材料八

中汽数据(天津)有限公司
电子认证业务规则
（CPS）

版本 V1.1

中汽数据(天津)有限公司

2021 年 7 月

版本控制

版本	生效日期	发布者
V1.0	**2021.5.30**	**中汽数据CA安全策略委员会**
V1.1	**2021.7.15**	**中汽数据CA安全策略委员会**

目 录

1 概括性描述

1.1 中汽数据 CA

中汽数据（天津）有限公司成立于 2017 年，是中汽数据有限公司的全资子公司，隶属于中国汽车技术研究中心有限公司（简称“中汽中心”），又名中汽中心数据资源中心。公司以汽车大数据为基础，汽车领域模型算法为支柱，深入开展节能低碳、绿色生态、市场研究等工作。面向“新基建”、“新四化”发展，在中国汽车工业云、智能网联、智能座舱、工业互联网（工业软件）等领域精准发力，通过中国汽车产业数据基础设施建设及国家级汽车产业数据体系构建，以“‘数’驱产业变革，‘智’领汽车未来”为使命，致力于打造“国家级汽车产业数据中心、国家级汽车产业链决策支撑机构、国家级泛汽车产业数字化支撑机构”。

中汽数据(天津)有限公司电子认证服务机构（简称中汽数据 CA），面向车联网提供电子认证服务，是车联网信息安全的重要基础设施，具备提供符合《中华人民共和国电子签名法》规定的数字证书和电子认证服务的能力。

作为国内专注于智能汽车行业电子认证服务的运营商，中汽数据 CA 依靠先进而实用的技术和优质的服务，为广大的、对通信和信息安全方面有各种各样需求的公众用户提供数字证书认证服务。

1.2 CPS 概述

本规则是由中汽数据 CA 根据《中华人民共和国电子签名法》《电子认证服务管理办法》以及《电子认证业务规则规范（试行）》编写，阐述在证书签发、管理、吊销以及更新等认证服务过程中的业务规则以及各参与方的责任。本规则适用于参与中汽数据 CA 认证服务的本公司的工作人员、注册机构、证书订户以及依赖方。

1.3 文档名称与标识

本文档称为《中汽数据(天津)有限公司电子认证业务规则》（简称中汽数据 CA CPS），

该文档没有分配对象标识符。

1.4 电子认证活动参与者

1.4.1 电子认证服务机构

电子认证服务机构（简称 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》的规定，依法设立的可信的第三方电子认证服务机构。

1.4.2 注册机构

注册机构（下文简称 RA）是经过 CA 正式授权管理的业务分支机构，包括证书注册审核（RA）中心，证书服务受理点（LRA）等。

1.4.3 订户

证书订户，即最终证书持有者。订户包括持有电子认证服务机构发放的证书的个人、单位、企业、组织、硬件设备、网站等参与认证服务的各种实体。当最终证书持有者为设备或证书申请属于特殊情况时，订户则指替代最终证书持有者申请及领用证书的人或实体。

1.4.4 依赖方

使用或信任电子认证服务机构所签发的证书进行交易的证书订户以及依照本业务规则在某些应用中信任证书真实性的所有实体被称为电子认证服务机构的依赖方。依赖方可以是证书订户也可以不是证书订户。

1.5 证书应用

1.5.1 适合的证书应用

中汽数据 CA 签发的订户证书适用于车联网、工业互联网、物联网、企业信息化等领域，以实现以下安全需求：

1. 身份认证：为证书订户身份的确认提供安全保证。

2. 保密传输：为信息的传输和交换提供安全保障。
3. 数字签名及验证：为依赖方进行网上行为的不可抵赖性提供依据。
4. 验证信息完整性：可以验证信息在传递过程中是否被篡改，发送方和接收方的信息是否完整一致。

目前中汽数据 CA 发放的证书包括：个人证书、机构证书、设备证书，证书申请人根据实际需求决定使用哪类证书。

- 个人证书：用于标识鉴别个人身份，适用于个人身份认证，电子签名，数据加解密等服务。
- 机构证书：主要应用标识鉴别机构的身份，适用于电子政务、机构信息服务平台以及电子商务平台等用于机构身份认证、电子签名和数据加解密等服务。
- 设备证书：包括各种服务器证书、设备证书和域名证书，用于标识鉴别各种设备身份，实现设备身份认证、数据加解密，保证传输数据完整性和安全性。

1.5.2 限制的证书应用

各类证书的订户都只能应用于证书订户主体身份合适的应用。如果参与方不遵守相关约定超出本 CPS 限定应用范围，将不受中汽数据 CA 的保护。

证书密钥的应用范围在订户证书的扩展项中进行了限制。基于证书扩展项限制判断证书有效性取决于应用软件。任何未经中汽数据 CA 认可的证书应用都将不受中汽数据 CA 的保护。

中汽数据 CA 发放的数字证书禁止在违反国家法律，法规或破坏国家安全情况下使用，由此造成的法律后果由订户负责。

1.6 策略管理

1.6.1 策略文档管理机构

中汽数据 CA 安全策略委员会是《中汽数据(天津)有限公司电子认证业务规则》（CPS）的最高管理机构，负责制定、维护和解释本 CPS。当需要编写或修订本 CPS 时，由中汽数据 CA 策略委会组织相关人员编写，并指定编写负责人。

1.6.2 联系方式

中汽数据 CA 的安全策略委员会为本 CPS 的联系人，负责本 CPS 的对外沟通及其他相关事宜，任何有关本 CPS 的问题、建议和疑问都可以与安全策略委员会取得联系，具体联系方式如下：

公司地址：天津市西青区中北镇万卉路 3 号新城市中心 B 座

邮　　编：300393

办公电话：022-60633100-8180

公司网址：www.catarc.info

电子邮箱地址：zqsjca@catarc.ac.cn

1.6.3 决定 CPS 符合策略的机构

中汽数据 CA 安全策略委员会负责审核批准 CPS，并作为 CPS 实施检查监督的最高决定机构。

1.6.4 CPS 批准程序

中汽数据 CA 的 CPS 由中汽数据 CA 安全策略委员会组织人员，按照信息产业部的相关规定编写。所有中汽数据 CA 的 CPS 的更新版本必须经过以下审批程序：

1. 中汽数据 CA 安全策略委员向中汽数据 CA 全体人员广泛征集 CPS 的修改建议并进行梳理汇集；

2. 中汽数据 CA 安全策略委员会组织专人修改 CPS；

3. 中汽数据 CA 安全策略委员会对修改后的 CPS 进行审议；

4. 中汽数据 CA 安全策略委员对 CPS 审议通过后，中汽数据 CA 将会根据《电子签名法》《电子认证服务管理办法》等行业法规的要求发布 CPS 最新版本并向信息产业部备案。

1.7 定义和缩写

缩写表

字母缩写	术　　语
CA	电子认证服务机构
CP	认证策略
CPS	认证业务规则
CRL	证书吊销列表
DN	证书甄别名
ICP	网络内容服务商
LDAP	轻量级目录访问协议
OCSP	在线证书状态协议
PIN	个人身份识别码
PKCS	公钥加密标准
PKI	公钥基础设施
RA	注册机构
RFC	意见申请

术语表

名称	术　　语
安全策略委员会	中汽数据 CA 认证服务体系内的最高策略管理监督机构和 CPS 一致性决定机构
电子认证服务机构	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	面向订户证书，负责订户证书申请审批和管理工作
数字证书	经 CA 数字证书签名包含数字证书使用者身份公开信息和公开密钥的电子文件
证书吊销列表	一个经电子认证服务机构数字签名的列表，标记了已经被吊销的公钥证书列表，表示这些证书无效
订户	被签发证书的自然人或者法律实体，且受订户协议或使用条款约束的自然人或法律实体
订户协议	认证服务机构与证书订户之间的协议，规定了各方的权力与责任
公钥	非对称密码算法中可以公开的密钥
私钥	非对称密码算法中只能由拥有者使用不公开的密钥
依赖方	依赖于证书所证明的基础信任关系并依此进行业务活动的个人或机构

2 信息发布与信息管理

2.1 信息的发布

中汽数据 CA 将通过在线方式向订户及证书应用的依赖方提供信息服务。中汽数据

CA 信息服务包含但不限于以下内容：CPS 现行版本，证书 CRL、订户协议、以及其他由中汽数据 CA 在必要时发布的信息，这些信息将严格遵守本 CPS，并符合国家和主管部门颁布的有关法律法规，这些信息将通过中汽数据 CA 网站对外发布。

