河北省电子认证有限公司

证书策略

版本 4.5

河北省电子认证有限公司

2025 年 4 月

版权声明

《河北省电子认证有限公司证书策略》受到完全的版权保护，本文件中所涉及的“河北CA CP”、“河北CA证书策略”及其标识等由河北省电子认证有限公司独立享有版权及其它知识产权。

未经河北省电子认证有限公司书面同意，本文件的任何部分不得以任何方式、任何途径（电子的、机械的、影印、录制等）进行复制、储存、调入网络系统检索或传播。

在满足下述条件下，本文件可以被书面授权，在非独占性的、免收版权许可使用费的基础上进行复制及传播：

●前文的版权说明和上段主要内容应标于每个副本开始的显著位置；

●副本应按照河北CA提供的文件准确、完整地复制。

对任何复制及传播本文件的请求，请寄往：河北省电子认证有限公司。

地址：石家庄市桥西区红旗大街88号翰林观天下23号楼27层

邮编：050081

电话：400-707-3355

电子邮件：hebca@hebca.com

修订历史

版本	日期	备注
1.0	2005 年 9 月 8 日	依据 RFC3647 结构进行编写。
2.0	2006 年 1 月 26 日	根据《电子认证业务规则规范 (试行)》的各项要求进行修改。
2.1	2006 年 8 月 10 日	根据 RFC3647 标准、《电子认证业务规则规范 (试行)》及《电子认证服务机构年检指引（试行)》进行制定。(内部修订)
2.2	2006 年 10 月 25 日	根据信产部电子认证服务管理办公室的审查意见进行修订。
3.0	2011 年 11 月	对证书生命周期中相关业务的内容进行修订完善。更正了不规范名称的文字描述。
3.1	2012 年 5 月	修订、补充身份鉴别方式、证书更新处理方式，在证书生命周期操作中增加证书变更，增加对河北 CA 数字证书载体不得转让他人的说明。
3.2	2014 年 12 月	修改退款策略。
3.3	2016 年 11 月	增加提供 7X24 小时证书状态服务的描述。
4.0	2017 年 12 月	修改用户提交资料内容

4.1	2018 年 9 月	修订退款策略
4.2	2019 年 12 月	修改初始身份确认及证书变更请求的处理
4.3	2021 年 9 月	修改初始身份确认、证书生命周期操作要求等
4.4	2021 年 12 月	增加撤销挂起的流程说明
4.5	2025 年 4 月	完善证书生命周期管理细则；简化法律责任和其他业务条款。

目录

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

1 概述

1.1 概要说明

证书策略（CertificationPolicy，以下简称 CP）是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

本《河北省电子认证有限公司证书策略》(以下简称：河北 CACP）本 CP 全部或者部分支持下列标准：

RFC3647：互联网 X.509 公钥基础设施-证书策略和证书业务声明框架

RFC5280：互联网 X.509 公钥基础设施证书和 CRL 属性

RFC2560：互联网 X.509 公钥基础设施-在线证书状态协议-OCSP

GB/T26855-2011：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

本 CP 适用范围为河北 CA 发放的数字证书。具体设定了证书策略、生命周期、使用、依赖和管理的角色、责任与要求，以及各相关主体的职责。为批准、签发、管理和使用证书和相关的可信服务制定业务，提供技术、策略和法律上的要求和规范

1.2 文档名称

本文档名称是“河北省电子认证有限公司证书策略（简称：河北 CA 证书策略或河北 CA CP)”。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

本文档所指电子认证服务机构为河北省电子认证有限公司（HebeiCertificateAuthorityCo.,Ltd.，简称河北 CA）是依法取得国家《电子认证服务许可证》《电子认证服务使用密码许可证》的第三方电子认证服务机构，负责数字证书的签发、管理和认证工作。

