协卡网络信任服务体系

EV 证书认证业务规则

UniTrust Network Trust Service Hierarchy

Extended Validation Certification Practice Statement

1.5.3 版本

生效日期：2023 年 04 月 18 日

上海市数字证书认证中心有限公司

上海市四川北路 1717 号嘉杰国际广场 18 楼

《协卡网络信任服务体系　EV 证书认证业务规则》

UniTrust Network Trust Service Hierarchy Extended Validation Certification Practice Statement

任何需要本文的的单位或者个人，可以与上海市数字证书认证中心有限公司战略发展部联系：

地址：上海市四川北路 1717 号嘉杰国际广场 18 楼 200080
电话：86-21-36393197
电子邮件：policy@sheca.com

商标说明

“UniTrust”、“协卡”是上海市数字证书认证中心有限公司注册（SHECA）的商标，也是 SHECA 的服务标识。

本文件历史变更记录

版本	生效日	作者	发布者	说明
V1.5.3	2023 年 04 月 18 日	俞晓卉	SHECA 安全认证委员会	修订发布
V1.5.2	2022 年 04 月 18 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.5.1	2021 年 11 月 15 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.5	2021 年 6 月 18 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4.9	2021 年 4 月 29 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4.8	2020 年 8 月 11 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4.7	2020 年 6 月 5 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4.6	2020 年 4 月 30 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4.5	2020 年 3 月 27 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4.4	2019 年 5 月 29 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4.3	2018 年 9 月 10 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4.2	2018 年 8 月 31 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4.1	2018 年 7 月 12 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.4	2018 年 6 月 1 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.3	2017 年 5 月 24 日	熊媛媛	SHECA 安全认证委员会	修订发布
V1.2	2016 年 5 月 25 日	崔久强	SHECA 安全认证委员会	修订发布
V1.1	2014 年 4 月 25 日	崔久强	SHECA 安全认证委员会	修订发布
V1.0	2013 年 4 月 28 日	崔久强	SHECA 安全认证委员会	初次发布

变更摘要

版本	描述
V1.5.3	披露新的中级根证书 SHECA OV Server CA G7; 更新中级根状态; 披露已撤销的中级根 ARL/CRL 更新频率
V1.5.2	披露新签发中级根 CECloud Secure Server CA V1，SHECA SM2 Identity CA G1 ，SHECA SMIME CA G1
V1.5.1	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
V1.5	ARL 更新频率 代码签名和时间戳证书算法长度要求更新
V1.4.9	披露新中级根 删除上一版本 3.2.4.1 第 2 条第（8）、（9）种域名验证的方式
V1.4.8	披露 LDAP 地址 机房电力供应
V1.4.7	披露新的根证书 UniTrust Global Root CA R1，UniTrust Global Root CA R2 新用于签发 EV 证书的根证书 UCA Root G2

	调整证书发起时机制
V1.4.6	删除上一版本 3.2.4 第 2 条第 (3) 种通过电话进行域名验证的方式 调整证书撤销机制 增加初步调查报告机制
V1.4.5	披露新的交叉根证书 UCA Global G2 Root 证书有效期变更 证书域名验证方式变更
V1.4.4	根证书增加 UniTrust PTC Root CA R1, UniTrust PTC Root CA R2 增加撤销代码签名证书的情形
V1.4.3	增加变更摘要
V1.4.2	修改 EV 证书层次架构图 修复部分措辞及语法错误
V1.4.1	数据源准确性,声明 825 天有效期限制 修改 IP 地址的验证流程 增加 CAA 记录检查要求
V1.4	UNTSH 证书层次架构调整 增加 OID 列表 修改域名验证方式
V1.3	证书撤销请求方、撤销流程等
V1.2	密钥对和证书使用
V1.1	增加证书撤销的情形 调整证书撤销流程 增加附录 C CRL 格式
V1.0	--

声明

本 EV 证书认证业务规则（CPS）全部或者部分支持下列标准：

- Guidelines For The Issuance And Management Of Extended Validation Certificates
- 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进行评估，审计评估报告将在 www.sheca.com 网站及 WebTrust 相关网站上进行公布。

目 录

1. 导言

本文档是协卡网络信任服务体系（UniTrust Network Trust Service Hierarchy）的 EV 证书认证业务规则（UniTrust Network Trust Service Hierarchy Extended Validation Certification Practice Statement，缩写为 UNTSH EV CPS）。协卡网络信任服务体系（UniTrust Network Trust Service Hierarchy）是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。

UNTSH EV CPS 阐述了 SHECA 在提供证书签发、管理、撤销、更新等证书服务时遵循的具体要求。UNTSH EV CPS 遵循《中华人民共和国电子签名法》的规定，根据协卡网络信任服务体系 EV 证书策略（UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policies，缩写为 UNTSH EV CP）制订，符合 UNTSH EV CP 的要求。UNTSH EV CP 是 UNTSH 关于 EV 证书的最重要的政策声明，建立了 UNTSH 内批准、签发、管理、使用、撤销、更新 EV 证书及相关信任服务时的业务、法律和技术等规则和要求。这些规则和要求保证了 UNTSH EV 证书信任的安全性和完整性，适用于 UNTSH 的所有参与方，从而提供了整个 UNTSH EV 框架内统一信任的保证。更多信息请参阅 UNTSH EV CP。

SHECA 运营的 UNTSH，包含了从属于它的用户、订户、依赖方等组成部分。UNTSH EV CP 确立了所有参与方必须遵循的要求，本 CPS 描述了 SHECA 及 UNTSH 内的各个参与方如何满足上述要求而采用的具体做法和措施，包括：

- 安全的管核心基础设施从而支撑整个 UNTSH 体系
- 根据 UNTSH EV CP 的要求签发、管理、撤销、更新 EV 证书

本 CPS 遵循 IETF RFC 3647 关于证书策略和证书认证业务规则的架构，符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的下列规范最新版本的要求：

- 扩展验证证书签发和管理指南（Guidelines for the Issuance and Management of Extended Validation (EV) Certificates)
- 扩展验证代码签名证书签发和管理指南（Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates)
- 公众可信证书签发和管理基线要求（Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates)

在本文件和上述规范发生歧义时，优先以上述规范的要求为准。SHECA 签发的 EV 证书在任何时候根据 UNTSH EV CP 规定均接受 CA/浏览器论坛（CA/Browser Forum）相关规范的要求。SHECA 明确声明所有包含 UNTSH EV CP 和本 CPS 策略标识符的证书，其签发和管理均符合 CA/浏览器论坛（CA/Browser Forum）的规范。

1.1 概述

本 CPS 阐述了 SHECA 签发 EV（Extended Validation）证书时遵循的程序，符合 CA/浏览器论坛（CA/Browser Forum）发布的扩展验证证书指南（Guidelines for Extended Validation

Certificates）的要求。该指南描述了 CA 机构在签发 EV 证书时必须满足一定的最低要求。

本 CPS 适用于 UNTSH 内的 EV ROOT CA、EV SSL CA 和 EV Codesigning CA，以及相关用户、订户、依赖方等实体。本 CPS 作为一个单独的文件，涵盖了和签发和管理 EV 证书相关的具体操作和流程，SHECA 还可以发布新的 CPS 作为本 CPS 的补充，以满足政府特定政策的要求或者其它行业标准和规范的要求。通常这些补充的策略也适用于相关证书订户和依赖方。本 CPS 只是 UNTSH 一系列相关文档中的一个，其余还包括：

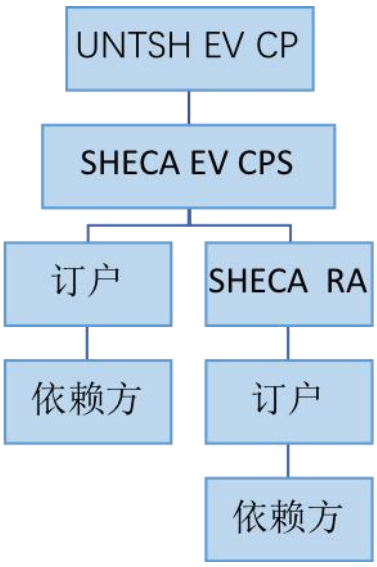
- 订户协议
- CA 和 RA 运营规范
- 依赖方协议
- 评估和审计规范
- 以及其它相关协议和规范

按照本 CPS 签发的 EV 证书, 其对象是向 SHECA 申请并通过所有相关身份鉴别的各类机构。所有 UNTSH EV 证书的订户及依赖方必须参照本 CPS 及相应 CP 的规定，决定对证书的使用和信任。

EV SSL 证书用于互联网上 SSL/TLS 身份验证，旨在通过 SSL/TLS 协议建立起安全的网络数据通讯管道。 持有该证书的机构的信息，可能会被浏览器等应用软件以特别的方式显示出来，使用户能够确认其访问的网站是由一个值得信赖的机构实体控制的。EVSSL 证书的首要目的是标识控制某一个网站的合法机构的身份（EV SSL 证书中包含的机构名称、营业地址、注册机构和注册号码等信息，能够给浏览器用户一个合理的保证，确保其正在访问的网站由一个合法的具体机构所控制）并启用加密通道（以便在互联网上实现用户浏览器和网站之间的信息加密传输）；其次是通过确认一个机构法律上和现实中的存在，帮助该机构获得运营某个网站的合法性声明，并提供协助解决网络钓鱼和其它形式在线欺诈的途（使得利用 SSL 证书进行网络钓鱼和在线身份欺诈更加困难, 并可以协助进行关于网络钓鱼和其它形式在线欺诈的执法调查）；此外, EV SSL 证书只关注证书中命名的主体的身份而不是该主体的行为, 并不提供任何关于该主体是否从事合法业务、是否符合法规要求、是否诚信经营以及跟该主体进行业务往来是否安全的担保、表示或保证。

1.1.1 UNTSH 架构

本 CPS 按照本 UNTSH EV CP 制定，RA 按照本 CPS 进行证书服务申请鉴别，订户、依赖方及其他相关实体按照本 CPS 及 EV CP 决定对证书的使用、信任并履行相关的义务。UNTSH 包含了根 CA、子 CA、注册机构（RA 中心），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 CPS 以及 EV CP 的要求。



1.1.2 UNTSH EV 证书层次架构

UNTSH 有 6 个 EV 根 CA，具体详见以下内容：

- 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。

UCA Global G2 Root 目前有 8 个在用的子 CA 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

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，其中 3 个正常使用，3 个已撤销的中级根，2 个已停用的中级根:

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

1.1.3 UNTSH EV 证书任等级

UNTSH 的 CA 发放的 EV 订户证书，都需要进行严格的身份鉴别。所有申请的各类机构主体，都必须提供证明材料以确认其真实存在，不面向个人提供 EV 证书服务。

