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

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—2015
*
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)
北京市西城区三里河北街16号(100045)
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 18 千字
2015年7月第一版 2015年7月第一次印刷
*
书号:155066·2-28790 定价 18.00 元

GM/T 0043-2015

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。

3.6

运营 CA　operating CA

国家根 CA 下所有提供第三方电子认证服务的 CA。

3.7

CA 证书　CA certificate

颁发给数字证书认证机构的证书。

3.8

终端实体证书　entity certificate

也称为用户证书，是由数字证书认证机构签发的个人证书、机构证书、设备证书等。

4　符号和缩略语

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　甄别名(Distinguished Name)

OID　对象标识符(Object Identify)

PKCS　公钥密码格式标准(Public Key Cryptography Standards)

PKI　公钥基础设施(Public Key Infrastructure)

RA　证书注册机构(Registration Authority)

URL　统一资源定位符(Uniform Resource Locator)

5　送检技术文档要求

送检单位提交的文档资料应包含但不限于以下内容：

a)　证书认证系统 CA 证书申请数据文件(数字证书制作数据，以光盘形式提交)。

b)　证书认证系统结构说明：

1)　以结构图的形式，说明整个证书认证系统的框架结构，包括证书认证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，说明整个证书认证系统硬件系统结构情况，并附以详细的文字说明；

3)　详细描述证书认证系统的安全机制、密码体制，以及密钥使用情况。

c)　证书认证系统签发数字证书说明：

1)　描述证书认证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和应用范围；

2)　证书认证系统签发的数字证书的使用说明。

d)　证书认证系统发布子系统说明：详细描述发布子系统的结构、部署，数字证书和数字证书注销列表的发布方式和策略。

e)　证书认证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 证书申请功能检测

运营 CA 的证书认证系统(以下简称“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甄别名(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检测

CA 证书申请文件应符合以下要求:

a) 符合 PKCS#10 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。其中申请信息由可甄别名(DN)、公钥和其他属性组成。申请文件的结构描述参见附录 A。

b) CA 证书申请文件应使用 SM2 算法,涉及 SM2 算法的公钥和签名部分应符合 GM/T 0009 的要求,其中相关算法标识符合 GM/T 0006 的要求。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(以 Windows 系统下所看到证书的 DN 顺序为准)、编码格式应符合如下要求:

——最后一项必须是 C=CN;

——如果有 CN 项,需要放在 DN 的最前面;

——其他项按照从小到大的顺序排列:如同时存在 OU 和 O 项,OU 在 O 之前,同时存在 S 和 L 项,L 在 S 前面;

——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) 应能成功验证 CA 证书申请文件中的签名值。

6.1.3 CA 证书导入功能检测

运营 CA 的 CA 系统应支持将根 CA 签发出的 CA 证书导入至系统中。

6.1.4 入根后签发功能检测

入根后的 CA 系统应具备证书签发等功能,其中包括:

a) 签发用户证书,应能使用根 CA 签发的二级 CA 证书成功签发用户证书(双证);

b) 签发 CRL,应能使用根 CA 签发的二级 CA 证书成功签发 CRL;

c) 提供证书、证书链和 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 数字证书基本项符合性检测

CA 系统所签发的用户证书,其证书格式应符合 GM/T 0015 和 GB/T 16264.8—2005 的要求,其中包括:

a) 用户证书应能使用 X.509 格式解码。

b) 用户证书的版本应为 V3。

c) 用户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。

d) 用户证书的签名算法 OID 应为 1.2.156.10197.1.501。

e) 用户证书的用户主题的构造顺序(以 Windows 系统下所看到证书的 DN 顺序为准)、编码格式应符合如下要求：

——最后一项必须是 C=CN；

——如果有 CN 项，需要放在 DN 的最前面；

——其他项按照从小到大的顺序排列：如同时存在 OU 和 O 项，OU 在 O 之前，同时存在 S 和 L 项，L 在 S 前面；

——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。

f) 用户证书的有效期编码规则为，在 2049 年之前(包括 2049 年)必须将该时间编码为 UTCTime 类型，在 2050 年之后，编码为 GeneralizedTime 类型，生效期必须早于失效期。

g) 签名证书的主题与加密证书的主题应完全一致。

6.2.2 数字证书扩展项符合性检测

CA 系统所签发的用户证书，其证书扩展项应符合 GM/T 0015 和 GB/T 16264.8—2005 的要求，其中包括：

a) 用户证书中必须存在颁发机构密钥标识符扩展项，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) 用户证书中必须存在使用者密钥标识符扩展项，该值应与证书中使用者公钥计算结果一致；

c) 用户证书中必须存在密钥用法扩展项，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 和防抵赖 nonRepudiation 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 和密钥协商 keyAgreement 3 项；

d) 用户证书中如果存在扩展密钥用法扩展项，需要检测确认扩展密钥用法中的用途不能与密钥用法扩展项中的定义冲突；

e) 用户证书中如果存在私有密钥使用期扩展项，该使用期不应大于证书有效期；

f) 用户证书中如果存在证书策略扩展项，通过该扩展项中存储的 URL 可以访问到互联网内容；

g) 用户证书中必须存在 CRL 发布点扩展项，根据 CRL 发布点扩展项中的 URL，应可以下载到对应的 CRL 文件，CRL 应符合 X.509 V2 标准，其颁发者应与用户证书的颁发者一致，且 CRL 中的签名值应能使用用户证书的颁发者证书进行验证；

