

ICS 35.040
L 80
备案号:44643—2014



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	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 检测对象	1
4.1 产品	1
4.2 项目	1
5 测试大纲	1
6 检测环境	2
7 检测内容	2
7.1 场地	2
7.2 网络	2
7.3 岗位及权限管理	3
7.4 安全管理	4
7.5 系统初始化	4
7.6 系统功能	4
7.7 系统性能	5
7.8 数据备份和恢复	5
7.9 第三方安全产品	5
8 检测方法	6
8.1 场地	6
8.2 网络	6
8.3 岗位及权限管理	7
8.4 安全管理	7
8.5 系统初始化	7
8.6 系统功能	7
8.7 系统性能	8
8.8 数据备份和恢复	8
8.9 第三方安全产品	8
8.10 文档	8
9 合格判定	9
9.1 项目合格判定	9
9.2 产品合格判定	9
附录 A (资料性附录) 测试大纲	10
A.1 测试目的	10
A.2 密钥管理系统的物理区域和网络结构	10

A.3	密钥管理系统的软硬件配置	10
A.4	密钥管理系统的模块及功能	10
A.5	测试内容	10
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)	14
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	15
C.1	证书认证密钥管理系统机房布局图	15
C.2	证书认证密钥管理系统机房位置摆放图	15

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