GZSK

Certificate Policy

（CP）V4.0

山东公众数科数字科技

有限公司

证书策略 V4.0

目 录

1.概括性描述　5

1.1 概述　5

1.2 文档名称与标识 6

1.3 电子认证活动参与者 6

1.4 证书应用　8

1.5 策略管理　10

1.6 定义和缩写 12

2.信息发布与信息管理　15

2.1 认证信息的发布 15

2.2 发布的时间或频率　16

2.3 信息库访问控制　16

3. 身份标识与鉴别　17

3.1 命名　17

3.2 初始身份确认　18

3.3 密钥更新请求的标识与鉴别　23

3.4 撤销请求的标识与鉴别　24

4. 证书生命周期操作要求 24

4.1 证书申请　24

4.2 证书申请处理　26

4.3 证书签发　27

4.4 证书接受　28

4.5 密钥对和证书的使用 29

4.6 证书续期　30

4.7 证书密钥更新　32

4.8 证书变更　34

4.9 证书撤销与冻结 36

4.10 证书状态服务　43

4.11 停止使用认证服务 44

4.12 密钥托管与恢复　45

5. 认证机构设施、管理和操作控制 46

5.1 物理控制 46

5.2 程序控制 50

5.3 人员控制 51

5.4 审计日志程序 54

5.5 记录归档 57

5.6 电子认证服务机构密钥更替 60

5.7 损害与灾难恢复 60

5.8 电子认证服务机构终止 61

5.9 重大事项报告 62

6. 认证系统技术安全控制 63

6.1 密钥对的生成和安装 63

6.2 私钥保护和密码模块工程控制 67

6.3 密钥对管理的其他方面 70

6.4 激活数据 71

6.5 计算机安全控制 73

6.6 生命周期技术控制 74

6.7 网络的安全控制 75

6.8 时间戳 75

7. 证书、证书撤销列表和在线证书状态协议 76

7.1 证书 76

7.2 证书撤销列表 78

7.3 在线证书状态协议 79

8. 认证机构审计和其他评估 79

8.1 评估的频率或情形 79

8.2 评估者的资质 80

8.3 评估者与被评估者之间的关系 80

8.4 评估内容 80

8.5 对问题与不足采取的措施 81

8.6 评估结果的传达与发布 81

8.7 认证业务审计 81

8.8 全面符合性评估 82

9. 法律责任和其他业务条款 82

9.1 费用 82

9.2 财务责任 83

9.3 业务信息保密 85

9.4 个人隐私保密 86

9.5 知识产权 88

9.6 陈述与担保 88

9.7 担保免责 90

9.8 有限责任 92

9.9 赔偿 92

9.10 有效期限与终止 96

9.11 对参与者的个别通告与沟通 97

9.12 修订 97

9.13 争议处理 98

9.14 管辖法律 98

9.15 与适用法律的符合性 99

9.16 一般条款 99

9.17 其他条款 100

10. 文件历史记录 101

1.概括性描述

1.1 概述

证书策略（CP，Certificate Policy）是电子认证服务机构制定的一组规则，用于说明特定证书类型、特定订户群体或特定应用场景下的安全等级、适用范围、参与方义务和证书管理要求。CP 是 GZSK 开展电子签名认证证书服务的基础策略文件，电子认证业务规则（CPS）用于说明本 CP 的具体实施方式。

本 CP 依据《中华人民共和国电子签名法》《电子认证服务管理办法》、工业和信息化主管部门发布的《电子认证业务规则规范》及相关监管要求、GB/T 26855-2011《信息安全技术 公钥基础设施 证书策略与认证业务声明框架》等编制，并与《山东公众数科数字科技有限公司电子认证业务规则》2.4 版保持一致。涉及密码技术、数字证书格式、网络安全、数据安全和个人信息保护的事项，同时遵守国家现行法律法规、国家标准、行业标准及密码主管部门要求。

本 CP 适用于山东公众数科数字科技有限公司（以下简称“GZSK”）面向社会公众提供的电子签名认证证书及本 CP 明确纳入管理的其他数字证书。GZSK 按照公开发布的 CP 和 CPS 提供服务，并接受工业和信息化等主管部门监督管理。

1.2 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证书策略（CP）V4.0》。本 CP 在 GZSK 官方网站发布，发布地址：https://www.aiotca.com/。

本 CP 与《山东公众数科数字科技有限公司电子认证业务规则》2.4 版配套使用。CPS 与 CP 发生表述差异时，对具体业务操作、身份查验方式和系统实施要求以经批准并备案的现行 CPS 为准；CP 用于确定证书等级、适用范围及总体安全策略。

本 CP 所适用的电子签名认证证书在证书策略扩展项中记载主管部门制定的相应等级证书策略 OID，具体见本 CP 第 1.4 节和第 7.1.6 节。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

山东公众数科数字科技有限公司（GZSK）是依法设立的第三方电子认证服务机构，承担电子签名认证证书的申请受理、身份查验、签发、续期、变更、撤销、冻结、密钥管理、证书查询、证书撤销列表（CRL）发布、在线证书状态查询（OCSP）、策略制定及信息发布等职责。

GZSK 对服务告知、身份查验、订户意愿确认、订户协议签署

及相关数据留存承担主体责任。上述核心职责由 GZSK 自行完成，不委托非同一法人主体的外部机构或个人实施。

1.3.2 内部证书注册与受理职能

GZSK 可设置 RA/LRA 等内部系统角色、业务受理岗位或受理点，用于证书申请材料接收、系统录入、审核流转和证书交付等工作。该等角色属于 GZSK 内部管理和操作体系，不构成独立的外部电子认证活动参与者。

涉及订户服务告知、身份查验、意愿确认、协议签署及数据留存等核心职责时，应由 GZSK 按照现行 CPS 直接履行，并建立可审计、可追溯的业务记录。

1.3.3 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”。

1.3.4 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。

1.3.5 其他参与者

除电子认证服务机构（GZSK）、订户和依赖方以外的参与者称为其他参与者。

1.4 证书应用

1.4.1 适合的证书应用

GZSK 签发的电子签名认证证书可用于电子政务、电子商务及其他合法社会化应用场景，为身份认证、电子签名、数据完整性和抗抵赖等提供可信支撑。证书的具体使用应同时满足证书扩展项、订户协议和应用系统的安全要求。

GZSK 电子签名认证证书按订户主体和风险等级划分为以下四类：

1）机构基础级电子签名证书：采用 SM2-256 密钥类型，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。证书策略 OID：2.16.156.339.2.1.2.1。

