山东公众数科数字科技有限公司
电子认证业务规则

2.4 版

山东公众数科数字科技有限公司

2026 年 7 月

目 录

1 概括性描述 1
1.1 承诺 1
1.2 基本信息 1
1.3 文档名称与标识 2
1.4 电子认证活动参与者 3
1.4.1 电子签名电子认证服务机构 3
1.4.2 订户 3
1.4.3 依赖方 3
1.4.4 其他参与者 3
1.5 证书应用 4
1.5.1 适合的证书应用 4
1.5.2 限制的证书应用 5
1.6 策略管理 5
1.6.1 策略文档管理机构 5
1.6.2 联系方式 6
1.6.3 CPS 批准程序 6
1.7 定义和缩写 7
2 信息发布与信息管理 9
2.1 认证信息的发布 9
2.2 发布的时间或频率 9
2.3 信息库访问控制 10
3 身份标识与鉴别 10
3.1 身份查验通用要求 10
3.2 初始身份确认 10
3.2.1 订户告知 10
3.2.2 证明拥有私钥的方法 11
3.2.3 组织机构身份的鉴别 11
3.2.4 个人身份的鉴别 13

3.3 订户意愿确认 13
3.4 订户协议 14
3.5 未验证的订户信息 15
3.6 互操作要求 15
3.7 命名 15
3.7.1 名称类型 15
3.7.2 对名称意义化的要求 16
3.7.3 订户的匿名或伪名 16
3.7.4 理解不同名称形式的规则 16
3.7.5 名称的唯一性 17
3.7.6 商标的识别、鉴别和角色 17
4 证书生命周期操作要求 17
4.1 通用要求 17
4.2 证书申请 17
4.2.1 信息告知 17
4.2.2 申请的提交 18
4.2.3 执行识别与鉴别功能 18
4.2.4 证书申请批准和拒绝 19
4.2.5 处理证书申请的时间 19
4.2.6 对拒绝证书申请原因说明 19
4.3 证书签发 19
4.3.1 证书签发中 CA 的行为 19
4.3.2 CA 通知证书申请者证书的签发 20
4.4 证书接收 20
4.4.1 证书接受： 20
4.4.2 证书拒绝： 20
4.4.3 CA 对订户的通告 21
4.4.4 电子认证服务机构在颁发证书时对其他实体的通告 21
4.4.5 电子认证服务机构对证书的发布 21

4.5 密钥对和证书的使用 21
4.5.1 订户私钥和证书的使用 21
4.5.2 信赖方公钥和证书的使用 22
4.6 证书续期 22
4.6.1 证书续期的情形 22
4.6.2 请求证书续期的实体 22
4.6.3 证书续期请求的处理 22
4.6.4 颁发新证书时对订户的通告 23
4.6.5 构成接受续期证书的行为 23
4.6.6 电子认证服务机构对续期证书的发布 23
4.6.7 电子认证服务机构对其他实体的通告 23
4.7 证书密钥更新 23
4.7.1 证书密钥更新的情形 23
4.7.2 请求证书密钥更新的实体 24
4.7.3 证书密钥更新请求的处理 24
4.7.4 颁发新证书时对订户的通告 24
4.7.5 构成接受续期证书的行为 24
4.7.6 电子认证服务机构对续期证书的发布 24
4.7.7 电子认证服务机构对其他实体的通告 24
4.8 证书变更 24
4.8.1 证书变更的情形 25
4.8.2 请求证书变更的实体 25
4.8.3 证书变更请求的处理 25
4.8.4 颁发新证书时对订户的通告 25
4.8.5 构成接受续期证书的行为 25
4.8.6 电子认证服务机构对续期证书的发布 25
4.8.7 电子认证服务机构对其他实体的通告 25
4.9 证书撤销与冻结 26
4.9.1 证书撤销的条件 26

4.9.2 证书撤销的发起 26
4.9.3 证书撤销的处理 26
4.9.4 撤销请求宽限期 27
4.9.5 电子认证服务机构处理撤销请求的时限 27
4.9.6 依赖方检查证书撤销的要求 27
4.9.7 CRL 发布方式及频率 27
4.9.8 CRL 备份及频率 27
4.9.9 在线状态查询要求 27
4.9.10 撤销信息的其他发布形式 28
4.9.11 密钥损害的特别要求 28
4.9.12 证书冻结的情形 28
4.9.13 请求证书冻结的实体 28
4.9.14 冻结请求的流程 28
4.9.15 冻结的期限限制 29
4.9.16 电子认证服务机构处理冻结请求的时限 29
4.10 证书状态信息服务 29
4.10.1 操作特征 29
4.10.2 服务可用性 29
4.10.3 可选特征 29
4.10.4 服务可用率 29
4.11 停止使用认证服务 30
4.11.1 停止订户服务的情形 30
4.11.2 处理停止服务请求的时限和方式 30
4.11.3 责任延续条款 30
4.11.4 操作记录 30
4.12 密钥托管与恢复 31
4.12.1 密钥托管与恢复的策略与行为 31
4.12.2 会话密钥的封装与恢复的策略与行为 31
5 认证机构设施、管理和操作控制 32

5.1 物理控制 32
5.1.1 场地位置与建筑 32
5.1.2 物理访问 32
5.1.3 电力与空调 32
5.1.4 水患防治 32
5.1.5 火灾防护 33
5.1.6 介质存储 33
5.1.7 废物处理 33
5.1.8 异地备份 33
5.2 操作过程控制 34
5.2.1 可信角色 34
5.2.2 职责分离 34
5.3 人员控制 35
5.3.1 资格、经历和无过失要求 35
5.3.2 技能要求 35
5.3.3 背景审查程序 35
5.3.4 培训要求 36
5.3.5 工作岗位轮换周期和顺序 36
5.3.6 未授权行为的处罚 36
5.3.7 独立合约人的要求 36
5.3.8 提供给员工的文档 37
5.3.9 每个角色的识别与鉴别 37
5.3.10 需要职责分割的角色 37
5.4 审计日志程序 37
5.4.1 规定事件记录的类型 37
5.4.2 规定事件记录的内容 38
5.4.3 处理日志的周期 38
5.4.4 审计日志的保存期限 38
5.4.5 审计日志的保护 38

5.4.6 审计日志备份程序 39
5.4.7 审计收集系统 39
5.4.8 对导致事件实体的通告 39
5.4.9 脆弱性评估 39
5.5 记录归档 39
5.5.1 归档记录的类型 39
5.5.2 归档记录的保存期限 39
5.5.3 归档文件的保护 40
5.5.4 归档文件的备份程序 40
5.5.5 记录时间戳要求 40
5.5.6 归档收集系统 40
5.5.7 获得和检验归档信息的程序 40
5.6 电子认证服务机构根证书密钥更替 41
5.7 损害和灾难恢复 41
5.7.1 事故和损害处理程序 41
5.7.2 计算资源、软件和/或数据的损坏 41
5.7.3 实体私钥损害处理程序 41
5.7.4 灾难后的业务连续性能力 42
5.7.5 业务连续性计划的保障方案 42
5.7.6 灾难恢复演练 42
5.8 电子认证服务机构终止 42
5.8.1 终止情形 42
5.8.2 终止程序 43
5.8.3 过渡安排 43
5.8.4 责任延续 43
5.9 重大事项报告 44
5.9.1 重大事件范围 44
5.9.2 报告时限与程序 45
5.9.3 报告内容 45

5.9.4 后续跟踪 45
6 认证系统技术安全控制 46
6.1 技术安全管理制度要求 46
6.2 密钥对的生成和安装 46
6.2.1 密钥对的生成 46
6.2.2 私钥传送给订户 46
6.2.3 公钥传送给证书签发机构 47
6.2.4 电子认证服务机构公钥传送给依赖方 47
6.2.5 密钥的长度 47
6.2.6 公钥参数的生成和质量检查 47
6.2.7 密钥使用目的 47
6.3 私钥保护和密码模块工程控制 48
6.3.1 CA 密钥 48
6.3.2 订户密钥 49
6.4 密钥对管理的其他方面 51
6.4.1 公钥归档 51
6.4.2 证书操作期和密钥对使用期限 51
6.5 激活数据 51
6.5.1 激活数据的产生和安装 51
6.5.2 激活数据的保护 52
6.5.3 激活数据的其他方面 52
6.6 计算机安全控制 52
6.7 生命周期的安全控制 53
6.8 网络安全控制 53
6.9 时间戳 54
7 证书、证书撤销列表和在线证书状态协议 54
7.1 证书 54
7.2 证书吊销列表 56
7.3 在线证书状态协议 56

8 认证机构审计及相关评估 56
8.1 审计评估制度 56
8.2 认证业务审计 58
8.3 全面符合性评估 60
8.3.1 评估周期 60
8.3.2 评估内容 60
8.3.3 审计抽样方式 60
8.3.4 问题整改与跟踪 60
8.3.5 评估报告与报送 60
9 法律责任和其他业务条款 61
9.1 费用 61
9.1.1 证书签发和更新费用 61
9.1.2 证书查询费用 61
9.1.3 证书撤销或状态信息的查询费用 61
9.1.4 其他服务的费用 61
9.1.5 退款策略 61
9.2 财务责任 61
9.3 业务信息保密 62
9.3.1 保密信息范围 62
9.3.2 非保密信息范围 62
9.3.3 保密信息保护措施 63
9.3.4 保密责任 63
9.3.5 依法披露 63
9.4 个人隐私保密 64
9.5 知识产权 64
9.6 陈述和担保 65
9.7 担保免责 65
9.8 偿付责任规则 66
9.8.1 订户申请本机构赔偿 66

9.8.2 本机构申请订户赔偿 66
9.9 赔偿 67
9.10 有效期限与终止 68
9.11 对参与者的个别通告与沟通 68
9.12 修订和发布 69
9.13 争议处理与举证 69
9.13.1 争议受理范围 69
9.13.2 争议处理流程 70
9.13.3 协商与调解 70
9.13.4 仲裁 70
9.13.5 诉讼管辖 71
9.13.6 适用条件 71
9.13.7 举证制度和能力体系 71
9.14 管辖法律 72
9.15 适用法律的符合性 72
9.16 一般条款 72
9.17 其他条款 73

1 概括性描述

1.1 承诺

山东公众数科数字科技有限公司（以下简称 GZSK）郑重承诺：

a）开展经营和服务活动时，严格遵守国家法律、行政法规，树立以人民为中心的服务理念，积极承担社会责任；

b）与客户建立业务关系前，开展应用业务调研，建立应用接入业务风险评估及内部定责机制，严禁为存在违法违规风险的业务提供电子认证服务；

c）使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务；

d）接受政府和社会监督，对主管部门检查发现的问题及时整改，建立问题纠治长效机制，持续符合整改要求。

1.2 基本信息

山东公众数科数字科技有限公司于 2020 年 9 月开始运营，是依法设立的第三方电子认证服务机构。公司严格按照《中华人民共和国电子签名法》和《电子认证服务管理办法》的要求，提供数字证书签发、更新、撤销及管理服务，并通过 PKI 技术、数字证书应用技术为核心的应用安全解决方案，为电子签名构建安全、可靠的信任环境。

机构基本信息如下：

1） 机构名称：山东公众数科数字科技有限公司；

2） 法定代表人：滕靖国；

3） 机构住所：山东省济南市历下区经十路 9777 号鲁商国奥城 4 号楼 20 层 2007；
经营场所：江苏自贸区南京片区浦滨路 320 号科创一号大厦 A 座 812 室；

4） 联系方式：电话 0531-58205220，邮箱 business@sinocipher.com，网址 https://www.aiotca.com/。

5） 许可证书信息：公司已经取得电子认证服务使用密码许可证（证书编号：0066）和电子认证服务许可证（许可证编号：ECP32011123061），证书发证机关和

批准日期、有效期的起止时间等信息详见 GZSK 官网（https://www.aiotca.com/）公布；

6) 证书链信息：GZSK 的证书链信息如下：

证书名称	证书项	信息	备注
GZSK 根证书	序列号	34b1eee2da2454ba12a719758bc62c41	
	颁发机构	ROOTCA	
	密码算法	SM2	
	密钥长度	256	
	有效期起	2021 年 11 月 25 日 10:04:39	
	服务时间至	2041 年 11 月 20 日 10:04:39	
国家根证书	序列号	69e2fec0170ac67b	
	颁发机构	ROOTCA	
	密码算法	SM2	
	密钥长度	256	
	有效期起	2012 年 7 月 14 日 11:11:59	
	服务时间至	2042 年 7 月 7 日 11:11:59	

