河北省电子认证有限公司

证书策略

版本3.1

河北省电子认证有限公司

2019年12月

目录

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

1. 引言

1.1. 概述

1.1.1.公司简介

2001 年 5 月，河北省人民政府办公厅成立了河北省电子商务工作协调小组（办字[2001]52 号），指导和规范全省电子商务的各项工作，并负责河北 CA 的规划。2002 年 3 月，河北省电子商务工作协调小组授权河北省电子商务认证有限公司建设河北省数字证书认证中心，负责全省数字证书的签发、管理和认证工作。2004 年 9 月，国家密码管理委员会办公室发布《关于同意河北省数字证书认证中心使用商用密码和建立密钥管理中心的批复》（国密办字〔2004〕368 号）。2005 年 1 月，上海格尔软件有限公司取得了河北 CA 的系统建设资格。2005 年 2 月，河北省数字证书认证中心实施方案通过了国家密码管理委员会办公室组织的专家论证。2005 年 5 月，河北省数字认证系统一期工程建设完成。

2005 年 9 月，河北省数字证书认证系统及密钥管理系统通过了由国家密码管理局组织的系统安全性审查，于 9 月 15 日取得《电子认证服务使用密码许可证》。

2006 年 11 月 17 日，我公司依法取得国家信息产业主管部门颁发的《电子认证服务许可证》，成为我省唯一一家依法设立的第三方电子认证服务机构。

2010 年 9 月，根据国家密码管理局《电子政务电子认证管理办法（试行）》

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

的要求，我公司通过了电子政务电子认证能力评估的审查，取得电子政务电子认证资质。

2010 年 9 月，由河北省省委常委、常务副省长赵勇签发成立河北省电子认证管理委员会，统筹协调全省电子认证工作，制定 CA 应用的相关标准规范，指导各部门推广应用数字证书。

2010 年 10 月，河北省电子认证管理委员会成立暨国家电子认证管理办法宣贯座谈会召开。会议传达了河北省网络与信息安全协调小组关于成立了河北省电子认证管理委员会的通知，对国家电子认证管理相关法律法规进行宣传。管理委员会成员单位、省直部分重要信息系统主管部门相关处室负责同志共 40 余人参加会议。

2011 年 8 月，按照国家密码管理局《关于做好公钥密码算法升级工作的通知》（国密局字[2011]152 号）。河北 CA 在 2011 年对电子认证系统进行了升级，由原来"SRQ15 电子认证系统"升级为"SZT0901 电子认证系统"，并于 2012 年 1 月通过国家密码管理局安全性审查，获得国家密码管理局同意 SM2 系统正式运行的批复。

2012 年 10 月 15 日，国家密码管理局组织相关专家亲临河北 CA，现场进行了互联互通测试并正式为河北 CA 签发 SM2 运营 CA 证书，河北 CA 成为全国第一家正式加入国家 SM2 信任源根 CA 的电子认证服务机构。

1.1.2.证书策略

本文件描述河北 CA 的证书策略（CP），是河北 CA 数字证书服务的策略声明，

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

适用于所有由河北 CA 签发和管理的数字证书及相关参与主体。为批准、签发、管理、使用、更新、吊销证书和相关的可信服务制定业务、法律和技术上的要求和规范。这些要求和规范保护河北 CA 数字证书服务的安全性和完整性，包含一整套在河北 CA 范围内一致适用的单一规则集，因此在整个河北 CA 架构内能够提供同样的信任担保。本 CP 并不是河北 CA 和各参与方之间的法律性协议，河北 CA 和各参与方之间的权利义务依靠他们之间签署的各类协议构成。

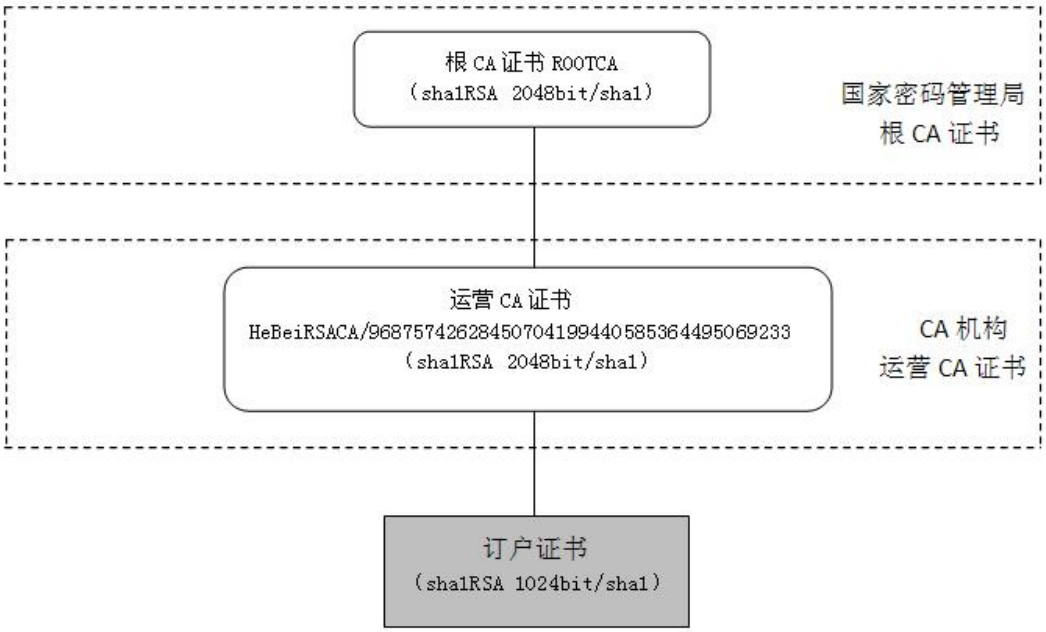
本 CP 满足《互联网 X.509 公开密钥基础设施证书策略和证书业务框架》（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework），即由互联网标准组织"互联网工程工作组"（Internet Engineering Task Force）制定的 RFC3647 标准的结构和内容要求，同时也满足《GB 26855-2011-T 信息安全技术公钥基础设施证书策略与认证业务声明框架》的结构和内容要求，并根据中国的法律法规和河北 CA 的运营要求进行适当的改变。

1.1.3.河北 CA 证书层次架构

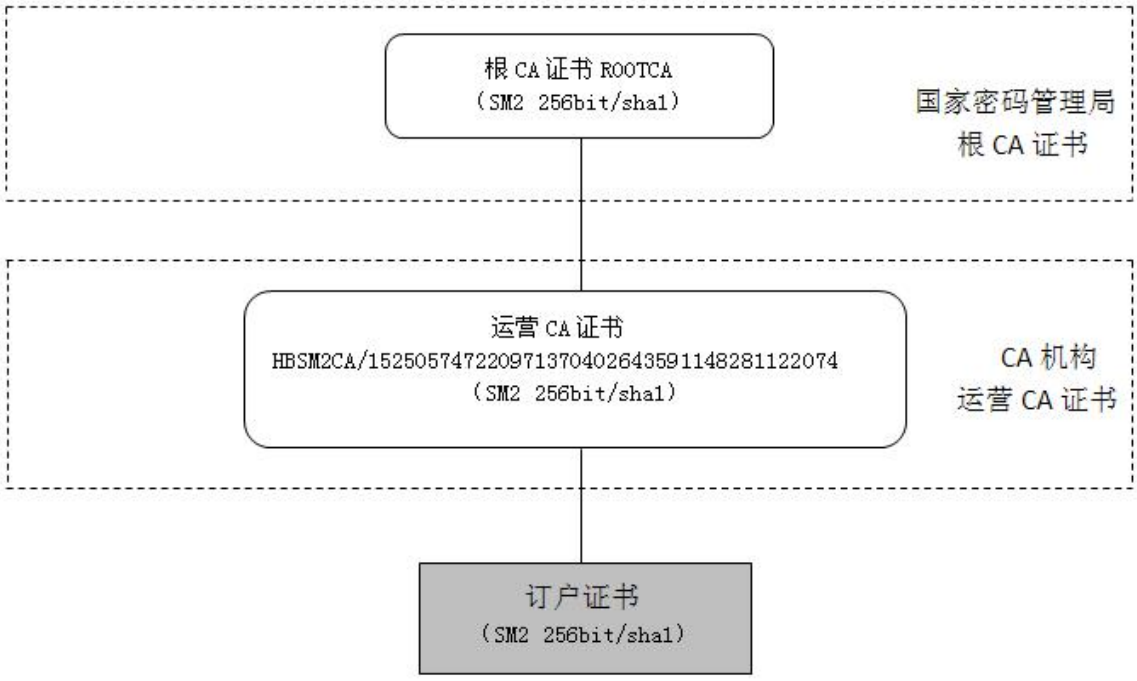
河北 CA 目前有 2 个根证书，分别为 HeBeiRSACA 证书（RSA）、HBSM2CA 证书（SM2）。

1）HeBeiRSACA（RSA）

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com



2）HBSM2CA（SM2）



1.2. 文档名称与标识

本文档称作《河北省电子认证有限公司证书策略》（简称《河北 CA CP》）。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

1.3. PKI 参与者

1.3.1.电子认证服务机构

电子认证服务机构（Certification Authority，简称 CA）是颁发证书的实体。河北 CA 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。河北 CA 通过给从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。CA 是向最终订户或其下 CA 签发证书的实体的术语，它的一个特例是根 CA，一个根 CA 是一类证书体系的最高层。

1.3.2.注册机构

注册机构（Registration Authority，简称 RA）代表 CA 建立起注册过程，确认证书申请者的身份，批准或拒绝证书申请者。在订户获得证书前，它必须以申请者的身份来注册证书。

证书申请者必须从 CA 或 RA 建立的注册过程来完成注册，并将注册信息提交给 CA 或 RA。CA 或 RA 将对申请者的身份及其它属性进行确认，然后决定是签发还是拒绝该请求。如果签发证书，则证书将被发送给申请者。RA 还可以根据订户需要吊销证书，尽管是 CA 完成最终的吊销工作，并将证书加入到证书吊销列表(CRL)中。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