2）机构高等级电子签名证书：采用 SM2-256 密钥类型，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。证书策略 OID：2.16.156.339.2.1.2.2。

3）个人基础级电子签名证书：采用 SM2-256 密钥类型，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。证书策略 OID：2.16.156.339.2.1.1.1。

4）个人高等级电子签名证书：采用 SM2-256 密钥类型，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。证书策略 OID：2.16.156.339.2.1.1.2。

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及相应证书策略执行，其 OID 为 2.16.156.339.2.2.1.1。

GZSK 还可签发设备证书、SSL 证书等其他数字证书。设备证书用于设备身份认证及加密，SSL 证书用于建立国密安全通道；此类证书不作为电子签名认证证书使用。

1.4.2限制的证书应用

GZSK 签发的证书不得用于违反中华人民共和国法律、行政法规、部门规章、国家安全要求、公序良俗或侵害国家利益、社会公共利益及第三方合法权益的活动。

订户和依赖方必须按照证书密钥用法、扩展密钥用法、证书策略 OID 和本 CP 规定的适用范围使用证书。超出证书限定用途或未经 GZSK 认可的应用，不属于本 CP 承诺的保护范围。基础级证书不得用于本 CP 明确要求采用高等级证书的高风险电子签名场景。设备证书和 SSL 证书不得用于电子签名。

1.5 策略管理

1.5.1策略文档管理机构

GZSK安全策略委员会是CP、CPS等策略文档的最高管理机构，负责策略文档的制定、维护、审核、批准、解释和实施监督。安全策略委员会应明确维护CP、CPS等策略文档的职能分工，建立修订和批准流程；对信息安全策略、根证书密钥、证书签发自动审核等重要操作进行审批；每年至少组织一次CP和CPS全面评审，并根据法律法规、监管要求、技术标准和业务变化及时修订；每年组织运营风险评估并形成报告。

1.5.2联系人

如对本CP有任何疑问，请与GZSK安全策略委员会联系：

CP/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

电子邮件：pubca@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

1.5.3 决定 CP 符合策略的机构

GZSK 安全策略委员会负责判断本 CP 与 GZSK 现行 CPS、适用法律法规、主管部门监管要求及相关技术标准的符合性，并负责批准本 CP。

1.5.4CP 批准程序

本 CP 由安全策略委员会主任及委员组织相关人员拟定或修订，提交安全策略委员会评审。评审通过后形成正式版本，并按照法律法规和主管部门要求进行发布与备案。

因国家政策法规、监管要求、技术标准或公司业务发生变化需要修订本 CP 时，由安全策略委员会组织修订和评审。正式版本应在公司官方网站发布，并按《电子认证服务管理办法》等规定履行备案义务。

1.6 定义和缩写

缩写

CA	电子认证服务机构
RA	证书注册管理内部角色/系统角色
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

定义

电子认证服务机构 certification authority	一个被终端实体所信任的签发公钥证书的证书认证实体，它是一个可信的权威机构，获得授权面向社会公众提供第三方电子认证服务的数字证书认证中心（简称CA、CA中心、CA机构、电子认证服务机构）。
证书策略 certificate policy	是一个指定的规则集合，它指出证书对于具有普通安全需求的一个特定团体和（或）具体应用类型的适用性。
电子认证业务规则 certification practice statement	关于电子认证服务机构在签发、管理、注销或续期证书（或续期证书中的密钥）时的业务实施声明。
证书撤销列表	一个经电子认证服务机构

certificate revocation list	数字签名的列表，它标出了一系列证书颁发者认为无效的证书。
数字证书 digital certificate	经权威的、可信赖的、公正的第三方机构(即电子认证服务机构，CA)，数字签名的包含公开密钥拥有者信息以及公开密钥的文件。
公钥基础设施 public key infrastructure	支持公开密钥体制的安全基础设施，提供身份鉴别、信息加密、数据完整性和交易抗抵赖。
注册机构 registration authority	GZSK 内部可设置的证书注册、受理和审核系统角色或岗位。其活动受 GZSK 直接管理，不承担可对外委托的独立 CA 主体职责；服务告知、身份查验、订户意愿确认、协议签署和数据留存等核心职责由 GZSK 依法自行履行。

2.信息发布与信息管理

2.1 认证信息的发布

GZSK 通过官方网站发布现行有效的 CP、CPS、CA 证书、证书

链、CRL 下载信息、证书状态查询信息、服务指南、联系方式及其他依法应公开的信息。公开信息应保持真实、准确、完整和可访问。

订户证书可按照现行 CPS 及订户授权情况发布到目录服务系统；证书撤销状态通过 CRL 和 OCSP 提供查询。涉及个人信息、商业秘密、内部管理和安全敏感信息的内容不作为公开信息发布。

2.2 发布的时间或频率

CP、CPS 及相关公开信息经批准后按照主管部门要求及时发布。CP、CPS、CA 证书等公开信息内容发生变更后，GZSK 应在 1 个工作日内完成相关公开信息更新。

证书签发后,按照现行 CPS 规定将证书发布到相应目录服务。CRL 每 24 小时自动发布一次；必要时可人工发布最新 CRL。OCSP 提供及时的证书状态查询。

公开信息服务原则上提供 7×24 小时访问能力；发生计划维护、故障或不可抗力时，按照业务连续性和应急管理要求处理。

2.3 信息库访问控制

公众可以通过 GZSK 官方网站自由查询和访问已经公开发布的 CP、CPS、CA 证书、证书链、CRL 及其他公开信息。

CA业务数据库中的非公开数据仅限经授权的CA/RA内部管理员、审计人员及其他可信角色按照最小权限原则访问。任何访问应受身份鉴别、权限控制和审计日志约束。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

GZSK 签发的数字证书符合 X.509V3 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。DN 的详细说明见本 CP 的 7.1.4。

3.1.2 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。

3.1.3 订户的匿名或伪名

订户不能使用匿名、伪名申请证书。

3.1.4 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，详见本 CP 7.1.4 的说明。

3.1.5 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。

3.1.6 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。

3.2 初始身份确认

GZSK在受理证书申请时，应对订户和/或受托人完成服务告知、身份查验、订户意愿确认和订户协议签署，并为每个证书申请建立独立、完整、可追溯的身份查验记录。身份查验核心职责由GZSK自行完成，不委托非同一法人主体的外部机构或个人。