1.3 文档名称与标识

本文档名称为《山东公众数科数字科技有限公司电子签名电子认证业务规则》，是 GZSK 对所提供的认证及相关业务的全面描述。

上版本 CPS 版本号为 V2.0，修改部分章节例如机构证书验证流程，发布日期为 2024 年 5 月。

本 CPS 版本号为 V2.3，参照《电子认证业务规则规范》修订，发布日期为 2026 年 7 月 18 日。

本 CPS 下涉及的电子签名认证证书，证书中记载了主管部门的证书策略 OID，证书等级区分描述如下：

个人高等级证书 OID:2.16.156.339.2.1.1.2

个人基础级证书 OID:2.16.156.339.2.1.1.1

机构高等级证书 OID:2.16.156.339.2.1.2.2

机构基础级证书 OID:2.16.156.339.2.1.2.1

1.4 电子认证活动参与者

1.4.1 电子签名电子认证服务机构

山东公众数科数字科技有限公司(GZSK)依照《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》等法律法规，依法建立的第三方电子签名认证服务机构。GZSK 承担证书签发、更新、撤销、密钥管理、证书查询、证书黑名单（又称证书撤销列表或 CRL）发布、政策制定等工作。

1.4.2 订户

订户是指向 GZSK 申请证书的实体。“证书订户”是指向 GZSK 申请证书的实体，通常为个人或机构，即为“最终用户”。

1.4.3 依赖方

依赖方是指信任证书、使用证书的实体，依赖方可以是证书订户，也可以不是证书订户。

1.4.4 其他参与者

除电子签名电子认证服务机构（GZSK）、订户和依赖方以外的参与者称为其他参与者。

1.5 证书应用

1.5.1 适合的证书应用

GZSK 签发的各类订户数字证书可广泛应用于电子政务、电子商务及其他社会化应用场景，提供身份认证、电子签名和数据加密等安全服务。通过数字证书机制，能够有效确保网络信息交互双方身份的真实性和合法性，并保障信息在传输过程中的完整性、机密性与不可否认性，为各类业务系统构建安全可信的支撑环境。

GZSK 可提供以下类型的数字证书：

A.电子签名认证证书：

1、机构基础级电子签名证书：支持签发 SM2-256 密钥类型的机构证书，用于处理机构事务，适用于除高等级证书规定场景外的其他电子签名低风险业务场景。

2、机构高等级电子签名证书：支持签发 SM2-256 密钥类型的机构证书，用于处理机构事务，适用于涉及生命健康、财产权益等高风险场景，例如金融、医疗等。

3、个人基础级电子签名证书：支持签发 SM2-256 密钥类型的个人证书，用于处理个人事务，适用于除高等级证书规定场景外的其他电子签名低风险业务场景。

4、个人高等级电子签名证书：支持签发 SM2-256 密钥类型的个人证书，用于处理个人事务，适用于涉及生命健康、财产权益等高风险场景，例如金融、医疗等。

本 CPS 下涉及的电子签名认证证书，证书中记载了主管部门的证书策略 OID，证书等级区分描述如下:

个人高等级证书 OID:2.16.156.339.2.1.1.2

个人基础级证书 OID:2.16.156.339.2.1.1.1

机构高等级证书 OID:2.16.156.339.2.1.2.2

机构基础级证书 OID:2.16.156.339.2.1.2.1

仅用于电子政务电子签名的证书，依照《GZSK 电子政务电子认证业务规则》

执行，OID 号为 OID:2.16.156.339.2.2.1.1。

B.其他证书：

1、设备证书：支持签发 SM2-256 密钥类型的设备证书，仅用于设备身份认证及加密场景，不适用于电子签名场景。

2、SSL 证书：支持签发 SM2-256 密钥类型的 SSL 证书，仅用于建立国密安全通道场景，不适用于电子签名场景。

1.5.2 限制的证书应用

GZSK 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的情况下使用，具体包含但不限于以下情形:

a.涉及人身关系，如婚姻、收养、继承等;b.涉及公共事业服务停止，如停止供水、供热、供气等;

c.法律、行政法规规定的其他不适用电子签名的应用场景或类型;

d.国家法律法规禁止的活动;

e.涉及订户生命健康、财产权益的场景禁止使用基础级电子签名认证证书。

1.6 策略管理

1.6.1 策略文档管理机构

本《电子认证业务规则》的管理机构是本机构安全策略委员会。由 GZSK 安全策略委员会负责本《电子认证业务规则》的制订、发布、更新等事宜。公司任命了安全策略委员会成员，成员名单在公司内部公示。

安全策略管理委员会具体职责如下:

a） 确定维护CPS和CP等策略文档的职能分工，建立合理有效的修订和批准流程;

b） 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批;

c） 每年至少进行一次CPS和CP全面评审，根据实际需要及时修订策略文档;

d） 每年组织运营风险评估并形成报告。

1.6.2 联系方式

如对本《电子签名电子认证业务规则》有任何疑问，请与 GZSK 安全策略委员会联系：

CPS 发布地址：https://www.aiotca.com/

联系电话：15666777090

联系部门：综合中心

联系人：滕靖国

邮件：business@sinocipher.com

数据中心地址：江苏自贸区南京片区浦滨路 320 号科创一号大厦 A 座 812 室

运营中心地址：山东省济南市历下区经十路 9777 号鲁商国奥城 4 号楼 20 层 2007

1.6.3 CPS 批准程序

本《电子签名电子认证业务规则》由安全策略委员会主任及委员组织相关人员拟定文档,提交安全策略委员会审议,审议通过后向行业主管部门报备并发布。

1.6.3.1 CPS 编制小组

安全策略委员会召开会议，指定相关部门人员成立 CPS 编写小组。CPS 编写小组根据《电子签名电子认证服务业务规则规范》编写电子签名 CPS,在编写过程中应及时向安全策略委员汇报制定进展，并就有关问题召集相关人员讨论。

1.6.3.2 审批

CPS 编写小组完成编写后，提交安全策略委员会进行评审。安全策略委员会会议通过后，即成为正式版本。

1.6.3.3 发布

在公司官方网站上发布

1.6.3.4 变更

因国家的政策法规、技术要求、标准发生变化以及公司业务发展的需要，要对本 CPS 进行修订时，可由安全策略委员会成员提议修改、安全策略委员会指定编写小组进行编写修改、提交安全策略委员会审核。经过批准通过后，按照前述方式进行对外发布。

1.6.3.5 备案

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，本 CPS 经安全策略委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

1.7 定义和缩写

1) 公钥基础设施（public key infrastructure（PKI））：基于公钥密码技术实施的具有普适性的基础设施，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务。
2) 加密（encipherment/encryption）：对数据进行密码变换以产生密文的过程。
3) 加密证书（encipherment certificate/exchange certificate）：用于证明加密公钥的数字证书。
4) 密码模块（cryptographic module）：实现密码运算功能的、相对独立的软件、硬件、固件或其组合。
5) 密码算法（cryptographic algorithm）：描述密码处理过程的运算规则。
6) 密钥 key（public key infrastructure（PKI））：控制密码算法运算的关键信息或参数。
7) 证书更新（Certificate update）：指在不改变密钥的情况下，用一个新证书来代替旧证书的过程。
8) 密钥更新（key update）：用一个新密钥来代替旧密钥的过程，通常指证书与密钥同时更新。
9) 密钥恢复（key recovery）：将归档或备份的密钥恢复到可用状态的过程。

10) 签名证书（signature certificate）：用于证明签名公钥的数字证书。

11) 身份鉴别/实体鉴别（authentication/entity authentication）：确认一个实体所声称身份的过程。

12) 数字签名（digital signature）：签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

13) 数字证书（digital certificate）：也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

14) 私钥（private key）：非对称密码算法中只能由拥有者使用的不公开密钥。

15) SM2 算法（SM2 algorithm）：一种椭圆曲线公钥密码算法，其密钥长度为256 比特。

16) 证书撤销列表（certificate revocation list （CRL））：由证书认证机构（CA）签发并发布的被撤销证书的列表。

17) 证书认证机构（certification authority（CA））：对数字证书进行全生命周期管理的实体。也称为电子认证服务机构。

18) 证书依赖方（certificate dependent）：依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是也可以不是一个证书持有者。

19) 高等级电子签名认证证书:（enhanced electronic signature certificate）：适用于涉及生命健康、财产权益等高风险场景的电子签名认证证书。

20) 基础级电子签名认证证书:（qualified electronic signature certificate）：适用于除高等级证书规定场景外的其他电子签名场景的证书。

21) 缩写

CA	电子认证服务机构
CP	证书策略
CPS	电子认证业务规则
CRL	证书撤销列表

IETF	互联网工程任务组
LDAP	轻量目录访问协议
OCSP	在线证书状态查询协议
PKI	公钥基础设施
LRA	证书注册受理点

2 信息发布与信息管理

2.1 认证信息的发布

本机构CA证书链、CRL、电子认证业务规则、依赖方协议、业务办理指南、投诉处理政策、投诉方式等，可从本机构公司网站（GZSK网站：https://www.aiotca.com/）获取。

用户证书可从本机构的目录服务或证书服务站点查询获取。已被撤销的证书信息可从目录服务或CRL站点查询获取。证书的状态（有效、撤销）可通过OCSP查询获取。

实际的应用场景中，用户证书和证书状态查询获取方式可以是以上方式的全部，也可以是其中之一，视具体的安全需求而定。

根据主管部门要求完成与国家电子认证服务管理平台的技术对接，完成机构及服务信息的备案，实现根据证书唯一编码、订户身份信息等维度查询本机构已签发证书列表的功能。

2.2 发布的时间或频率

《本机构电子认证业务规则》的变更，应在审批通过之日起十天内发布。一经发布，即时生效。对数字证书的订户及证书申请人均具备约束力，对具体个人不另行通知。

证书的发布：在证书签发时，本机构自动将该证书发布到目录服务。

CRL的发布：CRL发布频率为24小时一次，必要时支持人工发布最新CRL。

OCSP对证书状态的查询是及时的。

建立信息更新机制，信息发布动态管理流程，确保CPS、CP、CA证书等公开信息在内容发生变更后1个工作日内完成更新并对外发布。

2.3 信息库访问控制

本机构允许公众通过官方网站自由查询和访问已公开发布的 CP、CPS 及 CA 证书等公开信息。

而 CA 机构数据库中的其他非公开数据，仅限经授权的 RA/CA 管理员方可访问和查询。

3 身份标识与鉴别

3.1 身份查验通用要求

在受理证书申请时，GZSK 对订户和/或受托人进行告知、身份确认、意愿记录和协议签署，并为每个证书的申请建立独立的身份查验记录。身份查验义务由 GZSK 自行完成，未委托给外部机构或个人（非属同一法人主体的机构视为外部机构）。

3.2 初始身份确认

3.2.1 订户告知

3.2.1.1 告知内容

订户申请证书时，GZSK 告知以下内容：

a) 订户的权利和义务；

b) 服务收费的项目和标准；

c) 电子签名认证证书、电子签名的使用条件；

d) 信息安全保障措施；

e) CA 和订户的责任划分；

f) 订户签名私钥的存储方式及安全要求；

g) 订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利

用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

3.2.1.2 告知方式

高等级证书采用面对面、电话、视频或主管部门认可的其他方式告知，并保留告知记录。

基础级证书可采用高等级证书的告知方式，或采用强制阅读、短信、邮件等方式告知，并保留告知记录。

3.2.2 证明拥有私钥的方法

订户签名密钥对应按照 CPS6.2.1 的要求，由订户自己生成。

GZSK 通过以下两个条件来证明证书持有者对私钥的持有：

a. 通过证书请求中所包含的数字签名来证明证书持有者持有与注册公钥对应的私钥。
b. 订户在客户端生成签名密钥公私钥对；
c. 订户使用签名密钥私钥对证书请求信息签名，并连同签名密钥公钥一起提交 CA 系统；
d. CA 使用订户公钥验证该订户签名。

订户必需妥善保管自己的私钥，即只有订户可以持有自己的私钥。

如以上条件满足，则证书持有者可以被视作其私钥的唯一持有者。

3.2.3 组织机构身份的鉴别

机构订户需提供能提供真实身份的有效证件，配合 GZSK 完成查验。

有效证件指法律法规或国家有关文件规定证件，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等。

3.2.3.1 机构高等级证书

法人代表机构申请证书，GZSK 通过以下方式查验：

a)通过证件机读工具、权威数据库或主管部门认可的其他方式查验法定代表人身份证件的真实性和有效性；

b)通过面对面、远程人工面对面、生物特征（如活体人脸、指纹、声纹、掌纹等生物识别技术的应用，选择一种即可）验证或主管部门认可的其他方式进行查验；

对于机构高等级证书，受托人代表机构申请证书，GZSK 通过以下方式查验：

a)通过证件机读工具、权威数据库或主管部门认可的其他方式查验法受托人身份证件的真实性和有效性；

b)查验机构加盖公章的有效书面授权证明，核对受托人身份与授权文件信息一致;

c）通过面对面、远程人工面对面、生物特征验证或主管部门认可的其他方式进行查验;

d）通过机构对公账户随机金额打款验证方式进行查验。

3.2.3.2 机构基础级证书

法人代表机构申请证书，GZSK 通过以下方式查验：

a)通过证件机读工具、权威数据库或主管部门认可的其他方式查验法定法人身份证件的真实性和有效性；

b)采取高等级证书的身份查验方式核验；通过运营商三要素核对姓名、证件号码、手机号的一致性，并使用手机号的随机短信验证码核验;通过银行卡四要素核对姓名、证件号码、银行卡号、银行预留手机号的随机短信验证码核验；通过申请人持有的有效电子签名认证证书签名验证;通过主管部门认可的其他核验方式；

