ICS XX.XXX.XX
CCS R XX

DB2101

辽 宁 省 地 方 标 准

DB2101/T XXXX—2023

公共资源交易 数字证书（CA）互联互通 技术规范 Ukey 载体部分

Public Resource Transaction Digital Certificate (CA) Interconnection Technical Specification Ukey Carrier Part

（征求意见稿）

2023-XX-XX 发布 2023-XX-XX 实施

辽宁省发展和改革委员会
辽宁省市场监督管理局 发布

前　　言

根据辽宁省公共资源交易协会针对《公共资源交易 数字证书（CA）互联互通技术规范 Ukey载体部分》标准编制大纲要求，经过编制组广泛调查研究，认真总结公共资源交易领域数字证书（CA）互联互通技术实践，参考有关国家标准，并在广泛征求意见的基础上，制订本标准。

本标准主要技术内容是：1.适用范围；2.规范性引用文件；3.术语和定义；4.安全机制；5.软件要求；6.数字证书介质驱动安装程序要求；7.数字证书技术规范；8.CA认证机构接入规范；9.数字证书应用集成规范。

本标准由辽宁省发展和改革委员会负责日常管理，由辽宁省公共资源交易协会负责技术内容的解释。请各单位在本标准执行的过程中，总结经验，积累资料，并将有关意见和建议寄送至辽宁省公共资源交易协会（地址：辽宁省沈阳市皇姑区北陵大街34-3 号 3 楼，电话：024-67781777），以便今后修订时参考。

本标准主编单位：辽宁省公共资源交易协会

本标准参编单位：辽宁省发展和改革委员会
大连市公共资源交易中心
丹东市公共资源交易中心
葫芦岛市公共资源交易中心
辽宁省网联数字科技产业有限公司
辽宁思创网联科技有限公司
广联达科技股份有限公司

主要起草人（按姓氏首字母排列）：

薄　红	包汝斌	陈洪岭	关　红	吕国君	黄伊莹
金　萍	李宏达	李　智	邱笑萌	沈　云	佟　伟
吴　楠	王　磊	张汪洋	邹　毅		

目　录

1. 适用范围 1
2. 规范性引用文件 1
3. 术语和定义 2
3.1 招标投标相关的术语及定义 2
3.1.1 电子招标投标 2
3.1.2 招标人 2
3.1.3 招标代理机构 2
3.1.4 投标人 2
3.2 平台及工具软件 2
3.2.1 公共服务平台 2
3.2.2 电子招标投标交易平台 3
3.2.3 工具软件 3
3.2.4 平台及工具软件标识码 3
3.3 主体的术语及定义 3
3.3.1 主体 3
3.3.2 主体代码类型 3
3.3.3 主体名称 3
3.4 CA 数字证书相关的术语定义 3
3.4.1 CA 4
3.4.2 数字证书 4
3.4.3 加密证书 4
3.4.4 签名证书 4
3.4.5 用户 4
3.4.6 数字证书使用入口 4
3.4.7 加密 4
3.4.8 解密 4
3.4.9 数字签名 5

辽宁省地方标准

3.4.10 电子签章 5
4. 安全机制 5
4.1 密钥管理 5
4.2 数字证书介质的扩展区要求 5
5. 软件要求 5
5.1 数字证书介质接口要求 5
5.2 设备管理接口 5
5.3 访问控制接口 6
5.4 应用管理接口 6
5.5 文件管理接口 6
5.6 容器管理接口 6
6. 数字证书介质驱动安装程序要求 7
6.1 电子认证服务机构提供的数字证书介质安装程序应满足以下要求： 7
6.2 密码服务接口 7
6.3 硬件指标 7
7. 数字证书技术规范 8
7.1 数字证书格式 8
7.1.1 数字证书基本结构 8
7.1.2 基本证书域 8
7.1.3 证书扩展项及数据结构 9
7.2 标准扩展 9
7.2.1 颁发机构密钥标识符 10
7.2.2 主体密钥标识符 Subject Key Identifier 10
7.2.3 密钥用法 10
7.2.4 扩展密钥用法 10
7.2.5 证书策略 11
7.2.6 基本限制 11
7.2.7 互联网证书扩展 11