2.2 发布时间和频率

中汽数据 CA 将在成功签发证书的同时在目录服务器上发布证书相关信息（不包含任何交易数据，数据信息以数据库方式存放），在证书冻结或吊销后不超过 24 小时发布证书吊销列表（CRL）。

除非另有规定，中汽数据 CA 将至少每 24 小时发布一次各类证书的吊销列表（CRL）。在紧急情况下，中汽数据 CA 可自行决定缩短公布证书吊销列表的时间。

网站的公告、中汽数据 CA 的 CPS、证书应用情况、协议流程等信息不定期进行更新，无固定的发布时间或频率。

2.3 信息访问控制

对于公开发布的 CP、CPS 和 CA 证书等公开信息，本 CA 机构允许公众自行通过网站进行查询和访问。只有经授权的 RA/CA 管理员可以查询 CA 机构和注册机构数据库中的其他数据。

3 身份识别与鉴别

3.1 命名

3.1.1 名称类型

中汽数据 CA 签发的证书，含有颁发机构和订户证书主体的名称，对证书订户和其他属性进行的鉴别和记录采用甄别名（Distinguished Name，简称 DN），甄别名包含在证书主体内，是证书持有者的唯一标识。中汽数据 CA 的证书符合 X.509 标准，甄别名采用 X.500 的命名方式。

3.1.2 名称包含的内容

中汽数据 CA 签发的证书可以根据证书甄别名确定订户证书的主体。证书甄别名所采用的用户识别信息一般具有明确的、可追溯的、肯定的代表意义，应该使用反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。

个人证书通常包含个人真实姓名或证件号码，作为标识订户的关键信息被认证。

机构证书通常使用包括《营业执照》《事业单位法人证书》等证书中标识的统一社会信用代码和单位名称，作为标识订户的关键信息被认证。

设备证书应使用能标识该设备的标识或名称、域名、IP 等结合订户的其他信息一起被认证。

3.1.3 订户的匿名或伪名

中汽数据 CA 的订户在进行数字证书申请时不能使用匿名或伪名。

3.1.4 名称的唯一性

在中汽数据 CA 服务体系中，不同订户证书的甄别名是唯一的，对于同一订户，中汽数据 CA 可以用其甄别名为其签发多张证书。

3.1.5 商标的承认、鉴别和角色

中汽数据 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。中汽数据 CA 签发证书时不验证申请人是否使用商标。发生纠纷时中汽数据 CA 有权拒绝申请或者吊销已签发的证书。

3.2 初始身份认证

3.2.1 证明拥有私钥的方法

证书私钥由介质生成并直接保存在介质中，证书持有者通过证书申请书中包含的数字签名证明申请者持有与所要申请证书中的公钥相对应的私钥。中汽数据 CA 签发证书时，系统将自动使用订户申请书中的公钥验证签名的有效性和申请数据的完整性，来确

认使用者拥有私钥。

3.2.2 组织机构身份的鉴别

对于组织机构身份的鉴别，中汽数据 CA 或授权的注册机构需要验证组织的合法证件。组织机构应指定和授权证书的申请代表，在证书的申请书上签字表示接受证书申请的有关条款，经办人应持身份证件供鉴别身份，并承担相应的责任。

经办人经组织机构授权，到中汽数据 CA 受理机构提交书面材料办理或在线提交电子化材料办理。CA 受理机构对组织机构身份的鉴别通过现场核验的方式进行身份鉴别。

组织机构身份鉴别证明材料包括不限于如下：

- 数字证书申请表（签字加盖公章）
- 授权委托书（签字加盖公章）
- 经办人有效身份证原件及复印件
- 证明组织机构身份的证件，如营业执照副本及复印件等（复印件需要加盖公章）
- 如果申请服务器证书还需提交域名使用权证明、ICP 运营证明、设备所有权使用权书面承诺等合法身份证明（加盖公章）
- 如果申请设备证书还需提交加盖公章的《设备身份鉴别承诺书》

中汽数据 CA 对申请资料的原件、复印件或电子材料进行鉴别后批准或拒绝申请。中汽数据 CA 保存组织机构申请材料的期限为证书失效后 5 年，这个规定期限随法律、政策、主管部门的要求修改。

3.2.3 个人身份的鉴别

对于个人身份的鉴别，证书申请者需要向 CA 中心的审核人员提供有效的身份证明（身份证、驾驶执照、军官证等等）和充足的证书申请者信息。申请者信息根据不同的应用采取不同的要求。对于机构中的个人证书申请者，其申请材料需要加盖公章或者提供授权证明材料，或者由机构对该个人信息进行有效确认后，中汽数据 CA 将对该组织机构进行鉴别。

个人或授权代表人，到中汽数据 CA 受理机构提交书面材料办理或在线提交电子化材料办理。CA 受理机构对个人身份的鉴别主要通过现场核验方式进行身份核验。

个人身份鉴别证明材料包括不限于如下：

- 数字证书申请表（签字加盖公章）
- 有效身份证原件及复印件
- 如果委托他人办理需要授权委托书（签字）、委托人身份证原件和复印件

中汽数据 CA 对申请资料的原件、复印件或电子材料真实性进行鉴别后进行批准申请或拒绝申请的操作。批准后，中汽数据 CA 保存个人申请材料的期限为证书失效后 5 年，这个规定期限随法律、政策、主管部门的要求修改。

3.2.4 设备身份的鉴别

设备身份的鉴别由设备所属机构负责，设备所属机构应与中汽数据 CA 签订《设备身份鉴别承诺书》，并按照承诺书约定保证来自机构内证书申请设备身份的真实性、合法性。

3.2.5 没有验证的申请者信息

订户在申请证书时，除中汽数据 CA 要求必须验证的申请者信息外，其余的信息可不被要求必须验证。

3.2.6 授权确认

当申请者代表组织机构申请证书时，需出示足够的证明信息以证明其是否有权代表那个实体。组织在证明文件上加盖公章后，则证明本组织对办理人授权确认，一旦审核通过，中汽数据 CA 会将授权信息妥善保存。

个人如果需要代办人代办，需要对代办人证明信息签字授权确认。

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

在证书期满前，证书订户有必要获得新证书以保证证书可以持续使用。通常 CA 要求订户产生新的密钥对来代替将要期满的密钥对，称为“密钥更新”。证书的密钥更新时，通过订户使用原有私钥对更新请求进行签名，中汽数据 CA 使用订户原有公钥验证

确认签名来进行常规密钥更新的标识与鉴别。

3.3.2 吊销后密钥更新的标识与鉴别

中汽数据 CA 不提供吊销后的密钥更新服务。

3.4 吊销请求的标识与鉴别

当中汽数据 CA 根据本 CPS4.9.1 所述理由吊销订户证书时，无需进行鉴别。如果订户主动要求吊销证书，则按照本 CPS3.2 进行身份鉴别。

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

证书申请实体包括个人和具有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 注册过程与责任

4.1.2.1 申请及注册流程

中汽数据 CA 的证书申请人可以通过现场面对面方式或在线方式提交证书申请请求，但证书申请人需要遵循以下要求：

1. 订户需提供本 CPS 3.2 中所述的有效身份证明材料及相关申请文件，并保证所提供的证明材料真实有效；
2. 中汽数据 CA 的注册机构在审核订户申请后，将审核通过的订户信息提交至中汽数据 CA；
3. 中汽数据 CA 根据注册机构的请求签发证书；
4. 注册机构使用中汽数据 CA 提供的授权信息为订户制作证书；
5. 注册机构通过安全的方式将证书发给订户。

4.1.2.2 电子认证服务机构的责任

中汽数据 CA 按照本 CPS 以及国家的相关法律法规（《电子签名法》《电子认证服务管理办法》等）进行实施，具体责任如下：

1. 参照本 CPS 3.2 中的要求对订户提供身份信息进行采集、记录、鉴别和审核，通过审核后向订户签发证书。
2. 如身份鉴别过程由授权注册机构完成，中汽数据 CA 对所授权的注册机构有监督、管理和审计职责。
3. 中汽数据 CA 及授权的注册机构有妥善保管订户信息资料的责任。

4.1.2.3 注册机构的责任

注册机构主要负责对证书申请者身份的鉴别和订户信息的录入，具体责任如下：

1. 注册机构参照本 CPS 3.2 的要求对订户所提交的申请材料进行采集、记录和审核，通过审核后，向中汽数据 CA 提交证书申请。
2. 注册机构需要接受中汽数据 CA 的监督、管理和审计。
3. 应当按照 CA 机构的要求，向中汽数据 CA 提交订户身份审核资料或自行妥善保存。
4. 有义务告知证书订户使用数字证书时享有的权利和责任。

