ICS

备案号：

××

中 华 人 民 共 和 国 × × 行 业 标 准

××/T ××××—××××

证书认证密钥管理系统检测规范

KM of Certificate Authority System Test Specification

2005-04-01 发布　　2005-04-01 实施

国家密码管理局 发布

目　　次

前　言

本标准主要根据《认证系统密码及其相关安全技术规范》制定。

本标准凡涉及密码算法相关内容，按国家有关法规实施。

本标准中的附录A、B、C均为资料性附录。

本标准由国家密码管理局提出。

本标准由国家密码管理局归口。

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、上海市数字证书认证中心有限公司、北京数字证书认证中心有限公司、北京握奇智能科技有限公司。

本标准主要起草人：高利、田景成、姜玉琳、张宝欣、祝国鑫、袁峰、李伟平、谭武征、安晓江、张万涛、吴臣华。

本规范责任专家：刘平。

证书认证密钥管理系统检测规范

1 范围

本标准适用于在中华人民共和国境内、为电子签名提供电子认证服务，按照《证书认证系统密码及其相关安全技术规范》研制或建设的证书认证密钥管理系统的检测，也可为其它证书认证密钥管理系统的研制、建设提供参考。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

《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规范。

3.1

证书认证系统certificate authority（CA）

又称为签发系统，是被用户所信任的签发公钥证书及证书注销列表的管理系统。主要功能是对数字证书进行全过程管理。

3.2

密钥管理系统 key management system（KM）

为证书认证系统提供加密密钥对，对加密密钥进行全过程的管理。

3.3

数字证书 digital certificate

又称为证书，是由证书认证系统签名的包含公开密钥、公开密钥拥有者信息、签发者信息、有效期以及扩展信息的数字文件。

4 检测对象

4.1 产品

产品指证书认证密钥管理系统，主要由密钥管理服务器、密钥管理数据库服务器、密码机、KM管理终端、KM审计终端以及相关软件等组成。

4.2 项目

采用证书认证密钥管理产品，按照《证书认证系统密码及其相关安全技术规范》第9章所要求建设的证书认证密钥管理系统。

5 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。测试的内容应符合本规范第7章的要求，测试的方法应符合本规范第8章的要求。

测试大纲示例可参见附录A。

6 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密钥管理运营系统的实际环境。

7 检测内容

7.1 场地

7.1.1 工程建设

工程建设应符合《证书认证系统密码及其相关安全技术规范》中8.5 “物理安全”的要求。

7.1.2 物理区域

KM的物理区域应划分为密钥核心区和密钥管理区。

在密钥服务区放置密钥管理服务器及连接的密码机、数据库服务器、防病毒服务器、入侵检测探测设备，在密钥管理区放置KM管理终端、KM审计终端、入侵检测管理控制台。

密钥服务区必须设置独立的电磁屏蔽。

进入各区域的顺序，依次为密钥管理区、密钥核心区。

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：密钥管理服务器、密钥管理数据库服务器等。

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。

本项仅适用于项目检测。

7.2 网络

7.2.1 网络结构

KM与CA处于同一局域网内，应通过防火墙与CA连接。

KM与CA不处于同一局域网内，应通过网络密码机与CA连接。

网络密码机必须是经国家密码管理局审批的产品。

7.2.2 网络配置安全策略

7.2.2.1 防火墙

系统配置的防火墙其主要的安全策略为：

1．工作模式设置为路由模式。

2．关闭所有系统不需要的端口。

7.2.2.2 入侵检测

入侵检测探测设备部署在密钥服务区交换机上，保证对外来所有信息包的检测；

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；

入侵检测对信息包的检测与分析设置为高警戒级别。

7.2.2.3 漏洞扫描

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。

7.2.2.4 病毒防治

关键的服务器及操作、管理终端应部署防病毒产品，并及时更新病毒库。

7.2.2.5 密码机

密码机必须通过独立的物理端口与服务器连接。

密码机必须是经国家密码管理局审批的产品。

7.3 岗位及权限管理

7.3.1 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。

7.3.2 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。

7.3.3 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，负责用户密钥库的管理、数据备份/恢复等。

7.3.4 审计员

应设置审计员，该审计员由本系统初始化时产生，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。

7.4 安全管理

管理策略包括安全(系统安全、通信安全、密钥安全、安全审计）、数据备份和可靠性等，应符合《证书认证系统密码及其相关安全技术规范》中9.2“安全”、9.3“数据备份”和9.4“可靠性”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。