从信任等级来看，EV 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。

1.2 文档名称和标识

本文档的名称为《协卡网络信任服务体系 EV 证书认证业务规则》(UniTrust Network Trust Service Hierarchy Extended Validation Certification Practice Statement，缩写为 UNTSH EV CPS)。

本 CPS 的对象标识符（OID）与协卡网络信任服务体系 EV 证书策略（UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policies ，缩写为 UNTSH EV CP）的对象标识符（OID）一致，不再为其分配专门的对象标识符（OID)。

1.3 参与者及适用范围

1.3.1 证书管理中心 （CA）

CA 包括 EV Root CA 和 EV SSL CA 和 EV Codesigning CA。均由 SHECA 建设和运营。此外，SHECA 设立安全认证委员会，作为 UNTSH 的策略管理机构。

（1）EV Root CA

EV Root CA 是最高证书签发机构，是 UNTSH 内 EV 证书的信任源，主要职责包括:

- 签发和管理自身证书和下级 CA 证书
- 管理和发布相关证书、证书撤销列表（CRL）
- 管理和运营证书信息库

（2）EV SSL CA

EV SSL CA 的主要职责包括:

- 签发和管理订户 EV SSL 证书
- 管理和发布相关订户证书及证书撤销列表（CRL）
- 管理和运营证书信息库

（3）EV Codesigning CA

EV Codesigning CA 的主要职责包括:

- 签发和管理订户 EV Codesigning 证书
- 管理和发布相关订户证书及证书撤销列表（CRL）
- 管理和运营证书信息库

（4）安全认证委员会

安全认证委员会由 SHECA 发起设立，是 UNTSH 策略管理机构，主要职责包括:

- 制定和发布证书策略（CP）
- 制定和发布证书认证业务规则（CPS）
- 制定和发布运营相关规范
- 制定和发布相关服务规范
- 监督和指导 UNTSH 运营服务

1.3.2 注册机构（RA）

注册机构（RA），主要负责对 EV 证书申请者进行身份标识和鉴别，验证签发 EV 证书所需要的相关信息，为 CA 签发 EV 证书提供信息。

SHECA 作为 EV 证书的 CA 运营机构，自行担任 EV 证书 RA，不再另行设立 RA。

1.3.3 订户

订户是证书主体（Certificate Subject)指称的实体，是 EV 证书及其对应私钥的拥有人。

本 CPS 中出现的订户，均指各类机构。SHECA 只对各类机构发放 EV 证书，不向自然人提供 EV 证书服务。

1.3.4 依赖方

依赖方, 是指使用证书里的公钥来验证电子签名有效性的实体。依赖方可以是证书订户, 也可以不是订户。

依赖方根据证书中包含的身份信息，用以识别域名、软件代码名称及其所属法人机构的信息

依赖方应根据证书中所包含的信息，决定是否要信任该证书或是否可以用于特定用途, 并需经过合理的判断，包括但不限于验证该证书的撤销信息等。

1.3.5 其他参与方

无。

1.4 证书用途

1.4.1 适用范围

SHECA 签发的 EV 证书主要用于身份识别的应用。

依据本 CPS 签发的 EV SSL 证书，可用来验证证书中标识的域名的身份，以及持有该域名的法人机构身份；依据本 CPS 签发的 EV Codesigning 证书，可用来验证证书中标识的软件代码提供方或发布方的身份。凡是经过验证后确定是由 SHECA 签发的 EV 证书，均表明该证书中所包含的信息真实有效，并且已经通过了适当且可靠的身份鉴别程序。

1.4.2 禁止使用的情形

除用于上述规定的范围外，禁止使用于任何可能会造成人身伤亡、精神伤害，或者对社会秩序与公共利益有重大危害的应用或业务，并且不得用于《电子签名法》或其他相关法律法规明确禁止或排除的应用。

CA 机构证书不能用来做任何 CA 功能以外的用途, 订户证书不得作为 CA 机构证书来使用

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的制定、发布和修改等事宜，由 SHECA 安全认证委员会全权负责。

1.5.2 联系人

SHECA 指定战略发展部作为本 CPS 联系人，专门负责本 CPS 的对外沟通及其它相关事宜。 任何有关本 CPS 的问题、建议、疑问等，都可以与 SHECA 战略发展部联系。

联系人：上海市数字证书认证中心有限公司战略发展部。

电话：86-21-36393195

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

1.5.3CPS 批准人

本 CPS 由 SHECA 安全认证委员会批准。

1.5.4 CPS 批准程序

本 CPS 由 SHECA 安全认证委员会批准，包括本 CPS 的修订和版本变更。

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 在公布本 CPS 后向主管部门备案。

1.6 定义与缩写

见附录 A。

2. 发布和信息库责任

2.1 信息库

SHECA 信息库提供证书、证书撤销列表（CRL）、证书策略（CP）、电子认证业务规则（CPS）、相关协议、证书在线状态（OCSP）等相关信息的查询和下载。

信息库网址如下：

https://www.sheca.com/repository

SHECA 也提供在线证书状态查询（Online Certificate Status Protocol，OCSP）服务。

2.2 认证信息发布

SHECA 需要发布的信息包括证书策略（CP）、电子认证业务规则（CPS）、订户协议和、依赖方协议、其它和证书使用和服务相关的协议、证书、证书撤销列表、证书在线状态查询等。

SHECA 提供明确的访问位置和方法，通过在线的方式对外发布证书、证书撤销列表和证书在线状态查询，这种信息的发布通常是证书服务的一部分。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。

此外，SHECA 在其网站的固定位置 https://www.sheca.com/policy 发布证书策略、认证业务声明、相关协议等。

2.3 发布时间或频率

SHECA 安全认证委员会批准本证书策略后将立即公布至信息库。

SHECA 根据以下规则更新和发布证书吊销列表（CRL/ARL）。

对于订户证书，至少每 5 天公布一次 ARL，或在订户证书被撤销后的 24 小时内公布。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，至少每 6 个月公布一次 CRL 或者在根/中级根证书被吊销后的 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/中级根证书被吊销，SHECA 将在网站公布相关吊销信息。

2.4 信息库访问控制

SHECA 信息库公开对外发布，不对包括 CP、CPS、证书、证书状态信息和 CRL 的访问进行限制，SHECA 保留设置访问控制措施以防止恶意访问的权利。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

EV 证书的名称应符合 X.501 甄别名（Distinguished Name，DN）规定。

EV SSL 证书、EV 代码签名（Code Signing）证书命名规则和要求必须被记录在按照 CP 制定的本 CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第九部分的要求相一致。EV SSL 证书、EV 代码签名（Code Signing）证书的甄别名必须包含通用名（common name，CN=）内容，经过验证的通用名应当包含域名、机构电子邮件地址、机构的合法名称等。

- EV 订户证书甄别名格式如下

名称属性	说明	是否必选
Country(C)	国别 指机构营业场所所在国家名称	是
Organization(O) Name	机构名称 必须是政府主管机构核准的名称	是
Organization Unit(OU)	部门或下级单位名称	否
State or Province (S):	省、直辖市或自治区 指机构营业场所所在省级区域名称	是
Locality (L)	城市 指机构营业场所所在城市名称	是
Common Name (CN)	用以标识证书所标识的主体的名称 ● 对于 EV SSL 证书，此处填写域名 ● 对于 EV Codesigning 证书，此处填写机构名称	是
Business Category	机构类型 包括私营组织、政府实体、商业实体、非商业实体四类。其中： ● 私营组织（V1.0,Cause 5.(b)）指依法注册并获得相关执照的个体工商户、个人独资企业、律师事务所等 ● 政府实体 V1.0,Cause 5.(c)指政府机关、事业单位等 ● 商业实体 V1.0,Cause 5.(d)指依法注册的企业类法人 ● 非商业实体 V1.0,Cause 5.(e)指社会团体、民办非企组织等	是

Jurisdiction Of Incorporation Locality Name	注册管辖地所在城市名称	否
Jurisdiction Of Incorporation State Or Province Name	注册管辖地所在省、直辖市或自治区名称	否
Jurisdiction Of Incorporation Country Name	注册管辖地所在国别	是
Serial Number	机构注册编号 由政府主管部门分配的编号，如果没有相应编号的，可填入机构成立日期	是
Street Address	机构营业场所地址	否
postalCode	机构营业场所邮政编码	否

- EV Root 证书甄别名如下

甄别名（DN）	说明
Country(C)	C=CN
Organization(O)	O=UniTrust
Common Name(CN)	CN= UCA Extended Validation root

- EV Server CA 证书甄别名如下

甄别名（DN）	说明
Country(C)	C=CN
Organization(O)	O= UniTrust
Common Name(CN)	CN= SHECA RSA Extended Validation Server CA

- EV Codesigning CA 证书甄别名如下

甄别名（DN）	说明
Country(C)	C=CN
Organization(O)	O= UniTrust
Common Name(CN)	CN= SHECA RSA Extended Validation Code Signing CA

3.1.2 对命名有意义的要求

订户证书中包含的主体识别名称，应当能够明确确定证书持有机构以及所要标识的网域名或软件发布者的身份，并且可以被依赖方识别。主体识别名称应当符合法律法规等相关规定的要求。

3.1.3 订户的匿名或伪名

申请人在申请证书时不允许使用匿名或假名，订户证书不允许使用匿名或假名。

3.1.4 解释不同命名的规则

订户证书按照 ITU-T X.520 名称属性定义解释不同命名。

3.1.5 命名的唯一性

订户的命名在 UNTSH 信任域内必须是唯一的。但一个订户可以拥有两张或以上的使用同一个主体甄别名的证书。

SHECA 将审核申请人提交的机构中英文名称、域名等的唯一性。

3.1.6 命名纠纷的处理

SHECA 不承担解决证书申请中关于命名纠纷的责任，发生纠纷时，订户应自行向司法机构或主管部门提出解决申请。

通常，当申请人提交的名称有纠纷时，SHECA 按照先申请先得的方式进行处理。

3.1.7 商标的识别、鉴别和角色

在证书信息中包含商标时，申请者应向 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 尊重申请人的商标等知识产权，但没有认可、验证商标等知识产权的义务。

证书申请人不得在其证书申请中使用侵犯他人知识产权的名称。SHECA 不会去决定证书申请人在申请证书时是否包含着知识产权信息，也不承担任何关于调解、仲裁或以其他方式解决域名、商标等知识产权纠纷的责任。SHECA 有权不因此类纠纷拒绝或暂停任何证书申请。