1.3.3.订户

订户，即从 CA 接收证书的实体，包括所有接受河北 CA 证书的个人、单位。订户和申请人很多时候并不一致，如果订户和申请人不一致，则需要申请人保证获得明确、适当的授权。个人又分为自然人和从属于某一个单位的个人；单位包括各类政府组织、企事业单位和其它社会团体，一般而言，单位应该具有法人资格或者组织机构代码证号码；对于设备类证书，由于证书中包含主体的特殊性，订户通常应被理解为拥有该设备的单位或者个人，并由拥有该设备的单位或者个人承担相应的义务。

订户代表着证书中公钥所绑定的唯一实体，拥有对与其证书唯一对应的私钥的最终控制权。订户在本 CP 的范围内使用证书，并承担本 CP 约定的义务。

1.3.4.依赖方

依赖方是指信任证书、使用证书的个人和单位。依赖方可以是证书订户，也可以不是证书订户。

要信任或者使用一张证书，依赖方必须验证证书的吊销信息，包括查询证书吊销列表（CRL）或使用 OCSP 方式查询证书状态。依赖方必须经过合理的审核后才能够信任一张证书。

1.3.5.其他参与者

其他参与者是指为河北 CA 的电子认证活动提供相关服务的其他实体。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

1.4. 证书应用

1.4.1.适合的应用

证书类型	订户性质	举例
个人证书	社会自然人，政府、企业、事业等机构所属人员	社会自然人或政府、企业、事业等机构所属人员在电子事务处理过程中，代表其身份，行使数字签名
单位证书	政府、企业、事业等机构	政府、企业、事业等机构在电子事务处理过程中，代表其身份，行使数字签名
设备证书	个人、政府、企业、事业等机构所属的设备及其他资源	个人、政府、企业、事业等机构所属的在电子事务处理过程代表其设备及其他资源身份

1.4.2.限制的证书应用

一般而言，河北CA证书是一般性目的的证书，可以和不同的依赖方之间相互操作。尽管如此，河北CA证书在功能上是受到限制的，如个人证书只能用于个人用户的应用，而不能作为服务器或组织机构证书使用。

证书不设计用于、不打算用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

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，否则由

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

此造成的法律后果由用户自己承担。

1.5. 策略管理

1.5.1.策略文档管理机构

河北CA安全策略委员会是河北CA电子认证服务所有策略的最高管理机构，负责制定、维护和解释本CP。

河北CA安全策略委员会由来自于公司管理层、行政中心、营销中心、技术中心、运营服务中心等拥有决策权的合适代表组成。

河北CA安全策略委员会的所有成员在就证书策略进行管理和批准时，均享有一票决定权，如果选票相同，委员会主任可拥有双票决定权。

1.5.2.联系人

《河北省电子认证有限公司证书策略》由河北CA CP策略管理小组负责编写、更新和维护。

电话：400-707-3355传真：0311-83013591

地址：河北省石家庄市友谊南大街100号

邮编：050081

电子邮件：hebca@hebca.com

1.5.3.决定 CP 符合策略的机构

本CP由河北CA安全策略委员会批准，包括本CP的修订和版本变更。

河北CA安全策略委员会负责评估河北CA的CPS是否符合本CP，是批准和决定河北CA的CPS是否与本CP相适应的机构。

1.5.4.CP 批准程序

《河北省电子认证有限公司证书策略》由河北CA CP策略管理小组负责编写，交由河北省电子认证有限公司和法律顾问共同研究审议。审议通过后，在河北CA网站上及时公布变更后的正式文档，并于公布之日起三十日内向国家信息产业主管部门备案。

1.5.5.CP 修订

河北CA根据国家的政策法规、技术要求、标准的变化及业务发展情况及时修订本CP，CP编写小组根据相关的情况拟定CP修订建议，提交河北CA安全策略委员会审核，经该委员会批准后，正式在河北CA官方网站上发布。

1.6. 定义和缩写

③公钥基础设施（PKI）Public Key Infrastructure

是指支持公开密钥体制的安全基础设施，可提供身份鉴别、加密、完整性和不可否认性服务。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

③电子政务电子认证业务规则（CPS）Electronics Government Certification Practice Statement

是指关于认证机构在全部证书服务生命周期中的业务实践（如签发、管理、吊销、更新证书或密钥）所遵循规范的详细描述和声明。

③电子政务电子认证服务机构（CA）Electronics Government Certification Authority

是指受用户信任，负责创建和分配公钥证书的权威机构。

③注册机构（RA）Registration Authority

是指具有下列一项或多项功能的实体：识别和鉴定证书申请人，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。

③电子签名认证证书（证书）Digital Certificate

是指电子政务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。证书包含有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。

③证书吊销列表（CRL）Certificate Revocation List

是指经电子政务电子认证服务机构数字签名的一个列表，它指定了一系列证书颁发者认为无效的证书，也称黑名单。

③私钥（电子签名制作数据）Private Key

指在电子签名过程中使用的，将电子签名与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

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

方式，就相对应的公开密钥加密的文件或信息予以解密。

③公钥（电子签名验证数据）Public Key

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。

③LDAP（Lightweight Directory Access Protocol）

即轻量级目录访问协议，用于查询、下载数字证书以及数字证书废止列表（CRL），符合 ITU X.500。

③OCSP（Online Certificate Status Protocol）

即在线查询数字证书状态协议，用于支持实时查询数字证书状态信息。

2. 发布与信息库责任

2.1. 信息库

认证机构应有信息库用于各类信息的发布，如证书策略、认证业务声明、协议、证书、证书吊销列表。认证机构应在其认证业务声明、信赖方协议等中指明有关信息发布、获取的位置。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

2.2. 认证信息的发布

河北CA在官方网站https://www.hebca.com 发布信息库，该网站是河北CA发布所有信息最首要、最及时、最权威的渠道。

河北CA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访问河北CA的目录服务器获取证书的信息和吊销证书列表；同时，河北CA提供在线证书状态查询服务，订户或依赖方可实时查询证书的状态信息。

同时，河北CA也将会根据需要采取其他可能的形式进行信息发布。

2.3. 发布的时间和频率

河北CA在订户证书签发或者注销时，通过目录服务器或官方网站自动将证书和CRL发布，发布周期为24小时，即在24小时内发布最新CRL；在紧急的情况下，河北CA可以自行决定证书和CRL的发布时间。

信息库其他内容的发布时间和频率，由河北CA独立做出决定，这种发布应该是即时的、高效的，并且是符合国家法律的要求的。

2.4. 信息库访问控制

对于公开发布的CP、证书、CRL等公开信息，河北CA允许公众自行通过网站进行查询和访问。

只有经过授权的河北CA/RA管理人员可以查询电子政务电子认证服务机构和注册机构数据库中其他数据。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

3. 身份标识与鉴别

3.1. 命名

3.1.1.命名类型

根据证书对应实体的类型不同，河北 CA 签发证书的实体名字可以是人员姓名、组织机构名称、部门名称、域名等，命名符合 X.500 甄别名（Distinguished Name，简称 DN）规定。

河北CA的最终用户证书的主题域中包含一个X.500 甄别名 ,具体内容如下：

③最后一项必须是 C=CN；

③如果有 CN 项，需要放在 DN 的最前面；

③其它项按照从小到大的顺序排列 :如同时存在 OU 和 O 项 ,OU 在 O 前面，同时存在 S 和 L 项，L 在 S 前面。

3.1.2.对命名有意义的要求

订户的甄别名（DN），必须反映用户的真实身份、具有实际意义，并与法律不冲突。

3.1.3.订户的匿名或伪名

订户不能使用匿名、伪名申请证书，证书中也不能使用匿名、伪名。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

3.1.4.解释不同命名的规则

依X.500甄别名命名规则解释。

3.1.5.命名的唯一性

河北CA应保证签发给某个订户的证书，其主体甄别名，在河北CA信任域内是唯一的。当出现相同的名称时，以先申请者优先使用。

3.1.6.商标的识别、鉴别与角色

河北CA签发的证书的主体甄别名中不包含商标名。

3.2. 初始身份确认

3.2.1.证明拥有私钥的方法

通过证书请求所包含的数字签名证明证书申请人持有与注册公钥对应的私钥。在河北CA证书服务体系中，私钥在用户端生成，证书请求信息中包含由用户私钥所生成的数字签名，河北CA用其对应的公钥来验证签名。河北CA要求用户妥善保管自己的私钥，用户被视作其私钥的唯一持有者。

3.2.2.个人身份的鉴别

个人身份通过身份证进行鉴别。个人用户携带个人身份证原件到河北CA授

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

权的注册机构（RA）进行身份审核验证。

河北CA授权的注册机构按照河北CA个人身份鉴别规范对申请材料的真实性进行审核，并决定批准申请或拒绝申请。

个人身份的鉴别规范如下：

鉴别方式一：

采集个人活体头像、身份证姓名、身份证号等证件信息，与公安库中的信息进行对比，鉴别个人身份。

鉴别方式二：

由第三方进行用户身份鉴别，并由第三方提供鉴别通过后的用户信息。

鉴别方式三：

1）通过高拍仪公安身份证模块读取身份证信息，验证身份证真伪；

2）确认身份证照片与本人是否为同一人。

个人身份的鉴别规范简要说明了如何进行个人身份鉴别。河北CA保留根据最新国家政策法规的要求更新个人身份鉴别规范的权利。更新后的个人身份鉴别规范将发布在河北CA网站：http://www.hebca.com。

3.2.3.机构身份的鉴别

对于组织机构身份的鉴别，河北CA注册机构需要验证组织机构的合法证件。组织机构授权的经办人到河北CA网站www.hebca.com下载《授权委托书》,填写、打印并加盖公章，提供组织机构有效证件原件及经办人身份证原件到河北CA授权的注册机构进行身份审核验证，未携带《授权委托书》的现场填写《数字证书