申请高等级证书和基础级证书时，GZSK按照不同风险等级采用与证书等级相匹配的身份查验强度；所有写入证书的身份信息均应经过验证。

3.2.1 证明拥有私钥的方法

订户签名密钥对应由订户按照本 CP 第 6 章要求生成。GZSK 通过证书请求中包含的数字签名、订户公钥验证等方式确认订户实际控制与注册公钥对应的签名私钥。

订户应妥善保管签名私钥。签名私钥原则上由订户本人控制；GZSK 不得以违反现行 CPS 或法律法规的方式取得、留存或擅自使用订户签名私钥。

3.2.2 组织机构身份的鉴别

机构订户应提供能够证明机构真实、合法存在的有效证件或权威登记信息，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。GZSK 应对机构登记信息、法定代表人或受托人身份、授权关系及证书申请关键信息进行查验。

机构高等级证书：法定代表人申请时，应通过证件机读工具、权威数据库或主管部门认可的其他方式查验身份证件真实性和有效性，并采用面对面、远程人工面对面、生物特征验证或主管部门认可的其他高强度方式完成身份查验。受托人申请时，还应查验加盖机构公章的有效书面授权证明，核对受托人与授权文件一致，并可采用对公账户随机金额打款等方式加强机构真实性核验。

机构基础级证书：应验证机构真实存在及法定代表人或受托人身份，可采用高等级证书查验方式，或者运营商三要素+

随机短信验证码、银行卡四要素+随机短信验证码、有效电子签名认证证书签名验证以及主管部门认可的其他核验方式。受托人申请时应查验加盖机构公章的有效授权证明。

机构内设部门、职务等信息拟写入证书时，应取得足以证明其真实性和授权关系的材料并完成审核。

3.2.3 个人身份的鉴别

个人订户应提供政府部门签发的合法有效身份证件或身份信息，包括但不限于居民身份证、港澳台居民居住证、港澳居民来往内地通行证、台湾居民来往大陆通行证、护照、外国人永久居留身份证、军官证等。GZSK 应通过证件机读工具、权威数据库或主管部门认可的方式查验身份证件真实性和有效性。

个人高等级证书应采用面对面、远程人工面对面、生物特征验证（如活体人脸、指纹、声纹、掌纹等选择一种）或主管部门认可的其他高强度方式进行身份查验。

个人基础级证书可采用高等级查验方式，或运营商三要素+短信验证码、银行卡四要素+短信验证码、有效电子签名认证证书签名验证以及主管部门认可的其他方式进行身份查验。

订户委托他人办理时，GZSK 应查验订户本人有效书面授权证明，并查验订户和受托人的身份证件或身份资料。

3.2.4 没有验证的订户信息

证书中的订户身份信息必须经过验证，未经验证的信息不得写入电子签名认证证书。

姓名、证件号码、机构名称、电子邮箱、机构内设部门及职务等信息，应根据其性质采用有效身份证件、权威登记信息、随机验证码、授权证明等适当方式进行核验并留存相应记录。

3.2.5 授权确认

订户授权受托人办理证书业务时，GZSK 应核验有效书面授权证明、授权范围、授权期限及受托人身份。授权文件和身份查验记录应与对应证书申请建立关联并归档。

授权关系存在疑问、授权文件无效或无法确认受托人身份时，不得据此批准证书申请。

3.2.6 互操作准则

对于其他电子认证机构，可以与 GZSK 进行互操作，但是该电子认证服务机构的 CPS 必须符合 GZSK CP 的要求。

3.2.7 订户意愿确认

GZSK 应确认并记录订户申请和使用电子签名认证证书的真实意愿。意愿内容至少包括订户身份信息、CA 信息、签名私钥保存方及其保存义务、订户对电子签名的法律责任，以及

订户对上述事项充分知晓并同意的明确意思表示。

个人高等级证书应采用面对面确认、手抄提示语并录音录像、音视频远程确认或主管部门认可的其他方式记录意愿；个人基础级证书可在前述方式基础上采用强制阅读、短信或邮件确认等电子方式。机构证书应确认法定代表人或经有效授权受托人的申请意愿，并与证书等级对应。

3.2.8 订户协议

GZSK 应与订户签署或确认订户协议，明确证书使用规则、双方权利义务、服务费用、信息安全要求、责任承担、私钥保护及禁止违法违规使用证书等事项。订户可通过纸质签字/盖章、在线勾选或点击确认以及其他能够证明真实意思表示的方式确认协议。

GZSK 应完整保存订户协议内容、展示版本、确认时间、确认主体、确认方式及相关电子数据，以满足查询、审计和争议举证需要。

3.3 密钥更新请求的标识与鉴别

订户申请密钥更新时，GZSK 应验证原证书由 GZSK 签发、证书状态有效，并按照证书等级对应的身份查验要求确认订户身份和更新意愿。涉及受托人办理的，应重新核验授权关系。密钥更新将导致使用原加密密钥加密的数据可能无法继续

解密。订户申请密钥更新前，应妥善处理使用原密钥加密的数据；GZSK 应按照订户协议和现行 CPS 履行必要告知。

3.4 撤销请求的标识与鉴别

订户本人提出证书撤销请求时，GZSK 应按照与证书等级和撤销风险相匹配的方式对申请人身份、撤销意愿及证书信息进行核验，并留存撤销申请和处理记录。

因法律法规、主管部门要求、证书安全性不能得到保证、订户违反协议义务或其他符合本 CP 第 4.9 节规定的情形由 GZSK 主动撤销证书时，应按照现行 CPS 规定履行通知、申辩或其他程序；依法无需再次进行订户身份确认的情形除外。

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

任何组织和个人需要使用 GZSK 签发的证书时，均可向 GZSK 提出证书申请。

在申请设备证书时，需由设备的所有者向 GZSK 提出证书申请。

4.1.2 注册过程与责任

1、注册与申请过程

订户通过 GZSK 服务渠道提交证书申请及所需材料。GZSK 对申请材料进行接收、服务告知、身份查验、订户意愿确认和协议签署，并通过内部业务系统完成受理、审核和证书签发流转。内部 RA/LRA 系统角色仅用于 GZSK 内部业务处理，不改变 GZSK 对核心认证职责承担的主体责任。

2、责任

GZSK 应向订户告知证书及电子签名的使用条件、服务收费项目和标准、信息安全保障措施、双方责任范围、订户签名私钥存储方式和安全要求等事项。

订户应提供真实、完整、准确的申请信息和证明材料，确认订户协议，并对其签名私钥和激活数据承担妥善保管责任。

GZSK 应建立每个证书申请的独立身份查验和业务处理记录，确保申请、审核、签发和接受过程可追溯。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