3.2 初始身份的确认

3.2.1 证明拥有私钥的方法

EV 证书中所包含的公钥及其对应的私钥由用户自行产生。

证书申请者必须证明持有与其证书中列出的公钥相对应的私钥，证明的方法包括：PKCS#10、其它与此相当的密钥标识方法，或者 SHECA 接受的其它证明方式。

3.2.2 机构身份的鉴别

SHECA 仅向机构用户提供 EV 证书申请服务。对机构身份的鉴别和审核符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南的要求。同时，根据 Mozilla

验证规范（Mozilla Verification Requirements）中的相关要求，当证书申请中包含国际化域名（internationalized domain names，IDNs）时，SHECA 对域名持有人的身份进行验证以检测是否存在 IDNs 的同形异义欺骗（homographic spoofing）行为。

1、鉴别要求

EV 证书只面向政府机关、企业单位、事业单位、社会团体以及其他机构提供，对于申请人必须进行以下鉴别和验证：

- 机构必须依法存在
- 证书申请人和机构名称一致
- 证书申请经办人必须获得机构授权

2、鉴别方法

（1）机构身份确认

- 验证组织机构代码证、工商营业执照、社会团体登记证、事业单位登记证等相关证明文件
- 通过查询第三方数据库等方式验证机构名称、注册信息等与申请人提交信息是否一致
- 验证机构经营场所
- 验证电话等机构联系方式

（2）证书申请经办人身份确认

- 验证身份证、护照等个人身份证明材料
- 验证银行卡、电话账单等证明材料
- 验证机构对经办人授权办理的证明文件
- 通过电话等与机构人事部门联系，确认相关人员身份及授权

（3）域名确认

- 通过“Whois”查询方式验证域名持有人信息

3.2.3 个人身份的鉴别

EV 证书不接受个人申请。

3.2.4 域名的确认和鉴别

3.2.4.1 域名验证方式

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3.3.3.4.1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，WHOIS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日期，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，建立“/.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BR3.2.2.4.6条执行。

(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

(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。

3.2.5 IP 地址的确认和鉴别

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，同时 SHECA 还需要向该 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 EV 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 3.2.4 中的域名验证方式验证返回的域名。

3.2.6 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。

3.2.7 数据源的准确性

SHECA 在选择是否依赖一个数据源之前，会对该数据源的可依赖性、数据的准确性以及数据的抗更改和抗伪造性进行评估。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 EV SSL 证书的验证数据源，若 SHECA 获得可依赖数据或文件的有效时间参考 CA/浏览器论坛（CA/Browser Forum）发布的扩展验证证书签发和管理指南（Guidelines for the Issuance and Management of Extended Validation (EV) Certificates）。

3.2.8 没有验证的订户信息

EV 证书中包含的所有订户信息均应进行验证。

3.2.9 授权的确认

任何一个个人声称其代表或从属于一个机构时，应当进行如下验证：

- 通过第三方身份证明服务或数据库、提交政府主管部门签发的文件等方式确认该机构存在
- 通过电话、有回执的邮政信函、雇佣证明或任何同等方式来验证该人属于上述机构以及其代表行为被该机构授权

3.2.10 互操作原则

不做规定。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

随着密钥使用时间增加，其可能遗失或遭破解的风险也随之增加，订户应定期更新密钥，以确保相关密钥的安全性。

EV 证书到期前，订户应重新按照 3.2 关于证明私钥拥有方法的规定提交证书申请。

3.3.2 撤销后密钥更替的识别与鉴别

订户证书被撤销后，必须重新生成新的公私钥对，并按照 3.2 的规定申请新的 EV 证书。

3.4 撤销请求的标识与鉴别

当订户提出 EV 证书撤销请求时， SHECA 将以初始注册时申请人提供的联络方式验证其请求。

4. 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请请求提交者

机构代表人或其授权的代理人可以作为 EV 证书申请的提交者。

4.1.2 注册过程和责任

EV 证书注册操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南的要求

申请者应事先了解订户协议、CP 及本 CPS 等文件约定的事项，特别是其中关于证书适用范围、权利、义务和担保的相关内容。

申请者应向 SHECA 递交 EV 证书申请表及相应证明文件，此行为即意味着申请者已经了解和接受上述内容。

申请者应自行产生公私密钥对，产生 PKCS#10 证书请求文件并递交给 SHECA。

4.2 证书申请处理

4.2.1 执行识别与鉴别

（1）机构代表人亲自或指定代理人担任 EV 证书申请者，代表机构申请证书

（2）申请者提交证书申请表、身份证明材料，生成公私密钥对，产生 PKCS#10 证书请求文件并递交给 SHECA

（3）SHECA 按照 3.2 的规定执行身份鉴别和验证流程

（4）SHECA 验证验证申请者提交的申请材料后，根据验证结果决定接受、拒绝该申请或要求申请者补充递交相关材料

（5）SHECA 接受申请后即进入证书签发流程

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。

4.2.2 批准或拒绝证书申请

完成 4.2.1 识别与鉴别的执行后，如果用户满足相应要求，则视为 SHECA 已经批准该证书请求，申请者即成为 SHECA 的 EV 证书订户；否则应拒绝证书申请。

如果法律法规明确禁止某个申请，或 SHECA 认为批准该申请具有高风险性，SHECA 应拒绝该申请，

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 EV 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 EV 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。

对于法律法规、国家政府部门、行业监管部门或当地政府明确禁止从事商业活动或其它公开活动的机构，SHECA 有权拒绝为其签发 EV 证书。此外，如果证书申请相关人员受到法律法规、国家或地方政府的相关限制，SHECA 可不予受理由其参与的 EV 证书申请事宜。

4.2.3 处理证书申请的时间

SHECA 应在合理的期限内完成证书申请处理。

4.3 证书签发

4.3.1 证书签发期间 CA 的行为

CA 将在证书申请被批准后生成并签发证书。CA 为申请人生成和签发的证书基于其在证书申请中被批准的信息。签发证书的操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南的要求。

(1) 申请日自行生成 PKCS#10 格式的请求文件，以可靠方式递交给 CA
(2) CA 验证该请求文件确实来自申请人
(3) 以验证数字签名之方式，确认 PKCS#10 格式请求文件的完整性
(4) 检查请求文件中的机构名称等信息，与申请表中被验证过的名称相一致
(5) 验证无误后，即签发订户证书
(6) 签发完成后的证书将以离线或在线的方式通知订户下载或领取

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。

4.3.2 CA 通知订户证书签发

SHECA 签发证书后，将以电话或者电子邮件的方式通知订户。

4.4 证书接受

4.4.1 构成证书接受的行为

下列情形被视作接受证书：

- 下载或安装证书
- 反对证书或反对证书中内容的行为失败

订户接收到证书后，应进行以下操作：

（1）确认证书内容与申请时的一致性

（2）检查证书内容的正确性

（3）检查证书内的公钥，是否与 PKCS#10 证书请求文件中的公钥信息相同

（4）以 CA 证书验证证书的有效性和合法性

如果在执行上述程序时发现未符合的情形，应立即告知 SHECA 撤销该证书，并重新要求进行证书签发。

用户在收到所申请的证书后，必须确认已充分了解并同意其使用证书的权利和义务，如果不同意则视为拒绝接受证书，SHECA 应撤销该证书。

4.4.2 CA 发布证书

所有被签发的证书将被发布到可公开访问的信息库中。

4.4.3 CA 通知其他实体证书的签发

不做规定。

4.5 密钥对和证书使用

4.5.1 订户私钥和证书使用

与证书中包含的公钥相对应的私钥只有在用户签署订户协议并接受证书后方可使用。使用证书符合订户协议、CP 和本 CPS 的规定，并且必须与证书中密钥用途扩展项中定义的用途相一致。

订户应保护其私钥避免未经授权的使用，并且不再使用过期或被撤销的证书。私钥不得进行归档。

4.5.2 依赖方公钥和证书使用

作为依赖一张证书证书的条件，依赖方应当同意依赖方协议中的条款。

证书必须在合理的情况下被依赖。如果情况表明需要额外的保证，那么依赖方必须得到这种依赖被认为是合理的保证。

在依赖证书前，依赖方必须独立的进行以下评估：

- 对于任何特定用途来说证书被恰当的使用，并且确定证书的这些使用没有被 CP 或本 CPS 禁止或限制，SHECA 没有责任评估证书是否被适当的使用。
- 证书是按照证书中包含的密钥用途扩展项的用途被使用的。
- 该证书的状态及其证书链中所有证书的状态。如果证书链中任何一个 CA 证书被撤销，依赖方应独立的去判断订户证书所做的数字签名是否是在该 CA 证书被撤销前做出的。

经过评估后假定证书是被恰当的使用，那么依赖方应当利用合适的软件、硬件去进行数字签名验证或者其它想要进行的加解密操作，作为依赖证书的条件。这些操作包括识别证书链和验证证书链中所有证书的数字签名。

依赖方在信赖 SHECA 签发的证书前，至少要进行以下操作，来决定是否信赖该证书：

(1) 获得 SHECA 的 EV Root 证书
(2) 检查证书链中所有证书以及订户证书是否还处在有效期内
(3) 检查证书链中所有证书的数字签名是否有效
(4) 检查证书链中所有证书是否被撤销
(5) 以证书链中可接受的根证书内包含的公钥，验证包含于订户证书内的数字签名
(6) 检查订户证书是否被撤销

如果上述操作未能通过验证，表示依赖方获得的订户证书并非由 SHECA 签发，或者该证书已过期，或者该证书已被撤销，或证书数字签名无法被验证，依赖方不应该信赖该订户证书。

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，只延长证书有效期的情况下，为订户签发一张新证书。

4.6.1 证书更新的情形

SHECA 不提供 EV 证书更新服务。

4.6.2 要求更新的实体

不适用。

4.6.3 处理证书更新请求

不适用。

4.6.4 通知订户新证书签发

不适用。

4.6.5 构成更新证书接受的行为

不适用。

4.6.6 CA 对更新证书的发布

不适用。

4.6.7 CA 通知其他实体证书的签发

不适用。

4.7 证书密钥更新

证书密钥更新是指在是在不改变证书中包含的信息的情况下，由订户生成新的密钥对向 SHECA 申请签发一张新证书。

4.7.1 证书密钥更新的情形

证书密钥更新参照 3.3.1 规定。

被撤销后的证书，不能申请证书密钥更新，只能按照 3.2 初始申请证书的情形申请新证书。

4.7.2 要求证书密钥更新的实体

订户是申请进行证书密钥更新的实体。

4.7.3 处理证书密钥更新请求

参照 3.3 的规定对证书密钥更新进行用户身份鉴别和识别。

参照 4.3 的规定对证书进行签发。

4.7.4 通知订户新证书的签发

同 4.3.2。

4.7.5 构成密钥更新证书接受的行为

同 4.4。

4.7.6 CA 对密钥更新证书的发布

同 4.4.2。

4.7.7 CA 通知其他实体证书的签发

同 4.4.3。

4.8 证书变更

证书变更是指在是在不改变证书公钥的情况下, 订户由于证书中所包含的信息发生变化而要求重新签发新的证书。

4.8.1 证书变更的情形

SHECA 不提供 EV 证书变更服务，如证书主体名称或其中包含的任何信息发生变更时应按照 4.9 的规定撤销该证书，订户应按照 4.1、4.2、4.3、4.4 的规定重新申请签发证书。

