GZSK
Certificate Policy
（CP）V3.0

江苏公众数科数字科技有限公司

证书策略 V3.0

目 录

GZSK 1
1.概括性描述 5
1.1 概述 5
1.2 文档名称与标识 5
1.3 电子认证活动参与者 5
1.4 证书应用 6
1.5 策略管理 7
1.6 定义和缩写 8
2.信息发布与信息管理 11
2.1 认证信息的发布 11
2.2 发布的时间或频率 11
3.身份标识与鉴别 12
3.1 命名 12
3.2 初始身份确认 13
3.3 密钥更新请求的标识与鉴别 16
3.4 注销请求的标识与鉴别 16
4. 证书生命周期操作要求 17
4.1 证书申请 17
4.2 证书申请处理 18
4.3 证书签发 19
4.4 证书接受 19
4.5 密钥对和证书的使用 20
4.6 证书更新 21
4.7 证书密钥更新 22
4.8 证书变更 24
4.9 证书注销和冻结 25
4.10 证书状态服务 30
4.11 订购结束 31
4.12 密钥生成、备份与恢复 31
5.认证机构设施、管理和操作控制 32
5.1 物理控制 32
5.2 程序控制 35

5.3 人员控制 36
5.4 审计日志程序 38
5.5 记录归档 40
5.6 电子认证服务机构密钥更替 41
5.7 损害与灾难恢复 42
6. 认证系统技术安全控制 43
6.1 密钥对的生成和安装 43
6.2私钥保护和密码模块工程控制 45
6.3 密钥对管理的其他方面 48
6.4 激活数据 49
6.5 计算机安全控制 50
6.6 生命周期技术控制 50
6.7 网络的安全控制 51
6.8 时间戳 51
7. 证书、证书注销列表和在线证书状态协议 52
7.1 证书 52
7.2 证书注销列表 57
8. 认证机构审计和其他评估 57
8.1 评估的频率或情形 57
8.2 评估者的资质 58
8.3评估者与被评估者之间的关系 58
8.4 评估内容 58
8.5对问题与不足采取的措施 59
8.6 评估结果的传达与发布 59
9.法律责任和其他业务条款 59
9.1 费用 59
9.2 财务责任 60
9.3 业务信息保密 61
9.4 个人隐私保密 62
9.5 知识产权 63
9.6 陈述与担保 64
9.7 担保免责 65
9.8 有限责任 66
9.9 赔偿 66

9.10 有效期限与终止 68
9.11 对参与者的个别通告与沟通 69
9.12 修订 69
9.14 管辖法律 70
9.15 与适用法律的符合性 70
9.16 一般条款 70
9.17 其他条款 71
10. 文件历史记录 72

1.概括性描述

1.1 概述

证书策略（CP，Certificate Policy）是认证机构（CA，Certification Authority）制订的一组策略，表明 PKI 体系中的各个参与者的划分与其义务，并包含证书基本策略。

本文档依据 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》、《电子认证业务规则规范(试行)》等编写。

1.2 文档名称与标识

此文档的名称为《江苏公众数科数字科技有限公司证书策略 V3.0》，并在江苏公众数科数字科技有限公司（以下简称 GZSK）网站发布，网址：http://www.zhengj.cn。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

电子认证服务机构 CA（Certification Authority）承担证书签发、更新、注销、密钥管理、证书查询、证书黑名单（又称证书注销列表或 CRL）发布、政策制定等工作。

1.3.2 注册机构

注册机构 RA(Registration Authority)负责订户证书的申请受理、审批和管理，直接面向证书订户，并负责在订户和 CA 之间传递证书管理信息。

GZSK 与合作机构签署协议，合作机构可成为 GZSK 的注册机构，并遵照 GZSK 相关运营管理规范开展数字证书业务。

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 的订户证书是通用证书，从功能上可以满足下列安

全需要:

1、完整性，保障证书持有者在信息传递过程中信息不被篡改。

2、机密性：保障证书持有者信息的机密性，不会泄露给其他未授权者。

3、不可抵赖性：保障证书持有者的行为不可抵赖。

GZSK 证书支持相应的合法应用，具体应用场景和配套软件在相应 CPS 1.4 节中说明。

1.4.2 限制的证书应用

GZSK 签发的证书禁止使用于任何与国家或地方法律、法规规定相违背的应用系统。

各类证书的密钥用法在订户证书的扩展项中进行了限制。然而基于证书扩展项限制的有效性取决于应用软件，如果参与方不遵守相关约定，其对证书的应用超出限定的应用范围，将不受 GZSK 的保护。

任何未经 GZSK 认可的证书应用都将不受 GZSK 的保护。

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 GZSK 电子认证服务所有策略的最高管理机构，负责制定、维护、审核、批准和解释本 CP，并

作为 CP 实施检查监督的最高决定机构。

GZSK 安全策略委员会由公司各部门拥有决策权的合适代表组成。

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：

电话：025-86809587

邮件：gongzhongsk@163.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

1.5.3 决定 CP 符合策略的机构

GZSK 安全策略委员会负责制定、维护、审核、批准和解释本 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 定义和缩写

缩写

CA	电子认证服务机构

RA	证书注册机构
CP	证书策略
CPS	电子认证业务规则
CRL	证书注销列表
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、注销或更新证书（或更新证书中的密钥)时的业务实施声明。
证书撤销列表 certificate revocation list	一个经电子认证服务机构数字签名的列表，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	具有下列一项或多项功能的实体:识别和鉴别证书申请者，同意或拒绝证书申请，在某些环境下主动注销或冻结

	证书，处理订户注销或冻结其证书的请求，同意或拒绝订户更新其证书或密钥的请求。通常将注册机构简称为 RA，或 RA 机构。

2.信息发布与信息管理

2.1 认证信息的发布

GZSK 的 CPS、CP 以及相关的技术支持信息等在 GZSK 网站上发布。

GZSK 通过目录服务器（LDAP）发布订户的证书和 CRL，已被注销了的证书的信息可从 CRL 站点查获，证书的状态（有效、注销、冻结）可通过 OCSP 服务获得。

具体查询地址见 CPS2.1 认证信息的发布。

GZSK 也将会根据需要采取其他可能的形式进行信息发布。

2.2 发布的时间或频率

CPS、CP 以及相关业务规则在完成 1.5.4 所述的批准流程后的 15 个工作日内发布到 GZSK 网站上，并可确保 7X24 小时可访问。

订户证书的 CRL 发布周期为 8 小时。

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

3.2.1 证明拥有私钥的方法

证明订户拥有私钥的方法是通过证书申请消息（PKCS#10）中包含数字签名来完成的。

GZSK 在为订户签发证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断订户拥有私钥。

3.2.2 组织机构身份的鉴别

任何组织（政府机关、企事业单位等），在以组织名义申请机构证书、设备证书等各类型证书时，应进行严格的身份鉴别，包括以下内容:

1、确认机构是否是真实、合法存在的实体。

2、通过委托授权书等方式（可以是纸质或者经过有效电子签名的电子文件），确认相关文件是否已经盖章、经办人是否得到足够授权。并对经办人进行身份鉴别，鉴别证明包括但不限于经办人个人身份证、军官证护照等由政府机构颁发的能够证明个人身份的有效文件，或者通过实名制手机验证码和人脸识别等至少两种以上组合的个人身份鉴别技术方式进行确认。

3、核查证书申请关键信息与有效文件或其他证明资料是否相符。

4、订户可采用面对面或者其他 GZSK 认可的方式提交证明材料。

5、在申请机构高级证书时，还需进行个人身份的鉴别。

6、在申请设备证书时，需提供设备的品牌、型号、硬件序列号、照片以及相关合同和发票，还需提交域名使用权证明材料。

由机构申请的设备证书需提供企业营业执照、法定代表人身份证明材料，以及经办人的身份证明材料和企业出具的委托授权书。

3.2.3 个人身份的鉴别

个人身份鉴别包括如下内容:

1、鉴别证明包括但不限于个人身份证、军官证护照等由

政府机构颁发的能够证明个人身份的有效文件，或者通过实名制手机验证码和人脸识别等至少两种以上组合的个人身份鉴别技术方式进行确认。

2、核查证书申请关键信息（EMAIL、社会保障卡号等）与有效文件或其他证明资料是否相符。

3、订户可采用面对面或者其他 GZSK 认可的方式提交证明材料。

4、在申请设备证书时，需提供设备的品牌、型号、硬件序列号、照片以及相关合同和发票，还需提交域名使用权证明材料。

3.2.4 没有验证的订户信息

证书中的信息必须经过验证，未经验证的信息不得写入证书。

3.2.5 授权确认

当订户授权经办人办理证书业务时，GZSK 应进行通过委托授权书等方式，确认相关文件是否已经盖章、经办人是否得到足够授权。并对经办人进行身份鉴别，鉴别证明包括但不限于经办人个人身份证、军官证护照等由政府机构颁发的能够证明个人身份的有效文件，或者通过签发有效文件的权威第三方数据库确认。

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。

3.3 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

订户可访问到 GZSK 证书服务系统进行密钥更新申请，系统自动获取订户原证书信息，形成密钥更新申请，GZSK 的证书认证系统将对其进行身份验证。订户也可以到 GZSK 的注册机构申请密钥更新，注册机构必须验证订户与经办人的有效文件。

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。

3.3.2 注销后密钥更新的标识与鉴别

证书注销后不能进行密钥更新。

3.4 注销请求的标识与鉴别

订户本人注销时的身份标识和鉴别使用初始身份验证相同的流程，详见 3.2.2 组织机构身份的鉴别和 3.2.3 个人身份的鉴别。如果是因为订户没有履行本《电子认证业务规则》

所规定的义务，由注册机构申请注销订户的证书时，不需要对订户身份进行标识和鉴别。

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

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、注册过程

订户将证书请求发送到 RA，RA 验证请求并对其签名，然后通过安全加密通道发送给 CA.。

CA 接收到请求后，验证 RA 的签名，签发订户证书。

整个注册过程中，订户身份和申请资料必须进行鉴别，如果申请获得批准和接收，证书可以被签发。

2、责任

GZSK 及注册机构有责任向订户告知数字证书的使用条件、服务收费的项目和标准。

GZSK 及注册机构有责任向订户告知保存和使用订户信息的权限和责任。

订户有责任在其证书申请中提供真实准确的信息，并应当与 GZSK 及注册机构签订合同，明确双方的权利义务。

注册机构有责任对订户提供的证书申请信息和身份证明材料进行检查和审核。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

当 GZSK 及注册机构接收到订户的证书申请后，应按本 CP 第 3.2 节的要求，对订户进行初始身份确认。

4.2.2 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 CP 第 3.2 节的要求;

2、订户接收或不申明反对订户协议的内容;

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 CP 第 3.2 节的要求;

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。

4.2.3 处理证书申请的时间

GZSK 及注册机构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。

4.3 证书签发

4.3.1 证书签发中心注册机构和电子认证服务机构的行为

在订户申请通过鉴别后，RA 系统操作员录入订户申请信息，并提交 RA 系统审核员审核；RA 系统审核员审核通过后，向 CA 系统提交签发请求；CA 系统在获得证书签发请求后，对 RA 的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 电子认证服务机构和注册机构对订户的通告

订户证书签发成功后，将直接或通过 RA 通知订户，并向订户提供获取证书的方式，包括面对面下载。

4.4 证书接受

4.4.1 构成接受证书的行为

1、GZSK 及注册机构代替订户下载证书，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。在证书到期或被注销后，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 证书更新

证书更新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 证书更新的情形

证书订户可在证书到期前 90 天内到 GZSK 注册机构进行证书更新的申请。申请证书更新不需要填写信息，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

对于证书更新的请求，需验证和鉴别一下几个方面:

1、订户必须实际持有原证书的私钥，并且原证书由 GZSK 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

同本 CP 第 4.3.2 节。

4.6.5 构成接受更新证书的行为

同本 CP 第 4.4.1 节。

4.6.6 电子认证服务机构对更新证书的发布

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 构成接受密钥更新证书的行为

同本 CP 第 4.4.1 节。

4.7.6 电子认证服务机构对密钥更新证书的发布

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 证书注销和冻结

4.9.1 证书注销的情形

如有下列情况中的任何一种情况发生，则订户的证书将被注销:

1）订户书面申请注销数字证书;

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 提供证书注销服务;

8）当 CA 用于签发证书的私钥可能被泄露时，将根据应急预案注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 请求证书注销的实体

以下实体可以请求注销订户证书:

1、GZSK 及注册机构依据本 CP 第 4.9.1 节可以要求注销订户证书。

2、证书订户可以申请注销自己的订户证书。

3、政府主管部门及其他权力机关可以依法注销订户证书。

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，申请注销订户证书。

4.9.3 注销请求的流程

证书订户主动申请注销证书，同本 CP 第 4.2 节。

当出现被动注销的情形时，GZSK 将以电话、书面、短信等形式通知证书订户，告知拟注销的证书内容、注销原因、注销操作时限等事项，在确认订户收到注销通知后予以冻结，在注销请求宽限期后订户证书将予以注销。

4.9.4 注销请求宽限期

在主动注销的情形下，无宽限期。

在被动注销的情形下，订户在收到注销通知后的 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注销，若 3 个工作日未回复或申辩理由不被接受，则订户证书将予以注销。

4.9.5 电子认证服务机构处理注销请求的时限

在本 CP 第 4.9.4 节所规定的注销请求宽限期后的 24 小时内注销证书将被处理完毕。

4.9.6 依赖方检查证书注销的要求

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，确认证书未被注销。

4.9.7 CRL发布频率

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8小时自动发布最新CRL，也可人工发布最新CRL;

4.9.8 CRL发布的最大滞后时间

CRL发布的最大延迟时间不超过24小时。

4.9.9 在线状态查询的可用性

GZSK提供OCSP查询服务，服务7X24小时可用。

GZSK的OCSP符合RFC2560 标准。

4.9.10 在线状态查询要求

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

4.9.11 注销信息的其他发布形式

证书注销信息可以通过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，应及时提出证书注销请求。

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 及注册机构依据本 CP 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。

4.9.15 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。

4.11 订购结束

订户证书出现以下情形将被视为订购结束:

1、证书到期;

2、证书注销。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略与行为

为保证订户签名密钥的安全性，订户应在安全的环境下独立生成签名密钥对，并将产生的签名密钥通过加密等手段存储在安全的介质中，订户应及时备份签名密钥，并确保备份签名密钥的安全性，以防签名密钥丢失。

在生成签名密钥对之后与安装设备证书之前的时期内不应更改设备的任何配置，以防签名密钥丢失。在签名密钥丢失或可能泄漏后，需及时申请签名密钥更新。

在订户委托其他可信服务商代替订户生成签名密钥对的情况下，应要求服务商承担相应的保密责任。

证书订户的签名密钥由订户自行保管，GZSK 不接受订户签名密钥的托管和恢复。

证书订户的加密密钥由 GZSK 代订户向密钥管理中心申请生成，并由江苏省国家密码管理局进行监管。当证书订户需要恢复加密密钥时，可向 GZSK 申请恢复加密密钥。

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

江苏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

江苏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

江苏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

江苏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

江苏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、证书注销等事件;

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 每周检查相关操作日志，对发现的安全事件采取相

应的措施。

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 相应的业务持续计划，可确保灾难后的业务连续性能力。

5.8电子认证服务机构或注册机构的终止

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。

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

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

订户加密证书对应的私钥由密钥管理中心托管（KMC 仅提供密钥恢复功能），订户的签名证书对应的私钥由自己保管，密钥管理中心不负责托管签名私钥。

KMC 严格保证订户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

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 30 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。

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，与江苏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 的信息安全管理符合国家相关规定，主要安全技术和控制措施包括：采用安全可信任的操作系统、身份识别和验证、访问控制策略、人员职责分割、业务持续计划等各方面。