1.3.2 注册机构

注册机构是受理数字证书申请、更新、恢复和注销等业务的实体。

河北 CA 可以授权下属机构或委托外部机构作为注册机构，负责证书业务办理、身份鉴别与审核等服务。

河北 CA 授权外部机构作为注册机构，应与外部机构签署的合同中，明确双方的权利与义务，以及承担的法律责任。

1.3.3 订户

订户是指从电子认证服务机构接收证书的实体。在电子签名应用中，订户即为电子签名人。在本文档中订户也被称为用户。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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，电子签名依赖方是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。河北 CA 的证书体系中，依赖方是信任河北 CA 证书，可以对使用河北 CA 证书进行数字签名验证的实体，或者是使用河北 CA 证书公钥加密信息的实体。

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。

1.4 证书应用

1.4.1 适合的证书应用

河北 CA 签发的数字证书分为单位证书、个人证书和设备证书。具体如下：

“单位证书”是指颁发给组织机构的数字证书，用于信息活动中组织机构的身份认证和电子签名，以及数据加密等服务。

“个人证书”是指颁发给自然人的数字证书，用于信息活动中自然人、岗位角色的身份认证和电子签名，以及数据加密等服务。其中个人证书分为个人普通证书和个人事件证书。

“个人普通证书”是指个人长期持有的个人数字证书，一般有效期为 1 年。

“个人事件证书”一般用于一次性事件型电子签名，签名过后证书失效。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

“设备证书”是指颁发给设备（包含服务器）的数字证书，用于信息活动中标识设备的身份，实现设备身份认证以及数据的加解密，保证传输数据的完整性和安全性等。

1.4.2 限制的证书应用

河北 CA 颁发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，否则由此造成的法律后果由用户自行承担。

对于未经河北 CA 认可的证书应用软件，不适用河北 CA 的数字证书。

1.5 策略管理

1.5.1 策略文档管理机构

本 CP 的管理机构是河北 CACPS 策略管理小组。

1.5.2 联系人

本 CP 由河北 CACPS 策略管理小组负责编写、更新和维护。

网址：www.hebca.com

电话：400-707-3355

地址：石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层

邮编：050081

电子邮件：hebca@hebca.com

1.5.3 决定 CP 符合策略的机构

本 CPS 由河北 CA 安全策略委员会批准实行。

1.5.4 CP 批准程序

《河北 CACP》由河北 CA 安全策略委员会组织河北 CACPS 策略小组编写。CPS 策略小组完成编写 CP 草案后，由河北 CA 安全策略委员会和法律顾问对 CP 草案进行初步评审。初步评审后，将 CP 评审稿提交河北 CA 安全策略委员会审批。经河北 CA 安全策略委员会审批通过后，在河北 CA 网站上对外公布，并于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 CP：

- 公钥基础设施（PKI）PublicKeyInfrastructure

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。

- 证书策略（CP）CertificationPolicy

是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

- 电子认证业务规则（CPS）CertificationPracticeStatement

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、

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

吊销、更新证书或密钥）所遵循规范的详细描述和声明。

- 电子认证服务机构（CA）CertificationAuthority

是指受用户信任，负责创建和分配公钥证书的权威机构。

- 注册机构（RA）RegistrationAuthority

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。

- 电子签名认证证书（证书）DigitalCertificate

是指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。

- 证书吊销列表（CRL）CertificateRevocationList

是指经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。

- 私钥（电子签名制作数据）PrivateKey

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，亦可依据其运算方式，就相对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）PublicKey

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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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。

- LDAP（LightweightDirectoryAccessProtocol）

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 ITUX.500

- OCSP（OnlineCertificateStatusProtocol）

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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

2 信息发布与信息管理

2.1 认证信息的发布

本 CP 发布在河北 CA 的网站上（网址：http://www.hebca.com），供相关方下载、查阅。

河北 CA 通过网站（http://www.hebca.com）和目录服务器（LDAP）发布订户的证书、证书吊销列表（CRL），并提供 7X24 小时的证书状态服务，订户或依赖方可以通过访问河北 CA 的网站和目录服务器（LDAP）获取证书的信息和吊销证书列表（CRL）。同时，河北 CA 提供证书状态在线查询服务（OCSP）。