7.5 系统初始化

KM的初始化过程为：

1. 生成KM的机构密钥并安全备份；
2. 由国家根CA签发KM证书；
3. 生成超级管理员和审计员；
4. 由超级管理员生成业务管理员；
5. 由业务管理员生成业务操作员。

本项仅用于产品检测。

7.6 系统功能

7.6.1 支持多个 CA

系统应能为多个CA提供密钥服务。

本项仅用于产品检测。

7.6.2 密钥管理

7.6.2.1 密钥生成

应能预生成或实时生成SM2和国家密码管理局批准的其它算法的密钥对,预生成的密钥对应安全存放在备用库中，密钥对提供给CA后应安全存放在在用库中。

应能在CA提出密钥申请或更新时，提供密钥对，并将密钥对从备用库移至在用库中。

7.6.2.2 密钥恢复

应能在CA提出密钥恢复申请时，进行密钥恢复操作。

应能提供密钥的本地恢复功能，在本地恢复的密钥不能以明文的方式出现在载体之外，加密该密钥的密钥也不能以明文形式出现在载体之外。

通过密钥的本地恢复功能来完成司法取证。

7.6.2.3 密钥撤销

应能在CA提出密钥撤销申请时，进行密钥撤销操作。

7.6.2.4 密钥统计

应能分别对备用库、在用库和历史库存放的密钥进行统计。

7.6.3 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。

7.6.4 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。

审计数据应能归档并不能被篡改。

7.6.5 权限管理

超级管理员和审计员必须是平级关系。

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。

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。

7.7 系统性能

系统性能主要为密钥对生成时间。

系统应能够按照支持的算法计算密钥对生成速率。

7.8 数据备份和恢复

应有数据备份和恢复策略，能够实现对密钥管理系统的数据备份与恢复。

本项仅用于项目检测。

7.9 第三方安全产品

7.9.1 防火墙

防火墙的部署位置应符合《证书认证系统密码及其相关安全技术规范》条目8.1.4要求。

防火墙配置策略应符合本规范7.2.2.1要求。

防火墙产品应为通过国家相关机构检测认证的产品。

本项仅用于项目检测。

7.9.2 入侵检测

入侵检测产品部署位置应符合《证书认证系统密码及其相关安全技术规范》条目8.1.4要求。

入侵检测产品配置策略应符合本规范7.2.2.2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。

本项仅用于项目检测。

7.9.3 漏洞扫描

漏洞扫描产品部署应符合《证书认证系统密码及其相关安全技术规范》条目8.1.4要求。

漏洞扫描产品配置策略应符合本规范7.2.2.3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。

本项仅用于项目检测。

7.9.4 病毒防治

病毒防治产品部署位置应符合《证书认证系统密码及其相关安全技术规范》条目8.1.4要求。

病毒防治产品配置策略应符合本规范7.2.2.4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。

本项仅用于项目检测。

8 检测方法

8.1 场地

8.1.1 工程建设

1. 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。
2. 从监控屏可以看到机房的各个区域，无死角。
3. 查看屏蔽机房、消防等的相关部门出具的验收报告。