4.8.2 要求证书变更

不适用。

4.8.3 处理证书变更请求

不适用。

4.8.4 通知订户新证书的签发

不适用。

4.8.5 构成变更证书接受的行为

不适用。

4.8.6 CA 对变更证书的发布

不适用。

4.8.7 CA 通知其他实体证书的签发

不适用。

4.9 证书撤销和挂起

证书撤销和状态查询操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 13 部分的要求。

4.9.1 证书撤销的情形

4.9.1.1 订户证书撤销的情形

发生下列情形，订户证书应在 24 小时内被撤销：

- 订户提出吊撤要求；
- SHECA 获得证据，表明证书被误用；
- SHECA 了解到通配符被用于验证具有欺诈误导性质的域名 ；
- SHECA 发现证书的签发不符合 Baseline Requirement 和 CP/CPS 的相关要求；
- 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）；
- SHECA 依据 CP/CPS 的要求撤销证书；
- 在有效期内，订户证书中包含的信息发生变化、存在错误或失误、与订户实际信息不一致；
- 订户 EV SSL 证书里的信息做了实质性的更改；
- SHECA签发证书后发现EV SSL证书持有者申请其证书时提供的资料存在虚假信息；
- 证书申请是未得到授权或不能追溯到授权行为；
- 订户未按照 CP/CPS 或本协议的规定使用 EV SSL 证书或变更其用途；使用该证书来进行诸如钓鱼、欺诈等犯罪活动；
- 订户证书相对应的私钥证实或被怀疑出现遭到破解、损坏、遗失、暴露或篡改；

- 订户违背了 CP 及本 CPS、订户协议等规定的义务、陈述或担保，或者订户无法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；
- SHECA EV Root 证书或 EV 子 CA 证书相对应的私钥出现安全风险或存在被破解、泄露的疑虑；
- SHECA发现订户EV证书的颁发没有遵循《指南》或SHECA的EV证书政策；或者认为EV 证书里显示的信息不正确；
- SHECA终止营运并且尚未安排另外的EV证书签发机构来提供EV证书的撤销支持服务；或者SHECA不再具备签发EV SSL证书的权利或资质；
- 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
- 司法机关的判决使证书中的域名、证书主题等信息无法继续有效或继续被信任；
- 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 EV Code Signing 证书；
- 法律法规的相关规定或要求。

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 根证书撤销的情形

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 要求证书撤销的实体

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 证书撤销请求的处理程序

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 KEY 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 KEY 的用户，使用 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 KEY 用户以及 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 SHECA EV Root 证书或 EV 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 EV 证书问题报告和处理机制。

订户应在证书对应的私钥出现或疑似泄漏、被破解或被滥用时，应立即告知 SHECA，最长不超过 24 小时。SHECA 在接到订户报告后应在 24 小时内，对已经接受报告的证书进行调查和决定是否撤销或采取其他适当的行动处理机制，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。

SHECA 建立并保持 7*24 小时的 EV 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、私钥出现或怀疑出现泄漏、证书滥用、或其他与 EV 证书相关的舞弊、泄漏、滥用或不正当行为时，均可向 SHECA 进行报告或投

诉。报告方式如下：

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

在接受报告或投诉后，SHECA 在 24 小时内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,如果应用软件提供者要求撤销证书，SHECA 在收到请求的两个工作日内根据调查结果告知应用软件提供商。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。

4.9.4 撤销请求的宽限期

证书撤销请求应该在一个合理的期限内提出，SHECA 对此不进行强制规定。

但基于保护订户利益角度，订户在发生需要撤销证书的情形后，应立即申请撤销该证书。如果因怀疑或者证实证书的私钥已被破解、泄露或者任何影响证书安全性的情况发生而需要撤销证书，订户应至少在 24 小时以内提出。

4.9.5 CA 必须处理撤销请求的时间

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 依赖方检查撤销的规定

依赖方在信任 UNTSH EV 证书前，需要检查该证书的状态信息，包括查询证书撤销列表、通过 www.sheca.com 网站（http 方式）查询证书状态、通过在线证书状态协议（OCSP）方式查询等。

依赖方应根据其风险、责任及可能导致的后果，自行判断查询(或下载)证书撤销列表的间隔时间。

依赖方在使用 CA 签发的证书撤销列表前，应验证证书撤销列表是否为 CA 签发（验证证书撤销列表的数字签名），并应检查 CA 证书是否为撤销状态。

4.9.7 CRL 签发频率

SHECA 根据以下规则更新和发布证书吊销列表（CRL/ARL）。

对于订户证书，至少每 5 天公布一次 CRL，或在订户证书被撤销后的 24 小时内公布。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，至少每 6 个月公布一次 CRL，或在根/中级根证书被吊销后的 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/中级根证书被吊销，SHECA 将在网站公布相关吊销信息。

CRL 签发频率符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 13 部分的要求。

4.9.8 CRL 最大滞后时间

CRL 被签发后将在合理的时间内公布到信息库中。通常由系统在几分钟内自动完成该发布。

4.9.9 在线撤销/状态检查的可用性

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/Sheca/sheca.ocsp

4.9.10 在线撤销检查的要求

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超过 1 小时。

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”。

依赖方在依赖 SHECA 签发的证书前必须检查该证书状态。如果依赖方没有使用证书撤销列表来检查该证书的状态，那么依赖方应当通过 OCSP 方式检查该证书状态。

4.9.11 撤销公告可获得的其他方式

不做规定。

4.9.12 密钥损害的特殊要求

在 SHECA 的 CA 证书私钥实际或者被怀疑出现损害情形时，UNTSH 所有参与者都应通过合理的努力被告知。

在上述情形发生时，通常 SHECA 将按照以下流程来处理：

(1) 产生新的 CA 密钥对并签发相对应的新 CA 证书

(2) 撤销所有已签发的证书，使用新的 CA 密钥签发证书撤销列表，证书撤销列表包含所有已签发未到期的证书信息（包含 CA 密钥遭破解前签发的已经被撤销的证书）

(3) 以合理的努力告知订户及依赖方

(4) 为订户签发新的证书

(5) 将新的 CA 证书传递给订户

(6) 使用新的 CA 密钥来签发新的订户证书

订户的证书密钥被怀疑或证实遭破解时，应在 24 小时内告知 SHECA 撤销该证书。

4.9.13 证书挂起的情形

SHECA 不提供 EV 证书挂起服务。

4.9.14 谁能要求挂起

不适用。

4.9.15 挂起请求的程序

不适用。

4.9.16 挂起的期限

不适用。

4.10 证书状态服务

4.10.1 操作特征

证书状态可以通过 CRL、LDAP 目录服务、OCSP 进行查询。上述方式的证书状态服务应该对查询请求有合理的响应时间和并发处理能力。

4.10.2 服务的可用性

证书状态服务必须保证 7X24 小时可用。证书状态服务的可用性符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第 13 部分的要求。

4.10.3 可选功能

参照 4.9.9、4.9.11 的规定。

4.11 终止服务

当 SHECA EV Root 证书或 EV 子 CA 证书有效期满、证书被撤销、SHECA 结束运营时，所有 SHECA 已签发的证书即意味着服务终止，除非法律法规另有规定。

4.12 密钥托管和恢复

4.12.1 密钥托管和恢复的策略与实施

SHECA 不得托管任何 EV 证书订户的私钥，因此也不提供密钥恢复服务。

4.12.2 会话密钥封装和恢复的策略与实施

不做规定。

5. 设施、管理和运作控制

5.1 物理控制

5.1.1 场所位置与建筑

CA 和 RA 的操作在受到物理保护的建筑环境内进行，机房位于电信大楼内，符合存储高重要性系统和高敏感性信息的设施标准。

通过采用保安、门禁、视频监控等物理安全措施，可以防止未经授权的人员进入相关设施内，阻止并检测对敏感信息或系统进行的未经授权的使用、访问或披露。

5.1.2 物理访问

对物理安全每一层的访问都应是可被审计和可控的，确保每一层都只有经过授权的人员可以访问。SHECA 对 CA 机房的出入采取以下管理措施：

（1）设置多道门禁，以人员检查、智能卡或指纹方式进行身份识别，其中至少 2 道门禁必须同时两人以上经过身分鉴别后才可进入

（2）具备 24 小时视频监控录像设备，对进出机房情况进行记录

（3）用于 CA 私钥备份的密码设备，安全的存放于设有视频监控系统的保险柜内，保险柜钥匙和口令由两人分别保管

（4）所有重要的软硬件及密码设备等设备，都处在视频监控系统的保护之下，任何密钥管理相关操作必须 2 人以上方可进行。

5.1.3 电力和空调

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。

机房配备独立的空调系统以控制温度和相对湿度，并定期进行维护和测试。

5.1.4 防水措施

机房位于高层密闭式建筑内，除内部可进出的房门之外，外部均为混凝土建造，并且机房地板采用高架地板，可以有效防止洪水或其它水患造成的损害。

5.1.5 火灾预防与保护

机房采用防火材料进行装修，配备烟雾报警系统、自动气体灭火装置，一旦检测到火灾

发生时，能自动启用进行灭火。

火灾防护措施应当符合国家消防规定的要求。

5.1.6 介质存储

SHECA 采用电磁屏蔽、防静电干扰设备以及具备防火、防磁功能的保险柜，对备份关键系统数据或敏感信息的磁性存储介质进行保护，避免其受到水、火或其它物理因素造成的损害，并采取保护措施以阻止、检测和预防对这些介质未经授权的使用、访问或披露。

5.1.7 废物处理

SHECA 使用的硬件设备、存储设备、密码设备等，当废弃不用时，涉及敏感性和机密性的信息都被通过物理破坏的方式予以安全、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，并经过严格的验证，并保留相应的文件记录。

所有的涉密材料的销毁行为，都遵循国家有关的法律法规。

5.1.8 异地备份

SHECA 采取安全的异地备份方式，保持对关键系统数据或任何其它敏感信息（包括审计数据）的备份：

- 设置有异地备份机房，并配备相应设备，当日常营运的系统因外力因素无法正常运作时，备份系统可提供持续营运的能力
- CA 运营所需的相关数据，经备份后储存于具备温湿度控制、防磁、防静电干扰，且具有视频监控和物理访问控制措施的备份环境中
- 建立灾难恢复计划，并定期进行相应演练，以保持备份设施的可用性