辽宁省地方标准

7.3 证书撤销列表格式 11
8. CA 认证机构接入规范 14
8.1 系统接入总体要求 14
8.2 CA 系统功能要求 14
8.3 CA 系统接入接口要求 15
8.3.1. 注册用户到平台接口 15
8.3.2. 更新平台用户的数字证书接口 15
9. 数字证书应用集成规范 15
9.1 应用集成目标 15
9.2 应用集成要求 16
9.3 应用集成内容 16
9.4 统一证书应用接口规范 17
9.4.1 客户端接口 17
9.4.2 服务端接口 18
9.5 应用接入规范 18
9.4.3 提交创建应用 18
9.4.4 应用集成 SDK 18

辽宁省地方标准

公共资源交易 数字证书（CA）互联互通技术规范

Ukey 载体部分

1. 适用范围

本规范描述了支持的数字证书介质的各项要求，包括对安全机制、软件要求、硬件指标、数字证书应用集成等要求，用于指导电子认证服务机构在平台内进行数字证书介质的定制和选型。规范性引用文件

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（包括所有修改单）适用于本文件。

《GB/T 35275-2017 信息安全技术 SM2 密码算法加密签名消息语法规范》

《GB/T 35276-2017 信息安全技术 SM2 密码算法使用规范》

《GB/T 35291-2017 信息安全技术 智能密码钥匙应用接口规范》

《GB/T 36322-2018 信息安全技术 密码设备应用接口规范》

《GB/T 38540-2020 信息安全技术 安全电子签章密码技术规范》

《GB/T 38629-2020 信息安全技术 签名验签服务器技术规范》

《GM/T 0020-2012 证书应用综合服务接口规范》

《GM_T 0025-2014 SSL VPN 网关产品规范》

《GM/T 0026-2014 安全认证网关产品规范》

《GM/T 0033-2014 时间戳接口规范》

《GB/T 7408-2005 数据和交换格式信息交换日期和时间表示法》

《GB 18030-2005 信息技术中文编码字符集》

《GB/T 7027-2002 信息分类和编码的基本原则与方法》

《GMT 0034-2014 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》

《GBT 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》

3. 术语和定义

3.1 招标投标相关的术语及定义

3.1.1 电子招标投标

根据招标投标相关法律法规规章，以数据电文为主要载体，应用信息技术完成招标投标活动的过程。

数据电文是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。本规范中的“电子文件”是指按照特定用途和规定的内容格式要求编辑生成的数据电文。

3.1.2 招标人

提出并组织实施招标项目的法人或其他组织。

3.1.3 招标代理机构

依法设立并提供招标代理服务的社会中介组织。

3.1.4 投标人

参加招投标活动，有意向为招标人提供工程、货物和服务的法人、其他组织或自然人。

3.2 平台及工具软件

3.2.1 公共服务平台

为满足各电子招标投标交易平台之间信息对接交换、资源共享的需要，并为市场主体、行政监督部门和社会公众提供信息交换、整合和发布的信息平台。公共服务平台具有招标投标相关信息对接交换、招标公告和公示发布、主体共享、CA 互联、智能交互、资格信用和业绩验证、行业统计分析、连接评标专家库、提供行政监督通道等服务功能。

公共服务平台是为对接互联电子招标投标交易平台与监督平台、入场交易中心，并为市场主体、监督部门和社会公众交互聚合、公开共享和智能分析招标投标交易基本信息以及提供相关公

共技术支持的服务枢纽。

3.2.2 电子招标投标交易平台

通过网络技术以数据电文为主要载体，进行信息交换与传递，并为招标投标管理、交易、监督提供软件系统支撑的电子招标投标系统。

电子招标投标交易平台主要用于在线完成招标投标的全部交易过程，编辑、生成、对接、交换和发布有关招标交易数据信息。

3.2.3 工具软件

与交易平台兼容对接，用于制作、生成项目投标报价文件的标书制作工具、项目开标工具及专家评标工具等电子招标投标过程中使用的工具软件。

3.2.4 平台及工具软件标识码

按照交易平台、公共服务平台、行政监督平台、发布工具的行业、区域、注册登记顺序，以特定的编码规则赋码，作为该平台或发布工具在电子招标投标网络体系中信息交互共享的唯一识别码。

