黑龙江省数字证书认证有限公司
电子认证业务规则

2.0 版

黑龙江省数字证书认证有限公司

2022 年 2 月

目 录

1 概括性描述

1.1 概述

黑龙江省数字证书认证有限公司（简称 HLJCA），于 2006 年 12 月 4 日成立，是全省唯一从事跨行业数字证书签发的权威性机构，是获得国家密码管理局审批的商用密码产品使用和销售单位，是由中国联通集团参股的企业，严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》的要求及有关规定开展业务，为信息安全提供综合服务的有限责任公司，是政府指定的黑龙江地区数字证书安全认证体系的建设与管理主体。

HLJCA 电子认证业务规则（以下简称《电子认证业务规则》）严格按照工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范(试行)》制定，并报工业和信息化部备案。HLJCA 对所提供的全部证书服务生命周期中的业务实践（如签发、吊销、更新证书或密钥）所遵循规范的详细描述和声明（包括责任范围、作业操作规范和信息安全保障措施等内容）。

本《电子认证业务规则》适用于 HLJCA 及其员工、注册机构、证书申请人、订户和依赖方，各参与方必须完整地理解和执行本《电子认证业务规则》所规定的条款，并承担相应的责任和业务。

1.2 文档名称与标识

本文档名称为《黑龙江省数字证书认证公司电子认证业务规则》，是 HLJCA 对所提供的认证及相关业务的全面描述。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

HLJCA 是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构。

电子认证服务机构是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

1.3.2 注册机构

注册机构作为电子认证服务机构授权委托的下属机构，包括注册管理系统（RA 系统）和受理点，负责受理证书申请。

在证书申请人申请证书时，注册机构有责任验证证书申请人提供信息的准确性、可靠性和完整性。

1.3.3 订户

订户是指从 HLJCA 接收证书的实体。在电子签名应用中，订户即为电子签名人。

1.3.4 依赖方

依赖方是依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

在 HLJCA 证书服务体系中，是信任 HLJCA 证书，可以对使用HLJCA 证书机制进行的数字签名进行验证，使用其他 HLJCA 证书的公钥的实体。

HLJCA 负责保证数字证书身份的真实性。

1.3.5 其他参与者

其他参与者是指为 HLJCA 证书服务体系提供相关服务的其他实体。如目录服务提供者等与 PKI 服务相关的参与者。

1.4 证书应用

1.4.1 适合的证书应用

证书申请人、订户和依赖方等各类主体可以根据实际需要，自主判断和决定采用相应类型的证书，以及了解证书的应用类型、应用范围，选择自己的应用方式。

HLJCA 签发的证书，从功能上可以满足下列安全需要：

身份认证：保障采用 HLJCA 的证书持有者身份的真实性；

信息完整性：采用HLJCA 证书进行加密/数字签名时，可以验证信息在传递过程中是否被篡改，发送和接收信息是否完整一致；

数字签名：可以对数字签名的有效性进行验证。

1.4.2 限制的证书应用

HLJCA 发放的数字证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用，由此造成的法律后果由订户自己承担。

1.5 策略管理

1.5.1 策略文档管理机构

本《电子认证业务规则》由黑龙江安全策略管理委员会负责起草、发布、更新等事宜。

1.5.2 联系方式

联系人： 姜欣妍

电话号码：0451-55918888

传真号码：0451-87971111

电子邮件：zhux@hljca.com

网站地址：www.hljca.com.cn

联系地址：黑龙江省哈尔滨市香坊区公滨路 483 号；
黑龙江省哈尔滨市道外区东直路 482 号。

邮政编码：150000

1.5.3 决定 CPS 符合策略的机构

本《电子认证业务规则》由 HLJCA 安全策略管理委员会负责最后的审批和实施。

1.5.4 CPS 批准程序

本《电子认证业务规则》由 HLJCA 安全策略管理委员会组织 CPS 的编写，CPS 草案完成后，由 HLJCA 安全策略管理委员会进行 CPS 草案初步评审。初步评审后，将 CPS 评审稿提交 HLJCA 安全策略管理委员会审批。经 HLJCA 安全策略管理委员会审批通过后，在服务范围内进行发布。

本《电子认证业务规则》经 HLJCA 安全策略管理委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

1.6 定义和缩写

下列定义适用于本《电子认证业务规则》。

公开密钥基础设施（PKI）Public Key Infrastructure

支持公开密钥的管理并提供真实性、保密性、完整性以及可追究性安全服务的具有普适性的安全基础设施。

证书策略（CP）Certificate Policy

是一个指定的规则集合，它指出证书对于具有普通安全需求的一个特定团体和（或）具体应用类的适用性。

电子认证业务规则（CPS）Certification Practice Statement

关于证书电子认证服务机构在签发、管理、吊销、更新证书（或密钥）过程中所采纳的业务实践的声明。

电子认证服务机构（CA）Certification Authority

受用户信任，负责创建和分配公钥证书的权威机构。

注册机构（RA）Registration Authority

RA 是 CA 认证体系的一个功能组件，具有下列一项或多项功能的实体：识别和鉴别证书申请者，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理订户撤销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。

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

用于查询、下载数字证书以及证书撤销列表（CRL）。

证书撤销列表（CRL）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，供数字证书使用者在认证对方数字证书时查询使用。CRL 通常又被称为数字证书黑名单。内容通常还包含列表发行人的姓名、发行日期、下次废止列表的预定发行日期、更新或废止的数字证书序号，并说明更新或废止的时间与理由。声明了主体的名字或签发中心的身份，确定签名者的身份，包括签名者的公开密钥，表明了数字证书的操作时限，还包括数字证书的序列号。

电子签名认证证书（证书）Digital Certificate

是电子认证服务提供者签发的用以证明证书持有人的电子签名、身份、资格及其他有关信息的电子文件。证书包含公开密钥拥有者的信息、公开密钥、签名算法和 CA 的数字签名。

证书持有者、订户 subscriber

所有拥有任何 HLJCA 证书的个人或实体，不包括 HLJCA 管理员证书。

证书使用者、依赖方 relying party

使用证书中的数据进行决策的用户或代理。

私钥（电子签名制作数据） private key

指在公钥密码系统中，用户的密钥对中只有用户本身才能持有的密钥，是在电子签名过程中使用的，将电子签名和电子签名人可靠地联系起来的字符、编码等数据。

私钥是经由数字运算产生的密钥，用于制作电子签名数据，亦可依据其运算方式，就相应的公开密钥加密的文件或信息予以解密。

公钥（电子签名验证数据）public key

指在公钥密码系统中，用户的密钥对中可以被其它用户所持有的密钥。

公钥是经由数字运算产生的密钥，用于解密电子签名确认电子签名人的身份及电子签名的真实性。

公钥可以公开，一般标示于在线数据库、存储库或其他公共目录中，使任何希望得到公钥的人都能得到。

电子签名验证数据是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。如果电子签名制作数据表现为私钥，则电子签名验证数据就是公钥。

HLJCA 管理员证书

HLJCA 管理员证书的组成情况：超级管理员证书、业务管理员证书、业务操作员证书、审计管理员证书、各系统之间的通讯证书、CA 根证书等。

2 信息发布与信息管理

2.1 认证信息的发布

HLJCA 通过网站公布以下信息：《电子认证业务规则》修订及其他由 HLJCA 不定时发出的信息。CA 网址：http://www.hljca.com.cn。

本《电子认证业务规则》发布在 HLJCA 网站上，供相关方下载、查阅。

HLJCA 通过目录服务器发布订户的证书和 CRL，订户或依赖方可以通过 HLJCA LDAP 服务器获取证书的信息和证书撤销列表。同时，HLJCA 提供在线证书状态查询服务。（LDAP 查询因证书项可能涉及订户个人敏感信息，按照新的个人信息保护相关法律法规，不应公开发布。CA 机构有几种处理方法，一是仅对订户和依赖方提供查询入口，二是精确条件查询，三是获得订户明确授权后公开查询。）