5.2 过程控制（流程控制、过程控制）

5.2.1 可信角色

为保证 UNTSH 证书服务的可靠性和安全性，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）的人员都应是可信人员。

可信人员包括有权执行、访问或控制下列身份鉴别、密钥操作，可能会造成重大影响的所有员工、承包商和顾问：

- 验证证书申请信息
- 接受、拒绝或以其它方式处理证书申请、撤销、更新和注册等请求
- 签发、撤销证书，包括有权访问受限制部分的信息库、处理订户信息或其请求

- 访问、管理、维护关键系统或敏感数据

可信人员包括但不限于下列人员：

- 客户服务人员
- 证书业务管理人员
- 系统管理和操作人员
- 数据库管理和操作人员
- 被指定的工程技术人员
- 密钥管理和操作人员
- 内部审计评估人员
- 被指定管理基础设施可信性的管理人员

5.2.2 每项任务所需的人数

CA 和 RA 必须建立、保持和执行严格的控制程序，以确保基于工作职责进行的任务分割，并且确保由多名可信人员共同完成敏感操作。必须制定政策和控制措施以确保基于工作职责进行的任务分割。最敏感的任务，例如访问和管理 CA 密码设备或相关的密钥存储设备，必须要求多个可信人员进行操作。

这些内部控制流程必须被严格设计，以确保最少要求有 2 个可信人员拥有物理或逻辑访问控制权限。CA 密码设备的访问在其整个生命周期内必须严格确保由多个可信人员共同进行，包括从最初的设备接收到最后的逻辑或物理的破坏。一旦用于密钥操作的模块被激活，进一步的访问控制必须被启用，以便对设备物理和逻辑访问都保持分割控制。拥有对密码模块物理访问权限的人不得持有“秘密共享”，反之亦然。

确保单个人不能接触、导出、恢复、更新、废止存储的私钥。至少三个人，使用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

证书验证和签发等操作，至少需要两个可信人员参与，或者 1 个可信人员加自动验证和签发程序的组合共同参与。对于密钥恢复的人工操作，可以选择需要由两个经授权的管理员进行验证。

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。

在系统遇到紧急情况需要联合外部人员抢修时，应至少有 1 名 SHECA 人员在场，外部抢修人员在 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。

5.2.3 每个角色的识别和鉴别

CA 和 RA 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。

所有可信人员，必须通过鉴别和身份确认后，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。

相关人员根据业务需求执行的操作，均进行相应的记录，确保证书服务相关的作业具有可审计性，据此可进行相应的系统安全威胁及风险评估。

5.2.4 需要职责分割的角色

需要进行职责分割的角色，包括但不限于下列事项：

- 验证证书申请信息
- 接受、拒绝或以其它方式处理证书申请、撤销、更新和注册等请求
- 签发、撤销证书
- 访问严格受限或高敏感信息
- 处理订户信息或其请求
- CA 证书生成、签发和破坏
- 访问、管理、维护关键系统或敏感数据
- CA 系统上线或下线
- 密码设备管理和操作

5.3 人员控制

人员控制符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 14.1 部分的要求。

5.3.1 资格、经历和清白要求

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，不得有影响证书认证服务的兼职性行为，并且没有违法和信用不良记录，并且必须能够提交相应的证明文件。

- 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。
- 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。
- 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 背景调查程序

证书服务从业人员需要根据背景调查规范进行身份背景调查、业务能力调查等，通过审查后才能任职。一般每 2 年根据职务要求，对相应人员进行业务能力审查，作为其任职资质的依据。

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。

背景调查由人事部门和业务部门根据调查内容不同分别进行。

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 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

CA 和 RA 应当向员工提供胜任其工作职责所需要的培训，并定期开展。培训项目必须针对受训人员特定环境相关的下列因素，包括：

- UNTSH 安全准则和机制
- 在用硬件和软件的版本

- 所有人员的岗位职责
- 事件和损坏的报告处理流程
- 灾难恢复和业务连续性流程

为了使员工能够胜任工作，SHECA 按照员工岗位需要进行必要的岗前培训和工作中的再培训，培训应该包括但不限于以下内容：

- 岗位工作职责
- UNTSH 证书策略（CP）和电子认证业务规则（CPS）
- 电子签名法和相关法律法规
- 认证系统软硬件功能和模块
- 各类操作流程
- 证书和密钥基本知识和操作须知
- 灾难备份和系统恢复程序
- 安全管理策略要求等

对于认证系统重要更新或升级，以及新系统上线，对系统管理和证书操作人员均进行相应培训。

培训完成后，需要进行相应记录。

5.3.4 再培训的频率和要求

CA 和 RA 应持续向员工提供再培训，以提升其完成工作职责的技能，再培训的程度和频率应满足员工保持完全胜任工作职责的熟练水平的要求。

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 工作轮换的频率和顺序

不做规定。

5.3.6 未授权行为的处罚

CA 和 RA 应建立、维护和执行关于未经授权行为进行处罚的政策。处分措施应包括对未经授权行为进行评估、终止和处罚，处罚结果应和该类行为的频率和造成后果的严重程度相匹配。

通常，当员工被怀疑，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相应工作场所。根据情节严重程度，可以采取批评教育、开除、提交司法机构处理等措施。

一旦发现未经授权的行为，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 提供给人员的文件

SHECA 必须向其员工提供必要的培训以及让其胜任工作职责所需的文档，至少包括：

- CA 系统软、硬件的操作说明文件
- 密码设备的操作说明文件
- 证书服务指南和相关规范
- 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
- 安全管理规范

对于涉及敏感性和机密性的文件，应严格限制人员范围，在提供时必须明确相关保密要求，并视情况采取相应管理措施。

5.4 审计记录程序

5.4.1 事件记录的类型

CA 和 RA 必须记录下列审计事件类型，无论是手动生成或者是系统自动生成，都应该包含下列项目：

- 事件类型
- 事件结果
- 事件发生的的日期和时间
- 导致事件发生的实体或人员。

SHECA 所记录的日志和事件类型，包括但不限于以下内容：

- 运行事件，包括但不限于 CA 和子 CA 密钥的生成，系统上线和下线，系统和应用程序的启动和关闭，CA 密钥和信息的改变，密码设备生命周期相关事件，CA 私钥激活数据操作和物理访问日志，系统配置变更和维护，包含密钥、激活数据或个人信息的介质销毁的记录，
- 证书生命周期事件，包括但不限于签发、更新、证书密钥变更、撤销、挂起等

- 证书申请人身份证明材料及身份审核验证记录（包括验证内容、验证时间、验证方式等）
- 证书格式调整或变化
- CP、CPS 修订
- 可信人员事件，包括但不限于登录和注销尝试，口令创建、删除和设置，用户的系统权限变更，和相关人事变动
- 异常和事故报告
- 证书和信息库读写操作
- 证书生成政策的变更，例如变更有效期
- 物理和环境管理
- 安全管理事件
- 审计事件

5.4.2 处理日志的频率

根据运营需要，SHECA 每月或每季度会定期检查审计日志，以便发现重要的安全和操作事件，对发现的安全事件采取相应的措施，并对审查行为进行记录备案。

每年进行的审查不得少于 2 次。

5.4.3 审计日志的保留期限

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

所有的审计日志应当采取保护机制，防止未经授权的浏览、修改、读取、删除或篡改等，从而确保实现以下目的：

- 只有经授权人员可以读取审计纪录
- 只有经授权人员可以备份审计纪录
- 使用逻辑访问控制措施存目前和已归档的电子化审计纪录，并储存于不可擦写光盘片或其他无法更改的介质内
- 纸张及其它实体的审计纪录存放于安全场所

5.4.5 审计日志的备份程序

审计日志应当进行定期备份，包括每日增量备份和每周全量备份。

根据记录的性质和要求，SHECA 采取实时、每天、每周、每月和每年等多种形式的备份方式，采用在线或离线等各种备份工具。

5.4.6 审计收集系统

不做规定。

5.4.7 事件引发主体的通知

在事件被审计收集系统记录时，不要求或者不需要通知引起该事件的相关个人、单位、设备、应用程序等实体。

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 记录归档的类型

CA 和 RA 需要归档的记录包括但不限于下列类型：

- 5.4 收集的审计数据
- 证书系统建设和升级文档
- CP、CPS 及相关规范
- 证书
- 背景调查资料
- 审计评估资料
- 证书申请信息
- 证书申请资料
- 证书生命周期信息

5.5.2 归档的保留期限

归档记录至少应保存 7 年。其中，涉及到证书申请及审核确认的资料保存期限是从证书

到期或撤销后开始计算。

5.5.3 归档的保护

所有归档的记录需要采取适当的物理和逻辑访问控制措施，保证只有经过授权的可信人员才能访问。

归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 保存的申请者和订户基本情况信息和身份鉴别资料，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 归档备份程序

对于系统生成的电子归档记录，应当定期进行备份，备份文件进行异地存放。

纸质材料需要保存着安全的设施中。

5.5.5 记录的时间戳要求

归档记录必须保留时间信息，但是该时间信息不采用数字时间戳这种基于密码的方式进行。

归档的电子纪录(例如证书、证书撤销列表等)包含日期与时间信息，采用计算机操作系统的日期与时间。所有计算机系统都会定期进行校时，以确保电子纪录中日期与时间信息的准确性与可信度。

归档的书面纪录也将记载日期信息，必要时并将记载时间信息。书面纪录的日期与时间纪录不可任意更改，如需更改必须由审计人员签名确认。

5.5.6 归档收集系统

所有与认证服务相关的归档，都由内部人员按照权限和职责规定进行。 审计日志由内部系统产生，证书系统运营的相关文件记录，由具备权限的相关人员收集与管理。

5.5.7 获得和验证归档信息的程序

只有被授权的可信人员书面申请后才能够访问归档记录。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。

必须以书面申请获得正式授权后，才可取得归档资料；归档数据由审计人员负责验证，

书面文件必须验证文件签发者及日期等的真伪，电子文件则验证归档数据的数字签名或以密码学方式验证。

5.6 密钥变更

为降低 CA 密钥被破解的风险，SHECA 定期对 CA 证书密钥进行更新。

CA 用于签发证书的密钥对最大生命期不超过 30 年，有效期等同于对应的证书有效期。新的密钥对产生时，SHECA 将签发新的 CA 证书，并及时进行发布，让订户和依赖方能够及时获取新的 CA 证书。

