协卡网络信任服务体系
身份认证证书业务规则

UniTrust Network Trust Service Hierarchy

Identity Certificate Certification Practice Statement

(UniTrust NTSH ID-Cert 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

版本控制

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

变更摘要

版本	更新描述
V1.0	本文档为身份证书 CPS，适用范围包括个人身份证书、机构身份证书以及设备证书。

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文件规定了规定身份证书申请、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。

2、证书申请者须知：

（1）申请者在申请证书之前，已被建议接受适当的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。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。

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

1. 引言 8
1.1. 概述 8
1.2. 文档名称和标识 10
1.3. PKI 参与者 10
1.4. 证书用途 12
1.5. 策略管理 13
1.6. 定义和缩略语 14
2. 发布和存储库责任 19
3. 识别和认证 20
3.1. 命名 20
3.2. 初始身份验证 22
3.3. 密钥更新请求的识别和认证 25
3.4. 撤销请求的识别和认证 25
4. 证书生命周期操作要求 26
4.1. 证书申请 26
4.2. 证书申请处理 27
4.3. 证书签发 28
4.4. 证书接受 29
4.5. 密钥对和证书使用 30
4.6. 证书续期 30
4.7. 证书密钥更新 31
4.8. 证书变更 32
4.9. 证书撤销和冻结 32
4.10. 证书状态服务 36
4.11. 订阅终止 37
4.12. 密钥托管和恢复 38
5. 设施、管理和操作控制 38
5.1. 物理安全控制 38
5.2. 程序控制 40
5.3. 人员控制 41
5.4. 审计日志记录程序 43
5.5. 记录归档 44
5.6. 密钥更替 45
5.7. 泄露和灾难恢复 45
5.8. CA 或 RA 终止 45
6. 技术安全控制 46
6.1. 密钥对生成和安装 46
6.2. 私钥保护和密码模块工程控制 48
6.3. 密钥对管理的其他方面 50
6.4. 激活数据 50
6.5. 计算机安全控制 51
6.6. 生命周期安全控制 53

6.7. 网络安全控制 53
6.8. 时间戳 55
7. 证书、CRL 和 OCSP 配置文件 55
7.1. 证书配置文件 55
7.2. CRL 配置文件 57
7.3. OCSP 配置文件 57
8. 合规审计与其他评估 57
9. 其他业务与法律事项 58
9.1. 费用 59
9.2. 财务责任 60
9.3. 商业信息保密 61
9.4. 个人信息隐私 62
9.5. 知识产权 64
9.6. 陈述与保证 64
9.7. 免责声明 64
9.8. 责任限制 64
9.9. 赔偿 64
9.10. 期限与终止 65
9.11. 个人通知与参与者沟通 65
9.12. 修订 65
9.13. 争议解决程序 66
9.14. 管辖法律 66
9.15. 遵守适用法律 67
9.16. 杂项条款 67
9.17. 其他条款 67

1. 引言

1.1. 概述

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、信任的网络环境而努力。

SHECA 制定了本文档——《协卡网络信任服务体系 身份认证证书业务规则》（以下简称本 CPS），规定身份证书申请、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。

本 CPS 适用于 SHECA，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。

本 CPS 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
ROOTCA	2bb5b8c349b031919fc0c67967dfe7c2	国家根	SM3 With SM2	256	2012/07/14	2054/07/07	/
SHECA SM2	2da1a6bd0ce76c624e634b7d6a29d02a	ROOTCA	SM3 With SM2	256	2013/09/13	2033/09/08	2030/12/31

UCA ROOT G2	4452a0b2e90539467a53b04f236aa3c3	UCA Root G2	SHA256 With RSA	2048	2016/09/01	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 RSA Non-Public Root CA - G1	59129488c8b6dba021ac2c3e47a6e52b	UCA RSA Non-Public Root CA - G1	SHA256 With RSA	2048	2018/04/12	2043/04/11	2040/04/11
UCA RSA Non-Public CA - SHA256 - G1	61c5bfbf4e6438e0657511aad66374bc	UCA RSA Non-Public Root CA - G1	SHA256 With RSA	2048	2018/04/12	2033/04/11	2030/04/11
UCA SM2 Non-Public Root CA - G1	48acf2b838bf067de4108ecae9a5dfc7	UCA SM2 Non-Public Root CA - G1	SM3 With SM2	256	2018/04/12	2043/04/11	2040/04/11
UCA SM2 Non-Public CA - G1	66521c3abb2cc0257431daee9770c84e	UCA SM2 Non-Public Root CA - G1	SM3 With SM2	256	2018/04/12	2043/04/11	2040/04/11

本 CPS 证书产品及遵循策略 ID：

产品	策略 ID	应用
个人身份证书	1.2.156.112570.1.8.1.1	除电子签名认证证书以外的个人证书，用于身份鉴别、密钥协商、数据加解密等场景
机构身份证书	1.2.156.112570.1.8.1.2	除电子签名认证证书以外的机构证书，用于身份鉴别、密钥协商、数据加解密等场景
普通设备证书	1.2.156.112570.1.8.1.3	标识 IoT 设备、服务器、网关等设备身份的证书，用于身份鉴别、密钥协商、数据加解密等场景

注：本 CPS 定义的证书不包含公共可信设备证书（如 SSL 证书等）。

1.2. 文档名称和标识

文档名称：《协卡网络信任服务体系身份认证证书业务规则》；

版本：V1.0；

发布日期：【2026-10-31】；

CPS 文档 OID：1.2.156.112570.1.0.13；

遵循的证书策略 OID：见本 CPS 1.1 证书产品及策略 ID 表；

历史版本信息：见版本控制表；

获取方式：见本 CPS 1.5（官网信息库、邮件、书面索取）。

1.3. PKI 参与者

CA（认证机构，即 SHECA）

依法设立的第三方电子认证服务机构，建设运营协卡认证体系（UniTrust NTSH）。

责任：①独立生成密钥对、自主签发根 CA 证书；根 CA 只签发中级 CA 证书，中级 CA 签发最终用户证书；②根/中级 CA 密钥对的更新与切换，须按国家规定程序经 SHECA 安全认证委员会同意后实施；③保证 CA 签名私钥安全存放与保护、认证体系安全可靠运行；④通过目录服务器/CRL 公布证书的公开信息与状态；⑤与其他 CA 建立互联互通时，审查对方 CPS、证书业务文件、承诺及操作规程，仅按协议接受其鉴别过的信息；⑥向订户与依赖方保证证书信息准确、按本 CPS 签发。

