河北省电子认证有限公司

电子认证业务规则

版本 **4.4**

河北省电子认证有限公司

2021 年 **12** 月

版权声明

《河北省电子认证有限公司电子认证业务规则》受到完全的版权保护，本文件中所涉及的“河北CA”、“河北CA电子认证业务规则”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

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

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

1.1.1 电子认证业务规则

电子认证业务规则（Certification Practice Statement，简称 CPS）是关于认证机构（CA，Certification Authority）在全部证书服务生命周期中的业务实践（如签发、管理、更新证书或密钥）所遵循规范的详细描述和声明。

本文档的编写遵从《中华人民共和国电子签名法》《电子认证服务管理办法》等法律、法规。

为了规范证书业务的正常开展，河北省电子认证有限公司发布了《河北省电子认证有限公司电子认证业务规则》。

1.1.2 证书类别

目前河北 CA 提供“个人证书”、“单位证书”、“设备（服务器）证书”三类证书。其中：

“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、岗位角色的身份证明。

“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证明。

“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。

以上三类证书，是根据§3.2 初始身份确认的规定，经过河北 CA 注册机构鉴证的实体所拥有的数字证书。在满足《中华人民共和国电子签名法》及其他相关规定下，由其所产生的电子签名符合《中华人民共和国电子签名法》的要求。

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

1.2 文档名称

本文档名称是“河北省电子认证有限公司电子认证业务规则（简称：河北CA电子认证业务规则或河北CA CPS）”。

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（Hebei Certificate Authority Co., Ltd.，简称河北CA）是河北省唯一一家依法取得国家《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。

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

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

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

证书类型	订户性质	用途
个人证书	社会自然人，政府、企业、事业等机构所属人员	用于区分、标识、鉴别个人身份的场景，适用于个人身份认证和电子签名，以及数据加密等服务。
单位证书	政府、企业、事业等机构	用于需要区分、标识、鉴别机构身份的场景，适用于机构身份认证和电子签名，以及数据加密等服务。
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	用于标识各种设备身份，实现设备身份认证以及交互数据的加解密，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。

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

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的管理机构是河北 CA CPS 策略管理小组。

1.5.2 联系人

本 CPS 由河北 CA CPS 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 CPS 符合策略的机构

本 CPS 由河北 CA 安全策略委员会组织制定，报河北 CA 安全策略委员会批准实行。

1.5.4 CPS 批准程序

《河北 CA 电子认证业务规则》由河北 CA 安全策略委员会组织河北 CA CPS 策略小组编写。CPS 策略小组完成编写 CPS 草案后，由河北 CA 安全策略委员会和法律顾问对 CPS 草案进行初步评审。初步评审后，将 CPS 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 CPS：

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。

- 电子认证业务规则（CPS）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。

- 电子认证服务机构（CA）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。

- 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。

- 电子签名认证证书（证书）Digital Certificate

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）Certificate Revocation List

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）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）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。

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

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（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

- OCSP（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。

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 CPS 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 CPS 按照§1.5.4CPS 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。

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（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：

- 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。

个人证书的甄别名通常可包含个人的真实名称或者证件号码，作为标识订户的关键信息被认证。

机构证书的甄别名通常包含机构名称或者机构的证件号码，作为标识订户的关键信息被认证。

设备证书的甄别名通常包含订户所拥有的域名或者外网 IP，结合订户的其他信息一起被鉴别和认证。

3.1.3 订户的匿名或伪名

在CA证书服务体系中，除在特定场景外，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 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。

3.1.5 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注册机构将验证个人的身份证或证件的具体信息，核实个人订户身份的真实性。

鉴别方式可以采用面对面现场鉴别或远程鉴别。必要时，可以通过权威第三方数据库信息比对、手机短信验证码等其他可靠的方式鉴别。

鉴别审核批准后，河北CA注册机构按照法律法规的要求妥善保存订户申请材料，CA机构保存订户申请材料可以是纸质或电子数据形式。

本CPS简要说明了如何进行个人身份鉴别。河北省电子认证有限公司保留根据最新国家政策法规的要求更新个人身份鉴别方法与流程的权利。

3.2.3 组织机构身份鉴别

对于组织机构订户，河北 CA 注册机构需要鉴别：

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

（1）订户提交的组织身份信息。鉴别方法包括核对提交的组织有效身份证件或证件的具体信息。必要时可通过权威第三方数据库对身份证件信息进行比对。组织有效的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、组织机构代码证、事业单位登记证、社会团体登记证、政府批文等。

（2）组织授权经办人的授权证明。鉴别方法包括但不限于检查组织或组织的法定代表人授权给经办人办理证书事宜的授权文件或授权条款，也可以通过银行对公打款或法人代表手机短信验证方式核实。

