



# 中华人民共和国国家标准

GB/T 19771—2025

代替 GB/T 19771—2005

## 网络安全技术 公钥基础设施 PKI 组件最小互操作规范

Cybersecurity technology—Public key infrastructure—  
Specification for minimum interoperability for PKI components

2025-08-01 发布

2026-02-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会



目 次

前言 ..... III

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 2

5 最小互操作基本功能要求 ..... 3

    5.1 概述 ..... 3

    5.2 CA 系统 ..... 3

    5.3 RA 系统 ..... 4

    5.4 证书持有者 ..... 5

    5.5 证书验证者 ..... 5

    5.6 密码算法 ..... 6

6 互操作事务数据格式要求 ..... 6

    6.1 总体要求 ..... 6

    6.2 注册请求 ..... 6

    6.3 证书密钥更新 ..... 10

    6.4 撤销请求 ..... 11

    6.5 访问资料库 ..... 13

7 测试评价方法 ..... 13

    7.1 通用测试评价方法 ..... 13

    7.2 最小互操作基本功能测试评价方法 ..... 13

    7.3 互操作数据格式测试评价方法 ..... 15





## 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 GB/T 19771—2005《信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范》，与 GB/T 19771—2005 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了“范围”的内容，重新界定了文件的标准化对象和所覆盖的各个方面，并更改了文件的适用界限(见第1章，2005年版的第1章)；
- b) 更改了 PKI 四个组件的基本功能要求(见第5章，2005年版的第5章)，增加了对 BYOD 请求证书的功能要求(见 5.3.2、5.4.2)，增加了验证证书的最小步骤要求(见 5.2.2)，增加了对商用密码算法的支持(见 5.6)；
- c) 更改了互操作事务数据格式的要求，将对数字证书的数据结构、证书扩展、证书撤销列表的格式要求修改为符合 GB/T 20518—2018(见 6.1，2005年版的 6.1、6.2、6.3)；将对 PKI 事务消息格式的内容的要求修改为符合 GB/T 19714—2025(见 6.1，2005年版的 6.5)；更改了 PKI 事务的消息内容(见第6章，2005年版的 6.6)；
- d) 增加了对 CA 系统、RA 系统、证书持有者、证书验证者功能的测试评价方法，增加了互操作数据格式测试评价方法(见第7章)；
- e) 删除了规范性附录 A、规范性附录 B、规范性附录 C、规范性附录 D(见 2005 版的附录 A、附录 B、附录 C、附录 D)。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国科学院大学、北京数字认证股份有限公司、公安部第三研究所、中国科学院软件研究所、长春吉大正元信息技术股份有限公司、安徽信科共创信息安全测评有限公司、清华大学、广东省电子商务认证有限公司、深圳市电子商务安全证书管理有限公司、亚数信息科技(上海)有限公司、中科信息安全共性技术国家工程研究中心有限公司、联通在线信息科技有限公司、北京中关村实验室、奇安信网神信息技术(北京)股份有限公司、陕西省信息化工程研究院、国家信息技术安全研究中心、中孚信息股份有限公司、杭州海康威视数字技术股份有限公司、中国电子信息产业集团有限公司第六研究所、长扬科技(北京)股份有限公司。

本文件主要起草人：冯登国、荆继武、刘丽敏、郑亚杰、陈妍、丁肇伟、张建国、寇春静、张立武、贾珂婷、张严、秦岭月、李强、陈树乐、郑会涛、魏一才、胡建勋、梁斌、赵博鑫、孟佳颖、安锦程、赵晓荣、梁利、陈腾、王滨、王龙、赵华。

本文件及其所代替文件的历次版本发布情况为：

- 2005 年首次发布为 GB/T 19771—2005；
- 本次为第一次修订。



# 网络安全技术 公钥基础设施 PKI 组件最小互操作规范

## 1 范围

本文件规定了公钥基础设施组件最小互操作的基本功能要求和数据格式要求,描述了测试评价方法。

本文件适用于电子签名、电子签章、身份管理等活动中 PKI 的设计、开发、测试及其应用。

## 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 15852.2 网络安全技术 消息鉴别码 第 2 部分:采用专门设计的杂凑函数的机制
- GB/T 19714—2025 网络安全技术 公钥基础设施 证书管理协议
- GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式
- GB/T 25056—2018 信息安全技术 证书认证系统密码及其相关安全技术规范
- GB/T 32905 信息安全技术 SM3 密码杂凑算法
- GB/T 32907 信息安全技术 SM4 分组密码算法
- GB/T 32918.2 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分:数字签名算法
- GB/T 37092 信息安全技术 密码模块安全要求
- GB/T 43694 网络安全技术 证书应用综合服务接口规范
- GM/Z 0001—2013 密码术语

## 3 术语和定义

GB/T 25056—2018、GM/Z 0001—2013 界定的以及下列术语和定义适用于本文件。

### 3.1

**PKI 组件 public key infrastructure component**

构成 PKI 系统的组成要素,用于进行证书相关活动的实体。

### 3.2

**数字证书 digital certificate**

由证书认证机构对用户的公钥和身份信息进行确认,并用私钥进行签名的数据。

注:也称公钥证书。

### 3.3

**签名证书 signature certificate**

用于证明签名公钥的数字证书。

[来源:GM/Z 0001—2013,2.90]

3.4

**加密证书 encipherment certificate**

用于证明加密公钥的数字证书。

[来源:GM/Z 4001—2013,2.43,有修改]

3.5

**CA 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。

[来源:GM/Z 4001—2013,2.146,有修改]