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

申请表》。

组织机构有效证件类型如下：

1. 营业执照；

2. 事业单位法人登记证；

3. 社团登记证；

4. 民办非企业登记证；

5. 政府批文；

6. 其他有效证件。

如无法提供证件原件所有提供的复印件需加盖公章。

如该组织机构申请服务器证书还需提交域名使用权证明材料。

河北CA授权的注册机构按照河北CA组织身份鉴别规范对申请材料的真实性进行审核，并决定批准申请或拒绝申请。

组织机构有效身份证件的鉴别规范如下：

鉴别方式一：

1）核验用户提供的身份证明资料所载明的组织机构名称、统一代码证号等证件信息与申请表提交的用户信息是否一致、证明资料是否完整；（如用户提供的证件为复印件，还需鉴别用户印章是否有效）

2）从第三方数据库获取鉴别通过后的用户信息并与第三方数据库信息进行对比。

鉴别方式二：

1）通过高拍仪拍照解析营业执照二维码信息，并从国家信用信息公示系统

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

获取用户的单位名称、统一代码，与申请表提交的用户信息进行对别，并核验用户身份证明资料的完整性；（如用户提供的证件为复印件，还需鉴别用户印章是否有效）

2）从第三方数据库获取鉴别通过后的用户信息并与第三方数据库信息进行对比。

鉴别方式三：

由第三方进行用户身份鉴别，并由第三方提供鉴别通过后的用户信息。

经办人身份的鉴别流程如下：

鉴别方式一：

1）通过高拍仪公安身份证模块读取身份证信息，验证身份证真伪；

2）确认身份证照片与本人是否为同一人。

鉴别方式二：

从第三方平台获取经办人信息，并与申请提交经办人信息进行对比。

组织机构身份的鉴别规范简要说明了如何进行组织机构身份鉴别。河北CA保留根据最新国家政策法规的要求更新组织机构身份鉴别规范的权利。更新后的组织机构身份鉴别规范将发布在河北CA网站：http://www.hebca.com。

3.2.4.设备身份的鉴别

设备身份的鉴别会根据其设备拥有者的不同而不同，河北CA必须对订户进行身份鉴证，包括如下内容：

设备类订户需要提交数字证书申请表，设备拥有者身份证明的文件和复印

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

件、业务办理授权书、经办人有效身份证件的原件和复印件。

在设备名称被作为证书主题内容申请证书时 ,还需要验证该申请者是否拥有该权利 ,确认的方式可以是提供归属权证明文件或机构对该设备所有权或使用权的书面承诺等，并加盖公章。

如果认为有需要，河北CA还可以通过从第三方获取的信息来验证该申请者个人的身份，如果河北CA无法从第三方得到所有所需的信息，可委托第三方进行调查，或要求申请者提供额外的信息和证明材料。

此外，必要时，河北CA 还可以设定其它所需要的鉴别方式和资料。

3.2.5.没有验证的订户信息

订户提交鉴证文件以外的信息，视为没有验证的订户信息，河北CA不承诺相关信息的真实性，不承担相关的法律责任。

3.2.6.授权确认

为确保经办人具有特定的许可，可代表组织办理数字证书业务，组织机构需在《河北CA单位数字证书申请表》中申请单位声明处加盖单位公章。申请表上加盖公章则证明该组织机构对经办人的授权已确认。

3.2.7.互操作准则

对于其他的电子认证服务机构，可以与河北CA进行互操作，但是该电子认证服务机构的CPS必须符合河北CA CP要求，并且与河北CA签署相应的协议。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

河北CA将依据协议的内容，接受非河北CA的发证机构鉴别过的信息，并为之签发相应的证书。

如果国家法律法规对此有规定，河北CA将严格予以执行。

截至目前，河北CA未签发任何交叉证书。

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后，河北CA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

吊销后密钥更新对订户身份标识和鉴别的要求，与原始身份验证的流程相同。

3.4. 吊销请求的标识与鉴别

证书吊销请求可以来自订户，也可以来自河北CA、注册机构。当河北CA或者注册机构有充分的理由吊销订户的证书时，有权依法吊销证书，这种情况无须进行鉴证。河北CA或者注册机构的证书吊销请求，必须经过其管理机构或者监督机构进行确定才可以进行。如果订户主动请求吊销证书，则按照本CP第3.2节

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

所述进行身份鉴别。如果是司法机关依法提出吊销，CA 或者RA 将直接以司法机关书面的吊销请求文件作为鉴别依据，不再进行其他方式的鉴别。

4. 证书生命周期操作要求

4.1. 证书申请

4.1.1.证书申请实体

证书申请实体包括年满18周岁以上具有合法身份的中华人民共和国公民，及在中国境内的外国公民，或具有独立法人资格的组织机构（包括行政机关、事业单位、企业单位和社会团体等）。

4.1.2.注册过程与责任

证书申请人按照要求由经办人填写《河北CA数字证书申请表》并盖章或签字确认后，提交相关的身份证明材料。河北CA注册机构依据身份鉴别规范对申请人的身份进行鉴别，并决定是否受理申请。

申请过程中各方责任为：

申请人须按照要求提交证书申请材料，并确保申请材料真实准确。

河北CA注册机构负责接收申请人的申请材料，当面对申请人所提供的证书申请材料和身份证明进行查验。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

4.2. 证书申请处理

4.2.1.执行识别与鉴别

当河北CA、注册机构接受到订户的证书申请后，应按本CP第3.2节的要求，对订户进行身份识别与鉴别。

4.2.2.证书申请批准和拒绝

河北CA注册机构身份鉴别流程对申请人的身份进行识别或鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人提交的申请材料符合要求，交纳证书费用后，则河北CA注册机构批准证书申请，为证书申请人制作并签发数字证书。

证书申请人未能通过身份鉴别或提交的申请材料不符合要求，河北CA注册机构将拒绝申请人的证书申请，并通知申请人拒绝受理，同时向申请人说明原因（法律禁止的除外）。

被拒绝的证书申请人可以完善材料后，再次提出申请。

4.2.3.处理证书申请的时间

河北CA注册机构在申请符合要求的情况下，处理证书申请的时间不超过3个工作日。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

4.3. 证书签发

4.3.1.证书签发中 RA 和 CA 的行为

河北CA作为证书认证系统的运行者，授权设立注册机构（RA），在证书受理前RA 管理员负责证书申请的鉴别，在证书申请通过鉴别后，RA管理员将批准证书请求。批准的信息将会发送到河北CA的证书认证系统，证书认证系统签发证书后返回给RA系统。

4.3.2.CA 和 RA 通知订户证书的签发

河北CA通过授权注册机构，对订户的通告有以下几种方式：

1. 通过面对面的方式，通知订户到注册机构领取数字证书，注册机构把证书直接交给订户；

2. 邮政信函通知订户；

3. 其他河北CA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

根据不同的业务操作流程，以下任何一种情况均视为订户接受数字证书：

1. 订户领取数字证书；

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

2. 订户从网上下载该数字证书；

3. 与订户约定的其它方式。

4.4.2.CA 对证书的发布

订户接受证书后，河北CA将该订户证书发布到可被公开访问的目录服务系统。

4.4.3.CA 通知其他实体证书的签发

其他实体可以通过河北CA目录服务器查询河北CA已签发的数字证书信息。

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河北CA所签发的证书后，均视为已经同意遵守与河北CA、依赖方有关的权利和义务的条款。订户接受到数字证书，应采取合理措施妥善保存其证书对应的私钥避免未经授权的使用。订户只能在适用的法律、本CP以及订户协议规定的范围内使用私钥和证书。

对于签名证书，其私钥可用于对信息的签名，订户应知悉并确认签名的内容。对于加密证书，其私钥可用于对采用对应公钥加密的信息进行解密。在证书到期

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

或被吊销之后，订户必须停止使用该证书对应的私钥。

数字证书载体为商用密码产品，中华人民共和国国务院发布的《商用密码管理条例》规定，商用密码产品的用户不得转让其使用的商用密码产品。

4.5.2.依赖方公钥和证书的使用

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

1. 获得数字签名对应的证书及信任链；
2. 确认该签名对应的证书是由河北CA所签发；
3. 通过查询CRL或OCSP确认该签名对应的证书是否被吊销；
4. 证书的用途适用于对应的签名；
5. 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方有责任拒绝签名信息。

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。依赖方应将加密证书连同加密信息一起发送给接受方。

4.6. 证书更新

为保证证书及其密钥对的安全有效，河北CA为签发证书设置的有效期一般为一年。证书订户必须在证书有效期到期前到河北CA注册机构申请更新证书。更新证书时同时更新证书的密钥。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

4.6.1.证书更新的情形

1. 证书将要到期、已到期或河北CA其它策略要求的原因，且密钥对处于安全状态并且策略允许继续使用；

2. 订户或其授权代表提出证书的更新申请；

3. 河北CA的策略要求或相关法律法规引致其它原因。

4.6.2.请求证书更新的实体

由河北CA签发的原有证书在有效期内的个人、组织机构、设备等实体，以及河北CA签发的其他各类证书持有人。

4.6.3.处理证书更新请求

处理证书更新请求可以有以下两种方式：

1. 在线更新，只适合于证书未过期且未被注销的情形。即在证书即将过期前，通过河北CA网站提交更新申请，经过河北CA证实提交更新申请者拥有对应证书的私钥，并收到相关款项后，由河北CA签发新的证书。订户需在声明的处理时间之后，凭提交更新申请的证书公钥所对应的私钥下载新的证书。

2. 离线更新，适合所有证书更新情形。即订户或其授权代表到河北CA授权的注册机构提交更新申请，经过河北CA证实提交更新申请者拥有对应证书的私钥，并收到相关款项后，由河北CA签发新的证书。由河北CA授权的注册机构为用户完成证书更新。订户证书过期的，需按照订户身份类型提供身份证明材料，