GZSK 接收证书申请后，应按照本 CP 第 3 章及现行 CPS 要求执行服务告知、身份查验、订户意愿确认、订户协议确认和申请材料审核。未经完成相应等级身份查验或关键信息无法

核实的申请不得批准。

4.2.2 证书申请批准和拒绝

符合以下条件的证书申请可予批准：申请满足本 CP 第 3 章及现行 CPS 的身份查验要求；订户已明确表达申请意愿并确认订户协议；申请信息真实、完整、准确；符合证书等级和应用场景要求；已按照规定支付相关费用（如适用）。

存在以下任一情形的，应拒绝申请：身份查验未通过；申请信息不真实、不完整或存在重大疑点；订户未确认协议或未能形成有效申请意愿；拟使用场景违法违规或不符合证书策略；未按照规定支付相关费用；法律法规或主管部门要求拒绝的其他情形。

对拒绝申请的，GZSK 应按照现行 CPS 向申请人说明拒绝原因或提供必要的查询渠道，法律法规另有规定的除外。

4.2.3 处理证书申请的时间

在订户提交材料齐全、身份查验和审核通过的情况下，GZSK 原则上在 1 个工作日内完成证书申请处理；特殊业务或依法需要进一步核验的，按照服务约定和现行 CPS 执行。

4.3 证书签发

4.3.1 证书签发中 GZSK 的行为

订户申请通过鉴别和审核后，GZSK 内部受理/审核系统向 CA 系统提交证书签发请求。CA 系统应对申请数据、授权状态和内部请求完整性进行校验；对于有效且符合策略的签发请求，由 CA 系统签发证书。

证书签发过程中应执行岗位权限控制、职责分离、审计日志和系统安全控制。任何外部合作方不得绕过 GZSK 核心身份查验和审核流程直接触发电子签名认证证书签发。

4.3.2 GZSK 对订户的签发通告

证书签发成功后,GZSK 直接向订户发送签发通知或通过 GZSK 控制的服务渠道提供证书获取方式。通知和交付过程应能够与对应申请记录关联，并符合个人信息保护和数据安全要求。

4.4 证书接受

4.4.1 构成接受证书的行为

1、GZSK 或其内部授权受理岗位代替订户下载证书，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即代表用户接受了证书。

4.4.2 电子认证服务机构对证书的发布

订户接受证书后，GZSK 将该订户证书发布到 GZSK 的目录服务系统。

4.4.3 电子认证服务机构对其他实体的通告

GZSK 不会对其他实体进行通告，依赖方可以在信息库上自行查询。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在使用证书和私钥时必须遵守法律、本 CP 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。

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。

4.5.2 信赖方公钥和证书的使用

当依赖方接受到签名的信息后，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，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。

4.6 证书续期

证书续期是指不改变证书公私钥和除有效期外其他任何信息的情况下，为订户签发一张新的证书。

4.6.1 证书续期的情形

证书订户可在证书到期前 90 天内向 GZSK 申请证书续期。证书过期后，应按照新申请流程重新申请证书。证书续期不得降低原证书等级对应的身份查验和安全要求。

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

证书续期请求应至少验证：1）订户实际控制原证书对应私钥且原证书由 GZSK 签发；2）原证书状态和有效性；3）基于原注册信息并结合证书等级进行必要的身份复核；4）订

户续期意愿和订户协议有效性；5）费用支付情况（如适用）。原身份信息发生变化、原身份查验记录已不能满足现行要求或存在异常风险时，应重新进行相应等级的身份查验。

4.6.4 颁发新证书时对订户的通告

同本 CP 第 4.3.2 节。

4.6.5 构成接受续期证书的行为

同本 CP 第 4.4.1 节。

4.6.6 电子认证服务机构对续期证书的发布

同本 CP 第 4.4.2 节。

4.6.7 电子认证服务机构对其他实体的通告

同本 CP 第 4.4.3 节。

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

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

同本 CP 第 4.6.3 节

4.7.4 颁发新证书时对订户的通告

同本 CP 第 4.3.2 节。

4.7.5 构成接受密钥续期证书的行为

同本 CP 第 4.4.1 节。

4.7.6 电子认证服务机构对密钥续期证书的发布

同本 CP 第 4.4.2 节。

4.7.7 电子认证服务机构对其他实体的通告

同本 CP 第 4.4.3 节。

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

同本 CP 第 4.2 节.

4.8.4 颁发新证书时对订户的通告

同本 CP 第 4.3.2 节。

4.8.5 构成接受变更证书的行为

同本 CP 第 4.4.1 节。

4.8.6 电子认证服务机构对变更证书的发布

同本 CP 第 4.4.2 节。

4.8.7 电子认证服务机构对其他实体的通告

同本 CP 第 4.4.3 节。

4.9 证书撤销与冻结

4.9.1证书撤销的情形

如有下列情况中的任何一种情况发生，则订户的证书将被撤销：

1）订户书面申请撤销数字证书;

2）当 CA 有证据表明订户证书私钥遭到泄露或损坏;

3）当 CA 有证据表明订户将证书使用于法律、行政法规定义为非法事项上，或者 CA 发现订户证书未恰当使用;

4)当 CA 有证据表明订户未履行 CP/CPS 或订户协议中约定的义务；或者订户证书不符合 CP/CPS 的相关要求;

5）当 CA 有证据表明订户证书中的重要信息内容已经变更，CA 已经履行通知义务，而订户未申请变更证书的情形;

6）当 CA 有证据表明证书中所显示的信息为不准确或具有误导性；或者订户申请证书时，提供的资料不真实;

7）当 CA 因某些原因停止业务，并且没有安排其他的 CA 提供证书撤销服务;

8）当 CA 用于签发证书的私钥可能被泄露时，将根据应急预案撤销所有已签发的证书;

9）当证书的重要参数被国际国内主流标准认为有重大风险时;

10）当 CA 已经履行催缴义务，订户仍未按照规定支付相关费用;

11）法律、行政法规规定的其他情形。

4.9.2请求证书撤销的实体

以下实体可以请求撤销订户证书:

1、GZSK 依据本 CP 第 4.9.1 节可以依职权发起撤销订户证书。

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撤销请求的流程

证书订户主动申请撤销证书，同本CP第4.2节。

当出现被动撤销的情形时，GZSK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GZSK提出申辩理由，GZSK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CP第4.9.4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。