4.1.2.4 订户的责任

订户的责任如下：

1. 订户必须保证提供资料的真实、完整、准确、有效。
2. 订户须配合中汽数据 CA 或授权的注册机构完成对其身份信息及相关资料的采集、记录与审核工作。
3. 订户须了解并与中汽数据 CA 签署订户协议。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

证书申请者向中汽数据 CA 或相关注册机构提交证书申请后，中汽数据 CA 或授权

的注册机构按照本 CPS 3.2 所规定对申请人的身份进行识别与鉴别，检查申请者所提供的证明材料是否真实、完整和有效，同时鉴别证书申请书中的信息是否与订户提供的证明材料一致。

如果证书申请者为组织机构或设备，中汽数据 CA 还将检验申请者是否为合法被授权者或合法设备。

4.2.2 证书申请批准和拒绝

中汽数据 CA 按照本 CPS 所规定的身份鉴别流程对订户提交的申请材料及其身份信息进行识别与鉴别，并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别结果为合格，中汽数据 CA 或授权的注册机构等将批准证书申请，为证书申请人制作颁发数字证书。

如证书申请人未能通过身份鉴别，中汽数据 CA 或注册机构将拒绝证书申请人的申请，并将拒绝理由告知给对方。

被拒绝的申请人可准备符合本 CPS 所规定的相关材料后，再次提出申请。

4.2.3 申请材料现场核实双人控制

证书申请者通过现场面对面方式提交证书申请请求时，中汽数据 CA 会对用户申请材料进行现场核实。处理申请材料时，由双人控制，一人为受理人，检查申请者提供身份信息真实性，以及证件原件的真实性，并录入订户信息；另一人为审核员，通过受理申请单后，对材料和证书录入信息进行审核。

4.2.4 处理证书申请的时间

中汽数据 CA 或注册机构在收到订户的所有必须的证书申请信息后，将在 2 个工作日内处理证书申请。

中汽数据 CA 或授权的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响应了中汽数据 CA 的管理要求。

4.3 证书的签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

在证书订户申请通过身份鉴别后，中汽数据 CA 和注册机构的系统操作员（业务办理人员）负责录入订户的申请信息，并将申请提交给系统审核员（鉴证服务人员）审核；审核通过后，向 CA 签发系统提交证书申请。

CA 签发系统向注册系统返回证书下载凭证或证书。证书的最终签发意味着中汽数据 CA 最终完全正式批准了证书申请。

如果申请者申请签名证书，申请者需要将签名公钥连同证书申请材料提交给中汽数据 CA 或授权的注册机构，当申请者申请审核通过后，中汽数据 CA 将会为其签发签名证书。注册机构申请签发证书时，CA 系统需验证注册机构签名并确认注册机构的权限。

4.3.2 电子认证服务机构和注册机构对订户的通告

中汽数据 CA 会采用以下几种方式告知订户：

1. 电子邮件（e-mail）。
2. 采用现场方式面对面通知订户。
3. 其他的安全可行的方式。

4.4 证书接受

4.4.1 构成接受证书的行为

证书申请人按照中汽数据 CA 的证书申请流程完成证书申请后，中汽数据 CA 将为其签发数字证书，并通过面对面、邮寄、电子或在线等方式发给证书申请人，证书申请人从获得数字证书起，就被视为同意接受证书。

4.4.2 电子认证服务机构对证书的发布

中汽数据 CA 在签发完通用型证书后 24 小时内，将该订户证书发布到中汽数据 CA 的目录服务系统中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构对其他实体的通告

中汽数据 CA 不对其他实体进行通告，其他实体可以通过中汽数据信息服务自行查询。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在提交了证书申请并接受了中汽数据 CA 所签发的证书后，均视为同意遵守与中汽数据 CA、依赖方有关的权利和义务条款。

证书订户接收到数字证书，应妥善保管其所持有证书对应的私钥。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后才能使用对应的私钥，并在证书使用到期或吊销后，订户须停止使用该证书对应的私钥。

4.5.2 依赖方对证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书适用范围相一致，依赖方获得对方证书后，依赖方有义务进行如下确认操作：

1. 确认证书是依赖方信任的认证服务机构签发；
2. 确认该证书在有效期之内；
3. 确认该证书是否被吊销；
4. 确认密钥用法是否符合证书标识的密钥用途；
5. 验证订户数字签名有效性。

4.6 证书更新

证书更新指在不改变证书中除订户公钥以外信息的情况下，为订户签发一张新证书。

4.6.1 证书更新的情形

当订户的证书即将到期时，可向中汽数据 CA 或其授权的注册机构提出证书更新申

请。

4.6.2 请求证书更新的实体

请求证书更新的实体为证书订户。

4.6.3 证书更新请求的处理

当中汽数据 CA 或其授权注册机构接收到订户的更新申请后，需要鉴别该证书是否属于中汽数据 CA 签发的证书以及订户是否有权申请证书更新，并检验该证书的有效性（是否已过期），如果订户采用在线的方式申请更新，中汽数据 CA 或其授权注册机构还应检查该申请所附签名的真实性。

通过审核后，中汽数据 CA 或其授权注册机构将会为订户作证书更新处理。

4.6.4 颁发新证书时对订户的通告

同 4.3.2

4.6.5 构成接受更新证书的行为

同 4.4.1

4.6.6 电子认证服务机构对更新证书的发布

同 4.4.2

4.6.7 电子认证服务机构对其他实体的通告

同 4.4.3

4.7 证书变更

4.7.1 证书变更的情形

证书变更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。

4.7.2 请求证书变更的实体

任何使用证书的订户在证书发生本 CPS4.8.1 中涉及的情形时，均可向中汽数据 CA 或其授权注册机构提出证书变更申请。

4.7.3 证书变更请求的处理

当中汽数据 CA 或其授权注册机构接收到订户的变更申请后，需要鉴别该证书是否属于中汽数据 CA 签发的证书以及订户是否有权申请证书变更，并且检查证书的有效性以及变更后的订户身份证明材料，该过程与初始注册过程相同。

4.7.4 颁发新证书时对订户的通告

同 4.3.2

4.7.5 构成接受变更证书的行为

同 4.4.1

4.7.6 电子认证服务机构对变更证书的发布

同 4.4.2

4.7.7 电子认证服务机构对其他实体的通告

同 4.4.3

4.8 证书吊销

4.8.1 证书吊销的情形

如果有以下情况，证书将被吊销：

1. 中汽数据 CA、授权注册机构或订户认为或十分怀疑有威胁订户私钥安全的不利因素存在；
2. 中汽数据 CA、授权注册机构或订户认为申请者违背了订户责任条款中的义务、

要求或保证；

3. 证书订户与组织从属关系已被终止；
4. 中汽数据 CA、授权注册机构或订户认为证书的签发没有遵循本 CPS（或业务规则） 所要求的过程执行，证书没有签发给证书的主体，或证书的签发未通过证书主体的许可；
5. 证书中的信息不准确或被更改；
6. 订户根据证书吊销流程要求自愿撤销证书；
7. 由于法律或政策的要求中汽数据 CA 采取的作废措施。

4.8.2 请求证书吊销的实体

已申请中汽数据 CA 证书的订户可以请求证书吊销。

同时，中汽数据 CA 也可在 4.9.1 所述的情形下主动吊销订户的证书。

4.8.3 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流程

1. 证书吊销的申请人到中汽数据 CA 或其授权的注册机构提交书面资料，并注明吊销理由。
2. 中汽数据 CA 或授权的注册机构根据本 CPS 的相关要求对订户提交的吊销请求进行审核。
3. 中汽数据 CA 或授权的注册机构吊销订户证书后，应通知证书订户结果，订户证书在 24 小时内进入 CRL 列表，并对外发布。

4.8.4 吊销请求的宽限期

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

4.8.5 电子认证服务机构处理吊销请求的时限

中汽数据 CA 或其授权的注册机构会在吊销申请提交后的 4 小时内吊销证书并在 24 小时之内生效。

4.8.6 依赖方检查证书吊销的要求

依赖方必须在信任某个证书前，先查询吊销列表确认证书的状态信息，这一列表由中汽数据 CA 定期发布。

4.8.7CRL 发布频率

中汽数据 CA 可采用实时或定期的方式发布 CRL，一般为 24 小时定期发布。

4.8.8CRL 发布的最大滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.8.9 在线状态查询的可用性

中汽数据 CA 能够向安全保障要求高的订户提供 OCSP 在线证书状态查询服务。依赖方可以申请使用中汽数据 CA 提供的 OCSP 服务在线状态查询服务。

4.9 证书冻结

4.9.1 证书冻结的情形

如果有以下情况，中汽数据 CA 将会考虑冻结证书：

1. 订户提出暂停使用该证书；
2. 订户未能履行与中汽数据 CA 签订的协议中应尽的责任，如订户未按期缴纳证书服务费；
3. 注册机构、政府主管部门或国家司法机关，向中汽数据 CA 和其授权的认证服务机构提出证书冻结请求并获得批准。

