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)

OID:对象标识符(Object Identify)
PKI:公钥基础设施(Public Key Infrastructure)
URL:统一资源定位符(Uniform Resource Locator)

5 送检技术文档要求

证书认证机构提交的文档资料应包含但不限于以下内容。

a) CA 证书申请数据文件。
b) 证书认证机构的证书认证系统(以下简称“CA 系统”)结构说明:
   1) 以结构图的形式,说明整个 CA 系统的框架结构,包括 CA 系统的各子系统的构成、各子系统的功能和各子系统的实现原理,并附以详细的文字说明;
   2) 以拓扑图的形式,说明整个 CA 系统硬件系统结构情况,并附以详细的文字说明;
   3) 详细描述 CA 系统的安全机制、密码体制,以及密钥使用情况。
c) CA 系统签发数字证书说明:
   1) 描述 CA 系统签发数字证书的机制和签发的数字证书种类,说明各类数字证书的格式;
   2) 说明 CA 系统签发的各类数字证书的应用范围。
d) CA 系统发布子系统说明:
   详细描述发布子系统的结构、部署方式,数字证书和数字证书注销列表的发布方式和策略。
e) CA 系统使用密码算法的清单。

6 检测内容

6.1 入根检测

6.1.1 CA 证书申请功能

CA 系统应具备 CA 证书申请功能,其内容应包括:

a) 产生证书申请文件,应可以在申请时输入可辨别名(DN)中的相关信息;
b) 将申请文件导出。

6.1.2 CA 证书申请文件符合性

CA 证书申请文件应符合以下要求。

a) 应符合 GM/T 0092 格式要求,申请文件内容由申请信息、签名算法标识和对申请信息的数字签名组成。其中申请信息由可辨别名(DN),公钥和其他属性组成。申请文件的结构描述应符合 GM/T 0092 格式要求。
b) 对 CA 证书申请文件进行签名应使用 SM2 算法,涉及 SM2 算法的公钥和签名部分应符合 GM/T 0009,其中相关算法标识应符合 GM/T 0006。其中包括:
   1) 签名算法 OID 应为 1.2.156.10197.1.501;
   2) DN 项及编码要求:
      对于运营 CA 使用的证书中 DN 项的构造顺序符合 GM/T 0034,编码格式应符合如下要求:
      ——C 项应使用 PrintableString 编码;
      ——如果存在 E 项,应采用 IA5String 编码;
      ——未做约定的其他项,应采用 UTF8String 编码。

c) CA 证书申请文件的签名应有效。

6.1.3 CA 证书导入功能

证书认证机构的 CA 系统应支持将国家根 CA 签发出的 CA 证书导入至系统中。

6.1.4 入根后签发功能

入根后的 CA 系统应具备证书签发等功能，其中包括：

a) 签发终端实体证书，按照 GM/T 0034 要求，应能使用国家根 CA 为证书认证机构签发的 CA 证书成功签发终端实体证书；
b) 签发 CRL，应能使用国家根 CA 为证书认证机构签发的 CA 证书成功签发 CRL；
c) 提供证书、证书信任链和 CRL 的查询和下载服务。

6.2 数字证书和 CRL 格式符合性检测

6.2.1 数字证书基本域符合性

CA 系统所签发的终端实体证书，其证书基本域应符合 GM/T 0015—2023，其中包括：

a) 终端实体证书的版本应为 V3；
b) 终端实体证书的序列号长度应不大于 20 个 8 位字节，应为唯一正整数；
c) 终端实体证书的签名算法 OID 应为 1.2.156.10197.1.501；
d) 终端实体证书的证书主题的构造顺序见 GM/T 0034，编码格式应符合如下要求：
   ——C 项应使用 PrintableString 编码，
   ——如果存在 E 项，应采用 IA5String 编码，
   ——未做约定的其他项，应采用 UTF8String 编码；
e) 终端实体证书的有效期编码规则为，在 2049 年之前（包括 2049 年）应将该时间编码为 UTCTime 类型，在 2050 年之后，编码为 GeneralizedTime 类型，生效期应早于失效期；
f) 签名证书的主题与加密证书的主题应完全一致。

