子认证体系建设的相关要求。

（3）具有符合《卫生系统电子认证服务规范》、《卫生系统数字证书格式规范》、《卫生系统数字证书介质技术规范》、《卫生系统数字证书应用集成规范》和《卫生系统数字证书服务管理平台接入规范》等的电子认证服务体系。

（4）符合法律、行政法规规定的其他条件。

2．电子认证服务机构需满足业务运营的业务需求

（1）认证业务方面

应包括两类业务服务：用户证书服务和用户证书密钥服务。用户证书服务主要包括：证书申请与审核、证书签发、证书存储与发布、证书更新、证书撤销、证书冻结、证书状态查询、证书归档等。用户证书密钥服务主要包括：用户证书密钥的产生/传递/存储、用户证书私钥激活数据的产生/传递/存储、用户证书私钥恢复、用户证书密钥对的更新、用户证书私钥的归档和销毁等。

为保证认证业务的安全性，应加强业务流程的管控，严格制定各种业务流程或策略，主要包括证书申请审核流程和规范、证书更新的自动审核策略、证书撤销管理策略和流程、证书冻结策略和流程、证书状态查询服务策略、证书归档策略、用户证书密钥和私钥激活数据的传递策略、用户证书私钥恢复的管理规定和流程、用户证书私钥归档/销毁流程等。

（2）认证系统方面

认证系统功能方面，应符合 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）中的要求，能够提供用户证书的申请、签发、存储、发布、更新、撤销、冻结、状态查询、归档以及用户证书密钥管理等功能。

认证系统运行方面，应保证各层面的技术和管理安全性，主要包括：网络系统安全、主机系统安全、系统冗余与备份、系统运营维护安全管理、密码设备安全管理、CA 密钥和证书管理等。其中，系统冗余包括：网络链路冗余、主机冗余、电源冗余与后备发电等。系统备份包括：软件与数据备份、硬件设备备份等。系统运营维护安全管理包括：系统权限管理、系统操作管理、系统变更和升级、账户与口令管理、系统安全监控等。密码设备安全管理包括：认证系统密码设备管理、用户密码设备管理等。CA 密钥和证书管理包括：CA 密钥的生成和存储、CA 私钥激活数据的管理、CA 密钥的使用、CA 密钥的备份与恢复、CA 密钥的销毁、CA 证书的创建和发布、CA 证书的更新、CA 证书的撤销、CA 密钥和证书的归档等。

（3）物理环境与设施方面。

主要包括：运营场地、运营区域划分及要求、安全监控系统、环境保护与控制设施、支撑设备、场地访问安全管理、场地监控安全管理、注册机构场地安全等。

其中，运营区域分为：公共区（控制区）、服务区（限制区）、管理区（敏感区）、核心区（机密区）等。安全监控系统包括：门禁、入侵检测、监控录像等。环境保护与控制设施包括：空气和温湿度控制、防雷击和接地、静电防护、水患防治、消防设施等。支撑设备包括：供配电系统、照明等。

（4）组织与人员管理方面。

主要包括：职能与角色设置、安全组织、人员安全管理等。

其中，职能与角色设置中，必要的职能部门包括：安全策略管理部门、安全管理部门、

运营管理部门、人事管理部门、认证服务部门、技术服务部门等；必要的岗位角色包括：安全策略管理组织负责人、安全管理人员、密钥管理员、系统维护员、鉴别与验证员、客户档案管理员、客户服务员、审计员、人事经理等。人员安全管理包括：人员安全策略、可信背景调查、人员可信保障、人员异动处理等。

（5）文档、记录与介质管理方面。

主要包括：文档管理、记录管理、介质管理等。

其中，文档管理包括：文档归类、注册机构的文档、人员与制度、文档保存、使用控制、文档销毁等。介质管理包括：保管、使用、销毁等。

文档可分为以下几类：企业管理类、安全策略类、运营管理类、客户类。记录可分为以下几类：物理场地与设施日常管理记录、安全监控记录、密码设备管理记录、密码设备操作使用记录、CA 证书和密钥维护记录、认证系统运行日志、运营网络安全监测记录、认证系统操作日志、认证服务记录等。

（6）业务连续性方面。

主要包括：业务连续性计划、应急处理预案、灾难恢复计划、灾备中心等。

（7）审计与改进方面。

审计包括：系统审计、运营审计、注册机构审计等。系统审计的目的是发现电子认证服务机构业务系统运行和操作中存在的风险和问题，并依此采取相应的措施和手段，防止安全事故的发生，杜绝问题再次发生。运营审计是为了检查、确认电子认证服务机构是否按照其电子认证业务规则、业务规范、管理制度和安全策略开展业务，发现存在的问题。注册机构审计内容主要包括法律法规符合性、安全运营管理、风险管理等，检查其是否严格按照相关的安全策略及运营管理规范开展业务活动。

