系统机房布局和物理连线等资料性附录，供国内 PKI 厂商和运营商参考。

28.1.20 证书认证系统密码及其相关安全技术规范（GB/T 25056）

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》

本标准适用于在中华人民共和国境内建设并正式运行的、为公众服务的数字证书认证系统的设计、建设、检测、运行及管理，为实现数字证书认证系统的互联互通和交叉认证提供统一的依据，指导数字证书认证系统的建设和检测评估，规范数字证书认证系统中密码及相关安全技术的应用。其他数字证书认证系统的建设、运行及管理，可参照本标准。

本标准主要由范围、规范性引用文件、术语和缩略语、证书认证系统、密钥管理系统、密钥算法/密码设备及接口、协议、证书认证中心建设、密钥管理中心建设、证书认证中心运行管理要求、密钥管理中心运行管理要求、检测等 12 章内容和附录 A（资料性附录）KMC 与 CA 之间的消息格式、附录 B（资料性附录）安全通信协议、附录 C（资料性附录）密码设备接口函数定义及说明、附录 D（资料性附录）证书认证系统网络结构图、附录 E（资料性附录）证书申请和下载格式等组成。

其中，证书认证系统由功能描述、系统设计、数字证书、证书注销列表等 4 节内容组成。密钥管理系统由功能描述、系统设计、KMC 与 CA 的安全通信协议等 3 节内容组成。密码算法/密码设备及接口由密码算法、密码设备、密码服务接口等 3 节内容组成。协议由证书管理协议、证书验证协议、安全通信协议等 3 节内容组成。证书认证中心建设由系统、安全、数据备份、可靠性、物理安全、人事管理制度等 6 节内容组成。密钥管理中心建设由系统、安全、数据备份、可靠性、物理安全、人事管理制度等 6 节内容组成。证书认证中心运行管理要求由人员管理要求、CA 业务运行管理要求、密钥分管要求、安全管理要求、安全审计要求、文档的配备等 6 节内容组成。密钥管理中心运行管理要求由人员管理要求、运行管理要求、密钥分管、安全管理、安全审计、文档配备等 6 节内容组成。检测由系统初始化、用户注册管理系统、证书/证书注销列表生成与签发系统、证书/证书注销列表存储与发布系统、证书状态查询系统、安全审计系统、密钥管理系统检测、系统安全性检测、其他安全产品和系统等 9 节内容组成。附录 A 由概述、协议等 2 节内容组成。附录 B 由符号说明、身份认证、密钥交换、安全通信协议等 4 节内容组成。附录 C 由应用类密码设备接口函数、证书载体接口函数等 2 节内容组成。附录 D 由当 RA 采用 C/S 模式时 CA 的网络接口、当 RA 采用 B/S 模式时 CA 的网络接口、CA 与远程 RA 的连接、KMC 与多个 CA 的网络连接等 4 节内容组成。附录 E 由证书申请格式、证书下载格式等 2 节内容组成。

28.1.21 电子认证服务机构运营管理规范（GB/T 28447）

GB/T 28447-2012《信息安全技术 电子认证服务机构运营管理规范》

本标准规定了电子认证服务机构在业务运营、认证系统运行、物理环境与设施安全、组织与人员管理、文档、记录、介质管理、业务连续性、审计与改进等多方面应遵循的要求。本标准适用于在开放互联环境中提供数字证书服务的电子认证服务机构的建设、管理及评估。对于在封闭环境中（如在特定团体或某个行业内）运行的电子认证服务机构可根据自身安全风险评估以及国家有关的法律法规有选择性地参考本标准。国家有关的测评机

构、监管部门也可以将本标准作为测评和监管的依据。

本标准主要由范围、规范性引用文件、术语和定义、缩略语、电子认证服务机构运营的业务、业务运营中的风险、认证系统运行要求、物理环境与设施、组织与人员管理、文档/记录与介质管理、业务连续性要求、审计与改进等 12 章内容和附录 A（资料性附录）业务运营风险举例等组成。