对于机构基础级证书，受托人代表机构申请证书，GZSK 通过以下方式查验：

a)通过证件机读工具、权威数据库或主管部门认可的其他方式查验法受托人身份证件的真实性和有效性；

b)查验机构加盖公章的有效书面授权证明，核对受托人身份与授权文件信息一致;

c）采取高等级证书的身份查验方式核验；通过运营商三要素核对姓名、证件号码、手机号的一致性，并使用手机号的随机短信验证码核验;通过银行卡四要素核对姓名、证件号码、银行卡号、银行预留手机号的随机短信验证码核验；通过申请人持有的有效电子签名认证证书签名验证;通过主管部门认可的其他核

验方式。

3.2.4 个人身份的鉴别

订户需提供能表明其真实身份的有效身份证件，配合 CA 机构完成查验。

个人有效身份证件指政府部门签发的合法有效证件，包括但不限于:中国居民身份证、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、护照、外国人永久居留身份证、军官证。

GZSK 通过证件机读工具、权威数据库或主管部门认可的其他方式查验订户身份证件的真实性和有效性。

当订户委托他人代为办理时，GZSK 应查验订户本人签署的有效书面授权证明，要求受托人出示其有效身份证件或有效身份证件信息，并查验订户和受托人的身份证件或身份资料。

对于个人高等级证书，GZSK 通过以下方式查验：

a)面对面查验；

b)远程人工面对面查验；

c)生物特征验证（如活体人脸、指纹、声纹、掌纹等生物识别技术的应用，选择一种即可）查验；

d）主管部门认可的其他方式进行身份查验。

对于个人基础级证书，GZSK 可采用以下方式之一进行身份查验:

a)采取高等级证书的身份查验方式验证;

b)通过运营商三要素核对姓名、证件号码、手机号的一致性，并使用手机号的随机短信验证码核验;

c)通过银行卡四要素核对姓名、证件号码、银行卡号、银行预留手机号的随机短信验证码核验；

d)通过申请人持有的有效电子签名认证证书签名验证;

e)通过主管部门认可的其他核验方式。

3.3 订户意愿确认

意愿内容包括不限于：

a)订户身份信息:

b)CA 的信息:

c)签名私钥保存方及其保存义务:

d)订户对电子签名的法律责任:

e）订户对上述 a)至 d)项内容已充分知晓并同意的明确意愿表示。

个人高等级证书意愿记录：现场办理时，通过面对面确认或手抄提示语的方式，并采用录音录像或通过主管部门认可的其他方式记录订户意愿；远程办理时，通过音视频或通过主管部门认可的其他方式确认并记录订户意愿。

个人基础级证书意愿记录：与个人高等级证书相同的方式；采用强制阅读、短信或邮件确认等电子方式。

机构高等级证书意愿记录：法定代表人申请时，按照个人高等级证书意愿记录方式确认机构法定代表人的意愿；受托人申请时，查验加盖机构公章的授权文件，按照个人高等级证书意愿记录方式确认机构受托人的意愿。

机构基础级证书意愿记录：法定代表人申请时，按照个人基础级证书意愿记录方式确认机构法定代表人的意愿；受托人申请时，查验加盖机构公章的授权文件，按照个人基础级证书意愿记录方式确认机构受托人的意愿。

3.4 订户协议

本机构与订户签署或确认订户协议，对电子认证服务相关事项进行约定。协议内容涵盖证书使用规则、双方权利义务、服务费用、信息安全要求、责任承担及私钥保护，协议包含§3.2.1.1 要求的内容，并明确订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

本机构通过适当方式向订户展示电子认证服务协议，经订户确认后协议生效，确认方式包括纸质签字或盖章、在线勾选或点击确认，以及其他表明认可协议的操作形式。本机构完整保存订户协议确认过程及相关记录，以满足后续查询、审计和追溯的需要。

3.5 未验证的订户信息

本机构所签发的数字证书中不包含任何未经验证的订户信息，所有身份信息均经过严格、合规的验证程序：

1) 个人证书中的姓名、身份证号码等信息，均通过国家法律认可的有效身份证件（如居民身份证）进行实名核验；
2) 机构名称依据有效的营业执照进行核实确认；
3) 电子邮箱地址通过本机构系统自动发送随机验证码，由订户在申请过程中自行填写并回传，系统实时完成自动校验；
4) 机构内设部门名称及职务信息，须提供加盖单位公章的授权证明文件，经审核后予以确认。

上述验证机制确保了证书中所载信息的真实性、合法性与可追溯性，有效支撑数字证书在身份认证和安全应用中的可信性。

3.6 互操作要求

对于其他电子认证机构，可以与本机构进行互操作，但是必须符合本机构电子认证服务机构的《电子签名电子认证业务规则》要求。本机构目前没有签发其他交叉认证的证书。

3.7 命名

GZSK 严格按照《基于 SM2 密码算法的数字证书格式规范》要求为电子签名数字证书命名，不得使用匿名或假名。

3.7.1 名称类型

GZSK 签发的数字证书符合 X.509 V3 标准，根据证书类型的不同，签发的证书主体名字可能是个人名称、组织机构名称、部门名称、组织机构信息与个人信息组合体，域名、设备名称等，主体甄别名采用 X.500 的命名方式。

3.7.2 对名称意义化的要求

订户证书包含的命名应具有一定的代表性意义，需要填写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。

个人证书主体甄别名中的通用名是个人的真实姓名，证书扩展项中包含有效证件类型及其编号（或相关信息的映射，包括但不限于散列值、掩码等），作为标识订户的关键信息被鉴别和认证。

机构证书主体甄别名的通用名是机构的真实名称，证书扩展项中包含组织机构的有效证件类型及其编号，作为标识订户的关键信息被鉴别和认证。

3.7.3 订户的匿名或伪名

订户不能使用匿名、伪名申请证书。

3.7.4 理解不同名称形式的规则

DN 的命名规则由 GZSK 依照 X.500 甄别名命名规则定义。

证书主体 DN 项和部分扩展项编码规则如下:

代码	说明	示例
C	国家	CN
S	省份（可选）	北京
L	城市（可选）	北京
O	订户所在机构信息（可选）	XX 公司
OU	订户所在机构部门信息（可选）	XX 部门
CN	订户名称（个人姓名或机构法定名称）	张三/xx 公司
标准扩展 IdentifyCode	身份证号 / 机构代码	370105199001011234 /91320105MA12345678

3.7.5 名称的唯一性

GZSK 保证其为订户签发的证书，其主体甄别名，在 GZSK 的信任域内是唯一的。

3.7.6 商标的识别、鉴别和角色

GZSK 签发的订户证书的主体甄别名中不包含商标名。

4 证书生命周期操作要求

4.1 通用要求

本机构应在 CPS 中明确界定电子认证服务各参与方的责任，确保权责清晰、管理规范。相关责任包括但不限于以下内容：

1) CA 机构负责建立、运营和维护安全可靠的注册通道，保障订户身份核验及证书申请流程的合规性与安全性；
2) CA 机构负责与订户签署《电子认证服务协议》，明确双方在证书申请、使用、管理及安全义务等方面的约定；
3) CA 机构建立健全的信息记录与存档机制，对注册、审核、签发、吊销等全过程的关键数据和操作日志进行妥善保存，确保可审计、可追溯。
4) 订户应如实、准确、完整地提供申请所需的身份及相关信息，并对其真实性、合法性承担相应责任；

上述责任划分旨在保障电子认证服务的安全性、可信性和合规性，所有参与方均须严格遵守。

4.2 证书申请

4.2.1 信息告知

GZSK 在本 CPS 中阐述了受理证书申请的所有流程及要求，并通过网站、现

场咨询、热线电话等方式告知证书申请者及订户所必须提交的材料和办理流程。

订户告知方式和内容参见§3.2.1。

对于个人证书，申请者到GZSK受理点填写或到GZSK网站下载填写《证书业务申请单》，并提供个人身份证明文件及其复印件一份，例如:中国居民身份证、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、护照、外国人永久居留身份证、军官证等。

政府、机构部门中的个人申请证书时，还需提交个人所在单位许可授权证明(申请表加盖单位公章)及单位证明文件:如果是委托申请的，还需提供经办人被授权证明，证明代表他人提交证书申请的人是经过单位授权的。

对于机构证书，申请者填写《证书业务申请单》，并提供单位对经办人的授权委托证明，单位的企业法人营业执照、企业法人有效身份证明文件复印件，经办人的身份证及其复印件和GZSK可能需要的其他文件。

任何需要在各类应用中采用数字证书进行真实身份标识和鉴别，实现信息保密，并提供信息源发性证明、完整性保障和抗抵赖的个人或机构，都可以申请个人证书或机构证书。

组织机构申请机构证书时，由机构授权人员申请。

设备证书由域名或设备拥有机构，或获得域名或设备使用授权的机构中的授权人申请。

4.2.2 申请的提交

证书申请应由证书持有者或相应的授权人提交。

非证书持有者代表组织机构进行批量证书申请的还应获得该组织的授权。

GZSK CA提供现场、邮寄等多种方式的证书受理申请。

4.2.3 执行识别与鉴别功能

当GZSK接收到订户的证书申请后，应按本CPS第3.2节“初始身份确认”的要求，对订户进行初始身份确认。

4.2.4 证书申请批准和拒绝

符合以下所有条件，视为批准证书申请：

1、申请满足本 CPS 第 3.2 节“初始身份确认”的要求；

2、订户已经签订订户协议；

3、订户已按照规定支付相关费用。

符合以下任意条件，视为拒绝证书申请：

1、申请不满足本 CPS 第 3.2 节“初始身份确认”的要求；

2、订户不接收或申明反对订户协议的内容；

3、订户未按照规定支付相关费用。

4.2.5 处理证书申请的时间

GZSK 将在合理的时间内完成证书申请处理。在订户提交的资料齐全且审核通过的情况下，1 个工作日内处理完成。

4.2.6 对拒绝证书申请原因说明

符合以下任意条件，视为拒绝证书申请：

1、申请不满足本 CPS 第 3.2 节“初始身份确认”的要求；

2、订户不接收或申明反对订户协议的内容；

3、订户未按照规定支付相关费用。

4.3 证书签发

4.3.1 证书签发中 CA 的行为

线下面对面方式：在订户申请通过鉴别后，本机构业务操作员录入订户申请信息；本机构业务操作员审核通过后；CA 系统在获得证书签发请求后，对信息进行鉴别与解密，对于有效的证书签发请求，CA 将签发订户证书。

线上方式：本机构和订户之间建立安全通道，订户通过 CPS 第 3.2 节“初始

身份确认”方式身份鉴别通过后，向 CA 系统提交签发请求；CA 系统在获得证书签发请求后，对信息进行鉴别与解密，对于有效的证书签发请求，CA 将签发订户证书。

4.3.2 CA 通知证书申请者证书的签发

订户证书签发完成后，将直接签发结果通过以下方式通知订户：

1) 通过认证应用工具进行信息提示;
2) 通过信函、站内信或电子邮件发送:
3) 通过短信通知:
4) 通过电话通知:
5) 当面通知或通过实时视频等相当于面对面的方式通知;
6) 通过主管部门认可的其他方式。

并向订户提供获取证书的方式，包括面对面、远程线上建立安全通道下载。

4.4 证书接收

4.4.1 证书接受：

线下：本机构 CA 代替订户下载证书，下载的证书将保存在安全的数字证书载体中（如智能密码钥匙等），当订户接受了该数字证书载体同时在载体签收单签字即代表订户接受了证书。

线上：订户通过本机构和订户之间建立安全通道下载证书，证书下载成功表明订户已接收证书，系统记录包括接受时间、方式、操作人等信息。

4.4.2 证书拒绝：

线下：如果订户拒绝接受该证书可以通过拒绝接受该数字证书载体同时拒绝在载体签收单签字。

线上：如果订户拒绝接受该证书可以拒绝下载该证书或直接写明拒绝理由，证书超过 2 天未下载视为订户拒绝接受，系统记录包括接受时间、方式、操作人

等信息。

4.4.3 CA 对订户的通告

无论是拒绝还是批准订户的证书申请，本机构有义务告知订户申请结果。可通过面对面、电话、电子邮件、短信或其他本机构认为安全可行的方式对订户进行通告。

4.4.4 电子认证服务机构在颁发证书时对其他实体的通告

对于本机构签发的证书，本机构不通知其他实体。其他实体可以通过目录服务自行查询。

4.4.5 电子认证服务机构对证书的发布

除非与证书订户间有特别的约定，本机构在签发完证书后，会将证书发布到目录服务器中。本机构采用主、从目录服务器结构来发布所签发的证书。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，供订户和依赖方查询和下载。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在使用证书和私钥时必须遵守法律、本 CPS 以及订户协议的要求，妥善保存其私钥，避免未经授权的使用。订户应当对私钥的丢失、泄露或未经授权使用负责。

