协卡网络信任服务体系电子认证业务规则

UniTrust Network Trust Service Hierarchy Certification Practice Statement (UNTSH CPS)

Version 3.7.6

生效日期：[2023年08月23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
- RFC2459：互联网 X.509 公钥基础设施-证书和 CRL 属性
- RFC2560：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 20518-2006：信息安全技术 公钥基础设施 数字证书格式

本 CPS 已被提交给独立的审计机构，按照 AICPA/CICA WebTrust for Certification Authority 进行评估，本 CPS 符合上述审计标准的情况，将在 https://www.sheca.com 网站上进行公布。

版本控制

版本	发布日期	发布者
V3.7.6 (现行版本)	2023 年 08 月 23 日	SHECA 安全认证委员会
V3.7.5 (上一版本)	2023 年 07 月 21 日	SHECA 安全认证委员会
V3.7.4 (上一版本)	2023 年 06 月 12 日	SHECA 安全认证委员会
V3.7.3 (上一版本)	2023 年 04 月 18 日	SHECA 安全认证委员会
V3.7.2 (上一版本)	2022 年 04 月 18 日	SHECA 安全认证委员会
V3.7.1 (上一版本)	2021 年 11 月 15 日	SHECA 安全认证委员会
V3.7 (上一版本)	2021 年 6 月 18 日	SHECA 安全认证委员会
V3.6.9 (上一版本)	2021 年 4 月 29 日	SHECA 安全认证委员会
V3.6.8 (上一版本)	2020 年 8 月 11 日	SHECA 安全认证委员会
V3.6.7 (上一版本)	2020 年 6 月 5 日	SHECA 安全认证委员会
V3.6.6 (上一版本)	2020 年 4 月 30 日	SHECA 安全认证委员会
V3.6.5 (上一版本)	2020 年 4 月 2 日	SHECA 安全认证委员会
V3.6.4 (上一版本)	2019 年 5 月 29 日	SHECA 安全认证委员会
V3.6.3 (上一版本)	2018 年 9 月 10 日	SHECA 安全认证委员会
V3.6.2 (上一版本)	2018 年 8 月 21 日	SHECA 安全认证委员会
V3.6.1 (上一版本)	2018 年 7 月 12 日	SHECA 安全认证委员会
V3.6 (上一版本)	2018 年 6 月 7 日	SHECA 安全认证委员会
V3.5 (上一版本)	2017 年 5 月 24 日	SHECA 安全认证委员会

V3.4.2.3（上一版本）	2016 年 5 月 25 日	SHECA 安全认证委员会
V3.4.2.2（上一版本）	2015 年 9 月 18 日	SHECA 安全认证委员会
V3.4.2.1（上一版本）	2014 年 9 月 1 日	SHECA 安全认证委员会
V3.4.2 （上一版本）	2014 年 4 月 29 日	SHECA 安全认证委员会
V3.4.1 （上一版本）	2010 年 4 月 8 日	SHECA 安全认证委员会
V3.4 （上一版本）	2009 年 4 月 23 日	SHECA 安全认证委员会
V3.3 （上一版本）	2009 年 3 月 26 日	SHECA 安全认证委员会
V3.2 （历史版本）	2008 年 3 月 18 日	SHECA 安全认证委员会
V3.1 （历史版本）	2005 年 7 月 1 日	SHECA 安全认证委员会

变更摘要

版本	更新描述
V3.7.6	根据 Baseline Requirements 要求，修改版本； 增加组织机构鉴别方式； 调整 9.16.3 分割性要求，增加 CPS 向 CA/B forum 备案的要求
V3.7.5	披露新的中级根证书 Xinnet DV SSL /Xinnet OV SSL
V3.7.4	披露重签的交叉根证书 UCA Global G2 Root
V3.7.3	披露新的中级根证书 SHECA OV Server CA G7; 更新中级根状态； ARL/CRL 更新频率
V3.7.2	披露新的中级根证书 CECloud Secure Server CA V1，SHECA SM2 Identity CA G1，SHECA SMIME CA G1

V3.7.1	披露部分中级根停止签发时间
	披露政务外网的域名验证规则
	增加职位证书身份验证规则描述
	密钥恢复业务
V3.7	ARL 更新频率
	代码签名和时间戳证书算法长度要求更新
V3.6.9	披露新的中级根
	删除上一版本 3.2.5 第 2 条第(8)、(9)种方式域名验证的方式
V3.6.8	更新监管机构名称
	披露 LDAP 地址
	机房电力供应
V3.6.7	披露新的中级根证书 GlobalSign China CA for AATL
V3.6.6	披露新的根证书 UniTrust Global Root CA R1，UniTrust Global Root CA R2，UniTrust Global Root CA R3
	删除上一版本 3.2.5 第 2 条第（3）种方式域名验证的方式
	增加身份鉴别的方式
	证书更新期限调整
	增加初步调查报告机制
V3.6.5	披露新的交叉根证书 UCA Global G2 Root
	SSL 证书有效期变更
	SSL 证书域名验证方式变更
V3.6.4	根证书增加 UniTrust PTC Root CA R1, UniTrust PTC Root CA R2
	修改个人及单位证书申请流程

V3.6.3	增加变更摘要
V3.6.2	数据、文件及验证有效期 825 天的限制 SSL 证书更新流程 SSL 密钥更新流程 补充部分证书撤销原因
V3.6.1	UCA Global G2 Root 根结构调整 修改 IP 地址控制权验证方式 增加 CAA 标记检查要求 声明数据源 825 天有效期限制
V3.6	UNTSH 认证网络信任服务体系调整 增加 OID 列表 调整证书最大有效期 调整算法对象标识符
V3.5	调整身份验证方法 调整域名、IP 地址、通配符、邮箱验证方法 数据源准确性,增加资料 825 天有效期限制
V3.4.2.3	部分语言或者文字表述不妥当的描述
V3.4.2.2	调整证书签发及更新费用
V3.4.2.1	UNTSH 认证网络信任服务体系架构调整
V3.4.2	声明与 CABF BR 的符合性 调整 Email 验证方式 修改附录
V3.4.1	公司信息变更
V3.4	增加了关于证书语言版本的描述 修改了关于证书身份鉴别的内容 修改了扩展密钥用户的内容

V3.3	增加 CP/CPS 关系 UNTSH 认证网络信任服务体系架构调整 增加证书使用的限制性说明 修改归档资料保存期限
V3.2	增加附录
V3.1	--

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：8621-36393100，传真：8621-36393200 。电子邮件：CPS@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。

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数字证书认证服务的实施及使用，数字证书认证服务包括SHECA数字证书发放、管理和验证，涵盖了数字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）申请者在申请证书之前，已被建议接受适当的数字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方可使用证书与其他人建立通讯或引导他人使用证书。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、如果你是数字签名或数字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及其授权的证书服务机构。

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：

cps@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.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、信任的网络环境而努力。

SHECA 制定了本文档——《SHECA 电子认证业务规则（CPS）》（以下简称本 CPS）。本 CPS 接受《协卡认证网络信任服务体系证书策略》（UniTrust Network Trust Service Hierarchy Certificate Policies，简称《UniTrust NTSH 证书策略》）的约束，详细阐述了 SHECA 遵循《UniTrust NTSH 证书策略》的要求开展数字证书服务的过程、控制、管理和保障活动，规定了数字证书申请、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 概述

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 主要依据国家信息产业主管部门发布的《电子认证业务规则规范（试行）》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。本文档符合《UniTrust NTSH 证书策略》，落实并实现《UniTrust NTSH 证书策略》的规定和要求，适用于协卡认证体系运营管理的所有 CA，包括根 CA 及其下设的子 CA，所有协卡认证体系内 CA 签发的证书，包括自签发根证书、被签发的子 CA 证书和用户证书，都按照本文档的规定进行操作和管理，以及履行相关的权利义务关系。

本 CPS 详细阐述了 SHECA 在签发、管理数字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，并监督其实施，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，SHECA 授权建立的各类注册机构、服务受理点等服务机构，SHECA 的员工，各 SHECA 关联实体及其员工，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。SHECA 及其授权建立的各类服务机构承诺：严格按照本 CPS 的规定签发证书，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，公钥能与身份明确的实体唯一相对应。

SHECA 遵循 CA/浏览器论坛（CA/Browser Forum）(www.cabforum.org)发布的最新版本的 Guidelines、Baseline Requirement 以及 Minimum Requirements for Code Signing Certificates 进行签发和管理公共可信任 SSL 数字证书和代码签名证书，并将持续根据其发布的版本进行修订，如果本 CPS 和 CA/浏览器论坛（CA/Browser Forum）发布的 Guidelines、Baseline Requirement 以及 Minimum Requirements for Code Signing Certificates 等相关规范中的条款有不一致的地方，则以 CA/浏览器论坛正式发布的规范为准。

本 CPS 向社会公布 SHECA 关于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。

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，是中国第一家专业的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，实现根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）。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 电子认证业务规则（CPS）与证书策略（CP）关系

协卡认证体系下每个证书都有一个唯一的证书策略（CP）支持。证书策略主要阐明协卡认证体系数字证书服务各参与方必须达到的要求，电子认证业务规则（CPS）主要确定 SHECA 作为一个数字证书运营服务主体，在提供数字证书服务时，各参与方为实施和满足证书策略要求所采取的过程、操作和控制措施，详细描述和规定了提供数字证书服务的需要条件、操作过程、控制流程和遵循准则。证书策略（CP）和电子认证业务规则（CPS）都服务于协卡认证体系，决定协卡认证体系下数字证书的信任程度、信任范围和信任目的。电子认证业务规则（CPS）从属于证书策略（CP），在阐述相同主题时，以证书策略（CP）的内容为准。

1.1.3 目前，《SHECA 电子认证业务规则 (CPS) 》仅支持《UniTrust NTSH 证书策略》。如果有需要，《SHECA 电子认证业务规则（CPS）》可以支持多个证书策略，以应用于不同的目的或不同的依赖方团体。

1.1.4 协卡认证网络信任服务体系

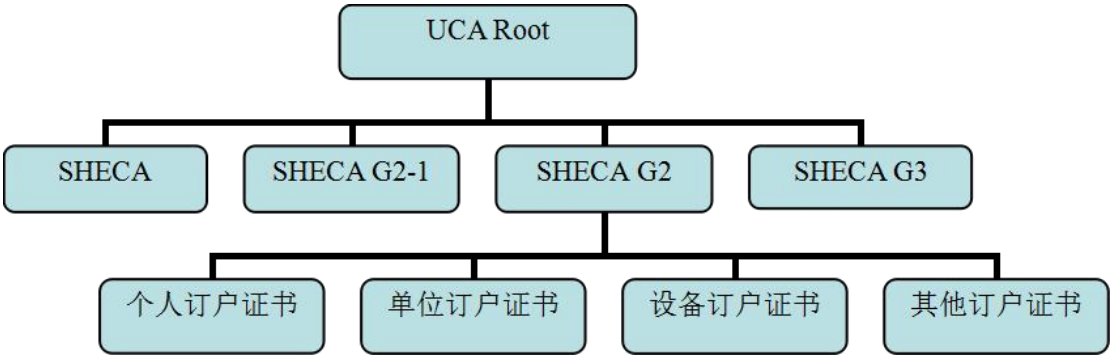
协卡认证网络信任服务体系（UniTrust Network Trust Service Hierarchy，缩写为 UNTSH，简称协卡认证体系）提出“一证在手，走遍天下”的数字证书服务理念，为电子政务、电子商务、社会化服务及其它网上作业活动的各个参与主体发放数字证书，可以实现跨行业、跨地域的电子认证服务。

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 下设子 CA，以签发用户证书。因此，协卡认证体系包含了根 CA、子 CA、各相关注册机构（RA 中心）、服务受理点（RAT）以及其他授权的服务关联实体，这些实体都是协卡认证体系内不同层次的服务主体。协卡认证体系所有和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。

协卡认证体系的 PKI 层次架构如下：

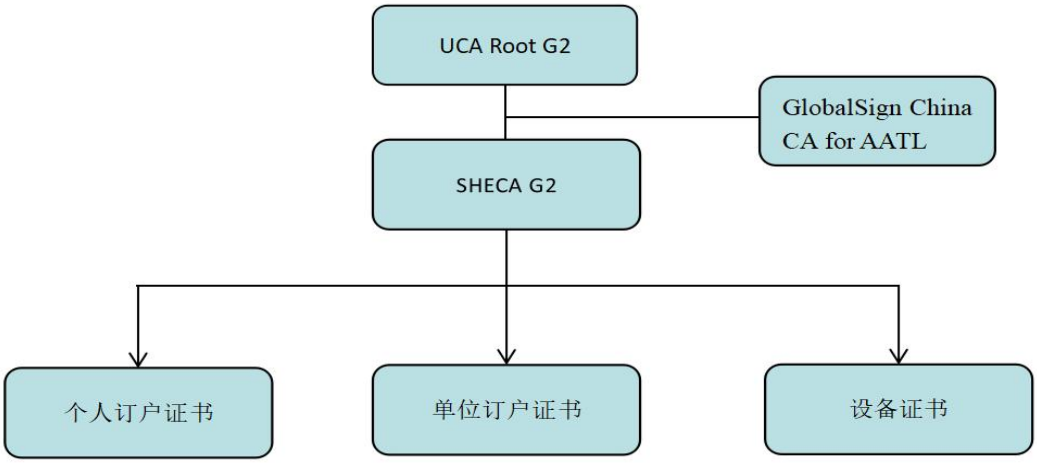
- UCA Root



UCA Root 根密钥长度为 2048-bit, 下设四个子 CA 证书, 其中：(1) SHECA、SHECA G2 及 SHECA G3 子 CA 不再签发订户证书； (2) SHECA G2 子 CA 签发密钥长度为 RSA 1024-bit 或 2048-bit 的个人订户证书、单位订户证书、设备订户证书和其他订户证书，不签署 SSL 证书；

UCA Root 有效期将于 2029 年 12 月 31 日到期, 2025 年 1 月 1 日起不再签发下级证书。

- UCA Root G2



UCA Root G2 根密钥长度为 2048-bit，下设两个中级根。

SHECA G2 子 CA 证书，签发密钥长度为 2048-bit 的个人订户证书、单位订户证书、设备订户证书；GlobalSign Root China CA for AATL 子 CA 证书，签发密钥长度为 2048-bit 的文档签名证书。

UCA Root G2 有效期将于 2036 年 12 月 31 日到期，2032 年 1 月 1 日起不再签发下级证书。

- UCA Global G2 Root

UCA Global G2 Root 根密钥长度为 4096-bit，有效期至 2040 年 12 月 31 日，2036 年 1 月 1 日起不再签发下级证书。

2020 年 2 月 21 日 ,Asseco Data Systems S.A. 的根证书 Certum Trusted Network CA 签发了交叉根证书 UCA Global G2 Root，有效期从 2020 年 2 月 21 日到 2025 年 2 月 21 日，该证书于 2023 年 4 月 28 日撤销。

2023 年 3 月 28 日， Asseco Data Systems S.A. 的根证书 Certum Trusted Network CA 重新签发了交叉根证书 UCA Global G2 Root, 有效期从 2023 年 3 月 28 日到 2025 年 2 月 21 日。

UCA Global G2 Root 目前有 10 个在用的中级根证书，2 个已停用中级根，4 个已撤销的中级根:

证书名称	密钥算法/长度	签名算法	签发证书	状态
SHECA SMIME CA G1	RSA 2048	SHA-256 with RSA Encryption	安全邮件证书	正常

SHECA RSA Code Signing CA G3	RSA 2048	SHA-256 with RSA Encryption	代码签名证书	已撤销
SHECA RSA Domain Validation Server CA G3	RSA 2048	SHA-256 with RSA Encryption	DV 安全站点证书	已撤销
SHECA RSA Organization Validation Server CA G3	RSA 2048	SHA-256 with RSA Encryption	OV 安全站点证书	已撤销
SHECA RSA Time Stamp Authority G1	RSA 2048	SHA-256 with RSA Encryption	时间戳证书	已撤销
SHECA DV Server CA G5	RSA / 2048	SHA-256 with RSA Encryption	DV 安全站点证书	正常
SHECA OV Server CA G5	RSA / 2048	SHA-256 with RSA Encryption	OV 安全站点证书	正常
SHECA EV Server CA G2	RSA / 2048	SHA-256 with RSA Encryption	EV 安全站点证书	正常
SHECA Code Signing CA G4	RSA / 3072	SHA-256 with RSA Encryption	代码签名证书	正常
SHECA Time Stamping CA G2	RSA / 3072	SHA-256 with RSA Encryption	时间戳证书	正常
TrustAsia RSA DV TLS CA - S1	RSA / 2048	SHA-256 with RSA Encryption	DV 安全站点证书	正常
TrustAsia RSA OV TLS CA - S1	RSA / 2048	SHA-256 with RSA Encryption	OV 安全站点证书	正常
Xinnet DV SSL	RSA / 2048	SHA-256 with RSA Encryption	DV 安全站点证书	正常
Xinnet OV SSL	RSA / 2048	SHA-256 with RSA Encryption	OV 安全站点证书	正常
SHECA Global G3 SSL	RSA / 2048	SHA-256 with RSA Encryption	安全站点证书	已停用
SHECA Global G3 Code Signing	RSA / 2048	SHA-256 with RSA Encryption	代码签名证书	已停用

- UCA Extended Validation Root

UCA Extended Validation Root 根密钥长度为 4096-bit，有效期将于 2038 年 12 月 31 日到期，2034 年 1 月 1 日起不再签发下级证书。下设 8 个子 CA 证书，

证书名称	密钥算法/长度	签名算法	签发证书/适用范围	状态
SHECA RSA Extended Validation Code Signing CA	RSA 2048	SHA-256 with RSA Encryption	EV 代码签名证书	已撤销
SHECA RSA Extended Validation Server CA	RSA 2048	SHA-256 with RSA Encryption	EV 安全站点证书	已撤销
SHECA EV Server CA G3	RSA 2048	SHA-256 with RSA Encryption	EV 安全站点证书	正常
SHECA EV Code Signing CA G2	RSA 3072	SHA-256 with RSA Encryption	EV 代码签名证书	正常
SHECA Extended Validation SSL CA	RSA 2048	SHA-256 with RSA Encryption	EV 安全站点证书	已停用
SHECA Extended Validation Code Signing CA	RSA 2048	SHA-256 with RSA Encryption	EV 代码签名证书	已停用
SHECA OV Server CA G6	RSA 2048	SHA-256 with RSA Encryption	EV 安全站点证书	已撤销
SHECA OV Server CA G7	RSA 2048	SHA-256 with RSA Encryption	EV 安全站点证书	正常

- UCA Root SM2

UCA Root SM2 根密钥长度为 256 位，SM2 算法，签名算法为 SM2 Signature with SM3，有效期到 2038 年 12 月 31 日，2033 年 12 月 31 日起不再签发下级证书，下设 8 个子 CA 证书。

证书名称	密钥算法/长度	签名算法	签发证书/适用范围	状态
UniTrust DV Secure Server	SM2 256	SM2 Signature with SM3	SM2 算法 DV 安全站点证书	正常
UniTrust OV Secure Server	SM2 256	SM2 Signature with SM3	SM2 算法 OV 安全站点证书	正常
SHECA SM2	SM2 256	SM2 Signature with SM3	个人订户证书、单位订户证书、设备订户证书	正常
TrustAsia SM2 DV TLS CA - S1	SM2 256	SM2 Signature with SM3	SM2 算法 DV 安全站点证书	正常
TrustAsia SM2 OV TLS CA - S1	SM2 256	SM2 Signature with SM3	SM2 算法 OV 安全站点证书	正常
TrustAsia SM2 Identity CA - S1	SM2 256	SM2 Signature with SM3	个人订户证书、单位订户证书	正常
SHECA SM2 Identity CA G1	SM2 256	SM2 Signature with SM3	个人订户证书	正常
CECloud Secure Server CA V1	SM2 256	SM2 Signature with SM3	SM2 算法安全站点证书	正常

- UniTrust Global Root CA R1

UniTrust Global Root CA R1 根密钥长度为 4096 位，RSA 算法，签名算法为 RSA SHA-384,有效期将于 2045 年 4 月 28 日到期, 2040 年 4 月 28 日起不再签发下级证书，下设 6 个子 CA 证书。

证书名称	密钥算法/长度	签名算法	签发证书/适用范围	状态
SHECA DV Server CA 1A	RSA / 4096	SHA-384 with RSA Encryption	DV 安全站点证书	暂停
SHECA OV Server CA 1A	RSA / 4096	SHA-384 with RSA Encryption	OV 安全站点证书	暂停
SHECA EV Server CA 1A	RSA / 4096	SHA-384 with RSA Encryption	EV 安全站点证书	暂停
SHECA Code Signing CA 1A	RSA / 4096	SHA-384 with RSA Encryption	代码签名证书	暂停
SHECA EV Code Signing CA 1A	RSA / 4096	SHA-384 with RSA Encryption	EV 代码签名证书	暂停
SHECA Time Stamping CA 1A	RSA / 4096	SHA-384 with RSA Encryption	时间戳证书	暂停

- UniTrust Global Root CA R2

UniTrust Global Root CA R2 根密钥长度为 384 位，ECDSA 算法，签名算法为 ECDSA SHA-384,有效期将于 2045 年 4 月 28 日到期，2040 年 4 月 28 日起不再签发下级证书。下设 3 个子 CA 证书。

证书名称	密钥算法/长度	签名算法	签发证书/适用范围	状态
SHECA DV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	ECC 算法 DV 安全站点证书	暂停
SHECA OV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	ECC 算法 OV 安全站点证书	暂停
SHECA EV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	ECC 算法 EV 安全站点证书	暂停

- UniTrust Global Root CA R3

UniTrust Global Root CA R1 根密钥长度为 256 位，SM2 算法，签名算法为 SM2 Signature with SM3,有效期将于 2045 年 4 月 28 日到期，2040 年 4 月 28 日起不再签发下级证书。下设 3 个子 CA 证书。

证书名称	密钥算法/长度	签名算法	签发证书/适用范围	状态
SHECA DV Server CA 3A	SM2 / 256	SM2 Signature with SM3	SM 算法 DV 安全站点证书	暂停
SHECA OV Server CA 3A	SM2 / 256	SM2 Signature with SM3	SM 算法 OV 安全站点证书	暂停
SHECA EV Server CA 3A	SM2 / 256	SM2 Signature with SM3	SM 算法 EV 安全站点证书	暂停

- UCA Root-G1

UCA Root-G1 自 2009 年 1 月 1 日起停止签发证书。

- UCA Global Root

UCA Global Root 自 2017 年 4 月 27 日起停止签发证书。

1.2 文档名称与标识

本文档的名称为《SHECA 电子认证业务规则(CPS)》，简称 SHECA CPS。“SHECA CPS”、“上海 CA CPS”、“上海 CA 电子认证业务规则”、“上海 CA 认证业务白皮书”、“SHECA 认证业务声明”、“上海 CA 认证业务声明”、“上海 CA 中心 CPS”、“上海 CA 中心电子认证业务规则”及其类似表述，无论出现在何种场所，均应被视为是指称本文档或者是对本文档的引用。本 CPS 将会根据 SHECA 第三方电子认证服务的发展定期更新。本 CPS 的版本信息应在电子认证业务规则（CPS）后注明版本号（如“1.2 版本”或“CPS1.2”）。

，SHECA 为本 CPS 分配了自定义的对象标识符（OID）：1.2.156.112570.1.0.2 。

本 CPS 定义符合 CA/B 论坛发布的 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 的 SSL 证书的 OID 为：