（3）经办人的个人身份信息。按照§3.2.2 个人身份鉴别进行鉴别。

（4）如该组织需申请服务器类型的证书，需域名使用权证明材料。例如要求提供域名所有权文件、归属权证明文件或者申请者对所有权的书面承诺等。

鉴别方式可以采用面对面现场鉴别或远程鉴别。当河北 CA 注册机构认为有需要时，可以增加其他方式，包括但不限于鉴别组织机构的法定代表人身份或要求经办人提交法定代表人的有效身份证件证明。

鉴别审核批准后，河北 CA 和注册机构按照相关法律法规的要求妥善保存订户申请材料，河北 CA 保存订户申请材料可以是纸质或电子数据形式。

本 CPS 简要说明了如何进行组织机构身份鉴别。河北省电子认证有限公司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方法与流程的权利。

3.2.4 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。

3.2.5 授权确认

个人申请数字证书，需本人办理。

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 CA 数字证书事宜的授权文件。组织在 CA 机构的数字证书申请表上加盖单位公章或采用其他安全有效方式体现申请机构真实意愿的方式，则证明本组织对办理人的授权确认。

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

3.2.6 互操作准则

互操作可能是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 CPS 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。

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。

3.3.2 吊销后密钥更新的标识与鉴别

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更，申请重新签发一张证书，对原证书进行吊销处理。证书变更的标书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。

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

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

身份确认相同。

如果是因为订户没有履行本 CPS 所规定的义务，由河北 CA 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 CPS 所规定的要求，通过现场面对面或在线方式提交证书申请，包括相关的身份证明材料。河北 CA 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 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 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。

注册机构：注册机构参照§3.2 初始身份确认的要求对订户的身份进行采集、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。

证书申请人应当提供真实、完整和准确的信息，河北 CA 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。

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

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

河北 CA 注册机构按照本 CPS 所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见§3.2.初始身份确认。

4.2.2 证书申请批准和拒绝

河北 CA 注册机构按照本 CPS 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。

如果证书申请人通过本 CPS 所规定的身份鉴别流程且鉴证结果为合格，河北 CA 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 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。

在必要时 CA 机构有权复核注册机构提交的订户申请材料，并有权拒绝不符合本 CPS 的高风险申请。

4.2.3 处理证书申请的时间

河北 CA 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 3 个工作日内处理证书申请。

河北 CA 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 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

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

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：

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

河北 CA 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。证书申请人收到 CA 证书后，需及时核对证书中的信息，如无异议视为接受数字证书。

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和目录服务器中。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。

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。

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

4.5 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

当依赖方接收到数字签名的信息后应该：

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依赖方信任的证书；
3. 检查证书是否有效；
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信息。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

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。

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

订户在证书有效期到期前，应按要求向河北 CA 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。

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。订户证书已过期的，需先按照§3.2.2 个人身份鉴别和§3.2.3 组织机构身份鉴别重新对用户身份进行鉴别，再进行证书更新。

2. 现场证书更新请求处理：

申请人到河北 CA 注册机构提交证书更新申请，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 注册机构为用户现场完成证书更新。订户证书已过期的，需先按照§3.2.2 个人身份鉴别和§3.2.3 组织机构身份鉴别重新对用户身份进行鉴别，再进行证书更新。

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。

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

4.6.6 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；
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

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 CPS 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。

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

4.7.4 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。

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

证书变更是指订户的证书信息发生变更，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。

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

4.8.4 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。

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 CPS；
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 CPS；
3. 数字证书的安全性得不到保证；

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. 法律、行政法规规定的其他情形。

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 注册机构提交证书吊销申请，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；

4. 强制吊销是指当河北 CA 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或其他安全可行的方式通告订户。

河北 CA 注册机构共同约定标识证书吊销请求流程，由河北 CA 注册机构负责对外公布。

4.9.4 吊销请求宽限期

当最终订户发现密钥泄漏等不安全事件时，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。

4.9.5 电子认证服务机构处理吊销请求的时限

河北 CA 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。

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

4.9.6 依赖方检查证书吊销的要求

在具体应用中，依赖方必须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。

4.9.8 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 注册机构审核后进行挂起证书处理；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。

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

4.9.10 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 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 注册机构确认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时，对订户证书进行强制挂起。

在证书挂起后，河北 CA 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 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

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。

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

4.10.2 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

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

订户的签名密钥对由订户的密码模块（如智能 USB KEY）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模块保管。

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 注册机构或网上进行申请，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

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

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

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 50174－93）
- 《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（GBJ45-1982）

2. 河北 CA 的系统机房设立在石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 28 层，系统机房实行分层访问的安全管理。