对于签名证书，其私钥可以用于数字签名，对于加密证书，其私钥可以用于数据解密。在证书到期或被撤销后，必须停止使用该证书及对应私钥。

CA 建立便捷的外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失密或证书被盗用等异常情况。

4.5.2 信赖方公钥和证书的使用

当依赖方接收到签名的信息后，有义务确认以下操作：

1） 获得数字签名对应的证书及信任链；

2） 验证证书的有效性，确认该签名对应的证书是否在有效期内或被撤销；

3） 确认该签名对应的证书是依赖方信任的证书；

4） 确认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，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。

4.6 证书续期

4.6.1 证书续期的情形

证书订户可在证书到期前 90 天内到本机构进行证书续期的申请。申请证书续期不需要填写信息，系统自动获取所有所需信息。证书过期后订户必须重新申请新证书。

4.6.2 请求证书续期的实体

请求证书续期的实体为证书订户。

4.6.3 证书续期请求的处理

对于证书续期的请求，需验证和鉴别以下几个方面：

1、订户必须实际持有原证书的私钥，并且原证书由本机构所签发；

2、验证证书有效性；

3、基于原注册信息进行身份鉴别；

4、订户已按照规定支付相关费用。

以上验证和鉴别通过后才可签发证书。

4.6.4 颁发新证书时对订户的通告

同§4.3.2。

4.6.5 构成接受续期证书的行为

同§4.4。

4.6.6 电子认证服务机构对续期证书的发布

同§4.4.5。

4.6.7 电子认证服务机构对其他实体的通告

同§4.4.4。

4.7 证书密钥更新

证书密钥更新是指不改变证书除有效期外其他任何信息的情况下，订户生成一对新密钥并申请为新公钥签发一张新证书。

证书密钥更新会造成使用原密钥加密的文件或数据无法解密，因此，订户在申请证书密钥更新前，必须确认使用原密钥加密的文件或数据已经解密，由此造成的损失，GZSK CA 不承担责任。

4.7.1 证书密钥更新的情形

证书密钥更新包括但不限于以下情形：

1、私钥泄露或怀疑密钥不安全；

2、证书到期；

3、私钥损坏；

4、其他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

请求证书密钥更新的实体为证书订户。

4.7.3 证书密钥更新请求的处理

若证书私钥泄露、证书到期、私钥损坏，应按照 3.2.4 节要求核验订户身份和申请信息；其他情形同§4.6.3。

4.7.4 颁发新证书时对订户的通告

同§4.3.2。

4.7.5 构成接受续期证书的行为

同§4.4。

4.7.6 电子认证服务机构对续期证书的发布

同§4.4.5。

4.7.7 电子认证服务机构对其他实体的通告

同§4.4.4。

4.8 证书变更

证书变更是指证书订户提供的注册信息发生改变，重新生成一对新密钥并申请为新公钥签发一张新证书。

证书变更会造成使用原密钥加密的文件或数据无法解密，因此，订户在申请证书变更前，必须确认使用原密钥加密的文件或数据已经解密，由此造成的损失，GZSK 不承担责任。

4.8.1 证书变更的情形

证书变更包括但不限于以下情形：

1、证书信息发生改变；

2、可能导致证书变更的其他情形。

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 证书变更请求的处理

同§3.2.4。

4.8.4 颁发新证书时对订户的通告

同§4.3.2。

4.8.5 构成接受续期证书的行为

同§4.4。

4.8.6 电子认证服务机构对续期证书的发布

同§4.4.5。

4.8.7 电子认证服务机构对其他实体的通告

同§4.4.4。

4.9 证书撤销与冻结

4.9.1 证书撤销的条件

如有下列情况中的任何一种情况发生，则订户的证书将被撤销：

1. 订户信息发生变化，且未申请证书变更的；
2. 订户提供的信息不真实；
3. 订户没有或无法履行有关规定和义务；
4. .GZSK CA、注册机构或最终订户有理由相信或强烈地怀疑一个订户的私钥安全已经受到损害；
5. 和订户达成的订户协议已经终止；
6. 订户请求撤销其证书；
7. 证书仅用于依赖方主导的系统并由依赖方提出撤销申请的；
8. 法律、行政法规规定的其他情形。

4.9.2 证书撤销的发起

以下实体可以请求撤销订户证书：

1、本 CA 依据本 CPS 第 4.9.1 节可以要求撤销订户证书。

2、证书订户可以申请撤销自己的订户证书。

3、政府主管部门及其他权力机关可以依法撤销订户证书。

4、依赖方及其他第三方有充分合理的理由，可提交书面报告，申请撤销订户证书。

4.9.3 证书撤销的处理

订户提交证书业务申请表，并注明撤销的原因。本 CA 按照本 CPS 第 3.2 节“初始身份确认”对订户提交的证书撤销申请进行审核。

证书订户主动申请撤销证书，同本 CPS 第 4.2 节。

当出现被动撤销的情形时，GZSK CA 将以电话、书面、短信等形式通知证书订户，告知拟撤销的证书内容、撤销原因、撤销操作时限等事项，在确认订户收

到撤销通知后予以冻结，在撤销请求宽限期后订户证书将予以撤销。

4.9.4 撤销请求宽限期

在主动撤销的情形下，无宽限期。

在被动撤销的情形下，订户在收到撤销通知后的 3 个工作日内可向本 CA 提出申辩理由，本 CA 将会对申辩理由进行评估，若确认其理由正当则不予以撤销，若 3 个工作日未回复或申辩理由不被接受，则订户证书将予以撤销。

4.9.5 电子认证服务机构处理撤销请求的时限

在本 CPS 第 5.9.4 节所规定的撤销请求宽限期后的 24 小时内撤销证书将被处理完毕。

4.9.6 依赖方检查证书撤销的要求

依赖方在信任此证书前应通过 CRL 或 OCSP 任一方式检查证书的有效性，确认证书未被撤销。

4.9.7 CRL 发布方式及频率

GZSK 可采用实时或定期的方式发布 CRL。发布 CRL 的频率根据证书策略确定，每 24 小时自动发布最新 CRL，也可人工发布最新 CRL。

4.9.8 CRL 备份及频率

本机构负责对 CRL 进行备份，最长时间间隔不得超过 24 小时，备份文件保存时间不少于证书失效后 10 年。

4.9.9 在线状态查询要求

订户可以自由进行在线状态查询，本 CA 不设置任何读取权限，本 CA 提供 POST 方式的 OCSP 查询服务。

4.9.10 撤销信息的其他发布形式

证书撤销信息可以通过 CRL 或者 OCSP 服务获得。订户可通过本机构官网下载最新的 CRL 获取 CRL 信息。

4.9.11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遭受安全威胁时，应及时提出证书撤销请求。

4.9.12 证书冻结的情形

如有下列情况中的任何一种情况发生，则订户的证书将被冻结：

1）订户书面申请冻结数字证书；

2）订户怀疑证书私钥遭到泄露或损坏；

3）订户的资信暂时出现问题或者无法证明其资信；

4）订户仍未按照规定支付相关费用；

5）法律、行政法规规定的其他情形。

4.9.13 请求证书冻结的实体

以下实体可以请求冻结订户证书：

1、本机构依据本 CPS 第 4.9.13 节可以要求冻结订户证书

2、证书订户可以申请冻结自己的订户证书。

3、政府主管部门及其他权力机关可以依法冻结订户证书。

4、依赖方及其他第三方有充分合理的理由，可提交书面报告，申请冻结订户证书。

4.9.14 冻结请求的流程

证书订户主动申请冻结证书，同本 CPS 第 4.2 节。

当出现被动冻结的情形时，本 CA 将以电话、书面、短信等形式通知证书订

户，告知拟冻结的证书内容、冻结原因、冻结操作时限等事项，在确认订户收到冻结通知后予以冻结。

4.9.15 冻结的期限限制

在主动冻结的情形下，无宽限期。

在被动冻结的情形下，订户在收到冻结通知后的 3 个工作日内可向本 CA 提出申辩理由，本 CA 将会对申辩理由进行评估，若确认其理由正当则撤销冻结。

4.9.16 电子认证服务机构处理冻结请求的时限

在本 CPS 第.9.16 节所规定的冻结请求宽限期后的 24 小时内冻结证书将被处理完毕。

4.10 证书状态信息服务

4.10.1 操作特征

证书状态可以通过 OCSP 服务获得。

4.10.2 服务可用性

本 CA 提供 7*24 小时不间断证书状态查询服务。

4.10.3 可选特征

无规定。

4.10.4 服务可用率

本 CA 提供不间断证书状态查询服务，确保服务可用率不低于 99%。

4.11停止使用认证服务

4.11.1停止订户服务的情形

出现以下情形之一时，本机构应停止为订户提供服务：

a）证书有效期满，订户不再进行证书更新、证书变更或证书密钥更新；

b）在证书有效期内证书被撤销后，且订户未进行证书变更或证书密钥更新；

c）订户提出停止服务申请；

d）订户违反法律法规或本 CPS 及订户协议的相关规定。

4.11.2处理停止服务请求的时限和方式

本机构应在确认停止服务情形成立后，及时处理停止服务请求：

a）撤销订户证书，如果证书未到有效期，将证书信息加入证书撤销列表（CRL），并在规定时限内发布；

b）如果本机构受订户委托保管订户签名私钥的，应安全销毁订户签名私钥及其相关备份；

c）妥善保存订户相关数据，保存期限不低于证书失效后五年；

d）根据订户要求或法律法规规定，依法处理用户数据的保存、销毁或转移。

4.11.3责任延续条款

停止服务后，本机构对订户在证书有效期内使用证书所产生的电子签名行为，仍依法承担相应的证明责任和法律责任。

4.11.4操作记录

本机构应完整记录停止服务的操作过程，包括停止事由、处理时间、操作人员、处理方式等信息，相关记录应至少保存至证书失效后五年，以满足后续查询、审计和追溯需要。

4.12 密钥托管与恢复

本机构仅涉及根密钥和用户加密密钥的管理，不涉及用户签名密钥托管服务。依据国家密码管理部门的相关规定，提供订户加密证书密钥的集中产生、保存和恢复。

4.12.1 密钥托管与恢复的策略与行为

本机构的根密钥保存在屏蔽机房中的服务器密码机中，采用(3,5)门限机制完成根密钥的备份恢复，保障密钥的安全。

本机构订户的加密密钥托管需满足《中华人民共和国电子签名法》可靠电子签名的要求。

订户加密证书密钥对可以由密钥管理中心系统集中安全产生和保存，密钥恢复是一种严格受控的过程，只有在如下情况下才允许进行密钥恢复：

- 证书持有者提出申请；
- 国家执法、司法机构因执法、司法的需要；
- 国家其他管理部门管理需要。

密钥恢复只有在必需的情况下才能进行，并且申请要提出充分的理由和提供有关文件、材料。

4.12.2 会话密钥的封装与恢复的策略与行为

会话密钥是指用户在使用证书建立加密通道时临时生成的加密密钥，该密钥由应用环境来决定使用，本机构不对其进行保存和恢复。

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

山东公众数科数字科技有限公司电子认证服务整体机房，位于山东自贸区南京片区浦滨路320号科创一号大厦A座812，占地面积160平方米。机房按功能分为四个区域，分别是公共区、服务区、核心区和管理区。

整体机房严格遵照国家机房相关规范标准建设，采用全模块化结构设计，符合国家相关机房标准。

其中，核心区为屏蔽机房，屏蔽效能达到BMB 3-1999《处理涉密信息的电磁屏蔽室的技术要求和测试方法》中C级要求。

5.1.2 物理访问

山东公众数科数字科技有限公司CA 中心机房全部区域均采用了门禁系统。CA机房、密管机房均需使用双人双因子认证才可进入。同时，多个门之间采用联动机制，保障区域间的严格隔离。

5.1.3 电力与空调

山东公众数科数字科技有限公司机房配置1套40kVA模块化UPS系统。

根据 GB 50462-2015《数据中心基础设施施工及验收规范》的有关规定，机房的温湿度控制符合相关标准。通过设备照明、人体体温及建筑热量的估算，采用美的工业空调工作。

5.1.4 水患防治

山东公众数科数字科技有限公司配备了防水检测装置，发现水害能及时报警。

5.1.5 火灾防护

机房消防报警系统采用柜式七氟丙烷自动灭火装置。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用户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，实现系统实时检测、定时监测和系统的手动、自动控制模式的设定，并完成了系统设计的有关各种联动动作。

5.1.6 介质存储

对于存放重要数据的存储介质，GZSK 制定了专门的管理控制制度，以防止重要信息的泄露与人为故意产生的危害和破坏。

5.1.7 废物处理

对于敏感的文件资料（包括纸介质、光盘或软盘废物等）抛弃前要进行粉碎处理；

对于存储或传输信息的介质，在抛弃前要做不可读取处理；

对于涉密介质在抛弃前要根据生产商的指导做归零处理；

对于加密机等重要设备废弃根据加密机管理办法销毁。

5.1.8 异地备份

山东公众数科数字科技有限公司采用了每天完全备份与增量备份相结合的方式对生产系统数据和信息进行备份。

制定了备份数据收集、保管、押运、恢复管理策略，确保备份数据的安全，防止泄漏和未经授权使用。每月对备份数据同城异地保管。并会定期检查备份系统和设备的可靠性和可用性，定期检查备份介质可靠性和数据完整性。

