ICS 35.040
L 80
备案号:44642—2014

GM

中华人民共和国密码行业标准

GM/T 0037—2014

证书认证系统检测规范

Certificate authority system test specification

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　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。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：长春吉大正元信息技术股份有限公司、上海格尔软件股份有限公司、国家信息安全工程技术研究中心、北京海泰方圆科技有限公司。

本标准起草人：刘平、高利、田景成、姜玉琳、张宝欣、李伟平、赵丽丽、祝国鑫、袁峰、谭武征、安晓江、张万涛、吴臣华。

证书认证系统检测规范

1 范围

本标准规定了证书认证系统的检测内容与检测方法。

本标准适用于为电子签名提供电子认证服务，按照 GM/T 0034—2014 研制或建设的证书认证服务运营系统的检测，也可为其他证书认证系统的检测提供参考。

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。

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

证书认证系统 certificate authentication system；CA

对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统。

3.2

证书注册系统 registration authority；RA

证书认证系统的一个组成部分，主要功能是对数字证书注册流程进行全过程管理，又称为注册系统。

3.3

CA 证书 CA certificate

给 CA 签发的证书，可以由 CA 给自己签发，也可以由另一个 CA 签发。

3.4

SM2 算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

4 缩略语

下列缩略语适用于本文件。

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

LDAP：目录服务系统(Lightweight Directory Access Protocol)

OCSP：在线证书状态查询协议(Online Certificate Status Protocol)

SOCSP：简明在线证书状态查询协议(Simple Online Certificate Status Protocol)

5 检测对象

5.1 产品

产品指证书认证系统，主要由签发系统服务器、注册系统服务器、OCSP 服务器、LDAP 服务器、密码机、证书与私钥存储介质，以及相关软件等组成。

5.2 项目

采用证书认证系统产品，按照 GM/T 0034—2014 要求建设的证书认证服务运营系统。

6 测试大纲

对检测对象的检测，应编制相应的测试大纲，并按照测试大纲的内容逐项进行。测试的内容应符合第 8 章的要求，测试的方法应符合第 9 章的要求。

测试大纲示例可参见附录 A。

7 检测环境

产品检测环境为按产品设计要求搭建的模拟环境。

项目检测环境为证书认证服务运营系统的实际环境。

8 检测内容

8.1 场地

8.1.1 工程建设

工程建设应符合 GM/T 0034—2014 中 8.5 对物理安全的要求。

8.1.2 物理区域

证书认证系统的物理区域，应划分为公共区、服务区、管理区、核心区。

在服务区应放置证书/证书注销列表的存储与发布服务器、LDAP/OCSP 查询服务器(如果存在 OCSP 查询服务器)及连接的密码机、注册管理服务器及连接的密码机、入侵检测或入侵防御探测设备、漏洞扫描设备；在管理区应放置注册管理终端、注册审计终端、证书/证书注销列表的生成与签发管理终端、入侵检测或入侵防御管理控制台；在核心区应放置证书/证书注销列表的生成与签发服务器及连接的密码机、数据库服务器、保管密钥备份材料及介质的保险箱等；在各区域间应放置防火墙。可参见附录 C。

