ICS 35.040
L 80
备案号:44643—2014

GM

中华人民共和国密码行业标准

GM/T 0038—2014

证书认证密钥管理系统检测规范

Key management of 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。

证书认证密钥管理系统检测规范

1 范围

本标准规定了证书认证密钥管理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密钥管理系统的检测，也可为其他证书认证密钥管理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 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

密钥管理系统 key management system;KM

实现密钥管理功能的系统。

3.3

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 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 GM/T 0034—2014 中第 9 章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

第 7 章的要求，测试的方法应符合第 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 GM/T 0034—2014 中 9.6 对物理安全的要求。

7.1.2 物理区域

KM 的物理区域应划分为密钥服务区和密钥管理区。

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、入侵检测或入侵防御探测设备、漏洞扫描设备；在密钥管理区放置 KM 管理终端、KM 审计终端、入侵检测或入侵防御管理控制台；在各物理区域间应放置防火墙。可参见附录 C。

密钥服务区应为屏蔽机房，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密钥管理区、密钥服务区。

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。

本条仅适用于项目检测。

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，参见附录 B。

网络密码机应是经国家密码管理主管部门审批的产品。

7.2.2 网络配置安全策略

7.2.2.1 防火墙

系统配置的防火墙的主要安全策略为：

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。

7.2.2.2 入侵检测

系统配置的入侵检测的主要安全策略为：

a) 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；

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) 入侵检测探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。

7.2.2.3 漏洞扫描

系统配置的漏洞扫描的主要安全策略为：

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。

7.2.2.4 病毒防治

系统配置的病毒防治的主要安全策略为：

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。

7.2.2.5 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。

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 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，负责本系统的审计员管理。

7.3.3 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。

7.3.4 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，负责用户密钥库的管理、数据备份/恢复等。

7.3.5 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。

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,应分别符合GM/T 0034—2014 中 9.3、9.4 和 9.5 的要求。

应制定相应的管理制度,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。

7.5 系统初始化

KM 的初始化过程为:

a) 生成 KM 的机构密钥并安全备份;

b) 签发 KM 机构证书;

c) 生成超级管理员和审计管理员;

d) 由超级管理员生成业务管理员;

e) 由业务管理员生成业务操作员;

f) 由审计管理员生成审计员。

本条仅用于产品检测。

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。

本条仅用于产品检测。

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 算法和国家密码管理主管部门批准的其他算法的密钥对,预生成的密钥对应安全存放在备用库中。预生成应包括自动和手动两种方式,自动方式应在备用库存放密钥数量少于设定的最低数量时自动补充到规定数量。

7.6.2.2 密钥分发

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。

7.6.2.3 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形式出现在载体之外,加密该密钥的密钥也不能以明文形式出现在载体之外。

应能通过密钥的本地恢复功能来完成司法取证。

7.6.2.4 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。

7.6.2.5 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

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

审计数据应能归档并不能被篡改。

审计过的记录应有明显标记。

7.6.5 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。

业务操作员能够进行其权限范围内的操作。

审计管理员能够添加、删除审计员并能够为其分配权限。

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。

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。

本条仅用于项目检测。

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 7.1.2 的要求。

防火墙配置策略应符合 7.2.2.1 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。

7.9.2 入侵检测

入侵检测产品部署位置应符合 7.1.2 的要求。

入侵检测产品配置策略应符合 7.2.2.2 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。

7.9.3 漏洞扫描

漏洞扫描产品部署应符合 7.1.2 的要求。

漏洞扫描产品配置策略应符合 7.2.2.3 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。

7.9.4 病毒防治

病毒防治产品部署位置应符合 7.1.2 的要求。

病毒防治产品配置策略应符合 7.2.2.4 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。

7.10 文档

证书认证密钥管理系统应配备相关的文档，符合 GM/T 0034—2014 中 11.6 的要求。

8 检测方法

8.1 场地

8.1.1 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。

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 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 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 7.2.2.1 的要求。

8.2.2.2 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 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 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 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 7.2.2.5 的要求。

8.3 岗位及权限管理

8.3.1 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。

8.3.2 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。

8.3.3 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。

8.3.4 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。

8.3.5 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。

8.4 安全管理

查看系统的管理策略和管理制度，应符合 7.4 的要求。

8.5 系统初始化

按 7.5 的要求进行初始化。

8.6 系统功能

8.6.1 支持多个 CA

连接两套 CA 系统，同时为其提供密钥服务，结果应符合 7.6.1 的要求。

8.6.2 密钥管理

8.6.2.1 密钥生成

能够实时生成密钥。

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。

8.6.2.2 密钥分发

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。

8.6.2.3 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 7.6.2.3 的要求。

8.6.2.4 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，密钥数量应有相应的变化，查看日志应有相应的记录。