1.2.156.1.112570.1.1.2.2。

SHECA 所设置的所有对象表号符及对应对象如下表所示：

OID	对象	
1.2.156.112570	万维信	UniTrust
1.2.156.112570.1	上海市数字证书认证中心	SHECA
1.2.156.112570.1.0	策略	Policies
1.2.156.112570.1.0.1	协卡网络信任服务体系证书策略	UniTrust Network Trust Service Hierarchy Certificate Policies (UNTSH CP)
1.2.156.112570.1.0.2	协卡网络信任服务体系电子认证业务规则	Certification Practice Statement
1.2.156.112570.1.0.3	协卡网络信任服务体系 EV 证书策略	EV Certificate Policy
1.2.156.112570.1.0.4	协卡网络信任服务体系 EV 证书认证业务规则	EV Certification Practice Statement

1.2.156.112570.1.1	协卡网络信任服务体系 服务器证书策略	SSL Server Certificates Policy
1.2.156.112570.1.1.1 2.23.140.1.2.1	DV 服务器证书策略	Domain Validation SSL Certificates Policy
1.2.156.112570.1.1.2 2.23.140.1.2.2	OV 服务器证书策略	Organization Validation SSL Certificates Policy
1.2.156.112570.1.1.3 2.23.140.1.1	EV 证书服务器策略	Extended Validation SSL Certificates Policy
1.2.156.112570.1.2	对象签名策略	Object Signing Policy
1.2.156.112570.1.2.1 2.23.140.1.4.1	代码签名策略	Code Signing Policy
1.2.156.112570.1.2.2 2.23.140.1.3	EV 代码签名策略	Extended Validation Code Signing Policy
1.2.156.112570.1.2.3	Windows 内核模式代码签名策略	Windows Kernel Mode Code Signing Policy
1.2.156.112570.1.2.4	Adobe 签名策略	Adobe Signing Policy
1.2.156.112570.1.2.5	文件签名策略	Document Signing
1.2.156.112570.1.3	客户端证书策略	Client Certificates Policy
1.2.156.112570.1.4	时间戳策略	TimeStamping Policy
1.2.156.112570.1.4.1	时间戳 AATL 策略	TimeStamping AATL Policy
1.2.156.112570.1.5	OCSP 策略	OCSP Policy

1.3 电子认证活动参与者

1.3.1 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 和子 CA，这些签发实体作为 CA，均可发放证书。根 CA 只签发子 CA 证书，子 CA 可签发最终用户证书或其它 CA 的证书。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，组织、个人及其它任何有明确身份标识的主体都可以成为本 CPS 声称的主体或实体）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，可以签发下一级的操作子 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 和操作子 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和证书撤销列表（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。

1.3.2 注册机构

注册机构（RA），作为电子认证服务机构授权委托的实体，负责对证书申请者进行身份标识和鉴别，初始化或拒绝证书申请和撤销请求，代表 CA 批准更

新证书或更新密钥的申请。SHECA 本身既是 CA 又是 RA，SHECA 还授权建立多家外部 RA。RA 除了为最终用户证书申请者建立起注册过程外，还要管理和服务下属受理点(RAT)。每个 RA 可以按照行业、行政地域或其它因素分成多个 RAT，对最终用户提供服务。RA 应遵循本 CPS 以及 SHECA 的授权，建立相应的 RAT。

RA 有责任妥善保存客户的数据，不允许将客户的数据透露给与证书申请无关的任何单位或个人，不允许用作商业利益方面的用途。RA 必须获得 SHECA 及其操作子 CA 的授权，根据授权从事各类证书服务，并依据授权拓展相应的下级服务机构。各类政府机构、企事业单位等均可以申请成为 SHECA 认证服务体系架构内的注册机构。

需要特别指出的是，外部 RA 机构不拥有 SHECA 的 SSL 证书和代码签名证书的相关服务操作权限，包括但不限于申请 SSL 证书和代码签名证书时的信息验证和证书签发等操作权限。

SHECA 按照申请单位的性质、证书发展预期、场地和人员情况等，经过合理的评估审计，合格后由安全认证委员会最终决定，对其发放授权委托书，授权其作为注册机构。

1.3.3 CA 证书服务受理点

证书服务受理点（RAT），简称受理点。

经过 SHECA 及其授权单位的审查，SHECA 及其授权单位可以授权某特定单位或实体成为受理点，负责办理和审批数字证书的申请、撤销、查询等证书服务。证书有关服务的申请手续、办理过程和受理要求，必须与 SHECA 正在实施的 CPS 以及 SHECA 与之签署的受理点授权协议书相一致。受理点负责向 SHECA CA 机构(SHECA 和 Sub CA)或 RA 提供证书服务申请实体的信息，包括申请实体的名称、可以表明身份的法定标识以及 SHECA 要求的任何合法的证明文件、联系方法（通信地址、电子邮件信箱、电话）等。受理点（RAT）根据这些信息为申请实体提供证书申请、证书制作、签名密钥生成、证书查询、证书撤销、证书更新等被授权的服务或根据申请实体的要求，提供申请实体任何其它合乎本 CPS 及 SHECA 公布的服务和技术支持。受理点（RAT）对其提供证书服务的受

理过程负有相关的法律责任，包括但不限于本 CPS 和授权协议中所规定的有关内容。

根据是否承担证书申请者费用的不同情况，受理点可以分为垫付型受理点和非垫付型受理点。除非特别声明，受理点通常指非垫付性受理点。

如果受理点满足和实现了 SHECA 对实行证书垫付服务的要求，并取得了 SHECA 及其授权机构的授权，则把该受理点称为垫付型证书受理点。

如果受理点没有承担证书申请者的费用（与垫付型证书受理点不同），则称该受理点为非垫付型受理点。

凡是直接向 SHECA 直接申请成为受理点的，SHECA 按照申请单位的性质、证书发展预期、场地和人员情况等，经过合理的评估审计，合格后由认证委员会最终决定，对其发放授权委托书，授权其作为注册机构。

凡是向注册机构申请成为受理点的，由注册机构决定是否授权，并不得违反 SHECA 的政策和策略。

1.3.4 证书垫付商

证书垫付商，是指能够为其所属或所服务的订户或潜在订户群体承担所有证书服务费用的团体或者组织。证书垫付商根据本 CPS 的规定、SHECA 公布的其它规定和法律、政策要求的情况，有权取缔由其支付费用的证书持有者的全部或部分证书服务，包括但不限于对持有者数字证书的取消。垫付商必须根据与 SHECA 签署的协议，事先预订证书数量并预先缴纳所有的证书费用，并可以根据 SHECA 的规定享受一定的优惠政策。垫付商必须承担其代付费用的全部证书持有者的身份真实性的责任。

1.3.5 订户

订户，即证书持有人，是指从 SHECA 接受证书的实体。包括已经申请并拥有 SHECA 签发的数字证书的个人、单位、企业、组织、机构、服务器、网站等各类主体或实体，以及其他任何具有确定的身份标识，并持有 SHECA 签发的各类证书的对象，包括任何实体或者非实体的人、物和组织等。

订户分为两类：（a）被垫付的证书持有者，其证书费用由证书垫付商承担；或（b）自支付的证书持有者，自行承担证书费用。

订户在申请证书之前，已被建议接受适当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发证机构。

1.3.6 依赖方

依赖方，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 SHECA 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，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 认证服务体系架构内的所有发证机构完全遵照 SHECA CPS 的规定签发证书。

依赖方应合理的信任证书以及相关的数字签名。如果信任数字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的信任该数字签名。

作为 SHECA 证书订户的依赖方, 享有 SHECA 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。非 SHECA 订户的依赖方，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。

1.3.7 证书申请者

证书申请者（Certificate Applicant），每一个期望作为SHECA或其下级操作子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或者其授权机构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发证机构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，并通知申请者鉴别失败，同时向申请者提供失败的原因（法律禁止的除外）。被拒绝的证书申请者可随后再次提出申请。

SHECA 及其授权的证书服务机构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发证机构为其签发证书。同时, 发证机构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。

1.3.8 其他参与者

以上未提及的，在整个 SHECA 和其服务架构内参与证书服务提供的其它实体，例如 SHECA 选定的第三方身份鉴别机构、PKI 应用技术服务提供者等等。

1.4 证书应用

1.4.1 正式证书和测试证书

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，有效期一般为 1 年。

测试证书申请者可以直接在网上申请，有效期一般不超过 3 个月。测试证书只能用于测试证书对于应用系统的适应性，以及实现证书应用目的技术可行性，不能用于任何正式的用途。特别指出，对于 SSL 可信网站，SHECA 不提供测试证书签发服务。

无论是正式证书还是申请测试证书，凡是涉及证书签发、申请、受理、操作、

管理、使用的单位和个人，应熟悉 SHECA 证书政策中的术语、条件、需求、建议以及权益等内容。

1.4.2 证书信任等级

SHECA 发放的订户证书，都需要进行严格的身份鉴别。所有申请的主体，无论是个人、单位、设备等，都必须提供证明材料以确认其真实存在，对于单位证书和设备证书，除了证明组织真实存在的材料外，还需要提供单位的授权文件。

从信任等级来看，各个根 CA 发放的订户证书是通用证书，所有的订户证书在信任程度上是一致的，没有安全保障级别的差异，没有特定的证书信任等级。但是，不同类型的证书，由于证书代表的订户主体不同，与此相应的应用要求也不同，因此应该被适当的应用到相应的用途。

1.4.3 适合的证书应用

SHECA 签发的证书，从功能上可以满足下列安全需要，除非被要求，否则 SHECA 通常并不承担该项功能的实现：

- 身份认证-保证采用 SHECA 信任服务的证书持有者身份的合法性;
- 验证信息完整性-保证采用 SHECA 数字证书和数字签名时，可以验证信息在传递过程中是否被篡改，发送和接收的信息是否完整一致;
- 验证数字签名-对信任体交易不可抵赖性的依据即数字签名进行验证。必须指出，对于任何电子通信或交易，不可抵赖性应根据法律和争议解决办法裁定。
- SHECA 证书支持机密性。机密性保证传送方和接收方信息的机密，不会泄露给其它未合法授权方。但 SHECA 对机密性事件，没有承担相应责任的义务。对于机密性用途而引发的所有直接或间接的破坏和损失，SHECA 不承担责任。

SHECA 签发的证书是通用证书，没有针对特定用途和范围进行限制，可以应用在电子政务、电子商务、社会化管理等各类网络作业活动中，以实现身份认证、电子签名等目的。按照证书类型的不同，证书都有其适用的应用。例如个人

证书用来发送签名加密邮件、个人网银业务等，单位证书用来进行 B2B 交易、网上申报税等，设备证书用来标识设备身份、进行信息通道加密等。法律法规和国家政策对此有限制的除外。证书申请者、订户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，选择自己的应用方式。任何超出本 CPS 及相应 CP 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。

1.4.3.1 身份证书的使用

身份证书分为身份证书 I、身份证书 II，标识各类单位、个人和设备的身份，可以用于各类电子政务、电子商务和其他社会信息化活动中，例如各类网上交易、支付、申报、管理、办公、访问控制等应用。

身份证书 I 只使用一对密钥对，用于进行签名、对签名进行验证、信息加密和解密。

身份证书 II 使用两对密钥对，一对为签名密钥对，用于进行签名、对签名进行验证；一对为加密密钥对，用于信息加密和解密。

1.4.3.2 电子邮件证书的使用

电子邮件证书标识用户的电子邮件地址，主要用于电子邮件的数字签名、加密，以及非商业性、政务性的访问控制，不得用于各类交易、支付、或者需要明确的用户身份验证的应用。

1.4.3.3 代码签名证书的使用

代码签名证书标识软件代码的来源或者所有者，只能用于各类代码的数字签名，不得用于各类交易、支付、加密等应用。

代码签名证书订户必须承诺，不得将代码签名证书用于对恶意软件、病毒代码、侵权软件、黑客软件等的签名。

1.4.3.4 SSL 证书的使用

SSL 证书标识 Web 网站或者 Web 服务器的身份，可以用于证明网站的身份或者资质、提供 SSL 加密通道，不得用于各类交易、支付的签名或验证。

除非在本 CPS 中特别声明, SHECA 没有义务承担因任何使用证书而产生的额外的经济赔偿责任。

1.4.4 限制的证书应用

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。例如，个人证书不能作为单位证书和设备证书来使用，单位证书不能作为个人和设备证书来使用，设备证书也不能作为个人和单位证书来使用。任何不符合的应用，不受本 CPS 的保护。

证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用，否则由此造成的法律后果由用户自己承担。特别的，证书不被设计用于、不打算用于、也不授权用于涉及人身伤害、环境破坏等的应用系统中，例如导航或通讯系统、交通控制系统或武器控制系统等。

1.5 策略管理

1.5.1 策略文档管理机构

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 制定本电子认证业务规则（CPS），并指定专门的机构——SHECA 安全认证委员会作为策略的管理机构。

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）及相应的 CPS 编写人员组成，负责审核批准 CPS，并作为 CPS 实施检查监督的最高决定机构。

SHECA 战略发展中心作为 CPS 的工作机构，负责起草 CPS 并根据要求提出修改报告，并负责此方面的对外咨询服务。

1.5.2 联系人

SHECA 将对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中心。

电话：86-21-36393197

传真：86-21-36393200

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

1.5.3 决定 CPS 符合策略的机构

作为电子认证业务的主管部门，工业和信息化部发布了《电子认证业务规则规范》，SHECA 根据规范的要求，制定本电子认证业务规则（CPS），并提交工信部备案。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，负责批准和决定本 CPS 是否符合相应 CP 的规定。

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。

战略发展中心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，保证 SHECA 认证服务体系内的运行符合本 CPS 的要求。

1.5.4 电子认证业务规则的发布

电子认证业务规则的发布方式包括：

1、以电子的方式，在 SHECA 网站的资料库中发布，网站地址：

https://www.sheca.com/repository

2、以电子的方式，通过电子邮件获取，电子邮箱地址：

getcps@sheca.com

3、以书面的方式，由 SHECA 公司战略发展中心发布。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

1.5.5 电子认证业务规则的变更和发布

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和为适应 CA/浏览器论坛（CA/Browser Forum）最新 Guidelines、Baseline Requirement、以及 Minimum Requirements for Code Signing Certificates 的修改，预期修改包括每半年一次检查电子认证业务规则与 CA/浏览器论坛最新 Guidelines、Baseline Requirement 以及 Minimum Requirements for Code Signing Certificates 是否符合，对于电子认证业务规则的不符合处立即进行更新。修改过的电子认证业务规则，将根据电子认证服务管理办法的要求，在规定的时间内向工信部进行备案。

在本 CPS 作出任何变动之前，SHECA 安全认证委员会将对战略发展中心提供的变更建议报告进行研究，最终作出变更的决定。

SHECA 将在决定形成决议后，在 SHECA 网站公布变更后的 CPS。对本 CPS 所做的修改，将于 SHECA 发布之日起立即生效，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。

SHECA 将对 CPS 进行严格的版本控制。修改后的版本在 SHECA 网站上公布（https://www.sheca.com）。

1.5.6 CPS 批准程序

SHECA 的 CPS 由战略发展中心起草拟订后，提交 SHECA 安全认证委员会审核。如果因为标准的变化、技术的提高、安全机制的增强、运营环境的变化和法律法规的要求等对 CPS 进行修改，由战略发展中心提交修改建议报告，提交 SHECA 安全认证委员会审核。经过该委员会批准后，SHECA 通过 https://www.sheca.com 进行公布。

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》的规定，

SHECA 在公布 CPS 后向工信部备案。

1.6 定义和缩写

1.6.1 SHECA

上海市数字证书认证中心有限公司的缩写。

1.6.2 协卡网络信任服务体系

由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）建设、运营的一个公开密钥基础设施，简称协卡认证，提供基于数字证书的电子认证服务。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，致力于创建和谐的网络信任环境，向互联网用户提供安全、可靠、可信的数字证书服务。

1.6.3 SHECA 安全认证委员会

SHECA 认证服务体系内的最高策略管理监督机构和 CPS 一致性决定机构。

1.6.4 电子认证服务机构

SHECA 及授权的下级操作子 CA 被称为电子认证服务机构（Certificate Authority，CA），也就是证书认证机构，是颁发证书的实体。

1.6.5 注册机构

注册机构（Registration Authority，RA）负责处理证书申请者和证书订户的服务请求，并将之提交给认证服务机构，为最终证书申请者建立注册过程的实体，负责对证书申请者进行身份标识和鉴别，发起或传递证书撤销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。

1.6.6 受理点

受理点（Registration Authority Terminal，RAT）是受理证书服务的终端机构，作为 SHECA 认证服务体系架构内直接面向用户的服务主体，经过 CA 或 RA 的

授权从事各类服务。

1.6.7 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。

1.6.8 录入员

负责录入证书申请者提交的信息，协助用户办理数字证书申请、撤销、更新等手续。

1.6.9 审核员

负责审核证书申请信息，协助用户办理数字证书申请、撤销、更新等手续。

1.6.10 证书制作员

负责为证书申请者下载制作证书，并提交给用户。

1.6.11 证书

证书，指电子签名认证证书，电子认证服务机构签发的用以证明证书持有人的电子签名、身份、资格及其他有关信息的电子文件。

1.6.12 数字证书

使用数字签名作为识别签名人身份和表明签名人认可签名数据的一种电子签名认证证书。本 CPS 中提及的证书为数字证书，包括签名证书和加密证书等。

1.6.13 电子签名

简称为签名，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。

1.6.14 数字签名

通过使用非对称密码加密系统对电子数据进行加密、解密变换来实现的一种电子签名。本 CPS 中提及的签名为数字签名。

1.6.15 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名义实施电子签名的人。

1.6.16 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。

1.6.17 私钥（电子签名制作数据）

在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。

1.6.18 公钥（电子签名验证数据）

是指订户验证电子签名的数据。

1.6.19 订户

从电子认证服务机构接收证书的实体，也被称为证书持有人。在电子签名应用中，订户即为电子签名人。

1.6.20 依赖方

依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

1.6.21 证书垫付商

是指能够为其所属或所服务的订户或潜在订户群体承担所有证书服务费用的团体或者组织，是一种特殊的证书服务受理点。

2.信息发布与信息管理

2.1 SHECA 信息库

SHECA 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。SHECA 信息库内容包括但不限于以下内容：CP、CPS 等策略类文档的现行和历史版本、证书、CRL，以及其它由 SHECA 不定期发布的信息。SHECA 信息库不会改变任何从发证机构发出的证书和任何证书撤销的通知，而是准确描述上述内容。

处理任何与 SHECA 相关的事宜时, SHECA 必须使用 SHECA 信息库作为主要的和正式的信息库。

SHECA 信息库将及时发布包括证书、CPS 修订和撤销的通知和其它资料等内容，这些内容必须保持与 CPS 和有关法律法规一致。SHECA 信息库可以通过网址： https://www.sheca.com/repository/ 访问，或由 SHECA 随时指定的其它通讯方法获得。SHECA 可在 SHECA 信息库外颁布订户证书和相关 CRL 资料。除 SHECA 授权者外，禁止访问资料库（或其它由发证机构维护的数据）中任何被 CPS 和/或 SHECA 信息库宣布为机密信息的资料。

2.2 认证信息的发布

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。SHECA 将及时公布新的信息。只有 SHECA 有权处理网站上的旧信息。

2.2.1 目录服务

在订户接受证书时，SHECA 同时公布一份该证书的副本。该发证机构还公布有效期内被撤销的证书。SHECA 通过目录服务发布证书和证书撤销的相关信息，用户可以通过访问 SHECA 目录服务器获取这些信息。同时还提供在线证书状态查询、证书撤销查询服务等。

2.1.2 公告和通知的发布

SHECA 将及时将电子认证业务业务规则、业务流程、技术和产品的变化等，通过公告和通知的形式在网站 https://www.sheca.com 上发布，同时，SHECA 也将会根据需要采取其他可能的形式进行发布。

SHECA 根据新的技术发展，会公布保护证书持有者私钥可能的有效措施。

2.3 发布的时间和频率

2.3.1 电子认证业务规则的发布时间和频率

SHECA 将及时发布电子认证业务规则（CPS）的最新版本，一旦对规则的修改、补充、调整等获得批准，SHECA 将在 https://www.sheca.com 上发布，并将最新的 CPS 发布在 SHECA 信息库内，并与原有 CPS 共同列出，以便检索。CPS 至少每年更新一次。

SHECA 根据技术进步、业务发展、应用推进和法律法规的客观要求，决定对 CPS 的改动，其发布时间和频率将由 SHECA 独立做出决定。这种发布应该是即时的、高效的，并且是符合国家法律法规的要求。

在 SHECA 没有发布新的 CPS，或者没有任何形式的公告、通知等形式宣布对 CPS 进行修改、补充、调整或者更新前，当前的 CPS 即处在有效的和正在实施的状态。只有 SHECA 有权利对这种状态进行任何形式的改变。

2.3.2 证书的发布时间和频率

一旦订户接受证书，发证机构将在 SHECA 的信息库和由 SHECA 和发证机构决定的其它一个或多个信息库里发布证书的副本。订户也可以在其它信息库中公布他们获得的 SHECA 证书。

证书签发后即发布到目录服务器 ldap2.sheca.com 上，可使用专业工具进行查询。用户还可以通过 https 的方式，在 https://www.sheca.com 查询获得证书。

2.3.3 CRL 的发布时间和频率

发证机构在撤销证书后，必须立即在 SHECA 信息库中发出撤销的公告。SHECA 将公布一项或多项以下内容：发布撤销证书的清单，该清单可通过安全通道索取。

通过 OCSP 协议，请求者可以实时查看和获得某一证书的状态，包括有效、被撤销。在满足要求以后，SHECA 还可以提供跟进服务，当指定的证书被撤销时，SHECA 将按照约定的方式通知请求该项服务请求者。

所有被撤销的证书列表 CRL，通过 SHECA 的 HTTP 服务、目录服务器等进行发布。SHECA 根据以下规则更新和发布证书撤销列表（CRL/ARL）：

对于订户证书应至少每 5 天一次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）字段的差必须小于等于 7 天。

对于根/中级根证书应至少每 6 个月一次或在根/中级根证书被撤销后的 24 小时内公布 ARL。根/中级根证书 ARL 的下次更新时间（nextUpdate）字段与本次更新时间（thisUpdate）字段的差必须小于等于 10 个月。如根/中级根证书被撤销，SHECA 将在网站公布相关撤销信息。

在紧急情况下，SHECA 可自行决定公布证书撤销列表的时间和频率。

2.3.4 公告、通知等信息的发布时间及频率

一旦需要就某些原因发布和电子认证服务相关的公告和通知，SHECA 将实时在 https://www.sheca.com 上发布。

这类信息的发布是不定期的，SHECA 将保证会在第一时间发布信息。

2.3.5 用户服务、业务架构、市场发展等信息的发布时间及频率

SHECA 将会随时在 https://www.sheca.com 网站上公布相关信息。

2.4 信息库访问控制

2.4.1 SSL 通道

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）。

2.4.2 权限管理和安全审计通道

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.身份标识与鉴别

3.1 命名

3.1.1 名称类型

认证机构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 生成或者签发的证书的主要识别名称（SubjectName），采用 X.501 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题中，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。

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白无误地表示出来。命名可以由 SHECA 和申请者协商解决，也可以由申请者独立完成。

3.1.2 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。但是，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、单位或者设备）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。

3.1.3 订户的匿名或伪名

本 CPS 中明确声明，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。除非在某些具有特殊要求的电子政务应用中，

可以允许 SHECA 按照一定的规则为用户指定特殊的名称，并且，SHECA 能够把该类特殊的名称与一个确定的实体（个人、单位或者设备）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。

3.1.4 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 DN 的内容格式都符合 X.500 的命名规则。下面是一般识别名称的命名规则：

识别名称（DN）	说明	内容（示范性）
1、Country(C)	公司所在国家名称	C=CN
2、Organization(O)	公司名称	O=SHECA
3、Organization Unit（OU）	单位或部门名称	OU=技术支持中心
4、Common Name（CN）	证书持有者的一般通用名称	CN=张山