RA（注册机构）

SHECA 授权委托的实体，负责对证书申请者进行身份标识与鉴别，初始化或拒绝证书申请和撤销请求，代表 CA 批准证书续期或密钥更新的申请。

责任：①按本 CPS 及授权协议建立并管理下属受理点（RAT）；②妥善保存客户数据，向 CA 提供审核资料，不向与证书申请无关的组织或个人透露、不用于商业用途；③接受 SHECA 的资质审核、规范执行检查与审计，对资格审核不严导致的损失承担责任；④遵循 SHECA 服务受理规范、系统运作规范和管理规范。

RAT（受理点）

SHECA 或 RA 授权的证书服务网点，负责办理和审批证书申请、撤销、查询等服务。

责任：①业务流程须与本 CPS 及授权协议书一致；②向 CA/RA 提供申请实体信息（名称、法定标识、证明文件、联系方式）；③对申请者信息真实性鉴别负责，审核不严导致的损失由 RAT 承担；④妥善保管申请者信息并接受监督审计。

订户

订户，即与电子认证服务机构签订协议，接受电子认证服务机构提供的服务的实体。订户应能对证书对应的私钥的使用负有法律责任。

责任：①保证申请信息完整、精确、真实；②妥善保管私钥及激活数据，发生私钥安全风险时及时通知 SHECA；③按本 CPS/CP 规定的用途使用证书与私钥；④接受证书即接受本 CPS 规定的权利与义务。

依赖方

依赖方，指基于对身份证书或者身份认证结果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。

责任：①信赖前合理审查证书（有效期、CRL/OCSP 状态、证书链）；②仅在 CPS 规定的范围内信赖证书及公钥；③对无法验证的签名，信赖风险自担。

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。

1.4. 证书用途

SHECA 根据本 CPS 颁发的证书用于数字身份认证、验证信息完整性与机密性。

在 SHECA 认证服务体系中，目前支持正式证书和测试证书。正式证书须通过规定身份鉴别；测试证书仅限测试，用户名须以 test/测试开头、有效期 3 个月。

类型与用途

个人身份证书——用于需要区分、标识、鉴别个人身份的场合，适用于个人身份认证、数字签名、数据加解密等场景；

机构身份证书——用于需要区分、标识、鉴别机构身份的场合,适用于机构身份认证、数字签名、数据加解密等场景；

普通设备证书——用于标识服务器等设备身份，实现个人或企业的设备身份认证、以及数据加解密和信息签名,以提供信息源发性证明、及实现信息保密和完整性保障。

注：本 CPS 定义的证书不包含公共可信设备证书（如 SSL 证书等）。

限制用途

各类证书严格遵照密钥用途和扩展密钥用途，不得混用。

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的应用场景或类型；

d)国家法律法规禁止的活动。

1.5. 策略管理

策略管理机构

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，负责 CPS/CP 及配套制度维护、修订批准。

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 身份认证服务体系内的运行符合本 CPS 的要求，负责起草修订与对外咨询。

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本 CPS，对于不符合处立即进行更新。

批准程序

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；

联系人

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

获取方式

通过官网知识库获取：https://www.sheca.com/repository；

通过电子邮件获取：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。

1.6. 定义和缩略语

下列术语定义适用于本 CPS。

术语	定义	来源
SHECA	上海市数字证书认证中心有限公司（Shanghai Electronic Certification	/

术语	定义	来源
	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（CA）	取得电子认证服务许可证，为需要第三方身份认证的主体，签发身份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。	
注册机构（RA）	具有下列一项或多项功能的实体：标识和鉴别证书申请者，同意或拒绝证书申请，在某些环境下主动吊销或挂起证书，处理订户吊销或挂起其证书的请求，同	GB/T 26855-2011，3.10

术语	定义	来源
	意或拒绝订户更新其证书或密钥的请求。	
受理点（RAT）	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。	/
公钥基础设施（PKI）	一套由硬件、软件、人员、策略和流程构成的，用于生成、管理、分发、使用、存储和撤销数字证书的，利用公钥技术提供安全服务的基础设施。	GB/T 31508-2015 第 3.19 条
数字证书	由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分个人 / 机构 / 设备证书，按用途可分签名 / 加密证书。	GB/T 25056-2018 第 3.9 条
订户协议	是指电子认证服务机构（CA）与证书申请者（即订户）之间签署的协议，规定了双方在颁发和管理证书的过程中所拥有的权利和义务。	GB/T 26855-2011 第 3.16 条
订户（Subscriber）	与电子认证服务机构签订协议，接受电子认证服务机构提供的服务的实体。订户应对证书对应的私钥的使用负有法律	GB/T 31508-2015,3.4

术语	定义	来源
	责任。	
申请者（Applicant）	向电子认证服务机构申请证书的自然人或法人。注：证书申请成功后，证书申请者即为订户。	GB/T 31508-2015,3.7
申请递交人（Application Deliverer）	向电子认证服务机构递交证书申请的自然人，可以是订户或者订户的授权代理人。	GB/T 31508-2015,3.8，有修改
证书主体（Subject）	证书中的 "主体（subject）" 项指明的、持有与证书中载明公钥相对应之私钥的实体。注：证书主体可以是订户自己，也可以是订户全权控制的设备、账号、域名、IP 地址等。当订户是法人机构时，证书主体还可以是该法人机构的下属机构、下属职员、授权代理人或设备等。	GB/T 31508-2015,3.6，有修改
证书持有者（Holder）	持有或控制电子签名制作数据的自然人或系统，必须是订户、订户的下属职员、授权代理人或者订户控制并经主体授权的信息系统。	/
电子签名人（Signer）	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。注：电子签名	《电子签名法》，根据《电子签名法释