4.9.2 请求证书冻结的实体

证书订户本人或其授权的代理人、证书注册机构、政府主管部门或国家司法机关。

4.9.3 冻结请求的流程

1. 证书冻结申请人向中汽数据 CA 或其授权注册机构提交证书冻结申请表和身份证明材料，同时说明证书冻结的理由，如果为证书持有者以外的人（如证书注册机构或国家司法机关）提交冻结申请，同样需要填写申请表并加盖公章；
2. 中汽数据 CA 或其授权注册机构鉴别冻结申请者身份的真实性，并确认申请者是否有权提出该申请；
3. 注册机构审核冻结申请后，将该申请提交至中汽数据 CA，等待中汽数据 CA 对该申请的处理；
4. 中汽数据 CA 在处理冻结申请后，会定期或实时产生 CRL 列表，并通知订户证书已被冻结。

4.9.5 电子认证服务机构处理冻结请求的时限

中汽数据 CA 或其授权的注册机构会在冻结申请提交后的 4 小时内冻结证书并在 24 小时之内生效。

4.9.6 证书冻结的期限限制

证书冻结的最长期限不得超过证书的有效期，如超过证书有效期而订户没有提出解冻申请，则该证书将会自动失效。

4.10 密钥损害的特别要求

当订户发现或有充足的理由发现其密钥被损害时，应当及时提出证书吊销请求。

4.11 密钥更新

中汽数据 CA 不采取密钥更新。

4.12 证书状态服务

中汽数据 CA 通过 LDAP、OCSP、以及 CRL 提供证书状态查询服务，如订户想了解证书状态可使用此类服务。中汽数据 CA 提供 7×24 小时的证书状态查询服务。

4.13 订购结束

在订户证书期满时，中汽数据 CA 会自动终止对订户证书的认证服务。此外，订户还可根据自身的需求申请认证服务的终止，该终止的请求流程与证书吊销流程相同。

中汽数据 CA 会针对证书订购期间及证书订购结束的操作过程进行详细记录，并进行妥善保存。

4.14 密钥生成、备份与恢复

订户的签名密钥由订户自己生成，中汽数据 CA 及其授权的注册机构不提供订户证书签名密钥的备份和恢复服务。

中汽数据 CA 的订户证书加密密钥对由中汽数据密钥管理中心提供。该机构负责订户加密密钥对的生成、管理和备份，并在出现法律纠纷时提供司法取证的依据。其密钥的生成、备份和恢复策略由该机构制定。

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

为了保证 CA 系统在运行中的稳定、安全和可靠，中汽数据 CA 在硬件设备、操作系统、数据库系统和目录服务系统的选用及物理环境的建设等各方面紧密结合 CA 系统的设计，于 2021 年通过国家密码管理部门的安全性审查和技术鉴定。

中汽数据 CA 机房位于北京市大兴区北京经济技术开发区博兴 6 路 3 号，该中心建立在安全可靠的物理环境内，中心机房具有防盗、防火、防雷、防辐射的能力。机房内

部配备 24 小时场地监控系统、指纹门禁系统、供电系统以及通风系统。

5.1.2 物理访问

中汽数据 CA 系统分为多个物理安全级别保护，在访问高级别前必须通过低级别的要求。中汽数据 CA 的任何敏感操作以及与认证完整生命周期相关所有行为（包括认证、鉴别、签发）都在其指定的物理安全级别中进行。

中汽数据 CA 的环境共分为五个区域：服务区、管理区、RA 区、CA 区、档案室，每个区域具有不同区域访问控制措施；

任何物理访问行为必须自动记录并有全程监控跟踪。中汽数据 CA 设置了以下安全访问级别：

普通级：机房外不涉及 CA 系统组件的区域，该级别主要包括日常的办公场所和公司内部的公共区域，利用员工权限卡可进入。

一般敏感级：机房内的服务区域，使用身份标识门禁卡和人体特征控制出入。

敏感级：机房内的 RA 区，采用身份标识门禁卡和人体特征鉴别身份，由双人访问控制出入，机房内部配有无死角监控系统。进入 RA 机房后，可通过身份标识门禁卡和人体特征进出 CA 管理区、KM 管理区，档案区属于敏感级，进入档案区应有相应权限。

高度敏感级：机房内 CA 系统核心组件所在的位置，即 CA 区和 KM 区（不含管理区），采用双人双因素认证方可进入机房，且其中至少有一种因素为人为特征。在此区域中的机房设计为六面钢板的屏蔽式结构，并安装了入侵检测系统，内部配有无死角监控系统。

5.1.3 电力与空调

中汽数据 CA 执行连续操作的所有硬件设备应配备空调系统、通风系统以及照明系统等，同时还要考虑到应急环境设施。

机房空调采用高效能、高灵敏度的空调系统，配合通风、温湿度调节等手段，控制机房内设备运行温湿度，保证系统正常运行。

中汽数据 CA 的电气系统符合电子数据处理设备的防火标准。机房电力供应按照机房设备负载要求设计，采取三向方式供电，机房采用两台 UPS 供电设备并行双路向机房内设备供电，A、B 路配电分别接入到机柜的两个 PDU 上，每台设备的两路电源分别

从 AB 路 PDU 取电。

5.1.4 水患防治

中汽数据为 CA 系统布置了漏水检测系统来防止水灾对 CA 系统的损坏，当出现漏水、水灾时，监控系统可以进行警示。

5.1.5 火灾防护

中汽数据 CA 的火灾自动报警系统设计依据 GB50116-98《火灾自动报警系统设计规范》进行设计，七氟丙烷自动灭火系统设计依据 GB50370-2005《气体灭火系统设计规范》进行设计。火灾自动报警系统通过设置在机房的温感、烟感探头采集消防数据，提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。机房关键区域均安装了七氟丙烷自动灭火系统，当火灾报警信号确认后，报警控制装置自动联动相关设备，并启动七氟丙烷自动灭火系统。该防火系统具有自动、手动及机械应急操作共三种启动方式。

5.1.6 介质储存

中汽数据 CA 将所有保存产品软件和数据、审计、归档文件、备份信息的介质都保存在 CA 中心的离线存贮设备或保险柜中，这些设备都配有适当的物理和逻辑访问控制来限制对非授权人员的访问和对存储介质的保护（防止意外的水灾、火灾或电磁干扰）。

5.1.8 异地备份

CA 机房位于北京市大兴区北京经济技术开发区博兴 6 路 3 号，异地备份于天津市西青区中北镇新城市中心 B 座。

5.2 程序控制

5.2.1 可信角色

基于认证服务的安全性需求，中汽数据 CA 必须保证只有被认定为可信的人员才能在安全性和敏感性高的岗位上工作，中汽数据 CA 的可信角色包括影响到以下操作的所

有员工：

1. 证书申请书中信息的鉴别
2. 证书申请、吊销请求、更新请求或其他注册信息的接收、拒绝、或其它业务的受理
3. 证书的发放、吊销和访问 CA 系统中受限制的部分
4. 对申请者信息和请求的处理

中汽数据 CA 的可信人员包括但不仅限于：

1. 证书业务审计员
2. 业务受理员
3. 鉴证服务人员
4. 网络安全管理员
5. 系统维护管理员
6. 技术支持人员

5.2.2 每项任务需要的人员

中汽数据 CA 根据各项敏感操作的安全要求规定所需的人员数量，即确保多个员工共同完成一项敏感操作。

CA 密钥、相关加密设备以及机密文件和数据的管理和操作应有多个可信人员共同完成。认证及注册系统的日常维护操作应由可信人员完成。

5.2.3 每个角色的识别与鉴别

所有中汽数据 CA 的可信人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别，CA 机构将完整地记录其所有的操作行为。

5.2.4 需要职责分割的角色

当某个可信人员被分配到多个信任角色时，其所能执行的操作不能完成完整的一项业务活动，即不能使某个可信人员的操作权限过高。需要职能分割的角色包括：

- 证书申请、更新、吊销等业务处理人员

- 订户资料管理人员
- 认证和注册系统维护人员
- 密钥管理人员
- 秘密分割持有者

5.3 人员控制

5.3.1 资格、经历和无过失的要求

所有员工应与公司签订保密协议。中汽数据 CA 的员工必须具备一定的资格，具体要求在《中汽数据 CA 组织结构和职责说明》中体现，需要有至少 3 个月的考察期，根据考察的结果安排相应的工作或辞退且脱离岗位。