在审计时发现与安全要求不相符的事项，应按照相应的调整策略和规程进行适当调整，必要时对调整后的事项进行评估，然后实施调整后的事项。

2.6　PKI/法规与标准

PKI 体系涉及密码技术、电子签名、电子认证、IC 卡技术、Java 技术等，须遵循相应的法规与标准。

2.6.1　国内法规

1．商用密码相关的政策法规

（1）商用密码管理条例，1999 年

（2）商用密码科研管理规定，2005 年

（3）商用密码产品生产管理规定，2005 年

（4）商用密码产品销售管理规定，2005 年

（5）商用密码产品使用管理规定，2007 年

（6）境外组织和个人在华使用密码产品管理办法，2007 年

（7）密码产品和含有密码技术的设备进口管理目录，2009 年和 2014 年

2. 电子签名与认证服务相关的政策法规

（1）电子签名法，2004 年
（2）电子认证服务管理办法，2005 年和 2009 年
（3）电子认证服务密码管理办法，2005 年和 2009 年
（4）电子政务电子认证服务管理办法，2009 年
（5）卫生系统电子认证服务管理办法，2009 年
（6）电子招标投标办法，2013 年
（7）非金融机构支付服务业务系统检测认证管理规定，2011 年
（8）电子银行业务管理办法，2006 年
（9）关于落实“两个减负”优化纳税服务工作的意见，2007 年

2.6.2 国内标准

1. 通用性标准

（1）GM/T 0001-2012《祖冲之序列密码算法》
（2）GM/T 0002-2012《SM4 分组密码算法》（原 SMS4 分组密码算法）
（3）GM/T 0003-2012《SM2 椭圆曲线公钥密码算法》
（4）GM/T 0004-2012《SM3 密码杂凑算法》
（5）GM/T 0005-2012《随机性检测规范》
（6）GM/T 0006-2012《密码应用标识规范》
（7）GM/T 0008-2012《安全芯片密码检测准则》
（8）GM/T 0009-2012《SM2 密码算法使用规范》
（9）GM/T 0010-2012《SM2 密码算法加密签名消息语法规范》
（10）GM/T 0011-2012《可信计算 可信密码支撑平台功能与接口规范》
（11）GM/T 0012-2012《可信计算 可信密码模块接口规范》
（12）GM/T 0013-2012《可信计算 可信密码模块符合性检测规范》
（13）GM/T 0014-2012《数字证书认证系统密码协议规范》
（14）GM/T 0015-2012《基于 SM2 密码算法的数字证书格式规范》
（15）GM/T 0016-2012《智能密码钥匙密码应用接口规范》
（16）GM/T 0017-2012《智能密码钥匙密码应用接口数据格式规范》
（17）GM/T 0018-2012《密码设备应用接口规范》
（18）GM/T 0019-2012《通用密码服务接口规范》
（19）GM/T 0020-2012《证书应用综合服务接口规范》
（20）GM/T 0021-2012《动态口令密码应用技术规范》
（21）GM/T 0022-2014《IPSec VPN 技术规范》
（22）GM/T 0023-2014《IPSec VPN 网关产品规范》
（23）GM/T 0024-2014《SSL VPN 技术规范》
（24）GM/T 0025-2014《SSL VPN 网关产品规范》
（25）GM/T 0026-2014《安全认证网关产品规范》
（26）GM/T 0027-2014《智能密码钥匙技术规范》

（27）GM/T 0028-2014《密码模块安全技术要求》
（28）GM/T 0029-2014《签名验签服务器技术规范》
（29）GM/T 0030-2014《服务器密码机技术规范》
（30）GM/T 0031-2014《安全电子签章密码技术规范》
（31）GM/T 0032-2014《基于角色的授权管理与访问控制技术规范》
（32）GM/T 0033-2014《时间戳接口规范》
（33）GM/T 0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》
（34）GM/T 0035-2014《射频识别系统密码应用技术要求》
（35）GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》
（36）GM/T 0037-2014《证书认证系统检测规范》
（37）GM/T 0038-2014《证书认证密钥管理系统检测规范》
（38）GM/Z 0001-2013《密码术语》
（39）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》
（40）GB/T 28447-2012《信息安全技术 电子认证服务机构运营管理规范》