OCSP 查询：http://218.7.71.19:9090/certauthquery/certcheck.do ；
LDAP 查询：218.7.71.18:10002；
链接：
https://pan.baidu.com/s/1bPTcJsJy6TrZ4WTvLC2c0w?pwd=pebv
提取码：pebv。

2.2 发布的时间或频率

《电子认证业务规则》一经发布，即时生效。对数字证书的订户及证书申请人均具备约束力。对具体个人不另行通知。

证书的发布：在证书签发时，HLJCA 通过 LDAP 自动将该证书公布。

HLJCA 的 CRL 每 24 小时自动更新，也可通过人工发布最新 CRL。

2.3 信息库访问控制

对于公开发布的 CPS、证书、CRL 等公开信息，HLJCA 允许证书使用者自行通过网站和LDAP 进行查询和访问。

HLJCA 设置了信息访问及控制权限，保证只有经过授权的 CA/RA 管理员才能查询电子认证服务机构和注册机构数据库中的其他数据。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

每个订户对应一个甄别名（Distinguished Name，简称 DN），DN 包含于每张证书的主题中，唯一标识证书用户的身份。

数字证书中的主体的X.500 DN应是C=CN命名空间下的X.500 目录唯一名字。

3.1.2 对名称意义化的要求

订户的甄别名必须具有一定的代表意义。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中绑定的实体信息。

3.1.3 订户的匿名或伪名

在 HLJCA 证书服务体系中，不允许订户（证书申请人）使用匿名或伪名。

3.1.4 理解不同名称形式的规则

DN 的具体内容由以下部分组成：

C，表示国家，内容为：中国（或 CN）。

S，表示省份，所在省份

L，表示城市，所在城市

O，表示单位或机构名称

OU，表示部门名称

CN，表示通用名

3.1.5 名称的唯一性

在 HLJCA 证书服务体系中，证书主体名称必须是唯一的。

3.1.6 商标的识别、鉴别和角色

本《电子认证业务规则》受到完全的版权保护，本文件中涉及的“HLJCA ”及其图标等是由黑龙江省数字证书认证有限公司独立持有的专有商标。其他参与者的商标为其拥有方所有。

HLJCA 签发的证书主体甄别名中将不包含商标名。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。在 HLJCA 证书服务体系中，私钥在用户端生成，证书请求信息中包含用私钥进行的数字签名，CA 用其对应的公钥来验证这个签名。

HLJCA 要求证书申请人必须妥善保管自己的私钥，因此，证书申请人视作其私钥的唯一持有者。

3.2.2 组织机构身份的鉴别

本条对组织机构的身份鉴别适用于单位身份证书。

单位申请者填写《数字证书申请表》，经过单位授权代表的签署及单位盖章后，携带以下资料到 HLJCA 进行身份审核及办理交费手续 （以下证件的复印件和申请表需要单位盖章证明）：

a）申请单位的营业执照副本及复印件，如果没有营业执照，则提供书面申请表上可选的其他有效证件的副本及复印件；部分有效证件如下：

营业执照 （三证合一）

企业法人营业执照

事业单位登记证

事业单位法人登记证

社会团体登记证

社会团体法人登记证

人民团体登记证

人民团体法人登记证

政府批文

其他有效证件

b）经办人身份证原件与复印件。

HLJCA的审核人员核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行表面审查，并进行批准或拒绝的操作。

c）黑龙江CA认可的其他合适的形式。

3.2.3 个人身份的鉴别

本条对个人身份的鉴别，适用于个人身份证书。

HLJCA的个人证书签发给合法的个人申请者，HLJCA需要审核个人申请者的身份。

个人申请者填写《数字证书申请表》，个人签字后，携带个人身份证（或军官证、护照等）原件与复印件到 HLJCA进行身份审核及办理交费手续。

HLJCA的审核人员核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行表面审查，并进行批准或拒绝的操作。

黑龙江CA认可的其他合适的形式。

3.2.4 没有验证的订户信息

订户提交鉴证文件以外的信息为没有验证的订户信息。

3.2.5 授权确认

为确保办理人具有特定的许可，代表组织获取数字证书，需要出具组织授权其该组织为办理 HLJCA 数字证书事宜的授权文件。

组织在 HLJCA 的数字证书申请表上加盖单位公章后，则证明本组织对办理人的授权确认。

3.2.6 互操作准则

对于非 HLJCA 的其它机构，如果双方之间有协议，那么HLJCA 将依据协议的

内容，接受该机构鉴别过的信息，并为之签发相应的证书。如果双方没有任何类似的协议，HLJCA 要求该机构要严格按照本《电子认证业务规则》的规定鉴别身份信息。HLJCA 会根据情况决定是否接受这些被鉴定审核过的材料，并作出是否接受受理的决定。

如果国家法律法规对此有规定，HLJCA 将严格予以执行。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

在常规密钥更新中，通过订户使用当前有效私钥对包含新公钥的密钥更新请求进行签名，HLJCA 使用订户原有公钥验证确认签名来进行订户身份标识和鉴别。

3.3.2 吊销后密钥更新的标识与鉴别

吊销后密钥更新中对身份标识和鉴别的要求，使用原始身份验证相同的流程，详见 §3.2.2 组织机构身份的鉴别、 §3.2.3 个人身份的鉴别。

3.4 吊销请求的标识与鉴别

订户本人吊销时的身份标识和鉴别使用原始身份验证相同的流程，详见 §3.2.2 组织机构身份的鉴别、 §3.2.3 个人身份的鉴别。

如果是因为订户没有履行本《电子认证业务规则》所规定的义务，由注册机构申请吊销订户的证书时，不需要对订户身份进行标识和鉴别。

4 证书生命周期操作要求

HLJCA 提供数字证书授权、申请、发放、变更、查询和管理等服务，提供网络信息安全及身份认证、电子签名、密钥管理等与数字证书密切相关的配套服务。本章节说明在证书生命周期方面对电子认证服务机构及相关实体的要求。

4.1 证书申请

4.1.1 证书申请实体

证书申请实体包含个人、企业单位、事业单位、社会团体、人民团体等各类组织机构以及 CA、RA、受理点和 CA 机构或 RA 机构的系统及相应的管理员。

4.1.2 注册过程与责任

证书申请人按照本《电子认证业务规则》所规定的要求，填写《数字证书申请表》，并准备相关的身份证明材料。HLJCA 依据身份鉴别规范对证书申请人的身份进行审核，并决定是否受理申请。

申请过程中各方责任为：订户要按照本《电子认证业务规则》的要求准备证书申请材料，并确保申请材料填写注册机构负责接收证书申请人的请求材料，对订户所提供的证书申请信息与身份证明资料的一致性进行审核。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

HLJCA 按照本《电子认证业务规则》所规定的身份鉴别流程对证书申请人的身份进行识别与鉴别。具体的鉴别流程详见 §3.2.2 组织机构身份的鉴别、 §3.2.3 个人身份的鉴别。

4.2.2 证书申请批准和拒绝

HLJCA 根据本《电子认证业务规则》所规定的身份鉴别流程对证书申请人的身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人通过本《电子认证业务规则》所规定的身份鉴别流程且鉴别结果为合格，HLJCA 将批准证书申请，为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴别，HLJCA 将拒绝申请人的证书申请，并通知申请人鉴别识别，同时向申请人提供失败的原因（法律禁止的除外）。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

电子认证服务机构处理证书申请在其规定的时间（三个工作日）内完成。处理证书申请材料的人员在进行身份鉴别后，根据数字证书的受理及制作流程，证书业务受理人员处理证书申请材料时，由双人控制，即录入人员对订户信息进行录入操作，审核人员对所录入信息正确性进行确认（录入人员与审核人员不兼任），最后制证人员完成证书的写入工作。