异地备份地点为：南京市应天大街 765 号办公楼五层，距离机房 30 公里。

5.2 操作过程控制

5.2.1 可信角色

在电子认证服务过程中，能从本质上影响证书生命周期操作的职位，都被视为可信角色，包括：

系统管理员:负责系统策略配置、用户与权限管理等;

技术运维员:负责物理环境、网络、服务器及系统软件的日常监控与维护等;

数据库管理员:负责数据库进行日常运维、性能优化及数据备份等;

系统审计员:负责系统和网络日志的审计、管理、审计报告生成等;

密钥管理员:负责根证书密钥材料管理、根证书密钥生存周期管理等;

业务操作员:负责证书申请的受理、审核，订户的身份与意愿鉴证:

客户档案管理员:负责客户证书相关档案资料的归档与保密等;

运营审计员:负责对客户签发、客户服务等核心业务进行独立审计等;

其他人员:对公司运营有重要影响的其他管理人员。

5.2.2 职责分离

所有涉及关键操作(密钥管理、审计、鉴证、系统管理)的角色实现双人操作或复核机制;涉及业务连续性相关操作(运维、鉴证、审计等)的角色按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作;禁止同一人员掌握可独立完成“发起、审批、执行、审计”全流程的任何组合，以下角色禁止相互兼任:

1) 系统管理员、技术运维员、数据库管理员、系统审计员之间不得兼任;

2) 同一证书业务的录入与审核环节不得由同一业务操作员完成;

3) 业务操作员、客户档案管理员、运营审计员之间不得兼任:

4) 密钥管理员不得与系统管理员、技术运维员兼任:

5) 密钥管理员不宜与除策略管理机构成员外的其他可信角色兼任。

5.3 人员控制

5.3.1 资格、经历和无过失要求

成为 GZSK 可信角色的人员资格要求如下：

1、遵守国家法律法规、服从 GZSK 的统一安排及管理；

2、具有良好的个人素质、修养及认真负责的工作态度；

3、具有良好的团队合作精神；

4、无违法犯罪记录。

5.3.2 技能要求

成为 GZSK 可信角色的人员技能要求如下：

1) 熟悉国密算法（SM2/SM3/SM4）和 PKI 体系，了解数字证书原理与 X.509 格式；

2) 掌握 CA/RA/KMS 系统的基本操作与运维，能配合完成证书签发、吊销、查询等流程；

3) 了解 GM/T 0034、GM/T 0038 等密码行业标准及《电子认证服务管理办法》等法规；

4) 具备基本的 Linux 系统操作和网络安全知识，能使用密码设备（如服务器密码机）；

5) 责任心强，注重合规与安全，能严格执行双人操作、权限分离等管理要求。

5.3.3 背景审查程序

GZSK 行政人事部需对可信人员进行相关工作背景调查。

调查程序包括：

1、对应聘人员的个人资料予以收集，提供包括但不限于履历、毕业证书、学位证书、资格证等相关证明。

2、通过电话、信函、网络等形式对其提供的资料真实性进行鉴定；

3、通过现场考核、日常观察等方式进行考察；

4、调查结束与可信人员签订保密协议。在职期间持续验证人员的可信度和工作能力。

5.3.4 培训要求

为了使员工更好地胜任工作，需要对员工进行必要的岗前培训和工作中的再培训，培训内容包括但不限于：

1、电子签名电子认证业务规则；

2、证书策略和电子认证业务规则；

3、PKI/CA 基本知识；

4、电子签名法和相关规章标准；

5、公司体系制度和相关文件。

GZSK 根据需要每年组织多次培训，每年至少接受一次培训，覆盖所有可信角色，每人每年培训时长不少于 20 学时，并通过考核。

5.3.5 工作岗位轮换周期和顺序

GZSK 根据公司工作情况安排制定在职人员的工作岗位轮换周期和顺序。

5.3.6 未授权行为的处罚

GZSK 根据公司相关安全管理规定对未授权行为进行处罚，包括解除或终止劳动合同、调岗、批评教育等方式，这些处罚应当符合法律法规要求。

5.3.7 独立合约人的要求

对于不属于GZSK内部工作人员，但从事与GZSK业务有关工作的独立合约人，GZSK 要求如下：

1、合约档案必须备案管理。

2、统一岗前培训和工作中的再培训。

独立合约人不承担属于可信人员的职责。

5.3.8 提供给员工的文档

提供给员工的文档包括培训资料和员工手册。

5.3.9 每个角色的识别与鉴别

GZSK 在雇用一个可信角色之前将会按照本 CPS 第 5.3.3 节的规定对其进行背景审查。

5.3.10 需要职责分割的角色

要求职责分割的角色包括但不限于：客户服务岗位、安全管理岗位、专业技术岗位、运行维护岗位。

5.4 审计日志程序

GZSK 建立了明确的审计日志程序：

1、确定 CA 中心的业务符合其 CPS 等文档中的定义。

2、CA 中心的管理人员需要定期对安全策略和操作流程的执行情况进行检查确认，进行运营风险评估。

3、必须准确完整地记录 CA 机构涉及运营条件和环境、密钥和证书生命周期管理的日志和事件。

4、各类日志、安全事件的记录应在安全和公正的情况下以自动或手动方式产生，并定期归档。授权安全管理人员定期检阅记录和跟进有关事项。

5、建立监测 CA 系统访问的检测系统，保证非授权的访问能够被发现。

5.4.1 规定事件记录的类型

GZSK 记录的日志信息包括但不限于以下类型：

1、CA 中心应对注册系统和证书受理操作的相关授权记录及管理记录；

2、密钥生成、备份、存储、撤销、归档和销毁管理；

3、密码设备生命周期管理；

4、证书申请、密钥更新、证书变更和证书撤销管理；

5、证书签发和 CRL 列表生成；

6、PKI 系统访问；

7、操作 PKI 系统和其他安全系统的行为；

8、安全配置文件变更；

9、系统崩溃、硬件故障和其他异常；

10、防火墙和路由器的工作情况，机房进出访问。

上述日志信息包括记录时间、设备名称、记录的实体身份、日志种类等。

5.4.2 规定事件记录的内容

1、事件记录应包括事件类型、发生时间、相关内容，以及操作身份的实体；

2、PKI 系统的审计事件记录应确保不能被篡改。

3、数字签名审核程序时成功或失败的指示符；

4、证书撤销时成功或失败的指示符；

5、引起事件发生的实体或操作员身份。

5.4.3 处理日志的周期

GZSK 每季度检查并审计相关操作日志、形成审计报告，对发现的安全事件采取相应的措施。

5.4.4 审计日志的保存期限

GZSK 所有审计日志永久保存。

5.4.5 审计日志的保护

GZSK 所有审计日志，采取严格的物理和逻辑访问控制策略，防止未授权的访问修改和删除。

5.4.6 审计日志备份程序

同本 CPS 第 5.1.8 节。

5.4.7 审计收集系统

GZSK 应用程序、网络和操作系统等都会自动生成审计数据和记录信息。

5.4.8 对导致事件实体的通告

对于审计收集系统中记录的事件，对导致该事件的个人、机构等主体，GZSK 会予以通告。

5.4.9 脆弱性评估

根据审计记录，GZSK 每季度进行系统、物理设施、运营管理、人事管理等方面的安全性评估，并根据评估报告采取措施。

5.5 记录归档

5.5.1 归档记录的类型

归档记录的类型包括：

1、审计日志、资料；

2、证书申请资料、身份验证资料、订户协议等；

3、电子认证政务电子认证业务规则、证书策略、电子认证业务规则、管理制度等；

4、人事档案、财务档案等。

5.5.2 归档记录的保存期限

GZSK 针对证书申请资料、身份验证资料、订户协议等业务纸质材料将保存

至证书失效后 10 年，电子资料永久保存。

5.5.3 归档文件的保护

对于电子形式的归档记录文件，确保只有被授权的可信任人员才允许访问存档数据，并通过适当的物理和逻辑访问控制防止对电子归档记录进行未授权的访问、修改、删除或其它操作。

对于书面形式的归档记录文件，GZSK 设有专门的档案管理人员对书面档案进行妥善保存，并有相应的查阅制度确保只有经批准的人员方可访问书面归档记录。

5.5.4 归档文件的备份程序

GZSK 所有存档的文件和数据库保存在 GZSK 的档案室。存档的数据库备份文件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。GZSK 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

GZSK 所有归档文件均有时间记录，由操作人员手工或系统自动添加。

5.5.6 归档收集系统

GZSK 应用程序、网络和操作系统各自收集归档文件，统一汇总管理。

5.5.7 获得和检验归档信息的程序

只有被授权的可信人员才能获得归档信息。当归档信息被恢复后会对其进行完整性检验。

5.6 电子认证服务机构根证书密钥更替

电子认证机构的CA证书即将到期时，只要CA密钥对的累计寿命没有超过本CPS第6.4.2节“证书操作期和密钥对使用期限”中规定的最大生命周期，那么CA证书可以使用原密钥进行更新，否则需要产生新的密钥对来签发新的CA证书。CA密钥变更时，必须保证整个证书链的平稳过渡。

5.7 损害和灾难恢复

5.7.1 事故和损害处理程序

GZSK制定了各种事故和损害的处理方案和应急预案，并规定了相应的处理程序。

5.7.2 计算资源、软件和/或数据的损坏

如果出现计算资源、软件或数据的损坏，应立即启动事故处理程序。

5.7.3 实体私钥损害处理程序

GZSK制定了私钥泄露的应急预案，其中明确规定了私钥泄露的内部处理流程、人员分工及对外通知处理流程。

对于实体私钥的损害，GZSK有如下处理要求和程序：

1) 当订户发现实体证书私钥损害时，订户必需立即停止使用其私钥，并立即通知GZSK撤销其证书。GZSK按CPS发布证书撤销信息。
2) 当GZSK发现订户的实体私钥受到损害时，GZSK将立即撤销证书，并通知订户，订户必需立即停止使用其私钥。GZSK按照CPS发布证书撤销信息。
3) 当GZSK的证书出现私钥损害时，GZSK将立即向国家密码管理局申请撤销CA证书并及时通过尽可能的途径通知依赖方，然后生成新的CA密钥对、签发新的CA证书。

5.7.4 灾难后的业务连续性能力

GZSK 有相应的业务持续计划，可确保灾难后的业务连续性能力。根据业务连续性计划，在灾难发生后的 48 小时内恢复电子认证服务，恢复点目标控制在 24 小时内。

5.7.5 业务连续性计划的保障方案

1) 建立 CA 中心的业务可持续性计划，并进行经常检查和更新，确保其持续有效。
2) 对 CA 系统中的重要部件制定完善的灾难恢复流程，并经常进行演练，确保流程操作的有效性。
3) 建立重要系统、数据、软件的备份，并存放在符合 CPS 要求的安全环境中，确保只有合理授权人员才可接触备份。
4) 定期测试备份设备、设施、后备电源等，确保其可用性。
5) 制定相关流程，对 CA 中心终止服务时的告知及业务承接做出计划。

5.7.6 灾难恢复演练

每年最少组织一次灾难恢复演练。

5.8 电子认证服务机构终止

当 GZSK 拟终止电子认证业务时，必须严格按照《中华人民共和国电子签名法》、《电子签名电子认证服务管理办法（试行）》及行业主管部门中对电子认证机构终止电子认证服务的规范要求进行相关工作。

5.8.1 终止情形

当本机构因技术性原因或商业原因需要终止电子认证服务时，应严格按照法律法规和主管部门要求，妥善处理终止事宜。

5.8.2 终止程序

1) 起草并发布 CA 终止声明，至少提前九十日通知证书订户、依赖方等相关实体，至少提前六十日向主管部门报告；
2) 确定具有资质的电子认证服务业务承接单位，并签署承接协议，明确约定承接机构的工作范围与责任；
3) 向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；
4) 停止证书状态服务并归档相关数据；
5) 停止其他电子认证相关服务并归档相关数据；
6) 停止密码设备并归档相关密钥数据；
7) 及时撤销或冻结业务管理员和业务操作员的操作权限；
8) 对所有存储文件记录进行整理和封存；
9) 对所有敏感文档和数据进行安全处理和封存；
10) 清除主机和密码硬件设备中的敏感数据；
11) 其他涉及 CA 运营的数据、密钥安全的操作；
12) 如有与订户电子签名认证证书签发、管理相关的外部合作机构，应在 CPS 中明确描述合作机构终止服务和通告相关的过程。

5.8.3 过渡安排

本机构终止服务前，应积极配合主管部门和承接单位完成业务平稳过渡，确保订户权益不受影响。终止过程中所有操作应完整记录并归档保存，保存期限不低于相关法律法规的要求。

5.8.4 责任延续

本机构终止服务后，对订户在证书有效期内使用本机构签发的证书所产生的电子签名行为，仍依法承担相应的证明责任和法律责任，直至证书有效期届满或承接机构依法承继相关责任为止。