术语	定义	来源
	人一般为证书主体中所载明的实体。	义》增加注
鉴别（Authentication）	确定个人、组织或事物如其所声称的个人、组织或事物的过程。在 PKI 上下文中，鉴别指的是证实以某个特定名称申请或试图访问某事物的个人或组织确实为真实的个人或组织的过程。	GB/T 26855-2011,3.2
标识（Identification）	建立个人或组织的身份的过程，也就是指明某个人或组织是特定的个人或组织。在 PKI 上下文中，标识包含两个过程：a）确定某个人或组织的给定名称与真实世界中该个人或组织的身份相联系。b）确定在该名称之下申请或试图访问某事物的个人或组织确实为指定的个人或组织。寻求标识的人可能是证书申请者，或者是 PKI 系统中可信任位的申请者，或者是试图访问网络或应用软件的人（如 CA 管理员试图访问 CA 系统）。	GB/T 26855-2011,3.5

下列缩略语适用于本 CPS 。

缩略语	中文全称	英文全称
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. 发布和存储库责任

SHECA 信息库（https://www.sheca.com/repository）保存并发布 CP/CPS 现行及历史版本、证书、CRL 及其他信息，是处理 SHECA 事宜的主要正式信息库，准确描述发证机构发布的证书与撤销通知，对信息不作更改。

CPS 至少每年更新一次，修订批准后及时发布并留存历史版本；订户证书 CRL 至少每 5 天一次或撤销后 24 小时内发布（nextUpdate-thisUpdate≤7 天）；根/中级根 CRL 至少每 7 个月一次或撤销后 24 小时内发布（间隔≤10 个月）；OCSP 响应可用性达到 99.9%；公告通知实时发布。

SHECA 经官网及目录服务（ldap2.sheca.com，可经 https://issp.sheca.com 查询）发布证书副本与撤销信息，提供在线证书状态查询。

敏感信息访问采用带安全套接层协议（SSL ）的超文本传输协议（HTTPS），以实现访问记录的安全模式（此时必须使用支持 SSL 的浏览器）。

SHECA 设置了访问控制和安全审计措施，保证只有经过授权的 SHECA 人员才能编写和修改 SHECA 在线公布的有关信息。

SHECA 在必要的时候，可以对某些与 SHECA 相关的信息实施权限控制，以确保只有 SHECA 的证书持有者才有权阅读这些信息。SHECA 可自主选择是否实行权限管理。

3. 识别和认证

3.1. 命名

设备证书的命名

设备证书的主体甄别名称（DN）采用 X.501 甄别名称，DN 结构符合 GB/T 16264.8；CN 为设备唯一标识（按设备类型确定，如设备序列号、内网 IP 地址或软硬件标识），O 为设备所属组织机构法定名称，OU 可选为设备所在部门或系统。设备证书的主体甄别名在其签发 CA 体系内唯一；同一设备的多个证书（如续期 / 重签）可具有相同主体甄别名。DN 项编码规则见表 1。

注 1：本 CPS 定义的证书不包含公共可信设备证书（如 SSL 证书等）。

注 2：SHECA 对设备证书申请人（设备所属组织机构）按照 3.2.3 执行规定的组织机构身份鉴别与授权确认；设备证书 CN 项的设备属性信息（设备名称、软硬件唯一标识等）以通过身份鉴别的组织机构提供的内容为准。SHECA 不对设备属性的物理真实性承担独立核验责任；组织机构应保证其提交信息的真实、准确、完整。

个人证书、机构证书的命名

个人证书、机构证书的命名采用实名，且证书可追溯至唯一实体。证书主体 DN 项或证书扩展项中，包含申请人个人有效身份证件类型及编号（或上述信息的映射形式，包括但不限于编号的杂凑值），或组织机构的有效证件编号。证书主题不应包含未经验证的信息。认证机构可为同一主体以相同

的甄别名称签发多个证书。DN 字段结构定义符合 GB/T 16264.8 的要求。DN 项编码规则见表 1。

表1 证书主体甄别名称（DN项）编码规范表

Name类型	说明	示例
C	证书主体所属国家或登记国家的ISO 3166-1二字符代码	CN
ST	证书主体省、自治区、直辖市等所在地或登记地信息（可选）。	江苏省
L	证书主体城市或地区所在地或登记地信息（可选）。	南京市
O	机构的完整法定名称。 个人证书不存在经验证机构关联关系时不得包含；存在经验证机构关联关系时应包含。 机构证书应包含。	xx公司
organizationIdentifier（OID 2.5.4.97）	机构登记标识。 个人证书包含O时应同时包含本属性；个人证书不包含O时不得包含本属性。 机构证书应包含本属性。	91310000XXXXXXXXXX
OU	证书主体所在机构的部门或组织单元名称，可选。	xx部门

	不应表示职务、岗位、机构角色、代理权限或授权范围	
CN	证书主体名称。 个人证书填写自然人法定姓名；机构证书填写机构名称	张三/xx公司
SerialNumber (OID 2.5.4.5)	个人证书主体唯一识别。机构证书不得包含本属性。	证件类型代码 ＋64位大写十六进制SM3杂凑值

3.2. 初始身份验证

3.2.1 证明拥有私钥的方法

SHECA 通过验证数字签名的方式，确认证书申请人拥有某一公钥对应的私钥。

3.2.1 个人订户身份的鉴别

a) 可接受的个人身份证件类型：个人身份证（或军官证、或学生证或护照等其它有效的身份证明文件）；

b) 现场面对面鉴别程序

1) 申请人应提交的资料：现场出示有效身份证件原件；认证机构应留存复印件（或影印件）；如果是委托办理，需同时递交申请人和被委托人的上述证件原件及复印件（或影印件），以及申请委托人亲笔签名的书面授权书。