核心区应为屏蔽机房，屏蔽效果应满足 GM/T 0034—2014 中 8.5.2.5 的相关要求。

进入各区域的顺序，依次为管理区、服务区、核心区。

在各区域放置的设备上，应在醒目的位置标识出设备在系统中的名称，例如：签发服务器、注册服务器等。

各区域应设置监控探头、消防探头及门禁系统，并设置监控室对各区域进行实时监控。

本项仅用于项目检测。

8.2 网络

8.2.1 网络结构

采用C/S模式的系统，网络结构应从外至内依次划分为公共区、服务区、管理区及核心区四个网段，各相邻网段之间采用不同的防火墙进行隔离，可参照B.1。

采用B/S模式的系统，网络结构应从外至内依次划分为公共区、服务区/管理区及核心区三个网段，各相邻网段之间采用不同的防火墙进行隔离，可参照B.2。

8.2.2 网络配置安全策略

8.2.2.1 防火墙

系统配置的防火墙其主要的安全策略为：

a) 工作模式设置为路由模式；

b) 关闭所有系统不需要的端口；

c) 对防火墙发现的安全事件应有相应的响应策略。

8.2.2.2 入侵检测

系统配置的入侵检测其主要的安全策略为：

a) 入侵检测探测设备部署在服务区交换机上，保证对外来所有信息包的检测；

b) 入侵检测管理控制台与入侵检测探测设备采取直连的方式，保证其独立的管理及检测；

c) 入侵检测对信息包的检测与分析设置为高警戒级别；

d) 入侵检测设备发现的安全事件应有相应的响应策略；

e) 入侵检测的特征库应及时更新。

注：入侵检测设备也可设置为入侵防御设备。

8.2.2.3 漏洞扫描

系统配置的漏洞扫描其主要的安全策略为：

a) 应定期对关键的服务器设备、网络设备及网络安全设备进行漏洞扫描。

b) 漏洞扫描发现的安全事件应有相应的响应策略。

c) 应及时更新漏洞库。

8.2.2.4 病毒防治

系统配置的病毒防治其主要的安全策略为：

a) 关键的服务器及操作、管理终端应部署防病毒产品。

b) 防病毒产品发现的安全事件应有相应的响应策略。

c) 应及时更新病毒库。

8.2.2.5 密码机

密码机应通过独立的物理端口与服务器连接。

密码机应是经国家密码管理主管部门审批的产品。

8.3 岗位及权限管理

8.3.1 签发系统

8.3.1.1 超级管理员

应设置超级管理员，该管理员由本系统初始化时产生，负责系统的策略管理和本系统的业务管理员管理。

8.3.1.2 审计管理员

应设置审计管理员，该管理员由本系统初始化时产生，负责系统的审计员管理。

8.3.1.3 业务管理员

应设置业务管理员，该管理员由超级管理员设置并授权，负责业务操作员管理等。

8.3.1.4 业务操作员

应设置业务操作员，该操作员由业务管理员设置并授权，负责用户证书库的管理、数据备份/恢复等。

8.3.1.5 审计员

应设置审计员，该审计员由审计管理员设置并授权，负责对涉及本系统安全的事件、各管理和操作人员的行为进行审计和监督。

8.3.2 注册系统

8.3.2.1 业务管理员

应设置业务管理员，该管理员的证书由CA签发，在RA初始化时授权。负责RA的业务操作员管理、RA系统策略的设置等。

8.3.2.2 业务操作员

应设置业务操作员，该操作员由业务管理员设置并授权，分别负责录入、审核、制证和查询统计等操作。

8.3.2.3 审计员

应设置审计员，该审计员的证书由CA签发，在RA初始化时授权。负责对涉及RA安全的事件、各管理和操作人员的行为进行审计和监督。

8.4 安全管理

管理策略包括安全(系统安全、通信安全、密钥安全、证书管理安全、安全审计)、数据备份和可靠性等，应分别符合GM/T 0034—2014中8.2、8.3和8.4的要求。

应设置相应的管理制度，保证密码使用的安全。如密码设备管理制度、密钥介质管理制度、数据备份/恢复管理办法、应急事件处理预案等。

本条仅用于项目检测。

8.5 系统初始化

应能按照 GM/T 0034—2014 中 8.1.5 的要求正确进行初始化。

本条仅用于产品检测。

8.6 系统功能

8.6.1 注册系统

8.6.1.1 申请信息的录入

应能提供录入和修改证书申请信息的界面，应能选择所申请数字证书的密钥类型及长度，可支持批量证书申请信息的导入。系统应能自动使操作员对其操作行为进行签名。

8.6.1.2 申请信息的审核

应能提供对申请信息审核的界面，应能读取需要进行审核的申请信息，将审核通过的信息提交至签发系统，将审核不通过的信息返回到录入界面。系统应能自动使操作员对其操作行为进行签名。

8.6.1.3 证书下载

应能提供下载证书的界面，并能将证书信息安全下载。系统应能自动使操作员对其操作行为进行签名。

8.6.1.4 权限管理

应提供业务管理员进行业务管理的界面，业务管理员能够通过此界面进行增加、删除操作员并设置其权限的操作。

8.6.1.5 证书模板更新管理

当 CA 给 RA 授权的证书模板发生变化时，RA 应能与 CA 进行模板同步更新。

8.6.1.6 日志

日志应记录事件发生的时间、事件的操作者、操作类型及操作结果等信息。

应能按时间、操作者、操作类型等对日志进行分类或综合查询。

8.6.1.7 审计

应设置单独的审计管理终端，提供审计管理的界面，能够对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计，审计应能验证记录的签名。

审计数据应能归档且不能被篡改。

审计过的记录应有明显标记。

8.6.2 签发系统

8.6.2.1 多层结构支持

应能将所下载的根证书和下级 CA 证书导入到证书存储区中，并能正确识别出根证书和下级 CA 证书，建立正确的认证路径。

本条仅用于项目检测。

8.6.2.2 证书签发

应能使用指定的密码算法签发数字证书，并且能够提供证书查询和下载服务。

8.6.2.3 CRL 签发

应能根据 CRL 签发策略正确签发 CRL 文件，并且能够提供 CRL 查询和下载服务。

8.6.2.4 CA 证书更新

应能正确完成 CA 证书的更新，通过新 CA 证书与旧 CA 证书的证书链，实现新旧证书更替。

本条仅用于产品检测。

8.6.2.5 证书更新

应能为已经注册的用户重新签发证书。

8.6.2.6 证书撤销

应能为已经注册的用户提供证书撤销服务。

8.6.2.7 证书状态查询

应能通过 OCSP 服务器或者 SOCSP 服务器提供实时证书状态查询服务。

8.6.2.8 RA 管理

应能签发 RA 服务器证书，并对其管理员进行授权。

8.6.2.9 证书模板

应能对所签发的证书类型及内容进行定义。

8.6.2.10 用户密钥恢复

应能通过密钥管理中心为已经注册的用户提供用户密钥恢复服务。

8.6.2.11 日志

日志应记录事件发生的时间、事件的操作者、操作类型及操作结果等信息。

应能按时间、操作者、操作类型等对日志进行分类或综合查询。

8.6.2.12 审计

应提供审计管理的界面，能够对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计。审计应能验证记录的签名。