4.9.7CRL 发布频率

GZSK 采用定期和必要时人工发布相结合的方式发布 CRL。CRL 每 24 小时自动发布一次；发生需要及时反映证书状态的情形时，可人工发布最新 CRL。

4.9.8CRL 发布的最大滞后时间

GZSK 对 CRL 进行备份，备份时间间隔最长不超过 24 小时。CRL 备份文件保存时间不少于证书失效后 10 年。

4.9.9在线状态查询的可用性

GZSK 提供 7×24 小时 OCSP 证书状态查询服务。OCSP 服务按照国家及行业现行标准实现，并应与 CRL 中的证书撤销状态保持一致。

4.9.10 在线状态查询要求

订户和依赖方可以进行在线证书状态查询。GZSK 原则上不对公开证书状态查询设置读取权限，并提供符合现行标准和 CPS 规定的 OCSP 查询方式。

4.9.11 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 GZSK 官网下载最新的 CRL 获取 CRL 信息。

4.9.12 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。

4.9.13 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。

4.9.14 请求证书冻结的实体

以下实体可以请求冻结订户证书:

1、GZSK 依据本 CP 第 4.9.13 节可以依职权发起冻结订户证书

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。

4.9.15 冻结请求的流程

证书订户主动申请冻结证书，同本 CP 第 4.2 节。

当出现被动冻结的情形时，GZSK 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且无异议后予以冻结。

4.9.16 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 GZSK 提出申辩理由，GZSK 将会对申辩理由进行评估，若确认其理由正当则撤销冻结。

4.9.17　电子认证服务机构处理冻结请求的时限

在本 CP 第 4.9.16 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

GZSK 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

GZSK 提供不间断证书状态查询服务，确保服务可用率不低于99%。计划维护、灾难或不可抗力等情形按照本 CP 业务连续性及应急管理要求处理。

4.11 停止使用认证服务

订户证书到期、被撤销、订户主动停止使用认证服务或出现订户协议、法律法规规定的其他终止情形时，相关证书服务关系终止。

停止使用认证服务不影响停止前已经依法形成的电子签名、审计记录、证据材料及依法应继续承担的责任。GZSK 应对停止服务的申请、身份确认、处理结果和通知过程进行完整记录。

4.12 密钥托管与恢复

4.12.1 密钥生成、备份与恢复的策略与行为

订户签名私钥由订户自行控制和保管，GZSK 不对订户签名私钥提供托管恢复服务。

对于依法、依策略允许进行恢复的加密密钥，GZSK 可通过密钥管理中心（KMC）提供密钥备份、恢复和管理服务。密钥恢复应执行严格身份鉴别、授权控制、职责分离和审计记录，不得将加密密钥恢复机制用于绕过签名私钥唯一控制要求。

4.12.2 会话密钥的封装与恢复的策略与行为

使用数字信封的方式来封装会话密钥，使用信息接收者的公钥对会话密钥进行加密，接收者用自己的私钥解密并恢复会话密钥。

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，位于江苏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 平米。机房按功能分为四个区域，分别

是公共区、服务管理区、核心区和密钥管理区。

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，符合国家相关机房的标准。

其中，核心区、密钥管理区为屏蔽机房，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RA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屏蔽机房设置在江苏自贸区南京片区浦滨路320号科创一号大厦A座812办公楼内，

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 制订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，防止泄露和未经授权使用。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。

5.2 程序控制

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:

客户服务岗位

安全管理岗位

专业技术岗位

运行维护岗位

5.2.2 每项任务需要的人数

GZSK 制定了规范的策略，在具体业务规范中严格控制任务和职责的分割，对于最敏感的操作，例如访问和管理 CA 的加密设备及其密钥,需要至少 3 个可信角色人员同时操作。其它操作，例如发放证书，需要至少 2 个可信角色人员。

5.2.3 每个角色的识别与鉴别

GZSK 在雇佣一个可信角色之前将会按照本 CP 第 5.3.2 节的规定对其进行背景审查。

5.2.4 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。

5.3 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 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。

5.3.3 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、证书策略和电子认证业务规则;

2、PKI/CA 基本知识

3、电子签名法和相关规章标准;

4、公司体系制度和相关文件。

5.3.4 再培训周期和要求

GZSK 根据需要至少每年一次组织再培训。

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。

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。

5.4 审计日志程序

5.4.1 记录事件的类型

GZSK 记录的日志信息包括但不限于以下类型:

1、证书生命周期中的各项操作，包括证书申请、证书密钥更新、证书撤销等事件；

2、系统、网络巡检记录，包括入侵检测系统的记录、系统日常运行产生的日志文件、系统故障处理工单、系统变更工单等;

3、人员访问控制记录;

4、系统巡检记录。

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 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，对发现的安全事件及时采取处置和整改措施。

5.4.3 审计日志的保存期限

GZSK 所有审计日志永久保存。

5.4.4 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。

5.4.5 审计日志备份程序

同本 CP 第 5.1.8 节。

5.4.6 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

5.4.7 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。

5.4.8 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、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 CP 第 6.3.2 节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 损害与灾难恢复

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。

5.7.4 灾难后的业务连续性能力

GZSK 建立业务连续性计划和灾难恢复机制。发生灾难或重大

故障时，应按照应急预案恢复认证业务；根据现行 CPS，目标为灾难发生后 48 小时内恢复电子认证服务，恢复点目标（RPO）控制在 24 小时内。

业务连续性计划应覆盖重要系统、数据、软件、密码设备、备份设施、后备电源、人员组织和对外通知，并定期检查和更新。

5.8 电子认证服务机构终止

当 GZSK 因技术、商业或其他原因拟终止电子认证服务时，应严格按照《中华人民共和国电子签名法》《电子认证服务管理办法》及主管部门有关要求办理，保障订户和依赖方合法权益。

GZSK 应至少提前 90 日通知证书订户、依赖方等相关实体，并按照主管部门要求提前报告；确定具备相应资质的承接单位并依法签署承接协议；在主管部门指导下完成必要的业务、证书状态信息、档案和相关关键数据移交；停止相关服务后对操作记录、敏感文档和数据进行归档或安全处理。

终止过程中应保证业务平稳过渡并完整保存操作记录。GZSK 终止服务后，对依法应继续承担的证明责任和法律责任，按照法律法规、承接安排和证书有效状态执行。

5.9 重大事项报告

GZSK 建立重大事项报告制度。重大事项包括但不限于证书认证系统迁移或重大改造、证书签发逻辑重大变化、新增远程证书注册子系统、证书链新增/变更/删除、重大安全事故、CA 私钥安全事件、核心系统长时间中断、重大数据安全事件以及主管部门要求报告的其他事项。

