协卡网络信任服务体系

EV 证书策略

UniTrust Network Trust Service Hierarchy

Extended Validation Certificates Policies

1.6.1 版本

生效日期：2019 年 5 月 29 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 证书策略》

UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policies

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

本文件版本变更记录

版本	生效日	作者	发布者	说明
V1.6.1	2019 年 5 月 29 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.6	2018 年 9 月 10 日	陈晓曈	SHECA 安全认证委员会	修订发布
V1.5	2018 年 8 月 31 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
V1.6.1	根证书增加 UniTrust PTC Root CA R1, UniTrust PTC Root CA R2 增加证书撤销的情形 修正知识库网址
V1.6	增加变更摘要
V1.5	修改 EV 证书层次架构图 修复部分措辞及语法错误
V1.4	UNTSH 证书层次架构调整 增加 OID 列表
V1.3	修改证书撤销请求方、撤销流程等
V1.2	修改密钥对和证书使用
V1.1	证书撤销的情形及流程 增加附录 C CRL 格式
V1.0	--

声明

本 CP 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 CP 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

目录.....5
1. 导言.....7
1.1 概述.....7
1.2 文档名称和标识.....8
1.3 参与者及适用范围.....9
1.4 证书用途.....10
1.5 策略管理.....11
1.6 定义与缩写.....11
2. 发布和信息库责任.....12
2.1 信息库.....12
2.2 认证信息发布.....12
2.3 发布时间或频率.....12
2.4 信息库访问控制.....12
3. 身份标识与鉴别.....13
3.1 命名.....13
3.2 初始身份的确认.....14
3.3 密钥更新请求的标识与鉴别.....15
3.4 撤销请求的标识与鉴别.....15
4. 证书生命周期操作要求.....16
4.1 证书申请.....16
4.2 证书申请处理.....16
4.3 证书签发.....17
4.4 证书接受.....17
4.5 密钥对和证书使用.....18
4.6 证书更新.....18
4.7 证书密钥更新.....19
4.8 证书变更.....20
4.9 证书撤销和挂起.....21
4.10 证书状态服务.....24
4.11 终止服务.....25
4.12 密钥托管和恢复.....25
5. 设施、管理和运作控制.....26
5.1 物理控制.....26
5.2 程序控制（流程控制、过程控制）.....27
5.3 人员控制.....28
5.4 审计记录程序.....30
5.5 记录归档.....31
5.6 密钥变更.....32
5.7 损害灾难恢复.....32

上海市数字证书认证中心有限公司 电话:（021）36393100 传真:(021)36393200
上海市四川北路 1717 号嘉杰国际广场 18 楼 200080 http://www.sheca.com/

5.8 CA 或 RA 的终止.....33
5.9 数据安全.....33
6. 技术安全控制.....34
6.1 密钥对生成和安装.....34
6.2 私钥保护和密码模块工程控制.....35
6.3 密钥对管理的其他方面.....36
6.4 激活数据.....37
6.5 计算机安全控制.....37
6.6 生命周期技术控制.....38
6.7 网络安全控制.....38
6.8 时间戳.....38
7. 证书、CRL 和 OCSP 描述（轮廓）.....39
7.1 证书描述.....39
7.2 CRL 描述.....40
7.3 OCSP 描述.....40
8. 审计和其它评估.....41
8.1 评估的频率或情形.....41
8.2 评估者的资质.....41
8.3 评估者和被评估者的关系.....41
8.4 评估内容.....41
8.5 对不足采取的行动.....41
8.6 评估结果沟通.....42
9. 其它事项和法律事务.....43
9.1 费用.....43
9.2 财务责任.....43
9.3 业务信息保密.....44
9.4 个人信息隐私保护.....45
9.5 知识产权.....46
9.6 陈述与担保.....46
9.7 担保免责.....48
9.8 有限责任.....48
9.9 赔偿.....48
9.10 有效期和终止.....48
9.11 对各参与方的个别通知和沟通.....49
9.12 修订.....49
9.13 争议解决条款.....50
9.14 管辖法律.....50
9.15 与适用法律的符合性.....50
9.16 其它条款.....50
9.17 其它条款.....51
附录 A 定义和名词解释.....51