4.2.4 处理证书申请提交人的核查

HLJCA 对申请提交人的授权文件进行核查，只有通过审查才能受理数字证书申请材料，审核内容一般包括以下内容：

1）数字证书申请表；

2）营业执照原件及复印件；

3）法人及经办人身份证原件及复印件；

4）申请材料的复印件均需加盖有单位公章；

5）个人办理数字证书需申请人签字。

4.3 证书签发

4.3.1 证书所含信息的审核验证及获得证书的方式

数字证书中至少包括以下内容：

1、电子认证服务提供者名称；

2、证书持有人姓名；

3、证书序列号；

4、证书有效期；

5、证书持有人的电子签名验证数据；

6、电子认证服务提供者提供的电子签名。

制作数字证书及证书中所包含的信息都经过了审核，只有审核通过的用户才能制作数字证书。在订户提供证书制作资料并通过身份真实性确认后一般在 3 个工作日可以接收数字证书。HLJCA 也采取电话短信、现场等方式通知，证书申请者获得数字证书方式一般采取通过邮寄、现场窗口进行颁发。

4.3.2 证书签发中电子认证服务机构的行为

HLJCA 批准证书申请后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

通常，HLJCA 所签发的证书在 24 小时后才生效。（与 CRL 列表发布时间一致）

4.3.3 电子认证服务机构对订户的通告

电子认证服务机构，对订户的通告有以下几种方式：

a）通过现场面对面的方式，HLJCA 把证书直接提交给订户，并告知订户证书信息已经正确生成；

b） 电话短信通知订户；

c）其他 HLJCA 认为安全可行的方式通知订户。

4.4 证书接受

4.4.1 构成接受证书的行为

数字证书签发完成后，注册机构将数字证书当面或者寄送给证书申请者，证书申请者从获得数字证书起，就被视为同意接受证书。

4.4.2 电子认证服务机构对证书的发布

HLJCA 在签发完证书后，就将证书发布到数据库和目录服务器中。

HLJCA 采用主、从目录服务器结构来发布所签发证书。签发完成的数据直接写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动发布到从

目录服务器中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

其他实体可以通过从目录服务器中查询到 HLJCA 已经签发的数字证书。

4.4.4 证书申请者接受证书的步骤和操作

HLJCA 目前主要以现场和线上的方式将载有证书和私钥的证书直接交付给用户，在这种情况下由HLJCA 代替用户产生证书申请和下载证书，将数字证书当面或者寄送给证书申请者，证书申请者从获得数字证书起，就被视为同意接受证书。

4.4.5 证书申请者已接受的证书发布到证书资料库

HLJCA 签发证书后， 24 小时内将证书的相关信息自动发布到目录服务器，订户可以通过www.hljca.com.cn网站进行证书信息查询。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在提交了证书申请并接受了HLJCA 所签发的证书后，均视为已经同意遵守与 HLJCA、依赖方有关的权利和义务的条款。订户接受数字证书后，应妥善保存其证书对应的私钥。

订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书之后才能使用对应的私钥，并且在证书到期或被吊销之后，订户必须停止使用该证书对应的私钥。

4.5.2 信赖方公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了

解对方的身份，并通过公钥验证对方电子签名的真实性。验证证书的有效性包括三个方面的内容：

a）用 HLJCA 的证书验证证书中的签名，确认该证书是 HLJCA 签发的，并且证书的内容没有被篡改。

b）检验证书的有效期，确认该证书在有效期之内。

c）查询证书状态，确认该证书没有被注销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

4.6 证书更新

4.6.1 证书更新的情形

证书更新是指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书。

在证书上都有明确的证书有效期，表明该证书的起始日期与截至日期。订户应当在证书有效期到期前，到 HLJCA 申请更新证书。

证书更新的具体情形如下：

a）证书的有效期将要到期；

b）密钥对的使用期将要到期；

c）因私钥泄漏而吊销证书后，就需要进行证书更新；

d）其他。

4.6.2 请求证书更新的实体

订户可以请求证书更新。

订户包括持有 HLJCA 签发的个人、机构等各类证书的证书持有人。

4.6.3 证书更新请求的处理

申请者到 HLJCA 填写《数字证书申请表》，并注明更新的原因。如果申请人是终端用户，则由终端用户填写该表单；

HLJCA 对申请者资料及申请表单进行识别与鉴定，然后对用户提交的证书更新申请进行审核，最后进行更新制证。

4.6.4 颁发更新证书时对订户的通告

HLJCA 服务机构颁发更新证书时对订户的通告为当面通知、电话、短信通知和网上在线查询。

4.6.5 构成接受更新证书的行为

当更新证书签发后，注册机构将数字证书当面或寄送给订户，或由订户自行下载。订户从获得数字证书起，就被视为同意接受更新证书。

4.6.6 电子认证服务机构对更新证书的发布

HLJCA 在签发更新证书后，就将更新证书发布到数据库和目录服务器中，对外进行发布。

4.6.7 电子认证服务机构对其他实体的通告

其他实体可以通过从目录服务器查询已更新的数字证书。

4.6.8 证书密钥更新的情形

证书密钥更新的具体情形如下：

a) 证书的有效期将要到期，证书更新；

b) 因私钥泄漏而吊销证书；

c) 其他。

4.6.9 证书更新请求者相关操作流程

HLJCA 应对鉴别证书更新请求者身份的方式规范、合理，申请者到 HLJCA 书面填写“证书申请表 ”，并注明更新的原因。HLJCA 对更新请求者的身份及申

请者资料、数字证书申请表单进行鉴别与鉴定，然后对用户提交的证书更新申请进行审核，最后进行更新制证。

密钥更新请求者到 HLJCA 书面填写《数字证书申请表》，并注明更新的原因。HLJCA 对密钥更新请求者的身份及所提供的资料及申请表进行鉴别与鉴定，然后对用户提交的证书更新申请进行审核，最后进行更新制证。鉴别证书变更请求者身份的方式规范、合理。

证书变更请求者到 HLJCA 书面填写《数字证书申请表》，并注明更新的原因。HLJCA 对证书变更请求者的身份及所提供的资料及申请表进行鉴别与鉴定，然后对用户提交的证书更新申请进行审核，最后进行更新制证。

HLJCA 服务机构颁发更新证书时对用户的通告方式：当面、电话短信及网上在线查询等方式。

HLJCA 在证书更新签发成功后， 自动将更新后的证书发布到目录服务器上，24 小时内更新被废止的数字证书状态，订户及依赖方在 HLJCA 的网站中可以查询并获得有关证书应用的相关信息。

4.7 证书吊销和挂起

4.7.1 证书吊销的情形

发生下列情形之一的，订户应当申请吊销数字证书：

1）数字证书私钥泄露；

2）数字证书中的信息发生重大变更；

3）认为本人不能实际履行数字证书认证业务规则。

发生下列情形之一的，HLJCA 可以吊销其签发的数字证书：

1）订户申请吊销数字证书；

2）订户提供的信息不真实；

3）订户没有履行双方合同规定的义务；

4）数字证书的安全性得不到保证；

5）法律、行政法规规定的其他情形。

4.7.2 请求证书吊销的实体

根据不同的情况，订户、HLJCA 可以请求吊销最终用户证书。

4.7.3 吊销请求的流程

证书吊销请求的处理采用与原始证书签发相同的过程。

订户到 HLJCA 书面填写《证书吊销申请表》，并注明吊销原因；HLJCA 根据要求对订户提交的吊销请求进行审核；HLJCA 吊销订户证书后，将当面通知订户证书被吊销，订户证书在 24 小时内进入 CRL，向外界公布。