详细的 DN 选用项说明可参照本 CPS 附录中 SHECA 证书格式中关于主题（SUBJECT）中选项的说明。

唯一标识项的命名规则由 SHECA 定义，命名参见本 CPS 附录中有关 SHECA 证书自定义扩展项的说明。

3.1.5 名称的唯一性

名称对 SHECA 的所有证书持有者，要求必须都是唯一的。SHECA 根据该名称有效的鉴别证书持有者。当出现相同的名称时，以先申请者优先使用，后申请者在唯一标识名称后面加识别码予以区别。

3.1.6 名称纠纷的处理

当订户或者申请者使用的名称相同时，SHECA 以首先申请注册的用户优先使用。SHECA 没有权利和义务处理因此产生的相关纠纷，相关用户可以向有关主管部门申请解决。

当订户或者申请者的名称，经有关主管部门的合法文件证明为其他订户或者申请者所有时，SHECA 将即刻注销先前用户对该名称的使用权，并撤销该用户申请的证书。该用户必须承担因此产生的法律责任。验证订户或者申请者使用该名称的合法性，并不在 SHECA 的业务职责范围。

3.1.7 命名机构

命名机构，即 SHECA 命名机构，协调所有 SHECA 相关甄别名的签发（Relative Distinguished Names，简称 RDN ）。 SHECA 命名机构为 SHECA 信息库中的主体名称确定了命名约定，该约定可能因证书类别和发证机构的不同而不同。这些命名约定也可因签发证书和再签发/再注册证书之间的不同而不同。

SHECA 命名机构有权指定其所发行的证书中的相关甄别名 (RDN)和证书序列号。SHECA 命名机构在指定相关甄别名时会要求申请者提供有关甄别名的使用权证明材料，或向相应的机构查询，以确定订户是否有权使用相应的甄别名。

3.1.8 商标的识别、鉴别和角色

在订户的证书中允许包含商标信息，但是不能用于对个人、单位或者设备等实体身份的标识。在证书信息中包含商标时，应向 SHECA 提供商标注册方所有权的文件证明，这种要求不是也不应该被认为是 SHECA 将对商标的归属进行判断和决定。

SHECA 尊重任何订户名称中的注册商标权，任何证书申请者不应使用任何可能侵犯知识产权的名称。SHECA 不对证书申请者是否拥有命名的知识产权进行判断和决定，也不负责解决证书中任何关于域名、商标等知识产权的纠纷，并且不保证这种权利的唯一性。对于因商标、服务标志等的归属问题造成的纠纷，SHECA 没有权利，也没有义务去拒绝或者质疑任何可能导致产生知识产权纠纷的证书申请，不负有仲裁或调停等责任，这不在 SHECA 的业务职责范围之内。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

SHECA 必须验证申请者拥有私钥的合法性和正确性。至少通过以下任何一

种方法验证申请者的私钥:

1、 在用户申请证书，以私钥对申请信息进行签名时，SHECA 及其授权的服务机构必须验证申请者申请信息内受保护的申请者身份信息、公钥和私钥的正确性、合法性和唯一性。

2、 SHECA 及其授权的服务机构为证书申请者提供完成证书申请所需要的初始化信息（如密码信封）。证书申请者在申请证书或证书的某些操作中必须使用这些初始化信息，向 SHECA 确保其是私钥的合法所有者。初始化信息一般通过离线的方式，安全地递交给证书申请者。

3.2.2 组织机构身份和域名的鉴别

SHECA 需要对证书申请者的身份进行程序性的鉴别，包括但不限于验证用户提供的身份证明材料、通过第三方进行调查、通过公共数据库调查、邮政地址调查等等。

SHECA 首先会要求申请者对其递交的材料作真实性声明，并承担相应的法律责任。SHECA 会按照本 CPS 的规定，对材料进行鉴别。SHECA 也可能采取附加的或者额外的方式进行这种鉴别。

如果申请者拒绝 SHECA 的身份鉴别要求，那么就被视作放弃对证书的申请。同时 SHECA 声明，SHECA 可以拒绝任何申请请求，并且没有对此说明原因的义务。

3.2.2.1 机构身份的鉴别

组织机构申请者身份的鉴别流程，会根据申请证书种类的不同而不同，SHECA 可以按照每种证书相应的要求进行不同的验证。如通过证明 e-mail 的有效性、 查询可信的数据库验证真实性、面对面鉴别身份材料以及其它可以获得申请者明确的身份信息的方式等；相应的证书申请流程规定了不同的鉴别程序。证书申请表上有申请者本身或被充分授权的证书申请者代表的签字。

在申请组织机构证书时，申请者应指定证书申请代表，并对其合法授权，证书申请代表在证书的申请表上签字表示接受证书申请的有关条款，并承担相应

的责任。SHECA 及其证书服务机构审核单位证书申请者的代表人是否符合要求。

对组织机构的身份鉴别按以下方式进行：

SHECA 或其注册机构、受理点等证书服务机构必须检查申请者所递交的文件，申请者需向 SHECA 提供机构或服务器确实存在的有效证明，包括但不限于营业执照等；申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。SHECA 可以通过查询第三方数据库或咨询相应的政府机构等方式，来对申请者及其申请材料进行验证。如果需要，SHECA 可以通过从第三方得到的电话号码等其他联络方式，用某种方式与申请机构进行联络以确认某个信息（例如，验证代理人的职位或者验证申请表中的某个人是否是申请人）。如果 SHECA 无法从第三方得到所有需要的信息，可要求第三方进行调查，或要求证书申请者提供额外的信息和证明材料。

若申请者在申请一张证书前已持有其他 SHECA 为其签发的身份证书，SHECA 及其注册机构可以通过验证申请者已持有有效身份证书的方式进行身份鉴别。例如，在 SHECA 的在线服务平台上通过身份证书登录该平台。

在域名、设备名称或者邮件地址被作为证书主题内容申请证书时，还需要合理验证该组织是否拥有该权利，例如要求提交域名所有权文件、归属权证明文件、查询第三方数据库、发送确认电子邮件等。

对于批量申请的单位身份证书，若经办人代表某单位为其内部各部门、实行控制的子公司或特定系统使用方申请仅限于组织机构内部使用的证书，由组该单位作为申请人统一申请。

除通过其他 SHECA 签发的身份证书验证身分外，需由经办人提供个人身份证件，填写申请表或批量申请表加盖申请人公章，列明需申请单位信息。

对证书中列示的信息，若为具有公信力的单位证照号码，按本章节要求进行身份鉴别。请参见《单位及个人证书申请审核指南》。

如果 SHECA 或其注册机构、受理点等证书服务机构已经预先明确了证书申请单位的身份，那么 SHECA 和其授权的证书服务机构可以信赖申请者提供的证明。

这种身份鉴别，通常是通过现场的方式进行。SHECA 也支持通过邮递的方式进行身份的鉴别，但是对此类的方式，SHECA 将会要求申请者提供额外的身份鉴别资料和证明，并通过电话、第三方调查、邮政地址调查等 SHECA 以为合理的方式辅助进行鉴别。

SHECA 和其授权的证书服务机构在规定期限内保存组织机构的全部申请材料，这个规定期限由法律、政策、主管部门的要求或者 SHECA 自行决定。

若某组织机构为其内部员工、内部机构等非法律实体申请职位证书，则对证书中录入的证书持有人信息以通过审核的组织机构提供的内容为准。职位证书仅用于组织机构内部的身份识别。

3.2.2.2 DBA/商业名称的鉴别

不适用。

3.2.2.3 国家的鉴别

如果 SHECA 签发的证书主题中包含国家代码，SHECA 会通过下列方法中的一种或多种方式进行验证:

1. 从 DNS 记录中获取到的 IP 地址所在国家;
2. 申请域名的 CCTLD;
3. 通过 3.2.2.1 中的方法查询政府机构或其他可信第三方数据源确认申请者的地址所在的国家。

3.2.2.4 域名的确认和鉴别

如果证书的名称为域名，除了在对申请者递交的书面材料进行审核外，SHECA 需要验证申请者拥有所申请证书中的域名控制权，以确定申请者是否有权使用相应的域名。即验证时，SHECA 需要执行以下流程:

1. 对于.onion 形式的域名，SHECA 拒绝签发证书;
2. 通过下述方法之一，进行域名控制权验证:

   (1) 直接与域名注册商验证申请人是域名联系人，并确认SHECA已执行以下操作:

a) 按照Baseline Requirements 章节3.2.2.1 or EV Guideline 章节11.2要求执行了申请者的身份鉴别。

b) 按照Baseline Requirements 章节 3.2.5 or EV Guideline 章节11.8执行了申请人代表/证书批准人的授权审核。

c) 此方法需按照BR章节3.2.2.4.1执行。

d) 从2018年8月1日起，SHECA将停止使用该方法进行验证，已按此方法完成的验证不能签发证书。

(2) 通过邮件、传真、SMS或邮递将一个随机值发送给域名联系人，并受到使用该随机值的确认回复，以验证申请人对域名的控制权，按照BR章节3.2.2.4.2执行。

(3) 给域名联系人发送构建邮件，通过将一封包含随机值的邮件发送给由‘admin’，‘administrator’，‘webmaster’，’hostmaster’或‘postmaster’作为前缀加上符号@，以授权域名为尾缀的邮箱，并受到使用该随机值的确认回复，以确认其申请人对正是域名的控制，按照BR章节3.2.2.4.4执行。

(4) 通过确认申请人发起域名证书申请的授权书来确认申请人的域名控制权，SHECA需确认域名授权文档来自于域名联系人，并且确认：①域名授权书在域名验证请求发起时或发起后，②WHOIS信息自域名授权文件提供之后未发生变化。按照BR章节3.2.2.4.5执行。从2018年8月1日起，SHECA将停止使用该方法进行验证，已按此方法完成的验证不能签发证书。

(5) 申请人更改其申请域名网站，建“/.well-known/pki-validation”目录，将请求码或随机值放置在文件目录中的方式验证，此方式按照BR3.2.2.4.18条执行。在验证过程中SHECA不使用重定向。

通过验证在文档内容中包含请求令牌或随机值:

a. 完整的请求令牌或随机值不能在用于检索文件的请求中出现

b. CA必须从请求中接收到了成功的HTTP响应（即接收到2xx HTTP状态码)

包含请求令牌或随机值的文件：

a. 必须被存放在授权域名上

b. 必须被放置在“/.well-known/pki-validation”目录

c. 必须经过“http”或"https"被检索

d. 必须通过授权的端口获取

每个证书请求中使用的随机值均是唯一的。随机值有效期为30天。在确认响应时，随机值在有效期内。

(6) 更改DNS通过确认DNS CNAME、TXT或CAA记录中存在的随机值或请求码，以授权域名或以下划线字符开头的标签为前缀的授权域名的方式，此方式按照BR第3.2.2.4.7条执行

自2020年6月3日开始，本方法不再适用。已用本方法验证的域名控制权，可在397天内复用。

(7) 通过确认完整域名名称在DNS A或AAAA记录查询中返回的IP地址的控制来确认申请人对域名的控制。按照BR章节3.2.2.4.8执行。

(8) 针对上海市政务外网域名，即以sh.cegn.cn结尾的域名，因上海市政务外网域名统一管理部门，即实际控制人为上海市大数据中心，认可加盖公章的申请文件。

上述方法中用到的随机值的有效期为从产生该随机值开始的 30 天。

上述验证方法，除 IP 地址（BR 章节 3.2.2.4.8）的方法外均可用于通配符证书的域名验证。

3.2.2.5 IP 地址的确认和鉴别

根据 CABForum 的要求，SHECA 不为 IANA 标注的 Reserved IP 签发证书。SHECA 将对在证书中列出的所有 IP 进行所有权的验证。

如果证书的名称为 IP 地址，除了在对申请者递交的书面材料进行审核外，SHECA 需要申请者提供额外的 IP 地址使用权证明材料，或 SHECA 还需向该 IP 地址注册服务机构或者其它权威第三方数据库查询，以确定申请者是否有权使用该 IP 地址。即验证时，SHECA 需要执行以下流程：

1 确认该 IP 地址不是内网 IP 地址，SHECA 拒绝为内网 IP 地址签发 SSL 证书

2 通过下列方式之一验证申请人对 IP 地址的控制：

(1) 通过验证指定网页上的包含 IP 地址的统一资源标识符的协商信息

(2) 通过互联网地址分配机构（IANA）或地区的互联网注册商（RIPE,APNIC,ARIN,AfriNIC,LACNIC）的 IP 地址分配文件验证

(3) 通过执行逆向 IP 地址查询后，以 3.2.5 中的域名验证方式验证返回的域名。

3.2.2.6 通配符域名的确认和鉴别

通常情况下，对于通配符“*”右侧直接接顶级域名的申请，除非申请者能够有效证明其对于该顶级域名的所有命名空间的控制权，否则 SHECA 将拒绝该类申请。

同时，SHECA 将通过“3.2.2.5 域名的确认与鉴别”来核实该通配符右侧的域名确实已经被有效注册，并归属于该申请者。

此外，必要时 SHECA 还将采取其它的审核方法，如访问由 Mozilla 维护的公共后缀清单（public suffix list http://publicsuffix.org/ ）来确认申请域名的归属权，申请者有义务协助 SHECA 进行相应的审核。

3.2.2.7 数据源及其准确性

SHECA 在使用任何数据源作为可靠的数据源之前，将对该来源的可靠性、准确性，及更改或伪造可抗性进行评估，遵守 CAB 论坛 BR 第 3.2.2.7 节，EV Guidelines 第 11.11 节对数据源的要求，即 SHECA 将考虑以下几个方面：

1 所提供的信息的年限；

2 该数据源更新的频率，确保数据保持更新；

3 数据的供应方，以及数据收集的目的；

4 数据的公开可用性及可访问性；

5 伪造或更改数据的难度。

对于 SSL 证书的验证数据源，若 SHECA 获得可依赖数据或文件的时间不超过 397 天,则可复用。

3.2.2.8 认证机构授权（CAA）

对于 SHECA 颁发的公共可信任的 SSL 证书，在证书签发之前，SHECA 将对待签发证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查。SHECA 将在查询 CAA 记录的 8 小时内，向证书申请者发放证书。若超过 8 小时，SHECA 将重新进行 CAA 检查。

SHECA 根据 RFC8659 的规定处理“issue”、“issuewild”及“iodef”的属性标签：若“issue”、“issuewild”标签中不包含“sheca.com”，“imtrust.cn”和“wwwtrust.cn”，则 SHECA 不签发对应的证书；当证书的请求或签发违反了 SHECA 或 FQDN 所有者的安全策略时，若 CAA 记录中出现“iodef”标签，则 SHECA 将与申请人沟通后再决定是否为其颁发证书。

SHECA 以下列 CAA 记录查找失败情况作为可签发证书的条件：

1) 在非 SHECA 的基础设施中查询 CAA 记录失败；

2) 至少尝试过一次重新查找 CAA 记录；

3) 域名所在区域不存在指向 ICANNA 根区域的 DNSSEC 验证链。

3.2.2.9 电子邮件的审核

当邮件地址被作为证书主题内容申请证书时， SHECA 应对该邮件地址的有效性进行确认，并审核申请者对邮件地址的使用权，只有通过审核后才可在证书中签入 email 项。具体的审核步骤如下：

1. 申请者完成生成证书申请请求文件后，系统检测到邮件地址则自动向该邮件地址发送随机值，随机值由系统产生，并且唯一；

2. 申请者收到邮件并回复该随机值进行确认；

3. SHECA 系统收到回复，并将回复中的随机值与发送的随机值进行比对，若结果一致，则电子邮件审核通过。

在收件人及邮件整体内容不作任何改变的前提下，带有原随机值的邮件可以被重复发送。邮件中的随机值自生成当天开始，有效期不应超过 30 天。

3.2.3 个人身份的鉴别

个人申请者身份的识别流程，会根据申请证书种类的不同而不同，SHECA 可以按照每种证书相应的要求进行不同的验证。如通过证明 e-mail 的有效性、查询可信的数据库验证真实性、面对面鉴别身份材料以及其它可以获得申请者明确的身份信息的方式等；相应的证书申请流程规定了不同的鉴别程序。证书申请表上有申请者本身或被充分授权的证书申请者代表的签字。

1、证明 e-mail 的有效性。通过审核和验证证书持有者的 e-mail 地址真实存在性来识别和鉴定个人的身份。

2、查询可信的信息数据库。通过核对和证实可信的数据库内必要的个人特征,识别和鉴定个人身份。由 SHECA 来选择和决定可信的数据库，包括现存的 SHECA 数据库和其它第三方的数据库。

3、面对面鉴定。个人申请者的识别和鉴别可以通过以下方法中的一种来进行:

SHECA 和其授权的证书服务机构将申请者本人和两份身份证明（原件和复印件）进行比较。身份证明文件必须是有效的身份证，或护照证件等。

如果 SHECA 或受理点已经明确确认申请者个人的身份, 那么 SHECA 或其授权的证书服务机构可以信任现有的证明。

4、SHECA 还可以通过从第三方获取的信息来验证该申请者个人的身份，如果 SHECA 无法从第三方得到所有所需的信息，可要求第三方进行调查，或要求申请者提供额外的信息和证明材料。

5、SHECA 也支持通过邮递的方式进行身份的鉴别，但是对此类的方式，

SHECA 将会要求申请者提供额外的身份鉴别资料和证明，并通过电话、第三方调查、邮政地址调查等 SHECA 认为合理的方式进行辅助鉴别。

6、对于以某个组织中的个人身份名义申请的，还需要提交其所在单位提供的证明材料。

7、在域名、设备名称或者邮件地址被作为证书主题内容申请证书时，还需要合理验证该个人申请者是否拥有该权利，例如要求提交域名所有权文件、归属权证明文件、查询第三方数据库、发送确认电子邮件等。

8、对于组织内部个人身份证书，仅限于组织机构内部使用，由组织机构作为申请人统一申请，实际使用人为单位员工个人。

9、若申请者在申请一张证书前已持有其他 SHECA 为其签发的身份证书，SHECA 及其注册机构可以通过验证申请者已持有有效身份证书的方式进行身份鉴别。例如，在 SHECA 的在线服务平台上通过身份证书登录该平台。

除第 9 种方式外，由经办人提供个人身份证件，填写申请表或批量申请表加盖申请人公章，列明个人身份证书信息，对列示在证书中的信息，若为组织内部使用的身份标识则不需额外检验；若为具有公信力的身份证件信息，按本章节要求进行身份鉴别。请参见《单位及个人证书申请审核指南》。

申请者必须承担材料真实性的责任，SHECA 和其授权的证书服务机构在进行了法律规定的有限审查以后，不承担对申请者的身份证明文件（如身份证等）进行合法性甄别的义务。

SHECA 和其授权的证书服务机构保存证书持有者在申请表中填写的详细信息。

3.2.4 没有验证的订户信息

通常，除了该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，下列信息时在申请时是可以不被要求验证的：

- 个人和单位身份证书中的电子邮件地址
- 证书中任何其它不被要求验证的信息

对于没有验证过的订户信息，SHECA 将对申请信息以书面或电子形式进行归档。SHECA 将不承诺这类信息的真实性，并且不承担由于这类信息的不真实、不完整等引起的任何责任和解决纠纷的义务。

3.2.5 授权确认

在个人委托他人代理申请或者组织机构委托其被授权人申请某一类型的证书时，SHECA 和其授权的证书服务机构还需审核申请人的身份和资格，包括必需的身份资料和授权证明，并且通过电话、信函或其他方式与其代表的实体进行核实确认，以审核其是否有权代表那个实体。

SHECA 可通过从第三方得到的电话号码等其他联络方式，用某种方式与组织机构进行联络以确认授权申请人的某个信息（例如，验证代理人的职位或者验证申请表中的某个人是否是申请人）。如果 SHECA 无法从第三方得到所有需要的信息，可要求第三方进行调查，或要求证书申请者提供额外的信息和证明材料。

3.2.6 互操作准则

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 UNTSH CP 要求，并且与 SHECA 签署相应的协议。SHECA 将依据协议的内容，接受非 SHECA 的发证机构鉴别过的信息，并为之签发相应的证书。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接受这些被鉴别审核过的资料，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 密钥更新请求的标识与鉴别

订户证书到期时，为了能够继续使用证书，订户需要获得一张新的证书。密钥到期后，用户可以选择更新（重新产生一组公钥和私钥密钥对），并向发证机构申请重新签发证书，这称之为证书密钥更新（re-key）；也可以选择保留原有密钥，向发证机构申请签发新的证书，SHECA 使用这一已经存在的密钥对为其签发新的证书，这称之为证书更新(renewal)。

通常，我们在表述证书更新（certificate renewal）时包含了证书密钥更新（re-key）和证书更新（renewal），其重点在于旧的到期证书已经被新的证书所代替，并不关注其中的密钥对是否进行了更替，是否产生了新的密钥对以取代旧的密钥对。除了一些可能的特定应用外，在证书更新时是否产生新的密钥对通常并不是重点。但是 SHECA 通常要求订户在更新证书时使用新的密钥对。当订户对密钥的安全性有顾虑时，必须重新注册、产生新的密钥对，并向发证机构申请重新签发证书。在这种情形下，为了风险管理和安全考虑，重新申请签发证书时，订户将不被允许使用旧的密钥对。

如果与证书相关的信息发生变化，订户可以选择保留原有密钥对或者使用新的密钥对重新签发证书。如果选择保留原有密钥对，订户需要保证其密钥对的安全性没有受到威胁。

国家主管部门对密钥的管理、更新等有规定的，SHECA 将严格予以执行。

3.3.1 常规密钥更新的标识与鉴别

对于证书有效期结束后的常规密钥更新，订户可以用原有的私钥对更新请求进行签名。发证机构将会对用户的签名和公钥、更新请求内包含的用户信息进行正确性、合法性、唯一性的验证和鉴别。

常规密钥更新的标识和鉴别包括：

- 订户对申请信息进行签名，CA 用其原有证书中的公钥对签名进行验证
- 订户注册信息没有发生变化，CA 基于其原有注册信息对其进行签发新的证书

订户也可以选择一般的初始证书申请流程进行常规密钥更新，按照要求提交相应的证书申请和身份证明资料。SHECA 在任何情况下都可将这种初始证书申请的鉴别方式作为密钥更新时的鉴别处理手段。

国家主管部门对密钥的管理、更新等有规定的，SHECA 将严格予以执行。

3.3.2 撤销后密钥更新的标识与鉴别

发证机构不提供证书被撤销后的密钥更新。订户必须重新进行身份鉴别和注

册，并生成新的密钥对，向 SHECA 申请重新签发证书。

3.4 撤销请求的标识与鉴别

SHECA 和其授权的证书服务机构对证书的撤销请求需要予以现场的身份鉴别验证。订户需要到 SHECA 及其授权的证书服务机构，递交和申请证书时相同的身份资料、证书和私钥进行身份鉴别。

如果由于条件的限制无法进行现场审核时，SHECA 将通过合理的方式，例如通过电话、邮递、其他第三方的证明等，对申请者的身份予以鉴别验证。

如果是司法机关依法提出撤销，SHECA 将直接以司法机关书面的撤销请求文件作为鉴别依据，不再进行其他方式的鉴别。

SHECA 保证对于撤销请求的鉴别，予以合理的进行。

3.5 授权服务机构的标识与鉴别

对于授权加入的各类证书授权服务机构，包括注册机构 RA 和服务受理点，SHECA 为其分配唯一的编号和操作权限，并依据此编号对其进行管理。

SHECA 为每一个 RA 签发一张数字证书，作为该 RA 的在证书系统内的唯一身份标识。CA 系统根据 RA 的签名，对 RA 进行身份的鉴别，以判断该 RA 是否为 SHECA 认可的机构，具有何种权限，是否接受其上传的各类服务请求和服务信息。

SHECA 为每个受理点的操作员签发一张数字证书，同一个受理点的操作员被分配在一个操作组内，该操作组的编号就是受理点的编号。CA 系统（包括 RA 系统）根据受理点的签名，对其进行身份的鉴别，以判断该受理点是否为 SHECA 认可的机构，具有何种权限，是否接受其上传的各类服务请求和服务信息。