8.1.2 物理区域

查看系统物理区域的划分、机房布局、设备放置等，应符合本规范7.1.2的要求。

8.2 网络

8.2.1 网络结构

查看网络结构，应符合本规范7.2.1的要求。

8.2.2 网络配置安全策略

8.2.2.1 防火墙

查看防火墙的配置策略，应符合本规范7.2.2.1的要求；

8.2.2.2 入侵检测

查看入侵检测的部署和策略设置，应符合本规范7.2.2.2的要求；

8.2.2.3 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，应符合本规范7.2.2.3的要求。

8.2.2.4 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，应符合本规范7.2.2.4的要求。

8.2.2.5 密码机

查看密码机连接的方式，应符合本规范7.2.2.5的要求。

8.3 岗位及权限管理

8.3.1 超级管理员

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

8.3.2 业务管理员

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

8.3.3 业务操作员

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

8.3.4 审计员

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

8.4 安全管理

查看系统的管理策略和管理制度，应符合本规范 7.4 的要求。

8.5 系统初始化

按本规范7.5的要求进行初始化。

8.6 系统功能

8.6.1 支持多 CA

连接两套CA系统，同时为其提供密钥服务，结果应符合本规范7.6.1的要求。

8.6.2 密钥管理

8.6.2.1 密钥生成

进行指定数量的密钥预生成操作，查看备用库，密钥数量应有相应的增加；

在为CA提供密钥或更新密钥服务后，查看备用库和在用库，密钥数量应有相应的变化；

8.6.2.2 密钥恢复

在为CA提供密钥恢复服务后，查看日志应有相应的记录。

进行密钥的本地恢复操作，结果应符合本规范7.6.2.2的要求。

8.6.2.3 密钥撤销

在为CA提供密钥撤销服务后，查看在用库和历史库，应有相应的状态标识。

8.6.2.4 密钥统计

对备用库、在用库和历史库密钥进行统计，结果应符合本规范7.6.2.4的要求。

8.6.3 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，结果应符合本规范7.6.3的要求。

8.6.4 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，结果应符合本规范7.6.4的要求。

8.6.5 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，结果应符合本规范7.6.5的要求。

8.7 系统性能

按照本规范7.7的要求进行测试，并记录测试结果。

8.8 数据备份和恢复

查看备份和恢复策略及采取的相应措施，应符合本规范7.8的要求。

8.9 第三方安全产品

分别查看防火墙、入侵检测、漏洞扫描和病毒防治的部署和相应的产品资质证明，应符合本规范7.9的要求。

9 合格判定

9.1 项目合格判定

本规范中 7.1.2、7.2.1、7.2.2.5、7.6.2.1、7.6.2.2 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。

除上述项外，其它项的检测结果累计3项以上(含3项)不符合相应检测要求的，即判定为不合格。

9.2 产品合格判定

本规范中 7.2.1、7.2.2.5、7.5、7.6.2.1、7.6.2.2 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。

除上述项外，其它项的检测结果累计3项以上(含3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　测试大纲

（资料性附录）

A.1. 测试目的

检测产品或项目是否符合《认证系统密码及其相关安全技术规范》。

A.2. 密钥管理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. 密钥管理系统的软硬件配置

描述检测环境中所使用的软硬件产品的型号及配置。

A.4. 密钥管理系统的模块及功能

描述密钥管理系统的主要模块及功能（可附图）。

A.5. 测试内容

A.5.1.　场地

测试用例：

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		
4.		查看多画面监控	符合		
5.		调用监控历史记录	符合		
6.	消防	查看消防设施	符合		
7.	物理区域	查看机房布局	符合		
8.		查看设备放置及物理连线	符合		

A.5.2.　网络

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		
2.	防火墙配置	查看防火墙配置策略	符合		
3.	入侵检测	查看入侵检测部署及配置	符合		
4.	漏洞扫描	查看漏洞扫描记录	符合		
5.	病毒防治	查看病毒防治日志	符合		
6.	密码机	查看密码机连接方式	符合		

A.5.3. 安全管理

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		

A.5.4. 初始化

序号	测试内容	测试方法	预期结果	测试结果	备注
1.	初始化密钥管理系统	进行密钥管理系统初始化操作	正确进行密钥管理系统初始化		
2.		产生超级管理员	正确产生超级管理员		
3.		产生审计员	正确产生审计员		