6.2.2 数字证书扩展域符合性

CA 系统所签发的终端实体证书，其证书扩展域应符合 GM/T 0015—2023，其中包括：

a) 终端实体证书中应存在颁发机构密钥标识符扩展域，其中的值应与发行者证书的使用者密钥标识符中的值一致；
b) 终端实体证书中应存在使用者密钥标识符扩展域，该值应与证书中使用者公钥计算结果一致；
c) 终端实体证书中应存在密钥用法扩展域，其中用户签名证书的密钥用法中应标识且只应标识数字签名 digitalSignature、防抵赖 nonRepudiation 一项或两项，用户加密证书的密钥用法中应标识且只应标识密钥加密 keyEncipherment、数据加密 dataEncipherment、密钥协商 keyAgreement（可选）；
d) 终端实体证书中如果存在扩展密钥用法扩展域，扩展密钥用法中的用途不应与密钥用法扩展域中的定义冲突；
e) 终端实体证书中如果存在私有密钥使用期扩展域，该使用期不应大于证书有效期；
f) 终端实体证书中如果存在证书策略扩展域，通过该扩展域中存储的 URL 可以访问到互联网内容；
g) 终端实体证书中应存在 CRL 发布点扩展域，根据 CRL 发布点扩展域中的 URL，应可以下载到对应的 CRL 文件，CRL 应符合 GM/T 0015—2023 的 5.3 CRL 格式要求，其颁发者应与终

端实体证书的颁发者一致，且 CRL 中的签名值应能使用终端实体证书的颁发者证书进行验证；

h) 终端实体证书中如果存在机构信息访问扩展域，则通过此扩展可获得终端实体证书的颁发者证书；

i) 终端实体证书中如果存在其他可选扩展域，其使用应符合 GM/T 0015—2023 的要求。

6.2.3 CRL 格式符合性

CA 系统所签发的 CRL，其格式应符合 GM/T 0015—2023，其中包括：

a) CRL 的版本应为 V2；

b) CRL 的签名算法 OID 应为 1.2.156.10197.1.501；

c) CRL 的签发者主题的构造顺序、编码格式应与签发者的证书中的主题完全一致；

d) CRL 的生效日期与下次更新日期编码规则为，在 2049 年之前（包括 2049 年）应将该时间编码为 UTCTime 类型，在 2050 年之后，编码为 GeneralizedTime 类型，生效期应早于失效期；

e) CRL 文件的签名应有效。

6.2.4 OCSP 符合性

如果 CA 系统提供 OCSP 证书状态查询服务，OCSP 对外请求/响应格式应符合 GB/T 19713 的要求，其中包括以下内容。

请求检测：

a) OCSP 协议版本为 V1；

b) 指定请求者名称；

c) 目标证书杂凑算法 OID 应为 1.2.156.10197.1.401；

d) 请求报文使用的签名算法 OID 应为 1.2.156.10197.1.501；

e) 支持 get/post 请求。

响应检测：

a) OCSP 返回的证书状态应符合 Good、Revoked、Unknown 三种状态之一；

b) 响应报文使用的签名算法 OID 应为 1.2.156.10197.1.501；

c) OCSP 响应签名证书中，extKeyUsage 扩展域中应包含 id-kp-OCSPSigning OID；

d) OCSP 响应应包括生成时间、本次更新时间、下次更新时间（可选）。编码规则为，在 2049 年之前（包括 2049 年）应将该时间编码为 UTCTime 类型，在 2050 年之后，编码为 GeneralizedTime 类型，生效期应早于失效期；