4. 证书生命周期操作要求

本章阐述了在 SHECA 认证服务体系架构下，根据公布的 CPS 实施证书的申请、签发、管理、更新、撤销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。

SHECA 数字证书支持安全电子商务、安全电子政务和其他的一般安全服务，以满足订户对于电子签名及其它网络安全服务技术的需要。为此，SHECA 及其授权的发证机构作为可信的第三方，完成订户关于证书服务的各个过程，以满足众多的、公开的、广泛分布的订户对通讯与信息安全的多种需要。

4.1 证书申请

SHECA 接受离线申请和在线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，但都应遵守证书申请操作所规定的步骤。

4.1.1 证书申请实体

在证书申请的过程中，参与整个申请过程的实体主要包括：

1、证书申请者，包含个人、企业单位、事业单位、政府机构、社会团体、人民团体等各类组织机构。任何合法的组织、个人和有明确身份归属的其他网络主体均可申请数字证书，以保证网上交易和网上行政作业的安全和可靠。

2、SHECA 授权服务受理机构，包括 RA、RAT 以及证书垫付商等，以及相应的系统、系统管理员、操作员等。

3、电子认证服务机构，包括 SHECA 以及 SHECA 授权的下级操作子 CA 等。

4、订户，发证机构已经为其签发证书，并不依赖于其是否已经接受证书。

5、密钥生成器，包括电子认证服务机构和用户自己选择的密钥生成器，包括但不限于智能密码钥匙（USB Key）、IC 卡、加密卡、加密机等硬件提供者和 IE 等。

6、主管部门，包括《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》等规定的各类主管部门。

4.1.2 证书类型

目前，SHECA 提供正式证书和测试证书两种类型。

4.1.2.1 测试证书

测试证书由 SHECA 公司受理点为用户制作，SHECA 不承担任何证书真实性的责任，仅供用户测试使用，SHECA 建议用户不要将测试证书应用到任何需要证明真实身份的场所，以免引起不必要的损失和纠纷。

SHECA 不对申请测试证书填写的信息进行保存或者公布，也不承担因为申请者填写的信息泄漏引起的任何责任。

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。

需要特别指出的是，对于 SSL 可信网站证书，SHECA 不提供测试证书的签发服务。

4.1.2.2 正式证书

正式证书是指申请者按照本 CPS 的规定和流程，递交真实的申请信息后经过认证机构批准获得证书，SHECA 对此类证书承担本 CPS 规定的义务和责任。证书申请者根据申请的证书种类，提交内容完整的带个人手写签名或者加盖公章的申请表格。该申请表可以从 SHECA 的网站下载或到 SHECA 和其授权的证书服务机构领取。证书申请表格的填写内容，依照申请证书类型的不同而不同。

SHECA 发放的证书分为中文版、英文版和中英文双语版。中文版证书的名称为申请者的中文名称，英文版证书的名称为申请者的英文名称，中英文双语版证书的名称为申请者的中文名称和英文名称，以中文名称为主。

申请者申请中文版证书时，个人证书以身份证（或其它法定个人证件）中的

中文名称作为证书名称，单位身份证书以营业执照或者其它法定机构证明文件中的中文名称作为证书名称，部门证书或职位证书以经过身份验证的所在法人主体授权的名称作为证书名称。申请者申请英文版证书时，个人证书以护照（或其它法定个人证件）中的英文名称作为证书名称，单位证书申请者应提交英文名称证明材料，不能提供英文名称证明材料的，SHECA 以营业执照或者其它法定机构证明文件作为证明文件，以其中的中文名称的通用英文翻译作为英文名称，其中的具体公司名称应该是中文名称的拼音或相近英文发音。申请者申请中英文双语版证书，以其法定证件中的中文名称为主，英文名称按照申请英文版证书的方式处理。

1、个人证书

（a）个人身份证书，SHECA 的个人身份证书是经 SHECA 签名的包含个人身份信息以及个人公钥的文件，证书的格式遵循 x.509 国际标准。它用于标志证书持有人在进行信息交换、电子签名、电子政务、电子商务等网络活动中的身份，并且保障信息在传输中的安全性和完整性，可以存储在硬盘、智能密码钥匙 (USB Key) 、IC 卡等介质中。

申请者申请个人身份证书，需要递交以下资料:

- 申请者按照要求填写并签字的书面申请表
- 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）原件和复印件；如果 SHECA 或受理点已经通过电话、邮递、第三方验证或者其他方式明确确认申请者个人的身份，申请人可以通过传真、邮递等方式递交身份证明文件的复印件，而不必递交身份证明文件的原件。
- 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及复印件，以及申请委托人亲笔签名的书面授权书。

(b) 个人 E-mail 证书，个人 Email 证书使用户个人可以在重要的邮件通信中对信件内容进行加密和签名操作。用证书对电子邮件内容和附件进行加密，则只有指定的收件人才能阅读该邮件，并且能够确保邮件在传输过程中不会被窃取和篡改。用证书对电子邮件进行签名，则可使接受方确认邮件的发送方，保证邮

件的不可抵赖性，且邮件在传送过程中不被篡改。

申请者申请个人 E-mail 证书，需要递交以下资料并接受 SHECA 对该电子邮件地址的验证：

- 申请者填写并签字的书面申请表（一式三份）
- 个人身份证（或军官证、学生证、护照等）原件
- 个人身份证（或军官证、学生证、护照等）复印件
- 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及复印件，以及申请委托人亲笔签名的书面授权书。
- SHECA 将通过向该 E-mail 地址发送不包含挑战-应答问题的邮件，确认申请人是否拥有该 E-mail。该验证邮件作为验证申请人是否控制该邮件的手段，包括随机产生的问题，例如数学运算、用户身份信息问答等，申请人应在规定的期限内回复邮件并对问题进行正确回答。SHECA 根据邮件回复情况决定是否为其签发证书，如果问题回答正确，即认为申请人控制该电子邮件。

2、单位证书

（a）单位身份证书，SHECA 的单位身份证书是经 SHECA 签名的包含单位身份信息的证书，用于标志单位身份证书持有人在进行信息交换、电子签名、电子政务、电子商务等网络活动中的身份，颁发给企事业单位、政府部门、社会团体等各类组织机构。证书可存放在硬盘、智能密码钥匙（USB Key） 、IC 卡等各类介质中。

申请单位身份证书，需要递交以下资料：

- 申请者填写并签字盖章的书面申请表
- 申请者的企事业单位的有效证件（营业执照或国家法律承认的其它有效证明文件）原件及复印件，复印件应加盖公章；如果 SHECA 或受理点已经通过电话、邮递、第三方验证或者其他方式明确确认单位申请者的身份，申请人可以通过传真、邮递等方式递交证明文件的复印件，而不必递交证明文件的原件。

- 受托申请人的身份证（或军官证、学生证、护照等有效证明文件）原件与复印件，复印件应加盖公章。

（b）单位 E-mail 证书，SHECA 的单位 Email 证书是经 SHECA 签名的，用于标志单位 E-mail 证书持有人电子邮件（E-mail）的身份。证书持有人可以在电子邮件中对信件内容进行加密和签名操作。

SHECA 将通过向该 E-mail 地址发送邮件的方式，确认申请人是否拥有该 E-mail，并根据邮件回复情况决定是否为其签发证书。但是，这不意味着 SHECA 可以保证该申请人确实合法的拥有该 E-mail。SHECA 没有义务也没有必要确认申请者申请证书服务的 E-mail 是否为申请者所有，只保证受理的申请者信息只能用于该 E-mail 证书的申请，以及这些信息和该 E-mail 证书信息的对应性。如果因为 E-mail 归属而产生纠纷，SHECA 不会也不应予以解决， SHECA 会根据有处理职能的相关部门的要求提供有关帮助，但这不是一种义务性的承诺。

申请单位 E-mail 证书需要递交的其它资料与申请单位身份证书所需资料相同。

（c）部门证书，根据各个单位的不同需要，对于颁发给某个部门使用并用来证明该部门身份的数字证书称之为部门证书。

申请部门证书需要递交的资料与申请单位身份证书所需资料相同。

(d) 职位证书, 职位证书包含证书持有者的职位的基本信息、公钥及 SHECA 的签名，用来标识网络通讯中证书持有者的身份，可以存贮在各种介质中，是单位证书中的一种。

申请职位证书需要递交的资料与申请单位身份证书所需资料相同。

3、SSL 证书

SSL 证书，也称为安全站点证书或 Web 服务器证书。SSL 证书和网站的 IP 地址、域名绑定，它可以保证网站的真实性和不被人仿冒，通过在用户端浏览器和 Web 服务器之间建立 SSL 安全通道，保证用户在网络通讯中的安全性。

申请 SSL 证书，需要递交以下资料:

- 申请者填写并签字（或盖章）的书面申请表

- 申请者（个人或组织机构）的身份证明材料原件和符合条件的复印件，或电子扫描件（具体要求同前述个人和单位证书的要求）。
- 申请者必须提交关于该域名（或者互联网 IP 地址）的书面承诺文件，包括域名所有权信息和用途保证，以表明该域名（或者 IP 地址）属于申请者所有，并且该证书会被合法使用。SHECA 将采取适当的方式审核申请人对域名的所有权，参考本 CPS 章节 3.2.5。
- 如果是委托办理，需同时递交申请者和受托人的身份证明文件及复印件，或电子扫描件，以及申请者亲笔签名的书面授权委托书。

对于 SSL 证书的验证数据源，若可依赖数据或文件的时间不超过证书最大有效期，且 SHECA 获得该数据或文件的时间不超过 397 天，则可复用。

4、代码签名证书

（a）个人代码签名证书，以个人身份申请的代码签名证书，用于对软件代码进行签名，以有效防止其软件代码被篡改，拥有者身份被冒用等。下载经过代码签名的软件时，可以确保软件的来源和软件的完整性。

申请个人代码签名证书，需要递交以下资料：

- 申请者按照要求填写并签字的书面申请表
- 个人身份证（或军官证、学生证、护照等其它有效的身份证明文件）原件和复印件；如果 SHECA 或受理点已经通过电话、邮递、第三方验证或者其他方式明确确认申请者个人的身份，申请人可以通过传真、邮递等方式递交身份证明文件的复印件，而不必递交身份证明文件的原件。
- 申请者必须书面承诺该代码证书不被用于任何恶意或者非法的用途。
- 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及复印件，以及申请委托人亲笔签名的书面授权书。

（b）单位代码签名证书，以单位身份申请的代码签名证书，用于对软件代码进行签名，以有效防止其软件代码被篡改，拥有者身份被冒用等。下载经过代码签名的软件时，可以确保软件的来源和软件的完整性。

申请单位代码签名证书，需要递交以下资料：

- 申请者填写并签字盖章的书面申请表
- 申请者的营业执照或其它法定机构证明文件的原件（正本或者副本）及复印件
- 申请者的营业执照原件（正本或者副本）及复印件，如果没有营业执照，则提供书面申请表上可选的其他有效证件原件（正本或者副本）及复印件；目前认可的有效证件如下：营业执照、事业单位法人登记证、社会团体登记证以及其他国家法律承认有效的证明文件。如果 SHECA 或受理点已经通过电话、邮递、第三方验证或者其他方式明确确认单位申请者的身份，申请人可以通过传真、邮递等方式递交证明文件的复印件，而不必递交证明文件的原件。
- 申请者必须书面承诺该代码证书不被用于任何恶意或者非法的用途。
- 受托申请人的身份证（或军官证、学生证、护照等有效证明文件）原件与复印件。
- 申请者对受托申请人的书面委托授权书（需加盖公章）。在提交申请表时，申请者在受托申请人签名后在申请表上加盖公章，就意味着对受托申请人的书面委托授权。

5、设备证书

（a）设备身份证书，颁发给各类非 Web 的应用服务器，实现应用服务器的身份标识和应用的加解密、电子签名等。应用服务器证书可以存放在硬盘、IC 卡、加密机、加密卡等各类设备上。

申请应用服务器证书，需要递交以下资料：

- 申请者填写并签字（或盖章）的书面申请表
- 申请者 (个人或组织机构) 的身份证明材料原件和符合条件的复印件 (具体要求同前述个人和单位证书的要求）。
- 申请者必须书面填写关于该应用服务器的归属性声明文件，以表明该应

用服务器属于申请者所有。

- 如果是委托办理，需同时递交申请者和受托人的身份证明文件及复印件，以及申请者亲笔签名的书面授权委托书。

(b) 互联网设备证书，颁发给各类 VPN 网关、网络接入设备等的证书，用于标识该设备的身份，实现设备的身份标识和应用的加解密、电子签名等。这类证书可以存放在硬盘、IC 卡、加密机、加密卡等各类设备上。具体申请要求参见 SSL 证书。

4.1.3 注册过程和责任

4.1.3.1 注册过程

证书离线申请流程

1、证书申请者携带相关证明到各个证书服务机构的受理点 RAT（或者通过线上方式向受理点提出申请），填写相关申请表格。

2、受理点 RAT 审核证书申请者和相关身份资料的真实性。如果身份鉴别未通过，受理点 RAT 将拒绝为用户发放证书，并将未通过的信息存档。

3、如果身份鉴别通过，受理点 RAT 通过服务系统录入、审核证书申请信息，用受理点操作员的证书签名后，再用其上级 RA 的证书加密，将信息递交给 RA 机构。

4、RA 机构收到所属受理点递交的信息后，解密后验证其签名，验证通过后将信息转交给 CA 发证机构。若验证不通过，则拒绝进行下一步操作，直接返回失败信息。

5、受理点向证书申请者发放密码信封。

6、RA 机构向 CA 发证机构发送证书申请者的证书申请数据。

7、CA 发证机构根据证书请求签发证书。

8、申请者接受并下载证书。

对于在线申请，SHECA 要求：

SHECA 支持在线证书申请。在线证书申请，在安全性和认证得到保证的情况下，允许申请人通过网络或传真提交他们的申请信息。申请者无须亲自到 SHECA 和其授权的证书服务机构所在地进行物理身份验证。这种申请方式适用于测试证书的申请、SHECA 已确定身份的申请者群体以及证书的更新申请。

4.1.3.2 各参与实体的责任

1、电子认证服务机构的责任

电子认证服务机构应承担的责任是: 保证电子认证服务机构本身的签名私钥在 SHECA 内部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。

电子认证服务机构对其授权的证书服务机构进行审计和管理, 保证整个申请过程的安全可靠。

电子认证服务机构保证整个 CA 系统安全可靠的运行。SHECA 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赔偿责任。为了表达明确，这些事件包括罢工或其他劳动纠纷、暴动、国内骚动、供应商故意或无意的行为、不可抗力、战争、火灾、爆炸、地震、洪水或其它灾难等。

由于技术的进步与发展, 电子认证服务机构会要求证书订户及时更换证书以保证证书的可靠性。

2、注册机构 RA 的责任

注册机构 RA 按照程序取得 SHECA 的授权，遵循本 CPS 和 SHECA 的授权运作协议和其它 SHECA 公布的标准和流程，接受并处理证书服务申请者的证书服务请求，并依据授权设置和管理各类下级证书服务受理机构，包括 RA、RAT 等。

RA 必须遵循 SHECA 制订的服务受理规范、系统运作规范和管理规范，SHECA 将不断的完善并及时发布有关的规范和标准内容。根据本 CPS、SHECA 公布的规范，RA 有权决定是否给申请者提供相应的证书服务。RA 必须按照 SHECA 的要求，按照 SHECA 建议或者强制的规范，建立起合理的机制，保证

所有证书服务（例如申请、更新、撤销等）信息传输的可信、安全、可靠。

RA 按照 SHECA 的要求和规范，确定下属证书服务受理机构的设置方式、管理方式和审核方式，这些方式的确定必须以书面的文件形式公布，涵盖并且不得与 SHECA 公布的相关条款产生冲突、矛盾或者不一致。

RA 依据本 CPS 的规定，确保其运营系统处在安全的物理环境中，并具备相应的安全管理措施。RA 必须能够提供证书服务全部的数据资料及备份，并按照 SHECA 的要求，保证其与下属证书服务机构间的信息传输安全。重要的是，RA 承诺，严格执行为订户保存申请资料的义务，并愿意承担因此而带来的法律责任。

电子认证服务机构根据本 CPS 和授权协议对 RA 进行管理，包括进行服务资质审核和规范执行检查。电子认证服务机构具有对所有证书服务申请者服务请求的最终处理权。电子认证服务机构有权对申请者的资料进行复查；因为对申请者的资格审核不严而导致的由证书使用引起的所有损失，由 RA 承担。

RA 必须妥善保管所有申请者的信息，不向任何无关的第三方泄漏。RA 必须对各类证书服务申请表、证书存储介质、密码信封等进行安全、可靠、严格的管理，确保其得到足够的保护。

RA 必须接受 SHECA 对其运作的监督和审计，并保证完全配合 SHECA 提出的审计要求。

3、受理点 RAT 的责任

受理点 RAT 按照程序取得 SHECA 或其上级 RA 的授权，遵循本 CPS 和相关的授权运作协议和其它 SHECA 公布的标准和流程，接受并处理证书服务申请者的证书服务请求。

RAT 必须遵循电子认证服务机构和其上级 RA 制订的服务受理规范、系统运作规范和管理规范，电子认证服务机构和其上级 RA 将不断的完善并及时发布有关的规范和标准内容。根据本 CPS、SHECA 和其上级 RA 公布的规范，RAT 有权决定是否给申请者提供相应的证书服务。

RAT 依据本 CPS 的规定，确保其运营系统处在安全的物理环境中，并具备相应的安全管理措施。RAT 必须按照 SHECA 的要求，按照 SHECA 建议或者强

制的规范，建立起合理的机制，保证所有证书服务（例如申请、更新、撤销等）信息传输的可信、安全、可靠。

电子认证服务机构和其上级 RA 根据本 CPS 和授权协议对 RAT 进行管理，包括进行服务资质审核和规范执行检查。电子认证服务机构具有对所有证书服务申请者服务请求的最终处理权。电子认证服务机构有权对申请者的资料进行复查。

RAT 对所有证书服务申请者真实性的信息鉴别负有责任，无论这种申请是否被决定受理与否。由于 RAT 对申请者的资格审核不严而导致的所有损失，由 RAT 承担。

RAT 必须妥善保管所有申请者的信息，不向任何无关的第三方泄漏。RAT 必须对各类证书服务申请表、证书存储介质、密码信封等进行安全、可靠、严格的管理，确保其得到足够的保护。

RAT 必须接受 SHECA 对其运作的监督和审计，并保证完全配合 SHECA 提出的审计要求。

4、垫付商的责任

垫付商必须承担其所有垫付的证书费用，并按 SHECA 规定的方式付清。

垫付商的垫付行为，就表明其愿意并且能够承担本 CPS 以及 SHECA 相关协议的规定，对证书服务申请者的身份真实性提供担保的责任。

5、证书申请者的责任

证书申请者必须严格遵守与证书申请以及私钥的所有权和安全保存相关的要求：

证书申请者承诺，在证书服务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，可供发证机构检查和核实；并且，证书申请者愿意承担任何因提供虚假信息、伪造信息等行为引起的法律责任。由于证书申请者自身原因导致发证机构无法正确为其签发证书的，由申请者自行承担有关损失和责任。

证书申请者必须仔细阅读和理解本 CPS 罗列的或者由 SHECA 推荐或使用的安全措施，以充分了解私钥保存的重要性，确保私钥的安全。

证书申请者在申请、接受证书及其相关服务前，需要熟悉本 CPS 的条例和与证书相关的政策、法规等，SHECA 在接到证书申请者的任何服务申请前，都认为该持有人已经了解本 CPS 的内容，并承诺遵守证书持有者证书使用方面的有关限制。

6、订户的责任

SHECA 一旦通过证书申请者的申请并为其签发证书，无论是否已经接受证书，证书申请者当然得就成为证书订户。

订户必须确保本身持有的证书用于申请时预定的目的。

订户必须保证私钥的安全。SHECA 只是告知，但并不要求证书申请者一定遵从 SHECA 提出的安全措施；订户可以选择任何自己认为可以保密的所有措施；同时，SHECA 声明，SHECA 并不承担因订户的私钥保存出现问题而带来的所有责任，除非订户能够合法的证明这种问题产生的主要责任在发证机构。

一旦发生任何可能导致安全性危机的情况，包括证书订户遗失私钥、遗忘或泄密以及其他未罗列的情况，证书订户应立刻通知 SHECA，采取申请作废等处理措施。如果证书订户明知私钥保存出现问题而未及时通知 SHECA，而给 SHECA 以及 SHECA 授权的有关证书服务机构、其他订户、证书依赖方或者其它相关方造成损失的，该订户必须承担相应的赔偿责任。

7、依赖方的责任

依赖方在信赖任何 SHECA 及其下级操作子 CA 签发的证书时，必须保证遵守和实施以下条款:

（a）依赖方熟悉本 CPS 的条款以及和证书相关的政策、法律，了解证书的使用目的和使用限制。

（b）依赖方在信赖 SHECA 及其下级操作子 CA 签发的证书前，必须对其进行合理的审查，包括但不限于：查看证书是否在有效期；检查 SHEC 公布的有效 CRL，以获得该证书的状态。SHECA 认为，依赖方一直是遵循了此条款的。一旦依赖方因为疏忽或者其他原因违背了此条款而给 SHECA 带来损失时，SHECA 保留采取相应法律行为的权利。

（c）所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本CPS 的有关条例,包括有关免责、拒绝和限制义务的条款。

8、目录服务的责任

SHECA 在目录服务器上公布证书订户的证书和相关 CRL。

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。

9、密钥生成器提供者的责任

一旦证书申请者选择了某种密钥生成器，则表明该申请者信赖由其产生的密钥对的安全性和可靠性,SHECA 并不为此提供任何形式的担保，也没有责任和权力对由此产生的纠纷进行处理。

10、主管部门

SHECA 承诺，将严格按照国家的法律法规和主管部门的书面要求提供符合要求的第三方电子认证服务。

4.2 证书申请处理

4.2.1 执行身份识别与鉴别

SHECA 和其授权的证书服务机构，有权利和责任对申请者的身份进行合理的鉴别。出于安全性和审计的需要，证书申请表应记录鉴别人的姓名、签名、验证结果和验证日期。

在接到订户的证书申请后，发证机构应完成以下鉴别工作，将其作为向该订户签发证书的先决条件：

- 确认证书申请者接受订户协议中的各项条款。
- 根据证书申请者所申请的证书种类，按照各类证书的不同鉴别要求对证书申请者的身份进行验证。
- 确认证书申请者合法的拥有与证书中所含公钥配对的私钥（可根据证书

种类不同采用不同的确认方法，如要求订户作出保证等方式）。

- 确认证书中包含的信息，除了未经验证的订户信息外，都是准确的。
- 确认任何受托人在代表其组织机构申请证书时，该受托人已得到了所代表的组织机构的合法授权。
- 确认任何委托办理的各方之间的授权合法性和委托方、受托方的身份。

此外，从 2017 年 9 月开始，SHECA 在证书签发过程中执行 CAA（Certification Authority Authorization）记录查询，并在审核记录中体现。

SHECA 认可的 CAA 标记为：sheca.com，imtrust.cn，wwwtrust.cn。

在签发了证书后，除非被通知该证书发生了本 CPS 所述的安全损害情况，SHECA 将不再负有继续监控和调查证书中信息准确性的责任。

SHECA 保留更新鉴别程序和要求的权利，更新后的鉴别程序和要求将发布在 https://www.sheca.com 中，也可通过以下地址索取：

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 ）

上海市数字证书认证中心有限公司

SHECA 客户服务部

SHECA 和其授权的证书服务机构的审核人员合理、审慎地进行申请者身份鉴别，并进行批准或拒绝的操作。

4.2.2 证书申请批准和拒绝

SHECA及其授权的证书服务机构收到申请者的申请，对申请信息及身份信息进行完整性、有效性、可靠性和真实性的鉴别，准确无误后，将批准该申请。SHECA及其授权的证书服务机构依照CPS的规定为申请者签发一张证书以证明已经批准了申请者的证书申请。