其中，电子认证服务机构运营的业务由用户证书服务、用户证书密钥服务、认证系统功能要求、认证业务流程要求等 4 节内容组成。认证系统运行要求由网络系统安全、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 6 节内容组成。物理环境与设施由运营场地、运营区域划分及要求、安全监控系统、环境保护与控制设施、支撑设施、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 8 节内容组成。组织与人员管理由职能与角色设置、安全组织、人员安全管理等 3 节内容组成。业务连续性要求由业务连续性计划、应急处理预案、灾难恢复计划、灾备中心等 4 节内容组成。

28.2 行业性标准

28.2.1 卫生系统电子认证服务规范

《卫生系统电子认证服务规范》（试行），2010 年 4 月

本规范依据《卫生系统电子认证服务管理办法（试行）》，定义了参与卫生系统电子认证服务体系建设的管理方、使用方和提供方开展电子认证服务的工作机制，描述了卫生系统电子认证服务的总体要求，规范了电子认证服务机构需要遵循的证书业务服务和证书支持服务的要求，提出了服务的保障要求。本规范适用于卫生系统电子认证服务体系建设的管理方、使用方和提供方。

本规范共包括 5 章正文和 1 个附录：第 1 章“范围”；第 2 章“服务总体要求”；第 3 章“证书业务服务”；第 4 章“技术支持服务”；第 5 章“服务的保障”；附录（资料性）“名词解释”。

其中，第 2 章包括证书分类、证书产品、服务模式、服务内容、平台接入等要求。卫生系统数字证书共分 6 类：内部机构证书、内部工作人员证书、内部设备证书、外部机构证书、外部个人证书、外部设备证书。电子认证服务机构交付给卫生系统用户的证书产品应包括：证书介质、证书初始保护口令、证书使用说明书以及证书管理工具等。证书服务模式包括 3 类：集中服务模式、多级服务模式、认证机构直接服务模式。电子认证服务机构提供的服务包括证书业务服务和技术支持服务两部分内容。其中，证书业务服务是指电子认证服务机构为卫生系统用户提供的证书申请、发放、更新、吊销、解锁、密钥恢复、证书查询等证书业务办理服务；技术支持服务是指电子认证服务机构在用户使用证书过程中提供的各种方式的咨询、培训、应急等服务内容。电子认证服务机构在卫生系统开展服务前，须接入卫生部数字证书服务管理平台，遵循卫生系统数字证书服务管理平台的数据同步接口要求，实现数字证书和黑名单的同步。

第 3 章规定了电子认证服务机构应为卫生系统用户提供的多种证书业务服务，包括证

书申请、证书发放、证书更新、证书吊销、证书解锁、密钥恢复和证书查询等。

第4章规定了电子认证服务机构应向卫生系统用户通过热线电话、网站、现场等服务方式，提供使用帮助、应用咨询培训、应急保障和应用集成支持等一系列技术支持服务。

第5章规定了电子认证服务机构的组织保障、制度保障、安全保障等要求。

28.2.2 卫生系统数字证书应用集成规范

《卫生系统数字证书应用集成规范》（试行），2010年4月

本规范依据《卫生系统电子认证服务管理办法（试行）》，参照国家密码管理局“公钥密码基础设施应用技术体系”系列技术规范，结合卫生系统业务特点，提出卫生系统数字证书应用集成目标、集成要求、集成内容，定义统一的证书应用接口，并提供证书应用接口的典型部署示例、登录认证流程示例和签名验证流程示例。

本规范用于指导并规范卫生信息系统证书应用集成实施工作，指导电子认证服务机构开发标准统一的证书应用接口，规范卫生信息系统实现基于数字证书的安全登录、数字签名和加密解密等安全功能。

本规范共包括5章正文和2个附录：第1章“范围”；第2章“应用集成目标”；第3章“应用集成要求”；第4章“应用集成内容”；第5章“统一证书应用接口规范”；附录A（资料性）“证书应用接口实施示例”；附录B（资料性）“名词解释”。

