协卡网络信任服务体系
电子签名认证证书电子认证业务规则

UniTrust Network Trust Service Hierarchy

Electronic Signature Certification Practice Statement

(UniTrust NTSH E-Sig CPS)

Version 1.0

生效日期：[2026年10月31日]

上海市数字证书认证中心有限公司

上海市四川北路 1717 号 18 楼

声明

本 CPS 全部或者部分支持下列标准：

- RFC3647：互联网 X.509 公钥基础设施-证书策略和证书业务声明框架
- RFC6960：互联网 X.509 公钥基础设施-在线证书状态协议-OCSP
- ITU-T X.509 V3（1997）：信息技术一开放系统互连－目录：认证框架
- RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构
- 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
- GB/T 20518-2018：信息安全技术 公钥基础设施 数字证书格式
- GB/T 25056-2018：信息安全技术 证书认证系统密码及其相关安全技术规范
- GB/T 19713-2025：网络安全技术 公钥基础设施 在线证书状态协议
- T/CQAE 11034-2025：电子认证业务规则规范

版本控制

版本	发布日期	发布者
V1.0 （现行版本）	2026 年 10 月 31 日	SHECA 安全认证委员会

摘要

版本	版本描述
V1.0	根据《T/CQAE 11034-2025：电子认证业务规则规范》要求，首次制订发布本 CPS。

版权说明

上海市数字证书认证中心有限公司(缩写为 SHECA)，完全拥有本文件的版权。本文件所涉及的“SHECA”及其图标等是由上海市数字证书认证中心有限公司独立持有的，受到完全的版权保护。

其他任何个人和团体可准确、完整的转载、粘贴或发布本文件，但上述的版权说明和上段主要内容应标于每个副本开始的显著位置。未经上海市数字证书认证中心有限公司的书面同意，任何个人和团体不得以任何方式、任何途径（电子的、机械的、影印、录制等）进行部分的转载、粘贴或发布本 CPS，更不得更改本文件的部分词汇进行转贴。

对任何复制本文件的其他请求，请和上海市数字证书认证中心有限公司联系。

地址：中华人民共和国上海市四川北路 1717 号嘉杰国际广场 18 楼（200080），电话：86-21-36393197。电子邮件：policy@sheca.com。

本 CPS 的最新版本请参见本公司网站 https://www.sheca.com/repository,对具体的个人、企业、政府和其他社会组织等不再另行通知。

SHECA 安全认证委员会负责本 CPS 的解释。

注意：

SHECA 数字认证服务遵从中华人民共和国的法律，对于任何因违反法律行为而影响 SHECA 数字认证服务的个人、机构或者其他组织，SHECA 将保留所有的法律权利，以维护 SHECA 的利益。

Copyrights@Shanghai Electronic Certification Authority Co.,Ltd
All Rights Reserved

关于SHECA CPS中主要权利及义务的概要

此概要仅是本CPS重要部分的简单描述，有关条款的完整论述以及其他重要条款和细节请看CPS全文。

1、本CPS文件规定了SHECA电子签名电子认证服务的实施及使用，电子签名电子认证服务包括SHECA电子签名认证证书发放、管理和验证，涵盖了电子签名认证证书整个生命周期内的操作流程、运行管理、运营环境、管理政策等。

2、证书申请者须知：

（1）申请者在申请电子签名认证证书之前，已被建议接受适当的电子签名电子认证相关方面的培训。

（2）从SHECA网站及其他渠道可以得到有关数字签名、证书及CPS的文件，证书申请者可以参加相关的培训和学习。

3、SHECA提供不同类型的证书，申请者应自行或向SHECA咨询决定何种证书适合于自己的需要。

4、申请者必须在接受证书后才可使用证书进行电子签名。申请者在接受证书的同时，就已表明其接受了本CPS规定的权利和义务，并承担相应的责任。

5、如果你是电子签名认证证书的接受者或者依赖方，你必须决定是否信赖它。在此之前，SHECA建议你应检查SHECA的证书目录服务，以确保该证书是正确和有效的，并使用证书检验数字签名是在证书有效期内由该证书的持有者生成的，而且有关信息并未改动。

6、证书持有人同意，如果发生危及私钥安全的状况时，及时通知SHECA。

7、意见与建议

如果使用者对以后 CPS 版本的编辑工作有任何意见与建议，请Email 至：

policy@sheca.com；

或请邮寄至：

中华人民共和国上海市四川北路1717号嘉杰国际广场18楼（200080 ）。

8、更多的信息请看SHECA网站（http:// www.sheca.com）。

目 录

目 录 6

1. 概括性描述 17

1.1 承诺 17

1.1.1 上海市数字证书认证中心有限公司（SHECA） 18

1.1.2 协卡认证网络信任服务体系 19

1.2 基本信息 19

1.3 文档名称与标识 21

1.4 电子认证活动参与者 21

1.4.1 电子认证服务机构 21

1.4.2 订户 22

1.4.3 电子签名依赖方 23

1.4.4 其他参与者 24

1.5 证书应用 24

1.5.1 证书应用分类 24

1.5.2 证书应用限制 25

1.6 策略管理 26

1.6.1 策略管理机构 26

1.6.2 策略文档的批准程序 27

1.6.3 联系人 28

1.7 术语和定义 28

1.8 缩略语 33

2. 信息发布与信息管理 34

2.1 SHECA 网站 34
2.2 认证信息的发布 34
3. 身份标识与鉴别 35
3.1 身份鉴别通用要求 35
3.1.1 通用要求 35
3.1.2 订户告知 35
3.2 初始身份确认 36
3.2.1 证明拥有私钥的方法 36
3.2.2 个人身份的查验 36
3.2.3 机构身份的查验 38
3.3 订户意愿记录 39
3.3.1 订户意愿记录内容 39
3.3.2 个人高等级电子签名认证证书的意愿记录 39
3.3.3 个人基础级电子签名认证证书的意愿记录 40
3.3.4 机构高等级电子签名认证证书的意愿记录 40
3.3.5 机构基础级电子签名认证证书的意愿记录 40
3.4 订户协议 41
3.5 未验证的订户信息 41
3.6 互操作要求 41
3.7 命名 41
3.7.1 名称类型 41
3.7.2 对名称意义化的要求 42
3.7.3 订户的匿名或伪名 42
3.7.4 不同名称形式的规则 42

3.7.5 名称的唯一性 43
4. 证书生存周期操作要求 43
4.1 通用要求 44
4.2 证书申请 44
4.2.1 线上业务流程 44
4.2.2 线下业务流程 48
4.2.3 证书申请批准和拒绝 52
4.3 证书签发 52
4.3.1 签发证书 52
4.3.2 对订户的结果通告 53
4.4 证书接受 53
4.4.1 向订户交付证书的方式 53
4.4.2 接受证书的行为 53
4.4.3 拒绝接受证书的行为 54
4.4.4 信息保存 54
4.5 密钥对和证书的使用 54
4.5.1 订户私钥的使用 54
4.5.2 依赖方对公钥和证书的使用 55
4.5.3 安全事件反馈 56
4.6 证书续期 56
4.6.1 证书续期的情形 56
4.6.2 证书续期请求的处理 56
4.6.3 更新证书的签发 57
4.6.4 构成接受更新证书的行为 57

4.7 证书密钥更新 57
4.7.1 签名证书密钥更新 57
4.7.2 加密密钥更新 58
4.8 证书变更 58
4.8.1 证书变更的情形 59
4.8.2 证书变更请求的处理 59
4.8.3 变更证书的签发 59
4.8.4 构成接受变更证书的行为 59
4.9 证书撤销和冻结 59
4.9.1 证书撤销的情形 60
4.9.2 请求证书撤销的实体 61
4.9.3 撤销请求的流程 61
4.9.4 撤销请求宽限期 62
4.9.5 依赖方检查证书撤销的要求 62
4.9.6 CRL 发布频率 62
4.9.7 CRL 发布的最大滞后时间 62
4.9.8 在线状态查询的可用性 63
4.9.9 在线状态查询要求 63
4.9.10 撤销信息的其他发布形式 63
4.9.11 密钥损害的特别要求 64
4.9.12 证书冻结的情形 64
4.9.13 请求证书冻结的实体 64
4.9.14 冻结请求的流程 64
4.9.15 冻结的期限限制 64

4.10 证书状态服务 64
4.10.1 操作特征 64
4.10.2 服务可用性 65
4.11 停止使用认证服务 65
4.12 密钥托管与恢复 65
4.12.1 CA 密钥的托管与恢复 65
4.12.2 订户私钥的保管与恢复 66
5. 认证机构设施、管理和操作控制 66
5.1 物理控制 66
5.1.1 场地位置与建筑 66
5.1.2 物理访问控制 67
5.1.3 电力与环境保障 68
5.1.4 水患防治 68
5.1.5 消防措施 68
5.1.6 存储媒体管理 68
5.1.7 设备管理 70
5.1.8 备份管理 70
5.2 操作过程控制 70
5.2.1 可信角色 70
5.2.2 职责分离 71
5.3 人员控制 72
5.3.1 可信人员资格要求 72
5.3.2 可信人员培训要求 72
5.4 审计日志程序 73

5.4.1 记录范围 73
5.4.2 记录内容 74
5.4.3 保存期限 74
5.4.4 日志审计内容 74
5.4.5 审计周期 74
5.5 记录归档 74
5.5.1 归档记录的类型 74
5.5.2 归档记录的保存期限 75
5.5.3 归档文件的保护 75
5.5.4 归档文件的备份程序 76
5.5.5 获得和检验归档信息的程序 76
5.6 电子认证服务机构 CA 证书密钥更替 76
5.7 损害和灾难恢复 77
5.7.1 事故和损害处理程序 78
5.7.2 计算资源、软件和/或数据的损坏 78
5.7.3 SHECA 私钥损害处理程序 78
5.8 电子认证服务机构终止 79
5.9 重大事项报告 79
5.9.1 重大事项范围 79
5.9.2 重大事项报告流程 81
6. 技术安全控制 82
6.1 技术安全管理制度要求 82
6.2 密钥对的生成和安装 82
6.2.1 密钥对的生成 82

6.2.2 私钥交付给订户 84
6.2.3 公钥传送给证书签发机构 85
6.2.4 电子认证服务机构公钥传送给依赖方 85
6.2.5 密钥长度 85
6.2.6 公钥参数的生成和质量检查 86
6.2.7 密钥使用目的 86
6.3 私钥保护和密码模块工程控制 87
6.3.1 密码模块的标准 87
6.3.2 私钥多人控制 87
6.3.3 私钥托管 88
6.3.4 私钥备份与恢复 88
6.3.5 私钥归档 89
6.3.6 私钥导入、导出密码模块 89
6.3.7 私钥在密码模块中的存储 89
6.3.8 激活私钥的方法 89
6.3.9 解除私钥激活状态的方法 90
6.3.10 销毁私钥的方法 90
6.3.11 密码模块的评估 91
6.4 密钥对管理的其他方面 91
6.4.1 公钥归档 91
6.4.2 证书操作期和密钥对使用期限 91
6.5 激活数据 92
6.5.1 激活数据的产生和安装 92
6.5.2 激活数据的保护 93

6.5.3 激活数据的其他方面 93
6.6 计算机安全控制 94
6.6.1 特别的计算机安全技术要求 94
6.6.2 计算机安全评估 94
6.6.3 计算机安全控制 95
6.7 生存周期安全控制 95
6.7.1 系统开发控制 95
6.7.2 安全管理控制 95
6.8 网络安全控制 96
6.9 时间戳服务 97
6.9.1 使用范围 97
6.9.2 使用方式 97
6.9.3 保障机制 97
6.9.4 技术标准 98
7. 证书、证书撤销列表和在线证书状态协议 98
7.1 证书 98
7.1.1 版本号 98
7.1.2 证书扩展项 98
7.1.3 算法对象标识符 99
7.1.4 名称形式 99
7.1.5 名称限制 99
7.1.6 证书策略对象标识符 100
7.1.7 策略限制扩展项的用法 100
7.1.8 策略限定符的语法和语义 100

7.1.9 关键证书策略扩展项的处理规则 100
7.2 证书撤销列表 100
7.3 在线证书状态协议 100
8. 认证机构审计和相关评估 101
8.1 审计评估制度 101
8.2 认证业务审计 102
8.3 全面符合性评估 103
9. 法律责任和其他业务条款 104
9.1 收费项目 104
9.2 财务责任 106
9.2.1 保险范围 106
9.2.2 其他资产 106
9.2.3 对最终实体的保险或担保 106
9.3 业务信息保密 106
9.3.1 保密信息范围 106
9.3.2 不属于保密的信息 107
9.3.3 保护保密信息的责任 107
9.4 个人隐私保护 108
9.4.1 隐私保护原则 108
9.4.2 作为隐私处理的信息 108
9.4.3 不被视为隐私的信息 108
9.4.4 保护隐私的责任 108
9.4.5 个人信息收集规则 109
9.4.6 个人信息存储与安全防护 109

9.4.7 使用隐私信息的告知与同意 110
9.4.8 依法律或行政程序的信息披露 110
9.4.9 其他信息披露情形 110
9.5 知识产权 111
9.6 陈述与担保 112
9.6.1 电子认证服务机构的陈述与担保 112
9.6.2 订户的陈述与担保 113
9.6.3 依赖方的陈述与担保 115
9.7 担保免责 115
9.8 赔偿责任限制 116
9.8.1 赔偿范围 116
9.8.2 赔付计算方式 117
9.8.3 赔付监督机制 117
9.9 赔偿 117
9.9.1 赔偿范围 117
9.9.2 赔偿限额 118
9.10 有效期限与终止 119
9.10.1 有效期限 119
9.10.2 终止 119
9.10.3 效力的终止与保留 120
9.11 对参与者的个别通告与沟通 120
9.12 修订 120
9.12.1 修订程序 120
9.12.2 通知机制和期限 121

9.12.3 必须修改 OID 的情形 121
9.13 争议处理与举证 121
9.13.1 争议处理 121
9.13.2 举证制度 122
9.14 管辖法律 122
9.15 与适用法律的符合性 122
9.16 一般条款 122
9.16.1 完整协议 122
9.16.2 转让 123
9.16.3 分割性 123
9.16.4 强制执行 123
9.16.5 不可抗力 123
9.16.6 版本标注 123
9.17 其他条款 124

1. 概括性描述

上海市数字证书认证中心有限公司(Shanghai Electronic Certification Authority Co.,Ltd.，缩写为 SHECA)是中国领先的第三方电子认证服务机构，首批获得电子认证服务许可证，以专业的管理、运营和技术保障能力向用户提供各类数字证书服务，为建设一个和谐、信任的网络和数字环境而努力。

SHECA 制定本文档——《协卡网络信任服务体系电子签名认证证书电子认证业务规则 (UniTrust NTSH E-Sig CPS)》（以下简称本 CPS）规定了电子签名认证证书申请、签发、更新、撤销、管理等业务流程、方式、遵循的标准和规范，以及相应的服务、技术措施和权利义务约定、法律保障等。

1.1 承诺

SHECA 严格按照《中华人民共和国电子签名法》等法律的规定及工业和信息化部、国家密码管理局的要求，提出、设计、建设并运行协卡认证网络信任服务体系（UniTrust Network Trust Service Hierarchy，缩写为 UniTrust NTSH，简称协卡认证体系）。协卡认证体系对外提供可靠的数字证书及相关服务，为基于互联网络的各类信息交互和交易活动建立信任关系，保证各参与方主体身份的真实性、信息的保密性、信息的完整性以及行为的不可抵赖性。

本 CPS 主要依据中国电子质量管理协会发布的《电子认证业务规则规范（T/CQAE 11034—2025）》编写，并遵循《中华人民共和国电子签名法》 、《电子认证服务管理办法》、《电子认证服务密码管理办法》等法律法规的要求，适用的证书链参见本 CPS 1.2 部分。

本 CPS 详细阐述了 SHECA 在签发、管理电子签名认证证书和运营维护证书服务设施的活动，并提供在实际工作和运行中应遵循的各项规范。CPS 详细叙述了认证业务的整个过程，并且提供法律上的约束并提醒当事人在本 CPS 条款规定的范围内产生、使用证书并进行证书验证。

作为实际应用和操作的文件依据，本 CPS 适用于 SHECA 电子签名认证证

书订户和依赖方。所有这些主体都必须完整地理解和执行 SHECA 电子签名电子认证业务规则规定的条款，享有相应的权利，承担相应的责任和义务。SHECA 承诺：严格按照本 CPS 的规定签发电子签名认证证书，在证书有效的情况下，保证证书能唯一地与身份明确的实体相关联，公钥能与经身份鉴别的实体唯一相对应。

本 CPS 向社会公布 SHECA 关于电子签名认证证书服务的基本立场和观点，任何和 SHECA 有关联的组织、机构、团体和个人，必须完整理解和准确解释其内容。SHECA 树立以人民为中心的服务理念，承担社会责任，严格遵守《电子签名法》等法律法规。

SHECA 郑重承诺：在开展经营和服务活动时，严格进行应用业务风险评估，绝不为存在违法违规风险的业务提供电子认证服务；同时，主动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，并建立问题纠治长效机制，确保持续符合合规要求。

1.1.1 上海市数字证书认证中心有限公司（SHECA）

上海市数字证书认证中心有限公司(Shanghai Electronic Certification Authority Co.,Ltd.，缩写为 SHECA，简称上海 CA)成立于 1998 年，是中国成立最早的专业第三方电子认证服务机构，全国运行经验最丰富、应用领域最广、用户群体最大的认证机构之一。

2005 年 4 月，获得国家密码管理局“电子认证服务密码使用许可证”；2005 年 9 月，获得工业和信息化部“电子认证服务许可证”，成为《中华人民共和国电子签名法》实施后首批获得国家运营资质的电子认证服务机构；2008 年 6 月，通过国际 WebTrust 认证；2008 年 12 月，实现 CA 证书内置于微软操作系统，是全国第一家实现全球化电子认证服务的机构。

SHECA 拥有一支专业、强大的技术研发队伍，专注于研发构建网络和数字信任体系建设所需要的技术、产品和服务，拥有多项自主研发、自主产权的核心技术与产品以及解决方案。

SHECA 作为依法设立的第三方电子认证服务机构，建设和运营的协卡认证

体系（UniTrust NTSH），是中国最有影响的数字证书发放和管理机构，发放和管理的数字证书得到广泛的应用。

1.1.2 协卡认证网络信任服务体系

协卡认证网络信任服务体系（UniTrust Network Trust Service Hierarchy，缩写为 UniTrust NTSH，简称协卡认证体系）提出“一证在手，走遍天下”的服务理念，为电子政务、电子商务及各类数字化活动的各个参与主体发放数字证书，可以实现跨行业、跨地域的电子认证服务。

协卡认证体系拥有清晰、完整的 PKI 层次架构，以实现不同应用对证书服务的不同需求。每个根 CA 下设中级 CA，以签发用户证书。因此，协卡认证体系包含了根 CA、中级 CA。协卡认证体系所有和电子签名认证证书相关的服务和管理，都完整、正确、全面的贯彻和实施本文档以及相应证书策略的要求。

1.2 基本信息

SHECA 的基本信息如下：

机构名称	上海市数字证书认证中心有限公司
法定代表人	李小山
机构住所、经营场地	注册地址：上海市虹口区四川北路 1717 号 18 楼
联系方式	电话：021-36393100
电子认证服务许可证信息	许可证编号：ECP31010920008 许可证有效期至：2025 年 09 月 23 日（换证过程中） 许可证首发日期：2005 年 09 月 23 日 发证机关：工业和信息化部

证书链及其包含证书信息如下：

证书名称	证书序列号	颁发者名称	密码算法	密钥长度	有效期起始	有效期终止	计划服务至
UCA Root G2	4452a0b2e90539467a53b04f236aa3c3	UCA Root G2	sha256 with rsa	2048	2016/09/1	2036/12/31	2033/12/31
SHECA G2	5c83ababcb04be79d7fce5a440b59304	UCA Root G2	sha256 with rsa	2048	2023/12/26	2036/12/26	2033/12/31
UCA Root SM2	7a4701fae41cd96c6054c0636aef04ad	UCA Root SM2	sm3 with sm2	256	2015/03/13	2038/12/31	2035/12/31
SHECA SM2 Identity CA G1	722c9edcae54f9d005671799ac824c07	UCA Root SM2	sm3 with sm2	256	2021/08/19	2036/08/18	2033/12/31
UCA Rapid Root	4e72c8d6c82a85545182ac7026209ae5	UCA Rapid Root	sha256 with rsa	2048	2015/01/28	2040/12/31	2037/12/31
SHECA Rapid	60b92635bf7785eab94b8b32dad89301	UCA Rapid Root	sha256 with rsa	2048	2015/01/28	2040/12/31	2037/12/31
UCA Rapid SM2 Root	72fbf12a198a89263b27b33cdddf7e74	UCA Rapid SM2 Root	sm3 with sm2	256	2017/11/1	2042/12/31	2039/12/31
SHECA Rapid SM2	59ed7a8cde0d698cf81e3ccc89bf16da	UCA Rapid SM2 Root	sm3 with sm2	256	2017/11/1	2042/12/31	2039/12/31
ROOTCA	2bb5b8c349b031919fc0c67967dfe7c2	国家根	sm3 with sm2	256	2012/07/14	2054/07/7	/
SHECA SM2	2da1a6bd0ce76c624e634b7d6a29d02a	ROOTCA	sm3 with sm2	256	2013/09/13	2033/09/8	2030/12/31
UCA RSA Non-Public Root CA - G1	59129488c8b6dba021ac2c3e47a6e52b	UCA RSA Non-Public Root CA - G1	SHA256WithRSA	2048	2018/04/12	2043/04/11	2027/12/31
UCA RSA Non-Public CA - SHA256 - G1	61c5bfbf4e6438e0657511aad66374bc	UCA RSA Non-Public Root CA - G1	SHA256WithRSA	2048	2018/04/12	2033/04/11	2027/12/31