1.导言

1.1 概述

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。

本文档名称为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），根据 CA/Browser Forum 制定的 Guidelines For The Issuance And Management Of Extended Validation Certificates(以下简称 EV Guidelines)以及国家电子认证服务主管机构发布的相关规定制定，适用于所有由 UNTSH 签发和管理的 EV 数字证书。

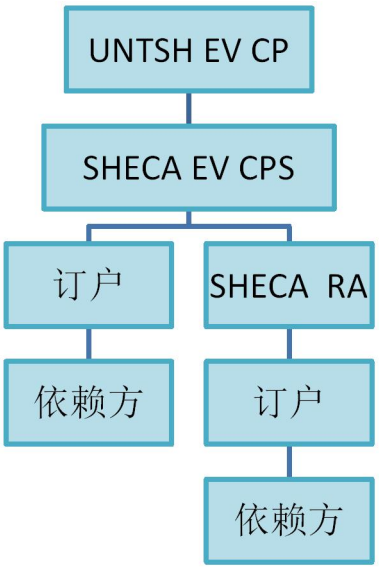
本 CP 作为 EV 证书最高策略，为整个 UNTSH 内的 EV 证书提供管理、操作和规范的依据，以及为 UNTSH 各参与方的权利义务关系确定一个限制范围和基本条款，明确了 UNTSH EV 证书和相关服务的操作流程框架，以及为安全、完整地实施这些流程所应该采取的业务、技术和法律方面的要求。

SHECA 作为一个证书服务机构（CA），在本 CP 的约束下生成和运营 EV 根证书和 EV 子 CA 证书，签发订户证书。SHECA 的 EV 证书电子认证业务规则（CPS）接受本 CP 的约束，详细阐述了 SHECA 作为电子认证服务机构提供的证书、如何提供证书以及相应的管理、操作和保障措施。所有 UNTSH 证书的订户及依赖方必须参照本 CP 及相关 CPS 的规定，决定对证书的使用和信任。

本 CP 受到独立的第三方审计持续的审查，SHECA 将在 www.sheca.com 上公布被审查的结果。

1.1.1 UNTSH 架构

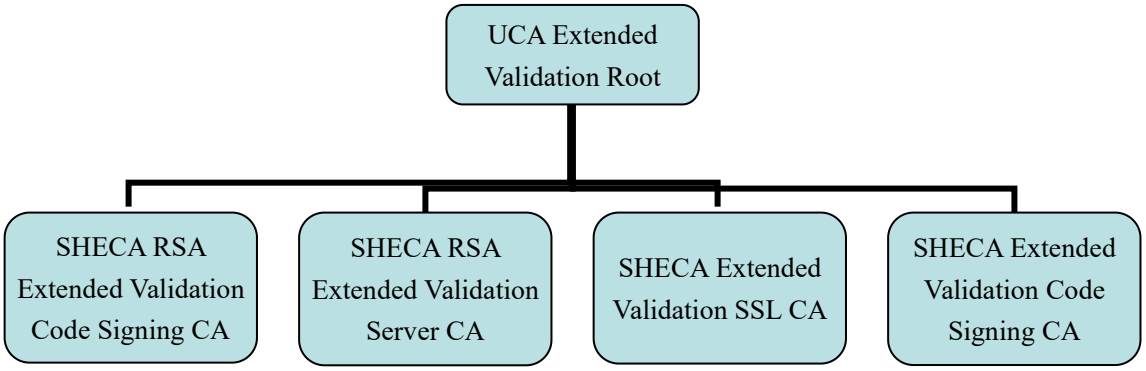
本 CP 是 UNTSH 内 EV 证书最高策略，UNTSH 的证书服务机构（CA）按照本 CP 制定 EV CPS，RA 按照本 CP 及 EV CPS 进行证书服务申请鉴别，订户、依赖方及其他相关实体按照本 CP 及 EV CPS 决定对证书的使用、信任并履行相关的义务。UNTSH 包含了根 CA、子 CA、注册机构（RA 中心），这些实体都是协卡认证体系内不同层次的服务主体。协卡认证体系所有和证书相关的服务和管理，都完整、正确、全面的贯彻和实施本 CP 以及 EVCPS 的要求。



1.1.2 UNTSH EV 证书层次架构

UNTSH 有 3 个 EV 根 CA，为 UCA Extended Validation Root，UniTrust PTC Root CA R1 和 UniTrust PTC Root CA R2。