3.6

**RA 系统 registration system**

为用户办理证书申请、身份审核、证书下载、证书密钥更新、证书注销以及密钥恢复等实际业务的系统。

3.7

**证书持有者 certificate holder**

与有效证书的主体相对应的实体。

3.8

**证书验证者 certificate verifier**

需要获取另一实体的公钥,并利用 PKI 获取证书并执行验证证书和签名功能的实体。

3.9

**资料库 repository**

存储数字证书和 CRL 等信息,并提供无需验证的信息检索服务的数据库。

3.10

**证书策略 certificate policy**

预先定义的界定证书的通用安全要求和适用范围的一组规则集。

3.11

**认证业务规则 certification practice statement**

证书认证机构签发某证书策略的证书时遵循的相关业务操作的规则。

3.12

**证书认证路径 certification path**

基于起始可信证书的有序证书序列。

注:通过处理该有序序列及其起始对象的公钥能得知该路径的末端对象的公钥。

3.13

**证书撤销列表 certificate revocation list**

标记一系列不再被证书发布者所信任的证书的签名列表。

[来源:GB/T 25056—2018,3.4]



## 4 缩略语

下列缩略语适用于本文件。

BYOD:自带设备(Bring Your Own Device)

CA:证书认证机构(Certificate Authority)

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

LDAP:轻量级目录访问协议(Lightweight Directory Access Protocol)



PKI:公钥基础设施(Public Key Infrastructure)

RA:注册机构(Registration Authority)

## 5 最小互操作基本功能要求

### 5.1 概述

PKI 系统是通过公钥密码技术提供安全通信、身份认证和数据完整性保障的框架,包括硬件、软件和标准化流程。PKI 系统由四个需要互相通信的 PKI 组件构成,分别是 CA 系统、RA 系统、证书持有者和证书验证者。这四个组件分别提供不同的功能,但一个实体可承担多个组件的角色。一个实体可同时承担 CA 系统和 RA 系统两个角色。证书持有者可为证书验证者,证书验证者不必为证书持有者。

互操作是 PKI 组件之间通过互相通信和协作,共同完成 PKI 功能的操作。最小互操作是 PKI 组件为了实现证书注册、证书密钥更新、证书撤销、资料库访问等 PKI 基本功能所需要的最低限度的互操作。最小互操作的基本功能是这些组件为了实现基本的 PKI 功能所应具备的互操作。

### 5.2 CA 系统

#### 5.2.1 总体要求

CA 系统应支持以下功能:

- a) 签发并传送证书给终端实体和其他的 CA;
- b) 接收来自 RA 系统的证书撤销请求;
- c) 将证书和 CRL 存入资料库;
- d) 为下级 CA 签发证书。

CA 系统生成自己的公私钥对并公布自己的证书。CA 系统可授权属于同一机构的 RA 系统去确认申请证书的使用者的身份或其他的特征属性,授权通过离线接受来自某个 RA 系统的证书请求完成。

CA 系统具备 5.4 中证书持有者的功能:请求、撤销、更新由其他 CA 系统签发的证书;也具备 5.5 中证书验证者的功能:检索证书和 CRL、验证证书认证路径。使用 CA 系统完成证书的生成和签发应符合 GB/T 25056—2018 中 5.3.4 的要求。

#### 5.2.2 签发签名证书

CA 系统应支持两种签名证书的证书请求:RA 系统发起的注册请求和自我注册请求。

根据不同类型,CA 系统采用不同方式鉴别申请证书主体的身份。

- a) RA 系统发起的证书请求。RA 系统应确保用户身份与公钥的绑定。CA 系统处理来自经授权的 RA 系统的证书请求。如请求被接受,CA 系统生成新证书并存储在资料库中,然后将该证书发给相应的 RA 或证书持有者。如请求由非经授权的 RA 系统发送,即签名无效或信息不匹配,CA 系统拒绝请求并向 RA 系统报告失败并说明原因。CA 系统应至少能支持 GB/T 20518—2018 中定义的签发机构密钥标识符(authorityKeyIdentifiers)、主体密钥标识符(subjectKeyIdentifier)、基本限制(basicConstraints)、密钥用法(keyUsage)、证书策略(certificatePolicies)等扩展。
- b) 自我注册请求。RA 系统可为提交请求的实体提供一份秘密信息。请求实体生成公私钥对,创建证书请求消息并使用相应私钥签名,被签名的部分可包括基于 RA 提供的秘密信息导出的认证信息。CA 系统接收请求,通过认证信息验证请求者身份,并确认其实体拥有私钥。若验证成功,CA 系统生成新证书并存入资料库,随后发送至证书持有者。若验证失败、签名无效或信息不匹配,CA 系统拒绝请求并向申请者报告失败原因。

### 5.2.3 签发加密证书

CA 系统应支持实体进行加密证书的申请。CA 系统处理来自授权的 RA 系统的加密证书的请求。如请求被接受,CA 系统响应证书申请,用户的加解密公私钥对可由第三方产生,CA 系统通过安全的方式获得加密公钥和用户加密私钥数据信封。CA 系统签发加密证书并存储在资料库中,并将该证书和加密私钥数据信封返回给相应的 RA 或证书持有者。

### 5.2.4 交叉认证

CA 系统应具备向其他 CA 签发证书的能力。交叉认证决策通过物理形式进行,并应按照与证书策略相关的认证业务规则进行安全可信检查。CA 系统应对签发的交叉证书的路径验证做出适当约束,应将 basicConstraints 设置为关键扩展并配置相应约束条件(如,路径长度的约束),宜将 nameConstraints、policyConstraints 和 policyMappings 设置为关键扩展并配置相应约束条件。如未设置这些扩展或不进行路径验证约束,即允许对方 CA 系统无限制地进行签名传递,签发交叉证书的 CA 应承担其证书策略对应的认证业务规则中承诺的全部责任,包括给其他无关 CA 签发的所有证书的责任。

### 5.2.5 证书密钥更新请求

申请者通过其原有私钥对更新请求消息进行签名以完成身份验证。CA 系统处理证书密钥更新请求,若签名有效,则签发新证书给证书持有者并存入资料库。若签名无效、请求实体处于非法状态或更新请求不符合 CA 系统的认证业务规则或证书策略,CA 系统拒绝该请求。

### 5.2.6 证书撤销

CA 系统应按照相关证书策略对应的认证业务规则,按时生成和发布包含所有被撤销但尚未到期的证书的完整证书撤销列表(CRL)。签发 CRL 的形式和周期由相关证书策略对应的认证业务规则决定。