其中，第4章，规定了卫生信息系统证书应用集成的5个方面的内容，包括：基于数字证书的身份认证、数字签名和验证、数据加密和解密、时间戳应用、密码设备应用等。

第5章介绍了统一证书应用接口和证书应用综合服务接口，并给出了证书应用综合服务接口的客户端接口函数定义、服务端COM组件函数定义、服务端Java函数定义等。

统一证书应用接口位于应用系统和密码设备之间，包括：证书介质应用接口、密码设备应用接口、通用密码服务接口和证书应用综合服务接口。证书应用综合服务接口是供应用系统直接调用的高级证书应用接口，一般情况下分成客户端接口和服务器端接口两个模块。

客户端接口是供应用系统客户端程序直接调用的高级接口，应支持所有主流操作系统。客户端接口应支持符合《卫生系统数字证书格式规范》的数字证书，支持使用符合《卫生系统数字证书介质技术规范》的证书介质。客户端接口可包括DLL动态库、ActiveX控件、Applet插件等多种产品形态，支持B/S和C/S等架构的应用系统，客户端接口还包括32个主要函数。

服务器端接口是供应用系统服务器端程序直接调用的高级接口，应支持所有主流操作系统，支持B/S和C/S等系统架构，支持符合《卫生系统数字证书格式规范》的数字证书，可通过添加证书信任列表的方式实现不同电子认证服务机构证书之间的交叉认证和互信互认。服务器端接口可包括COM组件、Java组件等多种形态。服务器端接口还包括36个主要函数。

28.2.3 卫生系统数字证书格式规范

《卫生系统数字证书格式规范》（试行），2010年4月

本规范描述了卫生系统电子认证服务体系中使用的数字证书的类型、数字证书和证书撤销列表的格式，制定了各类数字证书及证书撤销列表格式模板，用于指导电子认证服务

机构签发统一格式的数字证书和证书撤销列表，以保障数字证书在卫生系统内各信息系统之间的互信互认。

本规范在 GB/T 20518-2006《信息安全技术　公钥基础设施　数字证书格式》基础上，针对卫生系统的电子认证需求，在证书类型、证书格式模板、实体唯一标识扩展项等方面进行了扩充，以适应卫生系统的业务特点和应用需求。

本规范共包括 5 章正文和 3 个附录：第 1 章“范围”；第 2 章“数字证书类别”；第 3 章“数字证书基本格式”；第 4 章“数字证书模板”；第 5 章“CRL 格式”；附录 A（资料性）“证书主题 DN 命名示例”；附录 B（资料性）“证书格式编码示例”；附录 C（资料性）“名词解释”。

其中，第 2 章根据卫生系统用户特点及应用需求，数字证书按照内部用户和外部用户分成如下 6 类：内部机构证书、内部工作人员证书、内部设备证书、外部机构证书、外部个人证书、外部设备证书。

第 3 章规定了证书格式的基本结构、基本证书域、签名算法域、签名值域、命名规范。

第 4 章规定了 3 种证书模板：个人证书模板、机构证书模板、设备证书模板。

第 5 章规定了 CRL 的基本结构和模板。

28.2.4　卫生系统数字证书介质技术规范

《卫生系统数字证书介质技术规范》（试行），2010 年 4 月

本规范描述了在卫生系统中使用的数字证书介质的各项要求，包括对安全机制、软件要求、硬件技术指标要求等内容，用于指导电子认证服务机构在卫生系统内进行数字证书介质的定制和选型。

本规范共包括 4 章正文和 1 个附录：第 1 章“范围”；第 2 章“安全机制”；第 3 章“软件要求”；第 4 章“硬件技术指标”；附录（资料性）“名词解释”。

其中，第 2 章规定了证书介质初始化、证书介质的安装注册、介质口令管理、扩展区要求、介质类型要求等过程中具体的安全机制要求。

第 3 章规定了证书介质接口、安装程序、卸载程序过程中具体的软件要求。证书介质接口函数应遵守国家密码管理局《智能 IC 卡及智能密码钥匙密码应用接口规范》的函数定义和数据结构定义，提供设备管理、访问控制、文件管理和密码服务等相关密码服务接口。