5.9 重大事项报告

5.9.1 重大事件范围

重大事件包括但不限于以下情形：

a) 证书认证系统迁移或改造

符合以下任意之一：

1）机房迁移，或机房内服务区、管理区或核心区划设范围改变；

2）变更电子签名认证证书签发逻辑；

3）新增远程证书注册子系统；

4）新增、更改或者删除用于签发电子签名认证证书的证书链；

5）其他对电子认证服务安全、订户资料安全有影响的改变。

b) 重大安全事故

符合以下任意之一：

1）证书签发及验证服务连续停机时间超过 24 小时；

2）发生根证书密钥等关键数据泄露；

3）持续或较大范围未经授权的私钥访问记录或其他异常活动；

4）系统日志持续或较大范围显示异常操作（如非授权时间或网络地址访问敏感功能）。

c) 订户信息泄露事件

符合以下任意之一：

1）个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；

2）数据丢失导致无法恢复证书状态信息。

d) 合规性事件

符合以下任意之一：

1）涉及电子认证服务的司法判定；

2）收到行政部门违规通知或处罚决定。

e) 人力资源类事件

符合以下任意之一：

1）涉及 2 名及以上管理层人员或 10%以上可信人员的离职；

2）劳动纠纷参与人数超过员工总数 10%，且经法院或仲裁机构生效裁决确认由本机构承担法律责任。

5.9.2 报告时限与程序

a）重大事件发生后，发现人应立即向安全策略委员会报告，安全策略委员会应在 1 小时内启动初步响应，评估事件性质和影响范围；

b）安全策略委员会应在 2 小时内向主管部门进行口头或电话报告，说明事件基本情况；

c）安全策略委员会应在 24 小时内向主管部门提交书面报告，详细说明事件经过、影响范围、应急措施及后续处置方案；

d）重大事项报告应通过电话、电子邮件、书面文件等方式同步报送，确保信息传达的及时性和可靠性。涉及电子认证服务安全运营的，应同时报告国家密码管理局、工业和信息化部等主管部门。

5.9.3 报告内容

重大事项报告应包括但不限于以下内容：

a）事件发生的时间、地点、涉及的系统或范围；

b）事件的基本经过和当前状态；

c）事件造成的影响和后果；

d）已采取的应急措施和处置方案；

e）后续整改计划和预防措施；

f）需要主管部门协调解决的事项。

5.9.4 后续跟踪

重大事项报告后，本机构应持续跟踪事件处置进展，及时向主管部门报告事件处置的最新情况和整改结果，直至事件完全解决、系统恢复正常运行。事件处置完成后，应形成完整的事件处置报告，归档保存备查。

6 认证系统技术安全控制

6.1 技术安全管理制度要求

本机构已建立并实施覆盖密钥管理、系统开发、网络防护等领域的技术安全管理制度，并定期接受安全策略委员会的评审，频率每年一次。

6.2 密钥对的生成和安装

6.2.1 密钥对的生成

1、CA 签名密钥的生成

CA 的签名密钥在加密机内部产生，加密机具有国家密码主管部门的相应资质。加密机采用密钥分割或秘密共享机制进行备份。在生成 CA 密钥对时，GZSK 按照加密机密钥管理办法，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，密钥管理员凭借口令和 USBKEY 对密钥进行控制。在审计人员的监督下，由 5 名中的 3 名具有密钥管理及操作权限的人员同时进行操作，产生 CA 密钥。CA 密钥的生成、保存和密码模块符合国家密码主管部门的要求，并具有国家密码主管部门的相应资质。

2、订户密钥的生成

订户的签名密钥的生成由订户负责，订户应确保其密钥产生的可靠性，并负有保护其私钥安全的责任和义务，并承担由此带来的法律责任。

订户的加密密钥由 GZSK CA 的密钥管理系统生成，并通过安全的方式传输给订户。GZSK CA 的密钥管理系统是由国家密码管理局批准运营的专业密钥管理系统，负责为电子认证服务订户产生、备份、恢复加密密钥等服务。

6.2.2 私钥传送给订户

订户的签名私钥由订户自己生成，将不会进行传送。订户的加密密钥由 GZSK CA 的密钥管理系统生成，并通过安全的方式传输给订户。

6.2.3 公钥传送给证书签发机构

证书订户通过 PKCS#10 格式的证书请求或其他数字签名的文件包格式，以电子的方式将公钥提交给 GZSK CA 签发，数据传递过程中采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

6.2.4 电子认证服务机构公钥传送给依赖方

用于验证 GZSK CA 签名的验证公钥（证书链）以及证书状态等信息可从 GZSK 的信息库获得。

6.2.5 密钥的长度

GZSK CA 遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求，目前 GZSK CA 电子认证系统支持签发 SM2-256 密钥的证书，对不符合要求的(如 RSA 密钥长度小于 2048 位、使用 MD5、SHA-1 等不安全算法)拒绝颁发证书。

6.2.6 公钥参数的生成和质量检查

对于使用硬件密码模块的证书订户，公钥参数必须使用国家密码主管部门许可的加密设备生成。参数质量的检查同样通过国家密码主管部门许可的加密设备进行。

6.2.7 密钥使用目的

GZSK 签发的证书包含密钥用法扩展项，证书订户必须按照指定的用途使用密钥。

6.3 私钥保护和密码模块工程控制

6.3.1 CA 密钥

6.3.1.1 密码模块的标准和控制

GZSK CA 使用国家密码主管部门认可、批准的硬件密码模块生成根和存储 CA、运营 CA 和其他 CA 密钥。

6.3.1.2 私钥多人控制（m 选 n）

GZSK CA 的 CA 密钥存放在加密机中，加密机的管理密钥被分割保存在 5 张 USBKEY 中，USBKEY 可分别由 5 位经过授权的安全管理员掌握，并保存在保险箱中。当激活 CA 私钥时，必须由 5 个管理员中的 3 个管理员同时在场才能完成，从技术及制度上保证了敏感的加密操作的安全性。

6.3.1.3 私钥托管

GZSK 运营 CA 的私钥均未在其他地方托管。

6.3.1.4 私钥备份

CA 的私钥由加密机产生，加密机有双机备份，并保存在防高温、防潮湿及防磁场影响的环境中，对加密机的密钥备份操作须 5 人才可完成。

6.3.1.5 私钥归档

当 GZSK 的密钥对到期后，这些密钥对将被归档保存至少 10 年。

6.3.1.6 私钥导入、导出密码模块

GZSK CA 严格按照密钥管理规范进行备份密钥，除此之外的任何导入导出操作都不被允许。

6.3.1.7 私钥在密码模块的存储

CA 私钥以密文的方式加密存放在密码模块中。

6.3.1.8 激活私钥的方法

CA 私钥存放在硬件密码设备中，具有激活私钥权限的管理员使用含有自己

身份的 USBKEY 登录，启动密钥管理程序，进行激活私钥的操作。进行私钥激活的操作需要 3 名管理员同时在场并登陆系统。

6.3.1.9 解除私钥激活状态的方法

当硬件密码模块断电或重新初始化时，私钥进入非激活状态。

具有解除激活私钥状态权限的管理员使用含有自己身份的 USBKEY 登录，启动密钥管理程序，进行解除私钥的操作。进行解除私钥的操作需要 3 名管理员同时在场并登陆系统。

6.3.1.10 销毁私钥的方法

当 CA 的生命周期结束后，GZSK 将根据本 CPS 第 6.3.5“私钥归档”之相关规定将 CA 私钥进行归档，其它的 CA 私钥备份将被安全销毁。归档的私钥在其归档期结束后，需要在所有密钥管理员的参与下进行安全的销毁。

6.3.1.11 密码模块的评估

GZSK 使用国家密码主管部门许可的密码产品，接受其颁布的各类标准、规范、评估结果等各类要求。

6.3.2 订户密钥

6.3.2.1 密码模块的标准和控制

GZSK CA 使用国家密码主管部门认可、批准的硬件密码模块生成订户密钥。

6.3.2.2 私钥托管

订户签名私钥由订户自行保管，密钥管理中心不负责签名私钥托管，仅对订户加密密钥提供密钥恢复管理。KMC 严格保证订户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

6.3.2.3 私钥备份

订户的私钥由订户产生，建议订户自行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄漏。

6.3.2.4 私钥归档

当订户的加密密钥对到期后，这些密钥对将被归档保存至少 10 年。

6.3.2.5 私钥导入、导出密码模块

订户私钥严格按照密钥管理规范进行备份密钥，除此之外的任何导入导出操作都不被允许。

6.3.2.6 私钥在密码模块的存储

私钥以密文的方式加密存放在订户密码模块中。

6.3.2.7 激活私钥的方法

订户私钥存放在硬件密码设备中，服务器密码机管理员使用含有自己身份的 USBKEY 登录，启动密钥管理程序，进行激活私钥的操作。进行私钥激活的操作需要 3 名管理员同时在场；智能密码钥匙通过口令激活私钥。

6.3.2.8 解除私钥激活状态的方法

当硬件密码模块断电或重新初始化时，私钥进入非激活状态。
硬件密码设备服务器密码机管理员使用含有自己身份的 USBKEY 登录，启动密钥管理程序，进行解除私钥的操作。进行解除私钥的操作需要 3 名管理员同时在场；智能密码钥匙通过口令激活私钥

6.3.2.9 销毁私钥的方法

至少 3 名硬件密码设备服务器密码机的管理员使用含有自己身份的 USBKEY 登录，启动密钥管理程序，可以销毁服务器密码机内密钥；智能密码钥匙验证管理员口令后可以通过初始化接口销毁私钥。

6.3.2.10 密码模块的评估

GZSK 使用国家密码主管部门许可的密码产品，接受其颁布的各类标准、规范、评估结果等各类要求。

6.4 密钥对管理的其他方面

6.4.1 公钥归档

公钥归档的保存期限、保存机制、安全措施等与证书保持一致。归档要求参照本 CPS 5.5“记录归档”的相关规定。

6.4.2 证书操作期和密钥对使用期限

CA 证书的有效期不超过 20 年，订户证书有效期最长不超过 5 年。 CA 密钥对使用期限和 CA 证书的有效期保持一致。订户证书的密钥对使用期限和订户证书的有效期保持一致。

对于签名证书，其私钥只能在证书有效期内才可用于数字签名，但是 GZSK 保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期外。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

6.5 激活数据

6.5.1 激活数据的产生和安装

CA 私钥的激活数据，遵循本 CPS 第 6.3.2“私钥多人控制（m 选 n）”节中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 PIN 值，GZSK 出厂时设置了缺省的 PIN 值，为保证订户私钥的安全，订户接受证书后应立即修改 PIN 值。

订户领取数字证书后建议在办理点进行初始密码修改或订户认为安全的地方进行修改，若因未及时修改密码而产生的损失由订户自行承担，与山东公众数

科数字科技有限公司无关。

6.5.2 激活数据的保护

订户必须以加密的形式保存私钥，建议使用双因素认证（如硬件设备加强口令）来保护其私钥。

CA 的密钥管理者需保护他们所维护的密钥，并且需签署协议来确认他们知悉所承担的责任。

6.5.3 激活数据的其他方面

当私钥的激活数据进行传送时，应采取加密等保护措施，以防丢失或非授权访问。

当私钥的激活数据不需要时，应该销毁。确保他人无法通过残余信息、存储介质直接或间接的恢复激活数据。

6.6 计算机安全控制

本机构 CA 系统位于屏蔽机房内，与其他系统隔离。CA/RA 系统的安全防护设置有防火墙、入侵检测与防御系统、漏洞扫描系统。防火墙仅对必要的端口开放访问。

为了保证系统的正常运行，采用的安全技术和控制措施包括：采用安全可信任的操作系统、严格的身份识别和人员访问控制制度、人员职责分割、内部操作控制、业务持续计划等各方面。

本机构建立完善的系统安全维护机制，建立并实施符合 GB/T25056 一 2018 中 8.2 要求的计算机安全控制体系，：至少每半年对所有服务器及终端检查一次系统升级补丁，严格履行升级审批流程并完整记录实施过程；全面部署杀毒软件，确保病毒库每月至少更新一次，至少每月执行全盘病毒扫描；对于已无官方补丁支持的操作系统，采取网络隔离、功能限制等强化防护措施，并制定明确的系统替换计划，以有效防控安全风险，保障系统持续安全运行。

6.7 生命周期的安全控制

GZSK CA 的系统由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，其开发过程符合国家密码主管部门的相关要求，其产品源代码在国家密码主管部门处留有备份，以保证系统的延续性。

GZSK CA 的系统由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，其开发过程符合国家密码主管部门的相关要求，其产品源代码在国家密码主管部门处留有备份，以保证系统的延续性。

本机构按照 GB/T25056《信息安全技术证书认证系统密码及其相关安全技术规范》10、11、12 章节要求，建立完整管理体系，对证书全生命周期进行管理。

6.8 网络安全控制

本机构建立并实施符合 GB/T25056 一 2018 中 5.3.8 要求的网络安全控制体系，包括但不限于:

a. 网络结构满足 GB/T25056 一 2018 附录 A 中规定形式的一种;

b. 对所有 Web 服务配置防火墙、Web 应用防火墙、入侵检测系统和内容过滤等网络安全防护措施;

c. 建立并维护网络拓扑图，包含所有网络设备、连接关系和安全边界，定期更新，与机房实际情况保持一致:

d. 网络访问控制:

1）建立针对证书签发子系统及数据库的访问白名单机制，仅授权证书注册子系统的必要功能模块及必要的管理设备进行访问;

2）建立针对证书注册子系统和数据库的访问白名单机制:

e. 网络监控

1）定期对系统日志进行分析；

2）分析内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件；

6.9 时间戳

GZSK 提供时间戳服务，时间戳服务遵循国际标准时间戳协议(RFC3161)，本机构内部使用，证书、CRL、OCSP、电子认证服务系统等均包含时间信息，该时间信息来源于国家的标准时间源。

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

7.1.1 证书格式标准

本机构签发的电子签名认证证书的格式符合 GB/T20518《信息安全技术 公钥基础设施 数字证书格式》的要求。

证书中的签名算法域中标识的密码算法为国家密码管理主管部门批准的算法。

7.1.2 证书版本

本机构签发的电子签名认证证书采用 X.509 V3 版本格式。

7.1.3 证书内容

本机构签发的电子签名认证证书应包含以下主要内容：

a) 证书版本号（Version）：V3；

b) 证书序列号（Serial Number）：由证书认证系统分配的唯一整数，用于唯一标识本机构签发的每张证书；

c) 签名算法标识符（Signature Algorithm）：标识签发该证书所使用的密码算法，本机构使用国家密码管理部门批准的算法；

d) 颁发者名称（Issuer）：本机构的甄别名（DN）；

e) 证书有效期（Validity）：包括证书生效日期和失效日期，订户证书有

效期最长不超过 5 年；

f）证书主体名称（Subject）：订户的甄别名（DN），命名规则见本 CPS 第 6.3.7 节“命名”；

g）证书主体公钥信息（Subject Public Key Info）：包含订户的公钥及对应的算法标识符；

h）证书策略对象标识符（Certificate Policies）：证书扩展项中应包含主管部门制定的相应等级证书策略 OID.

i)证书扩展项（Extensions）：本机构可根据业务需要设置适当的证书扩展项，包括但不限于密钥用法、扩展密钥用法、CRL 分发点、权威信息访问等，扩展项设置应符合 GB/T20518 的要求；

j）证书颁发者的数字签名（Signature）：本机构使用 CA 私钥对证书的 TBSCertificate 部分进行数字签名。

7.1.4 证书用途说明

本机构宜在证书中明确证书用途、签名私钥的保存方式、相关的法律符合性等内容，便于订户及依赖方了解证书内容。证书包含的密钥用法扩展项明确了证书的允许用途，订户及依赖方应按照证书扩展项中声明的用途使用证书，超出限定用途的使用不受本机构保护。

7.1.5 证书状态查询

证书被撤销后，本机构将该证书序列号加入 CRL，同时提供在线证书状态查询服务（OCSP），供订户及依赖方验证证书的有效性。

7.1.6 证书保护

本机构应采取必要的技术和管理措施，保证证书内容的完整性，防止证书被未授权的修改。证书中的订户信息应真实准确，未经有效验证的信息不得载入证书。

7.2 证书吊销列表

本机构证书撤销列表(CRL)的格式符合 GB/T20518 一 2018 中 5.3 的要求。

7.3 在线证书状态协议

本机构在线证书状态服务符合 GB/T19713 一 2025 中第 7 章的要求。

8 认证机构审计及相关评估

8.1 审计评估制度

6.8.1.1 审计评估制度建立

本机构已制定完善的审计评估制度，对电子认证服务的合规性、有效性和安全性进行定期审查与评估，确保持续符合法律法规、标准规范及本 CPS 的要求。

6.8.1.2 审计评估类型

本机构审计评估包括以下两种类型：

a） 认证业务审计：对证书申请、续期、密钥变更、更新、撤销、冻结等业务中订户告知、身份查验、意愿记录、协议签署、资料保存的合规性进行审计；

b） 全面符合性评估：对年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况进行全面评估。

6.8.1.3 审计评估频率

a）认证业务审计：每年至少进行一次；

b）全面符合性评估：每年至少进行一次；

c）本机构安全策略委员会每年组织一次内部评审，对审计评估结果进行审议，并根据审议结果制定改进措施；

d）在发生重大安全事件、系统重大变更或主管部门有要求时，应适时开展

专项审计或评估。

6.8.1.4 审计评估人员要求

a）参与执行审计评估的人员应具备相应的专业背景，熟悉电子认证服务相关法律法规、标准规范及业务流程；

b）内部审计人员由本机构安全管理、业务管理、技术管理等相关部门人员组成，审计人员与审计对象无直接利益关系；

c）由外部机构执行审计时，外部机构应具备相应资质，审计人员与被审计部门无业务、财务往来或其他利害关系。

6.8.1.5 审计评估主题和方法

审计评估涵盖的主题包括但不限于：

a）物理环境安全：机房安全、门禁管理、监控系统等；

b）系统安全：操作系统、数据库、网络设备、密码设备的安全配置和运行状况；

c）证书生命周期管理：证书申请、审核、签发、更新、撤销等操作是否符合规定流程；

d）密钥管理：密钥生成、存储、备份、恢复、归档、销毁等环节是否符合安全要求；

e）人员管理：可信人员背景审查、培训、权限管理、职责分离等执行情况；

f）业务连续性：应急预案、灾难恢复计划、备份恢复演练等落实情况；

g）法律法规和标准符合性：CPS、CP 及相关管理制度与法律法规和标准规范的符合情况。

审计评估方法包括但不限于文档审核、现场检查、人员访谈、业务抽检、系统测试等。

6.8.1.6 问题整改与跟踪

对于审计评估中发现的问题，本机构应及时通知相关部门和人员限期整改，

并跟踪整改落实情况，形成闭环管理，确保问题得到有效解决。

6.8.1.7 评估报告与报送

审计评估完成后，审计人员应形成审计评估报告，提交安全策略委员会审议。全面符合性评估报告报送主管部门。审计评估结果作为本机构持续改进服务质量、提升安全管理水平的重要依据。

8.2 认证业务审计

8.2.1 审计周期

本机构认证业务审计每年至少进行一次。在发生重大安全事件、业务流程重大变更或主管部门有要求时，应适时开展专项审计。

8.2.2 审计内容

认证业务审计内容主要包括但不限于以下方面：

a）证书申请：订户申请材料的完整性、身份查验过程的合规性、审核记录的完整性；

b）证书续期：续期申请的处理流程、身份查验方式的有效性、相关记录的保存情况；

c）证书密钥更新：密钥更新请求的处理流程、身份确认方式的合规性；

d）证书变更：变更申请的受理流程、身份查验的规范性；

e）证书撤销与冻结：撤销或冻结申请的审批流程、处理时限的合规性；

f）订户告知：告知内容是否完整、告知方式是否符合要求、告知记录是否保存；

g）身份查验：查验方法和流程是否符合规定、查验过程和结果是否完整记录；

h）意愿记录：意愿记录内容是否完整、记录方式是否合规；

i）协议签署：订户协议是否包含规定内容、签署方式是否有效；

j）资料保存：申请材料、审计日志、业务记录等是否按规定期限保存，保存方式是否符合安全要求。

8.2.3 审计抽样方式

a）认证业务审计采用全面审计与抽样审计相结合的方式；

b）采用抽样方式进行审计，审计抽样率不低于 1%;对于高风险业务或曾发现问题的业务领域，适当提高抽样率；

c）抽样应覆盖不同证书类型（个人证书、机构证书、设备证书）、不同业务类型（新申请、续期、变更、撤销等）以及不同时间段，确保抽样的代表性。

8.2.4 审计人员要求

参与认证业务审计的人员应具备相应的专业背景和审计能力，熟悉电子认证服务相关法律法规、标准规范及业务流程。审计人员与被审计业务无直接利害关系。

8.2.5 问题整改与跟踪

对于审计发现的问题，本机构应：

a）及时通知相关部门和人员，明确整改要求和期限；

b）跟踪整改落实情况，确保问题得到有效解决；

c）对整改结果进行复核验证，形成闭环管理；

d）将整改情况记录归档，作为后续审计的参考依据。

8.2.6 审计记录与报告

审计完成后，审计人员应编制审计报告，如实记录审计结果和发现的问题。审计报告应提交本机构管理层审核，并作为持续改进服务质量的依据。审计记录应按规定归档保存，保存期限不少于证书失效后五年。

8.3 全面符合性评估

8.3.1 评估周期

本机构全面符合性评估每年至少进行一次。本机构安全策略委员会每年组织一次内部评审，对全面符合性评估结果进行审议。

8.3.2 评估内容

全面符合性评估内容包括但不限于以下方面：

a) 年度电子认证服务开展情况；

b) 电子认证服务许可条件符合性情况；

c) 认证规则和证书策略符合性情况；

d) 法律法规和标准规范的符合性；

e) 本 CPS 及 CP 的执行情况；

f) 上年度审计发现问题的整改落实情况。

8.3.3 审计抽样方式

采用抽样审计方式的，抽样率不低于 1%，确保抽样具有代表性，覆盖不同类型、不同时间段的业务。

8.3.4 问题整改与跟踪

对于评估发现的问题，本机构应及时通知被审计部门限期整改，并跟踪整改落实情况，确保问题得到有效解决。

8.3.5 评估报告与报送

评估完成后，审计人员应编制全面符合性评估报告，提交安全策略委员会审议。评估报告应在次年 1 月底前报送主管部门。评估结果作为本机构持续改进服务质量、提升安全管理水平的重要依据。

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

我们开展了服务成本核算，制定价格策略，证书及其相关服务的价格，在 公司网站 https://www.aiotca.com/上公布。公布的价格按照网站明确指定的时间生效，没有指定生效时间的，自该价格公布之日立即生效。

9.1.2 证书查询费用

在证书有效期内，对该证书信息进行查询，本机构不收取查询费用。

9.1.3 证书撤销或状态信息的查询费用

通过 CRL 查询证书是否撤销，本机构不收取信息访问费用。通过 OCSP 服务查询证书状态，本机构是否收费视具体的应用情况而定。

9.1.4 其他服务的费用

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

9.1.5 退款策略

如果由于本机构的原因，造成订户合同无法履行、订户证书无法使用，本机构会将有关费用全额退还给订户。

9.2 财务责任

山东公众数科数字科技有限公司保证其具有维持其运作和履行其责任的财

务能力，本机构已建立赔付专项备用资金，资金保障额度不低于上一年度营业收入的 1.5%，资金来源为公司自有资金，由财务部专项管理。有能力承担对订户、依赖方等造成的责任风险，并依据《中华人民共和国电子签名法》、《电子认证服务管理办法》和本文有关条款的规定进行赔偿。

9.3 业务信息保密

9.3.1 保密信息范围

本机构将以下信息视为保密信息，应按照本 CPS 及相关管理制度的要求严格保护：

a）订户身份信息：包括但不限于订户姓名、身份证件号码、联系方式、地址、银行账户信息等个人隐私信息及机构订户的组织机构代码、营业执照信息、法定代表人信息等；

b）证书申请资料：包括订户提交的证书业务申请单、授权委托书、身份证明材料、营业执照复印件等所有与证书申请相关的文件资料；

c）密钥信息：包括 CA 私钥、订户加密密钥等密码设备及密钥管理相关的敏感信息；

d）审计日志：包括系统操作日志、业务处理日志、安全事件记录等涉及系统运行和业务操作的详细记录；

e）客户资料：包括订户及依赖方的档案资料、服务记录、投诉处理记录等；

f）商业秘密：包括本机构的经营策略、财务数据、技术方案、管理流程、客户名单等未公开的商业信息；

g）其他经本机构确认为保密信息或法律法规规定应保密的信息。

9.3.2 非保密信息范围

以下信息不被视为保密信息：

a）本 CPS 及其所有版本；

b）证书链及根证书信息；

c）证书中已公开的订户信息（如证书主体名称等）；

d）本机构公开发布的服务指南、业务办理流程、收费标准等信息；

e）法律、行政法规规定应当公开的信息。

9.3.3 保密信息保护措施

本机构对保密信息采取以下保护措施：

a）建立信息分级分类管理制度，对不同级别的保密信息实施差异化的安全保护措施；

b）所有接触保密信息的员工须签署保密协议，明确保密义务和违约责任；

c）对保密信息的访问实施严格的授权管理，遵循最小权限原则，仅允许因工作需要接触保密信息的人员在授权范围内访问；

d）保密信息的存储应采用加密等安全技术措施，防止信息泄露或被未授权访问；

e）保密信息的传输应采用安全通信通道，确保传输过程中的机密性和完整性；

f）保密信息的销毁应按照相关规定执行，确保信息无法恢复；

g）建立健全保密信息访问审计机制，对保密信息的访问、使用、传输等操作进行记录，确保可追溯。

9.3.4 保密责任

本机构、订户、依赖方等电子认证活动参与者均有义务按照本 CPS 的规定，承担相应的保密责任。对于违反保密义务的行为，本机构将依据相关法律法规及内部管理制度追究相关人员的责任。