2) 个人身份信息真实性的鉴别：通过证件机读工具、权威数据库查验订户身份证件的真实性和有效性；

3) 实人查验：通过面对面目视比对，可通过人脸等生物识别技术比对进行辅助增强查验；

c) 远程鉴别程序

1) 申请人应提交的资料：有效身份证件影印件或证件信息。

2) 个人身份信息真实性的鉴别：通过权威数据库查验申请人身份证件的真实性和有效性；

3) 实人查验：通过人脸识别，及电信运营商三要素（或银行卡四要素）验证；

注1：电信运营商三要素方式指核对姓名、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；

注2：银行卡四要素方式指核对姓名、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；

d) 身份鉴别完成后的协议签署按照4.1.2的d）执行；

e) 认证机构以纸质或电子数据形式完整记录并保存身份查验过程和结果。

3.2.3 组织机构订户身份的鉴别

a) 可接受的组织机构身份证件类型：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) 现场面对面鉴别程序

1) 申请人应提交的资料包括：

——现场出示组织机构有效身份证件原件；

——法定代表人（或负责人）本人办理的应出具本人有效身份证件原件；授权经办人办理的，应出具法定代表人（或负责人）及本人有效身份证件原件，以及授权经办人持有的加盖机构公章的授权文件原件；

认证机构留存上述资料的复印件或影印件；

2) 组织机构身份信息真实性的鉴别：查验组织机构身份证件的真实性

和有效性，可通过权威数据库比对进行辅助增强查验；

3) 授权经办人办理时，认证机构收取并查验申请人加盖机构公章的授权文件原件，确认组织机构授权行为；

4) 法定代表人（或负责人）或授权经办人的身份鉴别程序参见 3.2.2 中的 b）；

c) 远程鉴别程序

1) 申请人应提交的资料：组织机构有效身份证件影印件或证件信息；授权经办人办理的，还应提交加盖机构公章的授权文件影印件。

2) 组织机构身份信息真实性的鉴别：通过权威数据库查验组织机构身份证件的真实性和有效性；

3) 授权经办人办理时，认证机构应查验申请人加盖机构公章的授权文件，并通过组织机构对公账户随机金额打款验证的方式，确认组织机构授权行为。

4) 法定代表人（或负责人）或授权经办人的身份鉴别程序参见 3.2.2 中的 c）；

d) 身份鉴别完成后的协议签署按照4.1.2的d）执行；

e) 认证机构以纸质或电子数据形式完整记录并保存身份查验过程和结果。

3.2.4 设备证书订户身份的鉴别

按照 3.2.3 对设备所属的组织机构进行身份鉴别。

3.2.5 未经验证的订户信息

除设备证书 CN 项设备属性信息以通过本章 3.2 机构身份鉴别的申请组织机构提供的内容为准，证书主体中不应包含未经验证的信息。

3.2.6 授权确认

授权经办人办理证书申请时，应提交授权委托书，授权确认程序参见 3.2.2

和 3.2.3 中相关内容。

3.2.7 互操作

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身份证书。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。

3.3. 密钥更新请求的识别和认证

针对密钥更新请求，SHECA 鉴别并确认以下信息：

a) 原证书由 SHECA 签发；

b) 能识别原证书的足够信息，包括但不限于证书序列号、证书主体名称、证书有效期等；

c) 订户信息没有发生变化；

d) 原证书公钥对应的私钥由证书持有人实际掌握，验证方法包括：使用当前有效的私钥对包含新公钥的密钥更新请求进行签名，或按照 3.2.2 或 3.2.3 进行身份鉴别。

原证书已失效或已撤销的，不允许进行密钥更新操作。

3.4. 撤销请求的识别和认证

订户发起撤销：订户申请撤销证书时，其身份标识与鉴别应执行与初始身份鉴别相同的流程。

CA/RA 发起撤销：认证机构或注册机构主动发起证书撤销的情形和流程，

参考 4.9 章节。

司法机关、监管部门发起撤销：司法机关、监管部门依法提出证书撤销申请时，认证机构核验该撤销申请的真实性。核验无误后，认证机构及时执行撤销操作，并完整保存撤销依据及操作记录。

4. 证书生命周期操作要求

4.1. 证书申请

证书申请主体

证书申请人或其授权经办人均可提交证书申请。

注册过程与责任

a) 事项告知

认证机构在受理证书申请时，向证书申请人告知证书签发机构、证书产品、证书服务价格等信息：

b) 申请的提交和受理

1) 认证机构提供面对面及远程证书申请受理服务，满足不同类型证书申请人的办理需求；

2) 证书申请人应参照 3.2.2 或 3.2.3 提交申请材料，并确保所提供的信息真实、完整和准确。

c) 认证机构按 4.2.1 执行身份标识与鉴别。

d) 订户协议签订

1) 订户协议应包含申请人的权利和义务、证书的使用条件、证书所产生的法律责任、保存和使用证书持有人信息的权限和责任、认证服务机构和证书持有人的责任范围、订户签名私钥的管控风险、订户对签名私钥的保管和使用责任、签名私钥激活数据的安全保护义务，

以及法律法规和国家有关文件规定的其他需要告知的事项。

2) 以面对面方式办理的，由申请人或申请人的法定代表人（或授权经办人）对订户协议进行手写签名，确认申请意愿并完成协议签署；

3) 以远程方式办理的，申请人或申请人的法定代表人（或授权经办人）通过“强制阅读+主动勾选+短信验证”的方式确认申请意愿并完成协议签署；也可由申请人或申请人的法定代表人（或授权经办人）持有效个人或机构电子签名认证证书对订户协议进行电子签名，确认申请意愿并完成协议签署；