UCA SM2 Non-Public Root CA - G1	48acf2b838bf067de4108ecae9a5dfc7	UCA SM2 Non-Public Root CA - G1	SM3WithSM2	256	2018/04/12	2043/04/11	2027/12/31
UCA SM2 Non-Public CA - G1	66521c3abb2cc0257431daee9770c84e	UCA SM2 Non-Public Root CA - G1	SM3WithSM2	256	2018/04/12	2043/04/11	2027/12/31

详细 CA 证书信息披露在 SHECA 官网信息库：

https://www.sheca.com/repository

1.3 文档名称与标识

CPS 版本号	V1.0
发布日期	2026 年 10 月 31 日
遵循的证书策略 OID	参见本文件 1.5 部分
CPS 的文档 OID	1.2.156.112570.1.0.11
历史版本信息	无

1.4 电子认证活动参与者

1.4.1 电子认证服务机构

SHECA 是依法设立的电子认证服务机构（CA），建设和运营协卡认证体系。作为被信任的第三方，协卡认证体系内有多个可以签发证书的实体，包括不同的根 CA 和中级 CA，这些签发实体作为 CA，均可发放证书。根 CA 只签发中级 CA 证书，中级 CA 可签发最终用户证书。协卡认证体系的 CA 为电子政务、电子商务和其它网络作业的各类参与方（以下称主体或实体，包括组织、个人及其它任何有明确身份标识的主体或实体）发放数字证书，保证公钥能与确定的主体身份唯一相对应。

SHECA 建立了完善的 CA 运行机制和严密的安全控制机制，独立生成密钥对，自主签发根 CA 证书（ROOT CA）。SHECA 根据证书发展策略、证书应用策略以及相关的授权和协议，可以签发下一级的中级 CA 证书。SHECA 更新根 CA 密钥对时，必须按照国家主管机构、法律和政策等规定的程序，经过 SHECA 安全认证委员会的同意。SHECA 安全认证委员会作为 SHECA 数字证书的政策制订机构，将决定 SHECA 根 CA 和中级 CA 密钥对的更新和切换的策略和行动。

SHECA 签发的证书与每一个证书申领实体的公钥绑定。SHECA 承诺，已签发的、在有效期内的证书，将采用证书目录服务器/证书撤销列表（Certificate Revocation Lists）服务器，公布该证书可以公开的信息和状态。

SHECA 根据业务需要，与 SHECA 认证服务体系中未涉及的其它 CA 机构建立互联互通关系。互联互通是指两个完全独立的、采用各自 CPS 的证书认证中心建立相互信任关系，从而使双方的客户可以实现互相认证。当 SHECA 需要建立与某一个 CA 认证服务机构的互联互通关系时，即信任某 CA 机构发放的证书，SHECA 将审查该 CA 机构目前已在执行的电子认证业务规则、证书业务相关文件、承诺以及操作规程。所有信任 SHECA 的机构，如果要接受与 SHECA 建立互联互通关系的 CA 所发放的证书，必须自行检查该 CA 的操作规范及其他证书业务相关的文件。互联互通并不表示 SHECA 批准了或赋予了其它非 SHECA 关联的独立 CA 机构任何权力。

1.4.2 订户

订户，即被颁发给一张证书的证书主体，在不同的阶段，也称为证书申请人、证书持有人。包括已经申请并拥有 SHECA 签发的电子签名认证证书的个人、法人和非法人组织等。

订户在申请证书之前，已被建议接受必要的电子认证技术使用方面的培训。订户可以从SHECA得到有关电子签名、证书、PKI等相关的文件和学习资料，SHECA会根据实际情况，通过网站、培训活动、宣传材料等提供。SHECA提供不同类型的证书，订户应决定何种证书适合于自己的需要。订户同意如遇危及私钥安全的状况时及时通知SHECA。

证书申请者（Certificate Applicant），每一个期望作为SHECA或其下级操

作中级CA 的证书订户的实体，都可以成为SHECA的证书申请者，根据其想要的证书类型，按照SHECA CPS的规定提供必要的信息，完成申请过程。

如果证书申请者不能提供SHECA所需的信息，其申请过程将延迟或终止。一经提交证书申请，就意味着所有的证书申请者已授权SHECA可进行安全问题的调查。所有这些调查必须符合相关的隐私权和数据保护等方面法律法规的要求，申请人同意协助SHECA采用后者认为适当的并与CPS一致的方式，来确定所有的事实、发生环境和其他相关信息。

如果该证书申请经过了SHECA的所有必要鉴别程序并鉴别合格，SHECA将依照CPS的规定为申请者签发证书，以证明已经批准了申请者的证书申请。如果申请者未能成功通过鉴别，SHECA将拒绝申请者的证书申请。被拒绝的证书申请者随后可再次提出申请。

SHECA 只有在经过证书申请者的同意后才签发证书。证书申请者一旦提交了证书申请，尽管事实上还没有接受证书，但仍被视为该订户已同意接受 SHECA 为其签发证书。同时，SHECA 可以根据其独立判断，拒绝给任何主体签发证书，并且不对因此而导致的任何损失或费用承担任何责任和义务。

1.4.3 电子签名依赖方

依赖方，指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。在 SHECA 认证服务体系范围内，任何使用证书进行网上作业的证书持有者和按照本 CPS 合理信任证书真实性的任何实体，称为 SHECA 的依赖方。依赖方可以是也可以不是一个订户。

对于依赖方，SHECA 承诺，证书主体中的所有信息都是准确的。SHECA 完全遵照本 CPS 的规定签发电子签名认证证书。

依赖方应合理信任电子签名认证证书以及相关的电子签名。如果信任电子签名时需要额外保证，依赖方必须在得到这些保证后才能合理信任。

作为订户的依赖方，享有本 CPS 规定的各种相应的权利，包括 SHECA 可能提供的证书保障，以及本 CPS 中涉及的权益。其他依赖方，SHECA 除了担保其所信任的并且由 SHECA 签发的证书和相关签名信息的真实性以外，不承担其它

义务和责任。

1.4.4 其他参与者

以上未提及的，在整个SHECA和其服务架构内参与提供证书服务的其它实体，例如PKI应用技术服务提供者等。

1.5 证书应用

1.5.1 证书应用分类

按照证书主体对象的类型和风险等级，分为个人高等级电子签名认证证书、个人基础级电子签名认证证书、机构高等级电子签名认证证书、机构基础级电子签名认证证书：

证书类型	主管部门证书策略 OID	SHECA 自定义策略 OID	含义
个人高等级电子签名认证证书	2.16.156.339.2.1.1.2	1.2.156.112570.149（适用于普通个人证书） 1.2.156.112570.1.12（适用于职务行为个人证书）	适用于高风险业务、符合《电子签名法》的个人电子签名认证证书
个人基础级电子签名认证证书	2.16.156.339.2.1.1.1		适用于低风险业务、符合《电子签名法》的个人电子签名认证证书
机构高等级电子签名认证证书	2.16.156.339.2.1.2.2	1.2.156.112570.149	适用于高风险业务、符合《电子签名法》的机构电子签名认证证书
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1		适用于低风险业务、符合《电子签名法》的机构电子签名认证证书

注 1：仅有包含了主管部门证书策略 OID 的上述 4 类电子签名认证证书适用于本 CPS。

注 2：SHECA 颁发的下列种类数字证书，如 SSL 证书、代码签名证书、设备证书、身份认证证书等，不适用于本 CPS，不得用于电子签名。

a）SSL 证书：面向 Web 服务、门户网站签发的数字凭证，用于服务器可信身份核验与传输通道加密，保障网站访问过程数据防窃听、防篡改；

b）代码签名证书：面向软件开发者签发的专用签名凭证，适用于应用程序、设备固件、

硬件驱动、软件安装包等载体，实现发布主体身份确权、程序完整性校验，防范恶意篡改与仿冒；

c）设备证书：面向各类硬件设备签发的专用数字身份凭证，适用于服务器、工控终端、物联网设备、密码硬件、网关等各类设备，实现设备身份鉴别、通信加密、数据完整性校验与接入授权，不含自然人、机构主体身份用途证书；

d）身份认证证书：面向自然人、机构实体、硬件设备签发的通用身份凭证，用于各类网络场景主体身份核验；身份认证证书载明的密钥用途中字段中不可否认性（Nonrepudiation）必须为 0，不具备电子签名防抵赖效力。

注 3：SHECA 颁发的电子政务电子签名证书适用于《电子政务电子认证服务业务规则》，仅用于电子政务应用场景，不适用于本 CPS。

注 4：对于不具备独立行为能力的个人，SHECA 不为其签发电子签名认证证书。

在 SHECA 认证服务体系中，目前支持正式证书和测试证书。正式证书的申请者必须通过规定的物理身份认证和 SHECA 需要的鉴别程序。测试证书只能用于测试证书对于应用系统的适应性，以及实现其技术验证可行性，不能用于任何正式的用途。SHECA 对测试证书有严格的规定，其用户名必须以英文“test”或者中文“测试”开头，而且有效期限定为 3 个月。

1.5.2 证书应用限制

每一类型的证书，都只能应用于证书所代表的主体身份适合的用途，否则不受本 CPS 的保护。例如，个人证书不能作为机构证书和设备证书来使用，机构证书不能作为个人和设备证书来使用，职务行为个人证书仅可在其任职单位规定的业务系统/场景中使用。

证书申请者、订户、证书主体、证书持有者和依赖方等各类主体可以根据实际需要，自主判断和决定采用相应合适的证书类型，以及了解证书的应用类型、应用范围，选择各自的应用方式。任何超出本 CPS、电子认证服务协议的规定使用证书的行为，都不会受到本 CPS 的保护，SHECA 不会为其提供任何保证或担保。

SHECA 签发的证书，禁止在如下场景中使用：

a) 涉及人身关系的，如婚姻、收养、继承等；

b) 涉及停止公共事业服务的，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。

涉及生命健康、财产权益等高风险活动的场景，禁止使用基础级电子签名认证证书。

1.6 策略管理

1.6.1 策略管理机构

根据《中华人民共和国电子签名法》、工业和信息化部《电子认证服务管理办法》和《电子认证业务规则规范》的要求，SHECA 制定电子认证业务规则（CPS），并指定专门的机构——SHECA 安全认证委员会作为安全策略管理机构。

SHECA 安全认证委员会，作为 SHECA 认证服务体系所有策略的制订管理机构，由 SHECA 的管理层主要成员、各相关部门主管（服务部门、运营部门、技术部门等）组成，负责 CPS 和 CP 以及配套制度的维护，并作为 CPS 实施检查监督的最高决定机构。

安全认证委员会人员名单，以加盖公章的公司红头文件作为正式依据，通过邮件推送至全体员工，并在办公场所公告栏纸质张贴，确保全体人员全面知悉公示内容。

安全认证委员会负责 CPS 以及配套制度的维护，包括但不限于以下职责:

a) 确定维护 CPS 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、CA 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 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。

SHECA 战略发展部作为 CPS 的工作机构，负责组织起草 CP、CPS 并根据要求提出修改报告以及此方面的对外咨询服务，并负责保存安全认证委员会重大决议的相关文件和会议记录。

1.6.2 策略文档的批准程序

1、决定 CPS 符合策略的机构

SHECA 安全认证委员会作为最高策略管理机构，是 CPS 符合策略的决定机构。

SHECA 保证其制订和发布的 CPS，其执行、解释、翻译和有效性均符合和适用中华人民共和国的法律规定。

战略发展部作为认证服务策略的工作部门，负责 CPS 实施的日常监督检查，保障 SHECA 电子签名电子认证服务体系内的运行符合本 CPS 的要求。

2、CPS 的变更和发布

SHECA 有权对 CPS 进行预期或非预期的修改，非预期修改包括基于行业及公司业务调整的必要修改，预期修改包括每年一次检查电子签名电子认证业务规则，对于电子签名电子认证业务规则的不符合处立即进行更新。

如果出现下列情况，那么必须对本 CPS 进行修改：

- 密码技术出现重大发展，足以影响现有 CPS 的有效性
- 证书策略发生重大变化
- 有关认证业务的相关标准进行更新
- 认证系统和有关管理规范发生重大升级或改变
- 法律法规和主管部门要求
- 现有 CPS 出现重要缺陷

3、具体程序

a) 由 SHECA 战略发展部根据需要成立起草小组，起草拟订后，由战略发展部提交 SHECA 安全认证委员会审批；

b) SHECA 安全认证委员会对战略发展部提供的变更建议报告进行研究，最终作出是否变更的决定，经过该委员会超过 1/2 之上人员同意视为批准；

c) SHECA 安全认证委员会审批通过后，变更后的 CPS 在 SHECA 官网 https://www.sheca.com 进行公布，对本 CPS 所做的修改，将于 CPS 所公布的发布日期生效，所进行的修改将取代以往 CPS 各版本中的任何冲突和指定条款；

d) SHECA 战略发展部在 CPS 公布后三十日内向工业和信息化部备案。

1.6.3 联系人

SHECA 对电子签名电子认证业务规则进行严格的版本控制，并由 SHECA 指定专门的机构和人员负责相关的事宜。任何有关 CPS 的问题、建议、疑问等，都可以与此联系人进行联系。

联 系 人：上海市数字证书认证中心有限公司战略发展部

电　　话：86-21-36393197

地　　址：中华人民共和国上海市四川北路 1717 号嘉杰国际广场 18 楼

邮政编码：200080

电子邮件：policy@sheca.com

CPS 的获取方式包括：

- 以电子的方式在 SHECA 官网的知识库中获取，网站地址：https://www.sheca.com/repository；
- 以电子的方式，通过电子邮件获取，电子邮箱地址：getcps@sheca.com；
- 以书面的方式，由 SHECA 公司战略发展部发布，获取地址：中华人民共和国上海市四川北路 1717 号嘉杰国际广场 18 楼 邮政编码：200080。

1.7 术语和定义

SHECA

上海市数字证书认证中心有限公司（Shanghai Electronic Certification Authority Co.,ltd），缩写为 SHECA。SHECA 是依照《中华人民共和国电子签名法》设立的第三方电子认证服务机构，致力于创建和谐的数字信任环境，向互联网用户提供安全、可靠、可信的数字证书服务。

协卡网络信任服务体系

协卡网络信任服务体系（UniTrust Network Trust Service Hierarchy），缩写为 UniTrust NTSH，简称协卡认证体系，是由 SHECA 建设、运营的一个公开密钥基础设施，提供基于数字证书的电子认证服务。

SHECA 安全认证委员会

SHECA 认证服务体系内的安全策略管理监督机构和 CPS 决定机构。

电子认证服务机构

取得电子认证服务许可证，为需要第三方电子认证的电子签名，签发电子签名认证证书并为有关各方提供真实性、可靠性验证的实体，在本 CPS 中指 SHECA。

受理点

受理点（Registration Authority Terminal，RAT）是受理证书服务的网点，作为 SHECA 直接面向用户的服务主体。

系统管理员

负责安装、配置和维护 CA 系统的软硬件系统，负责 CA 服务器的启动和中止，管理 CA 的操作员。

加密

对数据进行密码变换以产生密文的过程。

密码模块

实现密码运算功能，相对独立的软件、硬件、固件或这三者组合。

密码算法

描述密码处理过程的算法。

密钥

控制密码变换操作的符号序列。

私钥

非对称密码算法中只能由拥有者使用的不公开密钥，本文件亦称电子签名制作数据。

公钥

非对称密码算法中可公开的密钥，本文件亦称电子签名验证数据。

RSA 算法

一种基于大整数因子分解问题的公钥密码算法。

SM2 算法

由 GB/T 32918 定义的一种椭圆曲线公钥密码算法。

SM3 算法

由 GB/T 32905 定义的一种密码杂凑算法。

公钥基础设施（PKI）

基于公钥密码技术，具有普适性，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务的基础设施。

数字证书

也称公钥证书，由认证机构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。

电子签名认证证书

依据《中华人民共和国电子签名法》设立的电子认证服务机构颁发的，可证实电子签名人与电子签名制作数据有联系的数字证书。

注 1：如无具体限定，本 CPS 中的“证书”均指“电子签名认证证书”，本 CPS 中的“密钥”“私钥”均指电子签名认证证书所对应的“密钥”“私钥”。

注 2：可证实电子认证服务机构与电子签名制作数据有联系的数字证书，称为 CA 证书。

电子签名

具有识别签名人身份和表明签名人认可签名数据的功能的技术手段，简称为签名。

数字签名

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。

电子签名人

是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人。

电子签名依赖方

是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的人。

订户

被颁发给一张证书的证书主体。

注：在不同的阶段，也称为证书申请人、证书持有人。在电子签名应用中，订户即为电子签名人。

订户协议

是指电子认证服务机构（CA）与电子签名认证证书申请者（即订户）之间，就电子签名认证证书的申请、接受、使用、管理及法律责任等事宜所订立的、具有约束力的法律文件。

对象标识符（OID）

用于无歧义的标识对象的全局唯一值。

证书策略（CP）

指明证书对于具有普通安全需求的特定团体和 / 或应用类的适用性的规则集合。

证书策略对象标识符（CP OID）

对某个证书策略进行唯一标识的 OID。

证书链

证书链是一个用于证书验证的证书序列。

身份鉴别

证实某个实体就是所声称身份的过程。

激活数据

用于使密码模块进入可操作状态的数据。可为口令、生物特征等。

时间戳

对时间和其他待签名数据进行签名得到的，用于表明数据时间属性的数据。

证书续期

指在不改变订户信息的情况下，用一个新证书来代替旧证书的过程。

密钥更新

用新密钥替换旧密钥的过程。

密钥恢复

将归档或备份的密钥恢复到可用状态的过程。

证书撤销列表（CRL）

由电子认证服务机构签发并发布的被撤销证书的列表。

证书认证系统（CA 系统）

对数字证书的申请、签发、发布、更新、撤销、验证等数字证书全生命周期进行管理和服务的系统。

注：也称电子认证服务系统，包括证书签发子系统、证书注册子系统等。

高等级电子签名认证证书

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。

基础级电子签名认证证书

适用于除高等级电子签名认证证书规定场景以外的其他电子签名认证证书。

一次性电子签名认证证书

SHECA 所签发的证书有效期为 2 小时，且在证书接受后 60 分钟内仅能使用私钥完成一次签名后即失效的电子签名认证证书。SHECA 仅在云执钥®远程可靠电子签名服务中提供该类证书。

职务行为个人证书

是指 SHECA 签发的，由机构（单位）为其员工申请、供该员工在履行职务行为范围内使用的个人电子签名认证证书。职务行为个人证书仅可在其任职单位规定的业务系统/场景中使用。

1.8 缩略语

下列缩略语适用于本文件。

CA：电子认证服务机构（Certification Authority）

CPS：电子认证业务规则（Certification Practice Statement）

CP：证书策略（Certification Policy）

CRL：证书撤销列表（Certificate Revocation List）

DN：甄别名称（Distinguished Name）

LDAP：轻量级目录访问协议（Lightweight Directory Access Protocol）

OCSP：在线证书状态协议（Online Certificate Status Protocol）

OID：对象标识符（Object Identifier）

RTO：恢复时间目标（Recovery Time Objective）

RPO：恢复点目标（Recovery Point Objective）

2. 信息发布与信息管理

2.1 SHECA 网站

SHECA 网站发布的内容，包括但不限于：

- CP、CPS 等策略类文档的现行和历史版本
- 证书链
- 证书信息、状态信息等查询服务
- 详细的业务办理指南，包括服务网点地址、营业时间、联系电话等
- 订户协议、依赖方协议
- 投诉处理政策及投诉方式，包括投诉处理部门的地址、联系电话、电子邮件地址、内部监督部门名称等

2.2 认证信息的发布

发布渠道：SHECA 在 https://www.sheca.com 上公布与其相关的信息；该网站是 SHECA 发布所有信息最首要、最及时、最权威的渠道。只有 SHECA 有权处理网站上的旧信息。

信息更新：信息发布内容如有变化，SHECA 将在变化生效后 1 个工作日内更新。

监管备案：SHECA 严格按照国家电子认证服务管理平台的要求进行备案。

证书信息对接：SHECA 按要求与国家电子认证服务管理平台进行技术对接，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。

3. 身份标识与鉴别

3.1 身份鉴别通用要求

3.1.1 通用要求

SHECA 郑重声明：在订户及/或受托人申请办理电子签名认证证书过程中，SHECA 将严格按照相关规定，履行告知、身份确认、意愿记录及协议签署等 CA 机构法定义务，具体流程以业务办理环节的实际操作为准。

SHECA 不会将身份确认相关义务委托给任何外部机构或个人。

3.1.2 订户告知

3.1.2.1 告知的内容

在订户及/或受托人申请办理电子签名认证证书时，SHECA 会向订户及/或受托人告知以下内容：

- 订户的权利和义务；
- 服务收费的项目和标准；
- 电子签名认证证书、电子签名的使用条件；
- 信息安全保障措施；
- CA 和订户的责任划分；
- 订户签名私钥的存储方式及安全要求；
- 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。

针对不同类型或者等级的电子签名认证证书，SHECA 的告知内容可能存在差异，具体告知内容以证书申请流程中材料或页面为准。

3.1.2.2 告知方式

不同等级的电子签名认证证书，SHECA 采用不同的告知方式：

a) 高等级电子签名认证证书采用包括但不限于面对面、电话、视频或主管部门认可的其他方式告知，SHECA 会保留告知的记录，如签名纸质材料、录音文件、录像文件等；

b) 基础级电子签名认证证书采用 a)中的方式或者采用强制阅读、短信、邮件等方式告知，SHECA 会保留告知的记录，如系统操作日志、短信记录或日志、邮件记录或日志等。