A.6. 系统功能

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登录	拒绝登录		
3.	支持多 CA	2个以上CA机构从密钥管理系统申请密钥	每个 CA 均可正确申请加密密钥		
4.	业务管理员管理	增加业务操作员操作	业务操作员被增加		
5.		删除业务操作员操作	业务操作员被删除		
6.		对业务操作员授权操作	正确对业务操作员授权		
7.	密钥生成	定时产生备用密钥：执行指定数量的密钥预生成操作，查看备用库密钥数量	正确预产生密钥，密钥数量相应增加		
8.		即时产生备用密钥：执行指定数量的密钥即时预产生密钥操作，查看备用库密钥数量	正确预产生密钥，密钥数量相应增加		
9.	密钥恢复	在密钥恢复页面由经过授权的司法取证人员进行密钥恢复	成功进行密钥恢复		
10.	密钥撤销	CA 提供密钥撤销服务后，查看在用库状态	在用库状态随之改变		
11.	密钥统计	在用密钥统计：执行在用密钥统计	显示统计结果，获得当前在用密钥数量		
12.		备用密钥统计：执行备用密钥统计，获得当前备用密钥数量	显示统计结果，获得当前备用密钥数量		
13.	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取得查询结果	可以显示相应页面		
14.	审计	任意组合设置条件进行查询：如果存在符合条件的业务日志，则返回日志列表；如果不存在符合条件的业务日志，则返回空结果	可以显示相应页面		

A.7. 系统性能

序号	测试内容	测试方法	预期结果	测试结果	备注
1.	系统性能	运行测试程序	小于 30 秒		

A.8. 数据备份和恢复

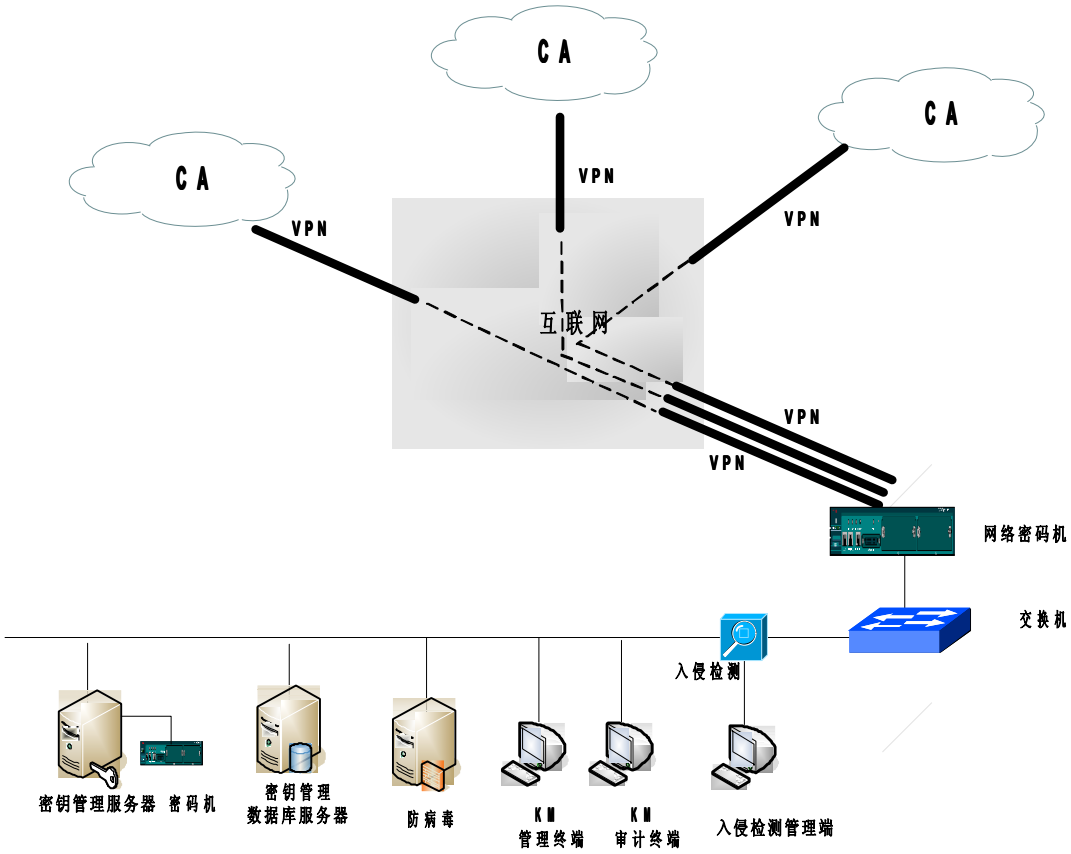
序号	测试内容	测试方法	预期结果	测试结果	备注
1.	备份	查看备份和恢复策略	符合		
2.		查看备份和恢复日志	符合		