### 5.2.7 为下级 CA 签发证书

CA 应能向层次更高的 CA 申请证书。在生成证书请求时,应使用 basicConstraints 扩展来明确该请求来自一个 CA 实体。在签发下级 CA 证书时,应在证书中明确授权的证书策略、层级限制以及名称限制。如缺少这些扩展,或者这些扩展存在但被设置为非关键项,则上级 CA 应对下级 CA 签发的所有证书承担与证书策略对应的认证业务规则中所承诺的所有的法律责任。

## 5.3 RA 系统

### 5.3.1 与互操作性有关的功能要求

RA 系统应支持以下功能:

- 1) 接受和验证证书请求;
- 2) 向 CA 系统发送证书请求;
- 3) 生成证书撤销请求。

RA 系统与其他组件进行互操作时,基本功能要求如下。

- a) 当物理证书介质与 RA 系统进行物理连接时,RA 系统通过验证签名消息来验证该介质中拥有与公钥相应的私钥材料。在密钥对和实体身份均经过验证之后,RA 系统签署并向相应的 CA 系统发送数字证书请求。
- b) 未与 RA 系统进行过物理接触的证书请求者,在发起证书请求时,应持有 RA 系统提供的认证

信息。此信息将作为实体在自我注册请求中向 CA 系统证明其身份的证据。

- c) RA 系统应支持对 CA 系统授权其所管理的实体证书请求进行证书撤销操作。该功能可与 CA 系统集成,也可在不同的设施中执行。
- d) RA 系统应将新签发的证书与 CA 的证书一同发送给证书持有者。
- e) RA 系统应代表不再拥有私钥并且怀疑该私钥已泄露的证书持有者产生并签署证书撤销请求。如果 CA 的认证业务规则允许,RA 系统应代表证书持有者的组织产生并签署证书撤销请求。

### 5.3.2 使用 BYOD 请求证书的 RA 系统功能要求

RA 系统应验证 BYOD 设备的密码模块是否符合 GB/T 37092 的要求。RA 应鉴别密码模块的安全等级是否与认证业务规则一致。

## 5.4 证书持有者

### 5.4.1 与互操作性相关的功能要求

证书持有者包括 CA、RA 和其他的终端实体。终端实体是个人、企业、用户、计算机系统或应用程序(CA 和 RA 除外)。

证书持有者应包括以下功能:

- a) 生成签名;
- b) 生成证书注册请求;
- c) 生成证书撤销请求;
- d) 生成证书密钥更新请求。

证书持有者同时也是证书验证者,具备 5.5 中定义证书验证者的功能。

### 5.4.2 证书持有者的 BYOD 功能要求

证书持有者 BYOD 作为证书介质申请或使用证书服务时,该设备应安装有符合 GB/T 37092 的密码模块并具备未被破坏的可信启动。该设备也应具备数字证书展示和通信能力,如:使用二维码交换证书和签名。BYOD 设备不应要求物理接入他人的设备进行证书展示和验证。

## 5.5 证书验证者

### 5.5.1 与互操作性有关的功能要求

证书验证者是使用证书的实体,包括 CA、RA、个人、企业、用户和计算机系统。

证书验证者应包括以下功能:

- a) 验证证书;
- b) 从查询服务器中检索证书和 CRL;
- c) 验证证书认证路径。

具有证书持有者身份的证书验证者也能产生签名、支持撤销或更新证书。

### 5.5.2 验证证书的最小步骤要求

证书验证者应能获得从信任起点开始的完整的证书路径。信任起点可为:

- a) 预埋的根证书;
- b) 预埋的 CA 证书;
- c) 经过验证后缓存的可信 CA 的证书。

证书验证者应从信任起点的证书开始,针对每个证书,逐一完成以下验证。

- a) 验证证书基本信息:
    - 1) 使用签发该证书的公钥验证签名;
    - 2) 验证证书有效期;
    - 3) 验证证书是否被撤销;
    - 4) 验证证书签发者的名称。
  - b) 验证关键证书扩展。
  - c) 如果证书是自签发证书,且不是路径中的最终证书,跳过本步骤。否则,验证主体名称是否在签发该证书的 CA 证书中的 nameConstraints 扩展(如适用)中一个允许的子树中,并验证 subjectAltName 扩展中的每个替代名称(关键或非关键)是否在该名称类型的一个允许的子树中。
  - d) 如果证书是自签发证书,且不是验证路径中的最终证书,跳过本步骤。否则,验证主体名称不在签发该证书的 CA 证书中的 nameConstraints 扩展(如适用)中的任何排除子树中,并验证 subjectAltName 扩展中的每个替代名称(关键或非关键)不在该名称类型的任何排除子树中。
  - e) 如果有证书策略(certificatePolicies)扩展,验证该扩展是否使用符合预期的策略。
- 上述验证过程,任意项未通过都表示该证书不能被信任。

## 5.6 密码算法

PKI 组件使用四类算法:密码杂凑算法、数字签名算法、消息鉴别码算法和对称加密算法。

PKI 组件使用密码算法的总体安全要求如下:

- a) 一个组件应实现至少一个数字签名算法,其他组件应能生成和验证由该算法生成的签名;
- b) 组件应至少支持一个加密算法。

对于上述四类算法要求如下:

- a) 应支持 GB/T 32905 规定的 SM3 密码杂凑算法;
- b) 应支持 GB/T 32918.2 规定的 SM2 数字签名算法;
- c) 应支持 GB/T 15852.2 规定的 MAC 算法 2(HMAC);
- d) 应支持 GB/T 32907 规定的 SM4 分组密码算法。

## 6 互操作事务数据格式要求

### 6.1 总体要求

PKI 互操作事务包括注册请求、更新证书、撤销证书、访问目录服务。CA 系统、RA 系统和证书持有者应能实现这些事务。PKI 事务的消息格式应符合 GB/T 19714—2025 第 6 章的要求。证书的数据结构、证书扩展、证书撤销列表应符合 GB/T 20518—2018 的要求。PKI 互操作事务中涉及证书应用综合服务接口的应符合 GB/T 43694 的要求。