3.1.2.3 职务行为个人证书的告知

职务行为个人证书会对证书订户所在机构和证书订户分别进行告知，告知内容同 **3.1.2.1 告知的内容。**

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

订户自行或委托上海 CA 按照本文件 6.2.1 规定的方式产生订户签名密钥对。

SHECA 通过验证数字签名的方式来确认订户拥有某个公钥对应的签名私钥。

3.2.2 个人身份的查验

3.2.2.1 个人身份信息有效性确认

SHECA 受理个人证书申请时，个人身份信息查验方式及内容如下：

a) 要求订户出示其有效身份证件或有效身份证件信息，有效证件类型仅限法律法规和国家有关文件规定的身份证件（如居民身份证、护照等）；

b) 通过证件机读工具、权威数据库（如公安部门身份信息库）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；

c) 当订户委托他人代为办理时，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并按照 b) 款方式查验验订户和受托人的身份证件或身份资料。

3.2.2.2 个人高等级电子签名认证证书的实人查验

SHECA 对申请个人高等级电子签名认证证书的订户，实人查验采用下列方式之一：

a) 面对面查验；

b) 远程人工面对面查验（通过实时视频等方式）；

c) 生物特征验证（如活体人脸识别、指纹等）；

d) 通过主管部门认可的其他方式。

SHECA 会以可追溯方式完整记录并保存每张证书的身份鉴别过程和结果，并为每张证书建立独立的身份验证记录。

3.2.2.3 个人基础级电子签名认证证书的实人查验

SHECA 对申请个人基础级电子签名认证证书的订户，实人查验采用下列方式之一：

a) 电信运营商三要素验证：核对姓名、证件号码、手机号在电信运营商的一致性，并通过对应手机号的随机短信验证码核验；

b) 银行卡四要素验证：核对姓名、证件号码、银行卡号、银行预留手机号在银行的一致性，并通过预留手机号的随机短信验证码核验；

c) 由申请人持有的 SHECA 签发的或认可的有效电子签名认证证书签名验证；

d) 通过主管部门认可的其他方式（如居民身份网络可信凭证、国家网络身份认证系统等）；

e) 第 3.2.2.2 条规定的方式。

SHECA 会以可追溯方式完整记录并保存每张证书的身份鉴别过程和结果，并为每张证书建立独立的身份验证记录。

3.2.3.4 职务行为个人证书的主体身份查验

SHECA 按照 3.2.2.1、3.2.2.2 或 3.2.2.3，对职务行为个人证书的主体身份进行查验。

3.2.3 机构身份的查验

3.2.3.1 机构身份信息有效性的确认

SHECA 受理机构证书申请时，机构身份信息查验方式及内容如下：

a) 查验机构有效证件，有效证件类型仅限法律法规和国家有关文件规定的证件（如营业执照、统一社会信用代码证书等）；

b) 法定代表人或受托人的身份证件信息查验按照 3.2.2.1 的规定执行；受托人办理时，额外查验机构加盖公章的有效书面授权证明。

3.2.3.2 机构高等级电子签名认证证书的实人查验

SHECA 对申请机构高等级电子签名认证证书的订户，实人查验采用下列方式之一：

a) 法定代表人本人办理：对法定代表人实人查验方法见 3.2.2.2；

b) 机构委托受托人办理：受托人实人查验方法见 3.2.2.2，并通过机构对公账户随机金额打款验证或主管部门认可的其他方式。

SHECA 会以可追溯方式完整记录并保存每张证书的身份鉴别过程和结果，并为每张证书建立独立的身份验证记录。

3.2.3.3 机构基础级电子签名认证证书的实人查验

SHECA 对申请机构基础级电子签名认证证书的订户，实人查验采用下列方式之一：

a) 法定代表人本人办理： 法定代表人实人查验方法见 3.2.2.3；

b) 机构委托受托人办理：受托人实人查验方法见 3.2.2.3；

c) 由订户持有的 SHECA 签发的或认可的基础级或高等级的有效机构证书签名验证；

d) 通过主管部门认可的其他方式（如居民身份网络可信凭证、国家网络身份认证系统等）；

e) 第 3.2.2.2 条规定的方式。

SHECA 会以可追溯方式完整记录并保存每张证书的身份鉴别过程和结果，并为每张证书建立独立的身份验证记录。

3.2.3.4 职务行为个人证书的订户身份查验

SHECA 按照 3.2.3.1、3.2.3.2 或 3.2.3.3，对职务行为个人证书的订户身份进行查验。

3.3 订户意愿记录

3.3.1 订户意愿记录内容

SHECA 对订户意愿记录内容包括但不限于：

a) 订户身份信息；

b) SHECA 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。

对于职务行为个人证书，SHECA 会分别记录订户所在机构和证书订户的意愿，意愿记录的内容和方式与个人和机构证书一致。

3.3.2 个人高等级电子签名认证证书的意愿记录

对申请个人高等级电子签名认证证书的订户，SHECA 可采用下列方式之一的方式进行意愿确认：

a) 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；

b) 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。

SHECA 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。

3.3.3 个人基础级电子签名认证证书的意愿记录

对申请个人基础级电子签名认证证书的订户，SHECA 可采用下列方式之一的方式进行意愿确认：

a）采用强制阅读、短信或邮件确认等电子方式；

b) 与高等级电子签名认证证书相同的方式（见 3.3.2）。

SHECA 保留完整、可追溯的订户意愿记录，具体记录以采取的方式不同而不同。

3.3.4 机构高等级电子签名认证证书的意愿记录

对申请机构高等级电子签名认证证书的订户，SHECA 可采用下列方式之一的方式进行意愿确认：

a) 法定代表人本人申请时，按照 3.3.2 的方式确认机构法定代表人的意愿；

b) 机构委托受托人申请时，查验加盖机构公章的授权文件，并按照 3.3.2 的方式确认受托人的意愿。

SHECA 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。

3.3.5 机构基础级电子签名认证证书的意愿记录

对申请机构基础级电子签名认证证书的订户，SHECA 可采用下列方式之一的方式进行意愿确认：

a) 法定代表人本人申请时，按照 3.3.3 的方式确认机构法定代表人的意愿；

b) 机构委托受托人申请时，查验加盖机构公章的授权文件，并按照 3.3.3 的方式确认受托人的意愿。

SHECA 保留完整、可追溯的订户意愿记录，具体记录以采取的方式不同而不同。

3.4 订户协议

SHECA 与订户签订订户协议，协议内容包含 3.1.2.1 规定的内容以及本 CPS 部分权利义务条款。

针对职务行为个人证书，SHECA 会分别与订户所在机构和证书订户签署协议，协议内容包含 3.1.2.1 规定的内容以及本 CPS 部分权利义务条款。

3.5 未验证的订户信息

SHECA 不会将未经验证过的订户信息包含在证书主体信息中。SHECA 在证书签发前，会对证书主体信息中载明的所有订户信息（包括但不限于姓名、机构名等）进行验证，确保证书主体信息中不包含任何未经核实的、被篡改的或已过期的信息。

3.6 互操作要求

对于非 UNTSH 认证服务体系内的其他证书服务机构，可以与 SHECA 进行互操作，但是该证书服务机构的 CPS 必须符合本 CPS 的要求，并且与 SHECA 签署相应的协议。

SHECA 将依据协议的内容，信任其他权威第三方电子认证服务机构签发的电子签名认证证书实施的电子签名。如果双方之间没有任何类似的协议，SHECA 会根据情况决定是否需要进行初始身份确认，并作出是否进行受理的决定。

如果国家法律法规对此有规定，SHECA 将严格予以执行。

3.7 命名

3.7.1 名称类型

SHECA依照特定的签发程序，保存与证书注册过程有关的特定记录，对特定对象的身份进行鉴别，以区别于其他的申请者。这一命名过程中出现的名称，包括甄别名和证书扩展项中包含的识别用户唯一身份的标识项，是一组能

辨别真实世界中实体的数据。

SHECA 生成或者签发证书的主体名称（SubjectName），采用 X.501 主体甄别名（Distinguished Name ， DN）的方式。

每个证书订户按照 X.509 的规定，将对应一个可分辨的名称，该名称由甄别名和可识别用户身份的唯一标识项组成。甄别名包含于每张证书的主体中，用户唯一标识项包含于证书扩展项中。该名称唯一标识证书订户的身份。

SHECA 作为可信第三方的认证机构负责确认公钥与已命名实体之间的联系。这种确认关系通过证书明清晰无误地表示出来。

3.7.2 对名称意义化的要求

标识名称所采用的用户识别信息，必须具有明确的、可追溯的、肯定的代表意义，不允许匿名或者伪名等出现。

3.7.3 订户的匿名或伪名

本 CPS 中明确声明，除 3.7.2 所规定的特殊情形以外，SHECA 不接受或者允许任何匿名或者伪名，仅接受有明确意义的名称作为唯一标识符。

3.7.4 不同名称形式的规则

SHECA 认证服务体系签发的证书，其甄别名符合 X.500 的甄别名命名规则。SHECA 对证书主体甄别名称（以下简称 “DN”）的命名规则，包括但不限于：

a) 针对个人和机构等不同类型的证书，分别约定其命名规则；

b) 确保命名具有实际意义，且能追溯到唯一实体的方法：

- 个人证书，主体 DN 项中包含个人姓名，在 DN 项或扩展项中包含有效证件类型及其编号（或相关信息的映射，包括但不限于摘要值、掩码等）；
- 机构证书，主体 DN 项中包含机构名称，在 DN 项或扩展项中包含组织机构的有效证件类型及其编号（或相关信息的映射，包括但不限于摘要值、掩码等）。

c) SHECA 不识别证书名称中的商标权；

d) 在不影响证书通用性的前提下，SHECA 可在证书中增加自定义的其他内容；

e）DN 项结构定义符合 GB/T16264.8 的要求，证书主体 DN 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

f）职务行为个人证书的 O 项为必填项，且必须为机构的名称。

注;应项目需要，在不影响主体身份真实在与准确性的前提下，SHECA 可能对 DN 的可选项赋予不同的内容，该类特殊情况将在 https://www.sheca.com 公布。

3.7.5 名称的唯一性

SHECA 签发给某个实体的证书，其主体甄别名，在该证书签发 CA 体系内是唯一的。属于同一实体的多张证书可以具有同样的主体甄别名。

4. 证书生存周期操作要求

本章阐述了在 SHECA 认证服务体系架构下，根据公布的 CPS 实施电子签

名认证证书的申请、签发、接受、密钥对和证书的使用、续期、证书密钥更新、变更、撤销或冻结等证书生命周期的全部过程，以及在这个过程中，各个参与方的责任与义务。

4.1 通用要求

a) SHECA 承担建立、运营和维护注册通道的责任；

b) SHECA 承担与订户签订订户协议的责任；

c) 订户承担提供准确、真实信息的责任；

d) SHECA 承担妥善记录并保存相关信息的责任。

4.2 证书申请

SHECA 提供线下申请和线上申请两种证书申请方式。根据订户申请的证书类型，SHECA 采用不同的申请注册程序，但遵守本文件第 3 章证书所规定的内容。

SHECA 严格按照本文件 3.1、3.2、3.3、3.4 规定，完成对订户的告知、身份确认、意愿记录、协议签署等动作,并依据既定准则批准或拒绝该申请;

SHECA 承诺，自明确受理之日至 SHECA 签发证书，处理的最长时效不超过 5 个工作日；如因特殊情况需超期的，SHECA 会与申请者协商确定处理时限。

4.2.1 线上业务流程

线上申请流程是指，SHECA 通过在线网页、小程序、APP、SDK、线上面对面或其他非面对面方式，为申请者提供的证书办理服务。SHECA 可采用自动化程序或在线人工辅助的方式完成全流程操作。需要提醒的是，受技术、网络、不可抗力等因素限制，如在线方式无法完成办理，申请者可通过线下流程获取证书服务。

1、告知

SHECA 按照本 CPS 要求履行订户告知事宜，并妥善保管告知的记录，记录

保存时间不低于证书失效后 5 年。

为提升服务透明度，SHECA 将以在线流程的形式展示告知内容，订户或受托人可自主选择是否阅读。该告知内容已完整载入 SHECA 与订户签署的《订户协议》中。若订户选择办理高等级证书，SHECA 将在进行意愿确认时，通过录音录像或主管部门认可的其他方式，向订户提请注意相关告知事项，以确保订户充分知悉相关内容。告知内容详见本文件 3.1.2.1。

2、身份鉴别

SHECA 依据本 CPS 开展身份查验工作，针对每份证书建立可追溯留存机制，完整保存全部核验流程记录与核验结果，记录保存时间不低于证书失效后 5 年。

1）基础级电子签名认证证书的身份鉴别

A. 个人的身份鉴别

SHECA 受理证书申请时，要求申请人完成实名与实人认证流程。若由受托人代为办理，还需额外核验受托人的授权委托材料及其实名实人认证。SHECA 基于商业安排和安全性考虑，可在具体流程中不接受个人委托受托人办理电子签名认证证书。

SHECA 接受的证件类型包括身份证、护照及其他国家权威机关颁发的身份证件。个人实名认证可通过申请人/受托人在线填写证件信息、上传证件正反面照片或复印件、提供电子版凭证或第三方预先收集并传入的订户身份证件信息等方式完成信息采集，具体以实际申请流程展现的为准。SHECA 将通过权威数据库查验订户身份证件的真实性和有效性。受限于技术条件或付费客户的要求，SHECA 不承诺所有权威机关颁发的身份证件均可在具体申请流程中获得支持。

个人实人认证所接受的认证方式详见本文件 3.2.2.3。同样，受限于技术条件或付费客户的要求，SHECA 不承诺本文件 3.2.2.3 所列方式均可在具体申请流程中获得支持。

B. 机构的身份鉴别

SHECA 受理证书申请时，要求申请人完成实名与实人认证流程。若由受托人代为办理，还需额外核验受托人的授权委托材料及其实名实人认证。

SHECA 接受的证件类型仅包括法律法规和国家有关文件规定的证件，纸质证件材料需加盖单位实体印章。机构实名认证可通过机构法定代表人或者负责人或受托人线上填写机构名称、统一社会信用代码、法定代表人信息等企业必要信息，或上传加盖公章的营业执照、电子营业执照等证件，或第三方预先收集并传入的订户身份证件信息等方式完成信息采集，具体以实际申请流程展现的为准。SHECA 将通过权威数据库查验订户证件的真实性和有效性。受限于技术条件或付费客户的要求，SHECA 不承诺所有法律法规和国家有关文件规定的证件证件均可在具体申请流程中获得支持。

对于机构的实人认证，通过本文件 3.2.3.3 完成机构实人认证；机构法定代表人或受托人的实人认证所接受的认证方式详见本文件 3.2.2.3。同样，受限于技术条件或付费客户的要求，SHECA 不承诺本文件 3.2.2.3 所列方式均可在具体申请流程中获得支持。

2）高等级电子签名认证证书的身份鉴别

A. 个人的身份鉴别

SHECA 受理证书申请时，要求申请人完成实名与实人认证流程。若由受托人代为办理，还需额外核验受托人的授权委托材料及其实名实人认证。SHECA 基于商业安排和安全性考虑，SHECA 可在具体流程中不接受个人委托受托人办理电子签名认证证书。

SHECA 接受的证件类型包括身份证、护照及其他国家权威机关颁发的身份证件。个人实名认证可通过申请人/受托人在线填写证件信息、上传证件正反面照片或复印件、提供电子版凭证或第三方预先收集并传入的订户身份证件信息等方式完成信息采集，具体以实际申请流程展现的为准。SHECA 将通过权威数据库查验订户身份证件的真实性和有效性。具体以实际申请流程的要求为准。受限于技术条件或付费客户的要求，SHECA 不承诺所有权威机关颁发的身份证件均可在具体申请流程中获得支持。

个人实人认证所接受的认证方式详见本文件 3.2.2.2。同样，受限于技术条件或付费客户的要求，SHECA 不承诺本文件 3.2.2.2 所列方式均可在具体申请流程

中获得支持。

B：机构的身份鉴别

SHECA 受理证书申请时，要求申请人完成实名与实人认证流程。若由受托人代为办理，还需额外核验受托人的授权委托材料并对受托人进行实名实人认证。

SHECA 接受的证件类型仅包括法律法规和国家有关文件规定的证件，纸质证件材料上传需加盖单位实体印章。机构实名认证可通过机构法定代表人或者负责人或受托人线上填写机构名称、统一社会信用代码、法定代表人信息等企业必要信息，上传加盖公章的营业执照、电子营业执照等证件，或第三方预先收集并传入的订户身份证件信息等方式完成信息采集，具体以实际申请流程展现的为准。SHECA 将通过权威数据库查验订户身份的真实性和有效性。具体以实际申请流程的要求为准。受限于技术条件或付费客户的要求，SHECA 不承诺所有法律法规和国家有关文件规定的证件证件均可在具体申请流程中获得支持。

对于机构的实人认证，通过本文件 3.2.3.2 完成机构实人认证；机构法定代表人或受托人的实人认证所接受的认证方式详见本文件 3.2.2.2。同样，受限于技术条件或付费客户的要求，SHECA 不承诺本文件 3.2.2.2 所列方式均可在具体申请流程中获得支持。

3、意愿确认

SHECA 依据本 CPS 对订户进行意愿确认，并保留完整、可追溯的订户意愿记录，记录保存时间不少于证书失效后 5 年。对于职务行为个人证书，SHECA 会分别对订户所在机构和证书订户进行意愿确认。

1）基础级电子签名认证证书意愿记录

A. 个人的意愿记录

SHECA 的意愿记录方式见本文件 3.3.3，意愿记录的内容见本文件 3.3.1。受限于技术条件或付费客户的要求，SHECA 不承诺 3.3.3 所列方式均可在具体申请流程中获得支持。

B. 机构的意愿记录

SHECA 的意愿记录方式见本文件 3.3.5，意愿记录的内容见本文件 3.3.1。受

限于技术条件或付费客户的要求，SHECA 不承诺本文件 3.3.5 所列方式均可在具体申请流程中获得支持。

1）高等级电子签名认证证书意愿记录

A. 个人的意愿记录

SHECA 的意愿记录方式见本文件 3.3.2，意愿记录的内容见本文件 3.3.1。受限于技术条件或付费客户的要求，SHECA 不承诺本文件 3.3.2 所列方式均可在具体申请流程中获得支持。

B. 机构的意愿记录

SHECA 的意愿记录方式见本文件 3.3.4，意愿记录的内容见本文件 3.3.1。受限于技术条件或付费客户的要求，SHECA 不承诺本文件 3.3.4 所列方式均可在具体申请流程中获得支持。

4、协议签署

凡是 SHECA 的证书申请者，SHECA 在决定签发电子签名认证证书前，均会要求签署订户协议，因证书产品不同，订户协议内容以实际申请流程展示的为准，但内容至少包含本文件 3.1.2.1 中内容以及 SHECA 认为必要的其他条款。

申请者在全文强制阅读后可通过点击、勾选、同意确认或电子签名方式签署协议，受限于技术条件或付费客户的要求，SHECA 不承诺以上方式均可在具体申请流程中获得支持。

SHECA 会妥善保管每张证书订户协议的签署记录，保存时间不少于证书失效后 5 年。

针对职务行为个人证书，SHECA 会分别与订户所在机构和证书订户签署协议。

4.2.2 线下业务流程

线下申请流程是指，SHECA 通过线下服务网点，采用面对面方式，为申请者提供的证书办理服务。

1、告知

SHECA 按照本 CPS 要求履行订户告知事宜，并妥善保管告知的记录。SHECA 通过《证书申请表》中“告知”部分或《订户协议》向订户展示告知内容（告知内容详见本文件 3.1.2.1），要求订户或受托人阅读。订户或受托人通过盖章、签字等操作确认知悉。SHECA 保留告知的记录，保存时间不少于证书失效后 5 年。

2、身份鉴别

SHECA 依据本 CPS 开展身份鉴别工作，针对每张证书建立可追溯留存机制，完整保存全部核验流程记录与核验结果，记录保存时间不少于证书失效后 5 年。

1）基础级电子签名认证证书的身份鉴别

A. 个人订户的身份鉴别

要求订户出示其有效身份证件原件，SHECA 接受的证件类型包括身份证、护照及其他国家权威机关颁发的身份证件。SHECA 通过人工查验、证件机读工具，或者通过权威数据库查验订户身份证件的真实性和有效性。通过人脸识别、人工比对等方式完成面对面的实人查验。

当订户委托他人代为办理时，还需查验订户本人有效身份证件原件及签署的有效书面授权证明，并对受托人按上述方式做身份鉴别。

SHECA 对每张个人证书的身份鉴别过程和结果建立独立记录，具体管理方式参考“5、材料留存”。

B. 机构订户的身份鉴别

要求订户出示机构的有效证件原件。查验机构有效证件，有效证件类型仅限法律法规和国家有关文件规定的证件（如营业执照、统一社会信用代码证书等），并通过人工查验或权威数据库查验订户身份证件的真实性和有效性。

如为法定代表人本人办理，按本段落（A）对法定代表人做身份鉴别。

如委托其他人代为办理，按本段落（A）对受托人做身份鉴别，并查验机构加盖公章的有效书面授权证明。

SHECA 对每张机构证书的身份鉴别过程和结果建立独立记录，具体管理方式参考“5、材料留存”。

2）高等级电子签名认证证书的身份鉴别

A. 个人订户的身份鉴别

要求订户出示其有效身份证件，SHECA 接受的证件类型包括身份证、护照及其他国家权威机关颁发的身份证件。通过人工查验、证件机读工具，或者通过权威数据库查验订户身份证件的真实性和有效性。通过人脸识别、人工比对等方式完成面对面的实人查验。

对于个人高等级电子签名认证证书的线下申请，SHECA 不接受委托办理。

SHECA 对每张个人证书的身份鉴别过程和结果建立独立记录，具体管理方式参考“5、材料留存”。

B. 机构订户的身份鉴别

要求订户出示机构的有效证件原件。查验机构有效证件，有效证件类型仅限法律法规和国家有关文件规定的证件（如营业执照、统一社会信用代码证书等），SHECA 将通过人工查验或权威数据库查验订户身份证件的真实性和有效性。