5.3.2 背景审查程序

中汽数据 CA 制定了可信人员背景审查程序。背景审查必须符合法律法规的要求，审查内容、方式和从事审查的人员不得有违反法律法规的行为。

在开始一个可信人员的雇佣关系前中汽数据 CA 将会至少执行以下背景检查：

1. 身份证明，如个人身份证、户口本、护照等
2. 学历、学位以及其他资格证书
3. 个人简历、包括教育、培训经历，工作经历及相关的证明人

背景审查具体操作内容至少包括以下内容：

1．验证先前的工作记录

2．验证身份证明的真实性

3．验证学历、学位以及其他资格证书的真实性

4．通过可靠途径确认教育、培训经历

5．通过适当途径了解是否有工作中的严重不诚实行为

背景审查中导致可信人员候选人或现有可信人员被取消资格的问题主要包括：

1. 备选人或可信人员伪造真实身份信息

2. 十分不合适或不可信的个人经历
3. 工作中有严重不诚实行为

5.3.3 培训要求

中汽数据 CA 向其员工和授权注册机构的人员提供与 CA 系统相关的硬件、软件及其 CA 应用程序的岗前和在岗培训，目的是为了让员工能够胜任其工作。中汽数据 CA 还会定期的修改和加强其培训计划。

中汽数据 CA 的培训计划主要包括：

1. PKI 基础
2. 产品体系、系统组成、各系统功能
3. 系统管理员划分、岗位、权限、功能及具体操作等
4. 数字证书生命周期管理与操作
5. 系统备份、审计、运维管理、安全防护等

5.3.4 再培训周期和要求

对充当可信角色或其他重要角色的人员，中汽数据 CA 每年至少提供一次培训。同时，当 CA 系统大环境有所改变时，培训内容也将随之更新。

5.3.5 工作岗位轮换周期和顺序

中汽数据 CA 可以根据具体工作情况安排制定员工的工作轮换周期和顺序。

5.3.6 未授权行为的处罚

当中汽数据 CA 的员工被怀疑或者已经进行了未授权的操作，例如未经授权滥用权力或超出权限使用中汽数据 CA 系统或进行越权操作，中汽数据 CA 在得到信息后立即终止该员工进入中汽数据 CA 认证服务体系，未授权行为的处罚包括解除或终止劳动合同、调离工作岗位、罚款、批评教育等，根据情节严重程度，实施包括提交司法机关处理等措施。

5.3.7 独立合约人的要求

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

a）正规劳务公司派遣人员；

b）具有相关业务的工作经验；

c）必须接受 CA 组织的岗前培训。

5.3.8 提供给员工的文档

为使得系统正常运行，CA 机构向其员工提供完成其工作所必须的文档。

5.4 审计日志程序

5.4.1 记录事件的类型

中汽数据 CA 记录与系统相关的事件信息，包括：电子认证服务系统的操作事件、证书生命周期事件、可信人员的操作事件、不符合规程的事件，这些记录信息称为日志。日志必须包含事件发生的日期、时间段、事件内容和事件相关的实体等内容。

5.4.2 处理日志的周期

中汽数据 CA 每天对系统的日志进行收集；每 2 个月对日志进行检查分析工作。

5.4.3 审计日志的保存期限

中汽数据 CA 系统审计日志本地保存期限为 2 个月，归档后进行长期保存，至少保存到证书失效后 5 年。

5.4.4 审计日志的保护

中汽数据 CA 通过物理或逻辑的访问控制来防止电子或手写的审计日志文档被未经授权的浏览、篡改、删除和其他损坏。

5.4.5 审计日志备份程序

中汽数据 CA 保证所有的审计日志都按照《中汽数据 CA 备份策略》定期进行备份。

5.4.6 对导致事件实体的通告

中汽数据 CA 在进行审查中发现的攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，中汽数据 CA 保留采取相应对策实施的权力。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。

CA 机构有权决定是否对导致事件的实体进行通告。

5.4.7 脆弱性评估

CA 机构每半年对系统进行漏洞扫描、每年对系统进行渗透测试等脆弱性评估，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

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

所有归档记录的保存期限为证书失效后 5 年以上。

5.5.3 归档文件的保护

中汽数据 CA 机构保护相关的归档文件，免遭恶劣环境的威胁，如温度、湿度等的破坏。只有被授权的中汽数据 CA 信任人员才可访问归档文件，中汽数据 CA 在安全机制上保证禁止对归档文件及其备份进行删除、修改等操作。

5.5.4 归档文件的备份

中汽数据 CA 每日对归档记录进行备份，每周对全部信息进行离线备份并保存在安

全环境中，对于电子记录每半年进行一次异地备份。

5.5.5 记录时间戳要求

所有归档记录都要在存档时加具体准确的时间标识以表明存档时间。

5.6 电子认证服务机构密钥更替

中汽数据 CA 的密钥对在生命周期结束时其服务也将终止。只有在密钥的累计使用时间未超过密钥最大生命周期的前提下中汽数据 CA 的密钥才可以被更新。新的密钥对替换旧密钥对并且支持新的服务。

在上级电子认证服务机构的 CA 证书期满前，要对密钥采取更新以加快上级电子认证服务机构密钥对顺利过渡为新的电子认证服务机构密钥对。电子认证服务机构的密钥更换程序需要：

1. 上级电子认证服务机构至少要在下级 CA 到期前停止签发新的下级 CA 证书。
2. 使用新密钥对签发上级 CA 证书，至此开始使用新的上级 CA 证书签发下级 CA 证书或订户证书。
3. 在使用前密钥对签发的最后一个证书期满之前，上级 CA 还会继续发布前上级 CA 私钥签署的 CRL。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

当发生故障时，中汽数据 CA 将按照《中汽数据 CA 业务连续性计划》实施恢复。

5.7.2 计算资源、软件和/或数据的损坏

CA 机构遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，CA 机构将按照《中汽数据 CA 业务连续性计划》实施恢复。

5.7.3 实体私钥损害处理程序

当怀疑或发现中汽数据 CA、中汽数据 CA 的授权注册机构或订户私钥被损坏，中汽数据 CA 将组织分析并形成行动方案。

当 CA 证书有必要吊销时，将会执行以下程序：

1. 立即向行业主管部门汇报，通过公司网站或公共媒体对订户进行通告。
2. 吊销所有证书并将证书的吊销状态传达给订户及依赖方。
3. 产生新的根密钥对，签发新的根证书以及下级 CA 证书。
4. 新根证书签发完毕后立即通过目录服务器、信息库以及网站等方式发布。

当订户证书私钥遭到损坏时，将会执行以下程序：

1. 应立即停止使用私钥，并立即通知中汽数据 CA 或授权的注册机构吊销其证书，中汽数据 CA 按照本 CPS 要求发布证书吊销信息。
2. 当中汽数据 CA 或其授权注册机构发现证书订户的实体私钥受到损害时，中汽数据 CA 将吊销证书并通知证书订户，订户必须立即停止使用私钥。

5.7.4 灾难后的业务连续性能力

当主运营场所发生灾难或不可抗力事故而不能正常运营时，中汽数据 CA 将利用备份数据和设备恢复各项业务的正常运行并应能够满足以下业务连续性要求：

- 在尽可能短的时间内恢复业务系统
- 能够恢复客户信息
- 能够恢复对客户的服务
- 有足够的人员继续业务并且不违反职责分割的要求

5.8 电子认证服务机构或注册机构的终止

如果有必要终止中汽数据 CA 的运作，中汽数据 CA 将按照相关的法律法规所制定的步骤终止运营，并按照相关法律法规要求进行档案和证书的存档。

中汽数据 CA 机构在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于中汽数据 CA 授权的注册机构和订户等。

在终止服务六十日前向工业和信息化部报告，按照相关法律规定的步骤进行操作。

中汽数据 CA 机构采用以下措施终止业务：

1）起草 CA 终止业务声明；

2）停止认证中心所有业务；

3）处理加密密钥；

4）处理和存档敏感文件；

5）清除主机硬件；

6）管理 CA 系统管理员和安全官员；

7）通知与 CA 终止运营相关的实体。

中汽数据 CA 根据与注册机构签订的运营协议终止注册机构的业务。

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 签名密钥的生成，其安全性通过管理手段和技术手段两方面保证。加密机采用密钥分割机制进行备份，按照《中汽数据 CA 密码设备及密钥管理策略》授权 3 个密钥管理员，凭借 USB Key 对密钥进行控制管理。