对于 CA 系统和 RA 系统物理上在一起且不支持远端 RA 系统的 PKI 产品,可忽略 CA 系统和 RA 系统之间的消息交互。

### 6.2 注册请求

#### 6.2.1 RA 系统发起的注册请求

##### 6.2.1.1 请求流程

RA 系统请求 CA 系统为一个终端实体签发签名证书流程如下:

- a) 终端实体通过物理方式(如提交实体 U 盘),在签名消息中向 RA 系统提供其公钥;
- b) RA 系统产生认证请求,利用签名消息保护请求,向 CA 系统为终端实体申请证书;
- c) CA 系统产生响应并发送给 RA 系统,响应消息中包含证书或错误代码的签名;
- d) RA 系统通过物理形式向终端实体提供 CA 的公钥和所签发的证书,终端实体也可直接从 CA 获得证书。

### 6.2.1.2 从 RA 系统到 CA 系统的证书请求

RA 系统建立证书请求的 PKIMessage,并发送给 CA 系统,其 PKIBody 的请求代码为 cr。其中,PKIHeader 的 sender 是 RA 的可辨别名,recipient 是 CA 的可辨别名。PKIBody 是 CertReqMessages,是一个 CertReqMessage 字段的序列,应包括如下信息:

- certReq 含有请求者希望包含在证书中的信息;
- pop 证明了对新证书私钥的拥有。

只支持终端实体产生签名密钥对,不支持终端实体产生加密密钥对。在进行签名私钥的拥有性证明时,如果由 RA 系统来实现,当 RA 系统修改主体名时,popSKInput 域出现,并且包含原来的主体名。否则,RA 系统不修改主体名,pop 域与请求者提交的主体名一致。

与证书内容相关的信息放入 CertReqMessage 的 certReq 中。

PKIProtection 字段含有根据消息头和消息体的 DER 编码序列计算的 RA 系统的签名。

### 6.2.1.3 从 CA 系统到 RA 系统的证书响应

CA 系统返回证书响应请求的 PKIMessage 给 RA 系统,其 PKIBody 的响应代码为 cp。其中 PKIHeader 的 sender 是 CA 的可辨别名,recipient 是 RA 的可辨别名。如果在证书请求中提供了 senderNonce,响应的 PKIHeader 应将其作为 recipNonce。PKIBody 是 CertRepMessage,CertRepMessage 含有唯一的 response 字段,是包含 certReqId,status 和 certifiedKeyPair 的序列。如果 CA 系统签发了一张证书,PKIBody 应含如下信息:

- certReqId 与请求中的 certReqId 匹配;
- status 是 granted 或者是 grantedWithMods;
- certifiedKeyPair 序列至少含有一个字段 certificate。

证书应满足如下要求:

- version 号应是 v3(2);
- publicKey 字段应与证书请求中相同或者是由 CA 所产生的公钥;
- 主体可辨别名应与证书请求中相同;
- 签发者名字应是 CA 的可辨别名;
- 如果 notBefore 出现在证书请求中,证书应从签发日和 notBefore 所指之日的较晚者之后生效;
- 如果 notAfter 出现在证书请求中,证书应在该日或之前期满。

证书应包括如下扩展(extensions):

- subjectKeyIdentifier 域;
- 在 certificatePolicies 字段中至少包括一个证书策略的 OID;
- authorityKeyIdentifier 域。

如果 status 是 granted 和 grantedWithMods,failInfo 字段可不存在。

如果 CA 拒绝了请求,PKIBody 应含有如下信息:

- status 是 rejected;
- failInfo 包含适当的错误代码。

如果 status 是 rejected,certifiedKeyPair 字段不必出现。



PKIProtection 字段含有根据消息头和消息体的 DER 编码序列计算的 CA 的签名。

## 6.2.2 新实体的自我注册请求

### 6.2.2.1 请求流程

如果新实体尚未从某一特定 CA 系统获取证书,可直接向该 CA 申请一张新的证书。在申请过程中,请求实体生成一个请求代码为 ir 的 PKIMessage 以请求新证书,该消息中包含对所请求证书中公钥相对应的私钥的拥有证明。实体利用 RA 提供的一个秘密密钥和消息鉴别码算法对 PKIMessage 进行保护。

如果 CA 接受自我注册请求,向证书持有者返回一个响应代码为 ip 的 PKIMessage。该消息包含证书或者事务出错的原因代码。

### 6.2.2.2 RA 系统与实体之间的事务

RA 系统给实体发送一个共享的秘密密钥。通过从该共享秘密中生成消息鉴别码,CA 系统对实体进行认证。

不指定该事务明确的内容和格式。秘密密钥和 CA 的公钥信息应以可信方式传递给实体。

### 6.2.2.3 从证书持有者到 CA 系统的自我注册请求

请求者建立一个 PKIMessage,其 PKIBody 的请求代码为 ir。PKIHeader 的 sender 是请求者的可辨别名,recipient 是 CA 的可辨别名。PKIBody 是 CertReqMessages,是一个 CertReqMessage 字段的序列。CertReqMessage 包括如下信息:

- certReq 含有请求者希望包含在证书中的信息;
- popoSKInput 包含公钥的 MAC 值;
- pop 证明对证书私钥的拥有。

其中 pop 域通过与 CertTemplate 中的公钥相对应的私钥来产生,产生 pop 的输入数据包括 popoSKInput 中的公钥 MAC 值和 CertTemplate 中的公钥。

与证书内容相关的信息放入为 CertRequest 的 certReq 中。

PKIProtection 域包含一个请求者利用从 RA 获得的秘密产生的值。

### 6.2.2.4 从 CA 系统到证书请求者的自我注册请求的响应

CA 系统返回证书响应请求的 PKIMessage 给证书持有者,其 PKIBody 的响应代码为 ip。其中,PKIBody 的 sender 是 CA 的可辨别名,recipient 是证书请求消息头中 sender 域的值。如果在证书请求中提供了 transactionID,响应的 PKIHeader 中包括同样的 transactionID。如果在证书请求中提供了 senderNonce,响应的 PKIHeader 应将其作为 recipNonce。PKIBody 是 CertRepMessage。如果 CA 系统签发了一张证书,PKIBody 应含有如下信息:

- status 是 granted 或者是 grantedWithMods;
- certificate 包含新的证书。

如果 status 是 granted 和 grantedWithMods,failInfo 字段不必存在。

如果 CA 拒绝了请求,PKIBody 应含有如下信息:

- status 是 rejected;
- failInfo 包含适当的错误代码。

如果 status 是 rejected,certificate 域可能不存在。

证书应包括如下扩展(extensions):

- subjectKeyIdentifier 域；
- 在 certificatePolicies 字段中至少包括一个证书策略的 OID；
- authorityKeyIdentifier 域。

PKIProtection 字段含有根据消息头和消息体的 DER 编码序列计算的 CA 的签名。

### 6.2.3 已知实体的自我注册请求

#### 6.2.3.1 请求流程

如果某一实体并非当前证书持有者,但是曾从特定 CA 系统获得过证书,该实体可直接向该 CA 系统提出新证书的申请。在申请过程中,请求实体生成请求代码为 cr 的 PKIMessage 以请求新证书,该消息中包含与证书请求中公钥所对应的私钥的拥有证明。实体利用 RA 提供的一个秘密密钥和消息鉴别码算法对 PKIMessage 进行保护。

如果 CA 系统接受自我注册请求,向证书持有者返回一个响应代码为 cp 的 PKIMessage。该消息包含证书或者事务出错的原因代码。

#### 6.2.3.2 RA 系统与实体的事务

RA 系统给实体发送一个共享的秘密密钥。CA 系统通过从共享的秘密中产生的消息鉴别码,对实体进行认证。

不指定该事务明确的内容和格式。秘密密钥和 CA 的公钥信息应以可信方式传递给实体。

#### 6.2.3.3 从证书持有者到 CA 系统的自我注册请求

请求者建立一个 PKIMessage,其 PKIBody 的请求代码为 cr。PKIHeader 的 sender 是请求者的可辨别名,recipient 是 CA 的可辨别名。PKIBody 是 CertReqMessages,是一个 CertReqMessage 字段的序列。CertReqMessage 包括如下信息:

- certReq 含有请求者希望包含在证书中的信息;
- popoSKInput 包含公钥的 MAC 值;
- pop 证明了对证书私钥的拥有。

其中 pop 域通过与 CertTemplate 中的公钥相对应的私钥来产生,产生 pop 的输入数据包括 popoSKInput 中的公钥 MAC 值和 CertTemplate 中的公钥。

与证书内容相关的信息放入为 CertRequest 的 certReq 中。

PKIProtection 域包含一个请求者利用从 RA 获得的秘密产生的值。

#### 6.2.3.4 从 CA 系统到证书请求者的自我注册请求的响应

CA 系统返回证书响应请求的 PKIMessage 给证书持有者,其 PKIBody 的响应代码为 cp。其中,PKIBody 的 sender 是 CA 的可辨别名,recipient 是证书请求消息头中 sender 域的值。如果在证书请求中提供了 transactionID,响应的 PKIHeader 中包括同样的 transactionID。如果在证书请求中提供了 senderNonce,响应的 PKIHeader 应将其作为 recipNonce。PKIBody 是 CertRepMessage。如果 CA 系统签发了一张证书,PKIBody 应含有如下信息:

- status 是 granted 或者是 grantedWithMods;
- certificate 包含新的证书。

如果 status 是 granted 和 grantedWithMods,failInfo 字段不必存在。

如果 CA 系统拒绝了请求,PKIBody 应含有如下信息:

- status 是 rejected;

- failInfo 包含适当的错误代码。

如果 status 是 rejected, certificate 域可能不存在。

证书应包括如下扩展(extensions):

- subjectKeyIdentifier 域;
- 在 certificatePolicies 字段中至少包括一个证书策略的 OID;
- authorityKeyIdentifier 域。

PKIProtection 字段含有根据消息头和消息体的 DER 编码序列计算的 CA 的签名。

#### 6.2.4 加密证书申请

拥有当前有效证书的证书持有者可向签发该证书的 CA 系统提出申请,申请产生加密密钥对并签发相应的证书。发出申请的实体产生临时加密密钥,并生成请求代码为 cr 的 PKIMessage,以申请加密证书,PKIMessage 中包括了临时加密密钥。利用当前有效证书的对应私钥,对 PKIMessage 进行签名并发送给 CA 系统。

如果 CA 系统的 CPS 支持集中产生加密密钥对,则 CA 系统执行如下操作:

- CA 系统按请求消息的要求产生密钥对,签发加密证书;
- CA 系统产生对称密钥,利用对称密钥加密新产生的私钥,使用临时公钥加密对称密钥,产生和返回响应消息给证书持有者。响应消息中包括了新生成的证书和加密后的私钥,或者是事务失败的代码。

用户的加解密公私钥对也可由可信第三方(如,密钥管理系统)产生,应采用符合 GB/T 19714—2025 中 7.5 规定的协议和消息格式获得产生的公钥和加密私钥数字信封。CA 系统签发加密证书并存储在资料库中,并将该证书和以用户公钥保护的加密私钥返回给相应的 RA 或证书持有者。

#### 6.2.5 组合证书申请

签名密钥证书和加密证书的申请可由一次事务完成。RA 系统发起的注册请求和自我注册请求(见 6.2.2.1、6.2.2.2、6.2.2.3)可和加密证书申请(见 6.2.2.4)组合在一起。在此情况下,CertReqMessages 包括两个 CertReqMessage 的序列。一个 CertReqMessage 等同于 RA 系统发起的注册请求和自我注册请求的情况,另一个 CertReqMessage 等同于加密证书申请的情况。消息使用签名证书申请的方式来加以保护。

如果组合申请中包括的是自我注册请求,则或者签名密钥证书申请成功,或者两个证书的申请都不成功。如果还需要额外的信息来提供 pop,申请者则使用自我注册请求中的私钥来对消息做签名。