法定代表人本人办理时，按本段落（A）对法定代表人做身份鉴别。

委托其他人代为办理时，按本段落（A）对受托人做身份鉴别，查验法定代表人有效证件原件和机构加盖公章的有效书面授权证明，并通过机构对公账户随机金额打款或监管部门认可的其他方式完成机构订户实人查验。

SHECA 对每张机构证书的身份鉴别过程和结果建立独立记录，具体管理方式参考“5、材料留存”。

3、意愿确认

SHECA 依据本 CPS 对订户进行意愿确认，并完整、可追溯地记录订户意愿，记录保存时间不少于证书失效后 5 年。对于职务行为个人证书，SHECA 会分别对订户所在机构和证书订户进行意愿确认。

1）基础级电子签名认证证书的意愿记录

A. 个人订户的意愿记录

通过面对面确认意愿，要求订户或受托人签字的方式记录订户意愿。

B. 机构订户的意愿记录

法人代表本人办理时，按本段落（A）的方式记录法定代表人意愿。

委托其他人代为办理时，查验加盖机构公章的授权文件，按本段落（A）的方式记录受托人意愿。

2）高等级电子签名认证证书的意愿记录

A. 个人订户的意愿记录

通过面对面确认意愿，要求用户手抄提示语并签字，同时采用录音录像的方式记录订户意愿。

B. 机构的意愿记录

法人代表本人办理时，按本段落（A）的方式记录法定代表人意愿。

委托其他人代为办理时，查验加盖机构公章的授权文件，按本段落（A）的方式记录受托人意愿。

4、协议签署

因证书产品不同，订户协议内容以实际的申请表中所附的订户协议为准，但内容至少包含本文件 3.1.2.1 中内容以及 SHECA 认为必要的其他条款。

订户或受托人通过在《证书申请表》中“订户协议”部分盖章、签字等操作完成协议签署。SHECA 妥善保管证书申请表和订户协议，保存时间不少于证书失效后 5 年。

针对职务行为个人证书，SHECA 会分别与订户所在机构和证书订户签署协议。

5、材料留存

个人订户：《证书申请表》、订户的身份证件复印件，如委托他人办理，还需留存受托人的身份证复印件、书面授权证明原件。系统留存身份鉴别记录、高等级证书的录音录像记录。

机构订户：《证书申请表》、加盖公章的机构证件复印件、加盖公章的法人代表身份证件复印件，如委托他人办理，还需留存加盖公章的办人的身份证件复印件、加盖公章的书面授权证明原件。系统留存身份鉴别记录、高等级证书的录音录像记录。

SHECA 可以对留存材料进行电子化处理并保存其影印件。

4.2.3 证书申请批准和拒绝

SHECA在进行鉴别程序时，如果申请者未能成功通过鉴别，SHECA将拒绝申请者的证书申请，并通知申请者鉴别失败。对于鉴别失败的具体原因，SHECA有权拒绝解释，法律法规对此有明确要求的除外。SHECA采用申请者向SHECA提交证书申请时使用的相同方法来通知证书申请者其证书申请失败。

如果发生下列情形，可以拒绝证书申请：

- 该申请不符合本文件 3.2 条款关于订户信息的初始身份确认规定
- 申请者不能提供所需要的真实准确的身份证明材料或其他需要提供的支撑文件
- 申请者不接受订户协议的有关内容和要求
- 申请者没有或者不能够按照规定支付相应的费用
- SHECA 认为批准该申请将会对 SHECA 带来争议、法律纠纷或者损失
- SHECA 明确知晓订户提供的证书请求文件中对应的私钥不符合本文件 6.2 中对密钥的规定

被拒绝的订户可以在准备真实、准确的材料后，再次提出申请。

4.3 证书签发

4.3.1 签发证书

SHECA 验证申请者身份信息的合法性和证书申请信息的完整性、有效性和可靠性，正确无误后，为申请者签发证书。证书的签发意味着 SHECA 正式地批准了证书申请。

4.3.2 对订户的结果通告

证书申请处理完毕后，SHECA 根据申请方式的不同采取以下几种方式向订户通告结果：

- 通过面对面的方式通知（如申请者到受理点领取等方式）
- 通过实时视频等相当于面对面的方式通知
- 通过网络页面、站内信、电子邮件（e-mail）方式通知
- 通过邮政、快递信函通知
- 通过短信、电话方式通知
- 通过证书使用工具进行信息提示
- 通过主管部门认可的其他方式通知
- 其他 SHECA 认为安全可行的方式

SHECA 没有上门为用户安装证书使用工具的义务。如果申请人需要，SHECA 可以上门安装，但需要收取相应的服务费用。SHECA 提供热线支持服务。热线支持电话为 021—962600。

4.4 证书接受

4.4.1 向订户交付证书的方式

- 面对面交付
- 邮政或快递交付
- 线上电子文件交付

SHECA 也可以通过其他安全的方式交付电子签名认证证书。

4.4.2 接受证书的行为

下列行为被认为订户已经接受了证书：

- 订户接收了包含有证书的密钥载体

- 订户页面确认点击同意接受证书
- 订户通过网络下载证书
- 订户使用证书对应的私钥进行电子签名或其他密码运算时
- 订户获悉了接受证书的通知，并且 24 小时内没有提出异议

4.4.3 拒绝接受证书的行为

若订户出现拒绝现场领取证书、拒收证书快递、不同意下载证书、在操作页面拒绝确认接收证书等任一情形，均视作订户拒绝接受证书；SHECA 在获取相关拒收记录后，将于 7 个工作日内完成证书撤销操作。

4.4.4 信息保存

SHECA 保存订户接受证书的记录，包括接受时间、方式等信息，保存期限至证书失效后五年。

4.5 密钥对和证书的使用

密钥交付的要求见本文件 6.2.2；

密钥参数的要求见本文件 6.2.5 和 6.2.6；

私钥管理服务的要求见本文件 6.2 和 6.3。

4.5.1 订户私钥的使用

只有当订户签署了订户协议，并且接受证书以后，订户才可以使用其证书以及与该证书相对应的私钥。该证书只能根据本 CPS 被依法地使用。订户只能在正当的应用范围内使用私钥和证书，并且与证书内容相一致。如果证书中的某些信息明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内进行使用，例如密钥用途、密钥扩展用途等。所有使用行为必须符合订户协议的要求。任何超出证书所标明的适用范围内的行为，都将由行为人独立承担责任。SHECA 对超出适用范围的任何使用行为，不承担任何由此产生的责任和义务。

订户使用证书时，必须妥善保管和存储与证书相关的密钥载体和/或私钥激活数据，避免遗失、泄露、被篡改或者被盗用。

订户超出本 CPS 规定的证书及私钥使用，SHECA 将不承担由此带来的任何后果。

4.5.2 依赖方对公钥和证书的使用

在信任证书和签名前，依赖方需要独立地做出合理的判断：

- 该证书是否由可信任的 CA 所签发；
- 判断该证书是否在既定的范围内被使用（如果证书中的某些信息明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内进行使用（例如电子签名认证证书，其密钥用途中 Nonrepudiation 必须为 1）；判断该证书没有被用于任何本 CPS 或法律法规禁止、限制的使用范围，SHECA 不负责也无法做到评估证书是否被适当的使用；
- 查询证书及其证书链内的所有证书的证书状态，确认证书是否在有效期、是否已撤销。若证书或其证书链任一证书已撤销，依赖方须自行核实该证书对应私钥生成的签名是否产生于证书有效期内；可以通过查询最新的撤销状态或查看证书链中提供的证书撤销列表（CRL）来确认证书状态；
- 确定经过签名的信息的范围，在验证签名时，应准确知道哪些数据已经被签名。

除非本 CPS 另有规定，证书并不是来自 SHECA 的对任何权力或特权的承诺。依赖方只能在本 CPS 规定的范围内信赖证书和证书中包含的公钥，并对此做出决定。

依赖方必须对此做出合理的判断，任何对超出证书所标明的适用范围的行为的信赖，都将由依赖人独立承担责任，SHECA 对此不承担任何责任和义务。

证书的使用并不表示订户一方可以按任何个人的利益而行事，或者有采取任何特殊行动的权力，证书仅表明订户的身份并对订户的签名进行验证。

进行签名的验证是为了确认签名是用签名者证书中所列的公钥相对应的私钥所创建,以及被签名的信息在该签名创建后没有被更改过。

SHECA 郑重指出：

- 依赖方如果信任无法验证的签名，那么应由依赖方承担所有风险
- 并且依赖方也无权做出任何假定数字签名是有效签名的判断
- 这就意味着，任何对签名的依赖，都必须经过上述合理和必要的判断

4.5.3 安全事件反馈

SHECA 通过网站、电子邮件、客户服务热线等方式，建立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。

4.6 证书续期

证书续期是指在不改变订户主体信息的情况下，在原证书到期前，为订户签发一张新证书。

证书续期的申请人必须是订户或其受托人。

4.6.1 证书续期的情形

订户在证书到期前 90 天内，可以申请证书续期。

4.6.2 证书续期请求的处理

在线续期证书，订户必须在线填写续期请求，并按照 SHECA 要求，用当下的私钥对续期请求信息进行数字签名后递交给 SHECA。SHECA 接收到续期请求后，在对申请者的身份和请求信息进行鉴别确认后，为其签发新的证书。

线下续期证书，订户按照原申请证书的流程，到 SHECA 服务网点提出续期请求。SHECA 按照原申请时的流程对证书续期申请进行身份鉴别和审核。SHECA 确认并批准续期申请后，为其签发新的证书。

若申请人上次完成身份鉴别之日起至本次续期申请日未满 1005 天，SHECA 允许申请人使用有效的原证书进行电子签名验证的方式进行身份鉴别，但新签发的证书有效期不应超过上次完成身份鉴别之日起后三年，否则，按照本文件 3.2 初始身份确认相同的过程来进行身份鉴别。

4.6.3 更新证书的签发

同本文件第 4.3 条。

4.6.4 构成接受更新证书的行为

同本文件第 4.4 条。

4.7 证书密钥更新

4.7.1 签名证书密钥更新

签名证书密钥更新是指订户生成新的签名密钥对并为其新公钥签发新证书，证书有效期至原证书到期日。订户在证书有效期内，可以申请证书密钥更新。

签名证书密钥更新的申请人必须是订户或其受托人。

签名证书密钥更新，不更新加密证书。

4.7.1.1 证书密钥更新的情形

如果出现密钥载体损毁或遗失，证书私钥已经被泄漏、被窃取、被篡改或者其它原因导致的密钥安全性无法得到保证的情形，订户必须选择证书密钥更新。

4.7.1.2 证书密钥更新请求的处理

SHECA 接收到证书密钥更新请求后，在对申请者的身份和请求信息进行鉴别确认后，为其签发新的证书，该证书的公钥为申请者递交的新的公钥。

SHECA 按照与初始身份确认相同的过程来进行密钥更新请求的身份鉴别。若发起方不是证书订户，SHECA 需取得订户同意。

4.7.1.3 密钥更新证书的签发

同本文件第 4.3 条。

4.7.1.4 构成接受密钥更新证书的行为

同本文件第 4.4 条。

4.7.2 加密密钥更新

加密密钥更新是指订户申请新的加密密钥对，SHECA 为其新公钥签发新加密证书，证书有效期至原证书到期日。订户在证书有效期内，可以申请加密证书密钥更新。

订户应慎重申请加密密钥更新，在申请前应做好原加密密钥的备份。因订户操作不当导致原加密密钥丢失的，SHECA 不承担任何责任。

4.7.2.1 证书密钥更新的情形

如果出现下列情形，订户可选择加密密钥更新：加密私钥已经被泄漏、被窃取、被篡改或者其它原因导致的密钥安全性无法得到保证。

4.7.2.2 证书密钥更新请求的处理

SHECA 接收到加密密钥更新请求后，在对申请者的身份和请求信息进行鉴别确认后，向证书认证密钥管理系统申请新的加密密钥对，并为其签发新的证书，并将加密证书和按 GM/T0009 规定格式或使用订户签名公钥进行数字信封加密保护的加密私钥交付给订户。

SHECA 处理加密密钥更新请求时的身份鉴别方式为：

a）若自申请人上次完成身份鉴别之日起至本次续期申请日未满三年，可使用有效的原证书进行电子签名验证的方式进行确认；

b）否则，按照初始签发证书相同的过程来进行身份鉴别。

4.7.2.3 构成接受密钥更新证书的行为

同本文件第 4.4 条。

4.8 证书变更

证书变更是指改变证书中除订户之外的信息而签发新证书的情形，新证书有效期至原证书到期日。

证书变更的申请人必须是订户或其受托人。

只有在证书有效期内，订户可选择证书变更。

当证书内所包含的证书主体信息发生变化时，订户必须申请进行证书变更，以确保不影响依赖方对证书的信任。

SHECA 在对申请者递交的资料进行鉴别确认后，将为其重新签发证书。

4.8.1 证书变更的情形

当订户的信息发生变化，造成实体身份发生变化时，用户必须对原有证书进行变更，或者将证书申请撤销后重新要求签发证书。包括：

- 订户名称、地址等信息发生变更
- 订户因为组织重组等原因发生变更
- 其它信息发生变更

如果证书内包含信息的变更可能影响订户权利义务的改变，则订户不能申请证书变更，只能撤销该证书，再重新申请新的证书。

证书变更的申请和证书申请所需的流程、条件是一致的。

4.8.2 证书变更请求的处理

SHECA 接收到证书变更请求后，按照 3.2 条的规定对申请者的身份和请求信息进行鉴别确认；若发起方不是证书订户，SHECA 需取得订户同意。在完成上述工作后为其签发新的证书，该证书仍然使用原有公钥。

4.8.3 变更证书的签发

同本文件第 4.3 条。

4.8.4 构成接受变更证书的行为

同本文件第 4.4 条。

4. 9 证书撤销和冻结

订户或其受托人、电子认证服务机构、依赖方、法律或者政府权力部门等可

以要求将证书撤销。

证书撤销后，证书持有者可以重新向 SHECA 申请电子签名认证证书，与初始申请时的程序手续相同。对于被撤销证书中公钥所对应的私钥，在证书撤销后适用的保存期内，如私钥未完成销毁，订户必须以可信的方式持续予以防护。

目前，SHECA 不提供证书冻结服务。一旦提供冻结服务，SHECA 将会通过网站等进行公布。

4.9.1 证书撤销的情形

1、除一次性证书外，若出现以下情况中的一种或多种，SHECA 在 24 小时之内撤销订户证书：

- 订户（或其授权的代理人）请求撤销证书，并确定请求撤销者是订户本人；
- 由于证书的不当使用而违反国家的法律法规；
- 订户告知 SHECA 原证书申请并未获得本人有效授权，且无事后补办授权的意愿
- SHECA 有证据指明，订户证书中公钥配套的私钥有泄露的风险，或不再符合本 CPS 中关于密钥长度及密钥参数设置和质量检查的要求（具体请参见本文件 6.2、6.3 和 6.5）；

2、除一次性订户证书外，若出现以下情况中的一种或多种，订户证书将在 SHECA 发现后 5 天内被撤销：

- SHECA获得证据，表明证书被滥用；
- SHECA发现证书的签发不符合CPS的要求；
- SHECA发现订户证书里的证书主体信息做了实质性的更改；
- SHECA签发证书后发现订户申请证书时提供的资料存在虚假信息；

- 订户违背了本CPS、订户协议等规定的义务、陈述或担保、或者订户不再能履行相关协议规定的义务；
- 订户没有履行付费义务；
- 继续使用证书会对SHECA的商业信用和信任模式造成损害；
- 由于技术或标准演变可能导致依赖方或应用软件提供方产生不可能接受的风险；
- SHECA依据本CPS的要求撤销证书；
- 法律法规的相关规定或要求。

注意：

SHECA 没有义务一定要公开某一张证书被撤销的原因。

当上述状况发生时，相关证书应被撤销并发布到证书撤销列表。被撤销的证书必须包含在之后所公布的证书撤销列表中，直到该证书有效期到期为止。

3、如订户不接受证书，则 SHECA 会立即撤销。

4.9.2 请求证书撤销的实体

能够要求撤销证书的实体包括：

- 订户、证书主体、受托人、SHECA 及依赖方
- 法院、政府主管部门及其他公权力部门

4.9.3 撤销请求的流程

1、证书订户或指定的代理人提出撤销申请，支持在线申请及线下网点现场申请。网站：https://www.sheca.com/

2、SHECA 进行证书撤销请求的鉴别和验证

a) 针对订户或其受托人发起的撤销请求，需要进行鉴别和验证，同本文件 3.2、3.3 条。

b) 针对非订户或其受托人的其他主体发起的撤销请求，SHECA 需要验证身

份与权限，核实撤销原因，并做出是否撤销的决定。

4.9.4 撤销请求宽限期

订户一旦发现证书存在需撤销情形，应立即提交证书撤销申请；若因客观事由造成申请延迟，延迟时长最长不得超过八小时。宽限期内，因订户未及时提交撤销申请所引发的一切损失与相关责任，均由订户自行承担，SHECA 不承担任何责任。

4.9.5 依赖方检查证书撤销的要求

依赖方在信任证书前应按照 4.5.2 要求进行验证。

4.9.6 CRL 发布频率

根/中级 CA 签发第一张证书后的 24 小时内发布 CRL。根/中级 CA 到期或撤销或私钥销毁之前，不得停止发布 CRL。

对于订户证书，至少每 5 天或在订户证书被撤销后的 24 小时内公布 CRL。订户证书 CRL 的下次更新时间（nextUpdate）字段与本次更新时间（thisUpdate）字段的差不超过 7 天。

对于根/中级 CA 证书，至少每 7 个月或在根/中级 CA 证书被撤销后的 24 小时内公布 ARL。根/中级 CA 证书 ARL 的下次更新时间（nextUpdate）字段与本次更新时间（thisUpdate）字段的差不超过 10 个月。如根/中级 CA 证书被撤销，SHECA 将在网站公布相关撤销信息。

在紧急情况下，SHECA 可自行决定证书撤销列表的时间和频率。

4.9.7 CRL 发布的最大滞后时间

CRL 一般在批准撤销请求后 24 小时内生效。特殊紧急情况下可以立即生效（不考虑网络传输条件的影响，因为网络因素造成的时效差异是被允许的）。生效表示 SHECA 将在 CRL 中公布被撤销的证书。

4.9.8 在线状态查询的可用性

SHECA 向证书订户和依赖方提供在线证书状态查询服务（OCSP），OCSP 的可用性符合 GB/T 19713 中的相关要求。OCSP 必须：

a) 由签发待查询撤销状态的证书的 CA 签名，或

b) 由 OCSP 响应程序签名，该响应程序的证书由颁发待查询撤销状态的证书的 CA 签名。该种情况下，OCSP 签名证书必须包含 GB/T 19713 定义的 id-pkix-ocsp-nocheck 类型的扩展。

SHECA 提供的 OCSP 服务网址为：

http://ocsp.sheca.com

http://ocsp3.sheca.com

SHECA 提供的 OCSP 服务可用性不低于 99.9%。

4.9.9 在线状态查询要求

1、对于订户证书的状态：

SHECA 实时更新 OCSP，且 OCSP 响应的最长有效期不低于 8 小时，不超过 7 天。

2、对于中级 CA 证书的状态：

SHECA 保证 1）每年至少更新一次 OCSP；2）在撤销中级 CA 证书后 24 小时内更新 OCSP。

SHECA 不设置任何的读取权限，用户可以自由进行在线状态查询。如果依赖方无法查询 CRL，则应通过 OCSP、访问网站或拨打客户服务热线等的方式对证书状态进行查询。

4.9.10 撤销信息的其他发布形式

SHECA 通过 CRL 的方式发布证书的撤销信息，SHECA 目前不提供其它的撤销信息发布方式。

4.9.11 密钥损害的特别要求

订户如果发现或者怀疑密钥安全被损害时，应该立即申请对该证书进行撤销。

如果 SHECA 自身的密钥发生损害，或者由于 SHECA 的原因致使 SHECA 提供给用户的密钥发生损害，SHECA 将主动、即时的撤销证书，并实时将证书发布到 CRL。

4.9.12 证书冻结的情形

SHECA 目前不支持证书冻结。

4.9.13 请求证书冻结的实体

不适用。

4.9.14 冻结请求的流程

不适用。

4.9.15 冻结的期限限制

不适用。

4.10 证书状态服务

4.10.1 操作特征

SHECA 提供两种证书状态查询服务：

1、CRL 查询：CRL 通过目录服务器进行发布，其可信度及安全性由 SHECA 的签名来保证。用户需要将 CRL 下载到本地后进行验证，包括 CRL 的合法性验证和检查 CRL 中是否包含待检验证书的序列号等信息。

2、OCSP 查询：用户可以通过 OCSP 协议查询证书状态。OCSP 提供实时的证书状态信息的查询。OCSP 响应中的撤销条目必须保留与 CRL 条目相同的时间。SHECA 至少每 24 小时公布和更新一次证书的目录服务和 CRL，并会根据有关法律、政策的要求以及证书服务的要求，调整更新和公布时间间隔；对于这

种调整，SHECA 将通过 https://www.sheca.com 进行公布。

4.10.2 服务可用性

SHECA 提供 7*24 小时可用的证书状态服务，服务可用率不低于 99.9%。

SHECA 保证 CRL 和 OCSP 查询的正常使用。一旦出现异常，用户可以通过 HTTP、访问网站或拨打客户服务热线等方式查询，从而获得证书状态信息。

SHECA 保证 CRL 和 OCSP 功能响应时间不超过 10 秒。

4.11 停止使用认证服务

下列情况，视为证书用户停止使用 SHECA 提供的证书服务：

1、证书到期后，证书订户不再延长证书使用期或者不再重新申请证书，自动终止与 SHECA 的服务。

2、在证书有效期内，证书订户提出终止服务。 一旦用户在证书有效期内终止使用 SHECA 的认证服务，SHECA 在批准其终止请求后，将在 5 天内撤销证书，并按照 CRL 发布策略进行发布。