3.3 主体的术语及定义

3.3.1 主体

招投标市场的参与者，使用电子招标投标系统或者工具软件进行电子招标投标活动的自然人、组织机构、国外企业等。

一个主体可以通过主体代码类型、主体代码、主体名称概念共同描述。

3.3.2 主体代码类型

主体包含招标交易主体、平台运营机构、监督机构等各类法人和其他组织，以及个人。

3.3.3 主体名称

主体的名称，可为组织机构名称、自然人姓名、国外企业名称等。

3.4 CA 数字证书相关的术语定义

3.4.1 CA

依据《电子签名法》和《电子认证服务管理办法》获得《电子认证服务许可证》向公众提供电子认证业务的机构，也称为电子认证服务机构。

3.4.2 数字证书

由 CA 基于 PKI 技术签发、认证和管理的一个可信数字化文件，具有数据电文交换中身份识别、电子签名、加密解密等功能。按主体不同，可分为个人证书、单位证书。

3.4.3 加密证书

用于证明加密公钥的数字证书，其中包含的公钥用来加密数据。

3.4.4 签名证书

用于证明签名公钥的数字证书，其中包含的公钥用来认证数字签名，而不能加密数据或执行其他的密码功能。

3.4.5 用户

参与电子招标交易的市场主体。

3.4.6 数字证书使用入口

交易平台/交易工具为用户提供的使用数字证书的入口。根据允许使用的数字证书不同，可以分为省内统一入口和省外互联入口，其中，省内统一入口是指可以使用省内数字证书的入口，省外互联入口是指可以支持省外数字证书漫游使用的入口。

3.4.7 加密

对数据进行密码变换以产生密文的过程。

3.4.8 解密

将密文转化为明文的过程。

辽宁省地方标准

3.4.9 数字签名

附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接受者确认数据单元的来源和完整性，并防止数据单元被人伪造。

3.4.10 电子签章

利用图像处理技术、电子签名技术将数字签名操作转化为与纸质文件盖章操作相同的可视效果，并保障电子信息真实性、完整性以及签名人不可否认性的过程。

4. 安全机制

4.1 密钥管理

数字证书介质的密钥空间必须能够至少保存 2 对 RSA 密钥对，2 对 SM2 密钥对和 2 个对称密钥（包含 1 个设备认证密钥和 1 个会话密钥的空间）。所有密钥必须安全存储。签名私钥必须在数字证书介质内生成，且不能以任何形式导出。加密私钥以密文方式导入，且不能以任何形式导出，对称密钥不能以明文导出。

4.2 数字证书介质的扩展区要求

数字证书介质内可创建用户私有文件区，对私有文件区操作时，用户应输入介质口令进行验证，扩展区的空间大小不小于 64K。

5. 软件要求

5.1 数字证书介质接口要求

介质接口及数据类型必须遵循国家密码管理局《智能密码钥匙密码应用接口规范》的要求，提供设备管理、访问控制、文件管理和密码服务等相关服务接口。介质有应用、容器，应用中可有多个容器，容器中可有多个私钥和证书。介质初始化后，无应用，无容器。

5.2 设备管理接口

设备管理主要完成介质的插拔事件处理、枚举设备、连接设备、断开连接、获取设备状态、设置设备标签，锁定设备、解锁设备和设备命令传输等操作。

设备管理接口函数如下表所示：

函数名称	功能
SKF_WaitForDevEvent	等待设备插拔事件
SKF_CancelWaitForDevEvent	取消等待设备插拔事件
SKF_EnumDev	枚举设备
SKF_ConnectDev	连接设备
SKF_DisconnectDev	断开设备
SKF_GetDevState	获取设备状态
SKF_SetLabel	设置设备标签
SKF_GetDevInfo	获取设备信息
SKF_LockDev	锁定设备
SKF_UnlockDev	解锁设备
SKF_Transmit	设备命令传输