8.6.2.5 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 7.6.2.5 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 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、记录的签名等信息进行审计操作，结果应符合 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、设置业务管理员权限等操作，结果应符合 7.6.5 的要求。

8.7 系统性能

按照 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 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(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 7.9 的要求。

8.10 文档

查看证书认证密钥管理系统所配备的文档，应符合 7.10 的要求。

9 合格判定

9.1 项目合格判定

7.1.2、7.2.1、7.2.2.5、7.6.2.1、7.6.2.3 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，其他项的检测结果累计 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

7.2.1、7.2.2.5、7.5、7.6.2.1、7.6.2.3 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，其他项的检测结果累计 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
（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 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

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 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		产生审计管理员	正确产生审计管理员		

A.5.5 系统功能

系统功能检测见表 A.5。

表 A.5 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		拔掉登录者证书介质	拒绝操作		

表 A.5（续）

序号	测试内容	测试方法	预期结果	测试结果	备注
4	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		
5	业务管理员管理	增加业务操作员操作	业务操作员被增加		
6		删除业务操作员操作	业务操作员被删除		
7		对业务操作员授权操作	正确对业务操作员授权		
8	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		
9		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		
10	密钥恢复	在密钥恢复页面由经过授权的司法取证人员和有密钥恢复权限的操作员进行密钥恢复	成功进行密钥恢复		
11	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		
12	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		
13		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		
14	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		
15	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		
16		对记录的签名进行验证	可以进行验证		
17		对审计过的记录设置标记	可以设置标记		

A.5.6 系统性能

系统性能检测见表 A.6。

表 A.6 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	系统性能	产生指定数量的密钥，计算每秒钟产生的密钥数	得出密钥对生成时间		

A.5.7 数据备份和恢复

数据备份和恢复检测见表 A.7。

表 A.7 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.8。

表 A.8 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 文档

文档检查见表 A.9。

表 A.9 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）
证书认证密钥管理系统网络结构图(包括一对多 CA)