审计数据应能归档且不能被篡改。

审计过的记录应有明显标记。

8.6.2.13 权限管理

超级管理员和审计管理员应是平级关系。

超级管理员能够添加、删除业务管理员并能够为其分配权限。

业务管理员能够添加、删除业务操作员并能够为其分配权限。

审计管理员能够添加、删除审计员并能够为其分配权限。

业务操作员能够进行其权限范围内的操作。

审计员能够审计事件发生的时间、事件的操作者、操作类型及操作结果等信息。

8.7 系统性能

系统性能主要为证书签发性能，测试从 RA 向 CA 提交证书申请，到 CA 将证书返回到 RA 后下载到证书载体的时间。

8.8 数据备份和恢复

应有数据备份和恢复策略，能够实现对签发系统和注册系统的数据备份与恢复。

本条仅用于项目检测。

8.9 第三方安全产品

8.9.1 防火墙

防火墙的部署位置应符合 8.1.2 的要求。

防火墙配置策略应符合 8.2.2.1 的要求。

防火墙产品应为通过国家相关机构检测认证的产品。

本条仅用于项目检测。

8.9.2 入侵检测

入侵检测产品部署位置应符合 8.1.2 的要求。

入侵检测产品配置策略应符合 8.2.2.2 的要求。

入侵检测产品应为通过国家相关机构检测认证的产品。

本条仅用于项目检测。

注：本条也适用于入侵防御产品。

8.9.3 漏洞扫描

漏洞扫描产品部署应符合 8.1.2 的要求。

漏洞扫描产品配置策略应符合 8.2.2.3 的要求。

漏洞扫描产品应为通过国家相关机构检测认证的产品。

本条仅用于项目检测。

8.9.4 病毒防治

病毒防治产品部署位置应符合 8.1.2 的要求。

病毒防治产品配置策略应符合 8.2.2.4 的要求。

病毒防治产品应为通过国家相关机构检测认证的产品。

本条仅用于项目检测。

8.10 入根

证书认证系统产品应支持接入国家根 CA。

运营的证书认证系统应接入国家根 CA。

8.11 证书格式

证书格式应符合 GM/T 0015 和 GM/T 0034—2014 的要求。

8.12 证书链

应确保证书链的有效性。

8.13 算法

证书认证系统应能使用 SM2 算法和国家密码管理主管部门批准的其他算法签发数字证书。
数字证书应采用 SM2 算法或国家密码管理主管部门批准的其他算法。

8.14 协议

证书认证系统采用的协议应符合 GM/T 0014 的要求。

8.15 文档

证书认证系统应配备相关的文档，符合 GM/T 0034—2014 中 10.6 的要求。

9 检测方法

9.1 场地

9.1.1 工程建设

分别使用授权的门卡和未授权的门卡通过门禁，授权的通过，未授权的无法通过。
从监控屏可以看到机房的各个区域，无死角。
查看屏蔽机房、消防等的相关部门出具的验收报告。