5.3 访问控制接口

访问控制主要完成设备认证、PIN 码管理和安全状态管理等操作。

5.4 应用管理接口

应用管理主要完成应用的创建、枚举、删除、打开和关闭等操作。

5.5 文件管理接口

文件管理接口函数用以满足用户扩展开发（如签章）的需要，包括创建文件、删除文件、枚举文件、获取文件信息、文件读写操作。

5.6 容器管理接口

容器管理接口函数用于创建、删除、枚举、打开和关闭容器。

6. 数字证书介质驱动安装程序要求

6.1 电子认证服务机构提供的数字证书介质安装程序应满足以下要求：

1) 提供无界面的安装程序，或支持无界面的安装指令。

2) 介质安装程序应支持 WINXP、WIN7、WIN8、WIN10 等主流 32 位和 64 位操作系统。

3) 驱动程序在驱动注册到 CSP 时，需要在相应注册表中添加键值为 SKFImage Path 注册项，该项内容应该包含一个指向 SKF 接口驱动文件的路径。

4) 安装程序可以在菜单或控制面板的“添加/删除程序”中卸载程序，卸载驱动程序时，不需要用户手动干预，能自动完成卸载。

5) 提供无 CSP 工具硬件驱动安装包（免驱设备无需提供）。

6.2 密码服务接口

密码服务接口函数提供对称算法运算、非对称算法运算、密码杂凑算法运算、密钥管理、消息鉴别码计算等功能。

6.3 硬件指标

标准名称	必要条件	备注
存储容量	>=64 Bytes	
非对称算法	遵循国密相关规范，如 SM2 等。	密钥对必须在芯片中生成，私钥不可导出。
对称算法	应遵循国密相关规范，如 SSF33、SM1、SM4 等。	
支持摘要算法	应遵循国密相关规范，如 SHA1、SHA256、SM3 等。	
RSA 数字签名和验证时间	<500 毫秒/次	
SM2 数字签名和验证	<500 毫秒/次	

时间		
RSA 公钥加密和私钥解密效率	>4 Kbit/s	
SM2 公钥加密和私钥解密效率	>4 Kbit/s	
存储要求	公私密钥对：>=4 对（2 对 RSA 密钥对，2 对 SM2 密钥对） 必须在提供保护口令前提下才能访问密钥	

7. 数字证书技术规范

7.1 数字证书格式

7.1.1 数字证书基本结构

数字证书结构采用 ANS.1 DER 编码，基本结构由基本证书域 TBSCertificate、签名算法域 SignatureAlgorithm 和签名值 SignatureValue 三部分组成。

7.1.2 基本证书域

基本证书域包含了证书结构中主体名称及颁发者 CA 等信息，这些信息主要包括版本、序列号、签名算法、颁发者、有效期、主体、主体公钥信息等。

1） 版本 Version

本项描述了数字证书的版本号。数字证书应使用版本 3（对应的数值是整数“2”）。

2） 序列号 Serial Number

本项是 CA 分配给每张证书的一个正整数，一个 CA 签发的每张证书的序列号必须是唯一的。序列号可以是长整数，最长可为 20 个 8 位字节的序列号值。证书更新时序列号应改变。

3） 签名算法 Signature

本项包含 CA 签发该证书所使用的密码算法的标识符，算法标识符应与证书中 Signature Algorithm 项的算法标识符相同。签名算法必须符合国家密码主管部门对密码算法的规定，并根据国家密码主管部门批准的最新算法及时调整，以适应国家最新技术标准要求。当算法为 SM2 时，算法标识定义见 GM / T 0006-2012《密码应用标识规范》。

4） 颁发者

本项标识了签名和发布数字证书的实体。它必须包含一个非空的甄别名称。

5） 有效期 Validity

本项是指一个时间段，在这个时间段内，CA 担保它将维护关于证书状态的信息。该项被表示成一个具有两个时间值的 SEQUENCE 类型数据：证书有效期的起始时间（notBefore）和证书有效期的终止时间（notAfter）。这两个时间都可作为 UTCTime 类型或者 GeneralizedTime 类型进行编码。GeneralizedTime 值必须用格林威治标准时间表示，且必须包含秒（即时间格式为 YYYYMMDDHHMMSSZ）。

6） 主体 Subject

本项描述了与主体公钥项中的公钥相对应的实体。主体名称可以出现在主体项或主体替换名称扩展项中（SubjectAltName）。如果主体是一个 CA，那么主体项必须与其签发的所有证书的颁发者相同，一个 CA 认证的每个主体实体的甄别名称应是唯一的。一个 CA 可以为同一个主体实体以相同的甄别名称签发多个证书。该项不能为空。该项被定义为 X.501 的 Name 类型。

7） 主体公钥信息

本项用来标识公钥和相应的公钥算法。公钥算法使用算法标识符 Algorithm Identifier 结构来表示。当算法为 SM2 时，算法标识定义见 GM / T 0006-2012《密码应用标识规范》。

7.1.3 证书扩展项及数据结构

本规范定义的证书扩展项提供了把一些附加属性同用户或公钥相关联的方法以及证书结构的管理方法。数字证书允许定义标准扩展项和专用扩展项。每个证书中的扩展可以定义成关键性的和非关键性的。一个扩展含有三部分，它们分别是扩展类型、扩展关键度和扩展项值。扩展关键度告诉一个证书的使用者是否可以忽略某一扩展类型。证书的应用系统如果不能识别关键的扩展时，必须拒绝接受该证书，如果不能识别非关键的扩展，则可以忽略该扩展项的信息。