5.7 损害灾难恢复

5.7.1 事故和损害处理程序

SHECA 建立事故和损害处理程序，进行事故调查、事故响应和处理。按照灾难恢复计划，备份信息应该被妥善保存，在一旦发生损害和灾难的时候应可以被有效使用，尽快恢复业务开展。

5.7.2 计算资源、软件、数据被损坏

SHECA 制定系统、数据等被破坏的恢复流程，每年进行相应演练。

如果出现计算机资源、软件和/或数据损坏的事件，必须将事件报告给安全管理部门，并立即启动事故处理程序，如有必要，可启动灾难恢复程序。

如果 CA 的计算机设备遭破坏或无法运作时，但 CA 私钥并未损毁的，则优先恢复数据库、知识库等备份系统的运作，并迅速重新实现签发、撤销和管理证书的功能。

5.7.3 实体私钥损害处理程序

当 CA 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，应立即撤销所有已签发证书，并采取合理的努力及时告知用户和依赖方。

5.7.4 灾难后的业务存续能力

CA 和 RA 应开发、建立、测试、维护并在必要时执行灾难恢复计划，以减轻任何人为或自然灾难造成的影响。灾难恢复计划应明确计划激活的条件、可接受的系统中断以及系统恢复时间。业务连续性的实施符合和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16 部分的要求。

在发生自然灾害或其他灾变，以致于无法在 24 小时内恢复证书状态服务时，将启用异地备份机房的设施，并于启用后 24 小时内恢复提供证书状态服务。

5.8 CA 或 RA 的终止

SHECA 终止服务时，按照《电子签名法》及相关规定处理，在规定时间内告知国家主管部门和用户，并妥善安排业务承接事宜。

因故结束其系统营运时，SHECA 将采取措施，通过合理安排业务承接方式将证书业务安全地转移至其他合法证书认证机构继续运作，确保对系统运营的影响减少至最低程度。

因业务正常结束、合约终止、公司整合、公司撤并等而导致无法继续提供证书服务时，SHECA 将按照以下流程处理:

（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）在终止服务之日 3 个月前，将终止服务及由其他证书认证机构承接相关业务的事实通知订户并公布于知识库。

（3）安排业务承接，将相关证书、密钥等转移至承接机构。

（4）将 CP、CPS、运营手册、订户协议、知识库、用户申请资料、审计记录等相关数据及其他业务承接所必须的相关文件，转移至承接机构。

（5）清除 CA 密钥。

（6）向订户正式宣公告，证书业务已全部转移至承接机构。

终止业务时，相关权利义务将依照订户协议办理。

5.9 数据安全

数据安全符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16 部分的要求。

6. 技术安全控制

6.1 密钥对生成和安装

6.1.1 密钥对生成

CA 密钥对由国家密码主管部门批准和许可的设备生成的。由于国家对于密码产品和认证系统有严格的管理要求，因此，SHECA 在密钥的生成、管理、储存、备份和恢复时应遵循国家相关规定进行，在此基础上，遵循 CNS 15135、ISO 19790 或 FIPS140-2 标准的相关规定，使用符合其标准的硬件设备生成和管理 CA 密钥。

CA 密钥生成过程需要在独立第三方公正方见证下进行，并由其出具见证报告。

订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成。

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 私钥分发给订户

私钥由订户自行生成，不需要将私钥传递给订户。

6.1.3 公钥分发给证书签发者

证书订户公钥以 PKCS #10 格式提交证书请求给 CA，应通过安全可靠的方式进行传输。

6.1.4 CA 公钥分发给依赖方

SHECA 的公钥公布在知识库，同时提供网页下载方式，供用户和依赖方查询下载。此外，SHECA 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 密钥长度

CA 和订户的 RSA 密钥长度，至少应该是 2048 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。

密钥长度符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 6.1.5 部分的要求。

6.1.6 公钥参数的生成和质量检查

按照国家密码主管部门的规定，CA 密钥使用经批准的加密设备生成，公钥参数的生成和质量检查均由相应设备进行控制。

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:

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 签发用于基础设施的证书（如 OCSP 响应验证证书）。

SHECA 签发的订户证书是 X509 v3 版本，包含了密钥用途扩展项。如果 SHECA 在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。

订户证书密钥用途扩展项包含 digitalSignature、keyEncipherment、dataEncipherment 及 keyAgreement。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

SHECA 采用由国家密码主管部门批准和许可的密码模块作为私钥的生成和保护设备，并在此基础上遵循 CNS 15135、ISO 19790 或 FIPS140-2 等级 3 硬件密码模块要求，该模块具备多人控制功能。

具体参照具备国家密码主管部门要求的生产资质的设备厂商提供的硬件产品资料。

6.2.2 私钥多人控制（m 选 n）

1. SHECA 采用多人控制策略来激活、使用、停止其私钥（m 选 n）。

CA 私钥的生成、启用、备份和恢复等操作采用多人控制的策略，按照 n out of m 方式（m>n, n>=3 ）进行。使用“秘密分割”技术将私钥保护信息分别写入 IC 卡等设备内，由受过 SHECA 安全认证委员会批准的三个或三个以上可信人员持有，并存放于安全可控的环境中。

保护私钥相关信息的智能卡或智能密码钥匙，以及保护口令，分别由职位独立的不同管理人员控制，并储存在具有安全控制管控措施的环境内。

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 的私钥不允许托管，也不向订户提供私钥托管服务。

6.2.4 私钥备份

SHECA 按照以下方式进行 CA 私钥备份:

(1) 钥储存于硬件密码模块内，按照 6.2.2 规定，以多人控制方式将私钥加密后进行备份，并将加密密钥保护信息以秘密分割方式存入多张智能卡内，由多人分别持有。

(2) 储存加密密钥分持信息的智能卡，存放在具备双重控制的安全环境内，由安全控管人员密封保管。

(3) 存储备份私钥的硬件密码模块存放于具备严格的安全可控环境内，至少有两人分别持有保险柜的相关令牌。

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 私钥导入或导出密码模块

CA 的私钥在硬件密码模块中生成和存储，只有在进行密钥备份和恢复时才允许将私钥导入至另一个硬件密码模块。导入和导出方式应遵循 6.2.2 和 6.2.4 规定。

6.2.7 私钥在密码模块中的存储

CA 私钥以密文的形式加密保存在硬件密码设备中。

6.2.8 激活私钥的方法

CA 私钥存放于硬件加密模块中，必须由 3 名以上经过授权的人员，经过身份鉴别后，插入其持有的 IC 卡并输入正确的保护口令，才可激活私钥。

相关流程应符合 5.2 规定。

6.2.9 解除私钥激活状态的方法

私钥被激活后，在进行身份鉴别后以退出登陆状态手工关闭方式解除激活状态，或设定预定时间后自动注销解除激活状态，以避免私钥遭到非法使用。

6.2.10 销毁私钥的方法

CA 的私钥到期后，由 SHECA 安全认证委员会授权多位人员执行硬件密码模块清零程序，将私钥进行销毁，并对硬件密码模块进行物理销毁。所有用于激活和备份私钥的 IC 卡也应一起被销毁。

6.2.11 加密模块评估

SHECA 使用国家密码主管部门批准和许可的密码产品，并参照 CNS 15135、ISO 19790 或 FIPS 140-2 等级 3 相关规定，选择所需要的硬件密码模块。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

CA 证书（包括根 CA 证书和子 CA 证书）的有效期到期后，应进行证书归档，包含在证书内的公钥，也同时一并进行归档。

6.3.2 证书操作期和密钥对使用期

证书有效期应当明确记录在 CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.4 部分的要求相一致。

公钥和私钥的有效期一致。CA 证书有效期和密钥对有效期一致，订户证书有效期可以小于其密钥对有效期，订户证书到期后，可在密钥对有效期内使用原密钥对申请更新证书。

对于 EV 证书，密钥对最长使用期限及证书有效期设置如下：

证书类型	密钥对最长使用期限	证书最长有效期
根证书	30 年	30 年
中级 CA 证书	25 年	25 年
EV SSL 证书	不做规定	27 个月
EV 代码签名证书	不做规定	39 个月
时间戳证书	15 个月	15 个月

6.4 激活数据

6.4.1 激活数据的生成和安装

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，采用多张智能卡分别生成，并采取多人分别持有方式（Duty Separation））进行保管。

智能卡中的激活数据由读卡设备存取，并使用智能卡保护口令（Pin 码）作为激活数据

存取时的身份鉴别手段。

6.4.2 激活数据保护

CA 私钥的激活数据，必须将存有激活数据的 IC 卡按照可靠的方式分割后由不同的可信人员掌管，智能卡应设置 PIN 码。

智能卡 Pin 码不能记录在任何纸张或其它介质上。如果错误输入超过 3 次，该智能卡将自动锁死。当智能卡发生移交时，新的保管人员必须重新设置 Pin 码。

订户私钥应使用保护口令或 PIN 码保护私钥。

6.4.3 激活数据的其它方面

不做规定。

6.5 计算机安全控制

6.5.1 特殊的计算机安全技术要求

SHECA 证书系统使用的计算机设备，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，应采取身份识别和验证、系统审计、角色权限控制、信息传输加密、物理访问控制、网络访问控制等方式进行管理和操作。

系统安全符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16.5 部分的要求。

通常，SHECA 通过相关操作系统、相关软硬件设备和管理措施，对证书认证系统采取以下管理控制功能：

(1) 登录采用身份识别手段
(2) 提供自行定义访问控制
(3) 具备安全审计能力
(4) 对于各种证书服务和角色访问控制的限制
(5) 具备可靠的角色及身份识别和鉴别
(6) 确保通讯和数据库安全。
(7) 具备角色及相关身份识别的安全、可靠的管道。
(8) 具备程序完整性及安全控制保护

6.5.2 计算机安全评估

SHECA 证书系统使用的计算机等设备，通过国家密码管理局、中国国家信息安全测评中心、上海市信息安全测评中心等或其它第三方机构的有关评估。

6.6 生命周期技术控制

6.6.1 系统开发控制

SHECA 证书系统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、过程控制、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。

系统开发遵循 ISO27001 规范的要求。

所有核心开发设备均采取严格的安全防范措施和恶意代码查杀手段，不允许安装和开发无关的软硬件。

6.6.2 安全管理控制

系统的信息安全管理，严格遵循国家信息化主管部门、国家密码管理局等有关运行管理规范和 SHECA 的安全管理策略进行操作。

整个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。

运行系统采用严格的管理体系来控制和监视系统的配置与变更，以防止未授权的修改。

6.6.3 生命周期安全控制

不做规定。

6.7 网络安全控制

SHECA 采用多级防火墙、入侵检测、安全审计、病毒防范等加强网络安全管理，并设置严格的访问控制权限，确保只有经过授权的人员经过身份鉴别后才可进行相应操作。对于不同安全等级的系统，严格划分内、外部网络，分别设置访问权限和管控措施。