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、证书注销列表和在线证书状态协议

7.1 证书

GZSK 签发的证书格式符合 GM/T 0015-2012 数字证书格式规范，包括以下证书域。

7.1.1 版本号

GZSK 签发的证书格式符合 X.509 V3 标准，该信息包含在证书版本属性内。

7.1.2 证书扩展项

证书扩展项是一个或多个证书扩展的序列，GZSK 签发的证书包含私有扩展项，私有扩展项将被设置为非关键性扩展。

包括但不限于如下私有扩展项:

1.个人身份证识别码(OID:1.2.156.10260.4.1.1): 用于表示个人的身份识别号码，该号码可以是身份证、护照或军官证号码。

2.个人社会保险号(OID:1.2.156.10260.4.1.2): 用于表示个人的社会保险号码。

3.企业工商注册号(OID:1.2.156.10260.4.1.3): 用于表示的企业工商注册号码

4.企业组织机构代码(OID:1.2.156.10260.4.1.4): 用于表示企

业的组织机构代码。

5.企业税号(OID:1.2.156.10260.4.1.5):用于表示企业税号码。

7.1.2.1 颁发机构密钥标识符

GZSK 订户证书及 CA 证书中包含颁发机构密钥标识符扩展项，此扩展项用于识别与证书签名私钥相对应的公钥，可辨别同一 CA 使用的不同密钥。该扩展项为非关键项。

7.1.2.2 主体密钥标识符

订户证书中包含主体密钥标识符扩展项，它标识了被认证的公钥，可用于区分同一主体使用的不同密钥（如证书密钥更新时）。该扩展项为非关键项。

7.1.2.3 密钥用法

密钥用法指明已认证的公开密钥用于何种用途。

对于 CA 证书的密钥用法，该项为关键扩展。密钥用法包含证书签名、CRL 签发，其他密钥用法不能出现。对于订户证书，该项为非关键扩展，SM2 类证书为关键扩展。

7.1.2.4 基本限制

基本限制项用来标识证书的主体是否是一个 CA，通过该 CA 可能存在的认证路径有多长，该项定义遵照 RFC5280 之规定。SM2 类

订户证书该项为关键扩展。

7.1.2.5 扩展密钥用法

本项指明已验证的公钥可用于一种或多种用途，可作为对密钥用法扩展项中指明的基本用途的补充或替代。该扩展项为非关键项。

7.1.2.6 CRL 发布点

系统签发的证书包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供的地址和协议下载 CRL。该扩展项为非关键项。

7.1.3 算法对象标识符

GZSK 签发的证书符合 RFC5280 标准，采用 SM2/SM3 密码算法签名。

SM2 算法其 OID 为：1.2.840.10045.2.1 附加参数为 1.2.156.10197.1.301。

7.1.4 主体名称

本项用于描述与主体公钥项中的公钥对应的实体的情况。GZSK 签发证书的甄别名符合 X.500 关于甄别名的规定，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。

DN 可以包含以下几部分:

1、 CN （commonName，OID: 2.5.4.3）: 如果是个人证书，则该部分只能是订户名称，订户名称填写个人姓名；如果是机构证书，则

该部分是订户名称的标准简称或全称，订户名称填写机构名称；如果是机构高级证书，则该部分为约定的其他内容；如果是设备证书，则该部分是设备编码、IP 或者域名。

2、E（emailAddress，OID：1.2.840.113549.1.9.1）：个人证书、机构高级证书该部分为必选部分。用于表示电子邮件地址。

3、G（givenName，OID：2.5.4.42），个人证书、机构高级证书该部分为必选部分。用于表示名。

4、SN（surname，OID：2.5.4.4），个人证书、机构高级证书该部分为必选部分。用于表示姓。

5、 OU（organizationalUnitName，OID：2.5.4.11）：机构高级证书该部分为必选部分，用于表示实体的部门名称，则 GZSK 必须对该部分进行验证。

6、 O（organizationName，OID：2.5.4.10）：机构证书、机构高级证书该部分为必选部分，表示实体的真实名称。使用英文时应与实体有效证件上的真实名称意义一致，并且不能产生歧义。

