申请材料进行管理	3 分
3	鉴证服务时间不超过 1 个工作日	5 分

8.1.4 技术支持服务质量指标

技术支持服务质量主要体现在问题解答和故障排除服务质量上。技术支持服务质量指标是通过对一般事件、严重事件、重大事件的应对来评价衡量的。

技术支持服务质量指标评价如表 8 所示。

表 8 技术支持服务质量指标评价

序号	技术支持服务质量指标主要内容	分值
1	能够提供与证书业务相关的技术支持，确保客户证书使用	1 分
2	对提供的技术支持服务有明确的一般事件、严重事件、重大事件的详细定义和分类； 能够在不影响客户业务情况下完成对一般事件、严重事件、重大事件的响应和处理； 对事件的响应处理遵循规划化的处理流程	3 分
3	一般事件处理不超过 1 天； 严重事件处理不超过 1 周； 重大事件处理不影响客户业务； 各种事件的处理文档化、规划化，有可以遵循的处理流程和机制； 事件处理整个过程被记录，可以查阅和审计	5 分

8.1.5 售后服务质量指标

8.1.5.1 客户投诉指标

客户对接受的电子认证服务不满意，可以向主管部门投诉电子认证服务机构。

客户投诉指标评价如表 9 所示。

表 9 客户投诉指标评价

序号	客户投诉指标主要内容	分值
1	一年内发生 3 次或 3 次以上的投诉举报事件	0 分
2	一年内发生投诉举报事件少于 3 次，且处理周期不超过 5 个工作日	1 分
3	一年内发生 1 次投诉举报事件，且处理周期不超过 3 个工作日	3 分
4	一年内无客户投诉事件发生	5 分

8.1.5.2 客户回访指标

客户回访是售后服务的重要环节，由于数字证书的特殊性，在提供电子认证服务时，客户回访将是电子认证服务质量的重要因素。

客户回访指标评价如表 10 所示。

表 10　客户回访指标评价

序号	客户回访指标主要内容	分值
1	有专门的人员进行客户回访和接收客户的回访； 对回访有记录、有备案	1 分
2	有文档化的客户回访计划、流程和机制； 有规范化的客户回访记录； 有专门的人员进行回访和接收客户的回访； 客户回访率占到总客户的 50%以上	3 分
3	对客户回访有规范化的管理，可审计、可追踪； 客户回访率占到总客户的 80%以上	5 分

8.1.5.3　客户纠纷指标

电子认证服务机构与客户发生纠纷时，应依据 CPS 承诺的方式、内容进行解决。

客户纠纷指标评价如表 11 所示。

表 11　客户纠纷指标评价

序号	客户纠纷指标主要内容	分值
1	一年内发生 3 次或 3 次以上的纠纷事件，且处理周期不超过 5 个工作日	1 分
2	一年内发生 1～2 次纠纷举报事件，且处理周期不超过 3 个工作日	3 分
3	一年内无客户纠纷事件发生	5 分

8.1.5.4　客户满意度指标

对客户进行随机抽查，对电子认证服务的总体满意程度评价。该指标反映了客户的直观感受。

客户满意度指标评价如表 12 所示。

表 12　客户满意度指标评价

序号	客户满意度指标主要内容	分值
1	差	0 分
2	一般	1 分
3	良	3 分
4	好	5 分

8.1.6　司法支持服务指标

司法支持服务质量指标是通过对司法支持服务办理周期来评价衡量的。

司法支持服务质量指标评价如表 13 所示。

表 13　司法支持服务指标

序号	司法支持服务质量指标主要内容	分值
1	能够为证书订户提供司法支持服务	1 分
2	对提供的司法支持服务有详细定义和分类； 能够及时受理客户的取证申请； 对客户的取证申请处理遵循规范化的处理流程	3 分
3	处理周期不超过 10 个工作日； 取证过程文档化、规范化，有可以遵循的处理流程和机制； 取证整个过程被记录，可以查阅和审计	5 分