证书系统必须经授权后由相关操作业务人员才可以执行管理操作，只有经过严格的身份识别后才能进行访问。

为防范网络入侵与破坏，安装和配置有防火墙、入侵检测与防病毒系统等，以增强网络安全。

证书系统服务器和内部数据库仅与内部网络连接，并使用防火墙进行隔离，仅允许内部设备联机并且必须经过身份识别，确认是被授权人员或系统方可访问。

6.8 时间戳

不做规定。

7. 证书、CRL 和 OCSP 格式

7.1 证书描述

7.1.1 版本号

SHECA 签发的 EV 证书版本为 X.509 V3。

7.1.2 证书扩展项

SHECA 签发的 EV 证书，其证书扩展项遵循 IETF RFC 5280 标准，并符合 Guidelines For The Issuance And Management Of Extended Validation Certificates 的要求。

证书策略扩展符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.3 部分的要求。

7.1.3 密钥算法对象标识符

SHECA 使用的算法对象标识符（OID）如下：

- sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

7.1.4 命名形式

SHECA 签发的 EV 证书，其命名形式的格式和内容符合 X.501 的甄别名（Distinguished Name；DN）命名方式，遵循 RFC5280 相关规定。

7.1.5 命名限制

SHECA 可根据需要使用命名限制扩展项（nameConstraints）。

7.1.6 证书策略对象标识符

SHECA 签发的 EV 证书，在证书中证书策略扩展项（certificatePolicies）中使用证书策

略对象标识符。

证书策略标识符符合和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.3 部分的要求。

7.1.7 策略限制扩展项的使用

SHECA 可根据需要使用策略限制扩展项（(policyConstraints)。

7.1.8 策略限定符的语法和语义

SHECA 可根据需要使用策略限制扩展项（(policyConstraints）语法。

7.1.9 关键证书策略扩展项的处理语义

不做规定。

7.2 CRL 描述

7.2.1 版本号

SHECA 签发 X.509 V2 版本的 CRLs。

7.2.2 CRL 和 CRL 扩展项

不做规定。

7.3 OCSP 描述

7.3.1 版本号

OCSP 版本为 RFC 2560 定义的 V1 版本。

7.3.2 OCSP 扩展项

OCSP 扩展项的使用符合 RFC 2560 规范。

8. 审计和其它评估

作为 UNTSH 的运营实体，SHECA 每季度执行一致性审计及运营评估来确保证书服务的可靠性、安全性和可控性。除去内部审计及评价，SHECA 同时聘请外部独立审计机构进行 WebTrust 的审计。

8.1 评估的频率或情形

SHECA 至少每年进行一次外部审计评估，每季度执行一次内部审计评估。

审计操作应当明确记录在 CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 17 部分的要求相一致。

8.2 评估者的资质

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 CP 和本 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。

在进行外部审计时，应选择具有国家或国际上认可资质的专业审计评估机构，在业界享有良好的声誉，具备丰富的实际操作经验。

8.3 评估者和被评估者的关系

在进行内部审计时，审计者和被审计对象是独立分工的关系，没有任何的利害关系足以影响评估的客观性，审计者应以独立、公正、客观的态度进行审计评估。

在进行外部审计时，被委托的审计机构应和 SHECA 之间没有任何利害关系足以影响评估的客观性和独立性。

8.4 评估内容

SHECA 进行的审计主要包括如下内容：

- 是否制订和公布 CP/CPS
- 是否按照 CP/CPS 进行证书运营和服务
- CPS 是否符合 CP 规定
- 证书和密钥生命周期管理
- 物理和环境安全控制
- 业务连续性管理

在进行内部审计评估时，除了对上述证书签发行为、运营安全等进行审计外，还必须就下列内容进行审计

- 对于审计年度内所有已签发的 EV 证书，应抽取不少于 3%的证书，进行身份审核过程的复查；
- 对于审计年度内所有已签发的 EV 证书，应抽取不少于 10%的证书，进行高风险申请人列表比对；
- 对于审计年度内所有从事与签发 EV 证书相关的可信人员的培训记录；

此外，在进行内部审计时，同时应成立风险评估小组，对 EV 证书的整体业务活动进行风险评估，识别内外部威胁及其可能产生的损害，分析评估现有制度、流程和系统对风险的控制程度，编制风险评估报告并提出相应的安全控制措施。评估报告完成后提交给 SHECA 安全认证委员会。

8.5 对不足采取的行动

完成内部和外部审计后， SHECA 必须根据评估的结果检查缺失和不足，提出修改和预防措施，并跟踪改善情况。

SHECA 根据需要可就整改情况开展后续跟踪评估。

8.6 评估结果沟通

完成审计评估后，SHECA 将通过 www.sheca.com 网站公布审计结果，但不会公布具体审计信息。

9. 其它事项和法律事务

9.1 费用

9.1.1 证书签发和更新费用

SHECA 对证书订户收取证书签发费用及证书更新费用。

证书签发、更新及其相关服务的价格，在 SHECA 网站 www.sheca.com 上予以公布，或者在与订户签署的相关文件中予以规定。

9.1.2 证书查询费用

不收取该费用。

9.1.3 撤销和状态信息查询费用

不收取该费用。

9.1.4 其他服务费用

不做规定。

9.1.5 退款策略

订户在完成证书申请但证书尚未签发时申请退费，SHECA 在扣除处理工本费后，将剩余款项无息退还给订户。

订户在证书签发后申请退费，SHECA 在处理工本费及按比例扣除已使用月份（不足一月的按一月计）的证书费用后，将剩余款项无息退还给订户。

9.2 财务责任

9.2.1 赔偿责任

SHECA 按照以下规定承担赔偿责任：

1、除未遵照本证书策略（CP）、电子认证业务规则（CPS）及相关操作规范的规定签发

证书而造成用户损失的，并且 SHECA 存在过失的情况外，SHECA 不承担赔偿责任。

2、如因不可抗力事件（例如地震等），或其它 SHECA 毋须承担责任的情况而造成用户损失的，SHECA 不承担赔偿责任。

3、如因工作人员故意或过失、未本证书策略（CP）、电子认证业务规则（CPS）及相关操作规范的规定办理证书申请、签发、更新和撤销等业务或违反相关法律法规要求而造成用户损失的，SHECA 承担相应赔偿责任。

4、SHECA 或其他有权提出证书撤销的主体在提出证书撤销要求后，在 SHECA 实际公布该订户证书前（以证书撤销列表载明的时间为准），如果因使用该订户证书而产生法律纠纷时，SHECA 没有违反相关规定处理撤销事宜的，不承担赔偿责任。

5、订户使用假冒、错误的证书或使用伪造证明文件申请证书而造成损失的，SHECA 不承担赔偿责任。

6、赔偿责任的时效按照相关法律的规定处理。

7、SHECA 每年聘请独立的第三方财务审计机构对财务情况进行审计，确保具备足够的现金资产用于赔偿可能发生的用户损失。

8、SHECA 视需要决定选择第三方保险服务，在未投保的情况下，将按照 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南要求，以自有资金承担赔偿责任，赔偿限额一并遵循指南的规定。

9.2.2 其他财产

SHECA 拥有足够的现金资产作为财务保证资金，当从事证书业务产生赔偿责任时用于支付相关赔偿事项。

9.2.3 对终端实体及依赖方的保险或担保范围

见 9.2.1 章节规定。

9.3 业务信息保密

9.3.1 保密信息范围

SHECA 确认下列信息属于保密信息：

1、保密信息包括 SHECA 与订户、SHECA 与其他证书服务相关方等之间的协议、往来

函和商务协定等；

2、私钥及与之相关的激活数据；

3、订户申请证书时提交的个人身份资料；

4、系统运营和管理日志及记录

5、审计记录

6、系统和网络配置资料

7、系统运营管理文档

8、其它 SHECA 明确为保密信息的文件

9.3.2 不在保密范围的信息

证书策略（CP）、电子认证服务规则（CPS）、证书申请表、证书及 CRL、外部审计评估结果等都是可以公开的信息。

9.3.3 保护保密信息的责任

除非法律法规、国家主管部门要求或订户书面授权，SHECA 绝不任意对外公布列入保密信息范围的资料。

如果司法机构因为处理证书纠纷需要提供相关材料的，SHECA 将按照法定程序予以提供。

9.4 个人信息隐私保护

9.4.1 隐私保护计划

SHECA 尊重所有的用户和他们的隐私，并按照法律法规的要求对个人隐私信息进行保护。

9.4.2 被视为隐私的信息

除证书中已经包括的信息外，证书订户的基本信息和身份认证资料，包括联系电话、地址等都将被作为隐私处理。

9.4.3 不被视为隐私的信息

订户证书中包含的信息不被视为隐私信息。

9.4.4 保护隐私信息的责任

SHECA 按照法律法规的要求承担隐私保护责任。

9.4.5 使用隐私信息的告知和同意

SHECA 在其认证业务范围内使用所获得的任何订户信息，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，也没有告知订户的义务，并且不需得到订户的同意。

9.4.6 依法律或行政程序的披露

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：

- 符合法律法规的规定并且经相关部门通过合法程序提出书面申请
- 法院以及公权力部门处理因使用证书产生的纠纷时提出书面申请
- 具有合法司法管辖权的仲裁机构提出书面申请

9.4.7 其它信息披露情形

不做规定。

9.5 知识产权

1、SHECA 的密钥、签发的证书和 CRL、公布的 CP/CPS、编写的相关文件等属于 SHECA 的知识产权。

2、订户拥有自己密钥的知识产权，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。

3、SHECA 不保证订户证书中载明的名称的知识产权归属。

9.6 陈述与担保

9.6.1 关于 EV 证书的陈述和担保

SHECA 签发的 EV 证书在其证书有效期内，其陈述和担保具体包括但不限于：

1、合法存在，自证书被签发之日起，SHECA 已经确认 EV 证书中指明的主体是一个在政府主管部门注册的有效机构；

2、身份，自证书被签发之日起，SHECA 已经确认 EV 证书中指明的主体的合法名称，

与政府主管机构官方记录中的名称相匹配；

3、域名使用权：自证书被签发之日起，SHECA 已经根据指南中相关条款的要求，采取了一切必要的合理措施验证 EV 证书中指明的主体拥有 EV 证书中列出的域名的所有权或独家使用权；