如果符合下述条件，可以批准证书申请：

- 该申请完全满足前面 3.2 条款关于订户信息的标识和鉴别规定
- 申请者接受或者没有反对订户协议的内容和要求

- 申请者已经按照规定支付了相应的费用，另有协议规定的情况除外

当SHECA及其授权的证书服务机构在进行鉴别程序时，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，并立即通知申请者鉴别失败。对于鉴别失败的原因，SHECA有权拒绝解释，并且不需要通知申请者。法律法规对此有明确要求的除外。如果是由于第三方信息而导致身份鉴别失败,SHECA将向申请者提供第三方的联系方式，以便申请者查询。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。

SHECA 根据反钓鱼联盟、防病毒厂商或相关联盟、负责网络安全事务的政府机构等第三方发布的名单，或公共媒体公开报道中披露的信息，建立和维护证书高风险申请人列表，在接受证书申请时将会查询该列表信息。对于列表中出现的申请人，SHECA 将直接拒绝其申请，或要求提供额外的申请材料、资金担保等以证明其证书不会被滥用或违法使用。对于已签发的证书，也将会定期根据列表予以复核，一旦发现证书持有人出现在列表中，SHECA 有权撤销该证书或采取适当机制进行谨慎处理。

SHECA 还可以根据其独立判断，拒绝为某一申请者签发证书，不需要为此做出解释，并且不对因此而导致的任何损失或费用承担责任和义务。除非证书申请者提交了欺骗性的或伪造的信息，在拒绝签发证书后，SHECA 将立即归还证书申请者所付的所有证书购买费用。

如果发生下列情形，可以拒绝证书申请：

- 该申请不符合前面 3.2 条款关于订户信息的标识和鉴别规定
- 申请者不能提供所需要的身份证明材料或其他需要提供的支持文件
- 申请者反对或者不能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
- RA 或者 CA 认为批准该申请将会对 CA 带来争议、法律纠纷或者损失

被拒绝的证书申请者可随后再次提出申请。

4.2.3 处理证书申请的时间

SHECA 最多在 7 个工作日内，对证书申请者提交的信息进行鉴别和审核，

并作出批准或者拒绝的决定。

4.3 证书签发

4.3.1 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发证机构为其签发证书。

发证机构在批准了证书申请之后，将为订户签发证书并通过 HTTP 和 LDAP 等方式发行证书。证书的发行意味着 SHECA 最终完全正式地批准了证书申请。

4.3.2 证书签发中注册机构和电子认证服务机构的行为

在证书申请获得批准后，申请人将会收到一个包含申请密码的标记物品，简称申请密码（如密码信封或密码卡片、条码、加密数字流等），以便保证在安全的状态下申请证书。

只有完全满足了下述情况，SHECA 和其授权的证书服务机构才向申请人发放密码：

- 遵守了 SHECA 证书的申请程序；
- 按规定支付了应当支付的证书费用；
- SHECA 和其授权的证书服务机构批准了该申请书。

注册机构完成申请者注册和证书申请操作后，按照本 CPS 的规范和 SHECA 相关的授权运作协议将申请信息和用户资料传给认证机构。

认证机构收到申请信息后，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。

如果证书申请者申请签名证书，那么：

1、证书申请者向 SHECA 发送公开密钥。SHECA 通过网络与申请者建立安全通道，申请者上传公钥至 CA 机构。SHECA 支持 PKCS10 标准的证书请求。

2、SHECA 确认证书请求的真实性。一旦确认，SHECA 就签发相应的证书。

如果证书申请者申请加密证书，那么：

1、申请者在申请签名证书时，可以同时申请加密证书。

2、SHECA 在收到申请加密证书的请求时，将从相应的国家密钥管理部门获取加密密钥对，为用户签发加密证书。

对于中级 CA 证书的签发，应由 CA 系统管理员授权后方可进行操作。

4.3.3 电子认证服务机构和注册机构对订户的通告

发送密码的方式根据SHECA证书的申请对象而不同,可以分以下几种方式：

1、通过面对面的方式，通知申请者（如申请者到受理点领取等方式）；

2、通过电子邮件（e-mail）方式通知；

3、邮政信函通知；

4、经过已经确认安全的通道通知；

5、其他 SHECA 认为安全可行的方式。

SHECA 没有上门为用户安装证书的义务。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 和其授权的证书服务机构提供热线支持服务。热线支持电话和信箱由 SHECA 和其授权的证书服务机构公布。

4.4 证书接受

4.4.1 构成接受证书的行为

在申请者完成申请程序，SHECA 和其授权的证书服务机构将证书本身、或者证书获得的方式、或者与证书相关的密码递送给申请者，就意味着申请者已经接受了证书。订户接受数字证书后，应妥善保存与其证书对应的私钥。

下列行为被认为订户已经接受了证书：

- 订户接受了包含有证书的介质
- 订户通过网络将证书下载或安装到本地存储介质，如本地计算机、IC 卡、智能密码钥匙（USB Key）、移动硬盘或其它移动存储介质

- 订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容
- 订户反对证书或者证书内容的操作失败

4.4.2 电子认证服务机构对证书的发布

一旦订户接受证书，SHECA 将在其信息库、目录服务中和由 SHECA 决定的其它一个或多个信息库里发布证书的副本。订户也可以在其它场所公布他们的证书。

订户、依赖方可以通过证书目录服务或者 HTTP 的方式查询自己或他人的证书。

如果订户书面提出申请，CA 可以不把该订户的证书发布到任何公开的信息库中。

4.4.3 电子认证服务机构对其他实体的通告

订户接受证书后，SHECA 将不专门对注册机构、受理点、主管部门等实体进行专门的通告，这些实体可以通过目录服务或者查询 SHECA 信息库来获得订户的证书及相关信息。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

只有当订户表示同意订户协议的要求（例如签署了订户协议），并且接受了以后，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 及相关 CP 规定的依法地被使用。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（如果证书中的某些字段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）。所有的使用行为必须符合订户协议的要求。

订户使用证书时，必须妥善保管和存储与证书相关的私钥，避免遗失、泄露、被篡改或者被盗用。任何人使用证书时都必须检验证书的有效性，包括该证书是否被撤销、是否还在有效期内、是否是正确的机构签发等。

在使用与 SHECA 所签发的证书有关的电子签名及经过电子签名的信息时，参与方按本 CPS 规定而享有的权利和应尽的义务。参与方 (发证机构、证书订户和依赖方)，均视为已被通知并同意遵守本 CPS、UNTSH CP 以及 SHECA 与各方签署的协议、规范中的条款。任何超出本 CPS 的规定的证书及私钥的使用，SHECA 将不承担由此带来任何后果。

SHECA 签发的各类证书，仅用于表明证书持有者在申请证书时所要标识的身份，以及验证证书持有者用于该证书内包含的公钥相对应的私钥做出的签名。这样，通过签名和签名的验证，保证证书持有者的身份真实性、信息的完整性、信息的不可抵赖性等。如果证书持有人将该证书用于其他用途，SHECA 将不承担任何由此产生的责任和义务。

如果证书中的某些字段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。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。

4.5.2 依赖方公钥和证书的使用

在信任证书和签名前，依赖方要独立地做出应有的努力和合理的判断：

- 该证书是否由可信任的 CA 所签发
- 对于任何给定的目的，证书被适当的使用；并且判断该证书没有被用于任何本 CP、相关 CPS 或者法律法规禁止的或者限制的使用范围。SHECA 和 RA 并不负责也无法做到评估订户证书是否被适当的使用
- 证书在被使用时是否与证书包含的内容相一致（如果证书中的某些字段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）
- 查询证书及其证书链内的所有证书的证书状态，是否在有效期内，是否已经被撤销。如果订户证书或者其证书链内的任何证书已经被撤销，依赖方必须独立的去了解该订户证书所对应的私钥做出的签名是否是在撤销前做出的。

除非本 CPS 另有规定，证书并不是来自发证机构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。

如果证书中的某些字段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。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。

4.5.3 签名及验证

签名只限于以下几种情况下才能被创建:

- 在证书的使用有效期内被创建
- 该签名能通过对证书链的确认来正确验证
- 依赖方没有发现或注意到签名者违背本 CPS 要求的行为
- 依赖方遵守本 CPS 的所有规定

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创建的,以及该签名创建后被签名的信息没有被更改过。

这样的验证将按本 CPS 规定的方式进行，验证方式如下所述:

1、确认验证签名的证书链 -- 要验证签名应首先确认所选择的证书链是与该数字签名最相配的证书链。从一张给定的证书到一个可接受的根证书，可能存在多个有效的证书链（例如交叉验证）。如果到一个可接受的根证书间存在多个证书链，确认签名的人在选择和验证证书链时可能会有不同的选择。在这种情况下, 验证数字签名的人最好选择终结于“较高信任级”的一级 CA 或终结于 SHECA 的根证书的证书链。

2、检查 SHECA 或其他机构的信息库，查看证书链上的证书是否被撤销。因为在创建签名期间，证书可能因被撤销而使证书不再有效。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。

3、确定经过签名的信息的范围，在验证签名时，应准确知道什么数据已经被签名。

4、确定签名者的适用范围和目的，发证机构可能对其签发的证书所对应的私钥的用途加以限制。这些限制将在证书里显示或伴随在证书的引用信息中，并以此警告接收方在某些情况下信任证书是不合理的。验证证书者必须检查证书中的警告和限制，以确保证书的合理使用。

SHECA 郑重指出：

- 依赖方如果信任无法验证的签名，那么应由其自身承担所有相关风险。
- 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，都必须经过合理和适当的判断。

在下列条件下，接收到被订户签名过的信息的接收方，可以信任与订户捆绑的签名：

- 签名是在合法证书的使用有效期内被创建，并且通过确认有效的证书链，该签名可以被验证。
- 信赖方是合理地信任该数字签名。如果信任签名时需要额外保证，信赖方必须在得到这些保证后才能合理地信任该签名。

当然，是否信赖经过验证的签名的最终决定，将由验证者独立地做出。

4.6 证书更新

证书更新是指在是在不改变证书中的公钥和其他任何证书包含的信息的情况下，为订户签发一张新证书。

证书更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，使用原证书的私钥对包含公钥的更新申请信息签名。为保证证书及其密钥对的安全可靠，SHECA 为签发的证书设置有效期，

一般为一年。在证书有效期到期前及到期后 30 天内，证书订户可以选择保留原有密钥，到发证机构申请更新证书。订户必须保证密钥的安全可靠。

针对 SSL 证书及代码签名证书，SHECA 对申请更新的用户按照新申请的要求进行身份验证，参见 3.2 章节。

4.6.1 证书更新的情形

当证书持有者的证书有效期即将结束时，SHECA 将作出合理的努力，在证书有效期满之前向证书订户或者证书申请受托人、证书申请时的垫付商或者代理商发送证书更新提示；合理的努力包括但不限于网站提示、系统提示、书面提示、E-mail 通知或者其它方式，但 SHECA 和其授权的证书服务机构采取了上述任意一项提示或者通知方式，均可被视作进行了合理的努力。

SHECA 签发的用户证书有效期从证书签发之日起计算。证书到期前的一个月，SHECA 会向相应的证书持有者发出更新的通知或相应的信息。

同时，SHECA 也接受订户自主提出的更新要求，对其证书进行更新处理。

4.6.2 请求证书更新的实体

所有持有 SHECA 签发的证书订户，包括个人、企业单位、事业单位、政府机构、社会团体、人民团体等各类组织机构等，在其证书的有效期即将到期前，均可以请求更新其持有的各类证书。

4.6.3 证书更新请求的处理

SHECA 和其授权的证书服务机构提供在线更新和离线更新两种手段。证书持有者可以自行选择合适的更新策略。对于证书更新，其处理过程需要确保提出证书更新请求的人是被更新证书所标识的订户，SHECA 在为其签发新证书时，可以要求更新申请者提交原有私钥签名，或者使用与初始签发证书相同的过程来进行鉴别。通常，在证书更新时，订户可以用原有的私钥对更新请求进行签名，发证机构将会对用户的签名和公钥、更新请求内包含的用户信息进行正确性、合法性、唯一性的验证和鉴别。包括：

- 订户对申请信息进行签名，CA 用其原有证书中的公钥对签名进行验证

- 订户注册信息没有发生变化，CA 基于其原有注册信息对其进行签发新的证书

在线更新证书，订户必须在线填写更新请求，并按照 SHECA 和其授权的证书服务机构的要求，用当下的私钥对更新请求信息进行签名，递交给发证机构。发证机构接收到更新请求后，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。

离线更新证书，订户按照原申请证书的流程，到 SHECA 和其授权的证书服务机构提出更新请求。发证机构按照原申请时的流程对证书更新申请进行身份鉴别和审核。发证机构确认并批准更新申请后，为其签发新的证书。

4.6.4 订户更新证书时的注意事项

订户在更新证书前，应确保即将到期证书的密钥对的安全可靠。一旦无法确认这种可靠性，那么 SHECA 和其授权的证书服务机构建议订户直接选择证书密钥更新。

4.6.5 构成接受更新证书的行为

在订户递交更新请求或者离线递交更新请求获得批准后，SHECA 和其授权的证书服务机构将证书本身、或者证书获得的方式、或者与证书相关的密码递送给订户，就意味着订户已经接受了证书。订户接受数字证书后，应妥善保存与其证书对应的私钥。

4.6.6 电子认证服务机构对更新证书的发布

一旦订户接受更新证书，SHECA 签发后将在其信息库、目录服务中和由 SHECA 决定的其它一个或多个信息库里发布证书的副本。订户也可以在其它场所公布他们的更新证书。

新证书签发后，根据订户的要求，SHECA 和其授权的证书服务机构可以撤销旧的证书。

4.6.7 电子认证服务机构对其他实体的通告

订户接受更新证书后，SHECA 将不专门对注册机构、受理点、主管部门等实体进行通告，这些实体可以通过目录服务或者查询 SHECA 信息库来获得订户的更新证书及相关信息。

4.7 证书密钥更新

当订户或其它参与者需要生成一对新密钥并申请为新公钥签发一个新证书，用户可以选择证书密钥更新服务。出于安全原因，SHECA 建议订户证书到期后，选择证书密钥更新，在更新证书的同时更新密钥。证书密钥更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，如订户甄别名、证书序列号、原证书对应的私钥对证书密钥更新请求签名等，并上送新的公钥申请签发新证书。

针对 SSL 证书及代码签名证书，SHECA 对申请更新的用户按照新申请的流程执行，参见章节 4.1，并按照 3.2 相关规定进行身份验证。

4.7.1 证书密钥更新的情形

如果出现下列情形，订户必须选择证书密钥更新：

- 证书到期并且密钥对的使用期也到期
- 证书密钥对已经被泄漏、被窃取、被篡改或者其它原因导致的密钥对安全性无法得到保证
- 证书被撤销后需要重新获得证书

此外，凡是在 SHECA 架构内部使用的证书，包括 RA、服务操作人员等的证书，到期后，必须进行证书密钥更新。

证书即将到期的订户，出于安全考虑，应尽量采取证书密钥更新，来获得新的证书。

4.7.2 请求证书密钥更新的实体

所有持有 SHECA 签发的证书订户，包括个人、企业单位、事业单位、政府机构、社会团体、人民团体等各类组织机构等，以及 SHECA 认证体系内的所有证书持有者，均可以请求证书密钥更新服务。

4.7.3 证书密钥更新请求的处理

SHECA 和其授权的证书服务机构提供在线更新和离线更新两种手段。通常，在证书密钥更新时，订户可以提交原证书的相关信息，例如证书甄别名、证书序列号、原证书对应的私钥对证书密钥更新请求的签名等信息，来标识其身份，发证机构将会对用户的更新请求内包含的用户信息进行正确性、合法性、唯一性的验证和鉴别。包括:

- 订户提交可以验证其身份的信息，CA 对其进行验证
- 订户用原证书对应的私钥对证书密钥更新请求进行签名，CA 对其签名进行验证
- 订户注册信息没有发生变化，CA 基于其原有注册信息对其进行签发新的证书

在线更新证书，订户须在线填写更新请求，并按照 SHECA 和其授权的证书服务机构的要求，用当下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，递交给发证机构。SHECA 和其授权的证书服务机构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。

离线更新证书，订户按照原申请证书的流程，到 SHECA 和其授权的证书服务机构提出更新请求，并递交新生成的公钥。SHECA 和其授权的证书服务机构按照原申请时的流程对证书密钥更新申请进行身份鉴别和审核。发证机构确认并批准更新申请后，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。

4.7.4 更新证书密钥时的注意事项

订户在选择证书密钥更新时，应将待更新证书加密过的信息和数据进行妥善

处理（例如备份待更新的证书和密钥，或者将用现有证书加密的文件进行解密，以及订户认为合理的处理方式），然后才能进行证书的更新。

如果订户未进行妥善处理而直接进行证书密钥更新，可能导致原加密信息和数据无法解密。由此造成的可能损失，SHECA 将不承担任何责任。

4.7.5 构成接受密钥更新证书的行为

在订户递交证书密钥更新请求或者离线递交证书密钥更新请求获得批准后，SHECA 和其授权的证书服务机构将证书本身、或者证书获得的方式、或者与证书相关的密码递送给订户，就意味着订户已经接受了证书。订户接受数字证书后，应妥善保存与其证书对应的私钥。

4.7.6 电子认证服务机构对密钥更新证书的发布

一旦订户接受密钥更新证书，SHECA 签发后将在其信息库、目录服务中和由 SHECA 决定的其它一个或多个信息库里发布证书的副本。订户也可以在其它场所公布他们的更新证书。

新证书签发后，根据订户的要求，SHECA 和其授权的证书服务机构可以撤销旧的证书。

4.7.7 电子认证服务机构对其他实体的通告

订户接受密钥更新证书后，SHECA 将不专门对注册机构、受理点、主管部门等实体进行专门的通告，这些实体可以通过目录服务或者查询 SHECA 信息库来获得订户的更新证书及相关信息。

4.8 证书变更

在证书有效期内，当证书信息发生变化，订户或者其他参与者可选择证书变更，保留原有公钥，申请签发新的证书。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。只有订户在有效期内，才可能发生证书变更。在证书内所包含的订户信息发生变化时，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。

订户信息发生变化，足以影响到该订户持有的证书标识的身份变化时，订户有义务向 SHECA 进行报告。

4.8.1 证书变更的情形

当订户或其他参与者的信息发生变化，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、电话、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 请求证书变更的实体

所有持有 SHECA 签发的证书订户，包括个人、企业单位、事业单位、政府机构、社会团体、人民团体等各类组织机构等，SHECA 的所有证书持有者，在信息发生变化，造成实体身份变化时，均可以请求证书变更服务。

4.8.3 证书变更请求的处理

SHECA 和其授权的证书服务机构，可以提供在线变更和离线变更两种方式。

在线变更证书，订户须在线填写变更请求，并按照 SHECA 的要求，用待变更的证书公钥相对应的私钥对变更请求信息进行签名，递交给发证机构。发证机构接收到证书变更请求后，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，该证书仍然使用原有公钥。

离线更新证书，订户按照原申请证书的流程，到 SHECA 和其授权的证书服务机构填写证书变更申请表。SHECA 和其授权的证书服务机构按照原申请时的流程对证书变更申请进行身份鉴别和审核。发证机构确认并批准变更申请后，为其签发新的证书，该证书的公钥为申请者原有的公钥。

目前，只提供离线变更方式。

4.8.4 变更证书的注意事项

证书修改后，证书的有效期从变更或重签的时间点开始，直至原证书有效期截止日期。

订户在变更证书前，应确保该证书密钥对的安全可靠。一旦无法确认这种可靠性，那么 SHECA 建议订户直接选择证书密钥更新。

4.8.5 构成接受变更证书的行为

在订户递交证书变更请求或者离线递交证书变更请求获得批准后，SHECA 和其授权的证书服务机构将证书本身、或者证书获得的方式、或者与证书相关的密码递送给订户，就意味着订户已经接受了证书。订户接受数字证书后，应妥善保存与其证书对应的私钥。

4.8.6 电子认证服务机构对变更证书的发布

一旦订户接受变更证书，SHECA 签发后将在其信息库、目录服务中和由 SHECA 决定的其它一个或多个信息库里发布证书的副本。订户也可以在其它场所公布他们的变更证书。

新证书签发后，旧的证书将被撤销，在 24 小时内通过 CRL 发布。

4.8.7 电子认证服务机构对其他实体的通告

订户接受变更证书后，SHECA 将不专门对注册机构、受理点、主管部门等实体进行专门的通告，这些实体可以通过目录服务或者查询 SHECA 信息库来获得订户的变更证书及相关信息。

4.9 证书撤销和挂起

订户、电子认证服务机构、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 或者其授权的证书服务机构申请数字证书，与第一次申请时的程序手续相同。对于被撤销证书里的公钥所对应

的私钥，在撤销后适用的保存期内，除非已被销毁，否则订户必须以可信的方法进行保护。

所有证书撤销的申请表格等格式文件，由 SHECA 和其授权的证书服务机构保存。

目前，SHECA 不提供证书挂起服务。一旦提供挂起服务，SHECA 将会通过网站等进行公布。

4.9.1 证书撤销的情形

4.9.1.1. 订户证书撤销的情形

1、若出现以下情况中的一种或多种，SHECA 及其授权的服务机构将在 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 CA 原证书申请并未被授权，也没有意图后续补充授权；
- CA 有证据指明，订户的与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 6.1.5 和 6.1.6）；
- CA 有证据指明，SSL 证书中的域名或 IP 地址不可信。

2、如果发生以下情形，订户证书将在 5 天内被撤销：

- SHECA 获得证据，表明证书被误用；
- SHECA 发现证书的签发不符合CP/CPS的要求；
- SHECA 依据CP/CPS 的要求撤销证书；
- 订户证书里的信息做了实质性的更改；
- SHECA签发证书后发现证书持有者申请其证书时提供的资料存在虚假

信息；

- 订户违背了CP及本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；
- 订户机构合法主体的身份发生变化、撤销或解散；
- 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
- 当CA 机构发现或被告知订户签名软件中含有可疑代码的情况下，CA 机构可以撤销代码签名证书；
- 法律法规的相关规定或要求。

3、除以上情况外，如 SSL 证书含有以下情况的任意一项或几项的也需要在 5 天内进行撤销证书的操作：

- SHECA 发现 SSL 证书的签发不符合 Baseline Requirement 的要求
- SHECA 了解到某通配符 SSL 证书被用于验证具有欺诈误导性质的域名；
- SHECA 机构由于某种原因终止运行，并且未安排其他 CA 提供撤销证书的支持性操作；
- SHECA 依据 Baseline Requirements 签发 SSL 证书的权利已届满或被撤销或终止，除非 CA 已作出安排，继续维护 CRL/OCSP；
- CA 机构得知订户不再能合法使用证书中包含的域名或 IP 地址，如法院或仲裁停止了域名注册商使用某域名的权限，或域名注册商与申请人之间的使用许可或服务协议终止了；
- 证书的技术内容或格式造成了对应用软件供应商或依赖方不可接受的风险，如 CA/浏览器论坛决定弃用某种算法或密钥长度，认为其风险水平不可接受，在一定期限内 CA 应撤销此类证书

4、根据 CP 或 CPS，其它 SHECA 认为可以进行撤销的理由

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。

4.9.1.2. 中级 CA 证书撤销的情形

若出现以下情况中的一种或多种，SHECA 应在 7 天之内撤销中级 CA 根证书:

1 SHECA 获得证据，显示中级证书公钥对应的私钥受到了损害，或不再符合 Baseline Requirements 第 6.1.5 和 6.1.6 章节的相关要求；

2 SHECA 获得证据，显示中级 CA 根证书被误用；

3 SHECA 发现证书的签发不符合 Baseline Requirements 及 CP/CPS 等规范的要求；

4 SHECA 认为证书中有信息不准确或具有误导性；

5 SHECA 因故停止运营，且未与其它 CA 联系以继续提供证书撤销服务；

6 SHECA 依据 Baseline Requirements 签发证书的权利失效、或被取消或被终止（除非 SHECA 继续维护 CRL/OCSP 信息库）；

7 SHECA 依据 CP/CPS 的要求撤销证书；

8 证书的技术内容或格式为应用软件供应商或证书依赖方带来了不可接受的风险。

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、订户授权代表及订户证书费用垫付商
- SHECA
- 法院、政府主管部门及其他公权力部门