LDAP 发布地址：ldap.hebca.com 端口号：389

OCSP 发布地址：ocsp.hebca.com 端口号：3018

2.2 发布时间或频率

- 本 CP 按照§1.5.4CP 批准程序所描述的批准流程，一经发布到河北 CA 网站，即时生效。对河北 CA 数字证书订户及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，河北 CA 通过目录服务器（LDAP）自动将该证书公布。
- 河北 CA 采用实时或定期的方式发布吊销证书列表（CRL），通常在 24 小时内自动发布最新的 CRL。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

2.3 信息库访问控制

对于公开发布的 CPS、CA 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 CA/RA 管理人员可以查询河北 CA 和注册机构数据库中其他数据。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

3 身份标识和鉴别

3.1 命名

3.1.1 名称类型

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（DistinguishedName，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：

- 最后一项必须是 C=CN；
- 如果有 CN 项，需要放在 DN 的最前面；
- 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 对名称意义化的要求

订户的甄别名（DN）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，描述了与主体中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

在 CA 证书服务体系中，原则上订户不使用匿名或者为名。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

3.1.4 理解不同名称形式的规则

DN 的具体内容依次由 CN、OU、O、C 四部分组成。其中 CN 用来表示用户名，OU、O 用来表示组织单位名称、C 用来表示国家。

3.1.5 名称的唯一性

在 CA 的证书服务体系中，订户信息中 DN 唯一标识该订户。

3.1.6 商标的承认、鉴别和角色

河北 CA 签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

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 个人身份鉴别

对于个人订户，河北CA或授权注册机构应验证个人有效身份证件或证件的

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

具体信息，核实个人订户身份的真实性。个人有效身份证件指政府部门签发的证件，包括但不限于居民身份证、港澳台居民居住证、港澳居民来往内地通行证、台湾居民来往大陆通行证、外国人永久居留身份证、护照等。

个人身份的鉴别流程应当明确记录在按照本CP制定的CPS中。

3.2.3 组织机构身份鉴别

对于组织机构订户，河北 CA 或授权注册机构应验证订户提交的机构有效身份证件或证件的具体信息、机构授予经办人的授权证明和经办人的身份证明材料，核实机构订户是合法存在的实体及确认申请人的意愿。机构有效身份证件指政府部门签发的证件或文件，包括但不限于营业执照、事业单位法人证书、社会团体法人登记证书、民办非企业单位登记证书、统一社会信用代码证书等。

机构身份的鉴别流程应当明确记录在按照本 CP 制定的 CPS 中。

3.2.4 设备证书订户份的身鉴别

个人订户、机构订户如需申请设备证书，可以向河北 CA 或授权注册机构提交申请。河北 CA 或授权注册机构会根据申请的证书类型按照§3.2.2 和§3.2.3 对个人、组织机构申请者进行身份鉴别。

当域名等信息被作为证书主题内容申请证书时，还需要合理验证该申请者是否拥有该权利，例如要求提交域名所有权或使用权文件等。必要时，CA 机构可通过第三方确认域名所有者信息。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

3.2.5 没有验证的订户信息

订户提交鉴证文件不属于鉴别范围内的信息，为没有验证的订户信息。

3.2.6 授权确认

当申请者代表个人或机构申请证书时，需要出示足够的证明信息以证明个人或机构是否真实存在，申请者是否已获得个人或机构的授权。CA 机构或授权的注册机构有责任确认该授权信息，并将授权信息妥善保存。

3.2.7 互操作准则

互操作可能是交叉认证、单身交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的 CA 中心之间建立相互信任关系，从而使双方的订户可以实现互相认证。

河北 CA 可根据业务需要，在遵循本 CP 的各项控制要求的基础上，与河北 CA 证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示河北 CA 批准了或赋予了其他 CA 中心或电子认证服务机构以河北 CA 名义开展电子认证服务的权限。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