注：“强制阅读+主动勾选+短信验证”是指通过强制全文阅读订户协议并主动勾选同意，以及实名手机号的随机短信验证码核验。

e) 认证机构将上述过程通过纸质或电子数据方式完整记录并保存身份查验过程和结果。

4.2. 证书申请处理

当 SHECA 或其注册机构接收到证书申请人的证书申请后，按照本 CPS 3.2 初始身份验证的要求对证书申请人的身份进行鉴别，并证实证书申请系证书申请人的真实意思表示。SHECA 或注册机构应对身份鉴别记录和结果进行签名，并妥善保存身份鉴别相关记录。

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 CPS 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 CPS 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。

SHECA 处理证书申请的最长响应时间应不超过 5 个工作日；如有特殊情况，应与证书申请人协商申请处理的时间期限。

4.3. 证书签发

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。

证书签发过程中，注册机构系统和认证机构系统相互进行身份认证，并确保申请信息传输的机密性；注册机构对签发请求进行签名，认证机构验证无误后方可签发证书。

证书申请处理完毕后，SHECA 根据申请方式的不同采取以下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

订户可通过 SHECA 提供的证书使用工具进行信息提示核对，或通过热线支持服务确认证书信息的正确性；SHECA 提供热线支持服务，热线支持电话为021—962600。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。

4.4. 证书接受

订户在接收证书前可通过 SHECA 提供的证书使用工具等对证书内容进行核对，确认证书中主体信息、有效期、公钥等内容的正确性；订户下载或接收证书成功后即视为订户已完成对证书内容的核对并接受证书。

订户使用证书对应的私钥进行数字签名或其他密码运算时，即视为订户确认其持有的私钥与证书中的公钥相对应，并接受证书。

构成接受证书的行为

- 订户使用自有密钥载体自行生成签名密钥的，订户下载证书成功即视为订户接受证书；
- 订户使用认证机构提供的密钥载体生成签名密钥、并在证书签发后由认证机构将密钥载体通过面对面方式交付给订户后、或通过快递邮寄给订户并签收后，即视为订户接受证书；

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。

对于订户以书面或具备同等法律效力的电子形式表示拒绝发布证书信息的，SHECA 不发布该订户证书信息；订户未明确表示拒绝的，SHECA 按本 CPS 中声明的发布方式发布证书信息。

4.5. 密钥对和证书使用

订户的私钥和证书应仅用于本 CPS、订户协议及适用的证书内容（密钥用法字段）中规定的用途，并与证书声明的用途一致。

订户应按证书密钥用法等证书内容的规定使用证书；超范围使用的，不受本 CPS 及认证机构的保障。

订户仅在接受了相应证书之后，方可使用对应的私钥；证书有效期届满、被撤销或被冻结后，订户应立即停止使用该证书对应的私钥。

依赖方在信任证书前，应按照依赖方协议完成以下核验：

- 检查是否载入符合实际用途的身份证书策略 OID；
- 密钥的用途是否符合相应 CP/CPS 的相关规定；
- 确认该证书未过期、未被撤销、未被冻结；
- 能够与主管部门认可的根 CA 建立信任链。

未按要求完成上述核验的，或核查结果未通过可信证书及电子签名造成损失的，由依赖方自行承担责任。

4.6. 证书续期

证书续期需由订户主动提出申请。

证书到期前一个月SHECA 向证书持有者发出续期通知；有效期满前 SHECA 以网站提示、系统提示、书面提示、E-mail 等任一方式向订户或其受托人、垫付商、代理商发送续期提示，即视为已尽合理通知义务。

证书到期前 30 天内订户可申请续期，订户可选择保留原有密钥申请证书续期，并须保证密钥的安全可靠。

SHECA 提供在线续期和离线续期两种手段，订户可自行选择。

证书续期无需重新提交注册信息：订户提交识别原证书的足够信息（如订户

甄别名、证书序列号等），并使用原证书私钥对包含公钥的更新申请信息签名。

SHECA 对签名、公钥及续期请求内用户信息进行正确性、合法性、唯一性的验证；订户注册信息未变化的，基于原注册信息签发新证书。签发新证书时，SHECA 可要求订户提交原私钥签名，或按初始签发证书的流程重新鉴别，以确保提出续期请求的是被续期证书所标识的订户。

在线续期：订户在线填写续期请求并以当前私钥签名提交，SHECA 鉴别确认后签发新证书。

离线续期：订户按现场面对面申请流程提交，SHECA 按原流程鉴别审核并批准后签发。

续期前，订户应确认即将到期证书的密钥对安全可靠；无法确认的，SHECA 建议订户直接选择证书密钥更新。

证书续期的签发与接受流程按本CPS 4.3、4.4 的要求执行。

4.7. 证书密钥更新

证书密钥更新适用于以下情形：

- 订户证书未到期，需提前更新密钥对的；
- 订户证书密钥载体损坏的；
- 订户证实或怀疑其证书密钥载体或私钥存在安全风险的；
- 法律法规和国家有关文件规定的其它需要进行证书密钥更新的情形。

注：已被撤销或已过期的证书不应进行密钥更新；订户在证书被撤销后需要重新获得证书的，按本 CPS 3.2 重新完成身份鉴别，并以新的密钥对重新申请签发证书。

证书订户本人或证书订户的授权经办人可提交证书密钥更新请求。

SHECA 处理密钥更新请求时，对原证书有效性、更新请求的数字签名信息或申请人身份信息进行核验，核验通过后方可执行密钥更新操作，按本CPS 3.2

的要求执行。

在线更新：订户在线填写更新请求，用当前的私钥对包括新生成的公钥在内的更新请求信息进行签名后提交；SHECA 鉴别确认后签发新证书，该证书的公钥为申请者递交的新公钥。

离线更新：订户按现场面对面申请证书的流程提交更新请求并递交新生成的公钥；SHECA 按原流程鉴别审核，批准后签发新证书。

更新证书的签发与接受流程按本CPS 4.3、4.4 的要求执行。

4.8. 证书变更

证书变更是指改变证书中除订户公钥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 按照 3.2 对申请者递交的资料进行鉴别确认后，为其重新签发证书。

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申请身份证书，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、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 CPS　6.2、6.3 和 6.5）；