强制吊销是指 HLJCA 确认用户违反本《电子认证业务规则》的情况发生时，对订户证书进行强制吊销，吊销后将立即通知该订户。

4.7.4 吊销请求宽限期

如果出现私钥泄露等事件，吊销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他吊销原因的吊销请求必须在 48 小时内提出。

4.7.5 电子认证服务机构处理吊销请求的时限

HLJCA 规定在一个工作日内处理完吊销请求。

4.7.6 依赖方检查证书吊销的要求

证书在吊销成功后，HLJCA 通过 CRL 发布证书吊销信息。依赖方通过以下两种方式进行所依赖证书的状态查询：

a）CRL 查询：利用证书中标识的CRL 地址，通过目录服务器查询并下载 CRL 到本地，进行证书状态的检验。

b）在线证书状态查询(OCSP)：服务系统接受证书状态查询请求，从目录服务器中查询证书的状态，查询结果经过签名后，返回给请求者。

注意：依赖方要验证 CRL 的可靠性和完整性，确保是经 HLJCA 发布并且签名的。

4.7.7 CRL 发布频率

HLJCA 可采用实时或定期的方式发布 CRL。颁发 CRL 的频率根据证书策略确定，一般为 24 小时定期发布。

4.7.8 CRL 发布的最大滞后时间

CRL 发布的最大滞后时间为 24 小时。

4.7.9 密钥损害的特别要求

数字证书密钥一旦损坏，证书只能被吊销而不能做挂起操作。

4.7.10 证书挂起的情形

证书用户暂停使用证书。

例如：证书持有者由于某种原因，如长期出差，短期内无法使用证书，可以申请证书挂起。

4.7.11 请求证书挂起的实体

由 HLJCA 颁发的证书有效期限未到的个人、机构等各种实体，以及其他凡是持有 HLJCA 各类证书而有效期限未到的证书持有者。

4.7.12 挂起请求的流程

订户到 HLJCA 书面填写《证书挂起申请表》，并注明挂起原因；HLJCA 根据 3.2 节的要求对订户提交的证书挂起请求进行审核，审核通过后对证书进行挂起操作。HLJCA 可以依法对订户证书进行强制挂起，挂起后将立即通知该订户。

证书被挂起后，订户必须在证书有效期前恢复证书。HLJCA 将通过电话提醒订户，若证书到期订户还没有提交恢复申请，HLJCA 有权自行吊销证书。对此造成的任何后果，HLJCA 不负任何责任。

4.7.13 挂起的期限限制

证书挂起的期限不能超过证书的有效期。

4.8 证书状态服务

4.8.1 操作特征

HLJCA 通过目录服务器为用户提供证书状态服务。

4.8.2 服务可用性

HLJCA 提供 7X24 小时的证书状态查询服务。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

4.8.3 可选特征

可选特征包括：用户名、用户的电子邮件、地址等。（提供付费服务）

4.9 订购结束、密钥生成、备份与恢复

4.9.1 订购结束

订购结束是指当证书有效期满或证书吊销后，该证书的服务时间结束。

订购结束包含以下两种情况：

a）证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可以终止订购；

b）在证书有效期内，证书被吊销后，即订购结束。

4.9.2 密钥生成、备份与恢复的策略和行为

订户的签名密钥对由订户的密码设备（如智能 USB KEY）生成，加密密钥对由密钥管理中心生成。

签名密钥对由订户的密码设备保管。

密钥恢复是指加密密钥的恢复，密钥管理中心不负责签名密钥的恢复。密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复。

a）订户密钥恢复：当订户的密钥损坏或丢失后，某些密文数据将无法还原，此时订户可申请密钥恢复。订户在 HLJCA 申请，经审核后，通过 HLJCA 向 KMC 请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。

b）司法取证密钥恢复：司法取证人员在 KMC 申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

4.9.3 会话密钥的封装与恢复的策略和行为

非对称算法组织数字信封的方式来封装会话密钥。数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解开并恢复会话密钥。

5 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

HLJCA 的建筑物和机房建设按照下列标准实施：

1. GM/T 0034-2014：《基于 SM2 密码算法证书认证系统密码及其相关安全技术规范》；

2. GB50174－93：《电子计算机机房设计规范》；

3. GB2887-89：《计算机站场地技术条件》；

4. GB/T-2887-2000：《电子计算机场地通用规范》；

5. GB6650-86：《计算机机房用活动地板技术条件》；

6. SJ/T30003—93：《电子计算机机房施工及验收规范》；

7. GB9361-88：《计算站场地安全要求》；

8. GBJ114-88：《采暖通风与空气调节规范》。

5.1.2 物理访问

为了保证本系统的安全，采取了一定的隔离、控制手段。机房的所有门都足

够结实，能防止非法的进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

1.门禁系统：控制各层门的进出，工作人员需使用身份识别卡和指纹识别才能进出，进出每一道门都有时间记录。

2.报警系统：任何非法闯入、非正常手段的开门以及长时间不关门，都会触发报警系统。

5.1.3 电力与空调

机房供电系统包括整个机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分计算机设备负荷和辅助设备负荷，计算机设备专用配电柜和辅助设备配电柜独立设置，分开计算机设备电源与动力线。

使用 UPS 不间断电源，最大限度满足机房计算机设备对供电电源质量的要求。市电电源供电与备用发电机供电在机房配电室进行切换，再经过 UPS 不间断电源对计算机设备供电。

按《电子计算机机房设计规范》（GB50174-93）规定和功能需要，采用机房精密空调，保持机房在恒温、恒湿的状态下运行。

5.1.4 水患防治

在机房建设时已采取相应措施，防止水侵蚀，充分保障系统安全运行。

5.1.5 火灾防护

根据国家有关消防规范，对 HLJCA 机房区域采用火灾自动报警系统及气体灭火进行保护。

5.1.6 介质存储

介质必须指定专人管理，并存储在专用的介质柜中，保证物理安全，注意防磁、防静电干扰、防火、防水。

5.1.7 废物处理

当 HLJCA 存档的敏感数据或密钥已不再需要或存档的期限已满时，应当将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.1.8 异地备份

HLJCA 对关键数据进行异地备份，遇到灾难情况发生时保证数据安全。

5.2 程序控制

5.2.1 可信角色

HLJCA、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。

可信角色包括：

a)系统管理员

系统管理员负责对数字证书服务体系在本单位的系统进行日常管理,执行系统的日常监控，并可根据需要签发服务器证书和下级操作员证书。

b)安全管理员

安全管理员对 CA 中心的物理、网络、系统的安全全面负责。并且拟订安全管理制度和操作流程，监督各岗位安全管理的执行情况。

c)审计管理员

审计管理员控制、管理、使用安全审计系统，安全审计系统分布于证书管理系统的各个子系统中，负责各个子系统的运行和操作日志记录。

d)密钥管理员

密钥管理员负责管理 CA 中心的密钥相关设备，进行 CA 中心密钥的生成、备份、恢复、销毁等操作。

e)证书业务管理员

证书业务管理员对注册机构操作员进行管理，并对注册机构业务进行管理。

5.2.2 每个角色的识别与鉴别

按照所担任角色的不同，分别进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。HLJCA 将独立完整地记录其所有的操作行为。

5.2.3 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即 HLJCA 的可信角色由不同的人担任。

至少两个人以上才能使用一项对参加操作人员保密的密钥分割和合成技术，来进行任何密钥恢复的操作。

5.3 人员控制

5.3.1 资格、经历和无过失要求

HLJCA 工作人员必须与公司签订劳动合同并无同行业重大错误记录、无违法犯罪记录，经过保密教育，签订保密协议后，方能取得可信人员的资质。

5.3.2 背景审查程序

所有目前的可信人员和申请调入的可信人员都必须书面同意对其进行背景调查。

背景调查分为：基本调查和全面调查。

基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查。

全面调查除包含基本调查项目外还包括对犯罪记录，社会关系和社会安全方面的调查。

调查程序包括：

a）人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

b）人事部门通过电话、信函、网络、走访、等形式对其提供的材料的真实

性进行鉴定。

c）用人部门通过现场考核、 日常观察、情景考验等方式对其考察。

d）经考核，人事部门和用人部门联合填写《可信人员调查表》，报主管领导批准后准予上岗。

5.3.3 培训和考核要求

HLJCA 对运营人员按照其岗位和角色安排不同的培训。培训有:系统硬件安装与维护、系统软件运行与维护、系统安全、应用软件的运行和维护、CA 中心的运行管理、CA 中心的内部管理、政策和规定及系统备份与恢复等。

