ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0043—2024
代替 GM/T 0043—2015

数字证书互操作检测规范

Test specification for digital certificate interoperability

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GM/T 0043—2015《数字证书互操作检测规范》，与GM/T 0043—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了OCSP符合性检测内容（见6.2.4）；

——更改了终端实体证书中应存在密钥用法扩展域的描述（见6.2.2，2015年版的6.2.2）；

——增加了对“基本限制”项的检测内容（见6.3.1）；

——增加了OCSP符合性检测方法（见7.2.4）。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：商用密码检测认证中心、格尔软件股份有限公司、北京数字认证股份有限公司、北京国富安电子商务安全认证有限公司、中金金融认证中心有限公司、卓望数码技术（深圳）有限公司、长春吉大正元信息技术股份有限公司。

本文件主要起草人：张立花、肖秋林、郑强、商晋、王小飞、张绍博、谢宗晓、黄福飞、王巍、丁肇伟

本文件及其所代替文件的历次版本发布情况为：

——2015年首次发布为GM/T 0043—2015；

——本次为第一次修订。

数字证书互操作检测规范

1 范围

本文件规定了数字证书互操作的送检技术文档要求、检测内容、检测方法以及判定规则。

本文件适用于对数字证书互操作检测进行指导。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 19713 网络安全技术 公钥基础设施 在线证书状态协议

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—2023 数字证书格式

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0018 密码设备应用接口规范

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/T 0092 基于 SM2 算法的证书申请语法规范

GM/Z 4001 密码术语

3 术语和定义

GM/T 0034、GM/T 0015—2023 和 GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

国家根 CA national root CA

整个国家 PKI 信任体系的顶点。

注：为证书认证机构签发 CA 证书，并对接入国家根 CA 的证书认证机构进行监督管理。

3.2

证书互操作 digital certificate interoperability

两个以上(含)证书实体之间进行加解密或签名验签的一种能力。

4 缩略语

下列缩略语适用于本文件。

CA：证书认证机构(Certification Authority)

CRL：证书撤销列表(Certificate Revocation List)

DN：可辨别名(Distinguished Name)

OCSP：在线证书状态协议(Online certificate status protocol)