设备管理主要完成设备的等待、设备插拔、枚举、连接、断开、设置设备标签、获取设备信息、锁定设备、解锁设备操作，并定义了 9 个设备管理类接口函数。

访问控制主要完成设备认证，修改设备认证密钥，校验 PIN，修改 PIN，解锁 PIN 和清除安全状态操作，并定义了 7 个访问控制接口函数。

文件管理函数用以满足用户扩展开发的需要，包括创建文件，删除文件，枚举文件，获取文件信息，文件读写操作，并定义了 6 个文件管理接口函数。

密码服务函数提供对称算法运算、非对称算法运算、杂凑运算、消息鉴别码计算等功能，并定义了 42 个密码服务接口函数。

28.2.5 卫生系统数字证书服务管理平台接入规范

《卫生系统数字证书服务管理平台接入规范》（试行），2010年4月

根据《卫生系统电子认证服务管理办法（试行）》相关要求，电子认证服务机构在开展服务前须接入卫生部数字证书服务管理系统。本规范描述了电子认证服务机构的CA系统（简称CA系统）接入卫生部数字证书服务管理系统的总体要求、CA系统功能要求以及CA系统接入接口要求等。

本规范用于指导相关电子认证服务机构将CA系统接入卫生部数字证书服务管理系统，实现系统接入过程标准化及安全控制，实现数字证书服务的统一管理。

本规范共包括5章正文和1个附录：第1章“范围”；第2章“系统接入总体要求”；第3章“CA系统功能要求”；第4章“CA系统接入接口要求”；第5章“WSDL文件”；附录（资料性）“名词解释”。

其中，第2章规定，根据《卫生系统电子认证服务管理办法（试行）》的规定，卫生部将建设集中的数字证书服务管理系统，用于卫生系统内所有证书用户信息的收集、查询、统计和分析，以及进行用户意见收集、服务质量监督等管理工作。卫生部通过数字证书服务管理系统对在卫生系统领域开展电子认证服务的CA机构实行接入控制及服务管理。拟为卫生系统领域提供服务的电子认证服务机构，须符合《卫生系统电子认证服务管理办法（试行）》的相关要求，将CA系统接入到卫生部数字证书服务管理系统。

第3章规定，电子认证服务机构的CA系统须具备如下基本功能：证书申请、证书更新、证书解锁、证书吊销、密钥恢复、证书信息发布。

第4章规定，电子认证服务机构的CA系统调用数字证书服务管理系统提供的数据同步接口，实现与卫生部数字证书服务管理系统之间数字证书和黑名单的信息同步等，并定义了3个数据同步接口函数原型：证书信息同步接口函数、黑名单信息同步接口函数、查询证书信息接口函数。

28.2.6 网上银行系统信息安全通用规范（JR/T 0068）

JR/T 0068-2012《网上银行系统信息安全通用规范》

本规范包含网上银行系统的描述、安全技术规范、安全管理规范、业务运作安全规范，本规范适用于网上银行系统建设、运营及测评。

本规范共包括引言、6章正文和3个附录：第1章“范围”；第2章“规范性引用文件”；第3章“术语和定义”；第4章“符号和缩略语”；第5章“网上银行系统概述”；第6章“安全规范”；附录A（资料性）“基本的网络防护架构参考图”；附录B（资料性）“增强的网络防护架构参考图”；附录C（规范性）“物理安全”。

其“引言”中指出，本规范是在收集、分析评估检查发现的网上银行信息安全问题和已发生过的网上银行案件的基础上，有针对性地提出的安全要求，内容涉及网上银行系统的技术、管理和业务运作三个方面。本规范分为基本要求和增强要求两个层次。基本要求为最低安全要求，增强要求为本规范下发之日起的三年内应达到的安全要求，各单位应在遵照执行基本要求的同时，按照增强要求，积极采取改进措施，在规定期限内达标。本规范旨在有效增强现有网上银行系统的安全防范能力，促进网上银行规范、健康发展。本规