

ICS 35.040  
L 80  
备案号:44642—2014



# 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 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	1
5 检测对象 .....	2
5.1 产品 .....	2
5.2 项目 .....	2
6 测试大纲 .....	2
7 检测环境 .....	2
8 检测内容 .....	2
8.1 场地 .....	2
8.2 网络 .....	3
8.3 岗位及权限管理 .....	4
8.4 安全管理 .....	4
8.5 系统初始化 .....	4
8.6 系统功能 .....	5
8.7 系统性能 .....	7
8.8 数据备份和恢复 .....	7
8.9 第三方安全产品 .....	7
8.10 入根 .....	7
8.11 证书格式 .....	7
8.12 证书链 .....	7
8.13 算法 .....	8
8.14 协议 .....	8
8.15 文档 .....	8
9 检测方法 .....	8
9.1 场地 .....	8
9.2 网络 .....	8
9.3 岗位及权限管理 .....	9
9.4 安全管理 .....	10
9.5 系统初始化 .....	10
9.6 系统功能 .....	10
9.7 系统性能 .....	11
9.8 数据备份和恢复 .....	11
9.9 第三方安全产品 .....	11
9.10 入根 .....	12

9.11	证书格式 .....	12
9.12	证书链 .....	12
9.13	算法 .....	12
9.14	协议 .....	12
9.15	文档 .....	12
10	合格判定 .....	12
10.1	项目合格判定 .....	12
10.2	产品合格判定 .....	12
附录 A (资料性附录)	测试大纲 .....	13
附录 B (资料性附录)	证书认证系统网络结构 .....	19
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 .....	22

## 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)

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