5.1.2 物理访问

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。

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. 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五年。
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。

5.1.4 水患防治

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。

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

5.1.6 介质存储

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 保存的相关数据已不再需要或归档期限已满时，应当采取措施销毁。纸张文件必须粉碎或烧毁，磁盘等存储介质在作废处置前应多次重写覆盖磁盘的存储区域，确定不可恢复并进行物理销毁。

5.1.8 数据备份

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。

数据备份严格按照既定的备份策略，通过预定义备份脚本对所有系统服务和数据库进行备份，并对备份数据的完整性、有效性进行恢复测试。

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

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

5.2.2 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身份鉴别和证书签发至少两个可信角色来完成。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，共同完成对电子认证系统的管理。

5.3 人员控制

5.3.1 资格、经历和无过失要求

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

5.3.2 背景审查程序

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 工作岗位轮换周期和顺序

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。

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，构成犯罪的，移交司法机关处理。

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

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。

5.4 审计日志程序

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、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 处理日志的周期

河北 CA 定期对日志进行审查。按照日志的不同类型，河北 CA 以每周、每月、每季度为周期对日志进行审查，并将审查内容和结果备案。在报警或异常事件发生后也要处理日志。

5.4.3 审计日志的保存期限

纸质审计日志处理和归档之后将至少保存五年。

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

5.4.4 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。

5.4.5 审计日志备份程序

对于河北 CA 认证系统的审计日志，河北 CA 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 对导致事件实体的通告

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

河北 CA 每年对系统进行脆弱性评估，以降低系统运行的风险。

5.5 记录归档

5.5.1 归档记录的类型

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

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 归档记录的保存期限

根据归档记录的不同类型和需要，保存期限为不少于五年。

用户纸质档案保存期限为电子签名认证证书失效后五年，用户电子档案保存期限为永久保存。

5.5.3 归档文件的保护

河北 CA 对各种电子、磁带、纸质形式的归档文件，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

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。

5.5.5 记录时间戳要求

所有记录都要有存档时具体准确的时间标识以表明存档时间。

5.5.6 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 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 CA 根证书到期和电子认证服务机构证书到期时，需要更换密钥采取的措施。

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. 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信任。

2. 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 CA 证书到期前的 60 天内停止签发新的下级证书（“停止签发日期”）；
- 产生新的密钥对，签发新的 CA 证书；
- 在“停止签发日期”之后，河北 CA 将采用新的 CA 密钥签发下级证书。

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 将继续使用旧的私有密钥签发的 CRL，直到旧的私钥签发的最后证书到期为止。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

发生故障时，河北 CA 将按照灾难恢复计划实施恢复。

5.7.2 计算资源、软件和/或数据的损坏

当计算资源、软件和/或数据受到破坏后，河北 CA 进行以下操作：

- 恢复环境，启动备份系统和备份数据并上线；
- 为用户恢复证书，重新进行认证；
- 尽快恢复原系统。

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

5.7.3 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，并按照本 CPS 中规定的程序进行吊销。详见§4.8 证书吊销和挂起。
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。详见§4.8 证书吊销和挂起。
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§4.7 证书密钥更新。

5.7.4 灾难后的业务连续性能力

河北 CA 采取了多种技术手段（例如数据热备、磁盘阵列、系统备机等），保证灾难后业务连续性，出现灾难后能够在最短的时间内恢复其业务能力。

5.8 电子认证服务机构或注册机构的终止

河北 CA 终止运营时，将严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》及其他相关法律规定的步骤终止运营。

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 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

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（KMC）生成。

6.1.2 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 USB KEY）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 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 上下载国家 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

河北 CA 支持 SM2 算法。订户用于加密和签名的 SM2 密钥对长度支持 256

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

位。

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。

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，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。

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

6.2.3 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。

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

在河北 CA 证书服务体系中，河北 CA 使用专用软件把私钥导入密码模块。

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。

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。

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

6.2.8 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 销毁私钥的方法

河北 CA 在进行用户密钥销毁时，需要多个具有销毁私钥权限的工作人员通过身份认证后方可进行。密钥销毁操作完成后，对数据库中密钥的备份进行销毁。

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

公钥属于安全数据，由河北省密钥管理中心定期归档、管理。

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。

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 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 USB Key）出厂时设置了初始的 PIN 值，证书制作时将此 PIN 值更改为系统随机产生的密码。

6.4.2 激活数据的保护

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的操作。

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。

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。

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

6.6 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，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：Digital Time Stamp）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.509 V3 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

S =hebei

C = CN

7.1.3 证书扩展项

- 颁发机构密钥标识符：

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

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。

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 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.509 V2 格式。