### 6.3 证书密钥更新

#### 6.3.1 更新流程

拥有当前有效(指在有效期内、未被撤销)证书的证书持有者可直接向签发该证书的 CA 系统要求签发一份新的证书。证书持有者生成请求代码为 kur 的 PKIMessage,包括证书申请和相应的 pop。证书持有者使用有效证书的对应私钥对该 PKIMessage 进行签名。

如果 CA 系统的 CPS 支持证书密钥更新,则 CA 系统返回请求代码为 kup 的 PKIMessage,包含新生成的证书或者是事务失败的代码。

如果新证书成功生成,则有两个可选的消息,分别是:证书持有者在收到新的证书后给 CA 系统发出确认,CA 系统响应确认消息。

#### 6.3.2 从证书持有者到 CA 系统的证书密钥更新申请

证书持有者建立一个 PKIMessage,其 PKIBody 的请求代码为 kur。PKIHeader 的 sender 是证书



持有者的可辨别名, recipient 是 CA 的可辨别名。PKIBody 是 CertReqMessages, 是一个 CertReqMessage 字段的序列。CertReqMessage 包括如下信息:

- certReq 包含了申请者要求包括在证书中的各种信息;
- pop 是新证书公钥的对应的 pop 证明。

pop 应由 publicKey 域的公钥对应的私钥产生。CertReq 的 publicKey 域是新证书的公钥。

如果消息中没有 signingAlg, CA 系统应使用终端实体的公钥对应的算法签名。

PKIProtection 域是使用当前有效证书的对应私钥对消息头和消息体的 DER 编码信息的签名结果。

### 6.3.3 从 CA 系统到证书持有者的证书密钥更新响应

CA 系统返回证书密钥更新响应请求的 PKIMessage 给证书持有者, 其 PKIBody 的响应代码为 kup。其中, PKIBody 的 sender 是 CA 的可辨别名, recipient 是证书请求消息头中 sender 域的值。如果在证书请求中提供了 transactionID, 响应的 PKIHeader 中包括同样的 transactionID。如果在证书请求中提供了 senderNonce, 响应的 PKIHeader 应将其作为 recipNonce。PKIBody 是 CertRepMessage。如果 CA 系统签发了新证书, PKIBody 应含有如下信息:

- status 是 granted 或者是 grantedWithMods;
- certificate 包含新的证书。

如果 status 是 granted 和 grantedWithMods, failInfo 字段不必存在。

如果 CA 拒绝了请求, PKIBody 应含有如下信息:

- status 是 rejected;
- failInfo 包含适当的错误代码。

如果 status 是 rejected, certificate 域可能不存在。

证书应包括如下扩展(extensions):

- subjectKeyIdentifier 域;
- 在 certificatePolicies 字段中至少包括一个证书策略的 OID;
- authorityKeyIdentifier 域。

PKIProtection 字段含有根据消息头和消息体的 DER 编码序列计算的 CA 的签名。

## 6.4 撤销请求

### 6.4.1 撤销流程

证书持有者可请求撤销自己的证书。证书持有者产生 RevReq 消息, 对该消息进行签名并发送给相应 RA 系统, 并在 RA 系统审查通过用户的身份后向 CA 发出相应撤销信息。该签名应使用未过期、未被撤销的签名证书的相应私钥产生(可为将要撤销的证书)。RevReq 消息应标识出将要撤销的证书以及将要撤销的原因。CA 系统回应 RA 系统一个 RevRep 消息, RA 系统再回应证书持有者相应的 RevRep 消息。

如果消息 rr(RevReq)中包含 transactionID, 则 CA 系统和 RA 系统所响应的 rp(RevRep)消息中也应包含相同的 transactinID, 其中从证书持有者所发出的 rr 和 RA 所发出的 rr 消息中的 transactinID 可不同。rp 消息至少应包含 status 字段以反映请求的状态和 revCerts 字段以表示将撤销的证书。

### 6.4.2 从证书持有者到 RA 系统的撤销请求

证书持有者建立一个 PKIMessage, 其 PKIBody 的请求代码为 rr。PKIHeader 的 sender 是证书持有者的可辨别名, recipient 是 RA 的可辨别名。PKIBody 是 RevReqContent, 是 RevDetails 的序列, 由

CertDetails 和三个可选字段组成的序列：原因标志、怀疑或丢失的日期和时间、crlEntryDetails (CRL Entry 扩展的序列)。CertDetails 最少包括以下信息：

- serialNumber 证书序列号；
- issuer 证书发放者的标识名。

或：

- subject 证书持有者的标识名；
- issuer 证书发放者的标识名。

CertDetails 还可在 extensions 字段中包含 subjectKeyIdentifier。如果请求者希望撤销签发给某个主体的所有证书，CertDetails 应仅含有 subject 和 issuer。即，仅希望撤销单个证书的请求只含有相应的序列号或是 subjectKeyIdentifier。

RevDetails 应包括带有 reasonCode 扩展的 crlEntryDetails，也可包括 invalidityDate 扩展来说明何时该证书作废。原因代码也可不是 removeFromCRL。

PKIProtection 字段含有请求者的签名，即消息头和消息体的 DER 编码进行签名。终端实体用相应 CA 所签发的当前有效签名证书的相应私钥进行签名。

#### 6.4.3 从 RA 系统到 CA 系统的撤销请求

RA 系统或证书持有者生成包含 PKIBody 元素 rr 的 PKIMessage。PKIHeader 的 sender 为 RA 的可辨别名，recipient 为 CA 的可辨别名；PKIBody 与从证书持有者到 RA 系统的撤销请求相同。

PKIProtection 字段含有 RA 系统的签名，即对头和正文的 DER 编码进行签名。RA 系统用相应 CA 系统所签发的当前有效签名证书的相应私钥进行签名。

#### 6.4.4 从 CA 系统到 RA 系统的撤销响应

CA 系统返回证书密钥更新响应请求的 PKIMessage 给证书持有者，其 PKIBody 的响应代码为 rp。其中，PKIBody 的 sender 是 CA 的可辨别名，recipient 是 RA 的可辨别名。如果在证书请求中提供了 senderNonce，响应的 PKIHeader 应将其作为 recipNonce。PKIBody 是 RevRepContent。如果 CA 系统撤销了证书，PKIBody 将包含以下信息：