9.1.2 物理区域

查看系统物理区域的划分、机房布局、设备放置等，应符合 8.1.2 的要求。

9.2 网络

9.2.1 网络结构

查看系统网络结构，应符合 8.2.1 的要求。

9.2.2 网络配置安全策略

9.2.2.1 防火墙

查看防火墙的配置策略，应符合 8.2.2.1 的要求。

9.2.2.2 入侵检测

查看入侵检测(入侵防御)的部署和策略设置，应符合 8.2.2.2 的要求。

9.2.2.3 漏洞扫描

查看漏洞扫描系统的日志，其中包括最后一次漏洞扫描时间，有无发现漏洞等，应符合 8.2.2.3 的

要求。

9.2.2.4 病毒防治

查看病毒防治系统的日志，其中包括病毒库更新、有无病毒攻击等，应符合 8.2.2.4 的要求。

9.2.2.5 密码机

查看密码机连接的方式，应符合 8.2.2.5 的要求。

9.3 岗位及权限管理

9.3.1 签发系统

9.3.1.1 超级管理员

以正确的方式登录超级管理员操作界面，系统应准入。
以错误的方式登录超级管理员操作界面，系统应拒绝。

9.3.1.2 审计管理员

以正确的方式登录审计管理员操作界面，系统应准入。
以错误的方式登录审计管理员操作界面，系统应拒绝。

9.3.1.3 业务管理员

以正确的方式登录业务管理员操作界面，系统应准入。
以错误的方式登录业务管理员操作界面，系统应拒绝。

9.3.1.4 业务操作员

以正确的方式登录业务操作员操作界面，系统应准入。
以错误的方式登录业务操作员操作界面，系统应拒绝。

9.3.1.5 审计员

以正确的方式登录审计员操作界面，系统应准入。
以错误的方式登录审计员操作界面，系统应拒绝。

9.3.2 注册系统

9.3.2.1 业务管理员

以正确的方式登录业务管理员操作界面，系统应准入。
以错误的方式登录业务管理员操作界面，系统应拒绝。

9.3.2.2 业务操作员

以正确的方式登录业务操作员操作界面，系统应准入。
以错误的方式登录业务操作员操作界面，系统应拒绝。

9.3.2.3 审计员

以正确的方式登录审计员操作界面，系统应准入。

以错误的方式登录审计员操作界面，系统应拒绝。

9.4 安全管理

查看系统的管理策略和管理制度，应符合 8.4 的要求。

9.5 系统初始化

按照 GM/T 0034—2014 中 8.1.5 的要求进行初始化，结果应符合 8.5 的要求。

9.6 系统功能

9.6.1 注册系统

9.6.1.1 申请信息的录入

在录入界面进行录入和修改证书申请信息的操作，结果应符合 8.6.1.1 的要求。

9.6.1.2 申请信息的审核

在审核界面进行申请信息审核的操作，结果应符合 8.6.1.2 的要求。

9.6.1.3 证书下载

在下载界面进行证书下载的操作，结果应符合 8.6.1.3 的要求。

9.6.1.4 权限管理

在权限管理界面进行增加、删除操作员操作，设置操作员权限的操作，结果应符合 8.6.1.4 的要求。

9.6.1.5 证书模板更新管理

进行增加、删除 CA 授权给 RA 的证书模板，结果应符合 8.6.1.5 的要求。

9.6.1.6 日志

分别按时间、人员、操作类型等对日志进行分类或综合查询，结果应符合 8.6.1.6 的要求。

9.6.1.7 审计

在审计界面对事件发生的时间、事件的操作者、操作类型及操作结果、记录的签名等信息进行审计操作，结果应符合 8.6.1.7 的要求。

9.6.2 签发系统

9.6.2.1 多层结构支持

查看入根测试报告，结果应符合 8.6.2.1 的要求。

9.6.2.2 证书签发

在 RA 进行证书申请和下载操作，查看 CA 日志，访问 CA 发布系统进行证书的查询，结果应符合 8.6.2.2 的要求。

9.6.2.3 CRL 签发

进行 CRL 的查询和下载操作，查看 CA 日志，结果应符合 8.6.2.3 的要求。

9.6.2.4 CA 证书更新

进行 CA 证书更新的操作，结果应符合 8.6.2.4 的要求。

9.6.2.5 证书更新

在 RA 进行证书更新操作，结果应能在 CRL 或证书状态查询中查看到。

9.6.2.6 证书撤销

在 RA 进行证书撤销操作，结果应能在 CRL 或证书状态查询中查看到。

9.6.2.7 证书状态查询

访问 OCSP 服务器或者 SOCSP 服务器，进行证书状态查询操作，结果应符合 8.6.2.7 的要求。

9.6.2.8 RA 管理

进行 RA 服务器证书的签发操作，并对其管理员进行授权，结果应符合 8.6.2.8 的要求。

9.6.2.9 证书模板

在证书模板管理界面进行定义、删除证书模板的操作，结果应符合 8.6.2.9 的要求。

9.6.2.10 用户密钥恢复

在 RA 进行用户密钥恢复操作，结果应符合 8.6.2.10 的要求。

9.6.2.11 日志

分别按时间、人员、操作类型等对日志进行分类或综合查询，结果应符合 8.6.2.11 的要求。

9.6.2.12 审计

在审计界面对事件发生的时间、事件的操作者、操作类型及操作结果、记录的签名等信息进行审计操作，结果应符合 8.6.2.12 的要求。

9.6.2.13 权限管理

在权限管理界面进行增加、删除业务管理员操作，设置业务管理员权限的操作，结果应符合8.6.2.13 的要求。

9.7 系统性能

按照 8.7 的要求进行测试，并记录测试结果。

9.8 数据备份和恢复

查看备份和恢复策略及采取的相应措施，应符合 8.8 的要求。

9.9 第三方安全产品

分别查看防火墙、入侵检测(入侵防御)、漏洞扫描和病毒防治产品的部署和相应的产品资质证明，应符合 8.9 的要求。

9.10 入根

查看 CA 证书的证书颁发者并验证其有效性。

9.11 证书格式

查看证书各项内容，应符合 8.11 的要求，并验证其有效性。

9.12 证书链

验证证书链的有效性，应符合 8.12 的要求。

9.13 算法

查看 CA 使用的密码设备中的算法应包括 SM2 算法。
查看证书认证系统可选择算法应符合 8.13 的要求。
用指定的算法应能成功签发数字证书。

9.14 协议

查看证书认证系统所采用的协议应符合 8.14 的要求。

9.15 文档

查看证书认证系统所配备的文档应符合 8.15 的要求。

10 合格判定

10.1 项目合格判定

8.1.2、8.2.1、8.2.2.5、8.6.1.3、8.6.2.2、8.10、8.11、8.12、8.13、8.14 为关键项，其中任何一项检测结果不符合相应检测要求的，即判定为不合格。

8.6.2.3 和 8.6.2.7 为组合关键项，其检测结果均不符合相应检测要求的，即判定为不合格。

除上述项外，其他项的检测结果累计 5 项以上(含 5 项)不符合相应检测要求的，即判定为不合格。

10.2 产品合格判定

8.2.1、8.2.2.5、8.5、8.6.1.3、8.6.2.2、8.10、8.11、8.13、8.14 为关键项，其中任何一项检测结果不符合相应检测要求的，即判定为不合格。

8.6.2.3 和 8.6.2.6 为组合关键项，其检测结果均不符合相应检测要求的，即判定为不合格。

除上述项外，其他项的检测结果累计 5 项以上(含 5 项)不符合相应检测要求的，即判定为不合格。

如果检测结果中出现连续不合格项，由检测组根据实际情况综合判定。

附 录 A
（资料性附录）
测试大纲

A.1 测试目的

检测产品或项目是否符合 GM/T 0034—2014。

A.2 证书认证系统的物理区域和网络结构

附图说明系统的机房布局、设备放置及物理连线、网络结构。

A.3 证书认证系统的软硬件配置

描述检测环境中所使用的软硬件产品的型号及配置。

A.4 证书认证系统的模块及功能

描述证书认证系统的主要模块及功能（可附图）。

A.5 测试内容

A.5.1 场地

场地检测见表 A.1。

表 A.1 场地检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	门禁	使用已授权身份识别设备（如：门卡）进入	通过		
2		使用未授权身份识别设备（如：门卡）进入	拒绝		
3	监控	查看实时监控	符合标准		
4		查看多画面监控	符合标准		
5		调用监控历史记录	符合标准		
6	机房屏蔽	查看机房屏蔽检测报告	符合标准		
7	消防	查看消防设施	符合标准		
8	物理区域	查看机房布局	符合标准		
9		查看设备放置及物理连线	符合标准		

A.5.2 网络

网络检测见表 A.2。

表 A.2 网络检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	网络结构	查看网络结构	符合标准		
2	防火墙配置	查看防火墙配置策略	符合标准		
3	入侵检测	查看入侵检测部署及配置	符合标准		
4	漏洞扫描	查看漏洞扫描记录	符合标准		
5	病毒防治	查看病毒防治日志	符合标准		
6	密码机	查看密码机连接方式	符合标准		

A.5.3 安全管理

安全管理策略检测见表 A.3。

表 A.3 安全管理策略检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	管理策略和制度	查阅管理策略和制度	符合标准		

A.5.4 系统初始化

系统初始化检测见表 A.4。

表 A.4 系统初始化检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	初始化签发系统	进行签发系统初始化操作	正确进行签发系统初始化		
2		产生超级管理员	正确产生超级管理员		
3		产生审计管理员	正确产生审计管理员		
4	初始化注册系统	进行注册系统初始化操作	正确进行注册系统初始化		
5		授权注册系统业务管理员	正确产生业务管理员		
6		授权注册系统审计员	正确产生审计员		