遵循本标准的 CA 必须支持密钥标识符、基本限制、密钥用法和证书策略等扩展。遵循本标准的应用必须至少能够识别密钥用法、证书策略、基本限制、颁发机构密钥标识符、主体密钥标识符和扩展的密钥用法。

7.2 标准扩展

7.2.1 颁发机构密钥标识符

本项提供了一种方式，以识别与证书签名私钥相应的公钥。当颁发者由于有多个密钥共存或由于发生变化而具有多个签名密钥时使用该扩展。识别可基于颁发者证书中的主体密钥标识符或基于颁发者的名称和序列号。

本项既可用作证书扩展亦可用作 CRL 扩展。本项标识用来验证在证书或 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。除了自签名证书外，所有证书必须包含本项，且必须为非关键扩展。

7.2.2 主体密钥标识符 Subject Key Identifier

本项提供一种识别包含有一个特定公钥的证书的方法。此扩展标识了被认证的公开密钥，它能够区分同一主体使用的不同密钥。

对于使用密钥标识符的主体的各个密钥标识符而言，每一个密钥标识符均应是唯一的。CA 签发证书时必须把 CA 证书中本扩展的值赋给终端实体证书 AuthorityKeyIdentifier 扩展中的 KeyIdentifier 项。 CA 证书的主体密钥标识符应从公钥中或者生成唯一值的方法中导出。终端实体证书的主体密钥标识符应从公钥中导出。

7.2.3 密钥用法

密钥用法扩展定义了证书中密钥的用途（如加密、签名、签发证书等）。密钥用法的限制可用于限定密钥是否能够用于某种操作。

所有的 CA 证书必须包括本扩展，而且必须包含 keyCertSign 这一密钥用途。用户证书则根据证书用途，分“签名”证书和“加密”证书，选择对应的密钥用途进行签发。此扩展可定义为关键的或非关键的，由证书颁发者选择。

7.2.4 扩展密钥用法

本项指明已验证的数字证书公钥可以用于的一种或多种用途，可作为密钥用法扩展项中指明的基本用途的补充或替代。

7.2.5 证书策略

本项包含了一系列策略信息条目，每个条目都有一个 OID 和一个可选的限定条件。

在用户证书中，这些策略信息条目描述了证书发放所依据的策略以及证书的应用目的；在 CA 证书中，这些策略条目指定了包含这个证书的验证路径的策略集合。

7.2.6 基本限制

本项用于识别证书主体是否是一个 CA，通过该 CA 可能存在的认证路径有多长。pathLenConstraint 字段仅在 CA 设置为 TRUE 时才有意义。它给出本证书之后认证路径中最多的 CA 证书数量。0 指明只可以向终端实体签发证书，本项出现时必须大于或等于 0。若未出现，则对人这功能路径的允许长度没有限制。CA 证书中必须包含本扩展且标记为关键扩展。

7.2.7 互联网证书扩展

1) 主体信息访问

本项指明了证书主体如何访问信息和服务，当证书主体是 CA 时，信息和服务中包含证书验证服务和 CA 策略数据，如果主体是终端用户，则描述提供的服务类型以及如何访问。本项可以包含在用户或 CA 证书中吗，且必须为非关键扩展项。

2) 机构信息访问

本项指明了包含本项扩展的证书颁发者如何获得 CA 信息和服务。信息和服务包括在线验证服务和 CA 策略数据。本项可以包含在用户证书和 CA 证书中，且必须为非关键扩展。

7.3 证书撤销列表格式

证书撤销列表（CRL）是由 CA 签发的、加盖时间标记已撤销的数字证书列表，CRL 公开发布，可用于业务系统鉴别数字证书的有效性。其结构采用 ANS.1 DER 编码。

1) TBSCertList 结构

TBSCertList 也可称为待签发的数字证书列表，主要包含了版本号、签名算法、颁发者、生效日期、下次更新时间、被撤销的证书列表、扩展项。

2) 版本号

CRL 版本号采用 v2 ，数值为“1”，表示版本 2 （V2）

3) 签名算法

CA 签发 CRL 所使用的密码算法的标识符，该算法必须与 CertificateList 中的 signatureAlgorithm 相同，当算法为 SM2 时，算法标识定义见 GM / T 0006-2012《密码应用标识规范》。