4、EV 证书授权：SHECA 已经根据指南中相关条款的要求，采取了一切必要的合理措施验证 EV 证书中指明的主体已经授权该证书的签发；

5、信息的准确性：自证书被签发之日起，SHECA 已经采取了一切必要的合理措施验证 EV 证书中包含的所有信息都是准确的；

6、订户协议：EV 证书中指明的主体已经和 SHECA 签署了合法有效的订户协议或者该主体的申请代表人已经承认和接受该使用条款；

7、证书状态：SHECA 遵循指南的要求，保持有关证书有效或撤销状态最新信息的知识库 7X24 小时在线可访问

8、撤销：SHECA 遵循指南的要求，当任何导致 EV 证书被撤销的情形发生时根据指南和本 CPS 的规定及时撤销该证书。

9.6.2 CA 的陈述和担保

SHECA 承担 CA 和 RA 职责，遵循以下规定：

1、SHECA 按照法律法规的要求提供证书服务。

2、SHECA 按照依照证书策略（CP）和电子认证业务规则（CPS）接受并处理证书申请、更新、撤销等请求

3、SHECA 在签发证书时进行可靠的身份识别和鉴别，严格审核订户申请信息的真实、准确、有效。

4、SHECA 妥善保管订户申请注册资料等

5、SHECA 的 CA 密钥出现安全问题时，将及时告知订户及国家主管部门。

6、SHECA 按照规定公布证书和 CRL

7、SHECA 在订户申请证书时，向订户提供相关协议并告知其权利义务。

8、SHECA 保证其私钥得到安全的存放和管理。

9、SHECA 按照国家主管部门的要求建立安全可靠的运营系统和安全管理机制

10、SHECA 保证证书中包含的信息都是准确的，不存在错误信息

ROORCA 和 CA 的保证和责任应当明确记录在 CPS 中，并且分布要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 18 和 7.1 部分的要求相一致。

9.6.3 RA 的陈述和担保

见 9.6.2 章节规定。

9.6.4 订户的陈述和担保

SHECA 仅向各类组织机构提供 EV 证书服务，不向个人用户提供。各类组织机构在申请和使用 EV 证书时应遵循以下规定：

1、在提出证书申请时，应了解并同意相关协议和 CP/CPS 等相关规范规定的内容；

2、提交申请时必须提供准确、真实、有效的信息及相应的证明文件；

3、妥善保管和使用私钥，按照规定合法使用证书，并遵守 CP/CPS 关于限制使用的要求；

4、接受证书时应确定证书内所包含内容的准确性，并验证证书内公钥与所拥有私钥的对应性；

5、在证书中相关信息发生变化或异动时及时告知 SHECA；

6、在私钥发生遗失、泄露或其它安全风险时及时告知 SHECA，按照规定办理撤销手续，并承担该证书被撤销状态未公布前因使用该证书所产生的风险与责任；

7、按照 SHECA 的规定及时更新证书；

8、接受任何由 SHECA 根据法律法规要求和技术发展所公示过的声明、改变、更新、升级等；

9、为了 SHECA 和 EV 证书收益人的利益，承诺并保证指南中订户协议要求部分规定的保证。

9.6.5 依赖方的陈述和担保

依赖方在信赖任何 SHECA 签发的 EV 证书时，应遵循以下规定：

1、接受或使用 SHECA 签发的证书，即意味着依赖方了解并同意 CP/CPS 中关于责任和义务的规定，并在 CP/CPS 规定的范围内信赖该证书。

2、获得 SHECA 的根证书和相关信任链，决定是否信任订户证书。

3、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 及其有效性，检查该证书是否被撤销；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

4、选择安全可靠的计算机及可信赖的应用系统等环境信赖 SHECA 签发的证书，并自行承担由与计算机环境或应用系统本身因素导致的损失。

9.6.6 其他参与方的陈述和担保

不做规定。

9.7 担保免责

在法律允许的范围内，SHECA 不承担以下责任：

1、SHECA 在签发证书时没有过错的。

2、不可抗力因素造成的损失。

3、SHECA 在收到证书撤销请求后合理的处理期限内造成的损失。

9.8 有限责任

在订户及依赖方因签发或使用证书而发生损害赔偿时，SHECA 按照法律法规的要求、用户协议或本 CPS 规定的责任范围内承担有限责任。

9.9 赔偿

SHECA 对自身原因造成的订户或依赖方损失的，应对订户或信赖方进行赔偿。

订户对自身原因造成认证机构、依赖方损失,应对认证机构和依赖方进行赔偿。

依赖方因自身原因造成 SHECA 损失的，应承担赔偿责任。

根据 CP 制定的本 CPS、订户协议以及其他文档中，需要对赔偿的范围、限额、免赔等进行具体规定。

9.10 有效期和终止

9.10.1 有效期

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尔日期，当新版本正式发布生效时，旧版本将自动失效。

9.10.2 终止

本 CPS 将持续有效，直到有新的版本取代。

9.10.3 终止的效果和存续

本 CPS 终止后，涉及保密信息、隐私保护、知识产权的条款，以及涉及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。

本 CPS 的效力，一直延续到按照本 CPS 所签发的最后一张证书到期或撤销为止。

9.11 对各参与方的个别通知和沟通

除非法律法规或者协议有特别的规定，SHECA 将以电子邮件、电话、传真、网站公布或其它合理的方式与订户进行沟通。

9.12 修订

9.12.1 修订程序

SHECA 负责制订和修改本 CPS，每年至少审查一次本 CPS 内容。

如果法律法规要求、OID 变化、相关国际标准变更等需要本 CPS 变更时，SHECA 将及时进行修订。

修订后的版本将按照规定向国家主管部门进行备案并公布于知识库。

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 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 www.sheca.com)，它等同于修改本 CPS。

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。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。

9.12.3 必须修改的情形

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
- 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

9.12.4 对象标识符变更

当本 CPS 发生修订时，相对应的证书策略对象标识符不会进行变更，仅增加版本识别代码。

9.13 争议解决条款

当出现争议时，有关方面应依据协议通过协商解决，协商解决不了的，可通过法律解决。

9.14 管辖法律

SHECA 运营的 UNTSH 体系，其所有的证书服务活动均接受中华人民共和国相关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。

9.15 与适用法律的符合性

本 CPS 必须符合《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》的规定。

9.16 其它条款

9.16.1 完整协议

不做规定。

9.16.2 转让

不做规定。

9.16.3 可分割性

本 CPS 的任何条款，如果因为修订或其它任何原因发现无效或不能执行，本 CPS 其余的部分仍将有效。

9.16.4 强制执行

不做规定。

9.16.5 不可抗力

在法律法规许可的范围内，本 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。

9.17 其它条款

不做规定。

附录 A 定义和名词解释

SHECA

上海市数字证书认证中心有限公司的缩写。

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。

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。

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。

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。

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、RAB 的授权从事各类服务。

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。

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。

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。

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。

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。

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。

钥（电子签名验证数据）

是指订户验证电子签名的数据。

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。

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。

附录 B 名词与缩写

AICPA American Institute of Certified Public Accountants, Inc.
ANS American National Standard
CA Certification Authority
CC Common Criteria
CCITSE Common Criteria for Information Technology Security Evaluation
CP Certificate Policy
CPS Certification Practice Statement
CRL Certificate Revocation List
DN Distinguished Name
FIPS Federal Information Processing Standard
ISO/IEC the International Organization for Standardisation, The International Electrotechnical Commission
ITSEC Information Technology Security Evaluation Criteria
LDAP Lightweight Directory Access Protocol
OCSP Online Certificates Status Protocol
OID Object Identifier
OECD Organization for Economic Co-operation and Development
PMA Policy Management Authority
PIN Personal Identification number
PKCS Public Key Cryptography Standard
PKI Public Key Infrastructure
RA Registration Authority
RCA Root Certification Authority
RSA Rivest,Shamir,Adleman(encryption algorithm)
TCSEC Trusted Computer System Evaluation Criteria
URL Universal Resources Location
SSL Secure Socket Layer
EV Extended Validation

EV 证书所需证书扩展项

1. 根CA（Root CA Certificate） 证书

Root CA证书遵循X.509 v3格式.

（a）基本限制 *basicConstraints*

所有v3版本CA证书必须存在本扩展，并且必须标记为关键的。CA域（CA field）的值必须置为“True”，并且不存在路径长度限制域（pathLenConstraint）。

（b）密钥用途 *keyUsage*

所有v3版本CA证书必须存在本扩展，并且必须标记为关键的。必须设置CertSign 位和cRLSign位，所有其它位均不应设置。

（c）证书策略 certificatePolicies

本扩展项不存在。

（d）扩展密钥用途 extendedKeyUsage

本扩展项不存在。

所有其它域和其它扩展项的设置符合RFC 5280。

2. 子CA（Subordinate CA Certificate）证书

（a）证书策略 *certificatePolicies*

本扩展项存在，并且必须是非关键的。策略标识符设置必须包扩SHECA的UNTSH EV 策略的标识符。

（b）证书撤销列表分发点 *cRLDistributionPoint*

包含本扩展项，并且必须是非关键的。该扩展项包含了SHECA发布CRL服务的HTTP地址URL。

（c）机构信息访问 *authorityInformationAccess*

本扩展项必须存在，并且是非关键的。应包含OCSP响应的HTTP地址URL。

（d）基本限制 *basicConstraints*

本扩展必须存在，并且必须标记为关键的。CA域（CA field）的值必须置为“True”，可以存在路径长度限制域（pathLenConstraint）。

（e）密钥用途 *keyUsage*

必须存在本扩展，并且必须标记为关键的。必须设置CertSign 位和cRLSign位，所有其它位均不应设置。

所有其它域和其它扩展项的设置符合RFC 5280。

3. 订户证书（Subscriber Certificate）

（a）证书策略 *certificatePolicies*

本扩展项必须存在，并且应当是非关键的。策略标识符设置必须包扩SHECA的UNTSH EV 策略的标识符。

certificatePolicies:policyIdentifier (Required)

EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)

id-qt 2 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier (Required)

URI to the Certificate Practice Statement

（b）证书撤销列表分发点 *cRLDistributionPoint*

包含本扩展项，并且是非关键的。该扩展项包含了SHECA发布CRL服务的HTTP地址URL：

（c）机构信息访问 *authorityInformationAccess*

包含本扩展项，并且是非关键的。应包含OCSP响应的HTTP地址URL。

（d）基本限制 *basicConstraints* (optional)

If present, the CA field MUST be set false.

（e）密钥用途 *keyUsage* (optional)

本扩展项如果存在，必须不设置CertSign and cRLSign 位。

（f）扩展密钥用途 *extKeyUsage*

id-kp-serverAuth [RFC5280]、d-kp-clientAuth [RFC5280]两者之一或者是上述两者的值必须存在，其它值不应存在。

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

（g）主体替换名称 *SubjectAltName*

根据RFC 5280填充，并且关键性被设置为FALSE。

所有其它域和其它扩展项的设置符合RFC 5280。