订户自行保管密钥载体的，订户应自行销毁签名私钥；订户使用 SHECA 管理的密钥载体生成签名密钥且在签名时私钥仅由订户控制的，SHECA 将在订户终止服务后 2 天内，安全销毁签名私钥及其所有备份，具体按照《云执钥®远程可靠电子签名服务策略》4.4 执行。

订户相关数据按本文件第 5.5 条的归档保存期限保留，到期后按规定销毁。

停止服务后，本 CPS 中涉及审计、保密信息、隐私保护、知识产权、赔偿及有限责任的条款继续有效。

SHECA 将完整记录以上操作记录。

4.12 密钥托管与恢复

4.12.1 CA 密钥的托管与恢复

SHECA 签名私钥不允许托管。SHECA 签名私钥的备份与恢复见本文件 6.3.4。

4.12.2 订户私钥的保管与恢复

订户使用认证机构管理的密钥载体生成并保管签名密钥的，订户私钥的保管恢复见本文件 6.3.2、6.3.3 和 6.3.4，具体按照《云执钥®远程可靠电子签名服务策略》执行。

策略名称	策略 OID
基础级远程可靠电子签名服务策略	1.2.156.112570.50.1.1
高等级远程可靠电子签名服务策略	1.2.156.112570.50.1.2

5. 认证机构设施、管理和操作控制

5.1 物理控制

SHECA 的电子认证服务系统位于安全稳固的建筑物内，具备独立的软硬件操作环境。只有经过授权的操作人员，才可以根据有关的安全操作规范进入相应的区域进行操作。SHECA 的 CA 密钥位于最高安全强度的环境内，避免被破坏或者被未经授权的操作。

5.1.1 场地位置与建筑

SHECA 的主机房位于上海宝山区富联 3 路 1 号，数据备份机房位于上海浦东亮景路 36 号，两个机房距离 35 公里。

SHECA 的建筑物及机房建设按照 GB/T 2887 以及 GB/T 9361 标准实施，屏蔽环境的屏蔽效能满足 BMB 3 C 级的要求。

机房采用高安全性的监控技术，以及门禁权限控制等安全管理手段，以确保物理通道的安全。进入 SHECA 机房时，有可控时间限制的门禁系统。机房实行全天候自动监控。

机房设置了监控室。监控室是安全管理人员和网络管理人员工作的地方，可对整个 CA 的进出人员实行监控，处理日常的安全事件。只有安全管理人员、网络管理人员使用身份识别卡和指纹鉴别才可以进入，刷卡离开。

机房区域划分为：公共区、服务区、管理区、核心区，具体如下：

a）公共区：机房入口之外的区域为公共区。

b）服务区：服务区是各种对外提供 web 服务的设备和系统所在区域，需要同时经过相关身份识别卡和指纹鉴别才可以进入，人员进出服务区有日志记录。所有的墙体采用高强度防护墙。

c）管理区：管理区是 CA 工作人员工作的区域。此区域必须通过身份识别卡鉴别通过后才可以进入。人员进出保留日志记录。

d）核心区：证书认证密钥管理系统和证书认证系统中的核心子系统及其所需的加密设备部署在该区域。核心区通过相关权限检验和身份鉴别才可以进入；屏蔽机房两名可信人员同时经过相关权限检验和身份鉴别才可以进入。核心区采用双人共管、双因素认证，并记录访问信息。核心区为屏蔽机房，加装高强度的钢制防盗门。所有进出屏蔽室的线路采取防电磁泄漏措施。核心区每五年进行一次屏蔽效能检测，确保达到 BMB 3 或 GJB5792A 中 C 级的要求。

5.1.2 物理访问控制

SHECA 的服务区、管理区和核心区的门禁系统可实现对人员进出控制，操作人员进入工作区域进行操作，必须通过双因素认证。进出每一道门都有日志记录。

操作人员进入机房区域，必须通过身份识别卡和指纹鉴别的身份检验。进出屏蔽机房，必须两人及以上同时进入，并有 24 小时视频监控。

监控记录包括对机房通道上所有踪迹的记录。所有经 SHECA 授权的人员在机房区域活动都需要有 SHECA 信息化支撑部人员陪同。SHECA 授权的人员清单经审批通过后提供给信息化支撑部，以保证只有经授权的人员才能进入机房。

非公共区域（包括服务区、管理区、核心区）的视频监控记录和门禁访问记录保存 5 年，上述记录在销毁前应进行安全审计，形成的审计报告存档备查。

5.1.3 电力与环境保障

CA 系统所在机房配备两路 UPS，该 UPS 配备两路不同市电保障供电不间断。

CA 系统空调系统使用独立的空调和通风设备，保持相对湿度在 40%-60%范围内，保持温度在 18-28℃范围内，以保证系统稳定运行。

5.1.4 水患防治

SHECA 的机房采取了加高地板的处置措施，能够防止水患侵蚀。

5.1.5 消防措施

机房采用防火材料建设，具备中央防火监控设备和自动喷淋系统。机房配备联动的火灾自动报警系统和自动灭火系统，包含温度和烟雾检测功能；机房配备了七氟丙烷灭火系统，同时配备专用氧气呼吸器。

SHECA 还通过与专业防火部门协调，建立了消防灭火等应急响应措施，机房通过了国家权威部门的消防测试。

5.1.6 存储媒体管理

SHECA 已制定详细的存储媒体使用、报废管理规定，规定包含使用权限、报废标准、销毁方法和审批流程；完整记录存储媒体领用、归还、报废等情况。

1、存储媒体使用

a）领用前，由领用人填写《固定资产的领用表》，经领用人和资产管理部门共同验收合格后方可领用；

b）使用人在存储媒体正式投入使用前，应对该设备进行识别，在显著的位置张贴标识（设备编号、设备名称、部门、责任人）；

c）储存过信息的存储媒体再次使用前必须经过格式化后才可使用；

d）外来信息如需复制到服务器上必须通过机房指定的存储媒体复制信息，并在复制前对磁盘上的信息进行安全扫描，通过后方可复制；

e）存储媒体变更时（上线、下线、替换、升级和配置改变），需求人填写

《系统变更申请单》，明确变更类型、变更原因及内容并上传变更方案，经部门负责人、分管领导和总经理审批；

f）存储媒体的维修原则上由已签订协议的维护方进行，当涉及公司系统停运，影响到业务停止时，必须填写《固定资产维修单》，经审批通过后，方可执行。外部维修应指定专人全程旁站陪同并与与维修单位和维修人员签订保密协议。禁止维修人员恢复、读取和复制被维修设备中的涉密信息。禁止通过远程维护和远程监控。

2、存储媒体归还

a）存储媒体归还，领用人发起归还流程，经部门负责人审批通过，并由相关技术部门核验设备使用状态，完成数据格式化处理后归还仓库。归还时若硬盘等存储介质缺失，归还人须提交书面情况说明。

3、存储媒体报废

a）存储媒体的报废使用，建议性年限管理（5 年）和技术性报废管理。达到报废年限后，经相关部门评估合格的可延期使用。延期使用的设备应每年进行评估。符合以下任一条件的存储媒体应予以技术性报废：

- 主要性能严重下降且无法满足业务最低运行要求；
- 存在无法修复的硬件故障或单次维修成本超过设备残值 50%；
- 经两次及以上大修仍频繁故障，MTBF 明显低于业务可接受水平；
- 原厂已停止备件供应超过 1 年且无兼容替代品；不符合国家政策。

b）存储媒体报废参照上述标准填写《固定资产处理表》，经资产管理部门负责人审批后，报财务总监、总经理审批；

c）报废处置前由相关技术部门拆除硬盘等数据存储介质；拆下的存储介质由仓库管理员统一编号、登记台账，移交市保密技术服务中心集中处置。

SHECA 完整记录存储媒体领用、归还、报废等情况。系统使用的存储介质，处在防磁、防静电干扰的环境中，得到了安全可靠的保护，避免诸如温度、湿度、和磁力等环境变化可能产生的危害和破坏。

5.1.7 设备管理

SHECA 已建立设备台账，设备台账包含每台设备的责任人、使用状态、维护周期和报废标准；定期进行设备盘点和核对，确保设备实际情况与设备台账相符。

SHECA 使用的硬件设备、存储设备、加密设备等，当废弃不用时，涉及敏感性和机密性的信息都被安全、彻底的消除。

文件和存储介质包含有敏感性和机密性信息时，在处理时都经过了特殊的销毁措施，保证其信息无法被恢复和读取。

所有处理行为将记录在案，以满足审查的需要，所有的销毁行为都遵循有关的法律法规。

5.1.8 备份管理

SHECA 进行异地的实时数据备份，备份位置上海浦东亮景路 36 号，距离主机房 35 公里。同时，SHECA 每天进行本地数据库文件全量备份，并落移动存储介质保存。异地备份的操作在 SHECA 灾难恢复计划中进行规定。SHECA 异地数据备份介质安全要求都符合 SHECA 备份标准和程序。备份提供归档检索与恢复功能。

5.2 操作过程控制

5.2.1 可信角色

证书服务具有高可靠性和高安全性的要求，所有涉及证书认证系统操作、维护与管理，即所有有权使用或控制那些可能影响证书的签发、使用、管理和撤销等操作（包括对 SHECA 信息库限制性操作）岗位的员工均视为可信角色，必须由可信人员担当。可信角色包括：

a) 超级管理员：其权限为添加、删除、修改 CA 业务管理员帐号

b) 系统管理员：负责系统策略配置、用户与权限管理等

c) 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

d) 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

e) 审计管理员：其权限为添加、删除、修改 CA 审计员帐号

f) 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

g) 密钥管理员：负责 CA 证书密钥材料管理、CA 证书密钥生存周期管理等

h) 业务管理员：其权限为添加、删除、修改 CA 业务操作员帐号

i) 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

j) 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

k) 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

l) 其他人员：对公司运营有重要影响的其他管理人员

安排上述职位是为了确保责任能够明确分担，建立有效的安全机制，保证内部管理和操作的安全。

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：

a) 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

b) 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

c) 业务操作员、客户档案管理员、运营审计员之间不得兼任

d) 密钥管理员不得与系统管理员、技术运维员兼任

e) 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 可信人员资格要求

SHECA 对可信人员进行严格的背景调查。背景调查需要核实的内容包括但不限于以下方面：

- 验证从业经历的真实性
- 验证身份证明的真实性
- 验证学历、学位及其他资格证书的真实性
- 确认无犯罪记录
- 具备履行岗位职责所需的专业技能
- 签署劳动合同
- 签署具备法律约束力的保密协议，承诺不得私自保存、复制、泄露 SHECA 证书服务体系的敏感信息

SHECA 不允许未与 SHECA 签署劳动合同的人员担任可信人员。

5.3.2 可信人员培训要求

SHECA 建立覆盖所有可信角色的持续培训体系。

a）岗前培训

所有可信人员上岗前须完成不少于 20 学时的培训并通过考核。

b）持续培训

可信人员应每年至少接受一次培训，每人每年培训时长不少于 20 学时，并通过考核。

c）培训内容包括但不限于：

- 电子认证服务相关法律法规与标准
- 岗位通用职责要求及各角色特定的工作要求

- 内部管理政策、制度及流程等
- PKI 和密码技术基础知识
- CPS、CP
- 安全管理策略和机制
- 订户身份鉴别和审核策略和流程
- 电子认证服务运营体系构成
- 电子认证服务技术体系构成
- 灾难恢复和业务连续性管理

5.4 审计日志程序

5.4.1 记录范围

包括但不限于：

a）CA 证书密钥操作：包括密钥生成、备份、存储、恢复、归档、销毁，以及密码设备的启用、停用、转移和销毁等；

b）证书生存周期关键过程：包括记录证书申请、审核、签发、更新、变更、撤销、密钥恢复等操作，CRL 的签发与发布等，所有操作的通过或拒绝结果均应明确记录；

c）证书认证系统和证书认证密钥管理系统访问行为：包括所有对系统的访问企图，包括成功的和失败的登录、退出、权限使用行为等；

d）证书认证系统和证书认证密钥管理系统操作与变更：包括对系统的各种关键查询、修改、删除等操作，系统组件的安装、升级、维修，人员，以及敏感信息的获取与取阅等；

e）网络安全事件：包括防火墙、路由器、入侵检测安全设备记录的告警信息，以及针对被攻击事件识别与相应处理过程、结果等；

f）系统环境事件：包括通用服务器、虚拟化平台、堡垒机等设备的管理员操

作日志及配置变更等；

g）机房门禁控制等物理环境事件：包括业务人员、安全运维人员、外部人员等在不同安全区域的进出记录等。

5.4.2 记录内容

SHECA 记录与 CA 系统相关的事件，包含事件时间、类型、内容、操作人、作用对象及结果。对系统的关键操作应由操作人员进行电子签名。

5.4.3 保存期限

SHECA 保留系统审计日志至少 5 年，法律法规另有规定的，按照相关法律法规执行。

SHECA 执行严格的物理和逻辑访问控制措施，以确保只有 SHECA 授权的人员才有可能接触到这些审查记录。这些记录处于严格的保护状态，严格禁止未授权的访问、阅读、修改和删除等操作。

5.4.4 日志审计内容

SHECA 日志审计内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

5.4.5 审计周期

SHECA 每季度对日志记录进行审查，形成审计报告，并基于结果采取改进措施。

5.5 记录归档

5.5.1 归档记录的类型

SHECA 对下列记录（包括但不限于）进行归档保存：

a）证书申请材料和订户意愿记录；

b）所有审计日志；

c）密码设备全生存周期管理记录；

d）密码设备的日常操作与使用记录；

e）根证书或密钥生存周期管理相关的全部记录；

f）证书认证系统运行日志；

g）已识别的安全事件及处置记录；

h）证书认证系统关键操作日志；

i）电子认证服务过程中其他操作记录；

j）其它 SHECA 认为需要归档的内容，如 CP、CPS、订户协议、依赖方协议的所有版本；CRL 文件的所有版本；各类内部评估、外部审计、合规性检查相关材料；可信人员的背景调查、录用、培训、考核、岗位变动、离岗等相关资料；投诉处理、争议解决相关资料等。

5.5.2 归档记录的保存期限

a) CA 证书和密钥生命周期内的管理事件记录，在其生命周期结束后，额外保留不少于 5 年；

b) 订户证书生命周期管理和操作记录，归档保留期限不少于证书撤销或失效后 5 年；

c) 与密码设备、CA 证书、CA 密钥相关的归档记录，长期保存；

d) CP、CPS、订户协议、依赖方协议的所有版本；各类内部评估、外部审计、合规性检查相关材料；可信人员的背景调查、录用、培训、考核、岗位变动、离岗等相关资料，长期保存；

e) 其它记录保留期限不少于 1 年。

5.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证，以保证归档文件能够得以长期有效的保存。只有经过授权的工作人员按照特定的安全方式才能接近和存取。除了法律的需要和认证操作规范的需要，任何人不得随意获得。

5.5.4 归档文件的备份程序

所有存档的文件和数据，通常保存在 SHECA 的主要存储场所。确有必要的，还将在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的工作人员才能在监督的情况下，对档案进行读取操作。SHECA 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。

对于需要持续保存、归档的文件和数据，将根据 SHECA 的备份策略进行归档和整理。

当认证系统因为异常情况导致无法正常运营时，按照 SHECA 的恢复策略，利用这些归档保存的数据进行系统的恢复。

5.5.5 获得和检验归档信息的程序

SHECA 设置专门的归档管理机构统一管理归档记录，明确管理职责、操作规范、安全要求。只有被授权的可信人员能够访问归档记录。归档记录的一致性在归档时进行验证。归档期间，所有被访问的记录在归还时必须验证其一致性。

5.6 电子认证服务机构 CA 证书密钥更替

SHECA 的 CA 证书有效期最长不超过 30 年，任何由其签发的证书，包括中级 CA 证书和订户证书，其有效期都短于 CA 证书的有效期，任何由中级 CA 其签发的订户证书，其有效期都短于中级 CA 证书的有效期。

CA 证书及中级 CA 证书的有效期，在证书内有明确的表示。

在证书到期前，SHECA 将对 CA 密钥进行更换，生成新的证书。在进行密钥的生成时，严格按照 SHECA 关于密钥管理的规范。CA 密钥更替必须遵循以下原则：

a) 在下级证书生命周期结束前停止签发新的下级证书，确保在 CA 的证书到期时所有下级证书也全部到期；

b) 在屏蔽机房内产生新的密钥对，签发新的 CA 证书，详见本文件 6.2.1；

c) 将新的 CA 公钥证书通过官网发布给订户和依赖方;

d) 在停止签发新的下级证书后至证书到期时，继续使用 CA 私钥签发 CRL，直到最后一张下级证书过期后；按 GB/T25056 一 2018 中 8.2.4.3 规定的方式，将旧 CA 密钥连同备份一同销毁，并保留相关记录；

e) 若是紧急更替，发现密钥泄露或存在安全隐患，应立即启动密钥更替程序；若是到期更替，在密钥到期前三年完成密钥更替，确保整个过渡过程安全、顺利，不出现信任真空期。

5.7 损害和灾难恢复

为了在出现异常或灾难情况时，能够在最短的时间内重新恢复认证系统的运行，设定业务连续性目标：灾难恢复的恢复时间目标（RTO）为不超过 24 小时，恢复点目标（RPO）为不超过 1 小时。为此，SHECA 制订了可靠的损害与灾难恢复的预案与流程：

- 证书库的恢复过程：根据 SHECA 业务连续性计划要求，证书库的物理设施、计算资源、网络线路、应用及对象存储均已实现 HA，数据库本地热备以实时或近实时复制为主，故障时优先在本地通过主从切换或日志回滚快速恢复，本地热备出现不可用时启用异地灾备节点恢复相应数据；加密机本地故障自动主备切换，本地集群失效则启用异地灾备加密机。在此环境中生成受影响并被撤销的证书列表，并重新向订户提供实体公钥证书；
- CA 密钥损害的恢复过程：见本文件第 5.7.3 条；
- 其他关键资产恢复过程：SHECA 的物理设施、计算资源、网络线路、软件均已实现 HA，数据库本地热备以实时或近实时复制为主，故障时优先在本地通过主从切换或日志回滚快速恢复；异地灾备以异步复制+定期全量备份构建跨区域冗余，当本热备出现问题不可用时，通过数据库主备地址切换、负载均衡或应用配置变更将流量切至异地数据库节点，并从异地备份恢复数据；

c) 根私钥应急处理：见本文件第 5.7.3 条；

d) 事件报告：见本文件第 5.9 条；

e) 定期验证：定期验证备份的设备、数据可用性，包括备份恢复测试和功能验证，SHECA 每年进行一次灾难恢复演练。

5.7.1 事故和损害处理程序

SHECA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，SHECA 将按照灾难恢复计划实施恢复。具体由 SHECA 灾难恢复计划决定。

5.7.2 计算资源、软件和/或数据的损坏

当认证系统运营使用的软件、数据或者其他信息出现异常损毁时，可以依照 SHECA 的系统备份与恢复操作手册，根据系统内部备份的资料，或者异地备份的资料，执行系统恢复操作，使认证系统能够重新正常运营。

当认证系统使用的硬件设备出现损毁时，可以依照 SHECA 的系统备份与恢复操作手册，启动备份硬件设备以及相关的备份操作系统和认证系统，重新恢复系统运行。

SHECA 将尽快完成恢复过程，在 24 小时内恢复证书服务。

5.7.3 SHECA 私钥损害处理程序

对于实体证书私钥的损害，SHECA 有如下处理要求和程序:

当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立即访问 SHECA 的证书服务网站撤销其证书，或者立即通过电话、电子邮件等方式通知 SHECA 撤销其证书。SHECA 按文件 4.9 发布证书撤销信息。

当 SHECA 发现证书订户的实体证书私钥受到损害时，SHECA 将立即撤销证书，并通知证书订户，订户必须立即停止使用其私钥。SHECA 按文件 4.9 发布证书撤销信息。

当 SHECA 的 CA 证书或其受委托的 CA 证书出现私钥损害时，SHECA 将立即撤销该 CA 证书并及时通过广达的途径通知依赖方，然后生成新的 CA 密钥对、签发新的 CA 证书。

5.8 电子认证服务机构终止

SHECA 如果因技术性原因或商业原因需要终止服务时，应遵循以下流程和通告机制，包括但不限于：

a) 起草并发布 CA 终止声明，至少提前九十日通知与证书订户、依赖方等相关实体，至少提前六十日向主管部门报告

b) 选聘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

c) 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

d) 停止证书状态服务并归档相关数据

e) 停止其他电子认证相关服务并归档相关数据

f) 停止密码设备并归档相关密钥数据

g) 及时撤销或冻结业务管理员和业务操作员的操作权限

h) 对所有存档文件记录进行整理和封存

i) 对所有敏感文档和数据进行安全处理和封存

j) 清除主机和密码硬件设备中的敏感数据

k) 其他涉及 CA 运营的数据、密钥安全的操作

l) 如果有与电子签名认证证书签发、管理相关的外部合作机构，SHECA 在官网发布该外部合作机构终止服务的通告

5.9 重大事项报告

SHECA 已建立重大事件的报告流程，包括事件发生后向公司管理层、上级机构和主管部门报告的程序、时限与内容。

5.9.1 重大事项范围

重大事件包括但不限于：

1、证书认证系统迁移或改造：包括系统软件、网络、部署的重大改变。符合以下任意之一：

- 机房迁移，或机房内服务区、管理区或核心区划范围改变
- 变更电子签名认证证书签发逻辑
- 新增远程证书注册子系统
- 新增、更改或者删除用于签发电子签名认证证书的证书链
- 其他对电子认证服务安全、用户资料安全有影响的改变