此外，证书依赖方或其它第三方也可发送邮件至 report@sheca.com，提交证

书问题报告告知 SHECA。

只有 SHECA 可以撤销根证书或者子 CA 证书。

4.9.3 撤销请求的流程

在申请证书撤销时，应按照以下流程进行处理：

1、证书订户代表人或指定的代理人提出撤销申请，可按照以下方式进行：

在线申请，仅适用持有智能密码钥匙（USB KEY）的订户： 登录 http://issp.sheca.com/（证书自助服务门户）

电子邮件：report@sheca.com

传真：021-36393200

电话：021-36393196

现场申请：SHECA 所有对外服务网点

2、SHECA 进行证书撤销请求的鉴别和验证

在证书有效期内，用户发现证书签发错误或者系统不兼容等问题而提出证书撤销，SHECA 会在 24 小时内对撤销请求进行调查。

针对撤销请求的鉴别和验证应视情况进行：

（1）对于持有智能密码钥匙（USB KEY）的用户，使用智能密码钥匙（USB KEY）登录 http://issp.sheca.com/（证书自助服务门户）进行证书撤销的在线办理即可；

（2）对于无智能密码钥匙（USB KEY）用户以及智能密码钥匙（USB KEY）丢失的用户，必须携带相关机构及个人的身份证明材料至 SHECA 各受理服务网点申请撤销业务。若用户所在地未设置 SHECA 受理服务网点，则可通过电话（最好由证书申请人）进行证书撤销申请，受理人员通过电话对用户个人信息及机构的单位身份进行审核，以确认与证书申请信息一致。

3、SHECA 应在接到撤销请求后 2 个工作日内进行证书撤销或其它合理处理。如果是应用软件提供者请求撤销证书的情况下，SHECA 应在收到请求的 2

个工作日内告知应用软件提供商是否要撤销证书。

如果基于调查，SHECA 确定撤销证书会对其客户产生不合理的影响，SHECA 应向应用软件提供商建议采取其他措施。

4、证书被撤销后，SHECA 及时将其发布到证书撤销列表

所有非经订户自身提出的撤销请求，必须经过合理授权后方可进行。

在根证书或子 CA 证书相对应的私钥出现安全风险时，经国家电子认证服务主管部门批准后可直接进行证书撤销。

SHECA 提供 7*24 小时的证书问题报告和处理机制。

4.9.4 撤销请求宽限期

一旦发现需要撤销证书，订户应该实时提出撤销请求，如果确实因为客观原因导致延迟的，这个时间也不得超过 8 个小时。如果在宽限期内，因订户未及时提出撤销请求而产生的任何损失和责任，SHECA 并不承担。

4.9.5 电子认证服务机构处理撤销请求的时限

SHECA 收到撤销请求后，应进行合理处理，不得拖延。

SHECA 应在收到撤销请求后的 24 小时内展开调查，并在两个工作日内根据以下标准判断是否进行撤销或其它合理处理。

1 所反馈问题的本质；

2 针对某张证书或某订户的问题报告的数量；

3 问题反馈方的身份（例如，来自具有法律强制力的机构针对某网站涉嫌参与非法活动的投诉效力要强于一个消费者声称未受到所订购货物的投诉）；

4 相关法律法规。

4.9.6 依赖方检查证书撤销的要求

证书撤销列表 CRL 作为公开的信息，依赖方可以通过下载的证书，在该证书拓展项中获取 CRL 列表，通过 https://www.sheca.com 网站（http 方式）查询

证书状态或通过在线证书状态协议（OCSP）方式查询等。

依赖方在信赖证书前，应根据 SHECA 和其授权的下级操作子 CA 最新公布的 CRL，主动检查该证书的状态。

同时，还需要验证 CRL 的可靠性和完整性，确保它是经过 SHECA 和其授权的下级操作子 CA 发行、包含 SHECA 和其授权的下级操作子 CA 的数字签名的。

4.9.7 CRL 发布频率

SHECA 每 24 小时更新和公布一次证书撤销列表（CRL）。对于子 CA 证书，至少每 6 个月签发和公布一次，对于根 CA 证书，必须每年公布一次。

SHECA 根据情况，可以自主决定缩短产生和更新 CRL 的时间。

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。

SHECA 承诺，在证书撤销后，最晚也将在撤销行为发生的 24 小时内发布证书撤销列表。

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 RFC6960 和 RFC5019 中的相关要求。

SHECA 提供的 OCSP 服务网址为：

http://ocsp3.sheca.com/ocsp/sheca/sheca.ocsp。

4.9.10 在线状态查询要求

2013 年 1 月 1 号开始，对于签发符合规定的证书，SHECA 支持使用 GET 的 OCSP 应用。

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。

在查询尚未签发证书的状态时，OCSP 的响应不能是“Good”，且 SHECA 对此进行监控。

自 2013 年 8 月 1 日起，根据 7.1.5 章节不符合技术约束条件的情况下 OCSP 响应不能是“Good”。

用户可以自由进行在线状态查询，SHECA 没有设置任何的读取权限。如果依赖方无法查询 CRL，则应通过 OCSP 或者访问网站的形式对证书状态进行查询。

4.9.11 撤销信息的其他发布形式

除了 X.509 V2 格式的 CRL 方式外，目前不提供其它的撤销信息发布方式。

4.9.12 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，并实时把证书发布到 CRL。SHECA 承担因密钥损害给订户造成的损失，并及时为其签发新的证书。

4.9.13 证书挂起的情形

SHECA 不支持证书挂起。

4.9.14 请求证书挂起的实体

不适用。

4.9.15 挂起请求的流程

不适用。

4.9.16 挂起的期限限制

不适用。

4.9.17 问题报告和处理机制

SHECA 建立并保持 7*24 小时的证书问题报告和受理机制，任何订户、依赖方、应用软件供应商或其他第三方发现证书可能存在问题、私钥出现或者怀疑出现泄露、证书滥用、或其他与证书相关的舞弊、泄露、滥用或不正当行为时，均可向 SHECA 进行通告或投诉。报告方式如下：

- 电子邮件：report@sheca.com
- 传真：021-36393200
- 电话：021-36393196

在接受通告或投诉后，SHECA 在 24 小时内开始调查证书问题报告，并向订阅者和提交证书问题报告的实体提供有关其调查结果的初步报告。对已经接受报告的证书进行鉴别和调查，并根据调查结果决定是否采取撤销或其他适当的方式进行处理,并在收到请求的两个工作日内根据调查结果告知报告人及其它相关方。鉴别和调查主要包括但不限于以下内容：

- 报告人的身份识别
- 问题的性质和产生原因
- 相应问题的出现次数和频率
- 证书签发等相关业务流程的重新审视及认定结果
- CP/CPS 和订户协议等相关规范的遵循
- 有关法律法规的遵循

此外，当 SHECA 发现涉及到恶意软件的代码签名证书被签发时，应当

- 在 1 个工作日内联系软件发布商，并要求其在 72 小时内回应
- 自发现起 72 小时内，SHECA 应当确定被当前事故影响的相关方数量
- 如果 SHECA 收到了软件发布商回应，则由 SHECA 和软件发布商共同决定撤销证书的合理时间
- 如果 SHECA 未收到来自软件发布商的回应，则通知软件发布商证书将在 7 天内被撤销，除非有已建档的证据表明撤销该证书会对社会大众产生巨大影响。

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 及其授权的发证机构的 CA 证书的签名来保证。CRL 仅提供定期的证书状态查询，目前 SHECA 每 24 小时发布一次 CRL。

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。

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。

4.10.2 服务可用性

证书状态服务必须保证 7X24 小时可用。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 方式查询，从而可以获得证书状态信息。

4.11 终止服务

下列情况，视为证书用户终止使用 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，将实时把该订户的证书撤销，并按照 CRL 发布策略进行发布。

4.12 密钥生成、备份与恢复

4.12.1 签名密钥生成、备份与恢复的策略与行为

为了保证订户签名私钥的安全性和唯一性，SHECA 建议订户自己生成密钥，

并进行备份，并在密钥丢失后进行恢复。

但是，订户可以委托 SHECA 代用户生成签名密钥对的有关操作，由于签名私钥遗失所造成的损失有订户自己承担，SHECA 对此不承担责任。

SHECA 将采取严格的措施保证用户密钥生成的安全性，并遵循国家密码管理相关规定和 FIPS 140-2 中关于密钥生成的相关规范。SHECA 不保留任何用户私钥的副本。SHECA 不提供订户私钥的托管和恢复服务。

4.12.2 加密密钥的生成、备份与恢复的策略与行为

证书用户的加密密钥由国家设立的专门密钥管理机构生成，其生成、备份策略由该机构制定。

针对密钥恢复，若证书用户需恢复密钥，需提交加密私钥的恢复申请，申请资料与申请证书的资料相同；录入员验证用户资料，确认用户申请恢复的密钥为该用户所有，录入密钥恢复申请数据；审核员审核申请数据，完成密钥恢复操作。所有操作及结果系统保留审计日志。录入员、审核员不可以互相兼任。用户需支付密钥恢复费用。

4.13 证书和 CRL 归档

用户信息和证书等数据，自证书到期或撤销后保留不少于 7 年。

CRL 文件采用刻光盘的形式进行归档，归档时间为 7 年。

5.认证机构设施、管理和操作控制

5.1 物理控制

SHECA 遵守的物理控制和安全策略，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 的根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 认证系统的主机房位于上海市电信大楼，备份机房位于 SHECA 办公地所在建筑内，均有三道物理的保护层，以监控和管理 SHECA 机房的物理通道。鉴于上海市所处的地理环境，发生地震等自然灾害的概率较小，SHECA 的主、备机房距离小于 5 公里，但主备机房均具备独立的防震、防火、防水、温控、门禁系统、视频监控系统和警报系统等，以保证认证服务的连续性和可靠性。所有机房的建设和管理严格按照 SHECA 的规定要求。机房内部一律禁止参观。只有经过 SHECA 授权的人员才能进入授权的部位和区域。机房采用高安全性的监控技术，包括视频、指纹、门禁等安全管理手段，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。

监控记录文件包括对机房通道上的所有踪迹的记录。所有经 SHECA 授权的人员在限制区域活动都需要有 SHECA 人员的陪同。SHECA 授权的人员清单会提供给 SHECA 运行负责部门, 以保证只有经授权的 SHECA 人员才能进入机房。对于要进入机房的 SHECA 的来访者，只有经过相应批准后，由 SHECA 授权的员工陪同才可进行。

所有 SHECA 授权的服务机构，包括注册机构、受理点等的证书服务系统也必须受到保护，确保只有经授权的员工才能进入该系统进行操作。SHECA 的管理员负责设置和检查注册机构、受理点管理员的权限。注册机构、受理点操作员的权限和责任在运作协议中也作出了规定。

5.1.2 物理访问控制

操作人员进入机房，必须通过 IC 卡门禁系统和指纹识别系统的身份检验，进出屏蔽机房、系统机房等重要区域，必须两人以上同时进入，并有 24 小时视频监控。

操作人员进入工作区域进行操作，必须通过指纹验证和权限检验。

5.1.3 电力与空调

CA 系统所在机房由上海电信北区大楼电力中心统一 UPS 供电，该 UPS 配备两路不同市电保障供电不间断，并配备柴油机作为备机供电。

CA 系统空调系统使用独立的空调和通风设备，保证温度、湿度处于可控的范围之内，以保证系统稳定的运行。

SHECA 参照电信设施管理的规定进行维护和保养。

5.1.4 水患防治

SHECA 的 CA 系统所处的环境为密闭式建筑，并且采取了加高地板的处置措施，能够防止水患侵蚀。

5.1.5 火灾防护

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，避免火灾的威胁。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 介质存储

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 废物处理

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 异地备份

1、系统备份

CA 系统进行异地的系统备份，预防系统因为不定因素不能正常运行。在主系统不能正常运行时，备份系统将投入使用，继续提供认证服务。

2、数据备份

SHECA 同时进行异地的数据备份。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。

5.2 程序控制

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。为了保证可靠的人员管理，员工、第三方服务人员、顾问等应该是被认定为可信的人员，才可在可信的岗位进行工作。SHECA 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）的员工、第三方服务人员等（统称“人员”），在本 CPS 中均视为可信角色。

SHECA 明确规定 CA 关键职能的职位，他们包括：

1、应用系统管理员

2、操作系统管理员

3、数据库系统管理员

4、网络系统管理员

5、RA 管理员

6、录入员

7、审核员

8、密钥控制小组

9、安全执行小组

10、其他人员等。

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。

SHECA 根据本 CPS 和授权协议，制订其授权的证书服务机构（RA、RAT 及其它）的管理规范，规范证书服务机构和服务系统管理人员、操作人员的操作。在与此相关的软件设计中，充分考虑安全的牵制和约束。SHECA 对其授权的证书服务机构的责任进行合理划分，并通过系统和技术实现以及管理的责任义务上进行保证。

5.2.2 每项任务需要的人数

CA 和 RA 应该建立、维护和执行严格的控制流程，基于工作要求和工作安排建立职责分割措施，贯彻互相牵制、互相监督的安全机制，确保由多名可信人员共同完成敏感操作。

职责分割的策略和控制程序是基于实际工作职责的要求。对于认证业务来讲，最重要的敏感操作就是访问和管理 CA 密码设备、分配和管理密钥材料以及密钥口令的保护等。这些操作必须要求多名可信人员参与完成。这些敏感的内部控制流程要求至少有两名可信人员参与，要求他们有各自独立的物理或逻辑控制设施，关于 CA 的密钥设备的生命周期过程被严格的要求多名可信人员共同参加。关键的控制要进行物理和逻辑上的分割，如掌握关键设备的物理权限的人员不能再持有逻辑权限，反之亦然。

SHECA 确保单个人不能接触、导出、恢复、更新、废止 SHECA 存储的私钥。至少三个人，使用一项对参加操作人员保密的密钥分割和合成技术，来进行

任何 CA 密钥生成、恢复的操作。

对于证书申请的鉴别和签发，也需要至少两个可信人员操作才能完成。

对于重要的系统数据操作和重要系统维护，需要安排至少一人进行操作，一人进行监督记录。

SHECA 对于其运行和操作相关的职能有明确的分工，贯彻互相牵制、互相监督的安全机制。

对于重要的系统操作和维护，SHECA 通常安排一人进行操作，一人进行监督记录。

5.2.3 每个角色的识别与鉴别

对于所有将要成为可信角色的人员，必须进行严格的识别和鉴证，确保其能够满足所从事工作职责的要求。主要包括:

- 根据实际需要确定不同的角色，为其划分权限和要求，并设定不同角色的背景要求
- 对人员进行背景调查，使其符合相应角色的可信要求
- 赋予可信角色在系统中的权限，并为其发放令牌

在进行可信调查前，首先需要确认该人员的物理身份的真实性和可靠性，更进一步的背景调查需要按照本 CPS 的要求严格进行。

所有 SHECA 的在职人员，必须通过认证后，根据作业性质和职位权限的情况，发放需要的系统操作卡、门禁卡、登录密码、操作证书、作业帐号等安全令牌。对于使用安全令牌的员工，SHECA 将完整地记录其所有的操作行为。

所有 SHECA 人员必须确保:

- 发放的安全令牌只直接属于个人或组织所有
- 发放的安全令牌不允许共享
- SHECA 的系统和程序通过识别不同的令牌，对操作者进行权限控制。

5.2.4 需要职责分割的角色

需要进行职责分割的角色，包括但不限于下列人员：

- 从事证书申请信息验证的人员
- 负责证书申请、撤销、更新和信息注册等服务请求的批准、拒绝或其他操作的人员
- 负责证书签发、撤销等工作或者能够访问受限、敏感信息的人员
- 处理订户信息的人员
- 生成、签发和销毁 CA 系统证书的人员
- 系统上线或者下线的人员
- 掌握重要口令的人员

密钥及密码设备管理、操作人员

对于证书服务的受理，必须通过录入员、审核员两个角色进行才能完成。

对于根密钥的操作，必须有 3 名以上的根密钥的管理员人员同时到场，才能进行有关的操作。

SHECA 在系统遇到紧急情况需要联合抢修时，应至少有 1 名 SHECA 人员在场，抢修人员在 SHECA 人员的陪同下，执行许可的操作，所有操作、修改都保留记录。

非 SHECA 员工因物理修理、消防、强电故障等情况，需要进入 SHECA 机房实施修理时，必须经同意后，首先认证修理者的身份，然后由 SHECA 指定的员工始终陪同和监护，完成约定部位的修理。

5.3 人员控制

5.3.1 资格、经历和无过失要求

充当可信角色的人员，必须具备相应的教育背景、工作资格、从业经历等条件，必须能够提交相应的证明文件。

1、SHECA 认证业务系统的各类操作人员，必须具备可信、工作热情高的特点，没有影响本职工作的其他兼职行为，没有在认证业务操作上的不尽职、不负责的经历，没有违法乱纪的不良记录。

2、系统操作人员，必须具备认证系统的相关作业经验，或者通过 SHECA 相关的培训，才能担任。

3、管理人员，必须具备认证操作的实务经验和多年的系统管理运营经验。

5.3.2 背景审查程序

充当可信角色的人员需要经过严格的背景调查程序，一般在 5 年内应该重新调查一次。背景调查必须符合法律法规的要求，调查内容、调查方式和从事调查的人员不得有违反法律法规的行为。

根据不同可信岗位的工作特点，背景审查应该包括但不限于以下内容：

- 身份证明，如个人身份证、护照、户口本等
- 学历、学位及其他资格证书。
- 个人简历，包括教育、培训经历，工作经历及相关的证明人
- 无犯罪证明材料

背景调查应使用合法手段，尽可能地通过相关组织、部门进行人员背景信息的核实。并由认证机构的人力资源部门和安全管理人员共同完成人员评估工作。

SHECA 员工需要有 3 个月的考察期，关键和核心部位的员工通过录入考察期后，还需要额外期限的考察。根据考察的结果安排相应的工作或者辞退并且剥离岗位。SHECA 根据需要对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。

SHECA 会对其关键岗位的职员进行严格的背景调查。背景调查需要核实的材料和程序包括但不限于以下方面：

- 验证先前工作记录的真实性
- 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
- 检验无犯罪证明材料并确认无犯罪记录
- 通过适当途径了解是否有工作中的严重不诚实行为

在背景调查中，如果发现下列情形，可以拒绝其获得可信人员的资格：

- 存在捏造事实或资料的行为
- 借助不可靠人员的证明
- 有某些犯罪记录或者事实
- 使用非法的身份证明或者学历、任职资格证明
- 工作中有严重不诚实行为

SHECA 授权的证书服务机构管理员、操作员的审查可以参照 SHECA 对可信任员工的考察方式，在此基础上，增加考察和培训条款，但不得违背本 CPS 及相应 CP、授权协议以及 SHECA 公示的证书服务规范的要求。

SHECA 确立流程管理规则，据此员工受到合同的约束，不许泄露 SHECA 证书服务体系的敏感信息。所有的员工与 SHECA 签定保密协议，合同期满以后 2 年内仍然不得从事与 SHECA 相类似的工作。

如果有必要，SHECA 可以与有关的政府部门和调查机构合作，完成对员工的背景调查。

5.3.3 培训要求

SHECA 对员工进行以下内容的培训：

- SHECA 安全管理策略
- 工作岗位职责
- PKI 基础知识
- SHECA 认证系统使用的软件介绍
- SHECA 认证系统管理控制体系

- 身份验证、审核策略和程序
- 灾难恢复和业务连续性程序
- 认证策略、本 CPS 政策及相关标准和程序
- 针对验证程序存在的一般威胁，包括钓鱼和其他社会工程学行为
- 电子认证相关法律法规等
- 其他需要进行的培训

SHECA 将员工参加培训的情况形成相应记录进行存档，且验证审核人员在上岗之前必须通过培训达到 Baseline Requirement 中要求的从事该项工作所必需的技能水平。

5.3.4 再培训周期和要求

根据 SHECA 策略调整、系统更新等情况，SHECA 可能要求员工进行继续培训，以适应新的变化。

对于公司安全管理策略，应该每年至少进行一次培训

认证系统运营相关的人员，每年至少进行一次相关技能和知识培训。

对于认证系统的升级、新的系统的使用、PKI/CA 和密码技术的进步等，都需要根据情况安排相应的培训。

5.3.5 工作岗位轮换周期和顺序

SHECA 认证系统的运行维护人员和负责系统设计、开发的人员承担不同的职责，双方的岗位互相分离，为了保证安全，后者不能成为前者，即实行开发员工和运行员工分离的原则。

为了配合认证系统的运营需要和岗位适应性的需要，SHECA 会根据情况选派适当的人选，在不同的岗位进行轮换。但是这种轮换不得和上述的岗位分离原则相违背。

5.3.6 未授权行为的处罚

当 SHECA 员工被怀疑，或者已进行了未授权的操作，例如未经授权滥用权利或超出权限使用 SHECA 系统或进行越权操作，SHECA 在得到信息后立即中止该员工进入 SHECA 认证服务体系内工作。根据情节严重程度，可以采取批评教育、实施包括提交司法机构处理等措施。

一旦发现上述情况，SHECA 立即撤销或终止该人员的安全令牌。

5.3.7 独立合约人的要求

只有在人力资源不足或者特殊需要的必要情况下，当满足下列条件时，CA 和 RA 可以允许独立承包人或顾问成为可信员工：

- 没有合适的可信人员承担相应角色，而独立承包人和顾问能够填补相应空缺
- 独立承包人或顾问能够被当作可信员工一样信赖

否则，独立承包人或顾问只能在可信人员陪同和直接监督下有权访问相关安全设施。

除了必须就工作内容签署保密协议以外，还需要对独立承包人或顾问进行必要的知识培训和安全规范培训，使其能够严格遵守 SHECA 的规范。

5.3.8 提供给员工的文档

为了使认证系统的运营持续正常安全的运行，应该给相关员工提供有关的文档，至少包括：

- 系统软、硬件的操作说明文件、密码设备的操作说明文件、WWW 服务的操作说明文件
- 认证系统本身的操作说明手册
- CP、电子认证业务规则和有关的协议和规范
- 内部操作文件，包括备份手册、灾难恢复方案等
- 岗位说明
- 公司相关培训资料

- 相关安全管理规范

5.4 审计日志程序

5.4.1 记录事件的类型

SHECA 必须记录与 CA 和 RA 运行系统相关的事件。这些记录，无论是手写、书面或电子文档形式，必须包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。包括但不限于:

1、证书订户服务申请和撤销的信息，如申请表、协议、身份资料和其他相关信息等。

2、CA 密钥的生成、存储、恢复、归档和销毁等。

3、认证系统各类服务系统密钥对的生成、内置、变更等成功和失败的纪录。

4、认证系统日常运作产生的日志记录文件。

5、CRL 的操作记录。

6、进出 SHECA 控制区域内的表格、安全令牌进出敏感区域的纪录、机房工作日志、系统日常维护记录、监控录像等。

7、系统软硬件设备上线、更换、下线等的纪录。

8、认证机构、注册机构和受理点之间的协议、规范和相关工作记录。

9、SHECA 还要记录与系统不直接相关的事件，例如：物理通道参观记录、人事变动。

10、可信人员管理记录，包括网络权限的帐号申请记录，系统权限的申请、变更、创建申请记录，人员情况变化。

11、系统安全事件，包括：成功或不成功访问 CA 系统的活动，对于 CA 系统网络的非授权访问及访问企图，对于系统文件的非授权的访问及访问企图，安全、敏感的文件或记录的读、写或删除，系统崩溃，硬件故障和其他异常。