A.9. 第三方安全产品

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		
2.	入侵检测	查看相应产品资质证明	符合		
3.	漏洞扫描	查看相应产品资质证明	符合		
4.	病毒防治	查看相应产品资质证明	符合		

附　录　B　证书认证密钥管理系统网络结构图（包括 1 对多 CA）

(资料性附录)

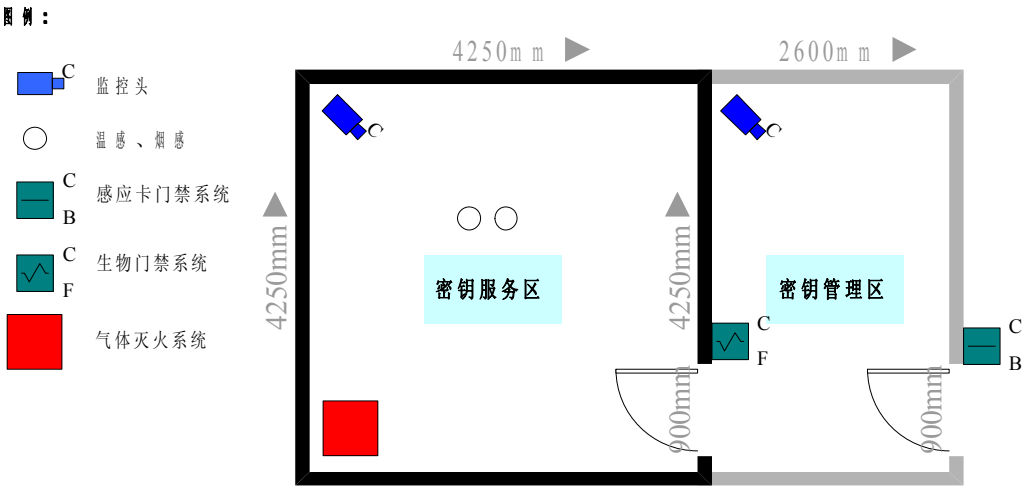


附图 B-1　KM 与多个 CA 的网络连接示意图

附　录　C　证书认证密钥管理系统机房布局及设备位置摆放示例图

(资料性附录)

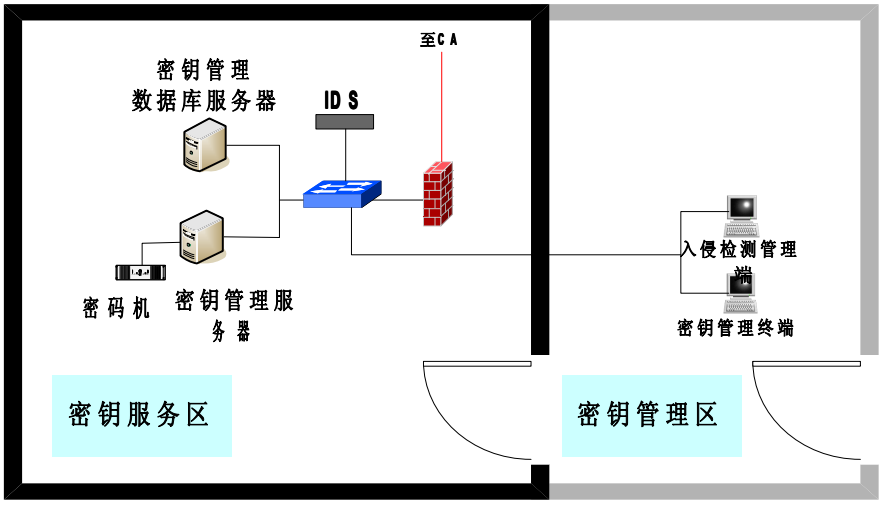
C．1 证书认证密钥管理系统机房布局图



注：此图为KM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

附图 C-1　证书认证密钥管理系统机房布局图

C．2 证书认证密钥管理系统机房位置摆放图



注：此图为KM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

附图 C-2　证书认证密钥管理统机房位置摆放图