2．行业性标准

（1）《卫生系统电子认证服务规范（试行）》，2010 年
（2）《卫生系统数字证书应用集成规范（试行）》，2010 年
（3）《卫生系统数字证书格式规范（试行）》，2010 年
（4）《卫生系统数字证书介质技术规范（试行）》，2010 年
（5）《卫生系统数字证书服务管理平台接入规范（试行）》，2010 年
（6）JR/T 0068-2012《网上银行系统信息安全通用规范》
（7）《电子招标投标系统技术规范 第 1 部分 交易平台技术规范》，2013 年
（8）《中国人民银行信息系统电子认证应用指引》，2011 年
（9）《非金融机构支付业务设施技术要求 V3》，2013 年

2.6.3　国际标准

1．PKCS 系列标准

PKCS 是公钥密码标准（Public Key Cryptography Standards）的缩写，它是由美国 RSA 实验室与遍布全球的安全系统开发者一起合作制定的一组规范，以推动公钥密码的发展。最早发布的 PKCS 文档是早期一群公钥技术使用者在 1991 年召开的一次会议上的成果，目前 PKCS 规范已被广泛引用和实施，部分 PKCS 规范已经成为多个国际组织正式或事实上的标准，如 ANSI X9 文档系列、PKIX、SET、S/MIME、SSL 等。PKCS 系列主要包括以下标准：

PKCS #1：RSA Cryptography Standard（RSA 密码标准）。
PKCS #2：已并入 PKCS #1，不存在。
PKCS #3：Diffie-Hellman Key Agreement Standard（DH 密钥协商标准）。
PKCS #4：已并入 PKCS #1，不存在。
PKCS #5：Password-Based Cryptography Standard（基于口令的密码标准）。

PKCS #6：Extended-Certificate Syntax Standard（扩展的证书语法标准）。

PKCS #7：Cryptographic Message Syntax Standard（密码消息语法标准）。

PKCS #8：Private-Key Information Syntax Standard（私钥信息语法标准）。

PKCS #9：Selected Attribute Types（可供选择的属性类型）。

PKCS #10：Certification Request Syntax Standard（证书请求语法标准）。

PKCS #11：Cryptographic Token Interface Standard（密码 Token 接口标准）。

PKCS #12：Personal Information Exchange Syntax Standard（个人信息交换语法标准）。

PKCS #13：Elliptic Curve Cryptography Standard（椭圆曲线密码标准），正在制定中。

PKCS #14：Pseudo-random Number Generation（伪随机数生成算法 PRNG），正在制定中。

PKCS #15：Cryptographic Token Information Format Standard（密码 Token 信息格式标准）。

2. ISO/IEC 7816 系列标准

ISO/IEC 7816 系列标准规定了 IC 卡（Integrated Circuit Cards）相关技术标准，由 ISO（International Organization for Standardization）和 IEC（International Electrotechnical Commission）组织共同维护，目前包括 14 个部分。

ISO 7816-1：Physical characteristics（卡的物理特性）。

ISO 7816-2：Cards with contacts：Dimensions and location of the contacts（触点集成电路卡：触点的尺寸与位置）。

ISO 7816-3：Cards with contacts：Electrical interface and transmission protocols（触点集成电路卡：电信号和传输协议）。

ISO 7816-4：Organization, security and commands for interchange（用于交换的结构、安全和命令）。

ISO 7816-5：Registration of application providers（卡应用提供者注册）。

ISO 7816-6：Interindustry data elements for interchange（行业间数据元）。

ISO 7816-7：Interindustry commands for Structured Card Query Language (SCQL)（用于结构化卡查询语言（SCQL）的行业间命令）。

ISO 7816-8：Commands for security operations（与安全相关的行业间命令）。

ISO 7816-9：Commands for card management（用于卡管理的命令）。

ISO 7816-10：Electronic signals and answer to reset for synchronous cards（同步卡的电信号和复位应答）。

ISO 7816-11：Personal verification through biometric methods（通过生物识别方法的个人验证）。

ISO 7816-12：Cards with contacts：USB electrical interface and operating procedures（带触点集成电路卡：USB 电气接口及操作规程）。

ISO 7816-13：Commands for application management in multi-application environment（在多应用环境中用于应用管理的命令）。

ISO 7816-15：Cryptographic information application（密码信息应用）。

3. IETF PKIX 系列标准

在 IETF（Internet Engineering Task Force）内有 PKIX（Public-Key Infrastructure (X.509)）