2、重大安全事故：包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形。符合以下任意之一：

- 证书签发及验证服务连续停机时间超过 24h
- 发生 CA 证书密钥等关键数据泄露
- 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
- 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）

3、订户信息泄露事件：包括订户身份信息、证书申请资料等敏感数据被泄露等。符合以下任意之一：

- 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
- 数据丢失导致无法恢复证书状态信息

a) 合规性事件：包括不符合相关法律法规、标准或监管要求的情形。符合以下任意之一：

- 涉及电子认证服务的司法判定
- 收到行政部门违规通知或处罚决定

4、人力资源类事件：包括一个月内核心管理层集体离职、大规模劳动纠纷、重大职场安全事件等。符合以下任意之一：

- 涉及 2 名及以上管理层人员或 10%以上可信人员的离职
- 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 CA 承担法律责任

5.9.2 重大事项报告流程

1、针对计划性重大事项(如证书认证系统迁移或改造)

- 立项及风险预评估：由技术部门发起变更申请，全面开展风险评估，编制完整操作流程与故障回退方案；
- 事前报审报备：于计划实施前规定时限，向公司管理层报送《重大变更实施方案》，同步按监管要求向主管部门完成事前报备，禁止未批先行实施。
- 仿真环境全量测试：涉及核心业务逻辑、证书链条调整的变更，须先在模拟环境完成全流程验证，出具合格测试报告后方可进入实操阶段；
- 错峰双人实施：变更操作限定业务低峰时段执行，操作全程双人交叉复核；
- 上线核验与事后通报：变更落地后开展固定周期系统稳定性监测；核验无异常后，向公司管理层、行业主管部门正式出具《变更完成通知书》；

2、针对突发性重大事项（如突发重大应急、高危安全类事件）

- 即时上报与初步研判：运维监控、安全审计及各岗位人员发现异常，发现人 1 小时内以即时通讯或口头形式上报应急领导小组组长；领导小组接报后 2 小时内组织技术专家研判，界定是否属于重大高危安全事项；
- 分级限时正式报送：经判定为重大高危安全事件后，严格执行分级上报时限：
- 公司管理层：确认事件后第一时间紧急汇报，同步同步风险概况供应急决策；
- 上级机构：确认事件 24 小时内以正式公文、邮件同步事件影响、处置措施；
- 若按规定需上报行业监管部门的（工业和信息化部、密码管理局等），按照监管报送规范上报；

- 完全持续跟进与闭环结案：事件处置周期内，每 24 小时向主管部门同步处置进展，直至风险完全消除；事件闭环后 5 个工作日内提交《重大事项整改总结报告》，包含事故根源、处置成效、长效优化方案。

6. 技术安全控制

6.1 技术安全管理制度要求

SHECA 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，并每年接受安全认证委员会的评审。

6.2 密钥对的生成和安装

密钥对是电子签名安全机制的关键，本 CPS 制订了相应的规定，确保密钥对的产生、传送、安装等具备保密性、完整性和不可否认性。

6.2.1 密钥对的生成

6.2.1.1 SHECA CA 密钥对的生成

SHECA 的 CA 密钥对是由通过国家密码主管部门批准和许可的硬件密码设备生成的。

在生成 SHECA 的 CA 密钥对时，必须经过安全认证委员会授权，有超过 3 位的具备权限的密钥管理和操作人员在场，同时操作硬件密码设备产生密钥对。任何人无法独自完成 CA 密钥对的产生，而且密钥在硬件密码设备内部生成并存储。任何和私钥有关的操作都在硬件密码设备进行，完成后将结果输出，私钥无法以明文方式输出到硬件密码设备之外。

CA 密钥的生成、备份、恢复、销毁过程应实施 M 选 N 多人控制机制，M 不少于 5，N 不少于 M/2，操作应在安全认证委员会授权下进行，并通过录音录像方式全程记录，保存期限不少密钥失效后十年。

6.2.1.2 订户签名密钥对的生成

SHECA 明确订户签名密钥对的生成、交付及控制方式，并符合以下要求之一：

1、订户使用自有密钥载体自行生成签名密钥的：

SHECA 应在证书申请时要求订户使用密钥载体符合 GM/T 0028 安全二级及以上的密码模块，订户应向 SHECA 提供密钥载体的品牌、型号、商用密码产品认证证书编号和/或硬件（软件）序列号等信息；SHECA 通过订户协议，明确订户签名私钥的管控风险，以及订户对签名私钥的保管和使用责任。

SHECA 如果明确知悉订户使用了不符合上述规定的密钥载体生成密钥的，将拒绝为其签发证书。

2、订户使用 SHECA 提供的密钥载体生成签名密钥、并在证书签发后由 SHECA 将密钥载体交付订户的：

SHECA 使用符合 GM/T 0028 安全二级及以上的、经检测认证合格的密码模块作为密钥载体，并对密钥载体本身的安全机制负责。在密钥载体交付给订户前，SHECA 应确保密钥载体和签名私钥的安全；SHECA 通过订户协议，明确在密钥载体交付订户后，签名私钥的管控风险，以及对签名私钥的保管和使用责任。

3、订户使用 SHECA 管理的密钥载体生成签名密钥且在签名时私钥仅由订户控制的：

密钥对在符合 GM/T 0028 安全二级及以上的、经检测认证合格的硬件密码模块内生成，并经 KEK 加密后存储在防篡改可信执行环境的数据库中，KEK 应存储在符合 GM/T 0028 安全二级及以上的、经检测认证合格的硬件密码模块内，SHECA 通过订户协议，明确签名私钥的管控风险、对签名私钥的使用责任和签名私钥激活数据的安全保护义务。

具体的保护措施按照《云执钥®远程可靠电子签名服务策略》执行。

SHECA 完整记录所有与签名私钥相关的操作日志，包括时间、方式、操作人员等信息，保存期限不少于证书失效后五年。

4、SHECA 如果明确知晓订户签名私钥非以上三种方式生成或保管的，将拒绝为其签发证书。

6.2.1.3 订户加密密钥对的生成

订户的加密密钥对，由 SHECA 证书认证密钥管理系统生成。

6.2.2 私钥交付给订户

6.2.2.1 CA 证书私钥

SHECA 证书认证系统自身的私钥是在系统的初始阶段产生的。它保留在 SHECA 的系统中，不传送给 SHECA 之外的其它方。

6.2.2.2 订户签名私钥

1、订户使用自有密钥载体自行生成签名密钥的：SHECA 不负责私钥和存储私钥的密钥载体的交付。

2、订户使用 SHECA 提供的密钥载体生成签名密钥、并在证书签发后由 SHECA 将密钥载体交付订户的：

a) 如 SHECA 使用硬件密码模块生成签名密钥的，SHECA 将密钥载体和私钥激活数据以安全的方式采用不同的物理通道分别交付给订户。

b) 如 SHECA 使用移动智能终端安全密码密码模块/协同签名密码模块生成签名密钥的，订户的私钥分量存储于客户端密码模块中，SHECA 不负责私钥分量和私钥分量激活数据的交付。

3、订户使用认证机构管理的密钥载体生成并保管签名密钥的：私钥不交付给订户，订户通过页面下载证书或确认同意接受即视为证书接受，具体按照《云执钥®远程可靠电子签名服务策略》执行。

6.2.2.3 订户加密私钥

1、如订户只申请签名证书的，不涉及加密私钥的交付。

2、订户使用自有密钥载体自行生成签名密钥的：SHECA 将按 GM/T0009 规定的格式或使用订户签名公钥进行数字信封加密保护的加密私钥交付给订户。

3、订户使用 SHECA 提供的密钥载体生成签名密钥、并在证书签发后由 SHECA 将密钥载体交付订户的：

a) 如 SHECA 使用硬件密码模块生成签名密钥的，SHECA 将按 GM/T0009 规定的格式或使用签名公钥进行数字信封加密保护的加密私钥写入密钥载体一并交付给订户。

b) 如 SHECA 使用移动智能终端安全密码密码模块/协同签名密码模块生成签名密钥的，SHECA 将按 GM/T0009 规定的格式或使用签名公钥进行数字信封加密保护的加密私钥存储于订户的客户端密码模块中。

4、订户使用认证机构管理的密钥载体生成并保管签名密钥的：只颁发签名证书，不涉及加密私钥的交付。

6.2.3 公钥传送给证书签发机构

订户以签名公钥向 SHECA 申请签发证书时，该请求信息（含签名公钥）应经签名私钥签名后传送给 SHECA。

订户加密公钥由 SHECA 证书认证密钥管理系统生成，无需将加密公钥传送给 SHECA。

6.2.4 电子认证服务机构公钥传送给依赖方

SHECA 的公钥包含在 CA 证书中，通过网站 https://www.sheca.com 进行发布。SHECA 支持在线传递公钥或从 SHECA 的网站下载的方式传递公钥，以供证书订户和依赖方查询使用。

6.2.5 密钥长度

订户的密钥对，对于采用 RSA 算法的密钥对，SHECA 确保 RSA 密钥长度为 RSA2048 位或以上且可以被 8 整除。采用 SM2 算法的密钥长度为 256 位。

SHECA 自身的 CA 密钥对，分别为 RSA2048 位、RSA3072 位、RSA4096 位和 SM2 算法的 256 位。

如果国家法律法规、监管部门等对密钥长度有明确的规范和要求，SHECA 将会完全遵从。

6.2.6 公钥参数的生成和质量检查

公钥参数必须使用国家密码主管部门批准许可的密码模块生成，例如由加密机、加密卡、USB Key、IC 卡等生成和选取，并遵从这些设备的生成规范和标准。SHECA 认为这些设备内置的协议、算法等已经具备了足够的安全等级要求。

对于参数质量的检查，同样由通过国家密码主管部门批准许可的密码模块进行，例如加密机、加密卡、USB Key、IC 卡等。SHECA 认为这些设备内置的协议、算法等已经具备了足够的安全等级要求。

6.2.7 密钥使用目的

SHECA 的根 CA 密钥仅在以下情况下签发证书和 CRL：

- 签发代表根 CA 的证书
- 签发中级 CA 证书和交叉 CA 证书
- 签发 OCSP 证书

中级 CA 密钥一般用于签发以下证书和 CRL：

- 签发证书
- 签发特定用途的 PKI 体系功能证书 (如 OCSP 证书)
- 签发 CRL
- 签发特定用途的 PKI 体系功能证书（管理角色证书、内部 CA 操作设备证书）；

SHECA 签发的电子签名认证证书是 X.509 v3 版本，证书的密钥用法（KeyUsage）项包含 digitalSignature 和 nonRepudiation，同时如果证书的扩展密钥用法（extKeyUsage）项内指明了其它用法，订户和依赖方均必须按照指明的用法使用密钥。

订户的签名密钥可以用于身份认证、不可抵赖性和信息的完整性保护等，加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安

全机制。

所有密钥的使用，都必须遵循本 CPS 的规范。

6.3 私钥保护和密码模块工程控制

SHECA 使用国家密码主管部门批准和许可的密码设备。所采用的密码设备均取得商用密码产品认证证书。

6.3.1 密码模块的标准

1、CA 私钥

SHECA 的密钥对密钥对必须在安全的物理环境中，由多个可信人员在国家密码主管部门批准和许可的硬件密码设备内部生成。密码设备符合 GM/T 0034 的要求。

2、订户私钥

订户的密钥对应在国家密码主管部门批准和许可的密钥载体内部生成，密钥载体满足 GM/T 0028 安全二级的要求。

6.3.2 私钥多人控制

1、CA 私钥

SHECA 采用多人控制策略来激活、使用、停止 CA 私钥（m 选 n）。

SHECA 的私钥采用（n，m）门限秘密分享机制（m 应大于等于 5，n 应为小于等于 m 且不小于 m/2 的整数）多人控制的策略生成。采用 5 人控制，需要至少 3 个或 3 个以上的密钥管理员来共同完成生成和分割程序。SHECA 系统在技术上已经建立了相应安全机制，对生成操作进行限制。

2、订户私钥

订户自行保管密钥载体的，私钥由订户唯一控制，订户应妥善保管密钥载体和私钥激活数据，防私钥被泄露、损坏、丢失或被非授权使用。当私钥发生上述安全问题时，订户有义务在第一时间告知 SHECA。

订户使用认证机构管理的密钥载体生成并保管签名密钥的，应妥善保管私钥激活数据，具体按照《云执钥®远程可靠电子签名服务策略》执行。

6.3.3 私钥托管

SHECA 的签名私钥不允许托管。

订户的加密私钥托管在 SHECA 证书认证密钥管理系统中。

订户使用认证机构管理的密钥载体生成并保管签名密钥，并由订户唯一控制签名私钥的，不视为私钥托管。

6.3.4 私钥备份与恢复

1、CA 私钥

SHECA 的私钥使用（n，m）门限秘密分享机制（m 应大于等于 5，n 应为小于等于 m 且不小于 m/2 的整数）多人控制的策略将密钥对中的私钥分割备份，并交由 m 个独立的分管者保管。采用 5 人控制，需要至少 3 个或 3 个以上的密钥管理员来共同完成密钥备份。

SHECA 密钥的恢复，同样至少 3 个或 3 个以上的密钥管理员来共同完成。

2、订户签名私钥

订户自行保管密钥载体的，自行根据所使用的密钥载体的安全机制进行私钥的备份与恢复，SHECA 不参与签名私钥的备份与恢复。

订户使用认证机构管理的密钥载体生成并保管签名密钥，并由订户唯一控制签名私钥的，SHECA 按照最小必要范围原则，仅以灾难恢复为目的开展密钥库的备份，SHECA 不提供对指定的单个或多个密钥进行备份与恢复的功能，具体按照《云执钥®远程可靠电子签名服务策略》执行。

3、订户加密私钥

订户加密私钥加密私钥由密钥管理中心备份，备份数据以密文形式存在。加密密钥的恢复，在按照本文件 3.2 执行订户身份确认后，按照 GM/T 0034 的方式恢复到密钥载体中|。

6.3.5 私钥归档

SHECA 的签名私钥在过期后，SHECA 应在 10 天内进行归档，归档保存至少 10 年。私钥归档应经过加密后按照严格的安全措施保存。

SHECA 不对订户的签名私钥进行归档。

订户的加密私钥在过期后保存在 SHECA 证书认证密钥管理系统的历史库中，保存期限不少于加密证书失效后五年。

6.3.6 私钥导入、导出密码模块

所有的私钥均应在密码模块中生成，密码模块中的私钥不能以明文的形式出现在密码模块之外。

SHECA 的私钥，严格的按照 SHECA 规定的程序和策略进行备份，除此之外的任何导出操作将不被允许。SHECA 的私钥，严格按照 SHECA 规定的程序和策略进行恢复，除此之外的任何导入操作均不被允许。

SHECA 不提供订户私钥从密码模块中导出、导入的方法，也不允许如此操作。

6.3.7 私钥在密码模块中的存储

所有的私钥均应在密码模块中生成，密码模块中的私钥不能以明文的形式存储在密码模块之外。

SHECA 的私钥，存储在硬件密码模块内部。

订户自行保管密钥载体的，私钥或者私钥分量存储于密码模块内部。

订户使用认证机构管理的密钥载体生成并保管签名密钥，并由订户唯一控制签名私钥的，签名私钥经 KEK 加密后存储在防篡改可信执行环境的数据库中，KEK 应存储在符合 GM/T 0028 安全二级及以上的、经检测认证合格的硬件密码模块内。具体按照《云执钥®远程可靠电子签名服务策略》执行。

6.3.8 激活私钥的方法

SHECA 的私钥，存储在硬件密码设备中，至少需要三名密钥管理员共同操

作才能激活。

订户自行保管密钥载体的，签名私钥由订户按照所使用的密钥载体的安全机制进行激活。

订户使用认证机构管理的密钥载体生成并保管签名密钥，并由订户唯一控制签名私钥的，签名人在本服务的客户端签名交互组件中完成身份验证后方可激活私钥，每次私钥调用操作，SHECA 均生成不可篡改的操作记录，并按本文件 5.4 和 5.5 的规定完成存储、审计和归档。具体按照《云执钥®远程可靠电子签名服务策略》执行。

6.3.9 解除私钥激活状态的方法

SHECA 的私钥一旦被激活，除非这种状态被解除，私钥总是处于活动状态。在某些私钥的使用当中，私钥每次被激活，只能进行一次操作，如果需要进行第二次操作，需要再次进行激活。

SHECA 解除 CA 私钥激活状态的方式包括退出、切断电源、移开令牌/钥匙，自动冻结。未经授权的任何人员，绝不可以进行相关操作。

订户自行保管密钥载体的，解除私钥激活状态由订户按照所使用的密钥载体的安全机制进行。

订户使用认证机构管理的密钥载体生成并保管签名密钥，并由订户唯一控制签名私钥的，签名完成后自动解除私钥激活状态，如需操作私钥应再次激活，具体按照《云执钥®远程可靠电子签名服务策略》执行。

6.3.10 销毁私钥的方法

SHECA 的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，按照密码设备中安全机制进行私钥销毁。同时，所有用于激活私钥的 PIN 码、IC 卡、动态令牌等也必须被销毁或者收回。私钥归档的操作按照本 CPS 的规定处理。

订户自行保管密钥载体的，可按所使用的密钥载体的安全机制销毁私钥。

订户使用认证机构管理的密钥载体生成并保管签名密钥，并由订户唯一控制

签名私钥的，在证书撤销或过期等情况下将销毁签名私钥，具体按照《云执钥®远程可靠电子签名服务策略》执行。

6.3.11 密码模块的评估

SHECA 使用国家密码主管部门批准和许可的密码产品。根据 SHECA 对产品性能、工作效率、供应厂商的资质等方面的评估，SHECA 可发布所支持的密码产品清单。

6.4 密钥对管理的其他方面

6.4.1 公钥归档

SHECA 在密钥对应的证书过期 5 年后对公钥进行归档。归档保留的时间为长期。

归档文件的保护、备份和检验要求参照本文件 5.5 的相关规定。

6.4.2 证书操作期和密钥对使用期限

公钥和私钥的使用期限与证书的有效期相关，但却并不完全保持一致。

1、对于用于签名的证书，其私钥只能在证书有效期内才可以用于数字签名，私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限以外。

2、对于用于加密的证书，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。

另外需注意的是无论是订户证书还是 CA 证书，在证书过期后且在密钥对最长使用年限内，允许使用原密钥对对证书进行更新。对于密钥使用期限无特殊规定的证书，CA 根据内部管理需要，为订户证书的密钥对设置适合的、安全的最大期限，在这个期限后,该密钥不能再使用。对于不同类型的证书，其密钥对最长使用期限及证书最长有效期如下：

证书类型	密钥对最长使用期限	证书最长有效期
CA 证书（2018 年之前签发）	30 年	30 年
CA 证书（2018 年之后签发）	25 年	25 年
中级 CA 证书	25 年	25 年
订户证书	6 年	3 年

6.5 激活数据

6.5.1 激活数据的产生和安装

1、SHECA 私钥的激活数据

CA 私钥激活数据的生成和安装由 CA 系统所使用的密码设备的安全机制进行保障，SHECA 采用 5 人控制，必须同时 5 人共同参与才能生成私钥，且需要至少 3 个或 3 个以上的密钥管理员来共同完成密钥激活。

2、订户私钥的激活数据

订户自行保管密钥载体的，私钥激活数据的生成和安装由所使用的密钥载体的安全机制进行控制。

订户使用认证机构管理的密钥载体生成并保管签名密钥，并由订户唯一控制签名私钥的，签名人在本服务的客户端签名交互组件中完成身份验证后方可生成激活数据，激活数据将以安全的方式传输给 SHECA，具体按照《云执钥®远程可靠电子签名服务策略》执行。

3、口令

SHECA 产生的口令，包括用于下载证书的口令、USB Key、IC 卡的登陆口令等，都是在安全可靠的环境下随机产生。这些口令，都通过安全可靠的方式，例如线下当面递交、邮政专递、短信等方式交给订户。对于非一次性使用的口令，SHECA 建议用户自行进行修改。

所有的保护口令都应该是不容易被猜到的，应该遵循以下几个原则：

- 至少 8 位字符
- 至少包含一个字符和一个数字
- 至少包含一个小写字母
- 不能包含很多相同的字符
- 不能和操作员的名字相同
- 不能使用生日、电话等数字
- 用户名信息中的较长的子字符串

6.5.2 激活数据的保护

SHECA 的 私钥的激活数据，由所使用的密码设备的安全机制进行保护，并交由 5 名密钥管理员分管。

订户的私钥激活数据由订户自行妥善保管。如果订户使用口令或 PIN 码保护私钥，订户应妥善保管好其口令或 PIN 码并定期修改，防止泄露或窃取。如果订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法获取。

6.5.3 激活数据的其他方面

私钥激活数据应通过安全信道/通道进行传输，以避免丢失、偷窃、修改、非授权泄露、或非授权使用。

SHECA 的私钥激活数据在不需要时应该销毁，并保护它们在此过程中免于丢失、偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部，比如记录有口令的在纸页必须粉碎。

订户私钥激活数据的重置：在所使用的密钥载体支持的前提下，SHECA 提供私钥激活数据重置的功能，在重置私钥激活数据前，SHECA 应对订户的身份进行鉴别，身份鉴别的方法和流程按本文件 3.2 执行。

6.6 计算机安全控制

6.6.1 特别的计算机安全技术要求

SHECA 认证系统的信息安全管理，按照国家密码管理局公布的《证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子认证服务管理办法》，参照 ISO17799 信息安全标准规范以及其它相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。

主要的安全技术和控制措施包括：

- 身份识别和验证管理
- 资源和信息存取权限控制
- 安全审计和日志
- 资料备份和保存的安全保护
- 人员职责分权，对 CA 工作角色进行分类，建立安全分散和牵制机制
- 内部操作程序控制
- 灾难备份恢复机制
- 个人计算机安全管理等
- 信息传递加密机制