对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由 HLJCA 组织培训与考核。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训并考核。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 HLJCA 组织的培训一次。

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

5.3.5 工作轮换周期和顺序

对于可替换角色，HLJCA 将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

5.3.6 对未授权行为的处罚

当 HLJCA 员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用 HLJCA 系统或进行越权操作，HLJCA 得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

5.3.7 独立合约人的要求

对不属于 HLJCA 内部的工作人员，但从事 HLJCA 有关业务的人员等独立签约者(如注册机构的工作人员)，HLJCA 的统一要求如下：

a) 人员档案进行备案管理；

b) 具有相关业务的工作经验；

c) 必须接受 HLJCA 组织的为期一周的岗前培训。

5.3.8 提供给员工的文档

为使得系统正常运行，HLJCA 提供给具有权限的相关人员所需文档。

6 业务连续性管理

6.1 制定业务连续性计划、明确业务恢复时间

为满足《电子签名法》和《电子认证服务管理办法》对电子认证服务机构的业务连续性要求，确定并减少因自然灾害等不可抗拒力以及其它人为因素带来的损失，有效地保障业务的连续性，HLJCA 制定业务连续性计划。主要内容有：故障恢复处理、设备与数据的备份、故障应急处理。

6.2 建立重要系统、数据和设备的备份管理规定

CA 系统的数据备份是在发生事故时，保证业务可恢复性的关键。HLJCA 系统备份主要包括数据库备份、应用系统备份、加密机备份、设备硬件备份。

6.3 建立根私钥被攻破、需要作废或被作废情况下的应变流程

根私钥是 HLJCA 的核心数据，一旦被攻破将给 HLJCA 带来巨大损失。所以，HLJCA 制定了应急机制：

1）立即停止使用和发放与根私钥相关的一切证书业务；

2）立即上报有关主管部门；

3）通过各种方式通知证书应用方及依赖方；

4）更换根私钥重新签发证书。

6.4 备份与恢复

6.4.1 定期备份数据

HLJCA 需要定期备份的数据包括：认证系统数据、用户数据、系统配置数据。为保障系统的业务连续性，我们为重要系统配备了备用设备，HLJCA 员工不定期对设备进行检查，发现问题及时处理。

6.4.2 证书数据

证书数据是以数据库的形式表现出来，所以 HLJCA 对数据库进行了备份。

6.4.3 对电源和通信线路进行备份

在电源方面采用一路市电加一路 UPS 电源和备用发电机，UPS 供电能力为 6 小时。

通信线路方面也是两路，一路是由中国联通公司提供，另一路由中国电信提供。

7 审计日志程序及处理情况

7.1 记录事件的类型

HLJCA 记录所有与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时间段、事件的内容和事件相关的实体等。

HLJCA 还可能记录与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。

7.2 处理日志的周期

HLJCA 每月对日志进行审查，并对审查日志的行为进行备案。

7.3 审计日志的保存期限

HLJCA 审计日志至少保存证书失效后五年。

7.4 审计日志的保护

HLJCA 执行严格的管理，确保只有 HLJCA 授权的人员才能对审查日志进行相应操作。 日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作，另外对日志要进行异地备份。审计日志的制作和访问进行岗位分离。

7.5 审计日志备份程序

HLJCA 所有的审查日志都进行备份。根据记录的性质和要求，分为实时、按天、按周、按月和按年等多种形式的备份，可采用在线和离线两种方式的备份工具。

7.6 审计日志收集系统

审计日志收集系统涉及：

证书签发管理系统；

证书注册管理系统；

密钥管理系统；

证书目录系统；

其他需要审计的系统。

7.7 对导致事件实体的通告

HLJCA 发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，并保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

HLJCA 有权决定是否对导致事件的实体进行通告。

7.8 脆弱性评估

HLJCA 每年对系统进行脆弱性评估，并根据日志的日常审计和监督实施，随时调整和系统运行密切相关的安全控制措施，以降低系统运行的风险。

7.9 审计事件

HLJCA 系统具有完善的日志审计系统，记录与系统相关的事件以备查阅。这些记录，无论是手写、书面或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段及事件相关的实体等。只有 HLJCA 授权的人员才能接近这些审查记录。审计日志处于严格的保护状态，严格禁止访问、阅读、修改和删除等操作。HLJCA 对以下事件进行了审计：

1）电子认证服务系统的操作事件

审计日志记载了以下内容：系统操作事件的日期、内容、发生的日间及事件相关的实体信息。

2）证书生命周期事件

详细记录了证书生命周期的申请、签发、更新、变更、吊销、挂起等操作。

3）可信人员的操作事件

审计日志记载了可信人员在证书整个生命周期内的操作记录。

4）不符合规定了事件

HLJCA 审计人员对不符合规定的事件操作进行了及时处理。

5）HLJCA 审计记录至少保存证书失效后五年。

6）黑龙江制定了确保审计日志不被未授权询问、复制、修改和删除的制度，对审计日志进行了严格的通道管理，确保只有 HLJCA 授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，严格禁止访问、阅读、修改和删除等操作。

7）HLJCA 保证所有的审查记录和审查总结都按照 HLJCA 备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具，有实时、每天、每周、每月和每年等各种形式的备份。

8 记录归档

8.1 归档记录的类型

归档记录包括所有审计数据、证书申请信息、与证书申请相关的信息等。

8.2 归档记录的保存期限

CA 数据库的保存期至少保存证书失效后五年。

8.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。HLJCA 保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

8.4 归档文件的备份程序

所有存档的文件和数据库除了保存在 HLJCA 的存储库，还在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。HLJCA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