A.5.5 系统功能

A.5.5.1 签发系统

签发系统功能检测见表 A.5。

表 A.5 签发系统功能检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	登录	使用已授权管理员证书和正确PIN码登录	登录成功并进入登录界面		
2		使用未授权管理员证书或错误PIN码登录	拒绝登录		
3		拔掉登录者的证书介质	拒绝操作		
4	多层结构	支持根证书和下级CA证书导入到证书存储区操作	根证书和下级CA证书被成功导入		
5		正确识别出根证书和下级CA证书，建立正确的认证路径	建立正确的认证路径		
6	业务管理员管理	增加业务操作员操作	业务操作员被增加		
7		删除业务操作员操作	业务操作员被删除		
8		对业务操作员授予相应的权限	正确对业务操作员授权		
9	证书签发	使用CA签名密钥签发各类证书	证书被正确签发		
10		提供证书查询和下载服务	正确查询和下载证书		
11	CRL签发	根据CRL签发策略正确签发CRL文件	正确签发CRL		
12		提供CRL查询和下载服务	正确查询和下载CRL		
13	CA证书更新	支持CA证书更新功能，通过新CA证书与旧CA证书的认证链，实现新旧证书更替	新CA证书生成成功、并生成新旧证书认证链		
14	证书更新	执行证书更新操作，通过CRL和证书状态查询查看证书状态	证书被正确更新		
15	证书撤销	执行证书撤销操作，通过CRL和证书状态查询查看证书状态	证书被正确撤销		
16	证书状态查询	通过OCSP服务器或者SOCSP服务器提供实时证书状态查询服务	查询到正确的证书状态		
17	RA管理	签发RA服务器证书，对RA管理员进行授权	RA服务器证书被正确签发，RA管理员被正确授权		
18	证书模板管理	在证书模板管理界面进行增加证书模板操作	证书模板被增加		
19		在证书模板管理界面进行删除证书模板操作	证书模板被删除		
20		在证书模板管理界面进行修改证书模板操作	证书模板被正确修改		
21	日志	在日志管理界面执行对时间、人员、操作类型等信息的查询操作	可以显示相应页面		

表 A.5（续）

序号	测试内容	测试方法	预期结果	测试结果	备注
22	审计	在审计界面对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计操作	可以显示相应页面		
23		对记录的签名进行验证	可以进行验证		
24		审计过的记录有明显标记	显示明显标记		

A.5.5.2 注册系统

注册系统功能检测见表 A.6。

表 A.6 注册系统功能检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	登录	使用已授权业务管理员证书和正确 PIN 码登录	登录成功并进入登录界面		
2		使用未授权业务管理员证书或错误 PIN 码登录	拒绝登录		
3		拔掉登录者的证书介质	拒绝操作		
4	业务操作员管理	在业务操作员管理界面进行增加业务操作员操作	业务操作员被增加		
5		在业务操作员管理界面进行删除业务操作员操作	业务操作员被删除		
6		在业务操作员管理界面进行对业务操作员授权操作	正确对业务操作员授权		
7	申请信息录入	在申请信息录入界面进行申请信息录入操作	申请信息被正确录入		
8		支持批量证书申请信息的录入操作	批量证书申请信息被正确录入		
9	申请信息审核	在申请信息审核界面进行申请信息审核通过操作	审核通过		
10		在申请信息审核界面进行申请信息审核拒绝操作	审核未通过		
11	证书下载	提供可以进行证书下载的操作	证书被正确下载		
12	证书模板更新	提供将 CA 给 RA 授权的证书模板进行更新的操作	授权模板被正确更新		
13	日志	在日志管理界面执行对时间、人员、操作类型等信息的查询操作	可以显示相应页面		
14	审计	在审计界面对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计操作	可以显示相应页面		
15		对记录的签名进行验证	可以进行验证		
16		审计过的记录有明显标记	显示明显标记		

A.5.6 系统性能

系统性能检测见表 A.7。

表 A.7 系统性能检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	性能	测试证书签发性能	小于 30 s		

A.5.7 数据备份和恢复

数据备份和恢复检测见表 A.8。

表 A.8 数据备份和恢复检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	备份	查看备份和恢复策略	符合标准		
2		查看备份和恢复日志	符合标准		

A.5.8 第三方安全产品

第三方安全产品检测见表 A.9。

表 A.9 第三方安全产品检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	防火墙	查看相应产品资质证明	符合标准		
2	入侵检测	查看相应产品资质证明	符合标准		
3	漏洞扫描	查看相应产品资质证明	符合标准		
4	病毒防治	查看相应产品资质证明	符合标准		

A.5.9 入根

入根检测见表 A.10。

表 A.10 入根检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	入根	查看 CA 证书的证书颁发者	颁发者根 CA 标识		
2		查看 CA 证书有效性	有效		

A.5.10 证书

证书格式检测见表 A.11。

表 A.11 证书格式检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	证书 DN 序	查看	符合标准		
2	密钥用法	查看 keyUsage 项和 extKeyUsage 项	符合标准		
3	CRL 发布点	查看 cRLDistributionPoits 项并验证	符合标准		
4	OCSP	查看 authorityInfoAccess 项并验证	符合标准		
5	证书格式检查	查看证书其他项	符合标准		

A.5.11 证书链

证书链有效性检测见表 A.12。

表 A.12 证书链有效性检测

序号	测试内容	测试方法	预期结果	测试结果	备注
1	证书链	查看	有效		

A.5.12 算法

算法测试见表 A.13。

表 A.13 算法测试

序号	测试内容	测试方法	预期结果	测试结果	备注
1	算法	查看密码设备中的算法	有 SM2 算法		
2		查看证书认证系统可选择算法	有 SM2 算法		
3	签发证书	用指定的算法签发数字证书	成功		