3.3 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

在常规密钥更新中，通过订户使用原有私钥对包含新公钥的密钥更新请求进行签名，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。河北 CA 或授权注册机构也可以使用初始身份验证相同的流程进行标识与鉴别。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后密钥更新等同于订户重新申请证书，其要求与§3.2 初始身份确认相同。

3.3.3 证书变更的标识与鉴别

证书变更是指订户的证书信息发生变化，申请进行证书信息变更。订户通过原有私钥对变更请求进行签名，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与鉴别。

河北 CA 或授权注册机构保留要求订户按照证书新办提交申请材料的权利。

3.4 吊销请求的标识与鉴别

吊销请求的标识与鉴别使用初始身份验证相同的流程，其要求与§3.2 初始身份确认相同。

如果是因为订户没有履行本 CP 和河北 CACPS 所规定的义务，由河北 CA 或

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

授权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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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 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，或具独立法人资格的组织机构(包括事业单位、企业单位、社会团体和人民团体等)。

4.1.2 申请过程与责任

证书申请人按照本 CP 和河北 CACPS 所规定的要求，通过现场面对面或在线方式提交证书申请，并准备相关的身份证明材料。河北 CA 或授权注册机构应明确告知证书用户所需承担的相关责任和义务，证书申请人表达申请证书的意愿后，河北 CA 或授权注册机构依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否受理申请。

订户：订户需要提供§3.2 初始身份确认所述的有效身份证明材料，并确保材料真实准确。配合河北 CA 或授权注册机构完成对身份信息的采集、记录和审核。

CA 机构：河北 CA 参照§3.2 初始身份确认的要求对订户的身份信息进行采集、记录，审核。通过鉴证后，河北 CA 向订户签发证书。如果用户身份信息的鉴别由授权的注册机构完成，河北 CA 应对授权的注册机构进行监督管理和审计。

注册机构：授权的注册机构参照§3.2 初始身份确认的要求对订户的身份进

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

行采集、记录和审核。通过鉴证后，注册机构向河北 CA 提交证书申请，由河北 CA 向订户签发证书。注册机构须接受河北 CA 的监督管理和审计。授权的注册机构应当按照河北 CA 的要求，向河北 CA 提交身份鉴证资料或自行妥善保存。

证书申请人应当提供真实、完整和准确的信息，河北 CA 或授权注册机构须按§3.2 初始身份确认的要求和流程对申请人身份材料信息进行审查。如证书申请人未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给河北 CA 或电子签名依赖方造成损失的，由证书申请人承担赔偿责任。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

证书申请人向注册机构提交初始的证书申请请求，注册机构须按照以下规定对订户的申领材料进行审查：

个人订户：参照 3.2.2 节的规定。

机构订户：参照 3.2.3 节的规定。

注册机构需要审查订户的证书申领表格是否按照要求填写、申领材料是否齐全、资质证明材料是否符合要求（如经办人是否在申请表上签字）。

4.2.2 证书申请批准和拒绝

河北 CA 或授权注册机构按照本 CP 所规定的身份鉴别流程对证书申请人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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

如果证书申请人通过身份鉴别流程且鉴证结果为合格，河北 CA 或授权注册机构将批准证书申请，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证，河北 CA 或授权注册机构拒绝申请人的证书申请，并通知申请人鉴证失败，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

河北 CA 或授权注册机构将作出合理努力来尽快确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在 1 个工作日内处理证书申请。

河北 CA 或授权注册机构能否在上述时间期限处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了河北 CA 或授权注册机构的管理要求。

4.3 证书签发

4.3.1 证书签发过程中电子认证服务机构的行为

河北 CA 在批准证书申请之后，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。

4.3.2 电子认证服务机构对订户的通告

河北 CA 通过注册机构对证书订户的通告有以下几种方式：

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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，来通知订户证书信息已经正确生成；