2、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；
- 继续使用订户证书会对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、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 CPS 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 依赖方检查证书撤销的要求

依赖方在信赖一个身份证书前，应当检查该证书的当前状态，确认该证书未被撤销。认证机构对依赖方未能检查证书是否已撤销，或依赖已撤销的证书而造成的任何损害不承担责任。

4.9.7 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。

4.9.8 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。

4.9.9 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%。

4.9.10 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。

4.9.11 撤销信息的其他发布形式

SHECA 目前不提供其它的撤销信息发布方式。

4.9.12 证书冻结的情形

SHECA 目前不支持证书冻结。

4.10. 证书状态服务

SHECA 提供证书状态实时查询服务，确保依赖方可实时获取证书的有效性信息，包括证书正常、已撤销、已过期等状态。

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。

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. 订阅终止

订购结束是指当证书有效期满或证书撤销后，该证书对应的认证服务终止。

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。

证书订户在证书有效期内提出终止服务的，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；SHECA 将完整记录以上操作记录。

订户的义务：订户自行保管密钥载体的，应自行销毁签名私钥；订购结束后，订户应立即停止使用该证书对应的私钥。

CA 的义务：认证机构应按本CPS 5.5 的规定完成证书相关信息的归档管理；撤销证书按 CRL 发布策略发布，保证状态信息的持续可用性。

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。

4.12. 密钥托管和恢复

SHECA不支持订户私钥的托管或恢复。

5. 设施、管理和操作控制

5.1. 物理安全控制

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，需要两名工作人员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。

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。

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。

SHECA 的机房采取了加高地板的处置措施，能够防止水患侵蚀。

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。

5.2. 程序控制

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

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。

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

事件响应程序：参考《信息化支撑部突发事件紧急处置和上报流程》执行。相关人员得知突发事件后，第一时间（5 分钟内）向事件相关分管领导电话报告，并在首报快报基础上持续跟踪关注，做到及时续报；相关领导应在 15 分钟内向公司主要领导电话报告；事件相关部门应在 40 分钟内以书面形式向公司报告。相关分管领导应及时指挥采取有效应对处置措施。

5.3. 人员控制

可信人员上岗前必须通过背景调查（从业经历、身份证明、学历证书真实性核验，确认无犯罪记录、具备专业技能），签署劳动合同与保密协议；未签劳动合同人员不得担任可信人员。

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

SHECA 与可信人员签署劳动合同，并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 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

SHECA 建立可信岗位人员常态化监督与违规问责机制。

1、操作监督：所有可信人员的证书系统操作、密钥管理操作全程日志记录，日志不可篡改；定期开展操作审计，抽查高风险操作（证书签发、吊销、密钥处理），独立审计人员有权复核操作记录。

2、权限管理：根据员工的岗位和职责，合理分配系统操作权限，遵循最小权限原则，确保员工只能进行其职责范围内的操作。关键操作需实行双人操作或复核机制。

3、问责机制：明确可信人员违规行为清单（越权操作、泄露敏感信息、私存密钥 / 证书资料、转借账号等）。一旦发生违规，立即暂停相关人员可

信岗位权限，开展事件调查；根据违规情节，采取警告、罚款、降职、辞退等相应处罚措施；涉嫌违法的，移交司法机关。所有调查、处置记录存档留存。

a) 岗位角色变更（调岗、职责调整）

人员发生岗位变更时，由直接上级 / 部门负责人开展权限评估：

- 即时回收该人员原岗位全部系统访问权限；
- 收回原岗位对应的实体令牌、操作证书、密钥载体；
- 严格遵循最小权限原则，仅依据新岗位职责重新分配对应权限；
- 所有权限回收与重新开通操作全程留痕，归档备查。

b) 员工离职（辞职、解聘、合同到期）

在员工正式离岗前，由直接上级 / 部门负责人逐项完成以下工作：

- 冻结 CA/RA 系统账号，撤销全部系统访问权限；
- 回收实体身份证书、USB 令牌、密钥载体，吊销该人员个人操作数字证书；
- 收回全部涉密文档、纸质与电子资料，完成工作交接，签署工作交接清单，交接人、部门负责人签字确认；
- 告知离职人员：保密义务在劳动关系终止后持续有效，不得泄露 SHECA 证书服务体系的任何敏感信息。

c) 通用管控要求

所有岗位变更、离职所涉及的账号冻结、权限回收、证书吊销、资产回收、资料交接等操作，均留存操作日志与纸质单据，长期归档，接受内部审计与外部合规核查。

5.4. 审计日志记录程序

记录事件范围：CA 密钥操作、证书生命周期关键过程（申请/审核/签发/更新/变更/撤销/密钥恢复、CRL 签发发布及通过/拒绝结果）、系统访问行为（含成功/失败登录）、系统操作与变更、网络安全事件、系统环境事件、物理环境事件（门禁进出）。

记录内容：事件时间、类型、内容、操作人、作用对象及结果，关键操作由操作人员电子签名。

保留期限：至少 5 年，法律法规另有规定的从其规定。

保护措施：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。

审查程序：审计内容系统异常、未授权访问、资源使用异常、配置变更等。每季度审查并形成报告、采取改进措施。

5.5. 记录归档

日常测试巡检文档，包括每日、每周、每月相关纸质文档，每年归档一次。

归档记录类型：证书申请材料与订户意愿记录、全部审计日志、密码设备全生命周期及日常操作记录、根证书/密钥生命周期记录、系统运行日志、安全事件处置记录、关键操作日志，以及 CP/CPS/订户协议/依赖方协议所有版本、CRL 版本、评估审计材料、人员资料、投诉争议资料等。

保留期限：CA 证书密钥管理事件在生命周期结束后额外不少于 5 年；订户证书记录在撤销或失效后不少于 5 年；密码设备/CA 证书/密钥相关记录及协议版本等长期保存；其他不少于 1 年。