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

其身份鉴别方式和处理过程与本文“§3.2.2组织机构身份的鉴别”、“§3.2.3个人身份的鉴别”要求相同。

4.6.4.通知订户新证书的签发

同本CP第 4.3.2节。

4.6.5.构成接受更新证书的行为

同本CP 第4.4.1节。

4.6.6.CA 对更新证书的发布

同本CP 第4.4.2节。

4.6.7.通知其他实体证书的签发

同本CP 第4.4.3节。

4.7. 证书密钥更新

证书密钥更新指订户或其他参与者生成一对新密钥并申请为新公钥签发一个新证书。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

4.7.1.证书密钥更新的情形

证书密钥更新的情形如下（以下的情形并不代表必须执行证书密钥更新）:

1. 证书的有效期将要到期或已经到期；
2. 因私钥泄漏而吊销证书；
3. 订户或其授权代表提出证书密钥的更新申请；
4. 河北CA的策略要求或相关法律法规引致其它原因。

4.7.2.请求证书密钥更新的实体

请求证书密钥更新的实体为证书订户。

4.7.3.处理证书密钥更新请求

同本CP 第4.6.3节。

4.7.4.通知订户新证书的签发

同本CP 第4.3.2节。

4.7.5.构成接受密钥更新证书的行为

同本CP 第4.4.1节。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

4.7.6.CA 对密钥更新证书的发布

同本CP 第4.4.2节。

密钥更新证书应在24小时内发布。

4.7.7.CA 通知其他实体证书的签发

同本CP第4.4.3节。

4.8. 证书变更

4.8.1.证书变更的情形

1. 订户主体名称、主体身份 ID等证书信息发生变更；

2. 订户或其授权代表提出证书的变更申请。

4.8.2.请求证书变更的实体

请求证书变更的实体为证书订户。

4.8.3.处理证书变更请求

证书变更按照初次申请证书的注册过程进行处理，同本CP 3.2。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

4.8.4.通知订户新证书的签发

同本CP 第4.3.2节。

4.8.5.构成接受变更证书的行为

同本CP 第4.4.1节。

4.8.6.CA 对变更证书的发布

同本CP 第4.4.2节。

4.8.7.CA 通知其他实体证书的签发

同本CP 第4.4.3节。

4.9. 证书吊销和挂起

4.9.1.证书吊销的情形和原因

发生下列情况之一，河北CA将吊销所签发的数字证书：

1. 订户申请吊销数字证书；
2. 订户主体消亡；
3. 订户变更数字证书的用途；
4. 数字证书中信息发证重大变更；

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

5. 数字证书对应的私钥泄露或出现其他证书的安全性得不到保证的情况；

6. 任何与提供证书服务相关的协议到期；

7. 订户或其授权代表提出证书注销申请；

8. 订户违反河北CA CPS或签订的相关证书协议；

9. 订户申请数字证书时，提供的信息不真实；

10. 订户没有按照规定缴纳数字证书服务费用；

11. 订户不能履行或违反了相关法律、法规和本协议所规定的责任和义务；

12. 其他情形，根据法律和行政法规的要求，河北CA采取的吊销措施。

吊销分为主动吊销和被动吊销。主动吊销是指由订户提出吊销申请，由河北CA注册机构进行审核，由注册机构RA操作员对其进行处理，吊销证书；被动吊销是指注册机构确认订户违反证书相关规定或已经消亡等情况发生时，采取吊销证书的手段以停止对该证书的服务。。

4.9.2.请求证书吊销的实体

根据不同情况，订户、河北CA、注册机构可以请求吊销用户证书。

4.9.3.证书吊销请求的处理程序

4.9.3.1. 订户请求吊销证书

1. 订户向注册机构提交吊销申请表和身份证明材料，同时说明吊销原因；

2. 注册机构核实申请吊销实体的身份和吊销理由的正当性；

3. 注册机构将吊销申请表提交给河北CA，由河北CA完成吊销。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

4. 河北CA提供7*24小时的吊销申请服务。

4.9.3.2. 订户被强制吊销证书

1. 当河北CA或注册机构有充分的理由确信出现本CP第4.9.1节中的情况时，可通过内部确定的流程吊销证书；

2. 河北CA提供7*24小时的证书问题报告和处理流程；

3. 当依赖方、司法机构、应用软件提供商、防病毒机构等第三方提请证书问题报告时，河北CA应组织调查并根据调查结果来决定是否吊销证书；

4. 河北CA吊销订户证书后，通过适当的方式，包括电子邮件、电话等，告知订户证书已被吊销及吊销理由。

4.9.4.吊销请求的宽限期

当最终订户发现密钥泄漏等不安全事件时，应该尽快提出吊销请求，自订户向河北CA注册机构提交吊销请求后24小时内因订户证书所发生的法律问题河北CA不承担任何责任，RA 应在收到吊销请求后立即吊销证书，没有宽限期。当最终订户发现数字证书私钥泄露或丢失、数字证书中的信息发生重大变更或用户不希望继续使用数字证书时，订户应当立即到河北CA注册机构申请吊销数字证书，吊销手续遵循河北CA的相关规定。河北CA接到用户的吊销申请后，在24小时内吊销用户的数字证书。用户应当承担所有在数字证书吊销之前使用数字证书而造成的后果。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

4.9.5.CA 处理吊销请求的时限

河北CA自接到吊销请求到完成吊销之间的间隔期限，不得超过24个小时。

4.9.6.依赖方检查证书吊销的要求

依赖方在依赖一个证书前必须查询河北CA发布的CRL确认他们所信任的证书是否被吊销。

4.9.7.CRL 发布频率

河北CA采用实时或定期的方式发布CRL，通常在24小时内自动发布最新的CRL。

4.9.8.CRL 发布的最大滞后时间

一个证书从它被吊销到它被发布到CRL上的滞后时间不能超过24小时。

4.9.9.在线状态查询的可用性

河北CA提供 7X24 小时LDAP目录查询服务。并提供OCSP 作为可选的在线状态有偿查询方式。

4.9.10. 在线状态查询要求

证书基本信息查询可对证书序列号、证书主题、证书状态、证书有效期进行

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

查询。

证书附加信息查询可对证书所相对应的订户信息如订户名、电子邮件地址等进行查询。

证书模版信息查询 ,每个证书模版均可根据其自定义的扩展项进行证书信息查询。

4.9.11. 吊销信息的其他发布形式

OCSP 作为可选的吊销信息发布形式。

4.9.12. 密钥损害的特别要求

如果出现密钥损害等事件，密钥恢复请求必须在发现损害或有损害嫌疑24小时内由证书持有者携带申请证书时提交过的身份证明材料原件和复印件 ,交由河北CA审核后，填写书面密钥恢复申请书，缴纳相应费用，由河北CA予以密钥恢复。

4.9.13. 证书挂起的情形

以下情况出现时证书挂起：

1. 订户怀疑证书或密钥受到攻击；
2. 订户要求挂起数字证书；
3. 订户的资信暂时出现问题或无法证明其资信。

挂起分为主动挂起和被动挂起。主动挂起是指由用户提出挂起申请 ,经河北

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

CA注册机构审核后，由RA管理员进行挂起证书处理；被动挂起是指河北CA注册机构确认用户上述描述的情况发生时，采取挂起证书的手段以暂停对该证书的服务。

4.9.14. 请求证书挂起的实体

由河北CA签发的、在有效期范围之内的证书订户，可以申请挂起证书。

4.9.15. 挂起请求的程序

主动挂起：订户向河北CA注册机构提交申请，注册机构根据“§3.2初始身份确认”的要求对订户提交的挂起请求进行审核。河北CA挂起订户证书后，订户证书在24小时内发布在CRL列表中，对外公布。

被动挂起：河北CA或河北CA注册机构确认用户违反《河北CA电子政务电子认证业务规则》的情况发生时，对订户证书进行强制挂起。

4.9.16. 挂起的期限限制

申请证书挂起的期限为：在证书有效期剩余的时期内。

4.10. 证书状态服务

4.10.1. 操作特征

河北CA 通过目录服务器为订户提供证书状态服务。用户需要将CRL 下载到

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

本地后进行验证，包括CRL的合法性验证和检查CRL中是否包含待检验证书的序列号。

4.10.2. 服务可用性

河北CA提供7X24小时的证书状态查询服务。

4.10.3. 可选特征

根据订户的要求，在支付相关费用后，可以由河北CA 查询数据库中该证书的状态。

4.11. 订购结束

订购结束是指当证书有效期满或证书吊销后，该证书的服务期限结束。订购结束包含以下两种情况：

1.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；

2.在证书有效期内，证书被吊销后，即订购结束；

河北CA详细记录吊销证书的操作过程；

河北CA定期将订购结束后的证书及相应的订户数据进行归档。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

4.12. 密钥生成、备份与恢复

4.12.1. 密钥生成、备份与恢复的策略与行为

订户的签名密钥对由订户的密码设备（如智能密码钥匙）生成，加密密钥对由河北 CA 密钥管理中心生成。

签名密钥对由订户的密码设备保管。

河北 CA 不负责签名密钥的恢复，只能对加密密钥进行恢复。

密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复。

1. 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。订户在河北 CA 注册机构进行申请，经审核后，通过河北 CA 向 KMC 发出密钥恢复请求；河北 CA 密钥系统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。
2. 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。

4.12.2. 会话密钥的封装与恢复的策略与行为

采用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密并恢复会话密钥。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

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

1. 河北 CA 的建筑物和机房建设所遵循的国家标准包括：

◈ 《计算站场地安全要求》：中华人民共和国国家标准（GB 9361 - 88）

◈ 《计算站场地技术条件》：中华人民共和国国家标准（GB 2887 - 89）

◈ 《计算机机房用活动地板技术条件》：中华人民共和国国家标准（GB 6650 - 86）

◈ 《电子计算机机房设计规范》:中华人民共和国国家标准(GB 50174 - 2008）

◈ 《加密屏蔽机房安装设计规范》中华人民共和国国家标准（GB12190-1900）

◈ 《电子计算机场地通用规范》中华人民共和国国家标准（GB/T2887-2000）

◈ 《电子设备雷击保护导则》中华人民共和国国家标准（GB7450-1987）

◈ 《高层民用建筑设计防火规范》中华人民共和国国家标准（GB50045-95）

◈ 《防静电活动地板通用规范》中华人民共和国国家标准(SJ/T 10796-2001)