2. 邮政信函或短信通知订户；

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

证书签发完成后，河北 CA 或授权注册机构将数字证书及密码当面、寄送或电子方式给证书申请人。证书申请人从获得数字证书起，就被视为同意接受证书。

个人事件证书签发完成后，将证书应用于对应的电子签名时起，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

河北 CA 在签发完数字证书后，系统自动将证书发布到数据库或目录服务器中。河北 CA 采用主、从目录服务器结构来分布所签发的证书。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，供订户和电子签名依赖方查询和下载。

查询方式包括但不限于用户在线自助或人工受理等。查询申请用户需要提供必要的查询条件信息，包括但不限于序列号、证书主体信息、办理渠道、证书链有效期。对于订户查询，CA 机构核实身份后提供查询服务。对于其他实体查询，

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

为保护证书订户的数据安全和隐私保护，CA 机构只承诺对其他实体提交的证书进行核实。

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

河北 CA 不对其他实体进行通告，其他实体可以通过河北 CA 网站访问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。

证书订户接受数字证书，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 依赖方对公钥和证书的使用

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:

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

a) 用 CA 机构的证书验证证书中的签名，确认该证书是 CA 机构签发的，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) 检验证书有效性，需要检查该证书没有被吊销。

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。

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对方的加密证书，检查证书是否有效，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

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。

每张数字证书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。订户在证书有效期到期前，应按要求向河北 CA 或授权注册机构提出更新申请。

4.6.2 请求证书更新的实体

河北 CA 签发的个人、组织机构、设备等各类证书的证书持有人。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.6.3 证书更新请求的处理

订户可采取现场面对面或在线方式两种方式提交证书更新申请。

河北 CA 采取以下两种方式处理证书更新请求：

1. 在线证书更新请求处理：

申请人在证书过期前，通过河北 CA 网站提交证书更新申请，经过河北 CA 验证提交更新申请者拥有对应证书的私钥，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，完成证书更新。

申请人证书已过期的，需先按照§3.2 初始身份确认，对证书更新申请进行审核，审核批准后为订户制作新的证书。

2. 现场证书更新请求处理：

申请人在证书过期前，申请人到河北 CA 或授权注册机构申请证书更新，经过河北 CA 验证提交更新申请者拥有对应证书的私钥，河北 CA 或授权注册机构为用户现场完成证书更新。或者用户提交书面更新申请以及订户身份证明、设备证书请求文件及域名证明材料，如：域名所有权或使用权文件等。CA 机构或授权的注册机构根据本§3.2 初始身份确认，对证书更新申请进行审核，审核批准后为订户制作新的证书。

申请人证书已过期的，需先按照§3.2 初始身份确认，对证书更新申请进行审核，审核批准后为订户制作新的证书。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.6.4 证书更新时对订户的通告

同§4.3.2 电子认证服务机构对订户的通告。

4.6.5 构成接受更新证书的行为

同§4.4.1 构成接受证书的行为。

4.6.6 电子认证服务机构对更新证书的发布

同§4.4.2 电子认证服务机构对证书的发布。

4.6.7 电子认证服务机构在证书更新时对其他实体的通告

同§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。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书。

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. 订户证书密钥遭到损坏；
3. 订户证实或怀疑其证书密钥不安全；

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4. 河北 CA 的策略要求或相关法律法规引致的其它可能导致密钥更新的情形。

4.7.2 请求证书密钥更新的实体

同§4.6.2 请求证书更新的实体。

4.7.3 证书密钥更新请求的处理

组织机构和个人按照本 CP 所规定的要求，准备资料并向河北 CA 提出申请。具体的鉴别流程详见§3.2.3 组织机构身份鉴别和§3.2.2 个人身份鉴别。

用户身份审核通过，为订户进行证书密钥更新操作。

4.7.4 证书密钥对订户的通告

同§4.3.2 电子认证服务机构对订户的通告。

4.7.5 构成接受密钥更新证书的行为

同§4.4.1 构成接受证书的行为。

4.7.6 电子认证服务机构对密钥更新证书的发布

同§4.4.2 电子认证服务机构对证书的发布。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.7.7 电子认证服务机构在密钥更新时对其他实体的通告