个人和机构订户的的签名密钥对应使用国家密码管理局认可的、中汽数据 CA 证书签发系统支持的介质生成。中汽数据 CA 并不承诺接受所有类型的密码产生设备。加密密钥对由中汽数据密钥管理中心（以下简称 KMC）生成和保存管理，并通过安全方式传输给订户。证书订户应采用适当的安全保护措施保护密钥的安全性。

6.1.2 私钥传送给订户

订户签名私钥是由订户证书存储设备产生，不需要传递。订户加密私钥由中汽数据密钥管理中心生成并保存。在制作证书时，加密私钥采用国家密码主管部门许可的算法加密，并通过安全通道传送到订户证书存储介质。

6.1.3 公钥传送给证书签发机构

订户通过中汽数据 CA 的注册管理系统生成的数字证书申请书和公钥，并提交给中汽数据 CA 签发，在传递过程中采用国家密码主管部门许可的密钥算法，采用适当的安全保护措施，保证传输中数据安全，避免公钥在提交给电子认证服务机构过程中被泄露和篡改。

6.1.4 电子认证服务机构公钥传送给依赖方

中汽数据 CA 为依赖方提供公钥证书的在线下载功能，依赖方可以通过访问中汽数据 CA 的对外发布网站获取中汽数据 CA 的公钥证书，中汽数据 CA 还提供面对面提交或线下安全方式向依赖方提供 CA 公钥证书。

6.1.5 密钥长度

密钥算法和长度符合国家密码管理部门的规定。

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

中汽数据 CA 密钥对采用了符合国家密码主管部门要求的硬件密码模块来产生、管理、保存、备份和恢复，CA 根密钥的操作只能由特定人员在特定的机房场所操作完成。中汽数据 CA 制定了规范化管理办法，会通过物理、逻辑等控制方式实现私钥的保护，订户应按照与中汽数据 CA 签署的协议内容妥善保管订户私钥。

6.2.2 私钥多人双因素控制（m 选 n）

中汽数据 CA 密钥的生成、更新、撤销、备份、恢复等操作采用多人双因素（USB Key+PIN）控制机制。管理密钥分割保存在五个 USB Key 中由五位经过授权的人员管理，五人中至少三人同时控制以上操作。

6.2.3 私钥托管

中汽数据 CA 不会把根 CA 私钥托付给任何第三方组织。

订户加密私钥由中汽数据密钥管理中心生成并负责存储、备份以及在发生法律纠纷时提供司法取证的依据。

中汽数据 CA 和密钥管理中心均不对订户签名私钥进行托管。

6.2.4 私钥备份

中汽数据 CA 私钥由加密机产生，有备份加密机，对加密机的备份操作需 3 人以上才可完成，备份形式包括加密机双机备份和加密导出备份，加密备份导出将 CA 私钥以加密的形式保存在硬件密码模块中。

订户加密私钥由中汽数据密钥管理中心负责备份至数据库供以后恢复及查询使用。

中汽数据 CA 和 KMC 都不对订户的签名私钥进行保存和备份。

6.2.5 私钥归档

中汽数据 CA 对已过期的 CA 密钥对进行归档，归档的 CA 密钥对保存期为 5 年。归档的 CA 密钥不能用于其他用途，在归档期结束后中汽数据 CA 会对密钥进行销毁处理。

订户加密密钥由中汽数据 KMC 按照国家密钥主管部门的要求归档保存，归档保存期限不小于 5 年。

6.2.6 私钥导入、导出密码模块

中汽数据 CA 的 CA 密钥对在硬件加密模块中生成并在其中使用，中汽数据 CA 有备份加密设备。CA 私钥从一个密码设备备份到另外的设备的全过程必须由中汽数据 CA 授权的多位（3 of 5）可信人员同时到场操作，且导入导出时私钥不以明文形式存在。

中汽数据 CA 不提供订户私钥从硬件密码模块中导出的方法，也不允许此操作。

6.2.7 私钥在密码模块中的存储

私钥在硬件加密模块中以加密的方式存储和使用。

6.2.8 激活私钥的方法

CA 私钥存放在硬件密码模块中，其激活数据已按照秘密分割要求进行分割，并采用 3 of 5 的机制对其访问加以控制，因此需要使用 CA 私钥时，持有 CA 私钥激活数据分割的人员必须按照要求共同完成，在操作过程中，每一个 CA 私钥激活数据分割的人员均采用双因素认证方式来验证身份。

订户使用 USBKey、智能卡、安全芯片等密码设备存放私钥。使用私钥前，订户须安装私钥存储设备的驱动程序，将密码设备插入相应的读取设备中并输入口令，才能激活私钥进行使用。

中汽数据 CA 签发的服务器证书，私钥由服务程序产生和保存，私钥存放在服务程序的软件密码模块中，订户必须设置私钥激活口令，当服务启动软件加密模块被加载后，输入口令私钥被激活。

6.2.9 解除私钥激活状态的方法

密钥管理员多半数以上（3 of 5）密钥管理员同时使用管理员卡登录密码机，可以进行密钥解除激活操作。

中汽数据 CA 签发的订户证书私钥，在订户退出登录状态、驱动程序关闭、或关闭计算机时，私钥激活状态解除。

中汽数据 CA 签发的服务器证书在服务程序关闭、操作系统吊销或关机时解除私钥激活状态。

6.2.10 销毁私钥的方法

在 CA 私钥不再被使用且超过归档保存期限后，中汽数据 CA 将会按照厂商的密码设备安全管理操作规定把 CA 私钥连同其备份、与其相关的操作卡片销毁。销毁过程需要多个（3 of 5）信任人员的参与。

订户加密私钥经授权后由中汽数据密钥管理中心负责归档及销毁，具体执行方法遵

循国家相关法律要求。建议订户在私钥生命周期结束后的一段时间内妥善保存私钥的，以便于解开加密信息。如果订户私钥无需继续保存可以通过私钥删除或密码设备格式化的方法销毁私钥。

6.4 激活数据

6.4.1 激活数据的产生和安装

中汽数据 CA 的私钥激活数据被分割成多个秘密共享分别存放在多个存储介质中，其产生和分发会被记录。

订户使用口令来激活他们用于存储私钥的介质（如 USB key），初始下载中汽数据 CA 提供初始口令，并采取安全、可靠方式传递给订户，随后口令由订户自己设置。

6.4.2 激活数据的保护

CA 私钥激活数据，中汽数据 CA 按照可靠方式分割后由不同可信人员掌管。

订户应妥善管理好自己的口令，防止泄露和窃取。应该经常对激活数据进行修改。

6.4.3 激活数据的其他方面

只有在拥有证书介质并知道口令时才能激活证书存储介质使用私钥。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

中汽数据 CA 的 CA 系统在网络逻辑上要与其他组件分开。这一分开能够阻止除认证全部流程以外的网络访问。中汽数据 CA 部署在多级网络且使用防火墙保护网络以防止内部或外部的入侵，并且限制访问系统的网络行为的来源。

6.5.2 计算机安全评估

中汽数据 CA 的核心操作软件满足相关的国际标准，相关技术满足信息技术以及安全技术评估标准，系统的安全策略要符合安全保障需求。通过了国家密码管理局等部门

的有关评估、审查。

6.6 生命周期技术控制

6.6.1 系统开发控制

中汽数据 CA 系统的开发由满足国家相关安全和密码标准的可靠软件开发商完成，同时与该开发商建立安全保密约定以保证系统的权威性与可靠性。其开发过程符合国家密码主管部门的相关要求。

6.6.2 安全管理控制

中汽数据 CA 认证系统安全管理遵循国家密码局有关运行管理规范进行操作，中汽数据 CA 制定安全管理策略、制度以及流程对运营管理的各个方面实施有效的控制。

6.6.3 生命期的安全控制

中汽数据 CA 根据国际安全标准和行业发展动态，将及时进行软硬件升级以保证 CA 系统生命周期的安全性。中汽数据 CA 对系统的任何修改和升级会记录在案并予以控制。

6.7 网络的安全控制

中汽数据 CA 在采用多层防火墙、入侵防护、安全检测、 病毒防范系统，并及时对上述安全产品进行版本更新，保障网络基础设施安全。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

中汽数据 CA 签发的证书均符合 X.509 证书格式，遵循 RFC5280 标准。

7.1.1 版本号

中汽数据 CA 所签发证书的版本号 X.509 V3，信息存放在证书版本属性栏内。

7.1.2 证书扩展项

- 证书版本号（Version）

X.509　V3

- 证书序列号（**SerialNumber**）

中汽数据 CA 分配给证书的唯一的数字表示符。

- 签名算法标识符(Signature)