证书认证密钥管理系统网络结构图如图 B.1 所示。

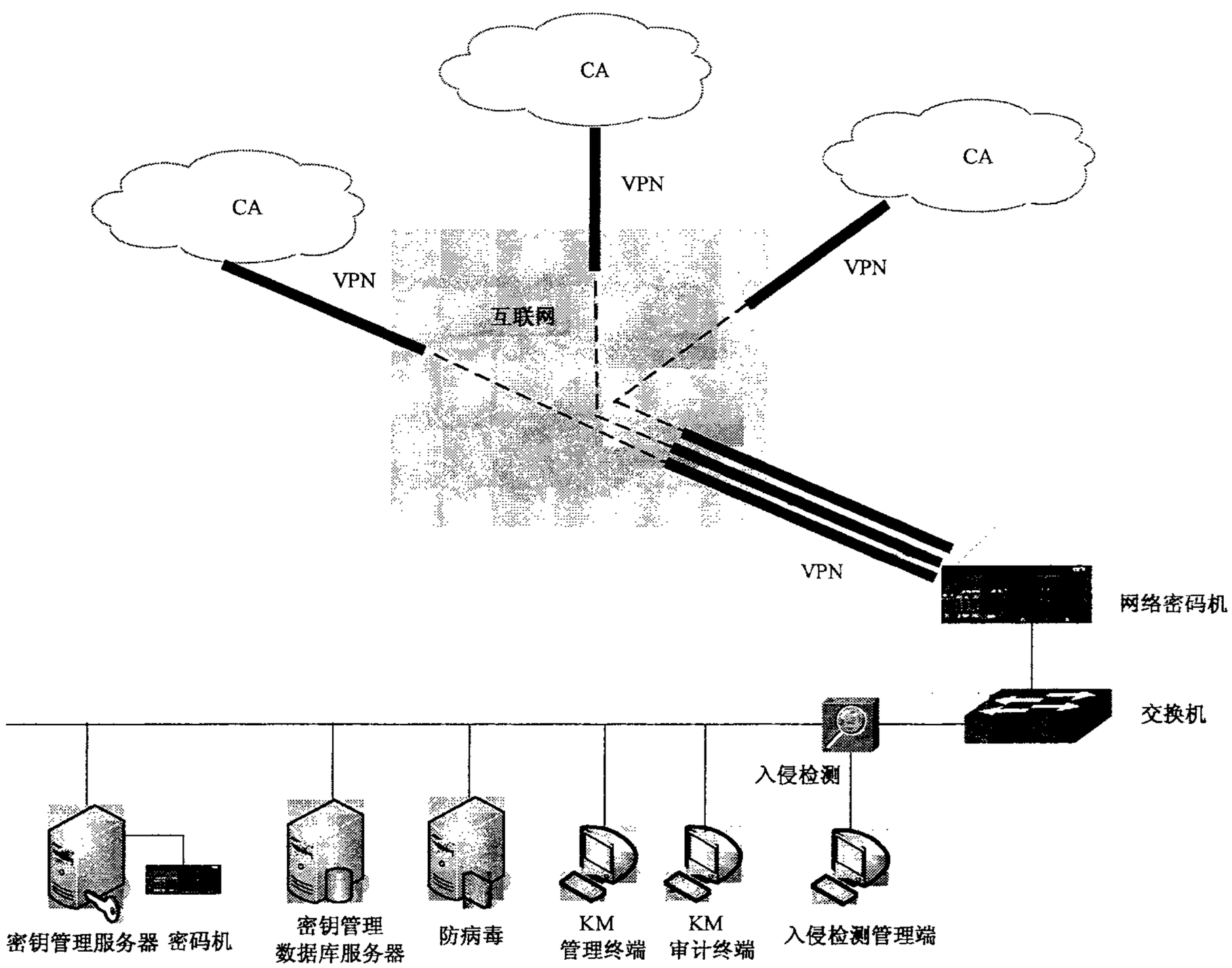
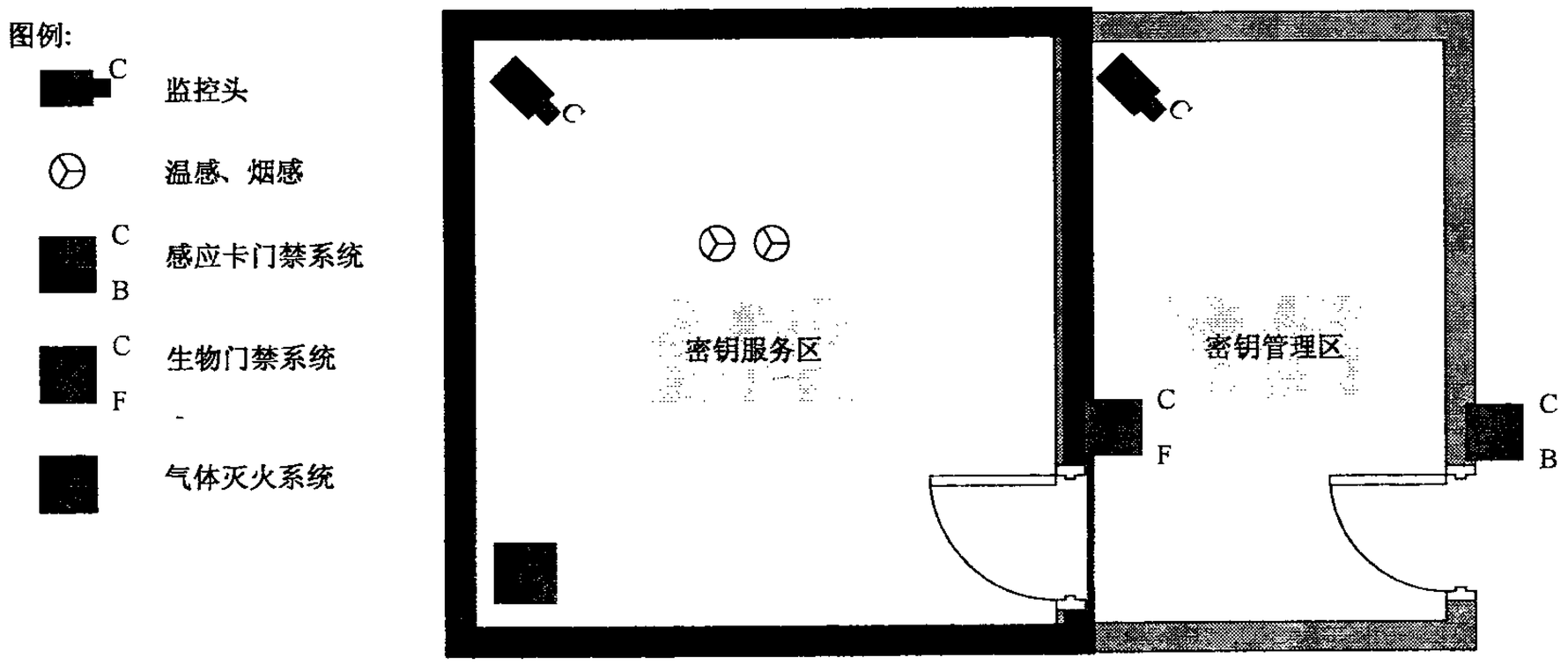