同§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。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指在证书有效期内，订户的证书信息发生变化，申请重新签发一张证书，对原证书进行吊销处理。

4.8.2 请求证书变更的实体

同§4.6.2 请求证书更新的实体。

4.8.3 证书变更请求的处理

同§3.3.3 证书变更的标识与鉴别。

4.8.4 证书变更时对订户的通告

同§4.3.2 电子认证服务机构对订户的通告。

4.8.5 构成接受变更证书的行为

同§4.4.1 构成接受证书的行为。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.8.6 电子认证服务机构对变更证书的发布

同§4.4.2 电子认证服务机构对证书的发布。

4.8.7 电子认证服务机构在变更证书时对其他实体的通告

同§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。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

发生下列情况之一的，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本 CP 或河北 CACPS；
4. 认为当前密钥管理方式的安全性得不到保证。

发生下列情况之一的，河北 CA 可以强制吊销其所签发的数字证书：

1. 订户提供的信息不真实；
2. 订户没有履行双方合同规定的义务，或违反本 CP 或河北 CACPS；
3. 数字证书的安全性得不到保证；
4. 法律、行政法规规定的其他情形。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.9.2 请求证书吊销的实体

根据不同情况，订户、河北 CA 可以请求吊销最终用户证书。

4.9.3 吊销请求的流程

证书吊销请求的处理采用与初始证书签发相同的过程。

1. 证书吊销的申请人到河北 CA 或授权注册机构现场提交证书吊销申请，并说明吊销原因；

2. 河北 CA 根据§3.2 的要求对订户提交的吊销请求进行审核；

3. 河北 CA 吊销订户证书后，注册机构将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；

4. 强制吊销是指当河北 CA 或授权注册机构确认发生§4.9.1 强制吊销证书情形时，对订户证书进行强制吊销，吊销后将通过官网公告、注册机构告知或其他安全可行的方式通告订户。

4.9.4 吊销请求宽限期

如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。订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：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.9.5 电子认证服务机构处理吊销请求的时限

河北 CA 或授权注册机构在接到吊销请求后立即处理，24 小时生效。河北 CA 每日签发一次 CRL，并将最新的 CRL 发布到目录服务器指定的位置，供请求者查询下载。

4.9.6 依赖方检查证书吊销的要求

在具体应用中，依赖方可以使用以下两种方式之一进行所依赖证书的状态查询：

1. CRL 查询：利用证书中标识的 CRL 地址，通过目录服务器提供的查询系统，查并下载 CRL 到本地，进行证书状态的检验。

2. 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 CA 机构发布并且签名的。

4.9.7 CRL 发布频率

河北 CA 可采用定期的方式发布 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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.9.8 CRL 发布的最大滞后时间

CRL 发布的最大滞后时间为 24 小时。

4.9.9 证书挂起的情形

1. 订户证书丢失或订户怀疑证书的私钥安全可能已经受到损害；

2. 订户的身份可信度暂时出现问题或无法证明其身份可信度。

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 CA 或授权注册机构审核后进行挂起证书处理；被动挂起是指河北 CA 或授权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。

4.9.10 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。

4.9.11 挂起请求的流程

主动挂起：订户向河北 CA 或授权注册机构提交申请说明挂起原因，注册机构根据§3.2 初始身份确认的要求对订户身份及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 或授权注册机构确认订户的身份可信度暂时

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

出现问题或无法证明其身份可信度时，对订户证书进行强制挂起。

在证书挂起后，河北 CA 或授权注册机构将通过适当的方式，包括电话通知、网站公示等，通知订户证书已被挂起及被挂起的理由。

4.9.12 挂起的期限限制

订户证书一旦被挂起将处于挂起状态。直至：

1、订户向河北 CA 或授权注册机构申请取消证书挂起，取消证书挂起的订户身份鉴别过程同§3.2 初始身份确认；

2、河北 CA 或订户将挂起的证书吊销；

3、被挂起证书已到期。

4.10 证书状态服务

4.10.1 操作特征

证书的状态可以通过河北 CAD 提供的 OCSP 服务获得。

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。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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.10.3 可选特征