e) 目标证书杂凑算法 OID 应为 1.2.156.10197.1.401。

6.3 数字证书互操作检测

6.3.1 证书信任链建立

CA 系统所签发的终端实体证书，应支持与国家根 CA 及国家根 CA 签发的对应证书认证机构的 CA 证书建立完整的信任链，其中包括：

a) 由国家根 CA 签发的证书认证机构 CA 证书的颁发者应与国家根 CA 证书使用者信息一致，包括 DN 顺序、编码格式等；

b) 终端实体证书的颁发者应与由国家根 CA 签发的证书认证机构 CA 证书使用者信息一致，包括 DN 顺序、编码格式等；

c) 由国家根 CA 签发的证书认证机构 CA 证书的颁发机构密钥标识符应与国家根 CA 证书使用

者密钥标识符一致；

d) 终端实体证书的颁发机构密钥标识符应与由国家根 CA 签发的证书认证机构 CA 证书使用者密钥标识符一致；

e) 整个证书链上所有证书的签名应有效；

f) 整个证书链上所有证书的有效期和证书状态都应正常；

g) 证书中如果存在“基本限制”，内容应符合 GM/T 0015—2023 的 5.2.4.2.12 基本限制扩展要求。

签名证书与加密证书均需要进行信任链建立检测。

6.3.2 签名证书互操作

CA 系统签发终端实体证书的载体采用经过商用密码检测认证的智能密码钥匙或其他硬件密码模块，CA 系统签发给实体的证书，应和实体提交的证书请求包含同样的公钥，使用签名证书公私钥对进行签名验签运算时，调用的密码应用接口应符合 GM/T 0016 或 GM/T 0018，智能密码钥匙或其他硬件密码模块通过调用此接口完成签名验签互操作检测。其中包括：

a) SM2 密钥数据格式应符合 GM/T 0009；

b) SM2 签名数据格式应符合 GM/T 0009；

c) 使用 SM2 私钥对输入数据签名时，该输入数据为待签数据经过 SM2 签名预处理的结果，签名过程应符合 GM/T 0009；

d) 使用 SM2 公钥对输入数据验签时，该输入数据为待签数据经过 SM2 签名预处理的结果，验签过程应符合 GM/T 0009。

6.3.3 加密证书互操作

CA 系统签发终端实体证书的载体采用经过商用密码检测认证的智能密码钥匙或其他硬件密码模块，CA 系统签发给实体的证书，应和实体提交的证书请求包含同样的公钥，使用加密证书公私钥对进行加解密运算时，调用的密码应用接口应符合 GM/T 0016 或 GM/T 0018，智能密码钥匙或其他硬件密码模块通过调用此接口完成加解密互操作检测。其中包括：

a) SM2 密钥数据格式应符合 GM/T 0009；

b) SM2 加密数据格式应符合 GM/T 0009；

c) 密钥对保护数据格式应符合 GM/T 0009；

d) 使用 SM2 公钥对输入数据加密时，加密过程应符合 GM/T 0009；

e) 使用 SM2 私钥对输入数据解密时，解密过程应符合 GM/T 0009。

7 检测方法

7.1 入根检测

7.1.1 CA 证书申请功能

查看 CA 系统产生并导出 CA 证书申请文件的功能，检测结果应符合 6.1.1 的要求。

7.1.2 CA 证书申请文件符合性

CA 系统向国家根 CA 提交 CA 证书申请文件，证书申请文件采用 DER 编码，并转化为 Base64 编码。对 CA 证书申请文件内容及格式进行检测，检测结果应符合 6.1.2 的要求。

7.1.3 CA 证书导入功能

国家根 CA 根据 CA 系统产生的 CA 证书申请文件为其签发二级 CA 证书。查看 CA 系统导入二级 CA 证书的功能，检测结果应符合 6.1.3 的要求。

7.1.4 入根后签发功能

CA 系统使用二级 CA 证书签发 CRL 和各类终端实体证书。查看 CA 系统签发数字证书和 CRL 文件的功能，以及 CA 系统提供数字证书、证书信任链、CRL 文件查询下载的功能，检测结果应符合 6.1.4 的要求。