A.5.13 协议

协议测试见表 A.14。

表 A.14 协议测试

序号	测试内容	测试方法	预期结果	测试结果	备注
1	协议	查看各模块间通信协议	符合标准		

A.5.14 文档

文档检查见表 A.15。

表 A.15 文档检查

序号	测试内容	测试方法	预期结果	测试结果	备注
1	文档	查阅相关文档	符合标准		

附 录 B
（资料性附录）
证书认证系统网络结构

B.1 当 RA 采用 C/S 模式时 CA 的网络结构

RA 采用 C/S 模式时 CA 的网络结构如图 B.1 所示。

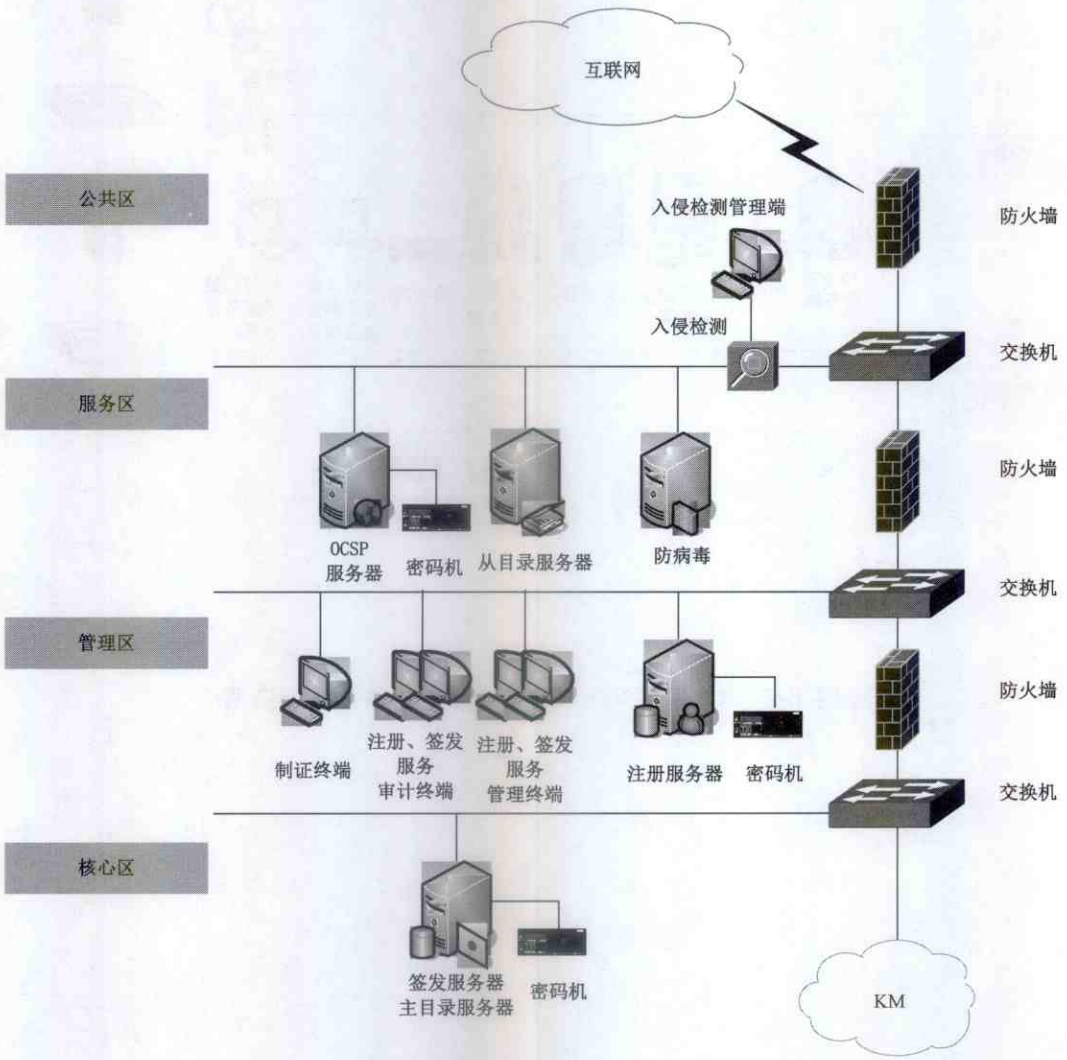