4) 颁发者

本项标识了签名并发布 CRL 的实体，颁发者必须包含一个非空的 X.500 甄别名称，颁发者名称字段定义为 X.501 类型 Name。

5) 生效日期

本项标识了 CRL 的办法日期，可以使用 UTCTime 或 GeneralizedTime 编码。遵循本标准的 CA 在 2049 年以前必须使用 UTCTime 编码本项，在 2050 年以后，必须使用 GeneralizedTime 编码本项。

6) 下次更新日期

本项标识了 CRL 的下次颁发时间，下次 CRL 可以在此时间之前签发，但不能晚于此时间签发。遵循本标准的 CA 签发 CRL 时必须包含 nextUpdate。

7) 被撤销的证书列表

当没有被撤销的证书时，证书撤销列表必须为空。否则被撤销的证书列表是一个集合，其中每一条 CA 机构撤销的证书都包含证书序列号、撤销时间、撤销理由。被 CA 撤销的证书由证书序列号唯一标识。

8) 扩展项

本项仅在 CRL version 为 2 时出现，如果出现，本项必须是一个或多个 CRL 扩展的序列。

9) CRL 扩展项及数据结构

CRL 扩展项采用 ANS.1 编码，每个 CRL 中的扩展项可以被指定为关键或非关键扩展。

10) 颁发机构密钥标识符

颁发机构密钥标识符识提供了一种识别与 CRL 签名私钥相对应的公钥的方式。在颁发者因有多个签名密钥对或签名密钥发生变化而同时具有多个签名私钥时，可通过本项有效识别出颁发者。

11) 颁发者可替换名称

本项是一个非关键扩展，可包含一个或多个可替换名称以供 CRL 颁发者使用。

12) 证书撤销列表号

本项是一个非关键的 CRL 扩展，表示 CA 机构为其签发的每个 CRL 分配一个单调增长的序列号。用户可通过本项确定一个特定的 CRL 何时取代另一个 CRL，遵守本标准的 CA 必须使用不大于 20 字节的证书撤销列表号。

13) 增量证书撤销列表指示

本项是一个关键的 CRL 扩展，表明一个 CRL 是增量 CRL。在一些存储为非 CRL 结构格式的应用中，使用增量 CRL 能够显著的减少处理时间。

14) 颁发分布点

本项是一个关键 CRL 扩展，表明一个特定 CRL 的分发点和范围，还表明这个 CRL 是否只包含了用户证书的撤销、CA 证书的撤销或者一系列的原因代码。

15) 最新证书撤销列表

本项扩展确定了如何获取完整 CRL 的增量 CRL 信息，本项必须为非关键扩展，并且不能出现在增量 CRL 中。

16) 证书撤销列表条目扩展

本标准中所有的证书撤销列表条目扩展都是非关键扩展。无论本项是否可用，CRL 颁发者都应该包括原因代码和撤销时间。

17) 原因代码

本项为非关键扩展，表明证书撤销的原因。CA 应尽可能在证书撤销列表条目中使用有意义的原因代码。如果的确是没有原因，可以选择不设置原因代码， 而不是使用“未指定(0)”的原因代码。

18) 撤销时间

本项是一个非关键扩展，表明知道或者怀疑私钥泄漏或者证书失效时间。这个时间可以比证书撤销列表中的撤销时间更早。本项包含的 GeralizedTime 必须使用格林威治标准时间。

19) 证书颁发者

证书撤销列表条目标识了在一个间接 CRL 中条目相关联的证书颁发者。即是一个在颁发者分发点扩展中具有间接 CRL 指示者集合的证书撤销列表。如果本项存在，证书颁发者扩展包含一个或多个和 CRL 条目对应的，从证书的颁发者域或颁发者替换名称域得到的名字。

8. CA 认证机构接入规范

8.1 系统接入总体要求

接入到平台中的电子认证服务机构必须符合以下要求：

1) 电子认证服务机构的 CA 系统建设必须遵循《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》。

2) 电子认证服务机构的 CA 系统应遵循《电子政务电子认证体系建设总体规划》（国密局联字[2007]2 号）中关于电子认证体系建设的相关要求，符合《电子政务电子认证服务管理办法》(国密局发[2009]7)相关要求。电子认证服务机构的 CA 系统必须具有电子认证服务许可证和电子认证服务使用密码许可证。

3) 电子认证服务机构的 CA 系统签发的证书为双证书（签名证书和加密证书），证书格式应遵循《平台数字证书格式规范》，使用的证书介质应符合《平台数字证书介质接口及使用规范》，相关应用接入应符合《平台数字证书应用集成规范》。