符合国家密码主管部门批准的算法对象表示符。

- 颁发机构密钥标识符（**Authority Key Identifier**）

此字段标识用于识别与中汽数据 CA 证书签名私钥相对应的公钥，用来辨别中汽数据 CA 使用的不同密钥。

- 主题密钥标识符（**Subject Key Identifier**）

此字段标识了订户证书被认证的公钥，它能够区分同一主体使用的不同密钥（如证书密钥更新时）。

- 签名算法标识符（**Signature algorithm identifier**）

中汽数据 CA 签发的的 RSA 算法数字证书采用 sha256RSA 签名算法，国产 SM2 算法数字证书采用 SM3_SM2 签名算法。

- 密钥用法（**Key Usage**）

此字段指示已认证的公钥有何种用途如电子签名、密钥加密、数据加密、不可抵赖等等。

- 基本限制（**BasicConstraints**）

用于鉴别证书持有者身份，如 CA 证书等。

- 增强型密钥用法（**Extended Key Usage**）

指明公钥的多种用途，对密钥用法中指明的基本用途的补充或替代，如：服务器验证、客户端验证、代码签名、安全电子邮件、时间戳、智能卡登录

- CRL 分布点（CRL Distrabution Point）

CRL 分布点包含可以获取 CRL 的地址和协议，用于依赖方验证证书状态。

- 自定义扩展

针对特别的订户，中汽数据 CA 签发的证书有可能包含私有扩展项，根据不同项目私有扩展项不同。

7.1.3 名称形式

中汽数据 CA 发放的所有证书都包含唯一的符合 X.509 标准证书签发者名称，同时也包含唯一的证书主体订户名称。

7.1.4 名称限制

订户证书的命名一定要有意义，可以通过名称确定证书主题中的个人、单位或者设备的身份，订户证书不应使用匿名或假名。在某些具有特殊要求的应用中，可以按照一定的规则为订户指定特殊名称，并且能够把该类特殊名称与一个确定的实体唯一的联系起来。

7.2 证书吊销列表

7.2.1 版本号

中汽数据 CA 定期签发 CRL（证书吊销列表），其所签发的 CRL 遵循 RFC5280 标准。采用 X.509 V2 格式。

7.2.2CRL 和 CRL 条目扩展项

version： CRL 版本号

signature：用于签发 CRL 的数字签名

issuer：签发者名称

this Update：这次签发时间

next Update：下次签发时间

revoked Certificates：被吊销的证书信息包括序列号和吊销日期

7.3 在线证书状态协议

中汽数据 CA 为证书订户提供 OCSP（在线证书状态查询服务），OCSP 为 CRL 的有效补充，方便证书订户及时查询证书状态信息。中汽数据 CA OCSP 服务遵循 RFC2560 标准。

8 认证机构审计和其他评估

8.1 评估的频率和情形

按照《中华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》等规定，中汽数据 CA 定期进行内审和外审。

内部审计是中汽数据 CA 对中心内部和注册机构的审计工作，结果供中汽数据 CA 机构改进、完善业务。中汽数据 CA 每年进行一次内部审计。

中汽数据 CA 还按照规定接受行业主管部门的定期评估和检查。

8.2 对问题与不足采取的措施

中汽数据 CA 在审计过程中发现的任何错误和不足将会及时提交到安全策略委员会，根据审计报告内容准备一份解决方案，并明确对此采取的行动。中汽数据 CA 将根据法律、法规迅速解决问题。

8.3 评估结果的传达与发布

当中汽数据 CA 接受行业主管部门审查评估后，评估结果由行业主管部门向公众发布。

中汽数据 CA 内部审计后，审计结果在公司内部进行传达。

9 法律责任和其他业务条款

9.1 费用

中汽数据 CA 在公司网站上公布数字证书的服务与收费的标准和相关信息，数字证书的服务与收费将坚持订户自愿的原则，即“按需选择，按项收费”；在证书有效期内，订户有义务向中汽数据 CA 接续交纳证书的使用服务费。

9.1.1 证书签发和更新费用

中汽数据 CA 根据市场需求情况和相关管理部门的规定向机构内的证书订户收取费用，中汽数据 CA 可在不高于收费标准的前提下针对不同订户群体推出不同的收费策略或优惠措施。

如果中汽数据 CA 签署的协议中指明的价格和中汽数据 CA 公布的价格不一致，以协议中的价格为准。

9.1.2 证书查询费用

在证书有效期内，对中汽数据 CA 证书订户的证书信息查询，中汽数据 CA 不收取查询费用，但保留对此项服务收取费用的权利。

9.1.3 证书吊销或状态信息的查询费用

查询证书是否吊销，中汽数据 CA 不收取查询费用。但保留对此项服务收取费用的权利。

对于使用在线证书状态查询（OCSP）不收取费用，但保留对此项服务收取费用的权利。

9.1.4 其他服务费用

中汽数据 CA 可根据请求者的要求，定制各类服务，具体服务费用，在与订户签订的协议中约定。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，中汽数据 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，中汽数据 CA 将不办理退证、退款手续。**

9.2 财务责任

9.2.1 保险范围

中汽数据 CA 保证其具有维持其运作和履行其责任的财务能力，能够承担对订户、依赖方等造成的责任风险，并依据 CPS 规定，进行赔偿担保。

9.2.2 其他财产

暂无规定。

9.2.3 对终端实体的保险或担保范围

如果中汽数据 CA 根据司法判定须承担赔偿和（或）补偿责任的，中汽数据 CA 将按照相关仲裁机构的裁决或人民法院的判决承担相应的赔偿责任。

9.3 业务信息保密

9.3.1 保密信息范围

保密信息包括但不限于以下内容：

1. 中汽数据 CA 与订户之间的协议、资料中未公开的内容等属于保密信息。除法律明文规定或政府、执法机关等要求，中汽数据 CA 承诺不对外公布或透露订户证书信息以外的任何其他隐私信息。
2. 订户私钥属于机密信息，订户应当根据本 CPS 的规定妥善保管，**非因中汽数据 CA 泄露私钥造成的损失，由此引起的后果中汽数据 CA 不承担责任，应当由订户或泄露方承担。**

9.3.2 不属于保密的信息

以下为中汽数据 CA 对外发布的非机密信息类型：

1. 中汽数据 CA 签发的证书和 CRL 中的信息不保密。
2. 本 CPS 的信息不保密。
3. 其他可以通过公共、公开渠道获取的信息不保密。

9.3.3 保护保密信息的责任

中汽数据 CA、证书订户、关联实体以及认证业务相关的参与方等，均有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

1、中汽数据 CA： 负责接收和保存保密信息的人员均为中汽数据 CA 授权的可信人员，这些可信人员有责任在接收到保密信息后保护保密信息的安全，防止其泄露、避免使用和发布给第三方。

2、订户：当证书信息的所有者出于某种原因，要求中汽数据 CA 公开或披露其所拥有的保密信息时，中汽数据 CA 可以酌情满足其要求；同时，中汽数据 CA 将要求该保密信息的所有者对这种申请进行书面授权，以表示其自身的公开或者披露的意愿。如果这种披露保密信息的行为涉及任何其他方的赔偿义务，中汽数据 CA 不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息引起的所有赔偿责任。

3、例外原则：当中汽数据 CA 在任何法律、法规或者人民法院以及其他权力部门通过合法程序的要求下，必须披露本 CPS 中规定的保密信息时，中汽数据 CA 可以按照法律、法规或法规条令以及人民法院判决的要求，向执法部门公布相关的保密信息。中汽数据 CA 无须承担任何责任。这种披露不能被视为违反了保密要求和义务。

9.4 用户隐私保密

9.4.1 隐私保密方案

中汽数据 CA 尊重所有订户和他们的隐私权，个人隐私信息保护遵循现行法律和政策规定，任何订户选择使用中汽数据 CA 的证书服务时，就表明已经接受中汽数据 CA 的隐私保护制度。

9.4.2 作为隐私处理的信息

中汽数据 CA 在管理和使用订户提供的相关信息时，除了证书中已经包括的信息外，该订户的基本信息和身份认证资料将被作为隐私处理，非经订户同意或者法律法规及权力部门的合法要求，不会任意对外公开。

9.4.3 不被视为隐私的信息

不被视为隐私的信息包括：证书订户持有的证书中的信息，以及该证书的状态信息等。

9.4.4 保护隐私的责任

中汽数据 CA、注册机构、订户、依赖方等机构或个人有义务遵照本 CPS 规定，承担相应的隐私保护责任。在法律法规或公共权力部门通过合法程序要求下，中汽数据 CA 可以向特定的对象公布隐私信息，中汽数据 CA 无需承担责任。