12、防火墙和入侵检测系统记录的安全事件。

5.4.2 处理日志的周期

SHECA 定期对日志记录进行审查，对审查记录行为备案，每年进行的审查不得少于 2 次。

5.4.3 审计日志的保存期限

SHECA 应保留系统审计日志至少 7 年，法律法规另有规定的，按照相关法律法规执行。

5.4.4 审计日志的保护

SHECA 执行严格的物理和逻辑访问控制措施，以确保只有 SHECA 授权的人员才能接近这些审查记录。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。

5.4.5 审计日志备份程序

SHECA 保证所有的审查记录和审查总结都按照 SHECA 备份标准和程序进行备份。根据记录的性质和要求，有实时、每天、每周、每月和每年等多种形式的备份，采用在线和离线的各种备份工具。

5.4.6 审计收集系统

SHECA 的审计收集系统涉及的对象包括：

- 证书管理系统
- 证书签发系统
- 证书目录系统
- 证书审批受理系统
- 备份恢复系统
- 访问控制系统（包括防火墙）
- 用户服务系统

- 网站、数据库安全保障系统
- 其他 SHECA 认为有必要审查的系统

SHECA 采用自动和手工结合的方式，进行上述系统日志的收集和审查，以保证系统安全运行的需要。

5.4.7 对异常事件的通告

在认证系统的运行出现影响安全控制措施的时候，必须通知安全管理人员，并采取有关的应对措施。如果严重影响到系统的运行，导致无法提供正常的证书服务，SHECA 将会通过网站和其它方式向用户进行通告。

在 SHECA 进行审查中发现的攻击现象，SHECA 将记录攻击者的行为，在法律许可的范围内追溯攻击者，SHECA 保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。是否通知攻击者或肇事者，由 SHECA 决定。

5.4.8 脆弱性评估

审计过程中被记录的事件部分的被用来监控系统脆弱性，逻辑安全脆弱性评估可以根据记录数据实时进行，也可以按天、月或年进行。

通常，SHECA 每年至少会进行一次系统安全性评估，其中包括从政策层面以及内部和外部对系统可能面临的威胁进行评估。根据评估结果，和系统日志的日常审计和监督实施，及时调整和系统运行密切相关的安全控制措施，以便将系统运作的风险降到最低。包括：

- 操作系统的脆弱性评估
- 物理设施的脆弱性评估
- 证书系统的脆弱性评估
- 网络的脆弱性评估

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:

1、SHECA 的系统建设和升级文档

2、证书申请信息、证书服务批准和拒绝的信息、与证书订户的协议、证书和 CRL 等

3、系统运行和认证服务产生的日志数据、认证系统证书密钥升级和更新信息等

4、电子认证服务规则、各类服务规范和运作协议、管理制度等

5、系统数据库数据

6、人员进出记录和第三方人员服务记录

7、监控录像

8、员工资料，包括背景调查、录用、培训等资料

9、各类外部、内部审查评估文档

证书订户的签名私钥和加密私钥由订户自己保存。有关私钥的保存责任应由订户本身承担。

5.5.2 归档记录的保存期限

除了法律法规和证书主管机构提出的保存期限以外，SHECA 制订的有关第三方电子认证服务运营信息的归档保存期限至少应该如下:

1、电子认证业务规则，证书策略，用户申请信息表格和相关协议，订户申请、更新、撤销的证书和过期证书，至少保存到证书有效期结束后 7 年。其中面向政务部门的电子政务电子认证服务，相关材料信息保存期为证书失效后十年。

2、证书用户申请、查询、撤销证书的服务记录，至少保存到证书有效期结束后 7 年。

3、订户证书和密钥的相关变动信息，至少保存 7 年。

4、认证机构的证书和密钥，以及相关的变动信息，至少保存 20 年。

5、视频监控录像内容在系统本地硬盘中保存 1 个月。每周对监控系统的视频监控录像内容进行备份。备份内容必须妥善保管一年，一年后按照规定进行归档保存。

6、其他信息保留期限至少 5 年。

7、业务管理类记录，保留不少于 2 年。

8、与法律政策的规定不一致的，选择两者中较长的期限予以保存。

此外，在不违反法律法规和主管部门的规定的前提下，SHECA 可以自主决定信息的定期存档期限，并且不需要对此做出说明和解释。

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。

SHECA 保护相关的档案信息，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏，以确保这些存档内容在规定的期内，能够满足任何合法的读取使用需要。对于认为必要的资料，SHECA 会采取异地备份的方式予以保存。

SHECA 保存的申请者和用户基本情况资料和身份鉴别资料，非经政府主管机构或者司法机构经过合法的途径予以申请，任意无关的第三方均无法获知。

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 记录时间戳要求

上面条款所述的全部存档内容，都有时间标识，比如系统自动记录的时间，或者由操作人员手工标注的时间。该时间信息不采用数字时间戳这种基于密码的方式进行。

5.5.6 归档收集系统

SHECA 认证系统的相关运营信息，由 SHECA 内部的工作人员或者具备安全控制措施的内部系统，依照人工和自动操作两部分进行产生和收集。并且由具备相关权限的人进行管理和分类。

5.5.7 获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。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 电子认证服务机构密钥更替

SHECA 的根证书有效期最长不超过 30 年，任何由其签发的证书，包括子 CA 证书和订户证书，其有效期都短于根证书的有效期，任何由子 CA 其签发的订户证书，其有效期都短于子 CA 证书的有效期。

根证书及子 CA 证书的有效期，在证书内有明确的表示。

在证书到期以前，SHECA 将按照 UNTSH CP 的规定对根密钥进行更换，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：

1、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。

2、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。

3、生成和管理 CA 密钥对时，严格遵守密钥规范。

4、及时发布新的 CA 证书。

5、确保整个过渡过程安全、顺利，不出现信任真空期。

5.7 损害与灾难恢复

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，SHECA 制订了可靠的损害和灾难恢复计划，以应对突发事故导致的系统问题。

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 应在尽快完成恢复过程，如果无法在 6 小时内完成恢复过程，并且事故导致证书服务无法进行，则应启动异地备份机制，在 24 小时内恢复证书服务。

5.7.3 SHECA 私钥损害处理程序

SHECA 的根私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，SHECA 应该：

1、立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其它公共媒体对订户进行通告，采取措施保证用户利益不受损失。

2、立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。同时 SHECA 立即生成新的密钥对，并自签发新的根证书。

3、新的根证书签发以后，按照本 CPS 关于证书签发的规定，重新签发下级证书和下级操作子 CA 证书。

4、SHECA 新的根证书签发以后，将会立即通过 SHECA 信息库、目录服务器、HTTP 等方式进行发布。

5、采取合理的努力及时告知用户和包含 Asseco Data Systems S.A.的依赖方。

SHECA 的子 CA 的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，操作 CA 应该：

1、立即向 SHECA 进行汇报并生成新的密钥对和证书请求，向 SHECA 申请签发新的证书。

2、SHECA 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其它公共媒体对订户进行通告，采取措施保证用户利益不受损失。

3、立即撤销所有由该子 CA 签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。

4、新的子 CA 证书签发以后，按照本 CPS 关于证书签发的规定，重新签发订户证书。

5、新的证书签发以后，将会立即通过 SHECA 信息库、目录服务器、HTTP 等方式进行发布。

证书订户的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，订户应该按照本 CPS 的规定，首先申请证书撤销，并按照规定重新申请

新的证书。

5.7.4 灾难后的业务连续性能力

为了避免由于突发灾难造成认证业务停顿，SHECA 制订了一套完整的业务连续性计划，并建立了相应的异地灾难备份系统，将认证提供运营所需要的软硬件设备、数据存储、证书和用户信息、业务操作规范和灾难恢复文件，在离开现有运营系统适当距离的安全场所，建立了备份系统和备份文件。

异地灾难备份中心的认证业务恢复系统，根据需要每年将至少开展一次灾难恢复计划的训练和测试，并根据实际情况的变化，及时更新恢复计划和灾难恢复文件，并保存相应的归档纪录。从而保证在出现异常灾难时，SHECA 认证系统能够在最多 24 小时以内恢复系统运行和服务提供，从而将风险减到最小。

5.8 电子认证服务机构或注册机构的终止

如果 SHECA 因故计划终止经营，SHECA 会按照相关的法律规定，向主管部门报告，并按照法定程序进行操作，包括：

1、在法律法规规定的期限前，向主管机构、证书持有者和其他所有相关实体进行通告。

2、安排业务承接。

- 保存所有的认证服务相关运营资料，包括证书、用户信息、系统文件、CPS、规范和协议等。
- 停止有关运营服务。
- 清除系统根密钥。

当 SHECA 授权的证书服务机构因故终止服务时，SHECA 将按照与其签订的相关协议处理有关业务承接事宜和其他事项。因故终止服务时，SHECA 将按照与 RA 的运营协议处理有关业务承接事宜和其他事项。

6. 认证系统技术安全控制

6.1 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。

6.1.1 密钥对的生成

6.1.1.1 SHECA 根密钥的产生

SHECA 的根密钥对是由国家密码主管部门批准和许可的设备生成的。目前，SHECA 采购的部分加密机完全符合 FIPS140-2 标准，其他加密机符合国家密码管理相关规定的要求，并部分遵循 FIPS140-2 标准的相关规定，主要是在密钥生成、密钥操作和密钥保护等方面遵循 FIPS140-2 的要求。由于 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，国家对于密码产品有严格的管理要求，因此，SHECA 在选择加密设备时，仅参照 FIPS140-2 标准的要求，是在国家密码管理政策许可前提下的选择性适用，具体参照设备厂商提供的资料。

在生成 SHECA 的密钥对时，必须有超过 3 位的具备权限的密钥管理和操作人员在场，同时操作硬件加密机产生密钥对。任何人无法独自完成根密钥对的产生，而且密钥在加密机内部生成。任何和私钥有关的操作都在加密机内部进行，完成后将结果输出，私钥无法以明文或者密文的方式输出到加密机外。

6.1.1.2 订户签名密钥对的生成

订户证书的签名密钥对由订户生成。每个签名证书订户，可以自主选择国家密码主管部门批准许可的设备生成签名密钥对，例如由加密机、加密卡、智能密码钥匙（USB KEY）、IC 卡等生成，订户应确保其密钥生成过程安全可靠。用户在选择这些设备前，可以事先向 SHECA 咨询有关的系统兼容和接受事宜。SHECA 并不承诺接受所有类型的密码产生设备。SHECA 可以向用户提供符合国家密码管理相关规定的 USB Key 作为订户签名密钥的生成和存储设备。

证书订户签名密钥对的产生，必须遵循国家的法律政策。SHECA 支持多种

模式的签名密钥对产生方式，证书申请者可根据其需要进行选择。不管何种方式，密钥对产生的安全性都应该得到保证。SHECA 在技术、业务流程和管理上，已经实施了安全保密的措施。

6.1.1.3 订户加密密钥对的生成

加密密钥对由相应的国家密钥管理机构生成，并以安全的方式传送。

6.1.1.4 其他事项

1、证书订户负有保护私钥安全的责任和义务，并承担由此带来的法律责任。

2、UCA Global G2 Root 和 UCA Extended Validation Root 这两个根下的所有证书，CA 不允许为用户生成密钥。

6.1.2 私钥传送给订户

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，不允许传送。

通常，SHECA 不提供代为生成密钥对服务。但是当用户通过书面申请要求并经 SHECA 批准后，SHECA 通过离线的安全通道、采用了防篡改封装的方式将私钥分发给最终订户。用于激活私钥的数据通过其他途径发给订户。CA 应记录这种设备的分发。

6.1.3 公钥传送给证书签发机构

证书订户以公钥向 SHECA 申请签发证书时，该请求信息内的公钥，得到订户私钥签名、用户身份验证和信息完整性的保护，并且通过安全可靠的方式进行传输。

证书签发成功的回复消息，得到电子签名和信息完整性的保护，并且以安全可靠的方式进行传输。

6.1.4 电子认证服务机构公钥传送给依赖方

SHECA 的公钥包含在 SHECA 自签发的根 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。

此外，CA 还支持通过浏览器内置方式、软件协议方式（例如 S/MIME）将公钥分发给依赖方。

6.1.5 算法类型及密钥的长度

SHECA 支持的密钥长度为 RSA1024 位或以上，其中公开可信任的订户证书的 RSA 密钥长度应为 RSA2048 位或以上，采用 SM2 算法的密钥对应为 256 位。自 2021 年 6 月 1 日起，代码签名证书及时间戳证书的 RSA 密钥长度为 3072 位。

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

如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，SHECA 将会完全遵从。

6.1.6 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加密设备生成，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 当然的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加密设备进行，例如加密机、加密卡、USB Key、IC 卡等。SHECA 当然的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。

6.1.7 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：

1 签发代表根 CA 的证书；

2 签发中级 CA 的证书和交叉证书；

3 根 CA 和中级 CA 的 CRL (ARL)；

4 特定用途的 PKI 体系功能证书(如 OCSP 证书)。

中级 CA 密钥一般用于签发以下证书和 CRL:

1 订户证书;

2 特定用途的 PKI 体系功能证书(如 OCSP 证书);

3 订户 CRL。

订户的密钥可以用于提供安全服务，如信息加密和签名等。

SHECA 签发的证书是 X509 v3 版本，证书内包含了密钥用途扩展项。如果其签发证书的密钥用途扩展项内指明了用途, 证书订户必须按照该指明的用途使用密钥。

所有密钥的使用，都必须遵循本 CPS 及相关 CP 的规范。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

SHECA 使用国家密码主管部门批准和许可的主机加密服务器。密码模块的标准、使用和控制都符合国家的有关规定，并部分遵循 FIPS140-2 标准的相关规定，主要是在密钥生成、密钥操作和密钥保护等方面遵循 FIPS140-2 的要求。由于 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，国家对于密码产品有严格的管理要求，因此，SHECA 在选择加密设备时，仅参照 FIPS140-2 标准的要求，是在国家密码管理政策许可前提下的选择性适用，具体参照设备厂商提供的资料。

所采用的主机加密服务器均取得国家商用密码产品型号证书。其主要功能包括:

1、生成密钥：可以生成 4096 位或 2048 位的 RSA 密钥，可以生成多对对称密钥（通信密钥）。由物理噪声源作为随机数，生成密钥速度快。

2、密钥存储：可以存储生成的 RSA 密钥和通信密钥。密钥以安全方式存储，非法者不能获得密钥。

3、权限管理：可以初始化管理员和操作员，负责管理员、操作员权限的判

断。 管理员口令采用分割权限的密钥管理机制。

4、密钥备份：可以根据需要，在满足权限的情况下将主机加密服务器内的密钥等重要信息进行加密后备份到其他存储介质中并且可以导入相同型号的主机加密服务器中。

5、生成输出密钥：可以使用主机加密服务器的 0 号或 6 号密钥，生成可以输出加密设备的 RSA 密钥对，该密钥对已加密。

6、采用硬件的物理噪声源随机数发生器芯片产生随机数。

7、使用 IC 卡保存 PIN，对管理员和操作员身份通过 IC 口令卡进行识，口令采用分割权限的密钥管理机制。

8、客户端主机在调用主机加密服务器进行业务调用时需要握手通过，即需要验证口令通过，同时验证版本号的兼容性。

9、密钥经过加密后保存在电子存储元件中，在内部的程序设计上，不允许密钥以明文形式输出，不以明文形式出现在磁盘及内存中。

6.2.2 私钥控制

1、SHECA 采用多人控制策略来激活、使用、停止其私钥（m 选 n）。

SHECA 的私钥采用多人控制的策略（即 n out of m 策略， m>n, n>=3 ）。目前采用五人控制, 需要至少三个或三个以上的密钥控制人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。具有权限的密钥管理人员，分别持有分割后的一段密码。所有和私钥相关的信息，例如控制 IC 卡、保护 PIN 码等，分别由不同的管理人员来控制。

2、订户证书的私钥应由订户控制

订户证书的私钥应由订户进行控制并负责私钥的安全, 如需指定人员对私钥进行管理，则指定的人员必须经过有效授权，以防私钥被泄露、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。

6.2.3 私钥托管

SHECA 不提供私钥的托管服务。

加密私钥的保护、管理、存档、备份、托管等，由上海密钥管理中心（KM）进行规范和决定。证书订户可以就加密私钥的托管问题，可以与相应的国家密钥管理部门进行联系。

6.2.4 私钥备份

为了保证业务持续开展，认证机构必须创建 CA 私钥的备份，以备进行灾难恢复操作。私钥备份以加密的形式保存在硬件密码模块中，存储 CA 私钥的密码模块应符合 6.2.1 的要求。CA 私钥复制到备份硬件密码模块中要符合 6.2.6 的要求。

对于订户签名证书，如果其私钥存放在软件密码模块中，建议订户对私钥进行备份，备份的私钥需要采用口令保护等授权访问控制，防止非授权的修改或泄露。

对于订户加密证书，其加密私钥的保护、管理、存档、备份、托管等，由相应的国家密钥管理部门进行规范和决定。证书订户可以就加密私钥的备份问题，可以与相应的国家密钥管理部门进行联系。

6.2.5 私钥归档

SHECA 的私钥经过加密后按照严格的安全措施保存。CA 的私钥不进行归档。

6.2.6 私钥导入、导出密码模块

SHECA 的私钥，严格的按照 SHECA 规定的程序和策略进行备份，除此之外的任何导入导出操作将不被允许。当 CA 密钥对备份到另外的硬件密码模块上时，以加密的形式在模块之间传送，并且在传递前要进行身份鉴别，以防止 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

SHECA 不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。

对于存放在软件密码模块中的私钥，如果订户愿意并且自行承担相关风险，订户可自主选择导入导出的方式，操作时需要采用口令保护等授权访问控制措施。

6.2.7 私钥在密码模块的存储

SHECA 使用国家密码主管部门批准和认可的密码设备及密码模块进行私钥存储，所有在密码模块中存储的私钥，都以密文的形式保存。

订户的私钥存储在符合国家密码管理规定的 USB Key 介质中，所有在 USB Key 中存储的私钥，都以密文的形式保存。对于使用软件密码模块生成的私钥，最好在硬件密码模块（如 USB Key 、SmartCard ）中存储和使用，也可以使用有安全保护措施的特定软件密码模块。

6.2.8 激活私钥的方法

SHECA 默认，只有在通过密码验证后，方可激活私钥，除非用户自己进行变更，并愿意承担变更后的责任。

SHECA 的私钥存放于硬件加密模块中，其激活数据按照 6.2.2 进行分割。必须经过三个被授权的人员共同操作，才能进行激活。未经授权的任何人员，绝不可以进行激活或者存取使用。

对于存放在订户计算机软件密码模块中的私钥，订户应该采用合理的措施从物理上保护计算机，以防止在没有得到用户授权的情况下，其他人员使用订户的计算机和相关的私钥。如果存放在软件密码模块中的私钥没有口令保护，那么软件密码模块的加载意味着私钥的激活。如果使用口令保护私钥，软件密码模块加载后，还需要输入保护口令才能激活私钥。

对于存放在诸如订户 USB Key 、智能卡、加密卡、加密机或者其它形式的硬件密码模块中的私钥，订户可以通过口令、指纹、IC 卡等方式进一步保护。当订户计算机上安装了相应的驱动后，将 USB Key 、智能卡等插入相应的设备中，输入保护口令或指纹，则私钥被激活。

6.2.9 解除私钥激活状态的方法

一旦私钥被激活，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。

订户解除私钥激活状态的方式由其自行决定，例如退出、切断电源、移开令牌/钥匙，自动冻结等。订户必须自行承担其解除私钥激活状态操作的风险和责任。

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，加密设备必须被清空。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，由订户决定其销毁方法，订户必须保证有效销毁其私钥，并承担有关的责任。涉及到密钥到期后保存和归档的，订户必须按照本 CPS 的规定执行。

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，接受其颁布的各类标准、规范、评估结果、评价证书等各类要求。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，选择需要的模块。

6.2.12 USB Key 生命周期管理

SHECA 向用户提供符合国家密码管理相关的规定的 USB Key 作为订户签名密钥的生成和存储设备。SHECA 保证证书申请者获得的 USB Key 能够满足证书和私钥的管理和应用需求:

- USB Key 在提供给证书申请者前得到了妥善的保管，包括采购、库存、发放等管理都有严格的规范予以执行。
- USB Key 在使用时必须通过密码认证后才可以进行。

- USB Key 存储的私钥不能被导出，并且以密文的形式存放。
- USB Key 一旦发放给证书申请者，将为证书订户持有，由该订户完全控制和拥有。
- SHECA 向订户提供一年的 USB Key 质保服务。
- 订户在更新证书时，可以不更换 USB Key。
- 订户证书遗失、撤销或更新后，由用户自行处置其所持有的 USB Key。SHECA 不负责销毁或者回收订户的 USB Key。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

公钥的归档，其操作过程、安全措施、保存期限以及保存策略和证书保持一致。归档要求参照本 CPS 中 5.5 的相关规定。

6.3.2 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。对于签名用途的证书，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。对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

证书操作期和证书内包含的有效期一致。对于订户证书，有效期最长不超过 4 年。对于 CA 证书，最长的有效期不超过 30 年。

另外需注意的是无论是订户证书还是 CA 证书，有效期到了后，在保证安全的情况下，允许使用原密钥对对证书进行更新。但是密钥对不能无限期使用。

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**
根证书（2018 年之前签发）	30 年	30 年
根证书（2018 年之后签发）	25 年	25 年
中级 CA 证书	25 年	25 年
DV SSL 证书（2019 年 9 月 1 日之前）	不做规定	825 天
DV SSL 证书（2020 年 9 月 1 日之后）	不做规定	398 天
OV SSL 证书（2020 年 9 月 1 日之前）	不做规定	825 天
OV SSL 证书（2020 年 9 月 1 日之后）	不做规定	398 天
EV SSL 证书（2020 年 9 月 1 日之前）	不做规定	825 天
EV SSL 证书（2020 年 9 月 1 日之后）	不做规定	398 天
代码签名证书	不做规定	39 个月
EV 代码签名证书	不做规定	39 个月

其它类型订户证书	不做规定	48 个月
时间戳证书	15 个月	135 个月
OCSP 证书	12 个月	12 个月

6.4 激活数据

6.4.1 激活数据的产生和安装

为了保护私钥的安全，证书订户生成和安装激活数据必须保证安全可靠，从而避免私钥被泄漏、被偷窃、被非法使用、被篡改、或者被非经授权的披露。

CA 私钥的激活数据，必须按照关于密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。订户私钥的激活数据，包括用于下载证书的口令（以密码信封等形式提供）、USB Key、IC 卡的登陆口令等，都必须在安全可靠的环境下随机产生。

SHECA 产生的激活数据，包括用于下载证书的口令（以密码信封等形式提供）、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。这些激活数据，都通过安全可靠的方式，例如离线当面递交、邮政专递等方式交给订户。对于非一次性使用的激活数据，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

6.4.2 激活数据的保护

对于 CA 私钥的激活数据，必须将激活数据按照可靠的方式分割后由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求。

订户的激活数据必须进行妥善保管，或者记住以后进行销毁，不可被他人所获悉。如果证书订户使用口令或 PIN 码保护私钥，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书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。同时，为了配合业务系统的安全需要，应该经常对激活数据进行修改。

6.4.3 激活数据的其他方面

当私钥的激活数据进行传送时，应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

当私钥的激活数据不需要时应该销毁，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。

考虑到安全因素，对于申请证书的订户激活数据的生命周期，规定如下：

1、订户用于申请证书的口令，申请成功后失效。

2、用于保护私钥或者 IC 卡、USB Key 的口令，建议订户根据业务应用的需要随时予以变更，使用期限超过 3 个月后应要进行修改。

6.5 计算机安全控制

6.5.1 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，认证机构应只允许有工作需求的必要人员访问证书服务器，一般的应用用户在证书服务器上没有账户。核心系统必须与其它系统物理分离，生产系统与其他系统逻辑隔离。