保护程序：物理+密码技术双重保护，仅授权人员按特定方式存取；主要存储+必要异地备份，数据库物理/逻辑隔离、禁止删除修改；异常时按恢复策略恢复。

访问控制：设专门归档管理机构，仅授权可信人员访问，归档及归还时验证一致性。

5.6. 密钥更替

CA 证书有效期最长不超过 30 年，下级证书有效期均短于 CA 证书。

更替原则：在下级证书生命周期结束前停止签发新下级证书，确保 CA 证书到期时下级证书全部到期；在屏蔽机房内生成新密钥对并签发新 CA 证书；新公钥经官网发布；停止签发后继续以旧私钥签发 CRL 直至最后一张下级证书过期；按 GB/T 25056-2018 8.2.4.3 销毁旧密钥及备份并保留记录。

紧急更替（密钥泄露或安全隐患）立即启动；到期更替在密钥到期前三年完成。

5.7. 泄露和灾难恢复

业务连续性目标：RTO 不超过 24 小时、RPO 不超过 1 小时。

恢复流程：证书库、物理设施、计算资源、网络、软件均实现 HA，数据库本地热备+异地灾备，故障时主从切换/日志回滚/流量切换恢复；生成受影响并被撤销的证书列表并重新提供公钥证书。

灾难恢复：按灾难恢复计划实施，24 小时内恢复证书服务。

私钥损害：订户私钥受损——立即停止使用并撤销（见 4.9）；CA/受托 CA 私钥受损——立即撤销 CA 证书、广泛通知依赖方、生成新密钥对并签发新证书。

定期验证：每年一次灾难恢复演练及备份恢复测试。

5.8. CA 或 RA 终止

终止程序：

- 起草并发布 CA 终止声明，至少提前 90 日通知订户/依赖方等、提前 60 日向主管部门报告；

- 选聘具备资质的业务承接单位并签署承接协议；
- 向承接方移交密钥及关键数据；
- 停止证书状态服务、其他服务、密码设备并归档相关数据；撤销/冻结相关操作权限；
- 封存存档记录、安全处理敏感数据、清除主机及密码硬件敏感数据；
- 外部合作机构终止服务在官网通告。

6. 技术安全控制

6.1. 密钥对生成和安装

CA 密钥生成：遵循 GM/T 0034。

- 由经国家密码主管部门批准许可的硬件密码设备生成，须经安全认证委员会授权、至少 3 名密钥管理人员在场共同操作；生成/备份/恢复/销毁实施 M 选 N 多人控制（M≥5，N≥M/2）；录音录像全程记录并保存至密钥失效后 10 年。
- CA 公钥在官网根证书列表中发布，CA 私钥在硬件密码设备内生成存储、无法以明文输出或传送。
- 根 CA 密钥仅签发根/中级 CA/交叉 CA/OCSP 证书；中级 CA 密钥签发订户证书、OCSP 等功能证书及订户 CRL。
- CA 密钥长度为 RSA 2048/3072/4096 或 SM2 256 位，RSA 公指数为奇数且在 2^16+1 至 2^256-1 间，模数为非素幂奇数且无小于 752 的因数。

订户签名密钥生成：按两种密钥生成方式分别要求：

- 自有密钥载体：订户用符合规定要求的密钥载体自行生成；通过订户协议明确私钥管控风险及保管使用责任；使用不符合规定的密钥载体生成的，拒绝签发证书。

- 认证机构提供密钥载体：认证机构按规定密钥载体生成；事先取得订户同意（纸质或电子）；订户协议明确交付后私钥管控风险及保管使用责任。

订户加密密钥生成：遵循 GM/T 0034。

SHECA 拒绝订户委托其它第三方管理密钥载体生成和保管签名私钥的证书申请。

密钥生成全过程遵循 GM/T 0034；SM2 密钥长度及算法参数生成遵循 GM/T 0003；密钥载体符合规定要求。

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。

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。

订户签名私钥传送：

- 自有密钥载体：SHECA 不承担私钥传送与安装责任。
- —认证机构提供密钥载体：密钥载体与私钥激活数据（如 PIN 码）经相互独立的安全通道分别传送给订户。

订户签名公钥传送给 CA：订户签名公钥通过安全方式提交（如商用密码算法保护的安全会话传输、经注册机构数字签名的消息传输），符合本 CPS 4.2；公钥经签名的 CSR 传送，签发前验证 CSR 签名。

订户加密密钥：以符合 GM/T 0034 的方式传送。

CA 公钥传送给依赖方：CA 公钥在官网根证书列表中发布。

CA 私钥在硬件密码设备内生成存储、无法以明文输出或传送。

认证机构提供密钥载体：交付前确保密钥载体和签名私钥安全。

自有密钥载体：订户的保管和使用责任通过订户协议明确。

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

CA 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。

6.2.2 私钥多人控制

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。

6.2.3 私钥托管

SHECA 的签名私钥不允许托管。

SHECA 的加密私钥托管在 SHECA 证书认证密钥管理系统中。

6.2.4 私钥备份与恢复

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。

6.2.5 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。

6.2.6 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。

6.2.7 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。

6.2.8 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。

6.2.9 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。

6.2.10 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。

6.2.11 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。

6.3. 密钥对管理的其他方面

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 CPS 5.5 的相关规定。

证书操作期和密钥对使用期限

无论订户证书还是CA证书，证书有效期届满后，对应私钥不应再用于电子签名操作。证书链中，下级证书的密钥使用有效期不应超过上级CA证书的有效期。

6.4. 激活数据

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。

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。

订户私钥的激活数据

订户自行保管密钥载体，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。

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。

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 CPS 3.2 执行。

6.5. 计算机安全控制

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。

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

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。

面向云原生与 Kubernetes 环境，建设覆盖“镜像—编排—运行时—网络—主机—数据”的一体化防护体系。在供应链侧，对容器镜像开展漏洞、恶意包、敏感信息扫描与签名验证，结合镜像仓库准入控制阻断不合规镜像；在运行时侧，部署 EDR 与基于 eBPF 的行为检测，联动 K8s Audit、容器日志、进程/系统调用和网络连接遥测，识别挖矿、Webshell、反弹 Shell、权限提升、异常 ServiceAccount 调用及横向移动。网络侧通过东西向流量检测、出向管控、WAF 防护，限制 C2、扫描探测与暴力破解；管理面重点保护 API Server、etcd、节点 kubelet 与凭据，关键日志防篡改并集中接入态势感知。产品能力形成“预防—检测—响应—溯源”闭环：基线核查、病毒木马查杀、沙箱研判、自动隔离 Pod/节点、阻断会话与工单编排，满足等保 2.0 三级对恶意代码防范、入侵防范、安全审计与集中管控的要求。