- UCA Extended Validation Root



UCA Extended Validation Root 根密钥长度为 4096-bit，下设 4 个子 CA 证书，其中：（1）SHECA RSA Extended Validation Code Signing CA 只签发密钥长度为 RSA 2048-bit 位代码签名证书，且支持 SHA256，并对 extKeyUsage 进行约束，设置仅适用于 id-kp-codeSigning；（2）SHECA RSA Extended Validation Server CA 只签发密钥长度为 RSA 2048-bit 安全站点证书，且支持 SHA256，并对 extKeyUsage 进行约束，设置仅适用于 id-kp-serverAuth 和 id-kp-clientAuth；(3)SHECA Extended Validation SSL CA，SHECA Extended Validation Code Signing CA 已停用，不再签发订户证书。

UCA Extended Validation Root 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。

- UniTrust PTC Root CA R1

UniTrust PTC Root CA R1 根密钥长度为 4096 位，RSA 算法，签名算法为 RAS SHA-384 目前无子 CA 证书。

有效期将于 2044 年 4 月 27 日到期，2039 年 4 月 27 日起不再签发下级证书。

- UniTrust PTC Root CA R2

UniTrust PTC Root CA R2 根密钥长度为 384 位，ECDSA 算法，签名算法为 ECDSA SHA-384,目前无子 CA 证书。

有效期将于 2044 年 4 月 27 日到期，2039 年 4 月 27 日起不再签发下级证书。

1.1.3 UNTSH　EV 证书信任等级

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 证书策略》（UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policies ，缩写为 UNTSH EV CP），简称为协卡认证体系 EV 证书策略。

本证书策略对象标号符（OID）为：1.2.156.112570.1.0.3。

1.3 参与者及适用范围

1.3.1 证书管理中心（CA）

CA 是颁发证书的实体，负责 EV 证书的签发、运营和管理，由 SHECA 建设和运营。CA 的主要职责包括：

- 证书的签发和管理
- 管理和发布证书、证书撤销列表（CRL）
- 管理和运营证书信息库
- 证书相关策略、CPS 和规范的制定和发布

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

订户是证书主题（Certificate Subject)指称的实体，是 EV 证书及其对应私钥的拥有人。SHECA 只对各类法人机构发放 EV 证书，不向自然人提供 EV 证书申请和签发服务。

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，用以识别网络主机服务器（或网站域名）、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 CP 签发的 EV SSL 证书，可用来验证证书中标识的网络主机服务器或互联网域名的身份，以及持有该网络服务器或互联网域名的法人机构身份；依据本 CP 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

SHECA 签发的 EV 证书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。

1.5 策略管理

1.5.1 策略文档管理机构

本证书策略的制定、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 CP 联系人，专门负责本 CP 的对外沟通及其它相关事宜。任何有关本 CP 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

1.5.3 决定 CP 符合策略的人

SHECA 安全认证委员会决定本 CP 的符合性和可用性。。

1.5.4CP 批准程序

本 CP 由 SHECA 安全认证委员会批准，包括本 CP 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 CP 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：

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、电子认证业务规则、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。

此外，SHECA 在其网站的固定位置 www.sheca.com/repository 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 至少在 7 天以内发布一次订户证书的证书撤销列表（CRL），应至少每 12 个月发布一次子 CA 证书（Sub-CA Certificate）的证书撤销列表（ARL），如果根证书被撤销，应及时在网站公布撤销信息。

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）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本 CP 制定的 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。

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络主机服务器、互联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

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题甄别名的证书。

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。

3.1.7 商标的识别、鉴别和角色

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。

在对机构身份进行鉴别时，鉴别流程应当明确记录在 CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第十一部分的要求相一致。当证书中包含国际化域名（internationalized domain names，IDNs）时应阻止国际化域名的同形异义欺骗（homographic spoofing）。

3.2.3 个人身份的鉴别

EV 证书不接受个人申请。

3.2.4 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。

3.2.5 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

3.2.6 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

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 发布的指南第十部分的要求相一致。

申请者应事先了解订户协议、本 CP 及相应 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

（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

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，

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。在用户提交资料完整有效的情况下，通常在 5 个工作日以上，不超过 10 个工作日。

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 12 部分的要求相一致。

4.3.2CA 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

4.4.2CA 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。

4.4.3CA 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、本 CP 和相关 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本 CP 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。
- 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。