发生重大事项时，应立即启动内部应急处置和报告流程。涉及重大安全事件的，应按照现行 CPS 要求及时向主管部门报告；安全策略委员会负责组织事件分级、书面报告、持续跟踪和整改闭环。

重大事项报告至少应包括事件时间、地点、影响范围、原因分析、已采取措施、后续处置计划、联系人及主管部门要求的其他信息。相关报告、处置记录和证据应归档保存。

6. 认证系统技术安全控制

GZSK 建立与电子认证服务相适应的技术安全管理制度，对 CA、RA/LRA、KMS/KMC、目录服务、CRL/OCSP、网络及运维管理系统实施分区分域、访问控制、职责分离、审计和生命周期安全管理。

密码算法、密码产品和密码模块应符合国家密码主管部门及现行标准要求。GZSK 电子认证系统支持签发 SM2-256 密钥类

型证书，对不符合现行安全要求的算法和密钥长度拒绝颁发证书。

6.1 密钥对的生成和安装

6.1.1 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 的密钥管理系统生成，并通过安全的方式传输给订户。GZSK 的密钥管理系统是由国家密码管理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。

6.1.2 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 的密钥管理系统生成，并通过安全的方式传输给订户。

6.1.3 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 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。

6.1.4 电子认证服务机构公钥传送给依赖方

用于验证 GZSK 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。

6.1.5 密钥的长度

GZSK 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 电子认证系统支持签发 SM2-256 密钥的证书。

6.1.6公钥参数的生成和质量检查

对于使用硬件密码模块的证书订户，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。

6.1.7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。

6.2　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

GZSK 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。

6.2.2私钥多人控制（m 选 n）

GZSK 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。

6.2.3私钥托管

GZSK 运营 CA 私钥不在其他地方托管。订户签名私钥由订户自行保管，KMC 不负责签名私钥托管；对订户加密密钥可按照现行 CPS 提供密钥恢复管理。

KMC 应采用经批准的密码产品和严格访问控制保护托管的加密密钥，密钥以受保护形式保存，所有备份、恢复和管理操作均应经过授权并完整审计。

6.2.4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。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。

6.2.5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。

6.2.6私钥导入、导出密码模块

GZSK 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。

6.2.7私钥在密码模块的存储

私钥以密文的方式分段加密存放在密码模块中。

6.2.8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。

6.2.9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。

6.2.10 销毁私钥的方法

当 CA 的生命周期结束后，GZSK 将根据本 CPS 6.2.5 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。

6.2.11 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 密钥对管理的其他方面

6.3.1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 CP5.5 的相关规定。

6.3.2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 密钥对使用期限原则上与 CA 证书有效期保持一致；订户密钥对使用期限与订户证书有效期及密钥用途要求相匹配。

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。

6.4 激活数据

6.4.1激活数据的产生和安装

CA 私钥的激活数据，遵循本 CP 第 6.2.2 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。

6.4.2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。

6.4.3激活数据的其他方面

当私钥的激活数据进行传送时，应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。

6.5 计算机安全控制

6.5.1特别的计算机安全技术要求

GZSK CA 系统部署在受控机房环境，与其他系统实施安全隔离。边界部署防火墙、入侵检测/防御、漏洞扫描等安全控制，仅开放业务必需的网络访问。

系统采用可信操作系统、严格身份鉴别和访问控制、人员职责分离、操作审批、日志审计、恶意代码防护、补丁管理和业务连续性等措施。按照现行 CPS，至少每半年检查服务器及终端系统补丁状态，履行升级审批并记录实施过程；病毒库至少每月更新并至少每月执行全盘病毒扫描。对停止官方安全支持的操作系统应采取网络隔离、功能限制等强化措施并制定替换计划。

6.5.2计算机安全评估

GZSK 的认证系统已通过国家密码管理局等有关部门的安全性审查。

6.6 生命周期技术控制

6.6.1系统开发控制

GZSK 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。

6.6.2安全管理控制

GZSK 认证服务系统的信息安全管理，严格遵循行业主管部门的规范进行操作，系统的任何变更都经过严格的测试验证后才能进行安装和使用。同时，按照 ISO27001 质量管理体系标准建立了严格的管理制度。

6.6.3生命周期的安全控制

GZSK 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。

6.7　网络的安全控制

GZSK 采用多重异构防火墙系统，所有外部网络和内部网络的沟通都通过受到严密保护的防火墙系统。限制外部对系统的非授权访问，还限制内部系统之间特别是安全级别低的系统对安全级别高的系统的非授权访问。

6.8　时间戳

GZSK 提供时间戳服务，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

GZSK 签发的电子签名认证证书格式符合 GB/T 20518《信息安全技术 公钥基础设施 数字证书格式》及国家密码主管部门相关数字证书格式要求，采用 X.509 V3 格式。证书签名算法使用国家密码主管部门批准的密码算法。

电子签名认证证书主要包含版本号、证书序列号、签名算法标识符、颁发者名称、有效期、主体名称、主体公钥信息、证书策略 OID、密钥用法/扩展密钥用法、CRL 分发点、权威信息访问等扩展项及 GZSK 数字签名。订户证书有效期最长不超过 5 年。

7.1.1 版本号

GZSK 签发的电子签名认证证书采用 X.509 V3 版本。

7.1.2 证书扩展项

证书扩展项的设置应符合 GB/T 20518 和相关密码标准。GZSK 根据证书类型设置密钥用法、扩展密钥用法、主体密钥标识符、颁发机构密钥标识符、基本限制、CRL 分发点、权威信息访问和证书策略等扩展项。

7.1.3 算法对象标识符

GZSK 电子签名认证证书采用国家密码主管部门批准的密码算法。目前电子认证系统支持 SM2-256 密钥类型证书，并按照国家现行标准使用相应算法标识符。

7.1.4 主体名称

证书主体名称采用 X.500 甄别名（DN）命名方式。个人证书、机构证书、设备证书等应根据证书类型使用具有实际意义并经过验证的主体名称；不得使用匿名或伪名。具体 DN 字段和验证规则按照现行 CPS 执行。