- status 是 granted 或是 grantedWithMods；
- revDetails 包含已撤销证书的 CertId。

如果 status 是 granted 或 grantedWithMods，failInfo 字段不必出现。

如果 CA 系统拒绝了请求，PKIBody 应含有如下信息：

- status 是 rejected；
- failInfo 包含适当的错误代码。

对于能确定有问题的证书，revCerts 包含被拒绝撤销证书的 CertId。PKIProtection 字段包含 CA 系统的签名，即对头和正文的 DER 编码进行签名。

若 CA 系统生成 CRLs，并且撤销请求被接受，CRL 将有以下值：

- userCertificate 字段中的被撤销证书的序列号；
  - revocationDate 收到撤销请求的日期和时间；
  - crlEntryExtensions。
- crlEntryExtensions 包括：
- revCerts 字段中的 reasonCode，除非 CA 系统的策略有专门规定；
  - (可选的)revCerts 字段中的 badSinceDate 扩展可为 invalidityDate。

#### 6.4.5 从 RA 系统到证书持有者的撤销响应

RA 系统在收到 CA 的响应消息后，返回含有响应代码为 rp 的 PKIMessage 给证书持有者。其中，

PKIBody 的 sender 是 CA 的可辨别名, recipient 是 RA 的可辨别名。如果响应的从证书持有者到 RA 系统的撤销请求消息中有 senderNonce, 则响应的 PKIHeader 中应将它作为 recipNonce。PKIBody 是 RevReqContent, 内容与从 CA 系统到 RA 系统的撤销响应相同, PKIProtection 字段包含 RA 系统的签名, 即对消息头和消息体的 DER 编码进行签名。

## 6.5 访问资料库

### 6.5.1 从资料库请求证书

证书验证者可使用 LDAP V3 向资料库请求证书。当使用 LDAP 时, 证书验证者可通过 LDAP 搜索请求从资料库中请求证书, 或是利用给定的 LDAP URL 来请求证书(即 authorityInformationAccess 扩展)。

### 6.5.2 从资料库请求 CRL

证书验证者可使用 LDAP V3 向资料库请求 CRLs。证书验证者可使用 LDAP 从资料库中请求 CRLs。当使用 LDAP 时, 实体可通过 LDAP 搜索请求从资料库中请求 CRLs, 或是利用给定的 LDAP URL 来请求 CRLs(即, cRLDistributionPoints 扩展中的 distributionPoint 字段)。

## 7 测试评价方法

### 7.1 通用测试评价方法

可采用人员访谈、文档查阅、人工核查等方法, 确认 CA 系统的功能是否符合 5.2 的要求, 确认 RA 系统的功能是否符合 5.3 的要求, 确认证书持有者的功能是否符合 5.4 的要求, 确认证书验证者的功能是否符合 5.5 的要求。

可采用人员访谈、文档查阅、人工核查等方法, 确认与互操作有关的数字证书的格式是否符合 6.1 的要求, 确认与互操作有关的 PKI 事务消息内容的格式是否符合 6.1 的要求。

### 7.2 最小互操作基本功能测试评价方法

#### 7.2.1 CA 系统功能测试评价

可采用人员访谈、文档查阅、人工核查等方法。CA 系统功能测评实施流程、预期结果和结果判定如下。

- a) 测评实施流程:
  - 1) 确认 CA 系统在处理 RA 系统发起的签名证书注册请求时的方法是否符合 5.2.2 a) 的要求;
  - 2) 确认 CA 系统在处理自我注册签名证书的请求时的方法是否符合 5.2.2 b) 的要求;
  - 3) 确认 CA 系统在处理加密证书请求时的方法是否符合 5.2.3 的要求;
  - 4) 确认 CA 系统在处理证书密钥更新请求时的方法是否符合 5.2.5 的要求;
  - 5) 确认 CA 系统在处理证书撤销时的方法是否符合 5.2.6 的要求;
  - 6) 确认 CA 系统在为下级 CA 证书签发证书时的处理方法是否符合 5.2.7 的要求;
  - 7) 确认 CA 系统是否能实现注册请求、更新证书、撤销证书、访问目录服务等事务;
  - 8) 确认 CA 系统是否支持 5.6 中要求的相关密码算法。
- b) 预期结果:
  - 1) CA 系统按照 5.2.2.a) 的要求处理 RA 系统发起的签名证书注册请求;
  - 2) CA 系统按照 5.2.2.b) 的要求处理自我注册签名证书的请求;

- 3) CA 系统按照 5.2.3 的要求处理加密证书请求；
  - 4) CA 系统按照 5.2.5 的要求处理证书密钥更新请求；
  - 5) CA 系统按照 5.2.6 的要求处理证书撤销请求；
  - 6) CA 系统按照 5.2.7 的要求为下级 CA 证书签发证书；
  - 7) CA 系统能实现注册请求、更新证书、撤销证书、访问目录服务等事务；
  - 8) CA 系统支持 5.6 中要求的相关密码算法。
- c) 结果判定：上述预期结果均满足为符合，其他情况为不符合。