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。

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。

4.6.6CA 对更新证书的发布

不适用。

4.6.7CA 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 和 4.3 的规定对证书密钥更新进行用户身份鉴别和识别以及证书签发。

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。

4.7.6CA 对密钥更新证书的发布

同 4.4.2。

4.7.7CA 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，如证书中包含的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。

4.8.6CA 对变更证书的发布

不适用。

4.8.7CA 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 13 部分的要求相一致。

4.9.1 证书撤销的情形

发生下列情形，订户证书可以被撤销：

- 订户提出吊撤要求；
- 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，证书申请材料中存在虚假信息，或证书申请未被有效授权；
- 乙方 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；
- 乙方未按照 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
- 证书未被正确使用，证书被滥用或被用于非法用途；
- 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；
- SHECA 确认订户违背了本 CP 及相应 CPS、订户等规定的义务、陈述或担保，或者订

户无法履行协议规定的义务；

- 订户没有履行付费义务；
- 继续使用证书将会对 SHECA 产生损害；
- SHECA EV Root 证书或 EV 子 CA 证书相对应的私钥出现安全风险，或 SHECA 不再具备签发 EV 证书的权利或资质，或 SHECA 发现签发证书时未遵循《指南》或 SHECA 的 EV 证书政策；
- 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
- 司法机构的判决导致证书可信度被削弱或被无法被信任，或法律法规直接或间接的规定和要求；
- 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；
- SHECA 将在 7 天内撤销任何违反 EV Guideline 及 SHECA EV CP/CPS 的要求的中级根证书。具体请参见《协卡网络信任服务体系 EV 证书认证业务规则》。

4.9.2 要求证书撤销的实体

下列实体能够要求吊销证书：

- 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

只有 SHECA 可以吊销根证书或者子 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。

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。

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 对此不强制进行规定。

4.9.5CA 必须处理撤销请求的时间

SHECA 在收到撤销请求后应采取合理的步骤进行处理，不得进行拖延。

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。

4.9.7CRL 签发频率

对于订户证书，SHECA 至少每 7 天签发和公布一次证书撤销列表，对于子 CA 证书，至少每 12 个月签发和公布一次证书撤销列表。

CRL 签发频率应当明确记录在 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 13 部分的要求相一致。

4.9.8CRL 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 13 部分的要求相一致。

4.9.10 在线撤销检查的要求

依赖方在依赖证书前必须检查该证书状态。如果依赖方没有检查打算依赖的证书的 CRL，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 CA 的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。

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 发布的指南第 13 部分的要求相一致。

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 的操作都应在受到物理保护的建筑环境内进行，可以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。

5.1.3 电力和空调

CA 和 RA 的安全设施应配备主备电源确保持续、不间断的电力供应。此外，还应配备主备空调系统以控制温度和相对湿度。

5.1.4 防水措施

CA 和 RA 的安全设施应通过建筑、设备装配和可行措施等防止洪水或其它水患造成的损害。

5.1.5 火灾预防与保护

CA 和 RA 的安全设施应通过建筑、设备装配和可行措施等防止和扑灭火灾或或其它烟雾、火苗造成的损害。

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

CA 和 RA 应保护备份关键系统数据或敏感信息的磁性存储免受水、火或其它物理因素的损害，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

CA 和 RA 应执行废物（纸张、介质或其它任何废物）处理流程，以防止对包含机密或隐私信息的废物进行未经授权的使用、访问或披露。

5.1.8 异地备份

CA 和 RA 应采取安全的异地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。

5.2 程序控制（流程控制、过程控制）

5.2.1 可信角色

被指定为管理基础设施可信性的员工、承包商和顾问等应当被视作在受信岗位上的可信人员，成为可信人员必须满足本 CP 筛选要求。

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，包括：

- 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
- 系统管理人员
- 被指定的工程技术人员
- 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。

证书验证和签发等其它人工操作，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。

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，需要采取身份标识证件、智能卡或 USB Key 等令牌、身份验证密码等方式，进行严格的角色授权和身份识别。身份鉴别应包括人力资源和安全检查，并按照本 CP 规定的流程进一步进行背景调查。

5.2.4 需要职责分割的角色

包括但不限于下列角色需要进行任务分割：

- 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
- 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 系统上线进入生产环境