电子认证服务机构接入平台，必须满足以下条件：

提供完整的 CA 业务证书链，CA 业务证书链可以是一个或多个；提供的方式可以由 CA 机构直接以文件方式提交，也可以由 CA 机构提交 CA 业务证书链的 LDAP 或 HTTP 链接地址。

4) 提供与 CA 业务证书链相对应的 CRL 发布服务，且按照发布策略及时发布。CA 机构可将 CRL 发布到 LDAP 服务器或 HTTP 服务器上，必须保证 CRL 发布服务可持续访问。

5) 提供稳定在线的在线证书状态查询服务，该服务必须按照 RFC 6960 中定义的 OCSP 协议，提供实时在线查询证书的状态。

8.2 CA 系统功能要求

接入到平台的电子认证服务机构的 CA 系统应该具备如下基本功能：

1) 证书申请/签发

用户可以以在线或离线两种方式向 CA 机构申请数字证书，在线方式指用户通过互联网登录

到 CA 机构的用户注册管理系统申请证书，离线方式指用户到 CA 机构指定的注册机构中申请证书。用户数字证书由 CA 系统的 CA 证书进行签发。CA 机构签发的数字证书格式必须符合《平台数字证书格式规范》。

2) 证书更新

CA 系统应提供证书更新功能，更新可分为证书有效期更新和证书可甄别名称更新。CA 系统在对证书更新后，须撤销更新之前的数字证书。

3) 证书撤销

CA 系统应提供证书撤销功能，证书撤销后，CA 系统应实时将该证书加入证书撤销列表中，并根据 CRL 发布策略及时将 CRL 发布到 CRL 发布服务中。

4) 密钥恢复

CA 系统应提供加密证书的密钥恢复功能，以保证用户可使用恢复的加密证书和加密密钥完成对历史密文信息的解密操作。

5) CRL 签发

CA 系统应提供 CRL 签发功能，并根据 CRL 发布策略及时将 CRL 发布到 CRL 发布服务上。

CA 系统签发的 CRL 必须符合《平台数字证书格式规范》。

8.3 CA 系统接入接口要求

电子认证服务机构的 CA 系统根据业务需要可调用平台提供的 HTTP/HTTPS 接口，实现将数字证书注册到平台以及更新平台中数字证书等功能。

8.3.1. 注册用户到平台接口

CA 系统调用本接口可根据业务需要将用户证书及其他信息（企业名称、企业证件号码、联系电话）注册到平台中。

8.3.2. 更新平台用户的数字证书接口

CA 系统调用本接口可根据业务需要更新已经注册到平台的用户数字证书。

9. 数字证书应用集成规范

9.1 应用集成目标

1) 遵循本规范要求新建或者修改的应用系统，在基于统一认证的多 CA 数字证书的身份认证机制下，可使用不同 CA 机构颁发的数字证书，实现数字证书的互通互认，并确保系统访问控制的高安全性和高可靠性；

2) 对信息系统的重要操作环节和重要数据实现基于多 CA 数字证书的数字签名功能，保护数据的完整性，并为后期纠纷处理及责任认定提供合法电子证据；

3) 对信息系统的敏感信息实现支持多 CA 的数字证书的数据加密功能，确保敏感信息在传输和存储阶段的安全性及多 CA 支持。

9.2 应用集成要求

在证书应用集成时，应根据应用系统本身的业务特点和业务需求，确定需要使用数字证书认证的用户及范围、确定需要加密、签名的重要操作环节和数据，具体集成要求如下：

1) 对于具有操作行为责任认定、证据保存需求的应用系统，应集成基于数字证书的数字签名的功能；

2) 对于具有数据加密和解密需求的信息系统，应集成基于数字证书的信息加密、信息解密功能；

3) 对于具有可信时间需求的应用系统，应集成时间戳功能，时间戳应遵循《GM/T 0033-2014 时间戳接口规范》；

4) 对于具有信息共享需求的多个应用系统，可采用统一的身份认证模式，实现统一的身份认证管理、用户信息共享和单点登录等功能。

9.3 应用集成内容

应用系统数字证书应用集成内容如下：

1) 基于多 CA 数字证书的互通互认的统一身份认证

2) 数字签名和验证。

信息系统中关键业务数据和操作的数字签名，应满足《电子签名法》以及其他相关政策法规规定的书面形式、原件形式及文件保存等要求，至少应包括数据原文、电子签名、可信时间等内容，并可在需要时查询、阅读、下载、验证，具备作为电子证据的真实性、可靠性和可验证性。