7.1.5 名称限制

证书主体名称必须具有真实、明确和可验证的含义，使用外文名称时不得产生歧义。写入证书的组织名称、个人姓名、部门、职务、域名、设备名称等应按其性质完成相应验证。

7.1.6 证书策略对象标识符

电子签名认证证书的 Certificate Policies 扩展项应包含主管部门制定的相应等级证书策略 OID：个人基础级 2.16.156.339.2.1.1.1；个人高等级 2.16.156.339.2.1.1.2；机构基础级 2.16.156.339.2.1.2.1；机构高等级 2.16.156.339.2.1.2.2。仅用于电子政务电子签名的证书按

相应电子政务策略执行。CA 证书策略扩展项按照根证书体系及主管部门要求设置。

7.1.7 策略限制与限定符

证书策略限制、策略映射、策略限定符等扩展项按照证书类型、信任体系和现行标准配置；未使用的扩展项不得产生误导性含义。

7.2 证书撤销列表

GZSK 证书撤销列表（CRL）格式符合 GB/T 20518 及相关现行标准要求。CRL 至少包含版本、签发者、thisUpdate、nextUpdate、签名算法以及被撤销证书序列号和撤销时间等信息。

CRL 每 24 小时自动发布一次，必要时可人工发布最新 CRL；CRL 应由具有相应权限的 CA 私钥进行签名并提供完整性保护。

7.3 在线证书状态协议

GZSK 提供 OCSP 在线证书状态查询服务。OCSP 服务按照国家及行业现行标准实现，并与 CRL 中的证书状态保持一致。GZSK 原则上提供 7×24 小时服务，服务可用率不低于 99%。

8. 认证机构审计和其他评估

8.1 评估的频率或情形

GZSK 建立内部审计、认证业务审计和全面符合性评估制度，并接受主管部门依法开展的监督检查和评估。安全策略委员会负责组织内部审计评估，确保评估覆盖电子认证业务合规性、技术安全、运营管理和风险控制。

内部综合审计和风险评估原则上每年至少开展一次；操作日志、安全运行和业务数据按照本 CP 及 CPS 规定的周期进行持续检查。发生重大系统变更、安全事件或主管部门要求时，可开展专项审计。

8.2 评估者的资质

内部审计人员应具备与电子认证、PKI、密码、网络安全、合规或审计相关的专业能力，并保持独立性。外部审计评估机构及人员应具备相应资质、专业能力和良好信誉。

8.3 评估者与被评估者之间的关系

内部评估人员与被评估业务岗位之间应保持职责分离，避免直接利益冲突。外部评估者不得与 GZSK 存在足以影响评估独立性、公正性和客观性的利益关系。

8.4 评估内容

评估内容包括但不限于：法律法规和 CP/CPS 符合性；服务告知、身份查验、订户意愿确认和协议签署；证书申请、签发、续期、变更、撤销和冻结；密钥与密码设备管理；物理与环境安全；网络与系统安全；日志审计和记录归档；个人信息和数据安全；业务连续性和重大事件管理；证书状态服务；人员和权限控制。

8.5 对问题与不足采取的措施

审计或评估发现的问题应明确责任部门、整改措施和完成期限，并进行跟踪验证形成闭环。存在重大风险或影响电子认证服务安全的，应立即采取控制措施并按照主管部门要求报告。

8.6 评估结果的传达与发布

内部审计、专项审计和符合性评估结果按照公司管理制度向安全策略委员会及相关责任部门传达；依法应向主管部门报送的报告，应在规定期限内报送。对外公开范围按照法律法规、主管部门要求和信息保密规则确定。

8.7 认证业务审计

GZSK 应对电子签名认证证书业务开展周期性认证业务审计。

审计应重点抽查身份查验记录、订户意愿记录、订户协议、证书申请和签发记录、撤销冻结记录、证书状态发布、费用和投诉处理等内容，确认实际业务与现行 CP/CPS 一致。

8.8 全面符合性评估

GZSK 应定期开展全面符合性评估，覆盖法律法规、监管要求、技术标准、策略文档、信息系统、密码设备、人员管理、安全管理、业务连续性和数据保护等方面。评估形成正式报告，并对问题整改情况进行持续跟踪。

9. 法律责任和其他业务条款

9.1 费用

根据市场和管理部门的规定，GZSK 会根据不同服务项目收取合理的费用。

9.1.1 证书签发和续期费用

数字证书的收费标准按照国家、地方及业界的收费标准执行。根据证书实际应用的需要，GZSK 在不高于收费标准的前提下可以对证书价格进行适当调整。

如果订户与 GZSK 签署的协议中价格与公布价格不一致，以协议中的价格为准。

9.1.2证书查询费用

暂不对此项服务收费，但保留对此项服务收费的权利。

9.1.3证书撤销或状态信息的查询费用

暂不对此项服务收费，但保留对此项服务收费的权利。

9.1.4其他服务费用

GZSK 保留对其他服务项目收费的权利。

9.1.5退款策略

除非 GZSK 违背了本 CP 所规定的责任与义务，订户可以要求退款。否则，GZSK 对订户收取的费用均不退还。

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。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。

9.2.1保险范围

GZSK 根据业务发展情况决定其投保策略。

9.2.2其他资产

无规定。

9.2.3对最终实体的保险或担保

无规定。

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、与订户之间的协议、资料中未公开的内容等属于保密信息。除非法律明文规定或政府、执法机关等的要求，GZSK承诺不对外公布或透露订户证书信息以外的任何其它隐私信息。

2、订户私钥属于机密信息，订户应当根据本CP的规定妥善保管，如因订户自己泄漏私钥造成的损失，订户应自行承担。

9.3.2不属于保密的信息

不属于保密的信息包括:

1、证书信息和CRL 中的信息。

2、经公开或通过其他途径成为公众领域的一部分数据和信息。

3、有权披露的第三方披露给接受方的数据和信息。

4、其他可以通过公共、公开渠道获得的信息。

9.3.3保护保密信息的责任

GZSK 有严格的管理制度、流程和技术手段来保护保密信息，包括但不限于商业机密、客户信息等。

9.4　个人隐私保密

9.4.1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。

9.4.2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。

9.4.3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。

9.4.4保护隐私的责任

GZSK 及其内部授权岗位、订户、依赖方等均应按照本 CP 的规定承担相应的隐私保护责任。

9.4.5使用隐私信息的告知与同意

GZSK 收集、使用、保存和处理订户个人信息应遵循合法、正当、必要和诚信原则，并按照适用法律法规履行告知、同意或其他合法性基础要求。电子认证业务所必需的身份查验、证书签发、状态管理和监管留存，应在订户协议、隐私告知或其他适当载体中明确。