7.2.1 CRL 版本号

X.509 V2。

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。

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

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

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（OCSP V1）。

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 CPS 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 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。

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

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

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，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。

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

9 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

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 证书的吊销或状态信息的查询费用

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服务费用。

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

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。

9.3.2 不属于保密的信息

- 与证书申请有关的信息不属于保密信息。
- 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。
- 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,

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

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 隐私保密方案

除非证书申请人主动提供，河北 CA 保证不会截取任何证书申请人的隐私资料。

河北 CA 应保护证书申请人所提供的身份证明资料。河北 CA 采取必要的安全措施防止证书申请人资料的遗失、盗用或篡改。

9.4.2 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。

9.4.3 不被视为隐私的信息

与订户证书相关的信息不被视为隐私信息，可以通过河北 CA 目录服务等方式向外公布。

9.4.4 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。

9.4.5 使用隐私信息的告知与同意

使用隐私信息，须获得本人同意。

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

9.4.6 依法律或行政程序的信息披露

当河北 CA 需要依法律或行政程序披露信息时，河北 CA 提供的相关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。

9.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定。

9.5 知识产权

9.5.1 河北 CA 自身拥有知识产权的声明

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。

9.5.2 河北 CA 使用其他方知识产权的声明

河北 CA 在认证业务系统中购置和使用的其它方软硬件产品、辅助设备和相关操作手册，其知识产权归产品供应商或开发商所有。

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

9.6 陈述与担保

9.6.1 电子认证服务机构的陈诉与担保

河北 CA 在提供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本 CPS 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 注册机构的陈述与担保

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本 CPS 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. 注册机构按本 CPS 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。

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

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. 订户了解本 CPS 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，应立即通知河北 CA 或注册机构吊销证书。

9.6.4 依赖方的陈述与担保

依赖方了解本 CPS 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本 CPS 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。

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

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。

9.7 担保免责

下列情况之一的，河北 CA 不承担任何责任。

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 承担信托或担保责任。
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 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。

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

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 §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、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。

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

9.10 有效期限与终止

9.10.1 有效期限

《河北 CA 电子认证业务规则》自发布之日起正式生效。

《河北 CA 电子认证业务规则》中详细注明版本号及发布日期。

9.10.2 终止

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

当河北 CA 终止业务时，《河北 CA 电子认证业务规则》自动终止。

当证书到期或吊销后，订户协议即终止。

9.10.3 效力的终止与保留

《河北 CA 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等条款。

9.11 对参与者个别通告与沟通

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。

9.12 修订

9.12.1 修订程序

当《河北 CA 电子认证业务规则》不适用时，由河北 CA CPS 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 法律顾问共同研究审议。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 电子认证业务规则》，并于三十日内向工业和信息化部备案。

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

9.12.2 通知机制与期限

河北 CA 将修订的《河北 CA 电子认证业务规则》通过河北 CA 网址发布，其地址为：http://www.hebca.com。在认为有必要时，河北 CA 将通过电子邮件、信件、媒体等方式通知有关各方。

9.12.3 必须修改业务规则的情形

当相关法律、适用标准及操作规范等有重大改变时，必须修改《河北 CA 电子认证业务规则》。

9.13 争议处理

证书订户、依赖方等实体在电子认证活动中产生争议按照以下方面处理：

1、争议内容的限定：

只限于涉及《河北 CA 电子认证业务规则》任一方面或涉及由河北 CA 签发数字证书方面的争议。

2、争议解决的通知：

当争议发生时，在采取任何解决途径之前，订户应首先通知河北 CA 及其他当事人。

3、争议解决流程：

1) 当事人首先通知河北 CA，并根据《河北 CA 电子认证业务规则》中的规定，明确责任方。
2) 由河北 CA 相关部门负责与当事人协调解决。
3) 协商不成，当事人可通过仲裁或司法程序处理。
4) 任何因与河北 CA 就本《电子认证业务规则》所产生的任何争议而提起诉讼的，受河北 CA 住所地的人民法院管辖。

9.14 管辖法律

《河北 CA 电子认证业务规则》在各方面适用中华人民共和国法律、法规的

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

管辖和解释，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。

9.15 与适用法律的符合性

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

9.16 一般条款

9.16.1 完整协议

《河北 CA 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。

9.16.2 转让

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

当人民法院或其他仲裁机构认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

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

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

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，也可以是战争、罢工、骚乱等社会异常事件或其它社会现象。

在数字证书认证活动中，河北 CA 由于不可抗力因素而暂停或终止全部或部分证书服务的，河北 CA 不承担违约责任。其他认证各方（如订户）不得提出异议或申请任何补偿。

9.17 其他条款

河北 CA 对《河北省电子认证有限公司电子认证业务规则》拥有最终解释权。

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