7、 L （localityName，OID：2.5.4.7）：个人证书、企业证书该部分为必选部分。用于表示所在地。

8、 S （stateOrProvinceName，OID：2.5.4.8）：个人证书、企业证书该部分为必选部分。用于表示所在省。

9、 C （countryName，OID：2.5.4.6）：该部分为必选部分，用于表示证书申请者所在国家或地区的英文简称，全部大写，中国订户标识应为：C=CN。

DN 中包含的国家、省市级名称必须使用权威部门颁发的标准名称（例如：ISO country code）。

7.1.5 名称限制

GZSK 签发的证书，其实体名称不允许为无意义的匿名或者伪名，必须是有明确含义的识别名称，使用英文名称时应能正确表达实体名称。

7.1.6 证书策略对象标识符

CA 证书的证书策略扩展项中，certificatePolicies:policyIdentifier 设置为 anyPolicy。

7.1.7 策略限制扩展项的用法

未使用本扩展域。

7.1.8 策略限定符的语法和语义

未使用本扩展域。

7.1.9 关键证书策略扩展项的处理规则

未使用本扩展域。

7.2 证书注销列表

7.2.1 版本号

GZSK 目前使用的是 X.509 V2 版本的 CRL。

7.2.2 CRL 和 CRL 条目扩展项

CRL 数据定义如下:

1、版本（Version）显示 CRL 的版本号。

2、CRL 的签发者（Issuer）指明签发 CRL 的 CA 的甄别名。

3、CRL 发布时间（thisUpdate）。

4、预计下一个 CRL 更新时间(next update)。

5、签名算法。

6、列出注销的证书，包括注销证书的序列号和注销日期。

7.3 在线证书状态协议

GZSK 系统提供在线证书状态查询服务。其他系统根据业务需要提供该项服务。

在正常的网络状态下，GZSK 可确保有足够的资源使 CRL 和 OCSP 服务在合理的时间内向用户反馈查询结果。

8. 认证机构审计和其他评估

8.1 评估的频率或情形

1、根据《中华人民共和国电子签名法》、《电子认证服务

管理办法》《电子认证服务密码管理办法》规定，每年一次接受主管部门的评估和检查。

2、GZSK 按照公司相关制度和规范要求，每年至少进行一次内部审计和风险评估。

8.2 评估者的资质

GZSK 的内部审计，由安全策略委员会负责组织跨部门的内部审计小组，由内部审计小组执行此项工作。

GZSK 聘请的外部审计机构，必须熟悉 PKI 技术及相关的法律法规、运营管理及标准规范要求，了解计算机信息安全体系，并在业界由良好的声誉。

8.3 评估者与被评估者之间的关系

GZSK 的内部审计，评估者与被评估者应无任何直接的工作联系，工作岗位不能重叠。

外部评估者与 GZSK 之间没有任何业务、财务往来或者其他足以影响评估结果的关系，评估者应在独立、公正、客观的前提下对 GZSK 进行评估。

8.4 评估内容

评估的内容包括但不限于以下方面:

1、物理环境和控制

2、密钥管理操作

3、证书生命周期管理

4、CA 业务规则

8.5 对问题与不足采取的措施

对于 GZSK 内部审计结果中的问题，由内部审计小组负责监督这些问题的责任部门进行改进和完善，从完成审计到采取行动纠正问题的时间一般不超过 30 天。

8.6 评估结果的传达与发布

GZSK 进行内部审计或聘请第三方进行外部审计，审计结果将只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

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 证书签发和更新费用

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 证书注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

江苏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、注册机构、订户、依赖方等都有义务按照本 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 在认证业务范围内使用所获得的任何订户信息，无论是否涉及到隐私，GZSK 都没有告知订户的义务，也无需得到订户的同意。

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。

根据《电子认证服务管理办法》要求，GZSK 有责任审计其注册机构电子认证业务是否符合本 CP 约定。

9.6.2 注册机构的陈述与担保

作为 GZSK 的注册机构，应遵照 GZSK 的证书策略和业务规则，承担电子认证业务中注册机构的应尽的责任和义务。

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

GZSK 有权修订本 CP 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。

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

当 GZSK、订户或依赖方出现争议时，有关方面应依据协议协商解决，协商解决不了的，可通过 GZSK 住所地人民法院诉讼解决。

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 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；	2022.9.13
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