图 B.1 RA 采用 C/S 模式时 CA 的网络结构示意图

B.2 当 RA 采用 B/S 模式时 CA 的网络结构

RA 采用 B/S 模式时 CA 的网络结构如图 B.2 所示。

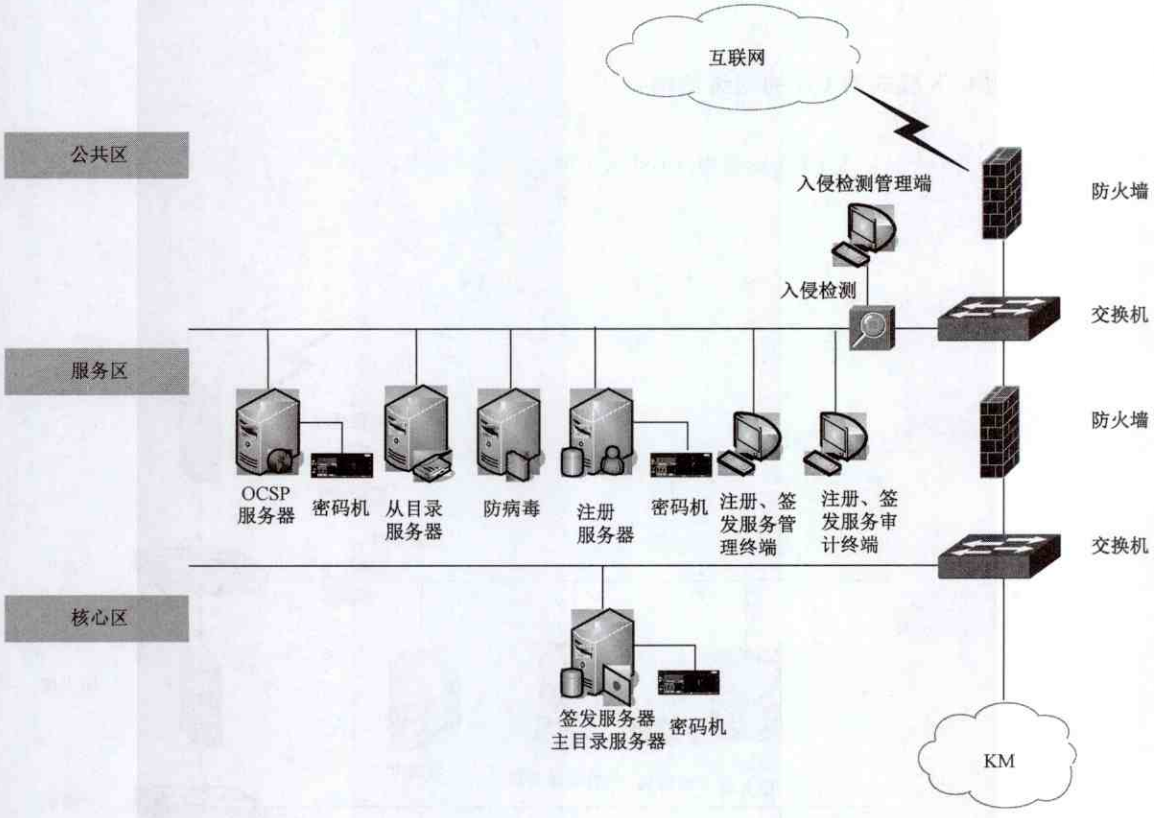


图 B.2 RA 采用 B/S 模式时 CA 的网络结构示意图

B.3 CA 与远程 RA 的连接

CA 与远程 RA 的连接如图 B.3 所示。

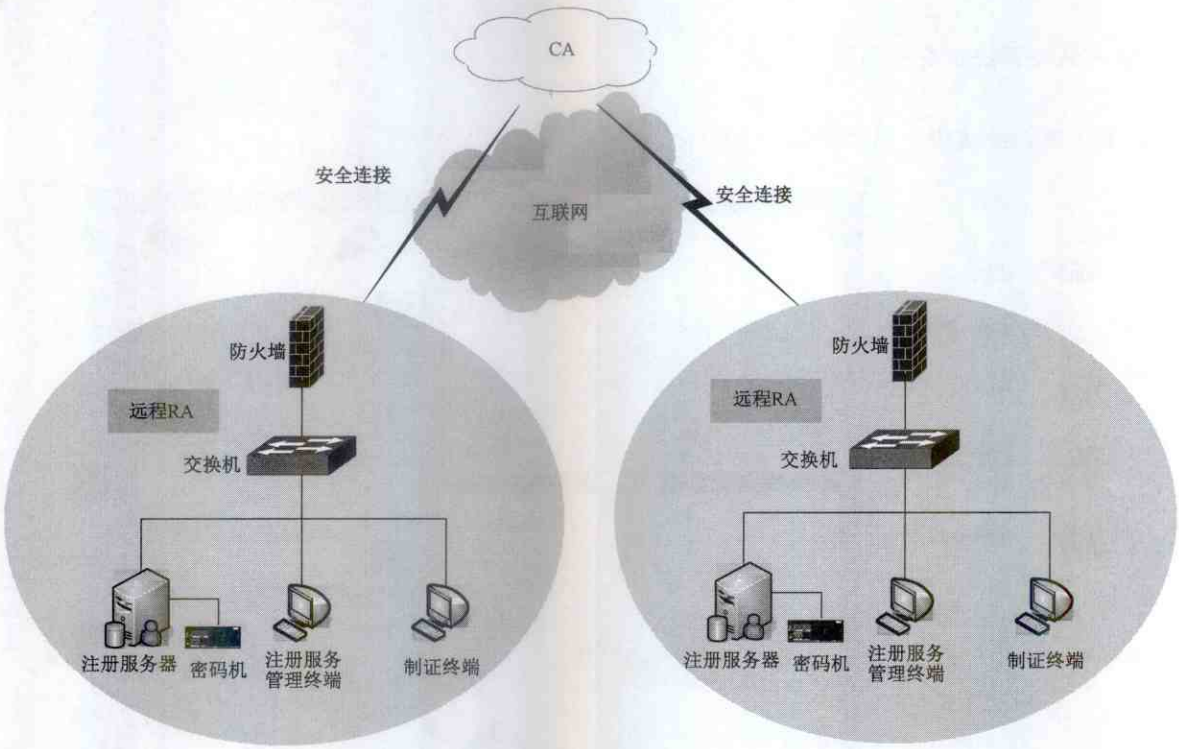
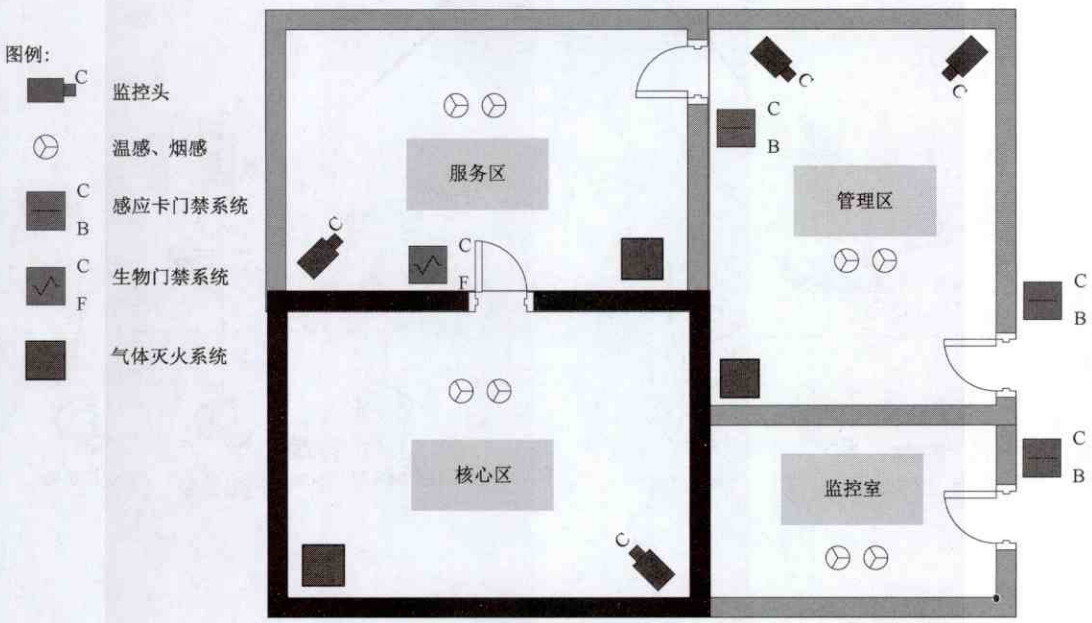