通过严格的安全控制手段，确保 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。此外，SHECA 只允许有工作需求的必要人员访问证书服务器，只为必要人员设立证书服务器账户。核心系统与其它系统物理分离，生产系统与其他系统逻辑隔离。

6.6.2 计算机安全评估

SHECA 的认证业务系统，通过了国家密码管理局、中国国家信息安全测评中心、上海市信息安全测评中心等部门的有关评估、审查和认证。

6.6.3 计算机安全控制

SHECA 建立并实施了符合 GB/T25056-2018 中 8.2 要求的计算机安全控制体系，包括但不限以下措施：

- 每季度检查一次系统升级补丁，记录系统升级审批及实施过程
- 对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划
- 所有服务器和操作终端均安装杀毒软件
- 病毒库更新间隔不超过 7 天
- 病毒扫描间隔不超过 7 天

6.7 生存周期安全控制

SHECA 已建立符合 GB/T25056-2018 中第 10、11、12 章要求的生存周期安全控制体系。

6.7.1 系统开发控制

SHECA 的开发控制包括可信人员管理、开发环境安全管理、产品设计和开发评估、使用可靠的开发工具等，设计的生产系统满足冗余性、容错性、模块化的要求。软件设计和开发过程遵循以下原则：

- 第三方验证和审查
- 安全风险分析和可靠性设计

同时，SHECA 制订的软件开发规范，参考国家相关标准，在实施中严格执行相关的规划和开发控制。

6.7.2 安全管理控制

SHECA 认证业务系统的信息安全管理，严格遵循工业和信息化部、国家密码管理局等主管部门的有关运行管理规范和 SHECA 的安全管理策略进行操作。

SHECA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行使用，任何修改和升级会记录在案并进行版本控制、功能测试和记录。SHECA 还对认证系统进行定期和不定期的检查和测试。

SHECA 采用严格的管理体系来控制和监视系统的配置，以防止未授权的修改。

硬件设备从采购到上线前，会进行安全性的检查，用来识别设备是否被入侵，是否存在安全漏洞等。加密设备的采购和安装，在更加严格的安全控制机制下，进行检验、安装和验收。

SHECA 认证系统所有的软硬件设备升级以后，废旧设备在进行处理时，必须确认其是否有影响认证业务安全性的信息存在。

6.8 网络安全控制

SHECA 认证系统采用多级防火墙和网络控制系统的保护，并且实施完善的访问控制技术。

SHECA 建立并维护认证系统网络拓扑图，覆盖所有网络设备、链接关系和安全边界，定期更新，以确保与机房实际情况保持一致。

为了确保网络安全，SHECA 认证系统安装部署了防火墙、入侵检测、安全审计、病毒防范系统、内容过滤，并且及时更新防火墙、入侵监测、安全审计、病毒防范系统的版本，以尽可能的降低来自网络的风险。

认证系统只开放与申请证书、查询证书等相关的操作功能，供用户通过网络进行操作。

SHECA 的所有 CA 和 RA 系统必须依据 GB/T25056-2018 中 5.3.8 要求的网络安全控制体系网络与证书系统安全要求进行防护。具体安全控制措施包括但不限于：

- 部署硬件防火墙进行网络边界保护
- 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

- 建立针对证书注册子系统和数据库的访问白名单机制
- 持续监控系统运行状况与安全事件，定期对系统日志进行分析，分析内容包括但不限于系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件
- 每月执行漏洞扫描，并及时应用安全补丁
- 通过正式流程管理逻辑访问权限
- 实施多因素身份验证机制
- 审查和监控访问权限配置
- 定期对担任受信任角色的人员开展安全培训
- 渗透测试至少每年开展一次

6.9 时间戳服务

6.9.1 使用范围

时间戳服务是 SHECA 提供的增值服务，主要用于代码签名、PDF 签名等用途，具体根据客户的选择提供。

6.9.2 使用方式

时间戳请求者需向 SHECA 发送请求，收到响应后必须验证状态无误，并确认时间戳令牌的字段和数字签名有效性。验证内容包括数据是否一致、证书标识符、数据印记及哈希算法 OID 是否正确，还需对照本地可信时间源验证响应及时性。如无法验证，应立即通知 SHECA 。

时间戳验证者也需验证数字签名，并确认数据与令牌中的哈希值一致。

6.9.3 保障机制

SHECA 使用网络时间协议（NTP）每至多八小时同步一次系统时间（默认设置），时间来源为协调世界时（UTC），并在闰秒时根据权威通知更新。SHECA 维护一个与蜂窝网络同步的内部 NTP 服务器，确保时间精度在一秒以内。所有

时间戳均与 UTC 保持同步，精度符合时间戳令牌（如有定义）的要求，SHECA 不会使用不准确的时钟签发时间戳。

6.9.4 技术标准

SHECA 提供的时间戳服务，符合 GB/T 20520 《网络安全技术 公钥基础设施 时间戳规范》标准。

7. 证书、证书撤销列表和在线证书状态协议

7.1 证书

SHECA 使用的证书详细格式，符合 GM/T 0015-2023、GB/T 20518-2018 等国家相关标准的要求，并遵循 ITU-T X.509 V3（1997）：信息技术一开放系统互连－目录：认证框架（1997 年 6 月）标准和 RFC 5280:Internet X.509 公钥基础设施证书和 CRL 结构（2008 年 5 月）。 如有冲突，优先适用国家相关标准要求。

7.1.1 版本号

SHECA 签发的证书，符合 X.509 V3 证书格式，这一版本信息存放在证书版本属性栏内。

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。SHECA 除了使用 RFC5280 中定义的证书扩展项，还支持 SHECA 规定的自定义扩展项。

1、证书扩展项

- 密钥用途

电子签名，防抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证 CRL 签名，只加密，只解密。

SHECA 签发的订户的电子签名认证证书的密钥用途为：电子签名，防抵赖。

- 证书策略

SHECA 签发的证书策略,符合 X.509 证书格式，这一策略信息存放在证书策略属性栏内。

- 基本限制

用于鉴别证书持有者身份，如最终用户等。

- 扩展密钥用途

其它类型证书的扩展密钥用途遵守 RFC5280，按需进行设置。

- CRL 发布点

CRL 分发点扩展项包含可以获取 CRL 的 URL，用于验证证书状态。

- 序列号

SHECA 签发的证书采用随机序列号。

2、自定义扩展项

- 个人证件号 SM3 摘要 OID: 1.2.156.112570.30.1.4.1
- 个人证件号脱敏形式 OID: 1.2.156.112570.30.1.4.3
- 统一信用代码 OID: 1.2.156.10260.4.4

7.1.3 算法对象标识符

符合国家密码管理部门批准的算法对象标识符。

7.1.4 名称形式

SHECA 签发的证书，其名称形式的格式和内容符合 X.500 的甄别名格式。

7.1.5 名称限制

SHECA 签发的证书，其识别名称不允许为匿名或者伪名，必须是有确定含义的识别名称。在某些具有特殊要求的电子政务应用中， SHECA 可以按照一定的规则为用户指定特殊的名称，并且能够把该类特殊的名称与一个确定的实体（个人、组织或者设备）唯一的联系起来。任何这一类特殊的命名，都必须经过

SHECA 安全认证委员会的批准。

7.1.6 证书策略对象标识符

对象标识符（OID）是标识对象或策略的唯一编号。证书中视情况包含对应的 OID，包括 CA/浏览器论坛要求的相关 OID。

SHECA 按照 X.509 标准签发的证书，其证书策略对象标识符，存放在证书内证书策略的相关栏目。

SHECA 披露所使用的电子签名认证证书中包含的 OID。具体请参考本文件 1.2。

7.1.7 策略限制扩展项的用法

无规定。

7.1.8 策略限定符的语法和语义

无规定。

7.1.9 关键证书策略扩展项的处理规则

无规定。

7.2 证书撤销列表

SHECA 定期签发 CRL，供用户查询使用。

用户可以通过证书中签发的 CRL 扩展项标明的 URL 下载 CRL。

SHECA 认证系统签发的 CRL 符合 GB/T 20518-2018 中 5.3 条的要求。

7.3 在线证书状态协议

SHECA 为用户提供 OCSP（在线证书状态查询服务）。OCSP 作为 CRL 的有效补充，方便证书用户及时查询证书状态信息。

SHECA 的 OCSP 符合 GB/T 19713-2025 中的要求。

8. 认证机构审计和相关评估

SHECA 作为 UNTSH 的运营主体，建立完备审计评估管理制度，包括认证业务审计和全面符合性评估，通过内部常态化审计和第三方外部审计结合模式，保障电子认证服务全流程安全、合规、可控。

8.1 审计评估制度

SHECA 已建立审计评估管理制度，制度覆盖审计类型、实施频次、人员资质、评估方法等核心内容：

1、审计评估类型

认证业务审计，聚焦证书全生命周期业务操作合规核查；

全面符合性评估，围绕机构年度整体认证服务合规、资质合规、策略合规开展全维度评审。

2、审计评估触发频次与启动条件

认证业务审计执行周期遵照本文件 8.2 条款约定常态化落地；全面符合性评估每年至少开展 1 次；

发生重大密钥泄露事故、重大合规投诉等事件时，触发临时专项审计评估。

主管部门依据法规发起的现场核查、专项巡检，按监管要求即时启动对应评估。

3、审计评估人员资质要求

内部审计人员：由战略发展部统筹配置，须具备 PKI、CA 认证、信息安全审计专业知识，拥有 2 年以上行业实操经验，熟练掌握本 CPS 及国内电子认证相关法规标准，通晓机房物理安全、网络安全、密钥管控等全维度安全管理知识；内部人员需保持岗位独立性，与被审计业务、被评估部门无利益关联。

外部审计机构及人员：选用具备合法经营资质、行业良好从业口碑的独立会计师 / 信息安全审计事务所；外部团队精通 PKI 技术、国密及电子认证国家标

准、信息安全防护体系，配备系统安全检测专用工具与技术能力，外部机构与 SHECA 无股权、业务、财务等利害关系，保障审计机构独立性。

监管主管部门委派评估人员：人员资质由主管单位按法规自主核定，SHECA 积极配合。

4、审计评估主题与实施方法

主题：覆盖证书全生命周期业务、机构许可资质存续、CPS 落地执行、物理环境安全、人员安全管控、软硬件与运维安全、灾备与归档管理、风险管控落地等全维度事项；

方法：分为全量全面审计、抽样审计两类，抽样审计严格执行本 CPS 约定抽样比例，不同审计类型差异化选用审计方式。

8.2 认证业务审计

1、审计周期

内部常规认证业务审计按季度开展；监管发起临时核查时按需追加专项审计。

2、审计核查内容

围绕证书全生命周期业务合规性核验，包含：证书申请、续期、密钥变更、证书更新、撤销、冻结全环节中用户告知履约、申请人身份鉴别、用户意愿留存、业务协议签署、业务档案资料归档保存的合规性。

3、审计实施方式

采用全面审计、抽样审计双模式：单笔批量异常业务、重大投诉关联业务执行全量全面审计；常规存量证书业务采用抽样审计，抽样数量不低于每季度发证量的 1%，或 200 张证书。

4、问题整改闭环

SHECA 完成内部评估后，评估人员需要列出所有问题项目的详细清单，由评估人员和被评估对象共同讨论有关问题，并将结果书面通知 SHECA 安全认证委员会和被评估者，进行后续处理。

工业和信息化部评估完成后，SHECA 根据评估的结果检查缺失和不足，根据其提出的整改要求，提交修改和预防措施以及整改计划书，并接受其对整改计划的审查，以及对整改情况的再次评估。

第三方审计师事务所评估完成后，SHECA 按照其工作报告进行整改。

被评估对象必须根据评估的结果检查缺失和不足，提交修改和预防措施以及整改计划书，并接受评估者对整改计划的审查，以及对整改情况的再次评估。

如果 SHECA 确认审计中发现的意外或不作为对证书体系的安全性、一致性或完整性会造成立即威胁，则 SHECA 必须在 30 天内制定改正行动计划，并在合理的期限内执行。

8.3 全面符合性评估

1、评估周期

每年至少进行 1 次正式全面符合性评估，评估周期应连续不间断。

2、评估核查内容

全年度电子认证服务实际落地开展情况，业务体量、服务范围与许可备案内容一致性；

《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务许可证》等法定许可条件持续符合性核查，人员、场地、系统、安全能力持续满足持证要求；

现行 CPS 及配套认证规则的落地符合性，制度条款与实际业务执行一致性；

配套延伸核查：物理环境安全、人员权限管控、系统运维、灾备备份、档案归档、授权合作机构全链条合规、年度风险评估落地成效。

3、抽样管控要求

评估采用抽样模式时，抽样比例不低于本文件 8.2 条业务认证审计的抽样标准，保障样本覆盖面满足合规核查要求。

4、整改跟踪管理

评估形成问题台账，书面送达被审计责任部门，明确整改期限与整改要求；评估小组逐项跟踪整改落地、复核验收整改成效，整改闭环资料纳入审计档案永久留存。其他要求参照本文件 8.2 条第四段执行。

5、年度报告报送

在 1 月 31 日之前将上一自然年度全面符合性评估正式报告按法规要求报送行业主管部门。

9. 法律责任和其他业务条款

9.1 收费项目

SHECA 根据服务成本核算，制定价格策略。SHECA 通过以下任意一种或多种方式公布收费标准：

- SHECA 官网 https://www.sheca.com
- 证书服务页面
- 合同、订单或订户协议
- 其他

收费项目和收费标准可能包括:

- 证书颁发或更新费用

  通过上述方式公布。

- 证书访问费用

  目前 SHECA 不收取任何费用。除非用户提出的特殊需求，SHECA 将与用户协商收取应该收取的费用。

- 撤销证书的费用

  目前 SHECA 不收取任何费用。除非用户提出的特殊需求，SHECA 将与用户协商收取应该收取的费用。

- 状态信息访问费用

目前 SHECA 不收取任何费用。除非用户提出的特殊需求，SHECA 将与用户协商收取应该收取的费用。

- 电子签名的费用

通常统一包含在证书基础费用内，不另行单独收取；若双方约定按次单独收取签名服务费，需在合同、订单或订户协议中单独明确约定。

- 签名验证的费用

签名验证相关费用一般包含在证书基础费用中，不另行单独收取，SHECA 保留单独收取该项服务费用的权利。

- 其他服务的费用

用户申领 CPS 、签名验证报告或其他纸质业务文件的，SHECA 将收取工本费、邮递服务费等费用。

若 SHECA 向订户收取费用，订户有义务向 SHECA 支付费用，若订户未按要求及时支付费用，SHECA 有权拒绝提供服务。如果 SHECA 证书服务页面展示的或协议中约定的价格和 SHECA 公布的价格不一致，以页面展示或协议约定的价格为准。

SHECA 具有维持其运作和履行其责任的经济能力，有能力承担对订户、依赖方等造成的风险。

退款策略

SHECA 对订户收取的费用，除了证书申请和更新费用因为特定理由可以退还外，SHECA 均不退还用户任何费用。

在实施证书操作和签发证书的过程中，SHECA 遵守严格的操作程序和策略。如果 SHECA 违背了本 CPS 所规定的责任或其它重大义务，订户可以要求 SHECA 撤销证书并退款。在 SHECA 撤销了订户的证书后，SHECA 将立即把订户为申请该证书所支付的费用全额退还给订户。订户需要填写退款申请表，并递交给 SHECA，以要求退款。

此退款策略不限制订户得到其它的赔偿。

完成退款后，订户如果继续使用该证书，SHECA 将追究其法律责任。

9.2 财务责任

9.2.1 保险范围

SHECA 根据业务发展情况决定其投保策略。

目前，SHECA 对其在本 CPS 下的履约和义务所产生的责任进行自我保险。SHECA 承诺自我保险的资金保障额度不低于上一年度电子认证业务营业收入的 1.5%。SHECA 建立赔付备用资金，资金保障额度不低于上一年度电子认证业务营业收入的 1.5%。该资金专项用于因 SHECA 原因导致的赔付，由公司财务部管理，并接受年度审计。

9.2.2 其他资产

SHECA 确保具有足够的财务实力来维持其正常经营并保证相应义务的履行并合理地承担对订户及对依赖方的责任。

9.2.3 对最终实体的保险或担保

如果 SHECA 根据司法判定须承担赔偿和/或补偿责任的，SHECA 将按照相关仲裁机构的裁定或法院的判决承担相应的赔偿责任。

9.3 业务信息保密

9.3.1 保密信息范围

1、保密信息包括 SHECA、SHECA 与订户、SHECA 与其他证书服务相关方、SHECA 关联实体之间的协议、往来函和商务协定等。除非法律明确规定和 SHECA 明确进行了书面许可，一般不能在未经另一方许可的情况下擅自公开。

2、与证书持有者证书公钥配对的私钥是机密的，证书订户应该遵照本 CPS 的规定妥善保管，不能公布给未经授权的任意第三方。如果因证书订户泄露私钥，

订户应自行承担一切责任。

3、对 SHECA 或 SHECA 对关联实体的审计报告、审计结果等相关信息是机密信息，除了 SHECA 授权和信任的员工，不能泄露给其他任何人。这些信息除了审查目的或法律规定的目的，不能用于其他用途。

4、有关 SHECA 认证系统的运营信息只能在严格指定的情况下，才能提供给经 SHECA 授权的员工，这种授权并不意味着对信息公开的授权。对 SHECA 来讲，所有涉及系统运营的信息，都在保密范围之内。

5、除非法律明文规定，SHECA 没有义务，也不会公布或透露订户证书中已经包括的信息以外的任何信息。

9.3.2 不属于保密的信息

1、与证书有关的申请流程、申请需要的手续、申请操作指南等信息是可以公开的。而且 SHECA 在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

2、非保密信息还包括证书中包括的相关订户信息。证书中的订户信息是可以公开的。

3、证书、证书内包括的公钥，供用户公开、自由查询和验证。

4、证书被撤销的信息，属于公开信息，SHECA 在目录服务器中公布这些信息。

5、这些非保密信息，并不能够被任意不被授权的第三方使用，SHECA 和信息的所有人保留所有这些信息的相关权利。

9.3.3 保护保密信息的责任

SHECA、任何订户、关联实体以及与认证业务相关的参与方等，都有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

当 SHECA 在任何法律法规要求或者法院以及其它公权力部门通过合法程序的要求下，必须披露本 CPS 中规定的保密信息时，SHECA 可以按照法律、法规、或法规条令以及法院判决的要求，向执法部门公布相关的保密信息。SHECA 无

须承担任何责任。这种披露不能被视为违反了保密要求和义务。

当保密信息的所有者出于某种原因，要求 SHECA 公开或披露他所拥有的保密信息时，SHECA 满足其要求；同时，SHECA 将要求该保密信息的所有者对这种申请进行书面授权，以表示其自身的公开或者披露的意愿。

如果这种披露保密信息的行为涉及任何其他方的赔偿义务，SHECA 不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息引起的所有赔偿责任。

9.4 个人隐私保护

9.4.1 隐私保护原则

SHECA 尊重所有用户及其隐私，SHECA 将严格按照《中华人民共和国个人信息保护法》的要求，参照 GB/T 35273-2020《信息安全技术 个人信息安全规范》制定措施，履行隐私保护职责，具体以订户签署的协议约定为准。SHECA 的个人信息保护政策详见公司官网 www.sheca.com.