2. 河北 CA 的系统机房设立在石家庄市友谊南大街 100 号，系统机房实行分层访问的安全管理。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

5.1.2.物理访问控制

为了保证本系统的安全，河北CA采取了严密的隔离、控制、监控手段。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进出，核心区域采用双身份识别卡结合指纹鉴定的方式才能进出。进出每一道门均保存历史记录。

2. 报警系统：任何非法闯入、非正常手段的开门、长时间不关门等异常情况都将触发报警系统。

3. 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，监控系统进行24小时不间断录像。所有录像资料至少保留一年。

4. 红外监控设备：与物理侵入报警系统配合，当有人非法入侵，系统警铃会发出警报同时发信息给机房工作人员，保证了机房的安全。

门禁和物理侵入报警系统均配备UPS不间断电源，提供至少8小时的不间断供电。

5.1.3.电力与空调

河北CA有安全、可靠的电力供电系统及电力备用系统以确保系统7X24小时正常供电。另外，河北CA还配有通风、空调等设备控制机房的温度和湿度。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

5.1.4.防水

机房内主要设备采用专用的防水插座,并采取了必要措施防止因下雨或水管破损，造成的地板渗水或空调漏水等现象。河北CA的系统有充分保障，能够防止水侵蚀。河北CA机房有专业的环境监控设备，每个空调的下方管道部署了水浸探头，当发生漏水问题，警铃报警并发送短信通知机房工作人员。

5.1.5.火灾防护

河北CA消防报警系统建设根据《卤代烷1211灭火系统设计规范(GBJ 110-87)》，采用七氟丙烷（HFC-227e）气体灭火系统。

机房消防报警系统通过设置在机房的温感和烟感采集消防数据,同时供系统实时处理火灾自动报警终端的报警数据和系统运行状态数据。系统管理分手动模式和自动模式两种，实现网络系统实时检测、监测和系统的手动、自动控制模式的设定，并完成了系统设计的各种有关联动动作。

5.1.6.介质存放

河北CA存储介质的存储地点与河北CA系统分开，并且能够防磁、防静电干扰、防火、防水，保证物理安全。存储介质由专人管理。

5.1.7.废物处理

当河北CA存档的纸张文件和材料已不再需要或存档期限已满时，必须采取

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

措施销毁，使信息无法恢复。密码设备和存放敏感信息的存储介质在作废处置前根据制造商提供的方法先将其初始化并进行物理销毁。

5.1.8.异地备份

河北CA每周对系统数据、审计日志数据和其他敏感信息进行日常备份，同时将备份的业务数据送到异地备份中心，进行异地备份保存。

5.2. 程序控制

5.2.1.可信角色

河北 CA 及注册机构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：

◈ 安全管理人员

◈ 密钥管理小组人员

◈ 审计管理小组人员

◈ 证书鉴别、注册、审核、签发人员

◈ 客户服务人员

5.2.2.每项任务需要的人数

河北CA制定了严格的策略和控制程序，保障基于不同权限的职责分离。敏

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

感操作要求多名可信人员共同参与完成。

5.2.3.每个角色的识别与鉴别

河北CA的工作人员，按照所担任角色的不同在进入机房或系统时，需要使用门禁卡、指纹、数字证书进行身份的识别与鉴别。河北CA完整地记录所有操作行为。

5.2.4.需要职责分割的角色

为保证系统安全，遵循可信角色分离、操作和管理分离的原则，即由不同的可信角色来完成重要操作。任何证书生命周期操作都要由审核、签发2个可信角色来完成。系统管理员、业务管理员、系统审计员、密钥管理员分别由不同的可信人员担任，进行权限与职责分割，共同完成对电子政务电子认证系统的管理。

5.3. 人员控制

5.3.1.资格、经历和清白要求

河北CA 所有员工已签订保密协议。对于充当可信角色或其他重要角色的人员，必须具备一定的专业资格。河北CA 要求充当可信角色的人员必须忠诚、可信，未兼职影响CA 运行的其它工作，无同行业重大错误记录，无违法记录等。一般情况下，由河北CA 人力资源部负责对河北CA员工的背景、资格及经历的真实性进行核实。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

5.3.2.背景调查程序

河北CA对员工在担任可信角色前进行相应的背景调查，并要求员工必须提交相关材料，以审查其是否具备胜任预期工作的条件。

5.3.3.培训要求

河北CA对工作人员根据其岗位和角色的不同进行长期、有计划的持续培训。培训内容包括：系统软硬件安装与维护、系统安全、应用软件的运行和维护、系统备份与恢复、CA中心的运行管理、CA中心的内部管理及相关法律法规等。同时，对新技术、系统功能更新或新系统的加入等进行专项培训。

5.3.4.再培训的频度和要求

对于充当可信角色或其他重要角色的人员，每年必须参加河北CA组织的再培训。认证策略调整、系统更新时，河北CA对全体人员进行再培训，以适应新的变化。

5.3.5.工作岗位轮换的频度和次序

对于可替换角色，河北CA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。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

5.3.6.未授权行为的处罚

当河北CA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河北CA系统或进行越权操作，河北CA得知后将立即对该员工进行工作隔离，并对该员工的未授权行为进行风险评估，采取相应的防范处理措施。根据评估结果对该员工进行相应处罚，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

对不属于河北CA工作人员，但从事与河北CA有关业务的独立签约者，统一要求如下：

1. 人员档案进行备案管理；
2. 具有相关业务的工作经验；
3. 必须接受由河北 CA 组织的为期一周的岗前培训。

5.3.8.提供给人员的文件

河北CA提供给内部员工的文件应包括培训材料和与员工工作相关文档。

5.4. 审计记录程序

5.4.1.记录事件的类型

在河北CA运行系统中，记录所有与物理环境安全、网络安全、密码安全、

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

证书处理系统应用与数据安全、人员操作行为、操作系统和数据库运行安全等相关事件，以备审查。这些记录，无论是自动生成的还是手写、书面、电子文档或录像形式，都包含事件的日期、事件的内容、事件的发生时间段、事件相关的实体等。河北CA 还将记录其它认为有必要做记录的事件，例如：机房参观记录、人事变动等。

5.4.2.处理日志的频度

河北CA应定期检查审计日志，以便发现重要的安全和操作事件，对发现的安全事件采取相应的措施。

5.4.3.审计日志的保留期限

纸质审计日志处理和归档之后将至少保存1年，河北CA 密钥的审计日志的保留期限为CA证书失效后1年。

5.4.4.审计日志的保护

河北CA执行严格的审计日志管理办法，确保只有河北CA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。审计日志的制作和访问进行岗位分离。河北CA将审计日志存储到硬盘中，实行安全保管。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

5.4.5.审计日志的备份程序

对审计日志的备份应该建立和执行可靠的制度，定期进行备份。

5.4.6.审计收集系统

河北CA审计数据的收集由审计人员完成。收集方式为系统自动记录和人工采集两种方式。

5.4.7.对导致事件主体的通知

河北CA 对审查中发现的攻击现象将做详细记录，在法律许可的范围内追溯攻击者或肇事者，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。

河北CA有权决定是否对导致事件的实体进行通告。

5.4.8.脆弱性评估

根据审计记录，河北CA应定期进行安全脆弱性评估，并根据评估报告采取补救措施。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

5.5. 记录归档

5.5.1.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。

5.5.2.归档记录的保留期限

河北CA的电子认证业务规则（CPS）应规定合理的归档记录保留期限。

5.5.3.归档文件的保

河北CA对各种电子、磁带、纸资形式的归档文件，都有安全保护措施和严格的管理程序，确保归档文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为。

5.5.4.归档文件的备份程序

所有归档的文件和数据库除了保存在河北CA，还将异地备份。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。河北CA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。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

5.5.5.记录时间戳要求

河北CA的档案在创建的时候须加盖带有河北CA数字签名的时间戳。

5.5.6.归档收集系统

河北CA 中的档案收集系统由人工操作和自动操作两部分组成。

5.5.7.获得和检验归档信息的程序

河北CA每年验证归档信息的完整性。

5.6. 密钥变更

因河北CA根证书到期而需要更替密钥对时采取的措施如下：

1. 河北CA的根证书是由国家密码管理局的根CA系统所签发，其密钥对由河北CA的证书系统中的加密机产生，证书到期更换密钥时将签发 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 张证书达到密钥更替的目的，使新旧证书之间互相认证。

2. 信任电子认证服务机构证书到期之前，河北CA将采取以下方式更替：

- ◈ 河北CA将在证书到期前的60天内停止颁发新的证书；
- ◈ 旧的证书到期后，河北CA将用新的密钥对签发证书。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

密钥更替时直接把当前CA证书吊销，签发到ARL并发布，然后签发一个新的CA证书，通过证书库和LDAP方式下发给证书应用系统。

3. 河北CA将继续使用旧的根私有密钥签发的CRL，直到旧的私钥签发的证书到期为止。

5.7. 损害与灾难恢复

5.7.1.事故和损害处理程序

河北CA应制订各种事故处理方案和应急处理预案，规定相应的事故和损害处理程序。

5.7.2.计算机资源、软件和/或数据的损坏

如果出现计算机资源、软件和/或数据损坏的事件，河北CA立即启动事故处理程序，如有必要，可按照灾难恢复计划实施恢复。

5.7.3.实体私钥损害处理程序

对于实体私钥的损害，河北CA处理程序如下：

1. 当证书订户发现实体证书私钥损害时，必须立即停止使用其私钥，并按照cp 4.8节中规定的程序进行吊销。

2. 当河北CA或注册机构发现证书订户的实体私钥受到损害时，河北CA或注册机构将立即吊销证书，并通知证书订户，订户必须立即停止使用其私钥。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