图 B.3 CA 与远程 RA 的连接示意图

附 录 C
（资料性附录）
证书认证系统机房布局及设备位置摆放示例图

C.1 证书认证系统机房布局图

证书认证系统机房布局图如图 C.1 所示。

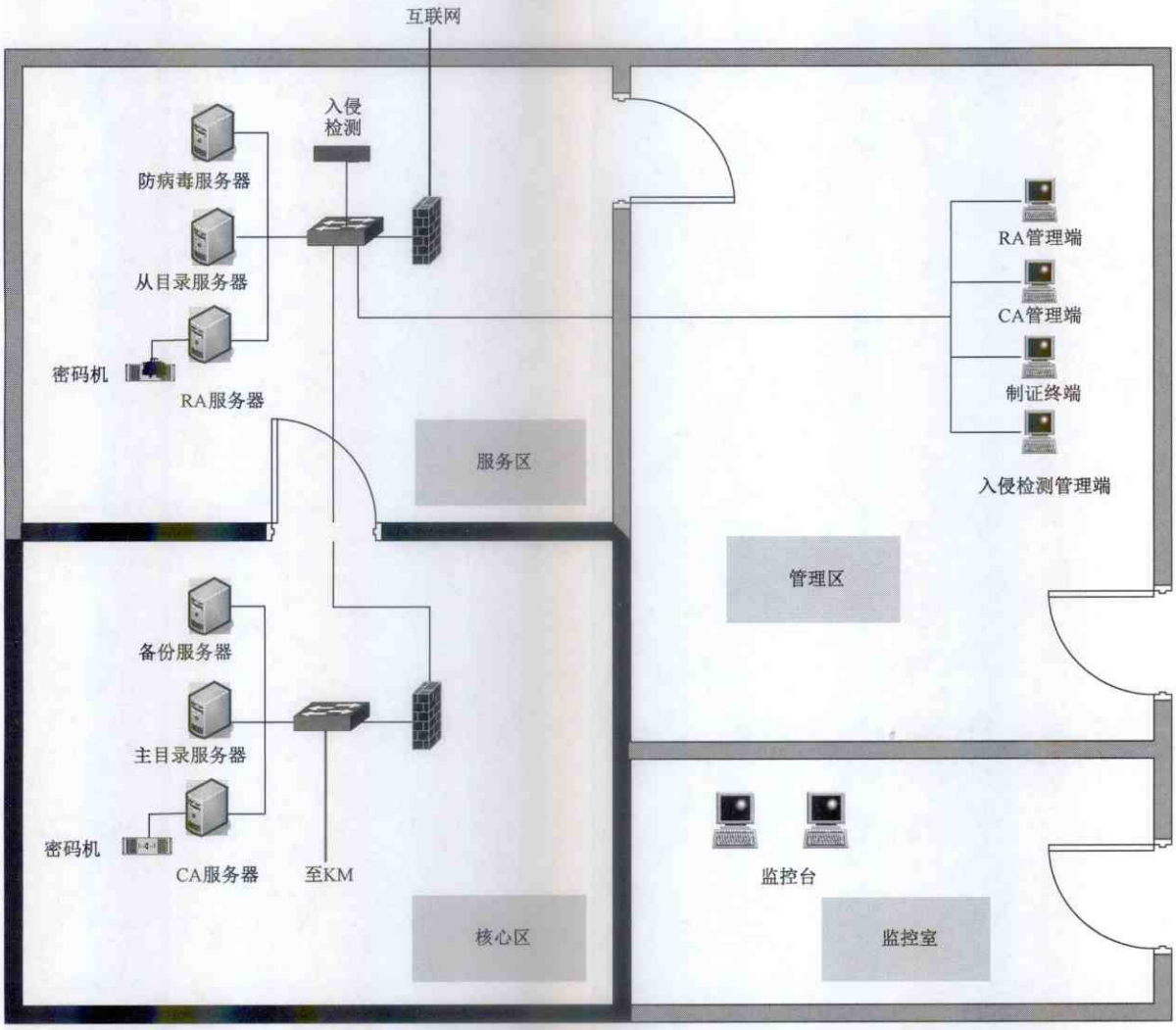


注：此图为 CA 机房示意图，其功能区域应该具备。但是根据机房规模涉及到弱电、强电、UPS 间等功能空间应按照用户的现场实际情况划分。

图 C.1 证书认证系统机房布局图

C.2 证书认证系统机房位置摆放图

证书认证系统机房位置摆放图如图 C.2 所示。



注：此图为CA机房示意图，其功能区域应该具备。但是根据机房规模涉及到弱电、强电、UPS间等功能空间应按照用户的现场实际情况划分。

图 C.2　证书认证系统机房位置摆放图

中华人民共和国密码
行业标准
证书认证系统检测规范
GM/T 0037—2014
*
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.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2 字数 48 千字
2014年5月第一版 2014年5月第一次印刷
*
书号:155066·2-27050 定价 36.00 元

GM/T 0037-2014