6.5.2 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 生命周期技术控制

6.6.1 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。

6.6.2 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。

6.6.3 生命期的安全控制

无规定。

6.7 网络的安全控制

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。

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。

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，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。

6.8 时间戳

认证系统的各种系统日志、操作日志都应该有相应的时间标识。这些时间标识不需要采用基于密码的数字时间戳技术。

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)。

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

SHECA 除了使用证书标准项和标准扩展项以外，还使用 SHECA 规定的自定义扩展项。

1、证书扩展项

- 密钥用途

电子签名，不可抵赖，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。

	SSL 证书	代码签名证书	时间戳证书	CA 证书
0 digitalSignature	√	√	√	×
1 nonRepudiation	×	×	×	×
2 keyEncipherment	√	×	×	×
3 dataEncipherment	×	×	×	×
4 keyAgreement	×	×	×	×

5 keyCertSign	×	×	×	√
6 cRLSign	×	×	×	√
7 encipherOnly	×	×	×	×
8 decipherOnly	×	×	×	×

其它类型证书的密钥用途遵守 RFC5280，按需进行设置。

- netscape 证书类型

该扩展项用来向使用网页浏览器的证书依赖方声明证书被认可的应用类型，该扩展项声明了如下的密钥用途: SSL 客户端验证, SSL 服务器缎验证, S/MIME, 对象签名等。

- 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。

- 预证书毒标识扩展项

预证书必须包含毒标识扩展（OID：1.3.6.1.4.1.11129.2.4.3）。该扩展名必须有一个 extnValue OCTET STRING，标准符合 RFC 6962 第 3.1 节规定的 ASN.1 NULL 值的编码表示，即十六进制编码字节 0500。

- 扩展密钥用途

	时间戳证书	**代码签名证书**	**SSL 证书**
服务器验证 **1.3.6.1.5.5.7.3.1**	×	×	√

客户端验证 **1.3.6.1.5.5.7.3.2**	×	×	√
代码签名 **1.3.6.1.5.5.7.3.3**	×	√	×
安全电子邮件 **1.3.6.1.5.5.7.3.4**	×	×	×
时间戳 **1.3.6.1.5.5.7.3.8**	√	×	×

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

有关自定义扩展项的内容，请参考本 CPS 附录中关于证书自定义扩展项说明。

7.1.3 算法对象标识符

SHECA 签发的证书密钥算法标识符为 sha1RSA、sha256RSA，其中公开可信任证书的密码算法从 2016 年 1 月 1 日不应该适用 sha1RSA。

SHECA 使用的算法对象标识符，符合 ISO 对象标识符（OID）管理的规范。例如：

1、签名算法：

- SHA256withRSAEncryption 对象标识符为：{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
- SM3withSM2Encryption 对象标识符为：{iso(1) member-body(2) cn(156) ccstc(10197) sm-scheme(1) sm3WithSM2Encryption(501)}

2、摘要算法：

- sha256 的对象标识符为：{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)}
- sm3 的对象标识符为：{iso(1) member-body(2) cn(156) ccstc (10197) sm-scheme(1) sm3(401)}

3、非对称算法：

- rsaEncryption 对象标识符为：{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
- sm2Encryption 对象标识符为：{iso(1) member-body(2) cn(156) ccstc(10197) sm-scheme(1) sm2Encryption(301)}

4、对称算法

本 CPS 建议使用国家密码管理部门认可的对称算法。

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.501 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、单位或者设备）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

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。具体请参考本 CPS 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。

7.2.1 版本号

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。

7.2.2 CRL 和 CRL 条目扩展项

无规定。

7.2.3 CRL 下载

可以通过证书中签发的 CRL 扩展项标明的 URL 下载 CRL。

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），签发的 OCSP 响应符合 RFC6960 标准。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。

7.3.1 版本号

RFC6960 定义的 OCSP V1。

7.3.2 OCSP 扩展项

与 RFC6960 一致。

7.3.3 OCSP 的请求和响应

一个 OCSP 请求包含以下数据:

- 协议版本
- 服务请求
- 目标证书标识
- 可能被 OCSP 响应器处理的可选扩展

在接受一个请求之后，OCSP 服务端响应时进行如下检测:

- 信息正确格式化
- 响应服务器被配置提供请求服务
- 请求包含了响应服务器需要的信息，如果任何一个先决条件没有满足，那么 OCSP 服务端将产生一个错误信息；否则的话，返回一个确定的回复。

所有确定的回复都由 SHECA 证书签发者密钥进行数字签名，主要回复状态包括：证书有效、已撤销、未知。回复信息由以下部分组成:

- 回复语法的版本
- 响应服务器名称
- 对请求端证书的回复
- 可选扩展
- 签名算法对象标识符号

- 对回复信息散列后的签名

如果出错，OCSP 服务器会返回一个出错信息，这些错误信息没有 SHECA 证书签发者密钥的签名。出错信息主要包括:

- 未正确格式化的请求（malformedRequest）
- 内部错误（internalError）
- 请稍后再试（trylater）
- 需要签名（sigRequired）
- 未授权（unauthorized)

8. 认证机构审计和其他评估

SHECA 作为 UNTSH 的运营主体，每季度内部进行一致性审计和运营评估，并每次抽取 SSL 数字证书至少 3% 数量的证书进行评估，以保证证书服务的可靠性、安全性和可控性。除了内部审计和评估外，SHECA 还聘请独立的审计师事务所，按照 WebTrust 对 CA 的规则进行外部审计和评估。

8.1 评估的频率和情形

1、根据《中华人民共和国电子签名法》、《电子认证服务管理办法》等的要求，每年一次接受主管部门的评估和检查。

2、SHECA 按照国家主管部门的要求、国家相关标准和本 CPS 的规定运营和服务，按照 SHECA 制订的内部评估和审计规范，每季度定期执行一次内部的评估审核。对授权机构的主要检查形式为抽查检验关联机构的证书签发流程及证书格式。

RA、RAT 以及其他 SHECA 授权的证书服务机构或其他形式的关联体，都必须遵循本 CPS 及相应 CP，并接受 SHECA 对其所有的流程和操作进行审计，检验其是否符合本 CPS 和与之相关的 SHECA 在授权协议规定的、或者其它公示过的信任服务政策的规定。SHECA 对关联机构的评估，一般一年进行一次。SHECA 在和所有机构的授权协议中，都明确的规定了这一点。评估人员由 SHECA 根据要求指派。评估人员必须熟悉 SHECA 的规范和信任服务的相关知识，了解保证安全的基本知识，审计 SHECA 的规范、协议提供服务等情况，独立、公正地对关联单位作出评估结论。

3、SHECA 聘请独立的审计师事务所，按照 WebTrust 对 CA 的审计规则，每年进行一次外部审计和评估。

4、SHECA 每年进行一次风险评估工作，识别内部与外部的威胁，并评估威胁事件发生的可能性及造成的损害，评估目前的应对策略、技术、系统以及相关措施是否足够应对风险。

8.2 评估者的资质

1、SHECA 无条件接收信息产业主管部门的评估。对 SHECA 实施评估的评估者所具有的资质和经验，由主管部门决定。

2、在进行内部评估审计时，SHECA 要求评估人员至少具备认证机构、信息安全审计的相关知识，有二年以上的相关经验，并且熟悉本 CPS 的规范，以及应具备计算机、网络、信息安全等方面的知识和实际工作经验。内部评估由战略发展中心组织实施。

3、如果 SHECA 认为有必要聘请外部的审计者实施内部评估，那么该审计者应该具备以下的资质：

- 必须是经许可的、有营业执照的评估机构，在业界享有良好的声誉；
- 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作；
- 具备检查系统运行性能的专业技术和工具。

8.3 评估者与被评估者之间的关系

1、外部评估者(信息产业主管部门或者其委托的其他机构)和 SHECA 之间是独立的关系，没有任何的业务、财务往来，或者其它任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对 SHECA 进行评估。

2、SHECA 的内部评估者，与被评估的对象之间，也应是独立的关系，没有任何的利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对被评估的对象进行评估。

SHECA 可以根据需要，选择专业、公正、客观的专业审计评估机构，协助进行内部评估。

8.4 评估内容

1、SHECA 按照信息产业主管部门依法提出的评估要求和规范，接受其任何内容的评估。

2、SHECA 内部评估审核的内容包括:

- 是否制订和公布 CPS
- 是否按照 CPS 来制订相关的操作规范和运作协议
- 是否按照 CPS 及相关操作规范和运作协议开展业务
- 服务的完整性：密钥和证书生命周期的安全管理、证书撤销的操作、业务系统的安全操作、业务操作规范审查
- 物理和环境安全控制：信息安全管理、人员的安全控制、建筑设施的安全控制、软硬件设备和存储介质的安全控制、系统和网络的安全控制、系统开发和维护的安全控制、灾难恢复和备份系统的管理、审计和归档的安全管理等。

3、第三方审计师事务所按照 WebTrust For CA 规范的要求，对 SHECA 进行独立审计。

8.5 对问题与不足采取的措施

1、信息产业主管部门评估完成后，SHECA 必须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。

2、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。

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。

3、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，并接受再次审计和评估。

如果认证机构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，则认证机构必须在 30 天内制定改正行动计划，并在

合理的期限内执行它。

8.6 评估结果的传达与发布

1、信息产业主管机构在完成评估后，按照法律法规的要求对评估结果进行处理。对于审计的结果，将通过 https://www.sheca.com 网站进行公布。

2、SHECA 的内部评估结果在与被评估对象的相关人员进行讨论确定后，将其视为机密资料进行处理，只有被评估对象和评估人员以及 SHECA 安全认证委员会可以了解。非经 SHECA 安全认证委员会的批准或者被评估对象的授权，评估人员不能泄露给任何其他无关的第三方知晓。在必要的情况下，对 SHECA 关联实体评估的结果，其通知方法将在 SHECA 和被评估实体的协议中写明。

3、第三方审计师事务所评估完成后，对于审计的结果，将通过 https://www.sheca.com 网站进行公布。

任何第三方向被评估实体通知评估结果或者类似的信息，都必须事先明确向 SHECA 表明通知的目的和方式，并征得 SHECA 的同意，法律另有规定的除外；SHECA 保留在这方面的法律权力。

9. 法律责任和其他业务条款

9.1 费用

SHECA 对证书订户收取费用。证书订户有义务根据 SHECA 公布的价格或者 SHECA 与之签署的协议中指明的价格向 SHECA 支付费用。

证书及其相关服务的价格，在 SHECA 的网站 https://www.sheca.com 上予以公布。公布的价格按照 SHECA 明确指定的时间生效，若没有指定生效时间的，自该价格公布之日起七天后生效。SHECA 也可以通过其他方法通知订户价格的变化。

如果 SHECA 签署的协议中指明的价格和 SHECA 公布的价格不一致，以协议中的价格为准。

9.1.1 证书签发和更新费用

SHECA 对证书签发和更新的费用，公布在 SHECA 的网站 https://www.sheca.com 上，供用户查询。

该公布的价格经过上海市物价局批准通过。

如果 SHECA 签署的协议中指明的价格和 SHECA 公布的价格不一致，以协议中的价格为准。

9.1.2 证书查询费用

对于证书查询，目前 SHECA 不收取任何费用。除非用户提出的特殊需求，需要 SHECA 支付额外的费用，SHECA 将与用户协商收取应该收取的费用。

如果证书查询的收费政策有任何变化，SHECA 将会及时在网站 https://www.sheca.com 上予以公布。

9.1.3 证书撤销或状态信息的查询费用

SHECA 对证书撤销和状态查询，目前不收取任何费用。如果该项查询的收

费政策有任何变化，SHECA 将会及时在网站 https://www.sheca.com 上予以公布。

如果 SHECA 签署的协议中指明的价格和 SHECA 公布的价格不一致，以协议中的价格为准。

9.1.4 其他服务费用

1、如果用户向 SHECA 索取纸质的 CPS 或其他相关的作业文件时，SHECA 需要收取因此产生的邮递和处理工本费。

2、有关证书恢复、密钥托管、签名密钥备份、签名密钥恢复等服务，如果提供该项服务，那么 SHECA 将会及时公布相关费用，供用户查询。SHECA 与之签署的协议中指明的价格和 SHECA 公布的价格不一致，以协议中的价格为准。

3、其他 SHECA 将要或者可能提供的服务的费用，SHECA 将会及时公布，供用户查询。

9.1.5 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 及其授权的证书服务机构，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。

9.1.6 支付能力

SHECA 授权的证书服务机构应具有维持其运作和履行其责任的经济能力，它应该有能力承担对订户、依赖方等造成的风险。

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，包括但不限于：

1、建筑物与硬件设施的火灾等意外险。

2、证书责任险，保险范围涵盖所有 SHECA 依据本 CPS 签发的订户证书。

目前，SHECA 没有提供第三方保险服务。

9.2.2 其他资产

无规定。

9.2.3 对最终实体的保险或担保

目前，SHECA 没有提供第三方保险服务。SHECA 将在其网站 https://www.sheca.com 上及时发布保险策略。

证书订户一旦接受 SHECA 的证书，或者通过协议完成对证书服务的认可，那么就意味着该订户已经接受了 SHECA 关于保险和担保的规定和约束。

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 和其授权的证书服务机构、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；同时，SHECA 在与其授权的证书服务机构或其他形式的关联实体签署协议时，都将此作为必须满足的要求。

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 应满足其要求；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 个人隐私保密

9.4.1 隐私保密原则

SHECA 尊重所有的用户和他们的隐私，如果有与此相关的明确的隐私保护法律（如个人信息保护法）的出台，那么本 CPS 将自动予以引用并将其作为隐私保护的基本依据来执行。

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 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。

认证机构、注册机构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）。

9.4.6 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：

- 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

9.4.7 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 中另有规定或者发证机构和订户间另有协议, SHECA 向在证书中所命名的订户承诺:

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

- 发证机构签发给订户的证书符合本 CPS 的所有实质性要求。
- 发证机构将按本 CPS 的规定，及时撤销证书。
- 发证机构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。发证机构的行为若符合相关法律和本 CPS 的规定，即被视为发证机构作出了符合上述描述的合理的努力。

3、发证机构对依赖方的陈述

发证机构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。
- 发证机构完全遵照本 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，发证机构向 SHECA 信息库和所有合理依赖证书中信息的依赖方证明：发证机构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 注册机构的陈述与担保

注册机构 RA 按照程序取得了 SHECA 的授权后，将保证:

- 遵循本 CPS 和 SHECA 的授权协议以及其它 SHECA 公布的规范和流程，接受并处理申请者的证书服务请求，并依据授权设置、管理各类下级证书服务机构，包括 RAT 等。
- RA 必须遵循 SHECA 制订的服务受理规范、系统运作和管理要求，根据本 CPS、SHECA 公布的规范，RA 有权决定是否给申请者提供相应的证书服务。
- 按照 SHECA 的要求和规范，确定下属证书服务受理机构的设置方式、

管理方式和审核方式，这些方式的确定必须以书面的文件形式公布，涵盖并且不得与 SHECA 公布的相关条款产生冲突、矛盾或者不一致。

- 依据本 CPS 的规定，确保其运营系统处在安全的物理环境中，并具备相应的安全管理和隔离措施。RA 必须能够提供证书服务全部的数据资料及备份，并按照 SHECA 的要求，保证其与下属证书服务机构间的信息传输安全。RA 承诺严格执行为所有证书用户提供隐私保密的义务，并愿意承担因此而带来的法律责任。
- 接受 SHECA 根据本 CPS 和授权协议对 RA 进行管理，包括进行服务资质审核和规范执行检查。
- 承认 SHECA 对所有证书服务申请者的服务请求拥有最终处理权。
- 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。
- 为订户提供必要的技术咨询，使订户顺利地申请和使用证书。

9.6.3 其他关联服务机构的陈述与担保

受理点 RAT 的陈述

- 提供认证服务和其自身的管理，必须遵守本 CPS、相关授权运作协议的规定。
- 作为被授权的证书服务机构，接受授权机构对其进行的资格审核和管理评估。
- 对所有证书服务申请者的隐私信息负有保密责任，无论这种申请是否被批准。
- 遵守本 CPS 中的所有条款，履行身份鉴别和服务受理的责任。
- 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。
- 为订户提供必要的技术咨询，使订户顺利地申请和使用证书。

9.6.4 订户的陈述与担保

一旦接受发证机构签发的证书，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 及其授权的证书服务机构检查和核实；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 或其授权的证书服务机构。
- 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。
- 订户向发证机构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发证机构，那么，发证机构视为：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。
- 除非经订户和发证机构间的书面协议明确规定，订户保证不从事发证机构（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。

9.6.5 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。

9.6.6 其他参与者的陈述与担保

垫付商的陈述:

- 垫付商必须承担其所有垫付的证书费用，并按 SHECA 规定的方式付清。
- 垫付商的垫付行为，就表明其愿意并且能够承担本 CPS 规定的，对证书服务申请者的身份真实性提供担保的责任。
- 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，导致签发数字证书错误、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 必须承担其它的义务或 SHECA 必须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 签发的数字证书。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 有限责任

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。

9.9 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 应承担赔偿责任。
- 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 应赔偿订户的损失。

- 因 SHECA 的根密钥出现问题，造成订户证书出现问题的，SHECA 应赔偿相关的损失。
- 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、注册机构（包括受理点）的赔偿责任

- 注册机构及其操作人员没有妥善保管订户的注册和身份验证的相关隐私信息，而造成订户信息泄漏、被冒用、篡改或者任意使用导致产生损失的，注册机构应负担损害赔偿责任。
- 如果因为操作人员故意、恶意或者疏忽，没有按照本 CPS 的规定办理证书服务注册，或者违反法律法规而造成订户损失的，注册机构应赔偿用户的直接损失，以及其他随之产生的附带损失和相关补偿。
- 因为注册机构的原因造成系统或者软件错误，未能在本 CPS 规定的时间内，将订户的证书申请、撤销、更新等请求信息发给 SHECA，而导致订户或者依赖方损失的，注册机构应负担所有的损害赔偿责任。
- 该类赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

3、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 及其授权的证书服务机构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 及其授权的证书服务机构，以及不当交付他人使用造成 SHECA 及其授权的证书服务机构、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 及其授权的证书服务机构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 及其授权的发证机构，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 及其授权的证书服务机构对于任何人（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、单位类证书，不超过 50，000 元

3、设备类证书，不超过 80，000 元

4、SSL 证书，不超过 100，000 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。

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 ））

上海市数字证书认证中心有限公司

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，战略发展中心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及最新版本的 SSL 基准要求规范，符合认证业务开展的实际需要。

本 CPS 的修订，由战略发展中心提出修订报告后，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。

所有以书面形式提供给订户的 CPS 修订，按以下规则发送：

- 接受者是公司或其它单位组织，则向在 SHECA 及其授权的证书服务机构登记的联系地址发送信息。
- 接受者是个人，则向其申请书上登记的地址发送。
- 这些通知可能用快递或挂号信的方式发送。
- SHECA 可以选择通过电子邮件或其他方式向订户发送通知，邮件地址在订户申请证书时已注明。

9.12.3 修订同意

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。

9.12.4 必须修改业务规则的情形

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

对 CPS 的修订将在发布 7 天以后生效。 除非在这 7 天结束前，SHECA 以同样的方式发表一个撤消修订的通知。

尽管如此，如果 SHECA 发表了一项修订，而如果该修订不能及时生效，将

导致对全部或部分 SHECA 认证服务体系的损害，那么该修订在它发布之日起立即生效。

9.13 争议处理

作为证书认证争议裁决的专家机构，SHECA 安全认证委员会专家组收集相关的证据以促进争议解决，协调 SHECA、当事人之间的相互关系，并作为争议建议报告的最终撰写人。

无论专家组是否完成建议报告并将建议传达，以及形成怎样的裁决决定，并不妨碍 SHECA、当事人及其他关联利益方采取与法律和本 CPS 一致的方式，寻找其它的解决措施。

9.14 管辖法律

本 CPS 接受《中国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 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《中国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》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。

SHECA 在根据修改 CPS 后，通过向 questions@cabforum.org 发送消息并接收其已发布到 CPS 的确认信息，通知 CA/浏览器论坛新添加到其 CPS 中的相关信息。公共邮件列表并在 https://cabforum.org/pipermail/public/ 上提供的公共邮件档案中建立索引（或论坛可能指定的其他电子邮件地址和链接），以便 CA/浏览器论坛可以考虑 对这些要求进行相应修订。

如上文所述，必须在 90 天内适当改变做法，修改 SHECA 的 CPS，并通知 CA/浏览器论坛。

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。

9.17 安全资料的财产所有

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介质。
- 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介质。
- 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。

附录

1 根证书

1.1 在用根

1、UCA Root

国家= CN

组织 = UniTrust

通用名 = UCA Root

序列号: 09

有效期: 2004 年 1 月 1 日 到 2029 年 12 月 31 日

证书 SHA1 摘要: 82 50 be d5 a2 14 43 3a 66 37 7c bc 10 ef 83 f6 69 da 3a 67

2、UCA Root G2

国家= CN

组织 = UniTrust

通用名 = UCA Root G2

序列号: 44 52 a0 b2 e9 05 39 46 7a 53 b0 4f 23 6a a3 c3

有效期: 2016 年 9 月 1 日 到 2036 年 12 月 31 日

证书 SHA1 摘要: 57 1e 0b 0b 40 f7 96 6d 1e bb 7a cf c6 4e 70 4d 31 9b f4 fd

3、UCA Global G2 Root

国家= CN

组织 = UniTrust

通用名 = UCA Global G2 Root

序列号: 5d df b1 da 5a a3 ed 5d be 5a 65 20 65 03 90 ef

有效期: 2016 年 3 月 11 日 到 2040 年 12 月 31 日

证书 SHA1 摘要: 28 f9 78 16 19 7a ff 18 25 18 aa 44 fe c1 a0 ce 5c b6 4c 8a

4、UCA Extended Validation Root

国家= CN

组织 = UniTrust

通用名 = UCA Extended Validation Root

序列号: 4f d2 2b 8f f5 64 c8 33 9e 4f 34 58 66 23 70 60

有效期: 2015 年 3 月 13 日 到 2038 年 12 月 31 日

证书 SHA1 摘要: a3 a1 b0 6f 24 61 23 4a e3 36 a5 c2 37 fc a6 ff dd f0 d7 3a

1.2 停用根

1、UCA Root-G1

组织 = UnitedCA

通用名 = UCA Root

序列号: 01 00 00 22

有效期: 2001 年 1 月 1 日 到 2013 年 1 月 1 日

证书SHA1摘要: 31 20 f2 95 41 77 30 07 5f 8c d4 2d 0c ae 00 8e b5 72 6e f8

2、UCA Global Root

国家= CN

组织 = UniTrust

通用名 = UCA Global Root

序列号: 08

有效期: 2008 年 1 月 1 日 到 2037 年 12 月 31 日

证书 SHA1 摘要: 0b 97 2c 9e a6 e7 cc 58 d9 3b 20 bf 71 ec 41 2e 72 09 fa bf

2 密码算法和密钥强度

2.1 根证书

	摘要算法	RSA 算法
UCA Root	SHA-1（注 1）	2048 位
UCA Root G2	SHA256	2048 位
UCA Global G2 Root	SHA256	4096 位
UCA Extended Validation Root	SHA256	4096 位

注 1：该根证书自 2016 年 1 月 1 日后不再签发任何使用 SHA-1 算法的子 CA 证书或订户证书。

2.2 子 CA 证书

	摘要算法	RSA 算法
UCA Root 下属子 CA 证书	SHECA G2：SHA256	SHECA G2& SHECA G2-1：2048 位
UCA Root G2 下属子 CA 证书	SHA256	2048 位
UCA Global G2 Root 下属子 CA 证书	SHA256	2048 位
UCA Extended Validation Root 下属子 CA 证书	SHA256	2048 位

注 2：该子 CA 证书自 2016 年 1 月 1 日后不再签发任何使用 SHA-1 算法的订户证书。