8.5 归档记录时间要求

所有记录都要在存档时加具体准确时间标识以表明存档时间。系统产生的记录，也要有时间标识。

8.6 归档收集系统

档案收集系统由人工操作和自动操作两部分组成。

8.7 获得和检验归档信息的程序

由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。HLJCA 每年会验证归档信息的完整性。

8.8 电子认证服务机构密钥更替

电子认证服务机构密钥更替指 HLJCA 根证书到期和电子认证服务机构证书到期时，需要更换密钥对而采取的措施。

HLJCA 根密钥由加密机产生，更换密钥时将签发 3 张证书：

使用旧的私钥对新的公钥及信息签名生成证书；

使用新的私钥对旧的公钥及信息签名生成证书；

使用新的私钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相信任。

电子认证服务机构证书到期时，更替办法同根密钥的更替一样。

9 损害和灾难恢复

9.1 事故和损害处理程序

HLJCA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，HLJCA 将按照灾难恢复计划实施恢复。

9.2 计算资源、软件和/或数据被破坏

HLJCA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，HLJCA 将按照灾难恢复计划实施恢复。

9.3 实体私钥损害处理程序

当 HLJCA 根证书被作废时，HLJCA 通知订户。

当 HLJCA 的私钥被攻破或需要作废时，HLJCA 根据 HLJCA 灾难恢复计划规定的灾难恢复步骤进行操作。

9.4 灾难后的业务连续性能力

针对证书系统的核心业务系统，证书签发管理系统和证书注册管理系统采用双机热备方式；对核心数据库，采用光盘和备份磁盘阵列的方式来确保证书系统的高可靠性和可用性。

发生自然或其它不可抗力性灾难后，采取的安全措施按照 HLJCA 灾难恢复计划实施。

9.5 电子认证服务机构的终止

因各种情况，HLJCA 需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

HLJCA 在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于 HLJCA 和订户等。

在终止服务六十日前向工业和信息化部报告，按照相关法律规定的步骤进行操作。

HLJCA 采用以下措施终止业务：

a) 起草 HLJCA 终止业务声明；

b) 停止认证中心所有业务；

c) 处理加密密钥；

d) 处理和存档敏感文件；

e) 清除主机硬件；

f) 管理 HLJCA 系统管理员和安全官员；

g) 通知与 HLJCA 终止运营相关的实体。

10 认证系统技术安全控制

10.1 密钥对的生成和安装

10.1.1 密钥对的生成

订户的签名密钥对由订户的密码设备（如智能 USB KEY）生成，加密密钥对

由 KMC 生成。

10.1.2 私钥传送给订户

订户的签名密钥对由自己的密码设备生成并保管。

加密密钥对由KMC 产生，通过安全通道传到订户手中的密码设备中。

10.1.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到 HLJCA。

订户的加密证书公钥，由 KMC 通过安全通道传递到 CA 中心。

从 RA 到 CA 以及从 KMC 到 CA 的传递过程中，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

10.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从 HLJCA 的网站上下载根证书和 CA 证书，从而得到 CA 的公钥。

10.1.5 密钥的长度

HLJCA 用于加密和签名的 SM2 密钥对的模长为 256 位，对称密钥的长度是 128 位。

10.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可的硬件产生。

10.1.7 密钥使用目的

订户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

10.2 私钥保护和密码模块工程控制

10.2.1 密码模块标准和控制

HLJCA 所用的密码设备都是经国家密码管理局认可的产品，其安全性达到以下要求：

接口安全：不执行规定命令以外的任何命令和操作；

协议安全：所有命令的任意组合，不能得到私钥的明文；

密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

10.2.2 私钥的多人控制

根 CA 系统的私钥的生成、更新、吊销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到 5 个管理员 USB KEY 中，只有其中三至五人在场并许可的情况下，才能对私钥进行上述操作。

订户的私钥由订户自己通过密码设备控制。

10.2.3 私钥托管

订户加密证书对应的私钥由密钥管理中心托管，订户的签名证书对应的私钥由自己保管，密钥管理中心不负责托管。

KMC 严格保证用户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

10.2.4 私钥备份

订户的签名密钥 HLJCA 和 KMC 都不备份。加密私钥由KMC 备份，备份数据以密文形式存在。

10.2.5 私钥归档

订户密钥对的归档是将已过生命周期或决定暂不使用的加密密钥以密文形式保存在数据库中，并通过数据库备份出来进行归档保存，归档后的密钥形成历史信息链，供查询或恢复。

HLJCA 提供过期的托管加密密钥的归档服务。

10.2.6 私钥导入或导出密码模块

使用HLJCA 软件可以把私钥安全导入到密码模块中，私钥无法从硬件密码模块中导出。

10.2.7 私钥在密码模块中的存储

私钥在硬件密码模块中加密保存。

10.2.8 激活私钥的方法

具有激活私钥权限的管理员使用含有自己的身份的 USB KEY 登录，启动密钥管理程序，进行激活私钥的操作，需要三名管理员同时在场。

10.2.9 解除私钥激活状态的方法

具有解除私钥激活状态权限的管理员使用含有自己的身份的 USB KEY 登录，启动密钥管理程序，进行解除私钥的操作，需要三名管理员同时在场。

10.2.10 销毁密钥的方法

具有销毁密钥权限的管理员使用含有自己的身份的 USB KEY 登录，启动密钥管理程序，进行销毁密钥的操作，需要三名管理员同时在场。

10.2.11 密码模块的评估

HLJCA 使用普华诚信信息技术有限公司的 SJJ1011 服务器密码机，该密码机已通过国家密码管理局的审批，符合国家有关标准。密码机采用以分组密码体制为核心的高强度密码算法和非对称密码体制，密钥采取分层结构，逐层提供保护。主要技术指标如下：

a) 通信接口：符合国际 ITU Ethernet RJ45 标准；

b) 带宽控制：10M/100M/1000M 自适应，充分满足突发业务需要；

c) 密钥管理：密钥不以明文形式出现在服务器密码机以外；

d) 身份鉴别：采用 USB KEY 对用户进行身份鉴别管理，以控制对加密系统的使用；

e) 处理速度：SM2 签名速度：350 次/秒
SM2 加密速度：180 次/秒

SM1 算法加密/解密速度：90Mbps

10.3 密钥对管理的其他方面

10.3.1 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥，由 HLJCA 和密钥管理中心定期归档。

10.3.2 证书操作期和密钥对使用期限

所有订户证书的有效期和其对应的密钥对的有效期都是一致的。

10.4 激活数据

10.4.1 激活数据的产生和安装

激活数据是私钥保护密码，证书存储介质（如：智能密码钥匙）出厂时设置

了缺省的 PIN 值，证书制作时激活证书存储介质的PIN。

10.4.2 激活数据的保护

HLJCA 采取加解密机制等多种方式保护激活数据，以避免未授权的使用。未授权用户尝试使用激活数据时，尝试达到预定的次数，激活数据会自动锁定。

10.4.3 激活数据的其他方面

只有在拥有证书介质并知道证书介质的PIN 值时才能激活证书存储介质，进而使用私钥。

10.5 计算机安全控制

10.5.1 特别的计算机安全技术要求

为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，并制定相应的操作规范。

对于设备维护制订了完整的保管和维护制度：

a)专人负责设备的领取和保管，做好设备的领用、进出库和报废登记；

b)对设备定期进行检查、清洁和保养维护；

c)制定设备维修计划，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修的有关情况等；

d)设备维修时，必须有专人在场监督。

10.5.2 计算机安全评估

HLJCA 电子认证服务系统已通过国家密码管理局组织的安全性审查。

10.6 生命周期技术控制

10.6.1 系统开发控制

系统开发采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

10.6.2 安全管理控制

HLJCA 制定了一系列的安全管理策略和规范来保证操作系统和网络符合设置的安全标准。

10.6.3 生命周期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了国家密码管理局审批，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。

10.7 网络的安全控制

网络安全的主要目标是通过规划网络拓扑结构、合理划分网络区域，采用常规网络安全防护技术和手段，防止来自于网络各方面的攻击，并加强对系统内部的安全管理。HLJCA 采取防火墙、病毒防治、入侵检测、漏洞扫描、数据备份与恢复等安全防护措施。

11 证书、证书吊销列表和在线证书状态协议

11.1 证书

HLJCA 签发的证书遵循 RFC3280 标准，采用 X.509 V3 格式。

11.1.1 版本号

X.509 V3。

11.1.2 证书扩展项

HLJCA 定义的证书扩展项可使用 IETF RFC 3280 中定义的如下证书扩展项：

机构密钥标识符 AuthorityKey Identifier

主体密钥标识符 SubjectKey Identifier

密钥用法 KeyUsage

扩展密钥用途 ExtendedKeyUsage

私有密钥使用期 PrivateKeyUsagePeriod

证书策略 CertificatePolicies

策略映射 PolicyMappings

主体替换名称 SubjectAlternativeName

颁发者替换名称 IssuerAlternativeName

主体目录属性 SubjectDirectoryAttributes

基本限制 BasicConstraints

名称限制 NameConstraints

策略限制 PolicyConstraints

证书撤销列表分发点 CRLDistributionPoints

限制任意策略 InhibitAnyPolicy

最新证书撤销列表 FreshestCRL

机构信息访问 Authority InformationAccess

主体信息访问 SubjectInformationAccess

私有扩展项支持以下类型

个人身份标识码 IdentifyCode

个人社会保险号 InsuranceNumber

企业工商注册号 ICRegistrationNumber

企业组织机构代码 OrganizationCode

企业税号 TaxationNumber

11.1.3 算法对象标识符

使用 SM2 算法，算法 OID 为 1.2.156.10197.1.502。

11.1.4 名称形式

HLJCA 数字证书中的主体的 X.500 DN 应是 C=CN 命名空间下的 X.500 目录唯一名字。DN_C（Country）属性的编码使用 PrintableString，其它属性的编码一律使用 UTF8String。