数字签名可选和图章结合起来应用，实现电子签章功能，从而实现电子签名的可视化管理，

方便用户查看、审阅和验证。

3) 数据加密和解密

数据加密时应采用对称算法和非对称算法相结合的方式，既保障加密机制的安全性、密钥分发的方便性，同时又提高了加解密操作的效率。根据业务需求，可使用单个数字证书加密，也可使用多个数字证书对数据共同加密，形成密文数据。

4) 密文数据应安全存储在数据库或磁盘上，待解密时间达到后方可解密。数据解密时，须使用数字证书对应的密码设备或证书介质解密。如果证书介质损坏或丢失，电子认证服务机构应在安全可控的前提下，为用户及时提供密钥恢复服务。

5) 时间戳应用

电子认证服务机构提供的时间戳服务应基于可靠的标准时间源，确保时间的准确和可信。

6) 密码设备应用

信息系统在使用数字证书安全功能时，应基于密码设备提供的密码服务。密码设备包括客户端用户使用的证书介质和服务器端使用的密码设备。

客户端证书介质是指具有密码许可资质的 USBKey、智能 IC 卡等 PC 终端上的密码设备，以及符合国家密码政策管理规定的 SIM 卡、SD 卡等手机终端上的密码设备。证书介质应用接口应支持所有主流操作系统，并符合《平台数字证书介质接口及使用规范》。

服务器端密码设备是指具有密码许可资质的加密机、加密卡等，应支持所有主流操作系统，并符合《公钥密码基础设施应用技术体系 密码设备应用接口规范》。

通用密码服务接口调用证书介质应用接口或密码设备应用接口，实现对底层密码设备和证书介质的调用，应支持所有主流操作系统，并符合《公钥密码基础设施应用技术体系通用密码服务接口规范》。

9.4 统一证书应用接口规范

统一证书应用接口是应用系统可直接调用的应用接口，分为客户端接口和服务端接口。

9.4.1 客户端接口

客户端接口是供应用在系统客户端应用程序直接调用的接口，应支持主流操作系统，支持 IE、Chrome、Firefox 等主流浏览器。客户端接口应支持符合《平台数字证书格式标准规范》的数字证

书，支持使用符合《平台数字证书介质接口及使用规范》的证书介质。客户端接口可以以 COM 组件、DLL 动态链接库和 ActiveX 控件的产品形态方式提供，支持 B/S 架构的应用。

9.4.2 服务端接口

服务器端接口是供应用系统服务器端程序直接调用的高级接口，应支持所有主流操作系统，支持 B/S 系统架构，支持符合《平台数字证书格式规范》的数字证书，可通过添加证书信任列表的方式实现不同电子认证服务机构证书之间的交叉认证和互信互认。服务端接口使用 HTTP/HTTPS 作为通讯接口协议，所有的请求都使用 POST 方法，请求参数保存在 POST 表单域内。

9.5 应用接入规范

平台提供了基于多 CA 数字证书互通互认的统一认证服务，为接入到平台的应用系统提供统一身份认证功能。

9.4.3 提交创建应用

应用管理员可向平台提交创建应用。应用管理员可以由平台超级管理员分配。应用系统开发者或管理者可以向平台超级管理员申请应用管理员权限。申请应用管理员权限时需要提供有效的身份证明材料。

提交应用时所需要提交的信息包括：应用名称、应用 LOGO、应用回调地址、应用 URL、应用类型、允许 CA 机构证书、应用图片介绍等，所提交的信息必须真实有效。

应用创建后，可获得由平台分配的 APP ID 和 APP KEY。APP ID 和 APP KEY 是应用系统的身份标识，特别是 APP KEY 不能泄漏或者扩散。

9.4.4 应用集成 SDK

应用开发者下载平台提供的平台接入 SDK，使用在上一步中的 APP ID 和 APP KEY 作为身份标识，修改应用以集成到平台。修改的内容包括：

1) 在应用首页放置“平台统一认证登录”链接，引导用户到平台统一认证服务进行身份认证。

2) 平台提供了多个 API，详见平台 OpenAPI 列表。应用开发者应遵循 OAuth2.0 规范，根据需要使用平台提供的多语言的 SDK 以更快地实现 OpenAPI 的调用，完成用户授权确认、身份

认证的流程。

3) 应用接入完成后，需要进行开发调试，开发调试完成后，即可由应用管理员为该应用申请上线。

辽宁省地方标准