ICS 35.040
L 80
备案号:49742—2015

GM

中华人民共和国密码行业标准

GM/T 0043—2015

数字证书互操作检测规范

Test specification for digital certificate interoperability

2015-04-01 发布　　2015-04-01 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：国家密码管理局商用密码检测中心、中金金融认证中心有限公司、卓望数码技术(深圳)有限公司、北京数字认证股份有限公司、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、北京国富安电子商务安全认证有限公司。

本标准主要起草人：李大为、赵宇、李志伟、罗干生、薛迎俊、邓开勇、周笔、田敏求、李冬、肖秋林、韩亚宁、谭武征、李丽仙、霍云、商晋、赵丽丽、常玉明。

数字证书互操作检测规范

1 范围

本标准依据 GM/T 0015 和 GM/T 0034 的要求规定了数字证书互操作的检测内容与检测方法。

本标准适用于证书认证系统签发的数字证书的检测。

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。

GB/T 16264.8—2005 信息技术 开放系统互连 目录 第 8 部分：公钥和属性证书框架

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0034 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

GM/Z 4001 密码术语

PKCS＃10 (v1.7) Certification Request Syntax Standard 认证请求语法标准

3 术语和定义

GM/Z 4001 所界定的以及下列术语和定义适用于本文件。

3.1

证书认证系统 certificate authentication system

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

证书认证机构 certification authority

对数字证书进行全生命周期管理的实体。也称为电子认证服务机构。

3.3

证书撤销列表 certificate revocation list

由证书认证机构 (CA)签发并发布的被撤销证书的列表。

3.4

数字证书 digital certificate

也称公钥证书，由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.5

根 CA root CA

整个国家 PKI 信任体系的顶点，为运营 CA 签发 CA 证书，并对运营 CA 进行监督管理。