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

6.6. 生命周期安全控制

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。

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 认证系统实施严格的变更管控机制，系统所有变更（含功能修改、版本升级、配置调整、补丁部署等）均纳入公司标准化变更管理流程管控，未经完整评审与正式审批，不得实施任何变更操作，变更实施过程全程留痕，所有修改、配置调整、版本升级操作信息统一记录于 OA 流程台账，变更实施完成后，执行上线验证，确认变更生效状态；并完成变更闭环归档。对于重大变更，后续开展事后复盘，评估变更效果、残留风险。

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。

6.7. 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。

关于安全通信，应用系统访问均采用 https 加 TLS1.2 防止在网络传输时给数据加密，防止被窃听、篡改、冒充。灾备数据备份传输时采用 ipsec 国密加密方式，做数据加密。

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

6.8. 时间戳

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。

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。

7. 证书、CRL 和 OCSP 配置文件

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. 证书配置文件

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。

- 序列号

SHECA 签发的证书采用随机序列号。

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。

证书扩展项（RFC5280）

- 密钥用途

签名证书：digitalSignature

加密证书：keyAgreement，dataEncipherment，keyEncipherment

- 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。

自定义扩展项

- 个人身份标识码 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: 1.2.156.10260.4.4，1.2.156.112570.11.210
- 全局唯一标识符 OID: 1.2.156.112570.30.1.3.1
- 项目标识符 OID: 1.2.156.112570.30.1.5

- 应用标识符 OID: 1.2.156.112570.30.1.6
- 应用自定义数据 OID:1.2.156.112570.40.1

SHECA 使用符合国家密码管理部门批准的算法对象标识符。

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。

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。

特殊名称，满足与确定实体（个人、组织或者设备）唯一联系起来，必须经过 SHECA 安全认证委员会的批准方能使用。

对象标识符（OID）是标识对象或策略的唯一编号，存放在证书内证书策略的相关栏目。具体请参考本 CPS 1.1。

7.2. CRL 配置文件

SHECA 目前签发 X.509 V2 版本的 CRL，此版本号存放在 CRL 版本格式栏目内。

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

7.3. OCSP 配置文件

SHECA 的 OCSP 版本为 RFC6960 定义的 OCSP V1。

SHECA 的 OCSP 符合 GB/T 19713-2025 中的要求。

8. 合规审计与其他评估

全面符合性评估：围绕现行 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，覆盖证书全生命周期管理、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；由 SHECA 安全认证委员会统筹，战略发展部执行。

全面符合性评估，每年至少开展 1 次。

发生重大合规事件时（如密钥泄露），触发临时专项评估。

主管部门发起的现场核查、专项巡检，按监管要求启动对应评估。

内部审计人员：由 SHECA 安全认证委员会统筹配置，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。

外部审计机构及人员：选用具备相应审计资质的会计师事务所/ 信息安全评估机构，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。

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。

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。

内部人员需保持岗位独立性，与被审计业务无利益关联，组织架构上独立于被评估部门。

SHECA 需对以上评估活动发现的问题制定整改计划，完整执行整改措施。

若评估发现对 CA 系统或密钥安全性存在重大威胁的缺陷，则触发事件上报机制，参考 5.2 中事件响应程序执行；经安全认证委员会审批，可暂停签发证书、撤销受影响的证书；涉及赔偿的按本 CPS 9.9 章执行；对于重大合规缺陷，SHECA 视情况决定是否进行临时专项评估以验证整改结果。

全面符合性评估报告：由安全认证委员会审批发布，经战略发展部同意后提供给外部审计或监管机构。

其他评估报告：对外提供前须取得 SHECA 书面同意。

9. 其他业务与法律事项

9.1. 费用

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:

- 证书签发或更新费用

  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。

- 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

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。

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。

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. 商业信息保密

保密信息

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。

非保密信息

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。

信息保密义务

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. 个人信息隐私

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。

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。

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。

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。

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）。

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

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

参照《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》执行。

9.6. 陈述与保证

参照《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》执行。

9.7. 免责声明

参照《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》执行。

9.8. 责任限制

参照《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》执行。

9.9. 赔偿

赔偿范围

参照《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》执行。

赔偿限额

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）：

1、个人类证书，不超过 2，000 元

2、组织类证书，不超过 5，000 元

3、设备类证书，不超过 10，000 元

9.10. 期限与终止

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。

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。

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. 个人通知与参与者沟通

除非法律法规或协议特别规定，SHECA 以合理方式与各方沟通，不采取个别方式；服务、规范、操作的通知以书面形式传达（快递或挂号邮件附回执）；电子邮件通知须在 SHECA 收到后 24 小时内收到书面确认材料方为有效；地址：上海市四川北路 1717 号嘉杰国际广场 18 楼（200080）。

9.12. 修订

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本 CPS，对于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

修订程序参考本 CPS 1.5 章节。

不实质降低保证的修订无需变更本 CPS CP OID；实质性改变证书可接受性的修订须更新 CP OID。

9.13. 争议解决程序

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 安全认证委员会调解或第三方调解机构介入

替代性争议解决方式：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

9.14. 管辖法律

无论合同或其他法律条款的选择及无论是否在中国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. 遵守适用法律

所有电子认证活动的参与方，都必须遵守《中国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. 杂项条款

参照《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》执行。

9.17. 其他条款

参照《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》执行。