3. 当河北CA的CA证书出现私钥损害时，河北CA将立即吊销CA 证书并及时通知依赖方，然后生成新的CA 密钥对、签发新的CA 证书。

对于上述1、2之情况也可根据实际情况参照cp 4.7节证书密钥更新。

5.7.4.灾难后的业务存续能力

河北CA在发生灾难后，应有如下几个方面的业务存续能力：

1. 在尽可能短的时间内恢复业务系统，最多不超过48小时；

2. 能够恢复客户信息；

3. 能够保证恢复后的运营场地符合安全要求；

4. 有足够的人员继续开展业务并且不违反职责分割的要求。

5.8. CA 或 RA 的终止

当河北CA及其注册机构需要停止其业务时，必须严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》及相关法规中对认证机构终止电子认证服务的规定要求进行有关工作。

在河北CA终止前，必须：

1. 委托业务承接单位；

2. 起草河北CA终止声明；

3. 通知与河北CA终止相关的实体；

4. 关闭从目录服务器；

5. 证书注销；

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

6. 处理存档文件记录；

7. 停止认证中心的服务；

8. 存档主目录服务器；

9. 关闭主目录服务器；

10. 处理河北CA业务管理员和河北CA业务操作员；

11. 处理加密密钥；

12. 处理和存储敏感文档；

13. 清除河北CA 主机硬件。

当RA因故终止服务时，河北CA将按照与其签订的相关协议处理有关业务承接事宜和其他事项。

6. 认证系统技术安全控制

6.1. 密钥对的生成与安装

6.1.1.密钥对的生成

订户的签名密钥对由订户的密码设备（如智能密码钥匙）生成，加密密钥对由密钥管理中心（KMC）生成。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

6.1.2.加密私钥传送给订户

订户的签名密钥对由订户的密码设备生成并保存。订户证书的加密私钥在KMC生成。加密私钥从 KMC 到订户的密码设备（如智能密码钥匙）的传递过程采用国家密码管理局许可的对称密钥算法加密。

6.1.3.公钥传送给证书签发机构

订户的签名证书公钥，经注册机构传送到河北CA，在此过程中采用国家密码管理局许可的对称密钥算法加密，保证传输中数据的安全。

河北 CA 从 KMC 取得用户公钥后为其签发证书，在此过程中采用国家密码管理局许可的对称密钥算法加密，保证传输中数据的安全。

6.1.4.CA 公钥传送给依赖方

河北CA应该通过安全可靠的途径将CA公钥传给依赖方，包括从安全站点下载、面对面的提交等方式。

河北CA也需要通过目录发布其CA 证书。

6.1.5.密钥的长度

河北CA同时支持RSA和SM2算法。订户用于加密和签名的RSA密钥对长度支持1024位和2048位，SM2密钥对长度支持256位。。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

6.1.6.公钥参数的生成和质量检查

对于使用硬件密码模块的河北CA订户，公钥参数必须使用国家密码主管部门批准许可的加密设备和硬件介质生成，例如加密机、加密卡、USB Key、IC卡等生成和选取，并遵从这些设备的生成规范和标准。河北CA认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

对于参数质量的检查,同样由通过国家密码主管部门批准许可的加密设备和硬件介质进行，例如加密机、加密卡、USB Key、IC卡等。

6.1.7.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。

6.2. 私钥保护和密码模块工程控制

认证机构必须通过物理、逻辑和过程控制的综合实现来确保CA私钥的安全。订户协议会要求证书订户采取必要的预防措施防止私钥的丢失、泄露、更改或未经授权的使用。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

6.2.1.密码模块的标准和控制

河北CA 使用国家密码管理局许可的产品，密码模块的标准符合国家规定，其安全性达到以下要求：

1．接口安全：不执行规定命令以外的任何命令和操作；

2．协议安全：所有命令的任意组合，不能得到私钥的明文；

3．密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

4．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。

6.2.2.私钥多人控制

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方式，只有其中三人以上在场并得到许可的情况下，才能对私钥进行上述操作。

订户的私钥由订户自己通过终端密码设备控制。

6.2.3.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。

KMC严格保证订户密钥对的安全，密钥以密文的形式保存，密钥库禁止外界非法访问。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

6.2.4.私钥备份

订户的签名私钥在河北CA和KMC都不进行备份。加密私钥由KMC备份，备份数据以密文形式保存。

6.2.5.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。

KMC 提供过期加密私钥的归档服务。

6.2.6.私钥导出、导入密码模块

CA的私钥，河北CA应严格按照根密钥管理规范进行备份，除此之外的任何导入导出操作将不被允许。当CA 密钥对备份到另外的硬件密码模块上时，以加密的形式在模块之间传送，并且在传递前要进行身份鉴别，以防止CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

河北CA不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。对于存放在软件密码模块中的私钥，如果订户愿意并且自行承担相关风险，订户可自主选择导入导出的方式，操作时需要采用口令保护等授权访问控制措施。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

6.2.7.私钥在密码模块的存储

河北CA 的私钥必须保存在硬件密码模块中。

6.2.8.激活私钥的方法

河北CA具有激活私钥权限的工作人员在通过智能密码钥匙密码验证后，启动密钥管理程序，进行激活私钥的操作。

6.2.9.解除私钥激活状态的方法

河北CA具有冻结私钥权限的工作人员在通过智能密码钥匙密码验证后，启动密钥管理程序，进行冻结私钥的操作。

6.2.10. 密码模块的评估

河北CA使用国家密码主管部门批准和许可的密码产品，接受其颁发的各类标准、规范、评估结果、评价证书等各类要求，河北CA可根据产品性能、工作效率、供应厂商的资质等方面的条件，选择所需要的模块。

6.3. 密钥对管理的其他方面

6.3.1.公钥归档

必须归档CA和最终订户证书，归档的证书可存放在数据库中。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

6.3.2.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保持一致，目前订户证书的有效期一般为一年。

6.4. 激活数据

6.4.1.激活数据的产生和安装

CA私钥的激活数据，必须按照关于密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。

订户私钥的激活数据，包括用于下载证书的口令（以密码信封的形式提供）、USB Key的PIN码等，都必须在安全可靠的环境下随机产生。

6.4.2.激活数据的保护

对于CA私钥的激活数据，必须通过秘密分割将分割后的激活数据由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求，签署协议确认他们知悉秘密分割掌管者责任。

对于订户私钥的激活数据，包括口令或 PIN 码，都必须在安全可靠的环境下产生。订户应妥善保管好其口令或PIN 码，防止泄露或窃取。同时为了配合业务系统的安全需求，应该经常对激活数据进行修改。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

6.4.3.激活数据的其他方面

当私钥的激活数据进行传送时，应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

6.5. 计算机安全控制

6.5.1.特别的计算机安全技术要求

河北CA数字证书认证系统的数据文件和设备由指定的工作人员进行维护。河北CA部署了入侵检测和漏洞扫描系统，未经授权，其他人员无法操作和控制CA认证系统。河北CA还部署了多级异构防火墙，确保系统网络安全。河北CA系统密码有最小密码长度要求，而且必须符合复杂度要求，工作人员定期更改系统密码。

6.5.2.计算机安全评估

河北CA根据法律法规和主管部门的规定，按照国家计算机安全等级的要求，实现安全等级制度。

河北CA的认证系统，通过了国家密码管理局的安全性审查。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

6.6. 生命周期技术控制

6.6.1.系统开发控制

系统开发采用先进的安全控制理念,保证开发环境的安全、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。系统的容错采用多路并发容错方式,确保系统在出错时尽可能不影响其他服务。

6.6.2.安全管理控制

河北CA认证系统的信息安全管理，严格遵循国家密码主管部门的有关运行管理规范进行操作。

河北CA认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安全和使用,任何修改和升级会记录在案并进行版本控制、功能测试和记录。河北CA还对认证系统进行定期和不定期的检查和测试。

河北CA采用一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

硬件设备由采购到接收时,会进行安全性的检查,用来识别设备是否被入侵，是否存在安全漏洞等。加密设备的采购和安装必须在更加严格的安全控制机制下，进行设备的检验、安装和验收。

河北CA认证系统所有的软硬件设备升级以后，废旧设备在进行处理时，首

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

先必须确认其是否有影响安全的信息存在。

6.6.3.生命周期的安全控制

河北CA的证书认证系统在系统设计、开发和运行过程中充分进行了安全性考虑 ,完全符合国家有关标准 ,使用的算法和密码设备均通过了有关部门的鉴定 ,整个系统安全可靠。

6.7. 网络的安全控制

系统网络安全的主要目的是保障网络基础设施、主机系统、应用系统及数据库运行的安全。河北CA采取了多级异构防火墙、病毒防护、入侵检测、漏洞扫描、数据备份、灾难恢复等安全控制措施。