主体的 X.500 DN 应为：

C= CN

S= XXXX

L= XXXX

O= XXXX

OU= XXXX

CN= XXXX

C（Country）应为 CN，表示国家；

S（） 表示省份；

L（） 表示城市；

O（Organization）中的内容分为 2 种：

a） 证书主体或者证书主体所属单位具有明确的上一级单位，则应为其上一级单位的名称全称；

b） 不存在a）中所述的上一级单位，则应为证书主体或者证书主体所属单位的所在省、 自治区、直辖市名称全称；

OU（Organization Unit）应为证书主体或者证书主体所属单位的名称全称；

CN（Common Name）中的内容分为 4 种：

a） 个人证书中应为证书主体的姓名；

b） 单位机构证书中应为证书主体单位的标准简称；

c） 服务器证书应为证书主体设备的域名或者 IP 地址或者设备编码；

d) 代码签名证书应为负责人的姓名，或者是所属单位的标准简称。

11.2 证书吊销列表

HLJCA 签发的证书吊销列表遵循 RFC3280 标准，采用 X.509 V2 格式。

11.2.1 版本号

X.509 V2。

11.2.2 CRL 和 CRL 条目扩展项

CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。

CRL 条目扩展项：不使用CRL 条目扩展项 。

11.3 在线证书状态协议

11.3.1 版本号

OCSP：v1。

11.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

12 电子认证服务机构审计和其他评估

12.1 评估的频率或情形

审计是为了检查、确认 HLJCA 是否按照《电子认证业务规则》及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。审计分内部审计和外部审计。

内部审计是由 HLJCA 自己组织内部人员进行的审计，审计的结果可供 HLJCA 改进、完善业务，内部审计结果不需要公开。

外部审计由HLJCA 委托第三方审计机构来承担，审计的依据包括 HLJCA 所有与业务有关的安全策略、《电子认证业务规则》、业务规范、管理制度，以及国

家或行业的相关标准。

12.2 评估者的资质

内部审计人员的选择一般包括：

HLJCA 的安全负责人及安全管理人员；

HLJCA 业务负责人；

认证系统及信息系统负责人；

人事负责人；

其他需要的人员。

外部审计的审计人员的资质由第三方确定。

12.3 评估者与被评估者之间的关系

评估者与被评估者应无任何业务、财务往来或其它利害关系，足以影响评估的客观性。

12.4 评估内容

对 HLJCA 规范评估应包括：

安全策略是否得到充分实施；

运营工作流程和制度是否严格遵守；

电子认证业务规范是否符合证书策略的要求；

是否严格按照本 CPS、业务规范和安全要求开展业务；

各种日志、记录是否完整，是否存在问题；

HLJCA 支持的证书认证操作规程是否与本《电子认证业务规则》表达一致，包括 HLJCA 的技术、手续和员工的相关管理政策和业务声明；

HLJCA 是否实施了相关技术、管理、相关政策和业务声明；

评估者或 HLJCA 认为有必要评估的其他方面。

12.5 对问题与不足采取的措施

对审计中发现的问题，HLJCA 将根据审计报告的内容准备一份解决方案，明确对此采取的行动。HLJCA 将根据国际惯例和相关法律、法规迅速解决问题。

12.6 评估结果的传达与发布

除非法律明确要求，HLJCA 一般不公开评估结果。

对 HLJCA 关联方，HLJCA 将依据签署的协议来公布评估结果。

13 法律责任和其他业务条款

13.1 费用

13.1.1 证书签发和更新费用

数字证书的收费标准按照国家和黑龙江省物价主管部门批准的收费标准执行。根据证书实际应用的需要，HLJCA 在不高于收费标准的前提下可以对证书价格进行适当调整。

13.1.2 证书查询费用

在证书有效期内，对该证书信息进行查询，HLJCA 不收取查询费用。

13.1.3 证书吊销或状态信息的查询费用

查询证书是否吊销，HLJCA 不收取信息访问费用。

对于在线证书状态查询(OCSP)，由 HLJCA 与订制者在协议中约定。

13.1.4 其他服务的费用

CA 可根据请求者的要求，订制各类通知服务，具体服务费用，在与订制者签订的协议中约定。

13.1.5 退款策略

在实施证书操作和签发证书的过程中，HLJCA 遵守并保持严格的操作程序和策略。一旦订户接受数字证书，HLJCA 将不办理退证、退款手续。

如果订户在证书服务期内退出数字证书服务体系，HLJCA 将不退还剩余时间的服务费用。

13.2 财务责任

HLJCA 保证其具有维持其运作和履行其责任的财务能力。它应该有能力承担对订户、依赖方等造成的责任风险，并依据 CPS 规定，进行赔偿担保。

13.3 业务信息保密

13.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

a) 在双方披露时标明为保密(或有类似标记)的；

b) 在保密情况下由双方披露的或知悉的；

c) 双方根据合理的商业判断应理解为保密数据和信息的；

d) 以其他书面或有形形式确认为保密信息的；

e) 或从上述信息中衍生出的信息。

对于 HLJCA 来说，保密信息包括但不限于以下方面：

a) 最终用户的私人签名密钥都是保密的；

b) 保存在审计记录中的信息；

c) 年度审计结果也同样视为保密；

d) 除非有法律要求，由 HLJCA 掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和公司的信息需要保密。

HLJCA 不保存任何证书应用系统的交易信息。

除非法律明文规定，HLJCA 没有义务公布或透露订户数字证书以外的信息。

13.3.2 不属于保密的信息

与证书有关的申请流程、申请需要的手续、申请操作指南等信息是公开的。HLJCA 在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

订户数字证书的相关信息可以通过 HLJCA 目录服务等方式向外公布。

HLJCA 在其目录服务器中公布证书的吊销信息，供网上查询。

13.3.3 保护保密信息的责任

a) 各方有保护自己和其他人员或单位的机密信息的并保证不泄露给第三方的责任。不将机密数据和信息(也不会促使或允许他人将机密数据和信息)用于协议项下活动目的之外的其他用途，包括但不限于将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储存机密数据和信息。

b) 当 HLJCA 在任何法律、法规或规章的要求下，或在法院的要求下必须提供本《电子认证业务规则》中具有保密性质的信息时，HLJCA 应按照要求，向执法部门公布相关的保密信息，HLJCA 无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

13.4 个人隐私保密

13.4.1 隐私保密方案

除非证书申请人主动提供，HLJCA 保证不会截取任何证书申请人的资料。

HLJCA 应保护证书申请人所提供的，证明其身份的资料。HLJCA 应采取必要的安全措施防止证书申请人资料被遗失、盗用与篡改。

13.4.2 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

13.4.3 不被视为隐私的信息

证书申请人提供的用来构成数字证书内容的资料不认为是隐私信息。

数字证书是公开的，通过 HLJCA 目录服务等方式向外公布。

13.4.4 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄漏、使用或发布给第三方。

13.4.5 使用隐私信息的告知或同意

使用隐私信息，须获得本人同意。

13.4.6 依法律或行政程序的信息披露

当 HLJCA 在任何法律、法规或规章的要求下，或在法院的要求下必须提供证书申请人的特定资料或隐私信息时，HLJCA 按照法律、法规或规章的要求或法院的要求，向执法部门公布相关信息，HLJCA 无须承担任何责任。这种提供不能被视为违反了隐私保护的责任和义务。