### 7.2.2 RA 系统功能测试评价

可采用人员访谈、文档查阅、人工核查等方法。RA 系统功能测评实施流程、预期结果和结果判定如下。

- a) 测评实施流程：
- 1) 确认 RA 系统在处理物理接触的证书请求者发起的证书请求时的方法是否符合 5.3.1 a) 的要求；
  - 2) 确认 RA 系统在处理未进行物理接触的证书请求者发起的证书请求时的方法是否符合 5.3.1 b) 的要求；
  - 3) 确认 RA 系统是否支持对 CA 系统授权其所管理的实体证书请求进行证书撤销操作；
  - 4) 确认 RA 系统是否支持将新签发的证书与 CA 的证书一同发送给证书持有者；
  - 5) 确认 RA 系统是否可代表不再拥有私钥并且怀疑该私钥已泄露的证书持有者产生并签署证书撤销请求；
  - 6) 确认 RA 系统是否能核实 BYOD 设备为符合 GB/T 37092 要求的密码模块，并是否能鉴别密码模块的安全等级与认证业务规则的一致性；
  - 7) 确认 RA 系统是否能实现注册请求、更新证书、撤销证书、访问目录服务等事务；
  - 8) 确认 RA 系统是否支持 5.6 中要求的相关密码算法。
- b) 预期结果：
- 1) RA 系统按照 5.3.1 a) 的要求处理物理接触的证书请求者发起的证书请求；
  - 2) RA 系统按照 5.3.1 b) 的要求处理未进行物理接触的证书请求者发起的证书请求；
  - 3) RA 系统支持对 CA 系统授权其所管理的实体证书请求进行证书撤销操作；
  - 4) RA 系统支持将新签发的证书与 CA 的证书一同发送给证书持有者；
  - 5) RA 系统代表不再拥有私钥并且怀疑该私钥已泄露的证书持有者产生并签署证书撤销请求；
  - 6) RA 系统支持核实 BYOD 设备为符合 GB/T 37092 要求的密码模块，并支持鉴别密码模块的安全等级与认证业务规则的一致性；
  - 7) RA 系统支持实现注册请求、更新证书、撤销证书、访问目录服务等事务；
  - 8) RA 系统支持 5.6 中要求的相关密码算法。
- c) 结果判定：上述预期结果均满足为符合，其他情况为不符合。

### 7.2.3 证书持有者功能测试评价

可采用人员访谈、文档查阅、人工核查等方法。证书持有者功能测评实施流程、预期结果和结果判定如下。

- a) 测评实施流程：
- 1) 确认证书持有者是 CA 系统、RA 系统或其他的终端实体中的一种；
  - 2) 确认证书持有者是否能生成签名、生成注册证书请求、发起证书撤销请求、发起证书密钥

更新请求；

- 3) 确认证书持有者是否具备 5.5 中定义证书验证者的功能；
- 4) 确认证书持有者是否能实现注册请求、更新证书、撤销证书、访问目录服务等事务；
- 5) 确认证书持有者的 PKI 组件是否支持 5.6 中要求的相关密码算法。

b) 预期结果：

- 1) 证书持有者是 CA 系统、RA 系统或其他的终端实体中的一种；
- 2) 证书持有者支持能生成签名、生成注册证书请求、发起证书撤销请求、发起证书密钥更新请求；
- 3) 证书持有者具备 5.5 中定义证书验证者的功能；
- 4) 证书持有者支持实现注册请求、更新证书、撤销证书、访问目录服务等事务；
- 5) 证书持有者的 PKI 组件支持 5.6 中要求的相关密码算法。

c) 结果判定：上述预期结果均满足为符合，其他情况为不符合。

#### 7.2.4 证书验证者功能测试评价

可采用人员访谈、文档查阅、人工核查等方法。证书验证者功能测评实施流程、预期结果和结果判定如下。

a) 测评实施流程：

- 1) 确认证书验证者是否是 CA 系统、RA 系统、个人、企业、用户或计算机系统中的一种；
- 2) 确认证书验证者是否能验证证书、从查询服务器中检索证书和 CRL、验证证书认证路径；
- 3) 确认具有证书持有者身份的证书验证者是否能产生签名、支持撤销或更新证书；
- 4) 查看并确认证书验证者是否能获得从信任起点开始的完整的证书路径，验证路径的步骤是否符合 5.5.2 的要求；
- 5) 确认证书验证者的 PKI 组件是否支持 5.6 中要求的相关密码算法。

b) 预期结果：

- 1) 证书验证者是 CA 系统、RA 系统、个人、企业、用户或计算机系统中的一种；
- 2) 证书验证者支持验证证书、从查询服务器中检索证书和 CRL、验证证书认证路径；
- 3) 承担证书持有者角色的证书验证者支持产生签名、支持撤销或更新证书；
- 4) 证书验证者支持获得从信任起点开始的完整的证书路径，验证路径的步骤符合 5.5.2 的要求；
- 5) 证书验证者的 PKI 组件支持 5.6 中要求的相关密码算法。

c) 结果判定：上述预期结果均满足为符合，其他情况为不符合。

#### 7.3 互操作数据格式测试评价方法

可采用人员访谈、文档查阅、人工核查等方法。测评实施流程、预期结果和结果判定如下：

a) 测评实施流程：

- 1) 查看并确认 RA 系统发起的注册请求事务消息内容是否符合 6.2.1 的要求；
- 2) 查看并确认新实体发起的自我注册请求事务消息内容是否符合 6.2.2 的要求；
- 3) 查看并确认已知实体发起的自我注册请求事务消息内容是否符合 6.2.3 的要求；
- 4) 查看并确认加密证书申请事务消息内容是否符合 6.2.4 的要求；
- 5) 查看并确认组合证书申请事务消息内容是否符合 6.2.5 的要求；
- 6) 查看并确认证书密钥更新事务消息内容是否符合 6.3 的要求；
- 7) 查看并确认证书撤销事务消息内容是否符合 6.4 的要求；
- 8) 查看并确认从资料库请求证书事务消息内容是否符合 6.5.1 的要求；

- 9) 查看并确认从资料库请求 CRL 事务消息内容是否符合 6.5.2 的要求。
- b) 预期结果：
  - 1) RA 系统发起的注册请求事务消息内容符合 6.2.1 的要求；
  - 2) 新实体发起的自我注册请求事务消息内容符合 6.2.2 的要求；
  - 3) 已知实体发起的自我注册请求事务消息内容符合 6.2.3 的要求；
  - 4) 加密证书申请事务消息内容符合 6.2.4 的要求；
  - 5) 组合证书申请事务消息内容符合 6.2.5 的要求；
  - 6) 证书密钥更新事务消息内容符合 6.3 的要求；
  - 7) 证书撤销事务消息内容符合 6.4 的要求；
  - 8) 从资料库请求证书事务消息内容符合 6.5.1 的要求；
  - 9) 从资料库请求 CRL 事务消息内容符合 6.5.2 的要求。
- c) 结果判定：上述预期结果均满足为符合，其他情况为不符合。