6.8. 时间戳

认证系统的各种系统日志、操作日志都应该有相应的时间标识。这些时间标识不需要采用基于密码的数字时间戳技术。

7. 证书、证书吊销列表和在线证书状态协议

7.1. 证书描述

河北CA 签发的证书符合X.509 V3证书格式。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

7.1.1.版本号

河北CA订户证书符合X.509 V3证书格式，版本信息存放在证书版本信息栏内。

7.1.2.证书标准项

1. 证书序列号

唯一标识该证书的一组字符。

2. 证书有效期

证书的有效期根据协议规定定义。

3. 主题

为证书订户申请证书时所填写的申请信息，即订户的甄别名。详细请参看cp 3.1节命名”。

河北CA采用经国家密码管理局签发的CA机构数字证书进行用户证书的签发。河北CA获得的国家密码管理局签发的CA机构证书如下：

1. SM2证书颁发者

CN = HBSM2CA
OU =hebca
O = hebca
L = shijiazhuang
S = hebei
C = CN

2. RSA证书颁发者

CN = HeBeiRSACA

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

OU = 河北省数字证书认证中心

O = hebca

L = 石家庄

S = 河北

C = CN

7.1.3.证书扩展项

1. 颁发机构密钥标识符：

颁发机构密钥标识符与验证签名的公开密钥相联系。河北CA 根证书公钥与此标识符相联系。

2. 主题密钥标识符：

通过主体密钥标识符识别相对应证书的公钥

3. 密钥用法：

密钥加密，数据加密，电子签名，验证证书签名，验证CRL 签名，只加密，只解密。

4. 基本限制：

用于鉴别证书持有实体身份，如终端用户等。

5. CRL 分发点：

由河北CA 定义的CRL 发布点。

7.1.4.算法对象标识符

对于使用RSA算法的数字证书，使用SHA1WithRSAEncryption 算法；对于使

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

用SM2算法的数字证书，使用SM3WithSM2Encryption算法。

7.1.5.名称形式

河北CA数字证书中的主题Subject的X.500 DN是订户的唯一标识。

7.2. 证书吊销列表

河北CA定期签发CRL，供用户查询使用。

依本 CP 签发的CRL 符合RFC5280 标准。CRL 至少包含如下表所述基本域和内容。

域	值或者值的限制
版本	V2
颁发者	签发CRL的实体，颁发者甄别。
生效日期	CRL 的签发日期
下次更新	CRL 下次签发的日期。CRL每隔24 小时更新
签名算法	签发CRL所使用的签名算法
颁发机构密钥标识符	由160位的颁发证书机构公钥进行散列运算后的值构成
吊销列表	列出吊销的证书，包括吊销证书的序列号和吊销日期

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

7.2.1.版本

河北CA目前签发X.509 V2版本的CRL ,此版本号存放在CRL版本格式栏目中。

7.2.2.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

河北CA采用经国家密码管理局签发的CA机构数字证书进行用户证书的签发。河北CA获得的国家密码管理局签发的CA机构证书如下：

1. SM2证书颁发者

CN = HBSM2CA

OU =hebca

O = hebca

L = shijiazhuang

S = hebei

C = CN

2. RSA证书颁发者

CN = HeBeiRSACA

OU = 河北省数字证书认证中心

O = hebca

L = 石家庄

S = 河北

C = CN

◈ CRL 发布

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

河北CA每隔24 小时自动发布最新的CRL。

◈ 签名算法

对于使用RSA算法的CRL，使用SHA1WithRSAEncryption算法；

对于使用SM2算法的CRL，使用SM3WithSM2Encryption算法。

7.3. OCSP 描述

河北CA为用户提供OCSP（在线证书状态查询服务），OCSP作为CRL的有效补充，方便证书用户及时查询证书状态信息。

7.3.1.版本号

RFC6960定义的OCSP V1版本。

7.3.2.OCSP 扩展项

无规定。

8. 认证机构审计和其他评估

8.1. 评估的频度和情形

1、根据《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》等相关法律法规的要求，接受上级主管部门每年一次的评估和检查。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

2、根据国家相关要求和《河北CA电子政务电子认证业务规则》的规定，河北CA按照内部审计评估制度，每年至少执行一次内部审计评估，包括对河北CA授权的注册机构和其他关联服务机构的审计评估。

8.2. 评估者的身份/资格

1、河北CA无条件接受主管部门的评估。对河北CA实施评估的评估者所具有的资质和经验，由主管部门决定。

2、在进行内部审计评估时，河北CA要求评估人员至少具备安全审计的相关知识，熟悉《河北CA电子政务电子认证业务规则》，并具备计算机、网络、信息安全等方面的知识和实际工作经验。

3、如果河北CA认为有必要聘请外部单位实施内部评估，那么该单位应该具备以下的资质和条件：

◈ 必须是经许可的、有营业执照的评估机构，在业界享有良好的声誉；

◈ 了解计算机信息安全体系、通信网络安全、PKI 技术标准和规范；

◈ 具备检查系统运行安全和可靠性的专业技术和工具；

◈ 熟悉认证机构的管理和运营模式以及相关法律法规；

◈ 与河北CA签订保密协议。

8.3. 评估者与被评估者之间的关系

1、外部评估者（包括主管部门）和河北CA之间是独立的关系，没有任何利益关联，评估者能够以独立、公正、客观的态度对河北CA进行评估。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

2、河北CA的内部评估者，与被评估的对象之间，也是独立的关系，没有任何的利益关联，评估者能够以独立、公正、客观的态度对被评估的对象进行评估。

8.4. 评估的内容

1、河北CA按照主管部门依法提出的评估要求和规范，接受其任何内容的评估。

2、河北CA内部评估审计的内容包括：

- ◈ 电子政务电子认证业务规则审查；
- ◈ 人事审查；
- ◈ 物理环境建设及安全运行管理规范审查；
- ◈ 系统结构及其运行审查；
- ◈ 密钥管理审查；
- ◈ 客户服务及证书处理流程审查。

8.5. 对问题与不足采取的行动

1、河北CA的主管部门评估完成后，必须根据评估的结果检查缺失和不足，按照整改要求提交整改计划书，并接受评估部门对整改计划的审查，以及对整改情况的再次评估。

2、河北CA完成内部评估后，评估人员需要列出所有问题项目的详细清单，由评估人员和被评估对象共同讨论有关问题，并将结果书面通知河北CA运营安全管理小组和被评估对象。被评估对象必须根据评估的结果检查缺失和不足，按

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

照整改要求提交整改计划书，并接受河北CA运营安全管理小组对整改计划的审查，以及对整改情况的再次评估。

8.6. 评估结果的传达与发布

1、主管部门在完成评估后，按照法律法规的要求对评估结果进行处理。

2、河北CA的内部评估结果在与被评估对象进行讨论确定后，将视为机密资料进行保存，只有被评估对象和河北CA安全策略委员会可以查阅。对河北CA关联方，河北CA将依据签署的协议来公布评估结果。

8.7. 其他评估

无规定。

9. 法律责任和其他业务条款

9.1. 费用

河北CA可根据提供的电子认证服务向本机构的证书订户收取费用，具体收费标准必须根据国家有关物价管理部门的批复文件执行，河北CA不得擅自提高收费标准，扩大收费范围。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

9.1.1.证书新增和更新费用

用户在获得河北CA证书服务前均需交纳证书相关费用。河北CA依据河北省物价局批准的收费标准，向用户收取相关费用。根据证书实际应用的需要，河北CA 在不高于收费标准的前提下可以进行适当调整。。

9.1.2.证书查询费用

河北CA目前对有效期内证书不收取证书查询费用。

9.1.3.吊销和状态信息查询费用

查询证书是否吊销，河北CA不收取信息访问费用。

对于在线证书状态查询（OCSP），由河北CA与订制者在协议中约定。

9.1.4.其他服务费用

河北CA可根据请求者的要求，提供各种通知服务，具体服务及费用在与请求者签订的协议中约定。

9.1.5.退款策略

在实施证书操作和签发的过程中，河北CA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，河北CA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体系，河北CA将不退还剩余时间的

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

服务费用。

9.2. 财务责任

河北CA向证书订户提供证书服务保障。订户因河北CA提供的电子签名认证服务从事民事活动遭受损失，河北CA不能证明自己无过错的，承担赔偿责任。

9.3. 业务信息保密

9.3.1.保密信息范围

保密信息的范围包括但不限于以下方面：

1. 在双方披露时标明为保密的；

2. 以合同或其他书面形式确认为保密信息的。

对于河北CA保密信息的范围包括但不限于以下方面：

1. 最终用户的私人签名密钥；

2. 保存在审计记录中的信息；

3. 年度审计结果；

4. 除非有法律要求，由河北CA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。

河北CA 不保存任何证书应用系统的业务信息或交易信息。除非法律明文规定，河北CA 没有义务公布或透露订户数字证书以外的信息。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

9.3.2.不属于保密的信息

1. 与证书申请有关的信息不属于保密信息。

2. 河北CA 在目录服务器中公布的证书信息及状态信息，不属于保密信息。

3. 其他可以通过公共渠道获得的信息。

9.3.3.保护保密信息的责任

河北CA 和订户均有保护保密信息的责任，并保证不将保密数据和信息（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；在信息披露时，如果已明确表示保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。

当河北CA需要配合司法机关依法取证时，河北CA 提供的相关保密信息不视为违反了保密要求和义务，河北CA不承担相关责任。

9.4. 个人隐私保密

9.4.1.隐私保密计划

河北CA应制定隐私保密计划对订户的个人信息保密。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

9.4.2.作为隐私处理的信息

作为隐私处理的信息包括：

1. 订户的有效证件号码如身份证号码、单位机构代码；

2. 订户的联系电话；

3. 订户的地址；

4. 订户的银行帐号。

9.4.3.不被认为隐私的信息

订户持有的证书内包括的信息，以及该证书的状态等，是可以公开的，不被视为隐私信息。

9.4.4.保护隐私的责任

河北CA、注册机构有妥善保管与保护本CP第9.4.2节中规定的订户隐私信息的责任与义务。

9.4.5.使用隐私信息的告知与同意

河北CA在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理和服务订户的目的。在使用这些信息时，无论是否涉及到隐私，河北CA都没有告知订户的义务，也无需得到订户的同意。

河北CA在任何法律法规或者法院以及公权力部门通过合法程序的要求下，

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

或者信息所有者书面授权的情况下向特定对象披露隐私信息时，也没有告知订户的义务，并且不需得到订户的同意。

河北CA、注册机构如果需要将订户隐私信息用于双方约定的用途以外的目的，事前必须告知订户并获得订户同意和授权，而且这种同意和授权要用可归档的方式（如传真、信函等）。