5.3 人员控制

人员控制应当明确记录在 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 14.1 部分的要求相一致。

5.3.1 资格、经历和清白要求

SHECA 的工作人员需要具备诚实可信、热情工作的性格和相应的教育背景，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。

担任系统管理、证书管理和内审控制的人员，必须具备相应的工作经验并了解认证服务相关知识和技能。

5.3.2 背景调查程序

SHECA 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，由人事部门和业务部门根据调查内容不同分别进行。

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

解决包含下列与特定环境相关的人员被训练因素

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：

- UNTSH 证书策略和电子认证业务规则
- 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。

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。

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。

5.3.7 独立合约人的要求

只有在必要的情况下，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。

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。

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，都应该包含事件发生的的日期和时间、导致事件发生的实体身份。CA 应在 CPS 中声明所记录的日志和事件类型：

- 运行事件，包括但不限于 CA 和子 CA 密钥的生成，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
- 可信人员事件，包括但不限于登录和登出尝试，口令创建、删除和设置，用户的系统权限变更，和人事变动
- 事故报告，包括但不限于未经授权的系统和网络登录尝试
- 证书和信息库读写操作的失败
- 证书生成政策的变更，例如变更有效期
- 物理和环境管理

5.4.2 处理日志的频率

认证机构应定期检查审计日志，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。

审查频率不低于一年两次。

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。

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。

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。

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：

- 5.4 收集的审计数据
- 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吊销后开始计算。

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。

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。

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。

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。

5.6 密钥变更

SHECA 定期对 CA 证书进行更新，密钥对最大生命期不超过 30 年。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

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。

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 16 部分的要求相一致。

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。

5.9 数据安全

数据安全应当明确记录在 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 16 部分的要求相一致。

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。

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。

6.1.4CA 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。

密钥长度应当明确记录在 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 9.5 部分的要求相一致。

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 签发的用户证书是 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。

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 CNS15135、ISO 19790 或 FIPS140-2 等级 3 硬件密码模块要求，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）

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可信人员持有，并存放于安全可控的环境中。

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 6.2.2 规定的方式以加密方式进行 CA 私钥的备份，私钥保护信息以秘密分割方式存入多张 IC 卡内由多人分别持有。 备份 CA 私钥的硬件密码模块要符合 6.2.6 的要求。

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。

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登出解除激活状态。

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 的公钥，包括所有根 CA 和子 CA 的公钥必须进行归档。

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。

根据密钥长度不同，密钥对有效期也相应不同：

- 4096 位 CA 密钥，最长允许使用年限是 30 年
- 2048 位 CA 密钥，最长允许使用年限是 27 年
- 2048 位订户密钥，最长允许使用年限是 27 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 IC 卡方式生成并采取多人分别持有方式进行。

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，IC 卡应设置 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，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 16.5 部分的要求相一致。

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。**（TCSEC C2）**

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，设计的产系统满足冗余性、容错性、模块化的要求。

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，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。

6.8 时间戳

不做规定。

7.证书、CRL 和 OCSP 描述（轮廓）

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。具体见附件：证书格式规范。

证书策略扩展应当明确记录在 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 9.3 部分的要求相一致。

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 9.3 部分的要求相一致。

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.509V2 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 RFC2560 定义的 V1 版本。

7.3.2OCSP 扩展项

OCSP 扩展项的使用符合 RFC 2560 规范。

8.审计和其它评估

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，并且熟悉本 CP 和相关 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

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。

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 200080
电话:（021）36393100 传真:(021)36393200
http://www.sheca.com/

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

9.6.1CA 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。

9.6.2RA 的陈述和担保

见 9.6.1 章节规定。

9.6.3 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

9.6.4 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。

9.6.5 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 CP 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。

根据本 CP 制定的 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 CP 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。

9.10.2 终止

本 CP 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 CP 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 CP 终止以后仍然继续有效存在。

本 CP 的效力，一直延续到按照本 CP 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 CP，每年至少审查一次本 CP 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 CP 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 CP 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 CP 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 CP。

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 CP 进行修改：

- 密码技术出现重大发展，足以影响现有 CP 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 CP 出现重要缺陷

9.12.4 对象标识符变更

当本 CP 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 CP 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 CP 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 CP 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 CP 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 CP 和依据本 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。

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，发起或传递证书吊销请求，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 CP 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。