h) 用户证书中如果存在机构信息扩展项，则通过此扩展项可获得用户证书的颁发者证书；

i) 用户证书中如果存在其他可选扩展项，其使用应符合 GM/T 0015 的要求。

6.2.3 CRL 格式符合性检测

CA 系统所签发的 CRL，其格式应符合 GM/T 0015 和 GB/T 16264.8—2005 的要求，其中包括：

a) CRL 应能使用 X.509 格式解码；

b) CRL 的版本应为 V2；

c) CRL 的签名算法 OID 应为 1.2.156.10197.1.501；

d) 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；

e) 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)必须将该时间编

码为 UTCTime 类型，在 2050 年之后，编码为 GeneralizedTime 类型，生效期必须早于失效期；

f) 应能成功验证 CRL 文件中的签名值。

6.3 数字证书互操作检测

6.3.1 证书信任链建立检测

CA 系统所签发的用户证书，应能够与根 CA 及根 CA 签发的对应二级 CA 建立完整的信任链，其中包括：

a) 二级 CA 证书的颁发者应与根 CA 证书使用者信息一致，包括 DN 顺序、编码格式等；

b) 用户证书的颁发者应与二级 CA 证书使用者信息一致，包括 DN 顺序、编码格式等；

c) 二级 CA 证书的颁发机构密钥标识符应与根 CA 证书使用者密钥标识符一致；

d) 用户证书的颁发机构密钥标识符应与二级 CA 证书使用者密钥标识符一致；

e) 能够成功验证整个证书链上所有证书的签名值；

f) 整个证书链上所有证书的有效期和证书状态都应正常。

签名证书与加密证书均需要进行信任链建立检测。

6.3.2 签名证书互操作检测

CA 系统签发的智能密码钥匙，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 的要求，智能密码钥匙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 的要求；

b) SM2 签名数据格式应符合 GM/T 0009 的要求；

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 的要求；

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 的要求。

6.3.3 加密证书互操作检测

CA 系统签发的智能密码钥匙，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 的要求，智能密码钥匙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 的要求；

b) SM2 加密数据格式应符合 GM/T 0009 的要求；

c) 密钥对保护数据格式应符合 GM/T 0009 的要求；

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

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

7 检测方法

7.1 入根检测

7.1.1 CA 证书申请功能检测

CA 系统执行 CA 证书申请操作，查看系统执行结果，结果应符合 6.1.1 的要求。

7.1.2 CA 证书申请文件符合性检测

CA 系统向根 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 证书申请文件进行符合性检测，检测结果应符合 6.1.2 的要求。

7.1.3 CA 证书导入功能检测

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。CA 系统执行 CA 证书导入操作，将二级 CA 证书导入系统中，查看 CA 日志，结果应符合 6.1.3 的要求。

7.1.4 入根后签发功能检测

CA 系统使用二级 CA 证书签发 CRL 和各类用户证书。在 RA 进行证书申请和下载操作，查看 CA 日志，访问 CA 发布系统进行证书的查询，下载证书链和 CRL，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 数字证书基本项符合性检测

读取存储在智能密码钥匙中的用户证书，然后进行数字证书基本项符合性检测，检测结果应符合 6.2.1的要求。

7.2.2 数字证书扩展项符合性检测

读取存储在智能密码钥匙中的用户证书，然后进行数字证书扩展项符合性检测，检测结果应符合 6.2.2 的要求。

7.2.3 CRL 格式符合性检测

根据用户证书中的 CRL 地址，下载 CRL 文件，然后进行 CRL 格式符合性检测，检测结果应符合 6.2.3 的要求。

7.3 数字证书互操作检测

7.3.1 证书信任链建立检测

根据 CA 系统提供的证书下载方式下载根证书和二级 CA 证书，读取智能密码钥匙中用户证书，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 签名证书互操作检测

通过建立两个用户 A 和 B，分别与用户签名证书 ScertA 和 ScertB 绑定。

用户 A 使用证书 ScertA 对应的私钥对一段数据进行签名，然后将签名后的数据发送给用户 B，用户 B 使用证书 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。

用户 B 使用证书 ScertB 对应的私钥对一段数据进行签名，然后将签名后的数据发送给用户 A，用户 A 使用证书 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 加密证书互操作检测

通过建立两个用户 A 和 B，分别与用户加密证书 EcertA 和 EcertB 绑定。

用户 A 首先产生会话密钥，并用该密钥对一段数据进行加密，然后使用证书 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用户 B。用户 B 收到密文数据后，先使用证书 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 首先产生会话密钥，并用该密钥对一段数据进行加密，然后使用证书 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用户 A。用户 A 收到密文数据后，先使用证书 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 合格判定

本标准中所有的检测项目均为关键项，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。

附 录 A
（资料性附录）
CA 证书申请文件 ASN.1 结构

```
CertificationRequest ::= SEQUENCE {
    certificationRequestInfo    CertificationRequestInfo,
    signatureAlgorithm          AlgorithmIdentifier{{ SignatureAlgorithms }},
    signature                   BIT STRING
}
CertificationRequestInfo ::= SEQUENCE {
    version                     INTEGER { v1(0) } (v1,...),
    subject                     Name,
    subjectPKInfo               SubjectPublicKeyInfo{{ PKInfoAlgorithms }},
    attributes                  [0] IMPLICIT Attributes{{ CRIAttributes }} }

SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm                   AlgorithmIdentifier,
    subjectPublicKey            BIT STRING }

AlgorithmIdentifier ::= SEQUENCE {
    algorithm                   OBJECT IDENTIFIER,
    parameters                  ANY DEFINED BY algorithm OPTIONAL }
                                    -- contains a value of the type
                                    -- registered for use with the
                                    -- algorithm object identifier value
```

subjectPublicKeyInfo 描述需要被认证的公钥的信息，包括公钥算法标识和公钥的比特串。当使用 SM2 椭圆曲线公钥密码算法时，其算法 OID 为 1.2.156.10197.1.301。