任何人选择使用 SHECA 的任何服务，那么就表示已经同意接受 SHECA 有关隐私保护的声明。

9.4.2 作为隐私处理的信息

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

9.4.3 不被视为隐私的信息

证书订户持有的证书内包括的信息，以及该证书的状态信息等，是可以公开的，将不被视为隐私信息。

9.4.4 保护隐私的责任

SHECA、任何订户、关联实体以及与认证业务相关的参与方等，都有义务按

照本 CPS 的规定，承担相应的保护隐私信息的责任。

当 SHECA 在任何法律法规或者法院以及公权力部门通过合法程序的要求下，或者信息所有者书面授权的情况下，SHECA 可以向特定对象公布相关的隐私信息。SHECA 无须为此承担任何责任，而且这种披露不能被视为违反了隐私保护义务。如果这种隐私披露导致了任何损失，SHECA 对此不应承担任何责任。

9.4.5 个人信息收集规则

SHECA 严格遵循合法、正当、必要原则管控个人信息采集范围：

a）最小必要采集：仅收集完成证书签发、身份核验、证书运维、合规存证必需信息，无业务关联信息一律不采集：

b）明示告知与单独授权：证书申请页面、纸质申请表等中完整公示个人信息保护政策，清晰载明收集目的、方式、范围等，并获取用户同意；

c）授权委托办理管控：受托人代办证书时，核验受托人授权委托书，同步采集受托人身份信息，明确告知委托代办信息处理规则，留存授权凭证归档；

d）禁止超范围采集：不采集与证书认证无关的隐私信息（户籍、婚姻、资产、医疗记录等），不强制收集非必要辅助材料。

9.4.6 个人信息存储与安全防护

a）存储期限管控：严格按照本 CPS 规定的留存期限保存，留存期限届满后启动不可逆安全销毁流程，纸质材料粉碎、电子数据全盘脱敏删除、备份介质物理销毁，留存销毁台账备查。

b）分级加密存储：普通个人信息（如手机号、邮箱等），传输、存储全程加密存储；敏感个人信息（如身份证号、人脸影像、证件扫描件等），采用国密算法加密存储，独立隔离数据库，禁止明文导出、展示。

c）访问权限与审计：实行最小权限访问机制，仅业务审核、合规审计岗位开放对应数据权限；全流程记录操作日志（如操作人员、时间、访问内容、操作行为等），日志留存不低于存储有效期；定期开展权限清理与访问审计。

d）介质与备份安全：离线数据库备份硬盘全程加密存储，备份介质专人管

控、分区隔离存放，每月至少一次校验备份完整性与加密有效性，防止备份数据泄露、篡改或丢失。

9.4.7 使用隐私信息的告知与同意

SHECA 在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理、和服务订户的目的。在使用这些信息时，无论是否涉及到隐私，SHECA 都没有告知订户的义务，也无需得到订户的同意。

SHECA 在任何法律法规或者法院以及公权力部门通过合法程序的要求下，或者信息所有者书面授权的情况下向特定对象披露隐私信息时，也没有告知订户的义务，并且不需得到订户的同意。

SHECA 如果需要将客户隐私信息用于双方约定的用途以外的目的，事前必须告知订户并获得订户同意和授权，而且这种同意和授权是要用可归档的方式（如传真、信函、电子邮件等）。

9.4.8 依法律或行政程序的信息披露

除非符合下列条件之一，否则 SHECA 不会将订户的保密信息和隐私信息提供给任何对象：

- 个人信息保护法或者其他法规规定的可以对外提供的情形
- 政府法律法规的规定并且经相关部门通过合法程序提出申请
- 法院以及公权力部门处理因使用证书产生的纠纷时合法的提出申请
- 具有合法司法管辖权的仲裁机构的正式申请
- 证书订户以书面方式进行授权

9.4.9 其他信息披露情形

证书订户以书面方式进行授权，要求 SHECA 向特定对象提供隐私信息时，SHECA 可以将信息提供给该订户指定的接受对象；非经订户本人的书面授权，SHECA 将拒绝任何第三者的披露请求。

除了政府法规和相关部门的合法请求，以及信息所有人的书面授权，或者

SHECA 的合法用途以外，SHECA 目前不存在任何其他的隐私信息披露情形。

9.5 知识产权

1、SHECA 自身拥有知识产权的声明

SHECA 享有并保留对证书以及 SHECA 提供的全部软件、系统的一切知识产权，包括所有权、名称权和利益分享权等。SHECA 自行决定 SHECA 关联实体采用的证书服务软件系统，以便保证系统的兼容和互通。

按本 CPS 的规定，所有 SHECA 发行的证书和 SHECA 提供的软件、系统、文档中，使用、体现和涉及到的一切版权、商标和其他知识产权均属于 SHECA，这些知识产权包括所有相关的文件、CPS、规范文档和使用手册等。SHECA 认证体系内关联实体在征得 SHECA 的同意后，可以使用相关的文件和手册，并有责任和义务提出修改意见。

订户自己产生的密钥的知识产权归其所有，但是公钥经过 SHECA 签发成证书后，SHECA 即拥有该证书的知识产权，只提供给证书订户和依赖方使用的权力。

在没有 SHECA 书面同意的情况下，使用者不能在任何证书到期、撤销的期间或之后，使用或接受任何 SHECA 使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

2、SHECA 使用其他方知识产权的声明

SHECA 在认证业务系统中使用的软硬件设备、辅助设施和相关操作手册，其知识产权为相关供应商所有，SHECA 保证都是合法的拥有相应权利，绝对没有故意侵害第三方的权利。

SHECA 尊重在证书中 DN 项内存放的订户的注册商标，但是并不保证该注册商标的所有权归属。证书订户的注册商标如果在证书注册时已经被前面的申请者占用，由此产生的注册商标和知识产权的纠纷处理并不在 SHECA 的责任范围内。

9.6 陈述与担保

除非 SHECA 在协议中作出特别约定，如果本 CPS 的规定与其他 SHECA 制订的相关规定、指导方针相互抵触，用户必须接受本 CPS 的约束。在 SHECA 与包括订户在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本 CPS 的规定执行；对协议中不同于本 CPS 的约定，按双方协议中约定的内容执行。

9.6.1 电子认证服务机构的陈述与担保

1、SHECA 的一般陈述

- 建立电子认证业务规则（CPS）和其他认证服务所必需的规范、制度体系
- 在本 CPS 相关条款规定的范围内，提供基础设施和认证服务，遵守本 CPS 的各项规定
- SHECA 保证其私钥得到安全的存放和保护，SHECA 建立和执行的安全机制符合国家相关政策的规定
- 所有和认证业务相关的活动都符合法律法规和主管部门的规定
- SHECA 和证书订户的关系以及 SHECA 和依赖方的关系并不是代理人和委托者的关系。证书订户和依赖方都没有权利以合同形式或其他方法让 SHECA 承担信托责任。SHECA 也不能用明示、暗示或其它方式，作出与上述规定相反的陈述

2、SHECA 对订户的陈述

除非本 CPS 中另有规定或者 SHECA 和订户间另有协议，SHECA 向在证书中所命名的订户承诺：

- 在证书中没有 SHECA 所知的或源自于 SHECA 的错误陈述
- 在生成证书时，不会因 SHECA 的失误而导致数据转换错误，即不会因 SHECA 的失误而使证书中的信息与 SHECA 所收到的信息不一致

- SHECA 签发给订户的证书符合本 CPS 的所有实质性要求
- SHECA 将按本 CPS 的规定，及时撤销证书
- SHECA 将向订户通报任何已知的，将在根本上影响证书的有效性和可靠性的事件

上述陈述仅仅是为保证订户的利益，而不是用于使任何其他方受益或被其他方强迫执行。SHECA 的行为若符合相关法律和本 CPS 的规定，即被视为 SHECA 作出了符合上述描述的合理的努力。

3、SHECA 对依赖方的陈述

SHECA 就其所发证书向所有按照本 CPS 合理地信赖签名（该签名可通过证书中所含的公钥验证）的人承诺：

- 除了未经验证的订户信息外，证书中的或证书中合并参考到的所有信息都是准确的
- SHECA 完全遵照本 CPS 的规定签发证书

4、SHECA 有关公开发布的陈述

通过公开发布证书，SHECA 向 SHECA 信息库和所有合理依赖证书中信息的依赖方证明：SHECA 已向订户签发了证书，并且订户已经按照本 CPS 中的规定接受了该证书。

9.6.2 订户的陈述与担保

一旦接受 SHECA 签发的证书，从接受之时起直至证书的整个使用有效期内，如果订户不另行通知，那么订户被视为向 SHECA 及所有合理信赖证书中所含信息的人作出如下保证：

- 在证书申请表上填列的所有声明和信息必须是完整、精确、真实和正确的，可供 SHECA 检查和核实；并且，愿意承担任何提供虚假、伪造等信息的法律责任
- 如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知 SHECA

- 用与证书中所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效证书并已被订户接受（证书没有过期、撤销）
- 未经授权的人员从未访问过订户私钥
- 订户向 SHECA 陈述的所有包含在证书中的有关信息是真实的。如果订户发现了证书中信息存在某些错误 ，但订户还没有及时通知给 SHECA，那么，SHECA 视为：订户承诺上述信息都是真实的
- 订户将按本 CPS 的规定，只将证书用于经过授权的或其它合法的使用目的
- 除非经订户和 SHECA 间的书面协议明确规定，订户保证不从事 SHECA（或类似机构）所从事的业务，例如：把与证书中所含的公钥所对应的私钥用于签发任何证书（或认证其他任何形式的公钥）或证书撤销列表
- 一经接受证书，既表示订户知悉和接受本 CPS 中的所有条款和条件，并知悉和接受相应的订户协议
- 一经接受证书，订户就应承当如下责任：始终保持对其私钥的控制，使用可信的系统，和采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用
- 一经接受证书，即表示订户同意使 SHECA 免于由下列原因直接或间接造成的任何责任和损失：订户（或其授权的代理人）虚假地或错误地陈述了事实；订户未能披露重要事实，而订户的这种有意或无意的错误陈述或失职造成了对 SHECA 和任何信任其证书的依赖方的欺骗；订户没有采用必要的合理措施防止其私钥被损害、丢失、泄露、被篡改或被未经授权使用。如果因此给 SHECA 造成任何责任、损失、任何诉讼及一切相关费用，订户将予以经济赔偿
- 不得拒绝任何来自 SHECA 的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等

9.6.3 依赖方的陈述与担保

依赖方在信赖任何 SHECA 签发的证书时，就意味着保证：

- 熟悉本 CPS 的条款，了解证书的使用目的
- 依赖方在信赖 SHECA 签发的证书前，已经对证书进行过合理的检查和审核，包括：检查 SHECA 公布的最新的 CRL，确认该证书没有被撤销；检查该证书信任路径中所有出现过的证书的可靠性；检查该证书的有效期；以及检查其它能够影响证书有效性的信息
- 一旦由于疏忽或者其他原因违背了合理检查的条款，依赖方愿意就因此而给 SHECA 带来的损失进行补偿，并且承担因此造成的自身或他人的损失
- 对证书的信赖行为就表明依赖方已经接受本 CPS 的所有规定，尤其是其中有关免责、拒绝和限制义务的条款
- 不得拒绝任何来自 SHECA 的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等

9.7 担保免责

SHECA 在下列情况下免于承担责任：

1、不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何赔偿责任。这些事件包括但不限于劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他大灾难等。

2、如果由于非 SHECA 的原因而造成的设备故障、线路中断，导致签发电子签名认证证书错误、延误、中断或者无法签发，SHECA 不负任何赔偿责任。

3、本 CPS 的内容，没有任何信息可以暗示或解释成，SHECA 承担其它的义务或 SHECA 对其行为作出其它的承诺。包括不承担其它任何形式的任何保证和义务，任何对特殊目的适用性的保证。

4、如果申请者故意或无意的提供不完整、不可靠或已过期的，包括但不限

于伪造、篡改、虚假的信息，而其又根据正常的流程提供了必须的审核文件，由此得到了 SHECA 签发的电子签名认证证书。由此引起的法律问题、经济纠纷应由申请人全部承担，SHECA 不承担与该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和举证帮助。

5、SHECA 不承担任何其他未经授权的人或组织以 SHECA 名义编撰、发表或散布不可信赖的信息所引起的法律责任。

6、对于由于证书、签名或根据本 CPS 而提供或设计的任何其他交易或服务的使用、签发、授权、执行或拒绝执行而导致的或与之有关的任何间接性的、特别性的、附带性的、或结果性的损失，或任何利益损失、数据丢失，或其他间接性的、结果性的或惩罚性的损失，无论是否可以合理预见， SHECA 将不会对此负责，即使 SHECA 曾经被警告过这种损害的可能性。

7、SHECA 对签发的各类证书的适用范围有明确的规定，若证书订户将其证书用于其他不被允许的用途，SHECA 不承担任何责任，无论这种使用是否造成损失。

8、SHECA 在法律许可的范围内，根据法律、政策等以及受害者的要求，如实提供电子政务、电子商务或其它网络作业中不可抵赖的电子签名依据，但并不对此承担法律或政策规定之外的责任。

9.8 赔偿责任限制

根据《中华人民共和国公司法》、《中华人民共和国电子签名法》和其他法律法规的规定，作为依法设立的有限责任公司，SHECA 在承担任何责任和义务时，只承担法律范围内的有限责任。

在本 CPS 和 SHECA 与任何一方签订的协议中，SHECA 不做任何其他保证和履行任何进一步的义务。

9.8.1 赔偿范围

财务赔偿范围涵盖 SHECA 在履行服务职责时可能面临的各种风险，包括但不限于：

a) 技术故障导致的证书签发错误或延误

b) 人为操作失误导致的信息错误

c) 安全漏洞导致的私钥泄露（非订户原因）

d) 其他经司法判定应由 SHECA 承担责任的情形

9.8.2 赔付计算方式

a) 每张证书的赔偿限额按 9.9.2 执行

b) 对于同一证书引发的多项索赔，合计赔偿不超过该证书对应的赔偿限额

c) 具体赔付金额由司法判决或仲裁裁决确定，或双方协商确定

9.8.3 赔付监督机制

a) SHECA 设立赔付监督小组，负责审核赔付申请的合规性

b) SHECA 每年对赔付情况进行内部审计（如发生赔偿事件）

9.9 赔偿

9.9.1 赔偿范围

在认证活动中产生的赔偿，都以本 CPS 的规定为处理依据，法律法规另有要求的除外。

1、SHECA 的赔偿责任

- 在签发证书时，如果未按照本 CPS 的规定进行处理，或者违反法律法规的要求而造成证书订户损失的，SHECA 承担赔偿责任
- 因为操作人员恶意、故意或者疏忽，未按照本 CPS 的规定办理证书的签发、撤销等请求，而造成证书订户损失的，SHECA 赔偿订户的损失
- 因 SHECA 的 CA 密钥出现问题，造成订户证书出现问题的，SHECA 赔偿相关的损失
- 证书订户或者其它有权提出撤销证书的人提出撤销请求后，到 SHECA

将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 SHECA 按照本 CPS 的规范进行了有关操作，SHECA 不承担任何损害赔偿责任

- 证书订户赔偿的追溯有效期限，按照有关法律法规的要求进行操作

2、订户的赔偿责任

- 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成 SHECA 或者第三方遭受损害的，订户应赔偿一切损害责任
- 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知 SHECA，以及不当交付他人使用造成 SHECA、第三方遭受损害的，订户应承担一切损害赔偿责任
- 订户使用证书或者依赖方信任证书的行为，有违反本 CPS 及相关操作规范，或者将证书用于非本 CPS 规定的业务范围的，订户或者依赖方应自行承担一切损害赔偿责任
- 用户使用或信赖证书时，未能依照本 CPS 等规范进行合理审核，导致 SHECA 或第三方遭受损害的，应由该用户承担一切损害赔偿责任
- 证书订户或者其它有权提出撤销证书的实体提出撤销请求后，到 SHECA 将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 SHECA 按照本 CPS 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任
- SHECA 与之签署的协议另有赔偿规定的，参照其规定

9.9.2 赔偿限额

SHECA 对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿责任，不可能超过如下所述对这些证书的封顶赔偿金额：

对于有关一张特定证书的所有签名和交易处理的总计，SHECA 对于任何人（或者其它实体）有关该特定证书的合计赔偿责任应该限制在一个不超出下述数额的范围内（单位：人民币元）：

分类	基础级证书	高等级证书
个人类证书	不超过 400 元	不超过 2，000 元
组织类证书	不超过 10，000 元	不超过 50，000 元

本条款限制适用于一定形式的损害，包括但不局限于任何人或实体（包括但不限于订户、证书申请者、接收方或信赖方）由于信任或使用 SHECA 签发、管理、使用或撤销的证书或已过期证书而导致的直接的、补偿性的、间接的、特别的、结果的、惩戒性的或意外的损害。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的赔偿均有限额而不考虑签名、交易处理或其它有关的索赔数量。当超过赔偿限额时，除非得到依法判决或仲裁，可用的赔偿限额将首先分配给最早得到索赔解决的一方。SHECA 没有责任为每张证书支付高出赔偿限额总和的赔偿，而不管高出赔偿限额总和在索赔提出者之间是如何分配的。

赔偿流程包括：申请、审核、审批、支付四个环节，原则每个环节不超过 15 个工作日，具体以实际赔偿案例为准，涉及鉴定、司法程序的，不记算在时效范围内。

9.10 有效期限与终止

9.10.1 有效期限

本 CPS 自发布之日起正式生效，文档中将详细注明版本号及发布日期，当新版本正式发布生效时，旧版本将自动失效。

由于必要的原因，SHECA 在获得国家主管部门的批准后，可以宣布提前终止 CPS 的有效期。

9.10.2 终止

本 CPS 将持续有效，直到有新的版本取代。

如果订户终止使用其证书，或者依赖方终止对证书的信任，订户证书已经被

撤销而没有重新申请证书，那么除了 CPS 中有关审计、归档、保密信息、隐私保护、知识产权、赔偿和有限责任的条款外，对于该订户或者依赖方来说，本 CPS 将不再对其有约束力。SHECA 与其另有协议规定的，按照协议中的规定执行。

9.10.3 效力的终止与保留

在 CPS 中涉及审计、保密信息、隐私保护、归档、知识产权的条款，以及涉及 SHECA 的赔偿及有限责任的条款，在本 CPS 终止以后仍然继续有效存在。

9.11 对参与者的个别通告与沟通

除非法律法规或者协议有特别的规定，SHECA 将以合理的方式与相关各方进行沟通，不会采取个别的方式进行。

无论何时任何人打算或要求发布任何本 CPS 中提及的服务、规范、操作等的通知、要求或请求，这些信息将用书面形式进行传达。

书面通信必须由提供书面单据的快递服务送达，或经由挂号邮件确认，须附回邮及回函。邮递地址如下：中华人民共和国上海市四川北路 1717 号嘉杰国际广场 18 楼（200080 ））

如果通过电子邮件方式发送通知给 SHECA，则这种通知只有在 SHECA 收到电子邮件通知后 24 小时内，收到书面确认材料，方为有效。

通过 SHECA 寄给其他人，地址如下:SHECA 邮递记录中的最新地址。

9.12 修订

SHECA 有权修订本 CPS。SHECA 有权把修订结果以 CPS 的修订版的形式通过网站 https://www.sheca.com 发布，或者放在 SHECA 信息库里。

9.12.1 修订程序

经 SHECA 安全认证委员会授权，战略发展部每年至少审查一次本 CPS，确保其符合国家法律法规和主管部门的要求，符合认证业务开展的实际需要。

本 CPS 的修订，由战略发展部提出修订报告后，必须经过 SHECA 策略最高

管理部门——SHECA 安全认证委员会审核并批准后才能开始修订。修订后的 CPS 正式对外发布后，应送交信息产业主管部门备案。

9.12.2 通知机制和期限

SHECA 有权在合适的时间修订和改变本 CPS 中任何术语、条件和条款，而且无须预先通知任何一方。

SHECA 在网站 https://www.sheca.com 和 SHECA 信息库中公布修订结果。如果关于本 CPS 的修改被放置在 SHECA 信息库中的规范更新和通知栏(查看 https://www.sheca.com)，它等同于修改本 CPS。这些修改将取代 CPS 原有版本中的任何冲突和指定条款。

修订同意期限：如果在修订发布 7 天内，证书申请者和订户没有决定请求撤销其证书，就被认为同意该修订，所有的修订和改变立刻生效。

9.12.3 必须修改 OID 的情形

无规定。

9.13 争议处理与举证

9.13.1 争议处理

争议受理范围：与本 CPS、证书服务相关的争议

处理流程：协商→调解→仲裁/诉讼

协商时限：收到争议通知后 15 个工作日内

调解规则：可申请 SHECA 安全认证委员会专家组调解或第三方调解机构介入

管辖法律与争议解决方式：适用中华人民共和国法律，可提交上海仲裁委员会仲裁或向上海市虹口区人民法院提起诉讼。

9.13.2 举证制度

SHECA 具备以下举证能力，能力覆盖证书全生存周期：

a) 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，保存期限至证书失效后五年

b) 签名环节：签名请求验证记录、签名操作日志、时间戳记录等

c) 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

d) 举证时限：收到合法有效的举证请求后，15 个工作日内提供相关举证材料，提供举证材料可能涉及成本，具体以公司收费内容为准

9.14 管辖法律

本 CPS 接受《中华人民共和国电子签名法》、《电子认证服务管理办法》以及其它中华人民共和国法律法规的管辖和解释。

无论合同或其他法律条款的选择及无论是否在中华人民共和国建立商业关系，本 CPS 的执行、解释、翻译和有效性均适用中华人民共和国的法律。法律的选择是确保对所有订户有统一的程序和解释，而不管他们在何地居住以及在何处使用证书。

9.15 与适用法律的符合性

所有电子认证活动的参与方，都必须遵守《中华人民共和国电子签名法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》《电子认证服务密码管理办法》以及其它中华人民共和国法律法规的规定。

9.16 一般条款

9.16.1 完整协议

本 CPS 直接影响 SHECA 权利、义务的条款和规定，除非通过受到影响的当

事人发出经过鉴定的信息或文件，或者在此另有其他规定，否则不能进行口头上的修正、放弃、补充、修改或终止。

在本 CPS 与其他规则、规范或协议发生冲突时，所有认证活动的参与方都将受本 CPS 规定的约束，但以下所示协议除外：

- 在本 CPS 的生效日期以前签定
- 该合同明确表示替代本 CPS 处理相关各方事务，或本 CPS 的规定被法律禁止执行

9.16.2 转让

CA、订户及信赖方之间的责任、义务不能通过任何形式转让给其他方。

9.16.3 分割性

本 CPS 的任何条款或其应用，如果因为任何原因或在任何范围内发现无效或不能执行，那么本 CPS 其余的部分仍将有效。相关当事人了解并同意，本 CPS 所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，均是可独立于其它条款的个别条款，并可加以执行。

9.16.4 强制执行

无规定。

9.16.5 不可抗力

在法律法规许可的范围内，依据相应 CP 制定的 CPS、订户协议等应该包括保护不可抗力条款，以保护各方利益。SHECA 将不对以下超越其控制能力的不可抗力事件，所造成本 CPS 规定的担保责任的违反、延误或无法履行负责：

构成不可抗力的事件包括战争、恐怖袭击、罢工、瘟疫、自然灾害、火灾、地震、供应商或卖方执行失败、互联网或其他基础设施的瘫痪和其它天灾等。

9.16.6 版本标注

在订户协议及电子签名依赖方协议中均标明对应本 CPS 的版本号。

9.17 其他条款

除非另外约定，以下与安全相关的信息资料和数据被认为是以下所指示的当事人的财产：

- 证书：证书是 SHECA 的财产。除非是那些没有 SHECA 明确的书面许可就不能公开在任何信息库或目录中的证书外，证书可完整非专属的、免费的复制和分发。关于版权声明的问题，可以向 SHECA 咨询
- CPS：本 CPS 是 SHECA 的私有财产
- 甄别名：甄别名归命名实体所有
- 私钥：私钥归订户私人所有(或他们代表的组织、机构或者任何其他实体)，而不管其存储和保护所使用的密钥载体
- 公钥：公钥归订户私人所有(或他们代表的组织、机构或者任何其他实体)，而不管其存储和保护所使用的密钥载体
- SHECA 的公钥:SHECA 所拥有的公钥是 SHECA 的财产，SHECA 允许使用这些公钥
- SHECA 的私钥:SHECA 的私钥是 SHECA 的私有财产，无论是部分还是整体