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)