8.1.7　服务保障质量指标

8.1.7.1　服务态度指标

对提供电子认证服务人员进行抽查，对接收服务的客户进行抽样统计。该指标包括规范的服务用语、服务礼貌等服务态度。

服务态度指标评价如表 14 所示。

表 14　服务态度指标评价

序号	服务态度指标主要内容	分值
1	存在对服务态度的投诉事件 1 次以上	0 分
2	存在对服务态度的投诉事件 1 次，但能够很好地解决，使客户基本满意	1 分
3	能够处理当客户的认证要求与政策、法律、法规相悖时，向客户耐心解释，争取客户理解，做到有理有节，遇有客户提出不合理要求时，能够向客户委婉说明，无与客户发生争吵现象； 能够对客户的咨询、业务办理、投诉等及时、耐心、准确地解答； 机构内部有明确的服务态度规范和相关培训	3 分
4	服务态度热情，得到服务客户的表扬； 有定期的客户服务培训计划； 机构内部有完整系统的客户服务审计抽查机制	5 分

8.1.7.2　服务设施指标

服务设施指标反映了机构提供客户服务的基础保障。

服务设施指标评价如表 15 所示。

表 15　服务设施指标评价

序号	服务设施指标主要内容	分值
1	具有独立的商业办公服务场所； 场所面积满足提供认证服务需要； 具备提供服务的局域网和互联网络接入； 具备独立物理机房； 具备接收服务的电话呼叫中心和网站设备	1 分
2	有国内信息安全检测机构的检测报告，无安全隐患	3 分
3	经过国内高等级的信息安全认证，系统安全可靠性高	5 分

8.1.7.3　业务连续性保障指标

业务连续性保障指标评价如表 16 所示。

表 16　业务连续性保障指标评价

序号	业务连续性保障指标主要内容	分值
1	能够提供持续的服务，无影响客户业务的情况发生； 制定了灾备方案； 灾后恢复之间不超过 72 h； 能够定期进行数据备份	1 分
2	制定了业务连续性计划； 灾后恢复时间不超过 36 h； 能够在不影响客户业务情况下进行业务连续性保障	3 分
3	能够对灾难事件进行明确的定义和划分； 制定了不同等级的灾难事件预案且灾后恢复之间不超过 24 h； 能够提供 7×24 h 的在线服务能力	5 分

8.1.7.4　服务纪律指标

服务纪律指标评价如表 17 所示。

表 17　服务纪律指标

序号	服务纪律指标主要内容	分值
1	未按照 CPS 规则对证书订户身份进行鉴证或泄露客户的资料	0 分
2	基本按照 CPS 规则对证书订户进行身份鉴证，无对外泄露客户的资料的情况发生	1 分
3	严格按照 CPS 规则对证书订户身份进行鉴证； 对客户的资料严格保密； 设定专用投诉电话，并将处理过程的资料备案归档	3 分
4	无与客户发生争吵的行为； 对客户的咨询、投诉等，能够及时、耐心、准确地给予解答	5 分

8.2 服务质量评价指标权重

指标体系中包括多级多项指标，为了保证量化分析和评价测定的可信度，有必要对不同指标赋予不同的权重。

指标权重表如表 18 所示。

表 18 指标权重

总指标	一级指标及权重	二级指标及权重
电子认证服务质量总指标	业务咨询服务质量指标（0.1）	
	业务办理服务质量指标（0.4）	电子认证服务信息公示指标（0.1）
		业务办理事项告知指标（0.2）
		业务办理周期指标（0.1）
		数字证书有效性服务指标（0.3）
		鉴证服务质量指标（0.3）
	技术支持服务质量指标（0.2）	
	售后服务质量指标（0.1）	客户投诉指标（0.4）
		客户回访指标（0.2）
		客户满意度指标（0.4）
	司法支持服务质量指标（0.1）	
	服务保障质量指标（0.1）	服务态度指标（0.1）
		服务设施指标（0.3）
		业务连续性保障指标（0.4）
		服务纪律指标（0.2）