9.4.6.依法律或行政程序的信息披露

由于法律执行、法律授权的行政执行的需要，河北CA将订户的隐私信息提供给有关执法机关、行政执行机关是允许的。包括：

1. 政府法律法规的规定并且经相关部门通过合法程序提出申请；
2. 法院以及公权力部门处理因使用证书产生的纠纷时合法的提出申请；
3. 具有合法司法管辖权的仲裁机构的正式申请。

9.4.7.其他信息披露情形

如果订户要求河北CA提供某类特定客户支援服务如资料邮寄时，河北CA则需要把订户的联系电话和地址等信息提供给第三者如邮寄公司。

9.5. 知识产权

河北CA 享有并保留对所有河北CA 签发的证书和提供的相关文件享有知识产权，河北CA 关联实体在征得河北CA 的同意后，可以使用相关的文件和手册。其它任何人未经河北CA 的书面同意，不得以任何方式、任何途径进行复制、存

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

储、使用或传播。河北CA 自行决定河北CA 关联实体采用的证书服务软件系统，以便保证系统的兼容和互通。

订户自己产生的签名密钥的知识产权归订户所有，但是签名公钥经过河北CA 签发成证书后，河北CA 即拥有该证书的知识产权，只提供给证书订户和依赖方使用的权力。

9.6. 陈述与担保

9.6.1.CA 的陈述与担保

河北CA在提供电子政务电子认证服务活动过程中承诺如下：

1. 河北CA遵守《中华人民共和国电子签名法》及相关法律法规的规定，接受主管部门的监督指导，对签发的数字证书承担相应的法律责任。

2. 河北CA保证使用的系统及密码符合国家相关标准，保证自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。

3. 除非已通过河北CA证书库发出的河北CA的私钥被破坏或被盗的通知，河北CA保证其私钥是安全的。

4. 河北CA签发给订户的证书符合《河北CA电子政务电子认证业务规则》的所有要求。

5. 在现有技术条件下，河北CA保证签发的数字证书在有效期内的有效性和可靠性。

6. 河北CA将向证书订户通报任何已知的、将在本质上影响订户证书的有效

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

性和可靠性事件。

7. 河北CA按要求及时吊销证书，并发布到CRL上供依赖方查询。

8. 河北CA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。

9. 证书公开发布后，河北CA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。

9.6.2.RA 的陈述与担保

河北CA注册机构在参与电子认证服务过程中承诺如下：

1. 提供给证书用户的注册过程完全符合《河北CA电子认证业务规则》的所有要求。

2. 在证书申请、审核、制作过程中，不会因失误而导致证书中的信息与证书申请人的信息不一致。

3. 注册机构按《河北CA电子认证业务规则》的规定，及时响应并向河北CA提交订户证书申请、吊销、更新等服务请求。

9.6.3.订户的陈述与担保

订户一旦接受河北CA签发的证书，就被视为向河北CA、注册机构及依赖方做出以下承诺：

1. 订户了解《河北CA电子认证业务规则》的所有条款和与其证书相关的证书政策，并同意承担证书持有人有关证书的相关责任和义务。

2. 订户在证书申请时提交的所有信息完整、真实、正确，可供河北CA或注

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

册机构检查和核实。

3. 订户妥善保管河北CA签发的数字证书载体（含数字证书和私钥）及密码，采取安全、合理的措施来防止证书数字证书载体及密码的遗失、泄露和被篡改等事件的发生。

4. 私钥为订户本身所访问和使用，订户对使用私钥的行为负责。

5. 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘密码、泄密以及其他情况，订户立刻通知河北CA或注册机构，申请采取吊销等处理措施。

6. 订户已知其证书被冒用、破解或被他人非法使用时，及时通知河北CA或注册机构吊销证书。

9.6.4.依赖方的陈述与担保

依赖方了解《河北CA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。

证书依赖方对证书的信赖行为表明了解《河北CA电子认证业务规则》的所有条款，并同意承担证书依赖方有关证书使用的相关责任和义务。

9.6.5.其他参与者的陈述与担保

其他参与者的陈述与担保同“§9.6.4依赖方的陈述与担保”。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

9.7. 担保免责

下列情况之一的，免除河北CA 的责任。

1. 如果证书申请人故意或无意地提供不完整、不可靠、不真实或已过期的信息，得到河北CA签发的数字证书，由此引起的法律和经济纠纷由证书申请人全部承担。

2. 河北CA 不承担任何未经授权的人或组织以河北CA 的名义散布的信息所引起的法律责任。

3. 河北CA不承担在法律许可的范围内，根据司法程序要求如实提供业务中“不可抵赖”的数字签名证据时引起的任何法律责任。

4. 河北CA不对任何一方在证书应用过程中引起的直接或间接的损失承担责任。

5. 河北CA 和注册机构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。河北CA 和证书持有人之间的关系以及河北CA 和依赖方之间的关系并不是代理人或委托者的关系。证书持有人和依赖方都没有权利以合同形式或其他方式让河北CA 承担信托责任。

6. 由于客观意外、外部原因导致的技术故障（含电力、通讯、设备或网络故障等）以及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，河北CA 不承担相关责任。关于不可抗力的描述参见“§9.16.5不可抗力”。

7. 订户因证书丢失、私钥泄漏等原因需办理挂起、吊销手续，在订户办理证书挂起或吊销手续前及自订户提交挂起或吊销申请后24小时内造成的损失，河北

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

CA 不承担相关责任。

以上未尽事宜，依照中华人民共和国现行法律、法规执行。

9.8. 有限责任

河北CA根据与订户签订的合同承担相应的有限责任，且责任仅限于涉及由河北CA提供的证书认证服务，对于因订户或依赖方及应用服务提供者的原因造成的损害河北CA不承担任何责任。

订户因依据河北CA提供的电子签名认证服务从事民事活动遭受损失，河北CA不能证明自己无过错的，承担有限责任。

9.9. 赔偿

河北CA按照《河北CA电子认证业务规则》“§9.7担保免责”和“§9.8有限责任”条款具有担保免责和承担有限赔偿的责任。河北CA在与订户和依赖方签定的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

河北CA对订户有限赔偿责任的赔偿金额上限为该订户实际缴纳数字证书当年注册开户费或年维护更新服务费的十倍。证书订户和依赖方在接受、使用或信赖证书时就表示同意在以下情况承担赔偿河北CA和/或有关各方名誉损失、直接和间接经济损失的责任：

1. 未向河北CA提供真实、完整和准确的信息，而导致河北CA或有关各方损失。

2. 未能保护订户私钥，或者没有使用必要的防护措施来防止订户私钥遗失、

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

泄密、被修改或被未经授权的人使用并造成损失。

3. 在知悉证书密钥已经失密或者可能失密时，未及时书面告知河北CA，并终止使用该证书，而导致河北CA或有关各方损失。

4. 订户如果向依赖方或者应用服务提供者传递信息时表述有误，而依赖方或者应用服务提供者用证书验证了该订户签署的一个或多个数字签名文件后相信了这些表述，而导致河北CA或有关各方损失。

5. 证书订户或依赖方对证书的非法使用，违反国家或河北CA 对证书使用的相关规定，造成了河北CA 或有关各方的利益受到损失。

9.10. 有效期与终止

9.10.1. 有效期

本CP在生效日期零时正式生效，上一版本的CP同时失效；本CP在下一版本CP生效之日或在河北CA终止电子认证服务时失效。

9.10.2. 终止

河北CA终止电子认证服务时，本CP终止。

9.10.3. 终止的效果与存续

本CP的终止，意味着认证机构认证业务的终止，但认证业务的终止不意味着认证机构责任的终止。认证机构在业务终止后应采取合理的措施，将认证服务

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

转到其他认证机构，保证订户的利益。

9.11. 对参与者的个别通告及信息交互

认证机构在必要的情况下，如主动吊销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为，可通过适当方式，如电话、电子邮件、信函等，个别通知订户、依赖方。

9.12. 修订

9.12.1. 修订程序

当《河北CA CP》不适用时，由河北CA CPS/CP 策略管理小组负责修订，交由河北省电子认证有限公司和河北CA 律师共同研究审议。审议通过后在河北CA的网站(http://www.hebca.com)上发布新版本的《河北CA CP 》，并于三十日内向信息产业部备案。

9.12.2. 通知机制和期限

修订后的CP经批准后将立即在河北CA的网站www.hebca.com上发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，河北CA将在合理的时间内通知有关各方，合理的时间应保证有关方受到的影响最小。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

9.12.3. 必须修订的情形

如果出现下列情况，河北CA必须对本CP进行修改：

1. 密码技术出现重大发展，足以影响现有CP的有效性；

2. 有关认证业务的相关标准进行更新；

3. 认证系统和有关管理规范发生重大升级或改变；

4. 法律法规和主管部门要求；

5. 现有CP出现重要缺陷。

9.13. 争议解决条款

当河北CA、订户和依赖方之间出现争议时，有关方面应依据协议通过协商解决，协商解决不了的，可通过法律解决。

9.14. 管辖法律

河北CA的CP受国家已颁布的《中国人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》法律法规管辖。

9.15. 符合适用法律

认证机构的所有业务、活动、合同、协议必须符合《中国人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》以及其它中华人民共和国法律法规的规定。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

9.16. 一般条款

9.16.1. 完整协议

CP、CPS、订户协议、依赖方协议及其补充协议将构成PKI参入者之间的完整协议。

9.16.2. 让渡

河北CA、注册机构、订户及依赖方之间的责任、义务不能通过任何形式转让给其他方。

9.16.3. 分割性

当法庭或其他仲裁机构判断协议中的某一条款由于某种原因无效或不具执行力时，不会导致整个协议无效。

9.16.4. 强制执行

合同（协议）一方或几方不履行合同（协议）条款的，其它方可以要求强制执行。

9.16.5. 不可抗力

依据本CP制定的CPS应包括不可抗力条款，以保护各方利益。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com

9.17. 其他条款

河北CA对本CP具有最终解释权。

地址：河北省石家庄市友谊南大街100号
客服热线：400-707-3355
传真：0311-83013591
网址：http://www.hebca.com