暂不提供可选特征证书状态查询服务。

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，该证书的服务时间结束。

订购结束包含以下两种情况：

- 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；
- 在证书有效期内，证书被吊销后，即订购结束。

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

证书订户的签名密钥对在订户持有或指定的证书载体中产生，证书载体包括但不限于智能密码钥匙、密码设备、密码模块。加密密钥对由密钥管理中心生成。

个人事件证书的签名密钥由签名设备生成密钥。个人事件证书的加密密钥对由密钥管理中心生成。

密钥恢复是指订户加密密钥对的恢复，密钥管理中心不负责签名密钥对的恢复。密钥恢复分为两类：用户密钥恢复和司法密钥恢复。

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 或授权注册机构申请，经审核后，通

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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：司法取证人员向河北 CA 申请，经审核后，河北 CA 向 KMC 发出密钥恢复请求，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 会话密钥的封装及恢复的策略与行为

采用非对称算法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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5 认证机构设施、管理和操作控制

本章规定参见河北 CACPS。

6 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

CA 系统和 RA 系统的密钥对是在密码机内部产生，密码机应具有商用密码产品认证证书。在生成 CA 密钥对时，河北 CA 按照密码机密钥管理制度，执行详细的操作流程控制计划，选定并授权 5 个密钥管理员，采取五选三方式，密钥管理员凭借智能密码钥匙对密钥进行控制。

证书订户的签名密钥对在订户持有或指定的证书载体中产生，证书载体包括但不限于智能密码钥匙、密码设备、密码模块。加密密钥对由密钥管理中心生成。

个人事件证书的签名密钥对由签名设备生成，加密密钥对由密钥管理中心生成。

6.1.2 私钥传送给订户

证书的签名密钥对由订户自己的密码设备生成并保管。加密密钥对由密钥管理中心产生，通过安全通道传到订户手中的密码设备中。

个人事件证书的签名密钥对由签名设备生成并保管。加密密钥对由密钥管理

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

中心产生，通过安全通道传递给证书申请方。

6.1.3 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，经注册机构传送到河北 CA。

从 RA 到 CA 以及从密码管理中心到 CA 的传递过程中，采用国家密码主管部门许可的通讯协议及密钥算法，保证了传输中数据的安全。

6.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从河北 CA 的网站 http://www.hebca.com 下载国家 CA 根证书和 CA 证书，从而获得河北 CA 的公钥。

6.1.5 密钥的长度

密钥算法和长度符合国家密码管理部门的规定。

6.1.6 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设备生成，符合国家的质量检查标准。

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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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

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：

- 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。

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，即采取五选三方式，将私钥的管理权限分散到 5 张管理员卡中，只有其中超过半数以上管理员在场并许可的情况下，才能对私钥进行上述操作。

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

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

由自己保管或控制，密码管理中心不负责托管签名私钥。

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。

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 私钥导入、导出密码模块

CA 私钥在硬件密码模块中产生。在需要备份或迁移 CA 私钥时，从密码块中导出的私钥必须由多人控制。

在订户使用数字证书时，私钥无法从密码设备中导出。必须通过密码验证之后，才可以使用存储在密码模块中的私钥进行加解密操作。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

6.2.7 私钥在密码模块的存储

CA 系统采用国家密码管理部门认可的密码设备，这些设备内置的协议、算法等均符合国家密码行业的标准要求。

订户私钥在密码设备或密码模块中加密保存。

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，需要超过半数以上的管理员同时在场。

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，需要超过半数以上的管理员同时在场。

6.2.10 销毁私钥的方法

河北 CA 在进行用户密钥销毁时，需要具有销毁私钥权限的工作人员通过身份认证后方可进行销毁私钥的操作，需要超过半数以上的管理员同时在场。密钥销毁操作完成后，还需要对数据库中密钥的备份进行销毁。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