8.3 服务质量评价方法

在本标准中，将定义服务质量的指标评价体系（分为两级：一级指标、二级指标，见 8.1），并针对每一指标给出总体评价值中的权重（见 8.2），服务质量的评价值满分为 5 分，计算公式为：

服务质量＝ Σ（指标分值×权重）

8.4 服务质量综合评价等级

8.4.1 综述

通过电子认证服务质量总指标，反映电子认证服务机构的总体服务质量状况。

根据电子认证服务质量，将提供电子认证服务的认证机构划分为 3 个级别：基本执行级（Ⅰ级）、计划跟踪级（Ⅱ级）、优化控制级（Ⅲ级）。

有重大安全事故、重大安全隐患或违背提供电子认证服务相关法律法规的电子认证服务机构不适合该服务质量综合评价与分级。

8.4.2 基本执行级(Ⅰ级)

基本执行级是电子认证服务的基本级别。电子认证服务质量总指标值在3.5以下。

该级别的电子认证服务机构建立了符合国家规定的最低服务质量管理体系和服务体系,建立了专门的服务部门,设置了完备的工作岗位,配备了具有一定服务水平的服务人员,能够提供包括业务办理服务、一般的技术支持服务和售后服务等服务内容,并能够按照服务规范执行服务纪律、密钥与证书管理、服务信息披露、服务信息管理、服务安全管理和业务连续性计划等。

8.4.3 计划跟踪级(Ⅱ级)

计划跟踪级是电子认证服务的普通级别,满足所有并不限于基本执行级要求。电子认证服务质量总指标值在3.5以上4.5以下。

该级别的电子认证服务机构建立了比较完整的质量管理体系和服务体系,能够针对电子认证服务制定详细的服务计划并执行,对服务整个流程具有完整的记录,可追踪、可审计,具备完善的文档化流程管理特点和过程执行审计特点。在基本执行级(Ⅰ级)的服务基础上,还应该根据客户需要提供专门的业务咨询服务,同时还能够执行快速的业务连续性计划,不影响客户业务服务。

8.4.4 优化控制级(Ⅲ级)

优化控制级是电子认证服务的最高级别,满足所有但不限于计划跟踪级要求。电子认证服务质量总指标值在4.5以上。

在计划跟踪级(Ⅱ级)基础上,该级别的电子认证服务机构建立了完整的可以指标量化的服务控制管理体系和服务体系,能针对客户不同需求提供定制服务和开发服务,提供满足客户不同层次安全需求的安全解决方案和集成应用产品,且整个服务过程按照规范流程进行,可审计,可追踪,能进行服务质量的综合管理和风险预警。

参 考 文 献

[1] 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
[2] GB/T 19714—2005 信息技术安全技术 公钥基础设施证书管理协议
[3] GB/T 19771—2005 信息技术安全技术 公钥基础设施 PKI 组件最小互操作规范
[4] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[5] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[6] GB/T 20518—2006 信息安全技术 公钥基础设施数字证书格式
[7] GB/T 20984—2007 信息安全技术 信息安全风险评价规范
[8] GB/Z 20985—2007 信息技术安全技术 信息安全事件管理指南
[9] GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南
[10] GB/Z 20988—2007 信息安全技术 信息系统灾难恢复规范
[11] GB/T 21053—2007 信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求
[12] GB/T 21054—2007 信息安全技术 公钥基础设施 PKI 系统安全等级保护评价准则
[13] GB/T 28447—2012 信息安全技术 电子认证服务机构运营管理规范
[14] 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
[15] 电子认证服务管理办法(工业和信息化部令第 29 号)
[16] 中华人民共和国电子签名法(中华人民共和国主席令第 18 号)
[17] 电子政务电子认证服务业务规则(国家密码管理局 局字 488,2010 年)
[18] 电子政务电子认证服务质量评价要求(国家密码管理局 局字 489,2010 年)