9.3.5 依法披露

本机构在法律法规或公共权力部门通过合法程序要求下，可以向特定对象披露保密信息，但应仅限于法律法规要求的范围和限度。本机构有权对相关请求的合法性和适当性进行审查，并依法履行信息披露义务，同时尽可能保护订户的合

法权益。

9.4 个人隐私保密

1、隐私保密方案

GZSK 制定了隐私保密方案，个人隐私信息保密方案遵守现行法律和政策规定。

2、作为隐私处理的信息

GZSK 在管理和使用订户提供的相关信息时，除了订户证书中已经公开的信息外，该订户的其他基本信息将被视为隐私处理，这些信息将只能由 GZSK 使用，非经订户同意或有关法律法规、公共权力部门根据合法的程序要求，GZSK 不会任意公开。

3、不被视为隐私的信息

订户证书中已经公开的信息不被视为隐私信息。

4、保护隐私的责任

GZSK、订户、依赖方等都有义务按照本《电子签名电子认证业务规则》的规定，承担相应的隐私保护责任。

5、使用隐私信息的告知与同意

GZSK 在认证业务范围内使用所获得的任何订户信息，无论是否涉及隐私，GZSK 都没有告知订户的义务，也无需得到订户的同意。

6、依法律或行政程序的信息披露

在法律法规或公共权力部门通过合法程序或订户书面申请授权要求下，GZSK 可以向特定的对象公布隐私信息，无需承担由此造成的任何责任。

7、其他信息披露情形

无规定。

9.5 知识产权

GZSK 享有并保留对证书以及 GZSK 提供的全部软件、资料、数据等的著作权、专利申请权等全部权利。

9.6 陈述和担保

1、电子认证服务机构的陈述与担保

GZSK 开展电子认证服务业务遵守《中华人民共和国电子签名法》等法律规定，接受行业主管部门的监管，对签发的数字证书承担相应法律责任。

2、订户的陈述与担保

订户确认已经阅读和理解了《电子签名电子认证业务规则》及有关规定的全部内容，并且受此《电子签名电子认证业务规则》文件规定的约束。

3、依赖方的陈述与担保

依赖方确认已经阅读和理解了《电子签名电子认证业务规则》及有关规定的全部内容，并同意受此《电子签名电子认证业务规则》文件规定的约束。

4、其他参与者的陈述与担保

其他参与者确认已经阅读和理解了《电子签名电子认证业务规则》及有关规定的全部内容，并同意受此《电子签名电子认证业务规则》文件规定的约束。

9.7 担保免责

有下列情况之一的，应当免除 GZSK 责任。

1、如果证书申请人故意或无意地提供了不完整、不可靠或已过期的信息，又根据正常的流程提供了必需的审核文件，得到了 GZSK 签发的数字证书，由此引起的经济纠纷应由证书申请人全部承担，GZSK 不承担与证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查帮助。

2、订户因个人原因未能保存好私钥造成订户私钥的遗失、泄密、被修改或被未经授权的人使用时，以此造成的相关损失。

3、订户在知悉证书密钥已经失密或者可能失密时，未及时告知 GZSK 并终止使用该证书，从而导致订户相应的损失。

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

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

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

7、由于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。

9.8 偿付责任规则

9.8.1 订户申请本机构赔偿

GZSK 的赔偿内容：

A. GZSK 承诺在现有的技术下，签发的电子证书不会被伪造、篡改。如果发生 GZSK 电子证书被篡改、伪造，一经确认，GZSK 承担相应的赔偿责任。
B. GZSK 必须妥善保管给订户所签发的电子证书和密码，不得泄露或交付他人。如因故意、过失导致他人知道或被盗用、冒用、伪造或者篡改的，给订户造成相应的经济损失，一经确认，GZSK 承担相应的赔偿责任。
C. 证书存储介质如果因 GZSK 的保管或使用不当而导致遗失、损坏等，则 GZSK 承担订户重新办理的申领以及介质等相关费用。
D. GZSK 主体资格灭失(如企业注销等)，GZSK 应承担其旗下所有还未到期及在用的证书再申请费用。
E. 非证书质量造成的证书使用损失，则 GZSK 不承担相关的法律责任。
F. 因证书质量造成的证书使用损失，赔付金额按实际直接损失计算，最高不超过证书办理金额的三倍。

9.8.2 本机构申请订户赔偿

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

订户接受证书就表示同意在以下情况下承担赔偿责任。

A. 订户通过隐瞒、欺诈、盗用等手段提交证书申请材料，以此造成的社会负面影响导致 GZSK 名誉受损，GZSK 有权对订户进行追责，必要的情况下可以通过法律手段。

B. 订户通过对证书的非法使用，即违反 GZSK 对证书使用的规定，造成了 GZSK 的利益受损，GZSK 有权对订户进行追责，必要的情况下可以通过法律手段。

9.9 赔偿

9.9.1 赔偿责任范围

本机构对因自身过错（包括但不限于签发证书时未按 CPS 规定处理、违反法律法规要求、操作人员过失或故意违规操作、证书吊销延迟等）对订户或依赖方造成的直接损失，承担赔偿责任。

在以下情形下，本机构不承担赔偿责任：订户提供虚假或不完整信息、订户未尽私钥保管义务、依赖方未按本 CPS 规定验证证书有效性、不可抗力事件导致的服务中断，或本机构已严格遵循法律法规及本 CPS 规定进行业务操作。

9.9.2 赔偿申请流程

订户或依赖方应在知道或应当知道损失发生之日起一年内提出赔偿申请，超出期限视为放弃权利：

（一）申请受理

订户向原证书受理机构提交赔偿申请书，说明赔偿事由，并提供相关证据及身份证明材料。受理机构应在收到申请后 3 个工作日内完成材料齐全性审核。

（二）审核与责任认定

受理机构将赔偿申请及相关材料报送本机构安全策略委员会，安全策略委员会应在 15 个工作日内完成调查取证和责任判定。责任判定结果应形成书面报告。

（三）审批与沟通

本机构法定代表人应在收到责任判定报告后 5 个工作日内完成审批。审批通过后，由指定代表人与申请方就赔偿金额进行沟通确认。

（四）支付

赔偿金额确认后，本机构应在 20 个工作日内完成赔付支付。

9.9.3 赔偿上限

赔付金额按实际直接损失计算，最高不超过证书办理金额的三倍。

9.9.4 赔偿监督

本机构安全策略委员会负责对赔偿事项进行监督检查，确认赔偿流程合规、责任判定准确、赔偿标准符合规定。监督情况应形成记录并存档备查。

9.10 有效期限与终止

1、终止

GZSK 终止电子认证服务时，本 CPS 终止。

2、效力的终止与保留

当 GZSK 拟终止电子认证业务时，为保证订户权益，必须严格按照《中华人民共和国电子签名法》、《电子签名电子认证服务管理办法（试行）》及行业主管部门中对电子认证机构终止电子认证服务的规范要求进行相关工作。

3、有效期限

本 CPS 在生效日期零时正式生效，上一版本的 CPS 同时失效；本 CPS 在下一版本 CPS 生效后或 GZSK 终止电子认证服务时失效。

9.11对参与者的个别通告与沟通

参与者如需要进一步了解任何本 CPS 中提及的服务、规范、操作等信息，可以通过电话、邮件联系 GZSK。

9.12 修订和发布

1、修订程序

CPS 中所列条款不能适应运营的实际需求，或者与现行法律相抵触时，GZSK 有权在合适的时间修订本 CPS 中任何术语、条件和条款，而且无须预先通知任何一方。

2、通知机制和期限

GZSK 有权修订本 CPS 中的任何条款，无需通知任何一方，但在修订后会及时公布在 GZSK 服务网站上。如在修订发布后 7 个工作日内，订户没有书面提出异议，将被视为同意该修改。

3、必须修改业务规则的情形

当本《电子签名电子认证业务规则》描述的规则、流程和相关技术已经不能满足电子认证业务要求或本《电子签名电子认证业务规则》依据的法律法规和部门规章变更时，GZSK 将依照有关规定修改本《电子签名电子认证业务规则》的相关内容。

9.13 争议处理与举证

9.13.1 争议受理范围

本机构与订户、依赖方及相关参与方之间因本 CPS、电子认证服务协议的履行、解释或证书的使用等事项发生争议时，可向本机构提出争议处理申请。受理范围包括但不限于：

1） 证书申请、签发、使用、吊销、更新、冻结等过程中产生的争议；

2） 证书内容真实性、有效性引发的争议；

3） 密钥管理及使用中产生的争议；

4） 对本机构服务质量、服务态度、服务时效的争议；

5） 因不可抗力或第三方原因导致服务中断引发的争议；

6） 与本 CPS 解释、适用相关的其他争议。

9.13.2 争议处理流程

争议处理应遵循以下流程：

1) 争议发生后，相关方应首先以书面形式向本机构客服部门提交争议处理申请，说明争议事由、诉求并提供相关证据材料；
2) 本机构客服部门应在收到申请后 2 个工作日内完成受理审查，决定是否受理并通知申请人；不予受理的应说明理由；
3) 受理后，本机构应在 15 个工作日内完成调查核实工作，形成处理意见并书面反馈争议方；
4) 争议方对本机构处理结果有异议的，可在收到处理意见之日起 7 个工作日内，向安全策略委员会书面申请复核；
5) 安全策略委员会应在收到复核申请之日起 15 个工作日内作出复核决定，该决定为本机构内部最终处理意见；
6) 争议处理过程中的所有通知、决定等文件应以书面形式送达，送达方式包括当面签收、邮寄、电子邮件等。

9.13.3 协商与调解

1) 争议各方应本着诚实信用、公平合理的原则，在争议发生后优先通过友好协商解决。协商期限为 30 个自然日，自一方提出书面协商请求之日起计算。
2) 协商不成的，争议方可申请调解。调解应遵循自愿原则，可由本机构指定的调解员主持，也可由双方共同委托的第三方调解机构主持。
3) 调解达成协议的，双方应签署书面调解协议；调解不成的，争议方可依法通过诉讼或仲裁途径解决。
4) 调解期限一般不超过 30 个自然日，经双方同意可适当延长。

9.13.4 仲裁

1) 争议各方可在争议发生前或发生后，以书面形式达成仲裁协议，将争议提交约定的仲裁委员会仲裁。

2) 仲裁适用该仲裁委员会届时有效的仲裁规则。仲裁裁决为终局裁决，对双方均有约束力。
3) 当事人未在仲裁规则规定的期限内达成仲裁协议的，可依法向人民法院提起诉讼。

9.13.5 诉讼管辖

1) 争议各方未约定仲裁或仲裁协议无效的，任何一方均有权向本机构住所地有管辖权的人民法院提起诉讼。
2) 适用法律为中华人民共和国法律，诉讼程序适用《中华人民共和国民事诉讼法》的相关规定。
3) 诉讼时效期间为三年，自权利人知道或者应当知道权利被侵害以及义务人之日起计算。

9.13.6 适用条件

1) 仲裁或诉讼应在协商或调解无法解决争议后方可启动，但紧急情况除外。
2) 争议方在启动仲裁或诉讼前，应书面通知本机构，说明争议事项及已采取的协商或调解措施。
3) 仲裁或诉讼期间，除争议事项外，本机构与争议方仍应继续履行本 CPS 及电子认证服务协议中其他未争议条款的权利和义务。

9.13.7 举证制度和能力体系

举证制度和能力体系覆盖证书全生存周期，包括但不限于:

1) 证书签发环节，身份验证记录、材料审查记录、告知记录、意愿确认记录等;
2) 签名环节，签名请求验证、签名操作日志、时间戳记录等;
3) 验证签名环节，验证请求记录、验证结果记录、异常情况处理记录等:
4) 举证材料 15 个工作日内提供。

9.14 管辖法律

GZSK 的《电子签名电子认证业务规则》受《中华人民共和国电子签名法》、《中华人民共和国民法典》法律管辖。

9.15 适用法律的符合性

本机构的各项策略均遵守并符合中华人民共和国各项法律法规和国家信息安全主管部门要求。

9.16 一般条款

1、完整协议

《山东公众数科数字科技有限公司电子认证业务规则》、订户协议、依赖方协议及其他补充协议构成电子认证服务各方的完整协议。

2、转让

本《电子签名电子认证业务规则》中各方的权利和义务，不能通过任何形式转让给任何实体。

3、分割性

本《电子签名电子认证业务规则》的某一条款被宣布为非法、不可执行或无效时，本机构将对该不符合性条款进行修改，直至该条款合法和可执行为止，但不会影响其它条款的有效性。

4、强制执行

无规定。

5、不可抗力

构成不可抗力的事件包括因自然现象引起的,如,火灾、旱灾、地震、风灾、大雪、山崩等，或是由社会原因引起的,如,战争、动乱、政府干预、罢工、禁运、市场行情等。但各方都有义务建立灾难恢复和业务连续性机制。

9.17 其他条款

本机构对本《山东公众数科数字科技有限公司电子认证业务规则》有最终解释权。