9.4.5 依法律或行政程序的信息披露

当中汽数据 CA 在法律、规章或法规条款的要求下，或在人民法院、仲裁机构的要求下必须披露本 CPS 中具有保密性质的信息时，中汽数据 CA 可以按照法律、法规、或法规条令以及法院判决、仲裁裁决的要求，向执法部门公布相关的保密信息。中汽数据 CA 无需承担任何责任。这种披露不能视为违反了保密的要求和义务。

9.4.6 其他信息披露形式

中汽数据 CA、订户、注册机构、依赖方等机构或个人都有义务遵循本 CPS 的规定，承担相应的隐私保护责任。当保密信息所有者出于某种原因要求中汽数据 CA 公开或披露其所拥有的保密信息或法律法规、相关权利部门通过合法程序的要求下，中汽数据 CA 可以向特定对象公布隐私信息，中汽数据 CA 无需承担由此造成的任何责任。

9.5 知识产权

中汽数据 CA 享有并保留对证书以及中汽数据 CA 提供的全部软件的一切知识产权，

包括（所有权、名称权、利益分享权等）。中汽数据 CA 网站上公布的一切信息均为中汽数据 CA 所有，禁止转载用于商业行为。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

中汽数据 CA 在提供电子认证服务活动中遵循如下承诺：

1. 遵守《中华人民共和国电子签名法》及相关法律规定，接受行业主管部门的管理，对所签发的数字证书承担相应的法律责任。
2. 保证所使用的系统及密码符合国家政策与标准，保证 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策和标准的规定。
3. 中汽数据 CA 的运营遵守本 CPS 规定并随着业务的调整对 CPS 进行修订。
4. 签发给订户的证书符合本机构的 CPS 的所有实质性要求。

9.6.2 注册机构的陈述与担保

注册机构在参与电子认证服务活动中遵循如下承诺：

1. 提供给证书订户的注册过程符合中汽数据 CA 的 CPS 的所有实质性要求。
2. 注册机构在批准证书前，完成了所有必要的鉴别与确认工作，并且需确认的信息是正确的、准确的。
3. 注册机构将按照本 CPS 的规定，及时向中汽数据 CA 提交证书申请、吊销、更新等服务请求。
4. 注册机构应当对订户的信息及与认证相关的信息妥善保存，并于适当的时间转交给中汽数据 CA 归档保存。
5. 注册机构应当根据相关协议内容配合中汽数据 CA 进行必要的电子认证业务合规性审计。

9.6.3 订户的陈述与担保

中汽数据 CA 的证书订户应该保证：

1. 订户确认已经阅读和了解了 CPS 及有关规定的全部内容，并愿意接受本 CPS 文

件规定的约束。

2. 订户在申请数字证书时，应当提供真实、完整、有效和准确的信息与资料，并在这些信息资料发生变化时及时通知中汽数据 CA 或其授权的注册机构。
3. 订户应当妥善保管私钥，采取安全的措施防止证书私钥的遗失、泄露和被篡改的事件发生，订户对使用私钥的行为负责。
4. 一旦发生任何可能导致安全性危害的事件，如遗失私钥、遗忘、泄露等情况，订户应立即通知中汽数据 CA 及其授权注册机构，申请采取吊销等保护措施。
5. 若要求更改证书或证书申请的信息，则应及时通知中汽数据 CA 及其授权注册机构；并且应通过证书策略允许的安全传递方式亲自发送通知。
6. 使用证书的行为应符合全部使用的法律法规及相关规定。

9.6.4 依赖方的陈述与担保

1. 依赖方必须熟悉本 CPS 的条款和订户数字证书相关的证书策略，并遵守本 CPS 中的所有规定。
2. 确定证书在规定的范围和期限内使用证书。
3. 获取并安装该证书对应的证书链。
4. 在信赖证书所证明的信任关系前了解确认该证书记载的内容与所要证明的内容一致。

9.7 担保免责

如有以下情况，应当免除中汽数据 CA 之责任。

1. 证书申请人或订户故意或过失提供或未按要求提供不准确、不真实或不完整信息而获得签发的证书，订户在使用该证书时产生的任何纠纷，证书申请人或订户自行承担全部法律责任，中汽数据 CA 对此不承担任何责任。
2. 由于非中汽数据 CA 原因造成的设备故障、网络中的导致的事故所造成的损失，损失方可以追究侵权方责任，中汽数据 CA 应当予以配合，但中汽数据 CA 不向任何方承担赔偿或补偿责任。
3. 数字证书超出使用范围或以非预期的方式使用，中汽数据 CA 不向任何方承担赔偿或补偿责任。

4. 由于不可抗力，如战争、自然灾害、政府命令、政策调整等造成的服务中断并由此造成的客户损失，中汽数据 CA 不承担相应的责任。

9.8 有限责任

中汽数据 CA 应承担的责任和义务包括：

1. 保证其使用和发放的公钥算法在现有技术条件下不会被攻破；
2. 保证中汽数据 CA 及其授权的注册机构的私钥被安全的存放和保护；
3. 保证中汽数据 CA 建立和执行的安全机制符合国家政策的规定。

除上述内容外，中汽数据 CA 及其授权的注册机构和相关的信任人员不承担其他任何责任和义务。

9.9 赔偿

9.9.1 赔偿范围

中汽数据 CA 的赔偿范围：

1. 由于中汽数据 CA 的原因，订户证书的签发过程没有按照本 CPS 的要求，导致订户证书签发有误；
2. 由于中汽数据 CA 操作人员的疏忽，导致订户证书内信息与用户提交的信息不一致并造成订户损失；
3. 中汽数据 CA 的 CA 私钥丢失或泄密。

9.9.2 赔偿限制

当中汽数据 CA 违反了本 CPS9.8 中的责任要求时，中汽数据 CA 承担赔偿责任（法律免责除外）。中汽数据 CA 所有的赔偿义务不得高于证书的赔偿上限，这种上限由中汽数据 CA 依据国家相关法律要求进行调整，并对外公布。

依赖方和证书订户在使用或信赖证书时，若有任何故意或过失行为导致中汽数据 CA 及其授权注册机构遭受损失，依赖方和证书订户应当承担损害赔偿责任，包括因形成诉讼或仲裁而产生的受理费、保全费、调查费、律师费、差旅费等必要费用。中汽数据 CA 及其授权的注册机构有权要求责任方予以全额赔偿。

当一个证书应证书订户的代理人要求被签发后，代理人和证书订户两者负有联带责任。如出现 9.9.1 中所述的责任，他们共同承担赔偿责任。证书持有者有责任就代理人所作任何不实陈述与遗漏及时告知中汽数据 CA 及其授权注册机构。

9.10 有效期限与终止

9.10.1 有效期限

除中汽数据 CA 特别声明本 CPS 提前终止，本 CPS 自对外发布之日起至新版本的正式发布前均有效，一旦新的版本发布则旧的版本自动失效。

9.10.2 终止

自新版本的 CPS 正式对外发布生效时，上一版本的 CPS 效力将自动终止。

当中汽数据 CA 中止电子认证服务时，本 CPS 自动终止。

9.11 修订

9.11.1 修订程序

本 CPS 的修改和更新，由中汽数据 CA 安全策略委员会负责，并组织 CPS 编写小组进行修改更新。修改完成之后，经安全策略委员会审核、批准，通过后方可对外发布。

9.11.2 通知机制和期限

中汽数据 CA 将在公司官方网站公布最新版本的 CPS，对具体个人不做另行通知。

9.11.3 必须修改业务规则的情形

当管辖法律、使用标准及操作规范等有重大改变时，必须修改本 CPS。

9.12 争议处理

中汽数据 CA 与订户或授权注册机构产生争议时，首先应遵循相应的协议进行协调，如需要诉诸司法程序，则处理办法依照国家相关法律规定。

9.13 管辖法律

本 CPS 在各方面服从中华人民共和国（港澳台地区除外）法律和法规的管制和解释，包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

9.14 一般条款

9.14.1 完整规定

本《电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

9.14.2 转让

中汽数据 CA 与电子认证服务业务相关的各实体之间的责任义务不能通过任何形式转让给任何第三方。

9.14.3 分割性

当人民法院或仲裁机构认定本规则中某条款无效时，不导致整个规则无效。

9.14.4 强制执行

在相应法律法规允许的范围内，中汽数据 CA 与认证服务相关的各实体之间的协议可以包含一个强制执行条款来保护中汽数据 CA 的利益。

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

在数字证书认证活动中，中汽数据 CA 由于不可抗力因素而暂停或停止部分或全部证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方不得提出异议或者申请任何补偿。