7.2 数字证书和 CRL 格式符合性检测

7.2.1 数字证书基本域符合性

读取存储在智能密码钥匙或其他硬件密码模块中的终端实体证书，然后对数字证书基本域内容及格式进行检测，检测结果应符合 6.2.1 的要求。

7.2.2 数字证书扩展域符合性

读取存储在智能密码钥匙或其他硬件密码模块中的终端实体证书，然后对数字证书扩展域内容及格式进行检测，检测结果应符合 6.2.2 的要求。

7.2.3 CRL 格式符合性

根据终端实体证书中的 CRL 地址，下载 CRL 文件，然后对 CRL 内容及格式进行检测，检测结果应符合 6.2.3 的要求。

7.2.4 OCSP 符合性

根据终端实体证书中的 OCSP 地址或证书认证机构发布的 OCSP 地址，对 CA 系统签发的终端实体证书进行在线实时状态查询，OCSP 请求与响应的检测结果应符合 6.2.4 的要求。

7.3 数字证书互操作检测

7.3.1 证书信任链建立

根据 CA 系统提供的证书下载方式，下载国家根 CA 证书和由国家根 CA 为 CA 系统签发的二级 CA 证书。读取智能密码钥匙或其他硬件密码模块中的终端实体证书，然后进行证书信任链建立检测，检测结果应符合 6.3.1 的要求。

7.3.2 签名证书互操作

由两个不同的 CA 系统(其中一个是被测 CA 系统)分别为证书用户 A 和证书用户 B 签发数字证书，并存储在智能密码钥匙或其他硬件密码模块中。

读取存储在智能密码钥匙或其他硬件密码模块中的证书用户 A 的签名证书 ScertA 和证书用户 B 的签名证书 ScertB。

证书用户 A 使用签名证书 ScertA 对应的私钥对随机产生的数据进行数字签名，然后将数字签名后的数据发送给证书用户 B，证书用户 B 使用签名证书 ScertA 的公钥对数据进行签名验证，应能验证成功。通信双方在验签过程中证书状态和证书信任链应能验证通过，检测结果应符合 6.3.2 的要求。

证书用户 B 使用签名证书 ScertB 对应的私钥对随机产生的数据进行数字签名，然后将签名后的数

据发送给证书用户 A，证书用户 A 使用签名证书 ScertB 的公钥对数据进行签名验证，应能验证成功。通信双方在验签过程中证书状态和证书信任链应能验证通过，检测结果应符合 6.3.2 的要求。

7.3.3 加密证书互操作

由两个不同的 CA 系统（其中一个是被测 CA 系统）分别为证书用户 A 和证书用户 B 签发数字证书，并存储在智能密码钥匙或其他硬件密码模块中。

从智能密码钥匙或其他硬件密码模块中，读取证书用户 A 的加密证书 EcertA 和证书用户 B 的加密证书 EcertB。

用户 A 产生会话密钥，并使用该密钥对随机产生的数据进行加密，然后使用加密证书 EcertB 对应的公钥对会话密钥进行加密，最后将密文数据发送给证书用户 B。证书用户 B 收到密文数据后，先使用加密证书 EcertB 的私钥解密会话密钥，然后用会话密钥解密密文数据，应能解密成功。通信双方在加解密过程中证书状态和证书信任链应能验证通过，检测结果应符合 6.3.3 的要求。

用户 B 产生会话密钥，并使用该密钥对随机产生的数据进行加密，然后使用加密证书 EcertA 对应的公钥对会话密钥进行加密，最后将密文数据发送给证书用户 A。证书用户 A 收到密文数据后，先使用加密证书 EcertA 的私钥解密会话密钥，然后用会话密钥解密密文数据，应能解密成功。通信双方在加解密过程中证书状态和证书信任链应能验证通过，检测结果应符合 6.3.3 的要求。

8 判定规则

如 CA 系统提供 OCSP 证书状态查询服务，本文件中所有的检测内容均为关键项，其中任何一项检测结果不符合相应检测要求的，即判定为不合格；如 CA 系统不提供 OCSP 证书状态查询服务，除 6.2.4 外，本文件其余检测内容均为关键项，其中任何一项检测结果不符合相应检测要求的，即判定为不合格。

中华人民共和国密码
行业标准
数字证书互操作检测规范
GM/T 0043—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 17 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39086　定价 31.00 元

如有印装差错　由本社发行中心调换
版权专有　侵权必究
举报电话:(010)68510107

GM/T 0043-2024