9.4.6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。

9.4.7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 陈述与担保

9.6.1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。

GZSK 应对内部 RA/LRA 系统角色、受理岗位和认证业务执行情况实施审计，确认相关业务活动符合本 CP、现行 CPS 及内部管理制度要求。

9.6.2 内部注册与受理岗位的陈述与担保

承担 GZSK 内部证书注册、受理、审核、客户服务等职责的岗位和人员，应遵守本 CP、现行 CPS、内部管理制度和授权范围，严格执行服务告知、身份查验、意愿确认、协议签署、数据留存和操作审计要求。

任何内部岗位不得将 GZSK 依法应自行履行的核心认证职责擅自转委托给外部机构或个人。

9.6.3订户的陈述与担保

订户确认已经阅读和理解了 CP 及有关规定的全部内容，并且受此 CP 文件规定的约束。

9.6.4依赖方的陈述与担保

依赖方确认已经阅读和理解了 CP 及有关规定的全部内容，并同意受此 CP 文件规定的约束。

9.6.5 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 CP 及有关规定的全部内容，并同意受此 CP 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须的审核文件，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。（不可抗力事件具体见本 cps 9.16.5）

9.8 有限责任

如果 GZSK 根据本 CP 或任何法律规定，以及司法判定需承担赔偿或补偿责任的，GZSK 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

9.9 赔偿

9.9.1 用户申请 GZSK 赔偿

GZSK 的赔偿内容:

1、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。

2、GZSK 必须妥善保管给订户所签发的电子证书和密码，

不得泄漏或交付他人。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。

3、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。

4、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。

5、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。

6、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。

GZSK 赔付流程如下:

1、订户向公众数科客服部赔付中心提交赔偿申请，客服部赔付中心指派专人根据订户提交的赔偿申请原因告知订户需提供的相关的申请说明及相关证明材料,对于某一行业专属项目的赔付申请需主管部门提交相应的情况说明。

2、赔付中心专人将根据订户所提交的材料交进行调查验证，涉及到的其他相关部门全力配合

3、当赔付中心专人确认为订户自有行为造成的损失，应电话联系订户，安抚其订户情绪，告知其造成的损失原因以及避免后期再次发生行为规范。

4、赔付中心专人出具相关报告，关闭此赔付流程。

5、当赔付中心专人确认不是订户责任则出具相关调查报告交由客服部经理。

6、客服部经理发起内部会审，附上相关赔付报告及订户申请材料，由相关部门（行政部、财务部、技术运维部）指派专人进行审核，当审核无误后在赔付报告上进行签字确认并交由各部门经理进行签字确认，最后提交给公司总经理审批，审批同意后发回客服部，由其按公司相关制度进行赔偿事宜。

7、当客户赔付完成后，关闭此流程。

9.9.2 GZSK 申请用户赔偿

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。

1、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。

2、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。

9.10　有效期限与终止

9.10.1 有效期限

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

9.10.2 终止

GZSK 终止电子认证服务时，本 CP 终止。

9.10.3 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》、《电子认证服务管理办法》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。

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 CP 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

9.12.1 修订程序

同本 CP 1.5.4.

9.12.2 通知机制和期限

本 CP 修订经批准后，应通过 GZSK 官方网站及时公布。涉及电子认证业务规则或证书策略变更的，GZSK 按照《电子认证服务管理办法》等规定，自公布之日起三十日内向工业和信息化主管部门履行备案义务。重大变更对现有订户权利义务产生实质影响的，应采用适当方式进行告知。

9.12.3 必须修改业务规则的情形

当本 CP 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 CP 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 CP 的相关内容。

9.13 争议处理

GZSK、订户、依赖方或其他参与者之间发生与电子认证服务有关的争议时，应优先依据订户协议、依赖方规则、本 CP 和现行 CPS 协商处理。

协商不能解决的，可依法通过调解、仲裁（存在有效仲裁协议时）或诉讼解决。诉讼管辖按照双方协议及中华人民共和

国法律确定。GZSK 应妥善保存证书申请、身份查验、意愿确认、协议签署、证书生命周期操作、日志、时间记录和证书状态信息等电子认证证据，以支持争议处理和举证。

9.14 管辖法律

GZSK 的 CP 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 与适用法律的符合性

GZSK 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

9.16.1 完整协议

CP、CPS、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。

9.16.2 转让

本 CP 中各方的权利和义务，不能通过任何形式转让给任何实体。

9.16.3 分割性

本 CP 的某一条款被宣布为非法、不可执行或无效时，GZSK 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。

9.16.4 强制执行

无规定。

9.16.5 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

GZSK 对本 CP 有最终解释权。

10. 文件历史记录

修订日期	版次	修订说明	发布日期
2020.11.15	V1.0	创建	2020.11.15
2022.9.13	V2.0	1、修订了 CP 3.2.2 条款，在“机构身份鉴别项”中增加对机构高级证书与设备证书鉴别项； 2、增加 5.1.8 节关于“同城异地备份”说明 3、修改 cp6.2.3 条款，“不允许托管”； 4、修订 CP 关于“激活私钥的方法”相关条款	2022.9.13

		5、修改 CP 关于“激活私钥”相关管理规定； 6、修改 CP 增加 9.7.1 小节赔付监督机制；	
2023.3.11	V3.0	1、修改 CP 版本号 V3.0； 2、修改 CP6.2.3 条款“私钥托管”内容； 3、修改了 CP 6.2.10“销毁私钥的方法”，规定了“需要在所有密钥管理员的参与下进行安全地销毁” 4、修改了 CP 6.2.4“私钥备份”，规定了对加密机的密钥备份操作需 5 人才可完成； 5、修改了 CP6.4.1 激活数据的产生和安装条款； 6、修改了 CP9.7 担保免责小节； 7、修改了 CP9.9 赔偿小节。	2023.3.11
2026.10.30	V4.0	根据《山东公众数科数字科技有限公司电子认证业务规则》2.4 版及工业和信息化主管部门电子认证业务规则规范相关要求进行全面修订：更新机构名称与联系方式；明确四类电子签名认证证书及 OID；强化服务告知、身份查验、订户意愿确认、协议签署和数据留存；取消外部 RA 承担核心认证职责的表述；CRL 周期调整为 24 小时；补充证书状态服务可用率、重大事项报告、业务连续性、终止服务、认证业务审计和全面符合性评估等要求；统一证书撤销、续期等术语。	2026.10.30