13.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定处理。

13.5 知识产权

除非额外声明，HLJCA 享有并保留对证书以及 HLJCA 提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。HLJCA 有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

按本《电子认证业务规则》的规定，所有由HLJCA 签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于 HLJCA 所有，这些知识产权包括所有相关的文件和使用手册。注册机构应征得 HLJCA 的同意使用相关的文件和手册，并有责任和义务提出修改意见。

13.6 陈述与担保

13.6.1 电子认证服务机构的陈述与担保

HLJCA 在提供电子认证服务活动过程中的承诺如下：

a）HLJCA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部的领导，对签发的数字证书承担相应的法律责任。

b）HLJCA 保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。

c）除非已通过 HLJCA 证书库发出了 HLJCA 的私钥被破坏或被盗的通知，HLJCA 保证其私钥是安全的。

d）HLJCA 签发给订户的证书符合 HLJCA 的 CPS 的所有实质性要求。

e）HLJCA 将向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件。

f）HLJCA 将及时吊销证书。

g）HLJCA 拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

h）证书公开发布后，HLJCA 向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

13.6.2 注册机构的陈述与担保

注册机构在参与电子认证服务过程中的承诺如下：

a）提供给证书订户的注册过程完全符合 HLJCA 的《电子认证业务规则》的所有实质性要求。

b）在 HLJCA 生成证书时，不会因为失误而导致证书中的信息与证书申请人的信息不一致。

c）注册机构将按 CPS 的规定，及时提交证书申请、吊销、更新等服务请求。

13.6.3 订户的陈述与担保

订户一旦接受 HLJCA 签发的证书，就被视为向HLJCA 及信赖证书的有关当事人作出以下承诺：

a）订户需熟悉本《电子认证业务规则》的条款和与其证书相关的证书政策，还需遵守证书持有人证书使用方面的有关限制。

b）订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供 HLJCA 检查和核实。

c）订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生。

d）私钥为订户本身访问和使用，订户对使用私钥的行为负责。

e）一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知 HLJCA，申请采取吊销等处理措施。

f）订户已知其证书被冒用、破解或被他人非法使用时，应及时通知 HLJCA 吊销其证书。

13.6.4 依赖方的陈述与担保

依赖方必须熟悉本《电子认证业务规则》的条款以及和订户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本《电子认证业务规则》的有关条款。

13.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同 13.6.4。

13.7 赔偿责任限制

13.7.1 赔偿责任范围

HLJCA 的赔偿责任范围：

a）证书信息与订户提交的信息资料不一致，导致订户损失。

b）因 HLJCA 原因，致使订户无法正常验证证书状态，导致订户利益受损。

c）HLJCA 在证书有效期限内承担损失或损害赔偿。

13.7.2 对最终实体的赔偿担保

在任何情况下，HLJCA 及发证机关将不会对任何间接的、特殊的、结果性的、附带性的损失负责，也不对由于数字证书、数字签名、或其他任何于此提供或考虑的交易或服务引起的，或与之有关的使用、移交、授权、执行、不执行、或无法使用等情况造成的利益损失、数据丢失、或其他间接性的、结果性的、或惩罚性的损失负责。即便是事先被提醒了该损失发生的可能性，HLJCA 和发证机关也不需负责。

13.7.3 责任免除

有下列情况之一的，应当免除 HLJCA 之责任。

a）如果证书申请人故意或无意地提供了不完整、不可靠或已过期的信息，又根据正常的流程提供了必须的审核文件，得到了HLJCA 签发的数字证书，由此引起的经济纠纷应由证书申请人全部承担，HLJCA 不承担与证书内容相

关的法律和经济责任，但可以根据受害者的请求提供协查帮助。

b）HLJCA 不承担任何其他未经授权的人或组织以HLJCA 名义编撰、发表或散布的不可信赖的信息所引起的法律责任。

c）HLJCA 不承担在法律许可的范围内，根据受害者或法律的要求如实提供网上业务中“不可抵赖 ”的数字签名依据所引起的法律责任。

d）HLJCA 不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。

e) HLJCA 不是证书持有人或依赖方的代理人、受托人、管理人或其他代表。HLJCA 和证书持有人间的关系以及 HLJCA 和依赖方间的关系并不是代理人和委托者的关系。证书持有人和依赖方都没有权利以合同形式或其他方法让 HLJCA 承担信托责任。

f) 由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。

g) 因 HLJCA 的设备或网络故障等技术故障而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障 ”引起原因包括但不限于：（1）不可抗力；（2）关联单位如电力、电信、通讯部门而致；（3）黑客攻击；（4）设备或网络故障。

h) HLJCA 已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

13.8 有限责任

HLJCA 根据与订户的合同承担相应的有限责任。

HLJCA 在与订户和依赖方签订的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

13.9 赔偿

HLJCA 按照本《电子认证业务规则》承担赔偿责任。

证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致 HLJCA 产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任。

a) 未向HLJCA 提供真实、完整和准确的信息，而导致 HLJCA 或有关各方损失。

b) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。

c) 在知悉证书密钥已经失密或者可能失密时，未及时告知 HLJCA，并终止使用该证书，而导致 HLJCA 或有关各方损失。

d）订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。

e）证书的非法使用，即违反 HLJCA 对证书使用的规定，造成了HLJCA 或有关各方的利益受到损失。

13.10 有效期限与终止

13.10.1 有效期限

本《电子认证业务规则》 自发布之日起正式生效。

本《电子认证业务规则》中将详细注明版本号及发布日期。

13.10.2 终止

当新版本的《电子认证业务规则》正式发布生效时，旧版本的《电子认证业务规则》 自动终止。

13.10.3 效力的终止与保留

《电子认证业务规则》的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

13.11 对参与者的个别通告与沟通

认证活动的某一参与方与另一参与方进行通信时必须使用安全通道，以使其通信过程在法律上有效。

13.12 修订

13.12.1 修订程序

当本《电子认证业务规则》不适用时，由 HLJCA 安全策略管理委员会组织 CPS 编写小组进行修订。

修订完成后，HLJCA 安全策略管理委员会进行审批，审批通过后将在 HLJCA

的网站(http://www.hljca.com.cn)上发布新的《电子认证业务规则》。

《电子认证业务规则》将进行严格的版本控制。

13.12.2 通告机制和期限

本《电子认证业务规则》在 HLJCA 的网站(http://www. hljca.com.cn)上发布。

版本更新时，最新版本的《电子认证业务规则》在 HLJCA 的网站发布，对具体个人不做另行通知。

13.12.3 必须修改业务规则的情形

当管辖法律、适用标准及操作规范等有重大改变时，必须修改《电子认证业务规则》。

13.13 争议处理

HLJCA、证书订户、依赖方等实体在电子认证活动中产生争端可按照以下步骤解决：

a) 当事人首先通知 HLJCA，根据本《电子认证业务规则》中的规定，明确责任方；

b) 由 HLJCA 相关部门负责与当事人协调；

c) 若协调失败，可以通过仲裁或司法途径解决；

d) 任何因与HLJCA 就本《电子认证业务规则》所产生的任何争议而提起诉讼的，受 HLJCA 工商注册所在地的人民法院管辖。

13.14 管辖法律

本《电子认证业务规则》在各方面服从中国法律和法规的管制和解释，包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

13.15 适用法律的符合性

无论在任何情况下，本《电子认证业务规则》的执行、解释、翻译和有效性均适用中华人民共和国的法律。

13.16 一般条款

13.16.1 完整协议

本《电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

13.16.2 分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

13.16.3 强制执行

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

13.16.4 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在数字证书认证活动中，HLJCA 由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

13.17 其他条款

HLJCA 对本《电子认证业务规则》拥有最终解释权。