6.2.11 密码模块的评估

河北 CA 使用通过国家密码管理局鉴定的服务器加密机，符合国家相关标准。

6.3 密钥对管理的其他方面

6.3.1 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，由河北 CA 和密钥管理中心定期归档。

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

激活数据是私钥保护密码，证书存储介质（如：智能 USBKey）出厂时设置了初始的 PIN 值，证书制作时将此 PIN 值根据应用情况，部分更改为系统随机产生的密码。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

6.4.2 激活数据的保护

证书存储介质的 PIN 值根据证书签发情况，部分由系统随机产生并发送至证书申请时经办人或法人预留的手机号。仍使用初始密码的，河北 CA 通过证书助手软件提示、使用注意事项等多种方式提示用户进行 PIN 值修改。

用户需要对激活数据进行妥善保护，不可泄露给其他人。如果发生激活数据丢失而造成私钥被盗用所进行的操作，将视同订户本人使用私钥进行操作。

6.4.3 激活数据的其他方面

激活数据在使用中可以修改，以提高其安全性。

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 部署了入侵防御和漏洞扫描系统，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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

6.5.2 计算机安全评估

河北 CA 使用通过国家密码管理局批准生产的密码设备，系统建设方案经国家密码管理局的审核，河北 CA 数字证书认证系统和密钥管理系统通过了国家密码管理局的安全性审查，完全符合国家相关安全性规范要求。

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 对系统的维护、配置修改和升级都进行详细的记录，通过日志来检查系统和数据的完整性及软硬件的工作情况。

6.6.3 生命期的安全控制

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，

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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、入侵防御、漏洞扫描、数据备份、灾难恢复等安全控制措施。

6.8 时间戳

数字时间戳（DTS：DigitalTimeStamp）是对时间信息的电子签名，主要用于实现确定在某一时间某个文件确实存在和确定多个文件在时间上的逻辑关系功能。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

7 证书、证书吊销列表及在线证书状态协议

7.1 证书

河北 CA 签发的证书符合 X.509V3 证书格式。

7.1.1 版本号

X.509V3。

7.1.2 证书标准项

- 证书序列号

唯一标识该证书的一组字符。

- 证书有效期

证书的有效期根据协议规定定义。

- 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§3.1 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：

CN=HBSM2CA
OU=hebca
O=hebca
L=shijiazhuang

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

S=hebei

C=CN

7.1.3 证书扩展项

- 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。

- 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。

- 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。

- 基本限制：

  用于鉴别证书持有实体身份，如终端用户等。

- 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 SM2 算法的数字证书，使用 SM3WithSM2Encryption 算法。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

7.1.5 名称形式

河北 CA 数字证书中的主题 Subject 的 X.500DN 是订户的唯一标识。

7.2 证书吊销列表 CRL

河北 CA 定期签发证书吊销列表（CRL），其所签发的 CRL 遵循 RFC3280 标准，采用 X.509V2 格式。

7.2.1 CRL 版本号

X.509V2。

7.2.2 CRL 和 CRL 条目扩展项

CRL 扩展项：颁发机构密钥标识符 AuthorityKeyIdentifier。

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：

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

- CRL 发布

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
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 SM2 算法的 CRL，使用 SM3WithSM2Encryption 算法。

7.3 在线证书状态协议（OCSP）

7.3.1 版本号

使用 OCSP 版本 1（OCSPV1）。

7.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

8 认证机构审计和其他评估

8.1 评估的频率或情形

1、根据《中华人民共和国电子签名法》、《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。

2、根据国家相关要求和本 CP 和河北 CACPS 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 或授权注册机构和其他关联服务机构的审计评估。

8.2 评估者的资质

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，熟悉本 CPS，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。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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。

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措施

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，

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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 运营安全管理小组可以查阅。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。

9 法律责任和其他业务条款

本章规定参见河北 CACPS。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com