图 B.1 KM 与多个 CA 的网络连接示意图

附 录 C
（资料性附录）
证书认证密钥管理系统机房布局及设备位置摆放示例图

C.1 证书认证密钥管理系统机房布局图

证书认证密钥管理系统机房布局图如图 C.1 所示。

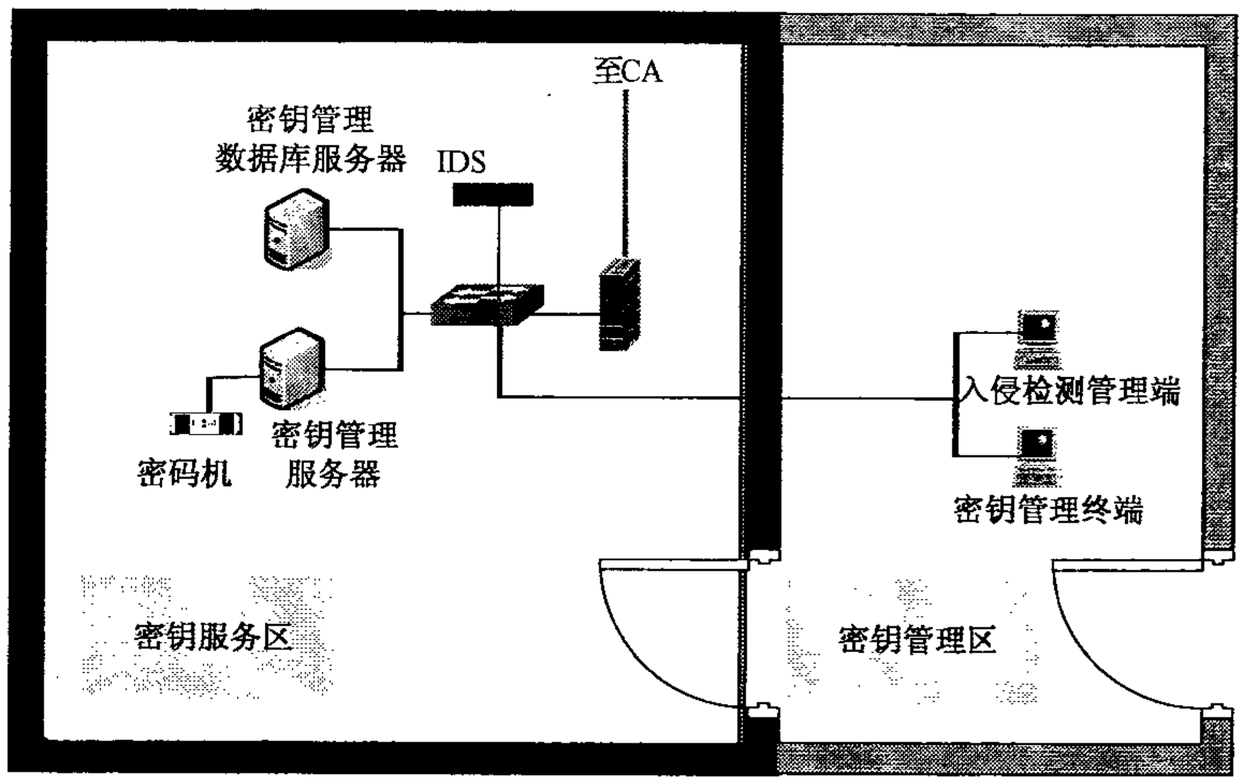


注：此图为 KM 机房示意图，其功能区域应该具备。但是根据机房规模涉及弱电、强电、UPS 间等功能空间应按照用户的现场实际情况划分。

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

证书认证密钥管理系统机房位置摆放图如图 C.2 所示。



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　证书认证密钥管理系统机房位置摆放图

中华人民共和国密码
行业标准
证书认证密钥管理系统检测规范
GM/T 0038—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 1.5 字数 30 千字
2014年5月第一版 2014年5月第一次印刷
*
书号:155066·2-27049

GM/T 0038-2014